



UNICORN IT GROUP

Case Study Booklet

Better-connected workplaces. Stronger protection. Less IT drama.

64 public projects across Australia and beyond — from remote connectivity and office fit-outs to cloud migration, managed IT and cyber security.



What we did. Why it mattered. What we used.

A project-by-project account of the problems we were asked to solve, the work delivered and the outcomes recorded.

The right solution starts with the problem

A faster internet plan is not always the answer to unreliable Wi-Fi. A new laptop does not replace a security programme. Moving files to the cloud is not the same as backing them up. The projects in this booklet show how those pieces fit together.

One team, across the working environment

- Managed IT and support for staff, devices and business services.
- Cyber security, identity protection, backup and recovery.
- Office networks, wireless, structured cabling and national connectivity.
- Cloud migration, Microsoft 365 and server modernisation.
- Business phones, collaboration, surveillance and workplace fit-outs.

About the project accounts

This edition contains the public case studies currently published by Unicorn IT Group. Private case studies and withdrawn projects are excluded. Client identities are anonymised where the project record does not name them. Pictures are existing project illustrations or supplied diagrams; they are not presented as photographs of client premises.

Delivery statements and outcome figures come from those existing project records. The added “why” and technology explanations describe the design rationale, not additional work or independently audited performance. Project results are historical, not guarantees for another environment. Product availability, carriers and support arrangements must be scoped for a new engagement.

Testimonials have been omitted from this edition rather than presenting unattributed quotes as verified endorsements.

PROJECT DIRECTORY

Find your next conversation

The right solution starts with the problem 2

Improving Internet on the Unicorn Farm 7

Built Private P2P Wireless Network in a Closed Mining Town 10

Printer Replacement at School 13

Medical Company Deployed 400 HP EliteBooks for Department of Health Contract 16

Not-for-Profit Unlocked Cheaper Office 365 Licences 19

Managed Services for a Freight Company in Welshpool 22

Moved an Entire Office Over One Weekend 27

Childcare Centre Secured Exits and Outdoor Areas with Meraki Cameras 30

Improving Customers Wireless and Internet 33

Global File Servers to SharePoint & Teams 36

Moved to WatchGuard Firewall for Secure Office Access 39

Essential Eight Security Uplift for a Law Firm 42

Law Firm Grew Rapidly and Needed a New Office 45

Moved to 3CX Phone System from a Major Telco 48

Decommissioned 5 Servers — Full Cloud-First Migration 51

Moved Servers to Next DC Datacenters 54

Replaced 40 Machines at a Local Shire 57

Connected Rear Warehouse with Fibre 60

Migrated 90 Servers to Cove Backup	63
Migrated 1000 Users from On-Premise Exchange 2019 to Office 365	66
Migrated 3000 Users from 15 Exchange 2013 Servers to Office 365	69
Migrated 2000 Virtual Servers to Azure and Decommissioned On-Premise VMware	72
10 Gbps Wavelength to the USA for a 3D Graphics and Movie Studio	75
Customer Wireless Rollout for a Regional Shopping Centre	78
30 Virtual Machines Migrated from VMware to Hyper-V for a Home Builder	81
Hyper-V Replication Across Two Next DC Data Centres	84
Free Passenger Wi-Fi at a Remote Airport via Bonded Starlink	87
Manufacturing Company Stopped Data Leaks with DLP in Days	90
Connected 3 Home Builder Offices with Dedicated Gigabit Air Fibre	94
Connected Display Homes to a Next DC Data Centre with Cisco Meraki SD-WAN	99
Remote Water Monitoring and Gate Control Over Starlink SD-WAN	103
Bonded Starlink and Guest Wi-Fi for an Outback Roadhouse	106
Farm-Wide Wi-Fi and Meraki Cameras for a Unicorn Farmer	109
3CX Phone System Connecting 32 Healthcare Sites Across Australia	112
Point-to-Point Wireless Link from Manager's Home to Office	116
Data Cabling, Ubiquiti PoE Network and 40 Meraki Cameras for a Local Supermarket	119
Manufacturing Company Server-to-Cloud Migration with Azure and Microsoft 365	122
Swoop Enterprise Ethernet NBN and Ubiquiti Upgrade for a Marketing Agency	125
School Saves \$2,000/Month by Switching to Swoop 1 Gbps Enterprise Ethernet NBN	129
Network Rebuild for a Financial Services Provider After Storm Damage	133

Wi-Fi 7 Upgrade for an MCG-Sized Warehouse	137
Attackers Caught Minutes After Guardz 24/7/365 MDR Deployment	142
Starlink and Ubiquiti Wireless for a Remote Cattle Station	146
New Office 365, Entra AD and Endpoint Manager Environment for a Drone Data Company	150
National Home Builder Turnaround After Malware Incident	156
100 Gbps Dark Fibre Link for Medical Research Campus	166
6-Hop Solar Microwave Network Delivers 100 Mbps Fibre to Remote Mine Site	170
Secure Public Wi-Fi Rolled Out Across 4 Employment Services Offices in Hobart	174
Small Real Estate Agency Moves to Fully Cloud Managed IT on the Silver Plan	178
New Motel Delivers Fast Guest Wi-Fi Across 100 Rooms	182
Industrial Estate Connected with P2P Wireless and Bonded SHDSL Before NBN	186
95 Meraki Cameras Secure an Exclusive Golf Course	190
Restaurant Fixed Poor Wi-Fi Coverage for Guest Wireless and Tablet Ordering	194
Local Cricket Club Recovered from a Business Email Compromise and Modernised Its IT	198
Local Vet Clinic Moved Into a Brand-New Building with a Complete IT Fit-out	204
New Doctor Surgery Opens with Full Cloud-First IT Setup	210
30 km Haul Road CCTV and Fibre Network for a Mine Site	216
Regional Vet Clinic Upgraded to Swoop Enterprise Ethernet and Ubiquiti	220
Dark Fibre Links a Laser Steel Factory 19 km From Its Office	224
Legal Firm IT Upgrade: 1.8 TB File Server Moved to Microsoft Teams	228
Mining Company Migrated 1200 Users from Exchange 2013 to Office 365	234

Print Publisher Gets 1 Gbps Swoop FTTP and Moves from POP3 to Office 365 239

Hyper-V and Synology Cluster Replicated Across Two NEXTDC Datacentres 244

New Doctor Surgery in Perth Fitted Out and Placed on Gold Managed Services 250

Let’s make your IT the quiet part of the day 257

PROJECT 01 / RURAL & AGRICULTURE

Improving Internet on the Unicorn Farm

Rural connectivity

A working farm spread across several sheds and a homestead was running the whole business on one weak connection at the house. Payroll, livestock software and cameras all fought for the same trickle of bandwidth.



The issues we needed to solve

- Single fixed wireless service at the homestead with no coverage past the first shed
- Office staff dropping out of cloud accounting and video calls several times a day
- Security cameras and weather sensors offline whenever anyone streamed or backed up
- No failover, so a single outage stopped orders and deliveries for the day

PROJECT 01 / DELIVERY

What we did — and why

01 / The work delivered

Site survey of every building, yard and shed with signal mapping before quoting anything

Why this mattered: Starting with the actual site and workload reduces the risk of buying equipment that cannot solve the underlying problem.

02 / The work delivered

Installed NBN Enterprise Ethernet from Swoop, our partner ISP

Why this mattered: Reliable connectivity is the foundation for the applications above it; changing software cannot repair an inadequate physical or network path.

03 / The work delivered

Upgraded the primary service and added a 4G/5G failover that switches over automatically

Why this mattered: The business needs a path through equipment or connection failures rather than making one component a single point of interruption.

04 / The work delivered

Point-to-point wireless links from the homestead to the machinery shed and packing shed

Why this mattered: Reliable connectivity is the foundation for the applications above it; changing software cannot repair an inadequate physical or network path.

05 / The work delivered

New router with traffic shaping so business apps get priority over streaming and backups

Why this mattered: A recoverable copy must exist independently of the production service; synchronising files alone is not a recovery strategy.

06 / The work delivered

Separate networks for staff, guests, cameras and farm sensors

Why this mattered: Guests, cameras and business systems have different trust levels, so they should not inherit unrestricted access to each other.

PROJECT 01 / BUSINESS RESULT

What changed for the business

6x

usable bandwidth at the sheds

99.9%

uptime with automatic failover

0

dropped calls reported since cutover

What we used — and its role

Swoop

The recorded carrier service provides the WAN connection; routing, wireless and user support remain separate design decisions.

The sales conversation

If your organisation recognises these same issues, start with the constraint rather than a product list: which part of the environment interrupts staff, exposes data or makes growth harder? We can review the current setup, identify dependencies and scope the relevant services before recommending a change.



A word from the stable

The right connection makes the rest of the office happier.

1300 904 635 | hello@uitg.com.au

PROJECT 02 / MINING & RESOURCES

Built Private P2P Wireless Network in a Closed Mining Town

Private wireless ISP

A closed mining town had no usable telco infrastructure and overloaded 5G, leaving 200 homes and small businesses without reliable internet. We designed and built a private point-to-point wireless network from a hilltop POP to every property.



The issues we needed to solve

- No telco willing to install fixed infrastructure in the closed town and NBN only wanted to install wireless
- 5G was overloaded and unusable for everyday work, streaming and payments
- 200 homes plus a cafe, general store, school, post office, restaurants, gym, rec center, child care center, pubs, healthcare center and fuel station needed reliable connectivity
- Network had to be completely isolated from the mining company's corporate traffic
- Town needed enough bandwidth for modern household and small-business use

PROJECT 02 / DELIVERY

What we did — and why

01 / The work delivered

Built a point-of-presence (POP) tower on a hill overlooking the town

Why this mattered: This workstream addressed the mining & resources operation's need for a maintainable service rather than leaving the original limitation in place.

02 / The work delivered

Installed two separate 1 Gbps network breakouts from the mining company, fully segregated from corporate traffic

Why this mattered: This workstream addressed the mining & resources operation's need for a maintainable service rather than leaving the original limitation in place.

03 / The work delivered

Deployed point-to-point wireless links from the POP to each house and business

Why this mattered: Reliable connectivity is the foundation for the applications above it; changing software cannot repair an inadequate physical or network path.

04 / The work delivered

Installed a UniFi UCG router at every home and small business for local routing and Wi-Fi

Why this mattered: This workstream addressed the mining & resources operation's need for a maintainable service rather than leaving the original limitation in place.

05 / The work delivered

Engineered the network so every property can push at least 500 Mbps back to the POP

Why this mattered: This workstream addressed the mining & resources operation's need for a maintainable service rather than leaving the original limitation in place.

06 / The work delivered

Set up monitoring and remote management so issues can be diagnosed without a site visit

Why this mattered: Installing a system is not the end of the security job: visibility and control are needed while staff continue to use it.

PROJECT 02 / BUSINESS RESULT

What changed for the business

200+

homes and businesses connected

500Mbps

minimum speed to the POP per property

2x 1Gbps

segregated internet breakouts at the tower

What we used — and its role

Ubiquiti / UniFi

Centrally managed switching, routing or wireless can be maintained as one office-network platform rather than as disconnected devices.

The sales conversation

If your organisation recognises these same issues, start with the constraint rather than a product list: which part of the environment interrupts staff, exposes data or makes growth harder? We can review the current setup, identify dependencies and scope the relevant services before recommending a change.



A word from the stable

A stronger signal beats shouting at the router.

1300 904 635 | hello@uitg.com.au

PROJECT 03 / EDUCATION

Printer Replacement at School

Managed print

A school was relying on 38 ageing printers spread across classrooms, offices and staff rooms. Devices were unreliable, expensive to run, and impossible to track. We partnered with Konica to replace the entire fleet and introduce secure swipe-badge print counting for students and teachers.



The issues we needed to solve

- 38 older printers failing regularly and costing more in toner and repairs each term
- No visibility into who was printing, how much, or where costs were going
- Printers placed in the wrong spots, causing congestion and wasted staff time
- Students and teachers sharing open print queues with no accountability
- Sustainability targets undermined by abandoned print jobs and unnecessary colour printing

PROJECT 03 / DELIVERY

What we did — and why

01 / The work delivered

Worked with Konica to audit every printer, page count, location and usage pattern

Why this mattered: Starting with the actual site and workload reduces the risk of buying equipment that cannot solve the underlying problem.

02 / The work delivered

Right-sized the fleet and repositioned devices where staff and students actually print

Why this mattered: A consistent device baseline makes deployment and ongoing support more predictable for staff and the service team.

03 / The work delivered

Replaced all 38 printers with modern, efficient multifunction devices

Why this mattered: A consistent device baseline makes deployment and ongoing support more predictable for staff and the service team.

04 / The work delivered

Introduced secure print release using student and teacher swipe badges

Why this mattered: This workstream addressed the education operation's need for a maintainable service rather than leaving the original limitation in place.

05 / The work delivered

Configured per-user and per-department print counting with clear reporting

Why this mattered: This workstream addressed the education operation's need for a maintainable service rather than leaving the original limitation in place.

06 / The work delivered

Set up follow-me printing so jobs release at the nearest printer and uncollected jobs never print

Why this mattered: This workstream addressed the education operation's need for a maintainable service rather than leaving the original limitation in place.

PROJECT 03 / BUSINESS RESULT

What changed for the business

38

old printers replaced

100%

badge-secured print release

40%

estimated reduction in wasted prints

What we used — and its role

Konica / managed print

A managed print platform brings device support and print administration into a maintainable workplace service.

The sales conversation

If your organisation recognises these same issues, start with the constraint rather than a product list: which part of the environment interrupts staff, exposes data or makes growth harder? We can review the current setup, identify dependencies and scope the relevant services before recommending a change.



A word from the stable

Old dependencies don't retire themselves.

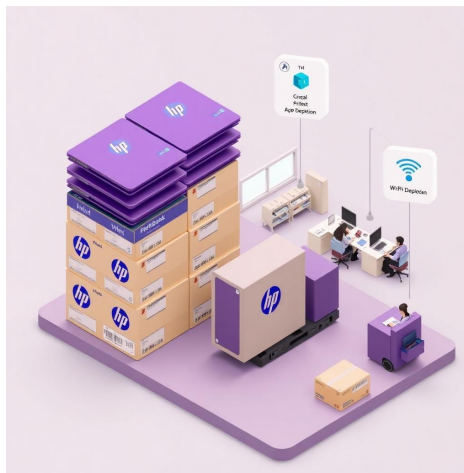
1300 904 635 | hello@uitg.com.au

PROJECT 04 / HEALTHCARE

Medical Company Deployed 400 HP EliteBooks for Department of Health Contract

Endpoint deployment

A medical company awarded a major contract by the Australian Department of Health needed 400 HP EliteBooks delivered fast to new staff across the country. We supplied the machines, accessories and asset labels, then configured Windows Autopilot policies in Microsoft Endpoint Manager so every laptop was ready to work straight out of the box.



The issues we needed to solve

- 400 new staff needed fully configured laptops before contract commencement
- No central IT team at every location to unbox, image and install software manually
- Medical compliance required consistent app deployment, security settings and asset tracking
- Previous device rollouts had caused delays, incorrect builds and missing accessories
- Staff were spread geographically and needed a zero-touch experience

PROJECT 04 / DELIVERY

What we did — and why

01 / The work delivered

Procured 400 HP EliteBooks with carry bags, extra chargers and pre-printed asset labels

Why this mattered: This workstream addressed the healthcare operation's need for a maintainable service rather than leaving the original limitation in place.

02 / The work delivered

Coordinated drop-ship direct from the supplier to each staff member's address

Why this mattered: This workstream addressed the healthcare operation's need for a maintainable service rather than leaving the original limitation in place.

03 / The work delivered

Captured hardware hashes and imported every device into Microsoft Endpoint Manager

Why this mattered: A consistent device baseline makes deployment and ongoing support more predictable for staff and the service team.

04 / The work delivered

Created Autopilot deployment profiles and dynamic device groups for the medical company

Why this mattered: A consistent device baseline makes deployment and ongoing support more predictable for staff and the service team.

05 / The work delivered

Built Endpoint Manager policies to push required healthcare apps, VPN, security baselines and Wi-Fi profiles

Why this mattered: This workstream addressed the healthcare operation's need for a maintainable service rather than leaving the original limitation in place.

06 / The work delivered

Tested the end-to-end experience on pilot devices before the bulk shipment

Why this mattered: A consistent device baseline makes deployment and ongoing support more predictable for staff and the service team.

PROJECT 04 / BUSINESS RESULT

What changed for the business

400

HP EliteBooks drop-shipped to staff

0

manual imaging or site visits required

Same day

productive once connected to Wi-Fi

What we used — and its role

Intune / Autopilot

Policy-driven deployment helps standardise devices and reduces manual setup when a user receives a replacement computer.

HP / Microsoft Surface

Business-class devices matched to staff roles create a more supportable endpoint estate than inconsistent personal or ageing computers.

The sales conversation

If your organisation recognises these same issues, start with the constraint rather than a product list: which part of the environment interrupts staff, exposes data or makes growth harder? We can review the current setup, identify dependencies and scope the relevant services before recommending a change.



A word from the stable

Old dependencies don't retire themselves.

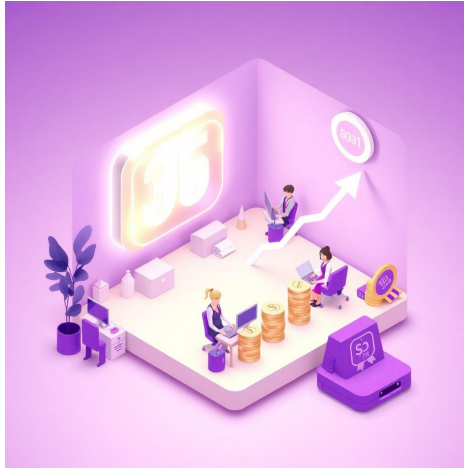
1300 904 635 | hello@uitg.com.au

PROJECT 05 / NOT-FOR-PROFIT

Not-for-Profit Unlocked Cheaper Office 365 Licences

Microsoft 365 licensing

A not-for-profit had been buying Office 365 the same way as a regular business and had no idea discounted nonprofit pricing existed. We reviewed their tenancy, moved them to the correct licensing model, and cut their annual bill by \$30,000 without removing a single feature.



The issues we needed to solve

- Not-for-profit was paying standard commercial rates for Microsoft 365
- No internal awareness of nonprofit eligibility or discounted licensing programs
- Budget pressure meant every dollar spent on software was a dollar away from their cause
- Existing licences were a mix of plans with overlapping features and wasted spend
- Leadership feared changing licences would disrupt staff email, files and Teams

PROJECT 05 / DELIVERY

What we did — and why

01 / The work delivered

Audited the current Microsoft 365 tenant, user roles and licence assignments

Why this mattered: Starting with the actual site and workload reduces the risk of buying equipment that cannot solve the underlying problem.

02 / The work delivered

Confirmed eligibility for Microsoft nonprofit pricing and verified organisation status

Why this mattered: Correct licensing addresses entitlement and predictable administration, rather than leaving the organisation reliant on unsupported or inconsistent software access.

03 / The work delivered

Right-sized every user to the cheapest plan that still covered their needs

Why this mattered: This workstream addressed the not-for-profit operation's need for a maintainable service rather than leaving the original limitation in place.

04 / The work delivered

Removed duplicate or unused licences and cleaned up inactive accounts

Why this mattered: This workstream addressed the not-for-profit operation's need for a maintainable service rather than leaving the original limitation in place.

05 / The work delivered

Managed the licence transition out of hours to avoid any downtime

Why this mattered: This workstream addressed the not-for-profit operation's need for a maintainable service rather than leaving the original limitation in place.

06 / The work delivered

Documented the new licence model so future hires stay on the right plan

Why this mattered: The improvement must remain usable and supportable after handover, not depend on knowledge held only by the installer.

PROJECT 05 / BUSINESS RESULT

What changed for the business

\$30,000

saved every year in licence costs

0

features or mailboxes lost

Same day

transition completed with no downtime

What we used — and its role

Microsoft 365

Cloud email and collaboration reduce dependence on local mail servers and make access and administration consistent across devices.

The sales conversation

If your organisation recognises these same issues, start with the constraint rather than a product list: which part of the environment interrupts staff, exposes data or makes growth harder? We can review the current setup, identify dependencies and scope the relevant services before recommending a change.



A word from the stable

Old dependencies don't retire themselves.

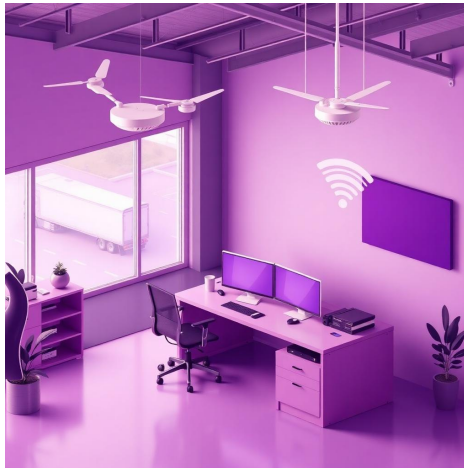
1300 904 635 | hello@uitg.com.au

PROJECT 06 / TRANSPORT & LOGISTICS

Managed Services for a Freight Company in Welshpool

Managed services

A freight company moved into a new office in Welshpool, Perth, with 12 staff, 12 machines, and a mix of Office 365, Xero and other SaaS apps. We delivered a complete managed IT setup including Swoop 250/250 Mbps NBN, Ubiquiti Wi-Fi across the office and yard, a UniFi Cloud Gateway, 3CX phone system, Guardz MDR security, and web hosting.



The issues we needed to solve

- New office had no internet, network or phone system in place before move-in
- Staff relied on Office 365, Xero and other SaaS apps that needed reliable, fast connectivity
- Yard and warehouse areas needed Wi-Fi coverage for handheld scanners, tablets and driver devices
- No internal IT resource to manage endpoints, backups, email security or support requests
- Business needed a professional phone system with hunt groups, voicemail and mobile softphones

PROJECT 06 / DELIVERY

What we did — and why

01 / The work delivered

Provisioned Swoop 250 Mbps symmetrical NBN Enterprise Ethernet for the Welshpool office

Why this mattered: Reliable connectivity is the foundation for the applications above it; changing software cannot repair an inadequate physical or network path.

02 / The work delivered

Installed a UniFi Cloud Gateway as the core router, firewall and VPN gateway

Why this mattered: Moving the workload or retiring obsolete dependencies reduces the amount of legacy infrastructure the business still has to operate.

03 / The work delivered

Deployed three Ubiquiti access points to cover the office, warehouse and truck yard with one seamless network

Why this mattered: This workstream addressed the transport & logistics operation's need for a maintainable service rather than leaving the original limitation in place.

04 / The work delivered

Configured a cloud-hosted 3CX phone system with desk phones, softphones and SIP trunks

Why this mattered: Communications need to follow how people work, with maintainable routing and extensions instead of the limitations of the old phone arrangement.

05 / The work delivered

Onboarded all 12 machines to our managed service with SentinelOne endpoint security and Guardz 24/7/365 MDR

Why this mattered: Installing a system is not the end of the security job: visibility and control are needed while staff continue to use it.

06 / The work delivered

Set up web hosting and domain DNS management for the company website and email

Why this mattered: This workstream addressed the transport & logistics operation's need for a maintainable service rather than leaving the original limitation in place.

07 / The work delivered

Enabled Office 365 backup and recovery independent of Microsoft's native retention

Why this mattered: A recoverable copy must exist independently of the production service; synchronising files alone is not a recovery strategy.

08 / The work delivered

Delivered ongoing help desk support with a single account engineer and monthly reporting

Why this mattered: This workstream addressed the transport & logistics operation's need for a maintainable service rather than leaving the original limitation in place.

PROJECT 06 / BUSINESS RESULT

What changed for the business

12 users and machines fully managed	250/250Mbps symmetrical Swoop NBN connection
3 Ubiquiti access points covering office and yard	1 cloud-hosted 3CX phone system
24/7 Guardz 24/7/365 MDR threat monitoring	

What we used — and its role

SentinelOne

Endpoint detection and response helps identify suspicious activity on computers and supports investigation and containment.

Guardz

Managed detection and response adds ongoing threat review and response beyond a one-off security installation.

Ubiquiti / UniFi

Centrally managed switching, routing or wireless can be maintained as one office-network platform rather than as disconnected devices.

Microsoft 365

Cloud email and collaboration reduce dependence on local mail servers and make access and administration consistent across devices.

3CX

A software-based phone system supports central call routing and flexible extensions without preserving the old PBX operating model.

Swoop

The recorded carrier service provides the WAN connection; routing, wireless and user support remain separate design decisions.

The sales conversation

If your organisation recognises these same issues, start with the constraint rather than a product list: which part of the environment interrupts staff, exposes data or makes growth harder? We can review the current setup, identify dependencies and scope the relevant services before recommending a change.



A word from the stable

Less IT drama. More getting on with the day.
1300 904 635 | hello@uitg.com.au

PROJECT 06 / QUESTIONS

A closer look at the solution

Why did the freight company choose managed services instead of hiring internally?

With only 12 users, a full-time IT employee was not cost-effective. Our managed service gives them enterprise-grade tools, security monitoring and help desk coverage for a predictable monthly fee.

How does the yard get reliable Wi-Fi?

We positioned three Ubiquiti access points to cover the office, warehouse and outdoor yard. Devices like tablets and handheld scanners roam seamlessly between them.

What happens if the NBN connection goes down?

The UniFi Cloud Gateway supports automatic 4G/5G failover with an optional USB modem. We can also add a second NBN link for higher availability if the business grows.

Is the 3CX phone system tied to the office?

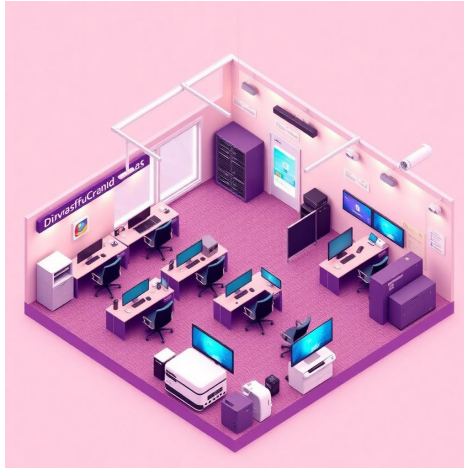
No. Staff can use 3CX softphones on their mobiles and laptops, so drivers, warehouse staff and admin can all stay reachable whether they are on-site or on the road.

PROJECT 07 / PROFESSIONAL SERVICES

Moved an Entire Office Over One Weekend

Office relocation & fitout

A business had to vacate its old office and be fully operational in a new building by Monday morning. We planned, packed, cabled and commissioned a complete technology environment over a single weekend so staff walked in and started work on time.



The issues we needed to solve

- Hard move-out deadline from the existing landlord with no option to extend
- New office needed a full network, internet, Wi-Fi, meeting rooms and desks before staff arrived
- No time to troubleshoot after go-live; everything had to work first thing Monday
- Security, printers and voice systems had to be online with the same numbers and access
- Staff expected the same or better experience from day one

PROJECT 07 / DELIVERY

What we did — and why

01 / The work delivered

Pre-staged all equipment, desks, chairs, monitors, docks and cables before the weekend

Why this mattered: Installing a system is not the end of the security job: visibility and control are needed while staff continue to use it.

02 / The work delivered

Installed a new WatchGuard firewall with segmented networks for staff, guests, voice and security

Why this mattered: Guests, cameras and business systems have different trust levels, so they should not inherit unrestricted access to each other.

03 / The work delivered

Deployed Ubiquiti switching and Wi-Fi with a full site survey for coverage and capacity

Why this mattered: Starting with the actual site and workload reduces the risk of buying equipment that cannot solve the underlying problem.

04 / The work delivered

Built 8 Microsoft Teams Rooms with displays, microphones, cameras and one-touch join

Why this mattered: Communications need to follow how people work, with maintainable routing and extensions instead of the limitations of the old phone arrangement.

05 / The work delivered

Installed and configured 4 managed printers with secure follow-me release

Why this mattered: This workstream addressed the professional services operation's need for a maintainable service rather than leaving the original limitation in place.

06 / The work delivered

Fitted door access control and CCTV cameras for physical security and after-hours monitoring

Why this mattered: Installing a system is not the end of the security job: visibility and control are needed while staff continue to use it.

07 / The work delivered

Cut over internet and voice services out of hours and tested every desk and room before staff arrived

Why this mattered: This workstream addressed the professional services operation's need for a maintainable service rather than leaving the original limitation in place.

PROJECT 07 / BUSINESS RESULT

What changed for the business

1 weekend to complete the entire move	8 Teams Rooms ready on Monday
4 secure managed printers deployed	100% of staff productive from the first morning

What we used — and its role

WatchGuard

A managed firewall platform combines traffic control, secure access and, where deployed, SD-WAN policy in a consistent operating model.

Ubiquiti / UniFi

Centrally managed switching, routing or wireless can be maintained as one office-network platform rather than as disconnected devices.

SharePoint / Teams / OneDrive

Shared cloud workspaces separate business files and collaboration from a single office server or an individual computer.

The sales conversation

If your organisation recognises these same issues, start with the constraint rather than a product list: which part of the environment interrupts staff, exposes data or makes growth harder? We can review the current setup, identify dependencies and scope the relevant services before recommending a change.



A word from the stable

Old dependencies don't retire themselves.

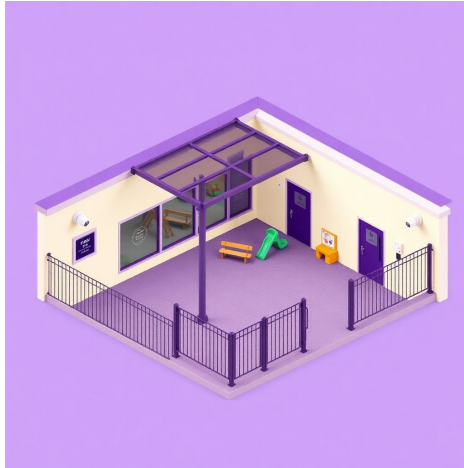
1300 904 635 | hello@uitg.com.au

PROJECT 08 / CHILDCARE & EARLY LEARNING

Childcare Centre Secured Exits and Outdoor Areas with Meraki Cameras

Cloud CCTV & child safety

A childcare centre needed reliable cameras to monitor entries, exits and outdoor public play areas without a complicated on-premise recorder. We installed Meraki cloud-managed cameras with onboard storage and a central portal so authorised staff can review footage securely from anywhere.



The issues we needed to solve

- No visibility of who was entering or leaving the centre at any time
- Outdoor play areas and car park were not covered by existing cameras
- Old DVR system was unreliable and slow to retrieve incident footage
- Staff needed secure remote access for management and compliance reviews
- Privacy and data retention requirements for children and families

PROJECT 08 / DELIVERY

What we did — and why

01 / The work delivered

Site survey of every gate, door, playground, path and car park area

Why this mattered: Starting with the actual site and workload reduces the risk of buying equipment that cannot solve the underlying problem.

02 / The work delivered

Installed Meraki cloud-managed cameras with onboard storage at key entry and exit points

Why this mattered: Moving the workload or retiring obsolete dependencies reduces the amount of legacy infrastructure the business still has to operate.

03 / The work delivered

Added weatherproof cameras to cover outdoor public play spaces and parking

Why this mattered: Coverage and controlled access make surveillance useful to the operation, rather than simply increasing the number of cameras.

04 / The work delivered

Configured a role-based cloud portal so only authorised staff can view or export footage

Why this mattered: Moving the workload or retiring obsolete dependencies reduces the amount of legacy infrastructure the business still has to operate.

05 / The work delivered

Segregated camera traffic onto a dedicated, secure network

Why this mattered: Coverage and controlled access make surveillance useful to the operation, rather than simply increasing the number of cameras.

06 / The work delivered

Set retention policies and mobile app access so incident clips can be found and shared quickly

Why this mattered: This workstream addressed the childcare & early learning operation's need for a maintainable service rather than leaving the original limitation in place.

PROJECT 08 / BUSINESS RESULT

What changed for the business

100%

entry and exit coverage

<2 min

to locate and share incident footage

30 days

onboard storage retention

What we used — and its role

Cisco Meraki

Cloud management gives the support team a common view of the deployed network or camera estate without needing to visit each location.

The sales conversation

If your organisation recognises these same issues, start with the constraint rather than a product list: which part of the environment interrupts staff, exposes data or makes growth harder? We can review the current setup, identify dependencies and scope the relevant services before recommending a change.



A word from the stable

The horn is optional. Layered protection isn't.

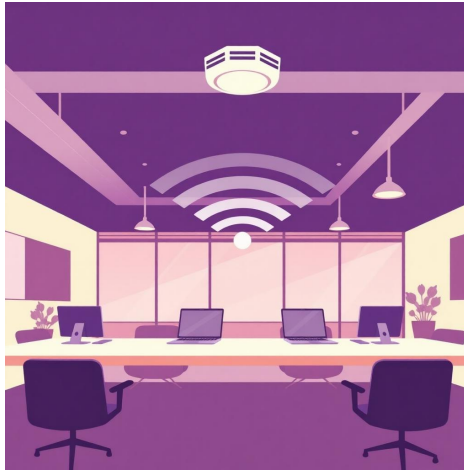
1300 904 635 | hello@uitg.com.au

PROJECT 09 / PROFESSIONAL SERVICES

Improving Customers Wireless and Internet

Wi-Fi & network upgrade

A multi-tenanted office with a customer-facing waiting area had consumer-grade access points bolted on over the years. Staff blamed the internet, but the real problem was the wireless design.



The issues we needed to solve

- Nine mismatched access points on overlapping channels causing constant reconnects
- Guests and staff sharing one flat network with one shared password
- Handheld scanners and EFTPOS terminals dropping mid-transaction
- No visibility on who or what was using the connection

PROJECT 09 / DELIVERY

What we did — and why

01 / The work delivered

Full wireless survey and heat map to find real dead spots and interference sources

Why this mattered: Starting with the actual site and workload reduces the risk of buying equipment that cannot solve the underlying problem.

02 / The work delivered

Replaced consumer gear with business access points on a properly planned channel layout

Why this mattered: This workstream addressed the professional services operation's need for a maintainable service rather than leaving the original limitation in place.

03 / The work delivered

Split traffic into staff, guest, payments and device networks with sensible limits

Why this mattered: Guests, cameras and business systems have different trust levels, so they should not inherit unrestricted access to each other.

04 / The work delivered

Guest portal with bandwidth caps so customers can browse without slowing the business

Why this mattered: Guests, cameras and business systems have different trust levels, so they should not inherit unrestricted access to each other.

05 / The work delivered

Cloud monitoring and alerting so we see a problem before staff report it

Why this mattered: Installing a system is not the end of the security job: visibility and control are needed while staff continue to use it.

PROJECT 09 / BUSINESS RESULT

What changed for the business

-92%

wireless drop-out tickets

3x

faster speeds on staff devices

1 day

install with no downtime in business hours

The sales conversation

If your organisation recognises these same issues, start with the constraint rather than a product list: which part of the environment interrupts staff, exposes data or makes growth harder? We can review the current setup, identify dependencies and scope the relevant services before recommending a change.



A word from the stable

A stronger signal beats shouting at the router.

1300 904 635 | hello@uitg.com.au

PROJECT 10 / INTERNATIONAL

Global File Servers to SharePoint & Teams

Cloud migration

A business with five on-premise file servers spread across the world was paying to maintain aging hardware while staff struggled to find the right version of any document.



The issues we needed to solve

- Five physical file servers in different countries, all out of warranty and nearing end of life
- No consistent backup or disaster recovery plan across sites
- Staff emailing files back and forth, creating duplicate and outdated versions
- VPN-only access for remote workers, causing slow performance and support tickets
- No central permissions model — every server had its own rules

PROJECT 10 / DELIVERY

What we did — and why

01 / The work delivered

Audited every server, share and permission set before touching any data

Why this mattered: Starting with the actual site and workload reduces the risk of buying equipment that cannot solve the underlying problem.

02 / The work delivered

Designed a clean Microsoft 365 information architecture with sites, libraries and channels mapped to how teams actually work

Why this mattered: Starting with the actual site and workload reduces the risk of buying equipment that cannot solve the underlying problem.

03 / The work delivered

Migrated data in phases by region, keeping each site live until cutover was verified

Why this mattered: Moving the workload or retiring obsolete dependencies reduces the amount of legacy infrastructure the business still has to operate.

04 / The work delivered

Set up SharePoint sync, Teams file tabs and retention labels so files stay organised by default

Why this mattered: Moving the workload or retiring obsolete dependencies reduces the amount of legacy infrastructure the business still has to operate.

05 / The work delivered

Trained each office on search, co-authoring and version history so old habits did not return

Why this mattered: The improvement must remain usable and supportable after handover, not depend on knowledge held only by the installer.

PROJECT 10 / BUSINESS RESULT

What changed for the business

5 → 0

on-prem file servers retired

100%

of staff with secure cloud access, no VPN required

-70%

file-related support tickets

What we used — and its role

Microsoft 365

Cloud email and collaboration reduce dependence on local mail servers and make access and administration consistent across devices.

SharePoint / Teams / OneDrive

Shared cloud workspaces separate business files and collaboration from a single office server or an individual computer.

The sales conversation

If your organisation recognises these same issues, start with the constraint rather than a product list: which part of the environment interrupts staff, exposes data or makes growth harder? We can review the current setup, identify dependencies and scope the relevant services before recommending a change.



A word from the stable

Old dependencies don't retire themselves.

1300 904 635 | hello@uitg.com.au

PROJECT 11 / PROFESSIONAL SERVICES

Moved to WatchGuard Firewall for Secure Office Access

Network security

A growing office was running on a basic ISP router with no real visibility into who or what was on the network. Staff needed secure, reliable access to cloud apps and the head office systems without the constant threat of malware or unauthorised devices.



The issues we needed to solve

- Consumer-grade router with default settings and no central security policy
- No separation between staff, guests, and sensitive company systems
- Infected devices and phishing links were reaching users unchecked
- Remote workers had no safe way into office resources
- No logging or alerting meant problems were only found after the damage was done

PROJECT 11 / DELIVERY

What we did — and why

01 / The work delivered

Replaced the ISP router with a WatchGuard Firebox sized for the office and expected growth

Why this mattered: This workstream addressed the professional services operation's need for a maintainable service rather than leaving the original limitation in place.

02 / The work delivered

Configured role-based network zones for staff, guests, servers, and voice/IoT devices

Why this mattered: Guests, cameras and business systems have different trust levels, so they should not inherit unrestricted access to each other.

03 / The work delivered

Enabled WatchGuard security services: antivirus, intrusion prevention, DNS filtering, and botnet protection

Why this mattered: This workstream addressed the professional services operation's need for a maintainable service rather than leaving the original limitation in place.

04 / The work delivered

Set up branch-office VPN and SSL-VPN access for remote and mobile staff

Why this mattered: This workstream addressed the professional services operation's need for a maintainable service rather than leaving the original limitation in place.

05 / The work delivered

Tuned alerting so the right people are notified without alert fatigue

Why this mattered: This workstream addressed the professional services operation's need for a maintainable service rather than leaving the original limitation in place.

PROJECT 11 / BUSINESS RESULT

What changed for the business

100%

of traffic inspected by the firewall

0

successful malware infections since cutover

24/7

visibility into network activity and threats

What we used — and its role

WatchGuard

A managed firewall platform combines traffic control, secure access and, where deployed, SD-WAN policy in a consistent operating model.

The sales conversation

If your organisation recognises these same issues, start with the constraint rather than a product list: which part of the environment interrupts staff, exposes data or makes growth harder? We can review the current setup, identify dependencies and scope the relevant services before recommending a change.



A word from the stable

The horn is optional. Layered protection isn't.

1300 904 635 | hello@uitg.com.au

PROJECT 12 / LEGAL

Essential Eight Security Uplift for a Law Firm

Cybersecurity & compliance

A busy law firm handling sensitive client matter needed more than antivirus. They wanted to meet the ACSC Essential Eight, protect client data, and satisfy their cyber insurance questionnaire without slowing their lawyers down.



The issues we needed to solve

- No formal patch management; applications and operating systems were updated ad-hoc
- Office macros were enabled by default, creating a common malware entry point
- Multi-factor authentication was not enforced across Microsoft 365 and remote access
- Backups existed but were never tested, and recovery time was unknown
- Staff had local administrator rights on their machines

PROJECT 12 / DELIVERY

What we did — and why

01 / The work delivered

Ran an Essential Eight maturity assessment to baseline the firm against ACSC guidelines

Why this mattered: Starting with the actual site and workload reduces the risk of buying equipment that cannot solve the underlying problem.

02 / The work delivered

Implemented application whitelisting and controlled Office macro settings

Why this mattered: This workstream addressed the legal operation's need for a maintainable service rather than leaving the original limitation in place.

03 / The work delivered

Enabled automated patching for operating systems and third-party applications

Why this mattered: Installing a system is not the end of the security job: visibility and control are needed while staff continue to use it.

04 / The work delivered

Rolled out MFA on all accounts, restricted legacy authentication, and hardened remote access

Why this mattered: Passwords alone leave accounts exposed; additional access checks make stolen credentials less useful to an attacker.

05 / The work delivered

Configured immutable, monitored backups with regular restore testing and documented recovery steps

Why this mattered: A recoverable copy must exist independently of the production service; synchronising files alone is not a recovery strategy.

06 / The work delivered

Removed local admin rights and introduced just-in-time elevation for trusted software installs

Why this mattered: This workstream addressed the legal operation's need for a maintainable service rather than leaving the original limitation in place.

PROJECT 12 / BUSINESS RESULT

What changed for the business

M3

Essential Eight target maturity reached

100%

of staff using MFA across all systems

4 hrs

documented recovery time for critical data

The sales conversation

If your organisation recognises these same issues, start with the constraint rather than a product list: which part of the environment interrupts staff, exposes data or makes growth harder? We can review the current setup, identify dependencies and scope the relevant services before recommending a change.



A word from the stable

The horn is optional. Layered protection isn't.

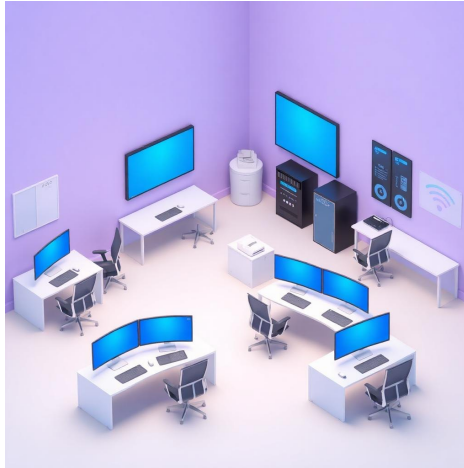
1300 904 635 | hello@uitg.com.au

PROJECT 13 / LEGAL

Law Firm Grew Rapidly and Needed a New Office

Office fitout & IT deployment

A fast-growing law firm moved into a larger office and needed more than furniture. We delivered a complete technology fitout so lawyers and support staff could walk into a fully working, secure workplace from day one.



The issues we needed to solve

- New office was an empty shell with no desks, chairs, meeting rooms or IT infrastructure
- Staff needed reliable, high-quality workstations with consistent docking and large screens
- Five Teams meeting rooms required video conferencing, displays, microphones and clean cable management
- No secure Wi-Fi, managed print or internet connectivity in place
- Firm needed private, resilient access to servers hosted in a data centre

PROJECT 13 / DELIVERY

What we did — and why

01 / The work delivered

Supplied and installed desks, ergonomic chairs, 34-inch widescreens and USB-C docking stations for every workstation

Why this mattered: A consistent device baseline makes deployment and ongoing support more predictable for staff and the service team.

02 / The work delivered

Built five Microsoft Teams meeting rooms with displays, speakers, microphones and one-touch join

Why this mattered: Communications need to follow how people work, with maintainable routing and extensions instead of the limitations of the old phone arrangement.

03 / The work delivered

Deployed enterprise Wi-Fi with separate networks for staff, guests and meeting room devices

Why this mattered: Guests, cameras and business systems have different trust levels, so they should not inherit unrestricted access to each other.

04 / The work delivered

Installed managed secure print so confidential documents only release when the user authenticates

Why this mattered: The improvement must remain usable and supportable after handover, not depend on knowledge held only by the installer.

05 / The work delivered

Ran dark fibre from the office to Next DC data centre for private, low-latency server access

Why this mattered: Reliable connectivity is the foundation for the applications above it; changing software cannot repair an inadequate physical or network path.

06 / The work delivered

Supplied internet breakout through Swoop, our partner ISP, with redundant paths

Why this mattered: The business needs a path through equipment or connection failures rather than making one component a single point of interruption.

07 / The work delivered

Racked Dell servers in the data centre and connected them back to the office over the private link

Why this mattered: This workstream addressed the legal operation's need for a maintainable service rather than leaving the original limitation in place.

PROJECT 13 / BUSINESS RESULT

What changed for the business

5

Teams meeting rooms ready on move-in day

34"

widescreens with docks at every desk

Dedicated

dark fibre link to Next DC Datacenters

What we used — and its role

SharePoint / Teams / OneDrive

Shared cloud workspaces separate business files and collaboration from a single office server or an individual computer.

Swoop

The recorded carrier service provides the WAN connection; routing, wireless and user support remain separate design decisions.

The sales conversation

If your organisation recognises these same issues, start with the constraint rather than a product list: which part of the environment interrupts staff, exposes data or makes growth harder? We can review the current setup, identify dependencies and scope the relevant services before recommending a change.



A word from the stable

Old dependencies don't retire themselves.

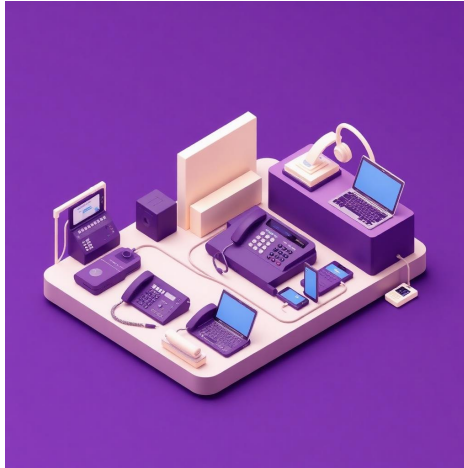
1300 904 635 | hello@uitg.com.au

PROJECT 14 / PROFESSIONAL SERVICES

Moved to 3CX Phone System from a Major Telco

Voice & telephony

A growing business was locked into expensive traditional handsets and call plans from a major telco. Monthly line rental, per-handset fees, and call charges were climbing while the system offered none of the flexibility their hybrid team needed.



The issues we needed to solve

- High monthly costs for line rental, handsets, and call plans from a major telco
- Staff working from home had no way to answer or transfer office calls professionally
- Adding a new extension required a technician visit and a long-term contract change
- No visibility into call queues, missed calls, or staff availability
- International and mobile calls were becoming a significant monthly expense

PROJECT 14 / DELIVERY

What we did — and why

01 / The work delivered

Audited existing usage and call patterns to size the right 3CX licence and SIP trunk plan

Why this mattered: Starting with the actual site and workload reduces the risk of buying equipment that cannot solve the underlying problem.

02 / The work delivered

Deployed 3CX in the cloud with apps for Windows, Mac, iOS, Android, and web browsers

Why this mattered: Communications need to follow how people work, with maintainable routing and extensions instead of the limitations of the old phone arrangement.

03 / The work delivered

Configured auto-attendants, call queues, ring groups, and out-of-hours routing

Why this mattered: Communications need to follow how people work, with maintainable routing and extensions instead of the limitations of the old phone arrangement.

04 / The work delivered

Migrated existing numbers and set up softphones so staff could take calls from anywhere

Why this mattered: Communications need to follow how people work, with maintainable routing and extensions instead of the limitations of the old phone arrangement.

05 / The work delivered

Negotiated competitive SIP trunk rates and call routing to reduce per-minute charges

Why this mattered: Communications need to follow how people work, with maintainable routing and extensions instead of the limitations of the old phone arrangement.

06 / The work delivered

Trained the team on the new system and provided ongoing management and reporting

Why this mattered: The improvement must remain usable and supportable after handover, not depend on knowledge held only by the installer.

PROJECT 14 / BUSINESS RESULT

What changed for the business

\$1,000+

saved every month on phone system costs

Hundreds

of dollars saved monthly on call charges

Minutes

to add or reconfigure an extension

What we used — and its role

3CX

A software-based phone system supports central call routing and flexible extensions without preserving the old PBX operating model.

The sales conversation

If your organisation recognises these same issues, start with the constraint rather than a product list: which part of the environment interrupts staff, exposes data or makes growth harder? We can review the current setup, identify dependencies and scope the relevant services before recommending a change.



A word from the stable

Good calls start with a properly connected office.

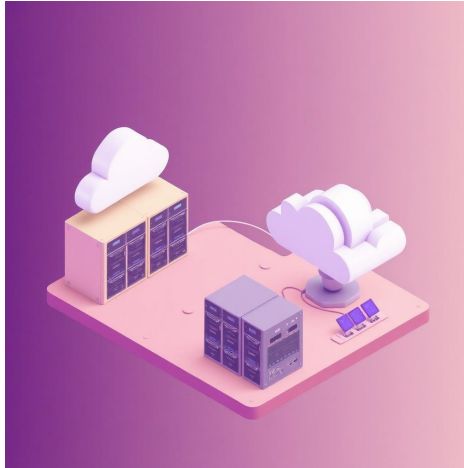
1300 904 635 | hello@uitg.com.au

PROJECT 15 / PROFESSIONAL SERVICES

Decommissioned 5 Servers — Full Cloud-First Migration

Cloud & infrastructure migration

A mid-sized business was running five ageing on-premise servers that powered everything from domain services and file storage to line-of-business applications. Hardware refresh quotes were climbing, and the existing setup was holding back remote work and modern security.



The issues we needed to solve

- Five physical servers nearing end of life across domain, files, applications, and backup roles
- Traditional Active Directory tied users to the office and made remote onboarding slow
- Computers were managed manually with no consistent policy, patching, or device compliance
- Legacy antivirus offered limited visibility and no managed threat response
- File shares and business apps required VPN or office presence to access
- No clear disaster recovery plan if the server room went offline

PROJECT 15 / DELIVERY

What we did — and why

01 / The work delivered

Migrated Active Directory to Microsoft Entra ID with hybrid identity and passwordless-ready policies

Why this mattered: Moving the workload or retiring obsolete dependencies reduces the amount of legacy infrastructure the business still has to operate.

02 / The work delivered

Enrolled all endpoints into Microsoft Intune / Endpoint Manager for policy, patch, and compliance control

Why this mattered: Installing a system is not the end of the security job: visibility and control are needed while staff continue to use it.

03 / The work delivered

Replaced legacy antivirus with SentinelOne managed endpoint protection and 24/7/365 SOC monitoring

Why this mattered: Installing a system is not the end of the security job: visibility and control are needed while staff continue to use it.

04 / The work delivered

Migrated file shares and shared drives into Microsoft Teams and SharePoint with permissions mapped to business roles

Why this mattered: Starting with the actual site and workload reduces the risk of buying equipment that cannot solve the underlying problem.

05 / The work delivered

Lifted on-premise applications to cloud-hosted or SaaS alternatives with secure remote access where needed

Why this mattered: Moving the workload or retiring obsolete dependencies reduces the amount of legacy infrastructure the business still has to operate.

06 / The work delivered

Decommissioned the five physical servers once data, identity, and app access were verified

Why this mattered: Moving the workload or retiring obsolete dependencies reduces the amount of legacy infrastructure the business still has to operate.

PROJECT 15 / BUSINESS RESULT

What changed for the business

5 → 0

on-premise servers decommissioned

100%

of endpoints under central management

24/7/365

managed threat detection and response

What we used — and its role

SentinelOne

Endpoint detection and response helps identify suspicious activity on computers and supports investigation and containment.

Intune / Autopilot

Policy-driven deployment helps standardise devices and reduces manual setup when a user receives a replacement computer.

SharePoint / Teams / OneDrive

Shared cloud workspaces separate business files and collaboration from a single office server or an individual computer.

The sales conversation

If your organisation recognises these same issues, start with the constraint rather than a product list: which part of the environment interrupts staff, exposes data or makes growth harder? We can review the current setup, identify dependencies and scope the relevant services before recommending a change.



A word from the stable

Old dependencies don't retire themselves.

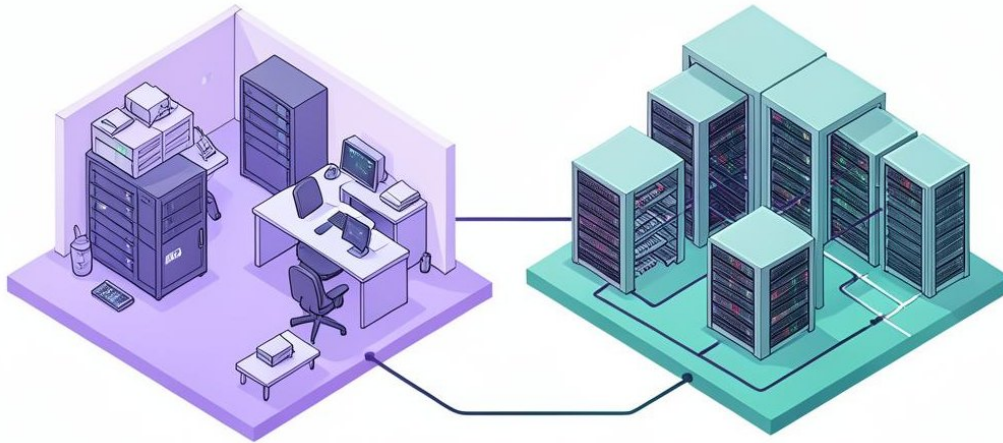
1300 904 635 | hello@uitg.com.au

PROJECT 16 / PROFESSIONAL SERVICES

Moved Servers to Next DC Datacenters

Data centre relocation

A business running its core systems on two on-premise Hyper-V hosts, direct-attached storage, and a WatchGuard firewall needed a more resilient home for its infrastructure. We relocated the entire stack into Next DC Datacenters and connected it back to the office with dedicated dark fibre.



The issues we needed to solve

- Two on-premise Hyper-V hosts and shared storage sitting in a small office server room with limited cooling and power redundancy
- WatchGuard firewall handling all office and remote-access traffic from the same cupboard as the servers
- Business-critical VMs — including line-of-business apps, file services, and domain controllers, office 365 sync — exposed to office power and network outages
- Internet bandwidth constrained by a generic connection that could not scale with cloud backup and remote worker demand
- No clear disaster recovery path if the office went offline

PROJECT 16 / DELIVERY

What we did — and why

01 / The work delivered

Planned and executed the physical relocation of two Hyper-V hosts and storage into a Next DC rack with redundant power and cooling

Why this mattered: The business needs a path through equipment or connection failures rather than making one component a single point of interruption.

02 / The work delivered

Re-racked and reconfigured the existing WatchGuard firewall to secure the new data centre environment

Why this mattered: This workstream addressed the professional services operation's need for a maintainable service rather than leaving the original limitation in place.

03 / The work delivered

Supplied enterprise internet from Swoop, our partner ISP, directly into the data centre suite

Why this mattered: This workstream addressed the professional services operation's need for a maintainable service rather than leaving the original limitation in place.

04 / The work delivered

Connected the office to the data centre via dedicated dark fibre, also supplied by Swoop, for low-latency, private site-to-site connectivity

Why this mattered: Reliable connectivity is the foundation for the applications above it; changing software cannot repair an inadequate physical or network path.

05 / The work delivered

Re-addressed and tested all VMs, VPN access, and failover paths before the final cutover

Why this mattered: The business needs a path through equipment or connection failures rather than making one component a single point of interruption.

06 / The work delivered

Documented the new topology and handed over monitoring so the business could see traffic, uptime, and capacity at a glance

Why this mattered: Installing a system is not the end of the security job: visibility and control are needed while staff continue to use it.

PROJECT 16 / BUSINESS RESULT

What changed for the business

2

Hyper-V hosts now in a resilient data centre

0

shared office power or cooling dependencies

1

dark fibre link between office and Next DC
Datacenters

What we used — and its role

WatchGuard

A managed firewall platform combines traffic control, secure access and, where deployed, SD-WAN policy in a consistent operating model.

Swoop

The recorded carrier service provides the WAN connection; routing, wireless and user support remain separate design decisions.

Hyper-V

Virtualisation consolidates server workloads and supports the recorded migration or cluster design without a separate physical machine for every application.

The sales conversation

If your organisation recognises these same issues, start with the constraint rather than a product list: which part of the environment interrupts staff, exposes data or makes growth harder? We can review the current setup, identify dependencies and scope the relevant services before recommending a change.



A word from the stable

Old dependencies don't retire themselves.

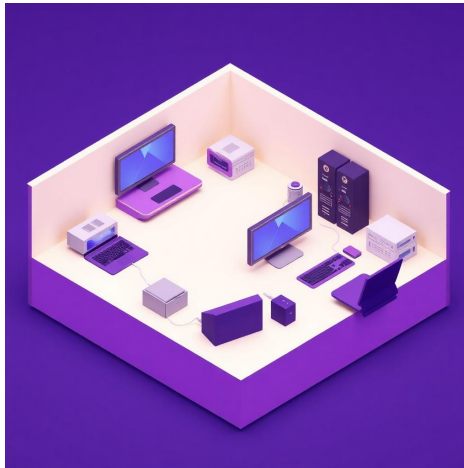
1300 904 635 | hello@uitg.com.au

PROJECT 17 / LOCAL GOVERNMENT

Replaced 40 Machines at a Local Shire

Endpoint refresh

A local shire was running a mixed fleet of aging whitebox PCs with unknown parts, expired or unclear warranties, and machines failing during critical council and public-facing work. They needed a standardised, supportable fleet that could be repaired quickly and keep staff productive.



The issues we needed to solve

- 40 mixed-age whitebox machines with non-standard parts and no clear warranty trail
- Frequent downtime in customer service and planning teams when hardware failed
- No consistent docking or monitor setup, so hot-desking and hybrid work were clunky
- Old screens were small, mismatched, and causing eye strain and layout issues
- Retired machines contained sensitive data and could not simply be thrown out

PROJECT 17 / DELIVERY

What we did — and why

01 / The work delivered

Standardised the fleet on HP EliteBook laptops with unified next-business-day (NBD) support

Why this mattered: A consistent device baseline makes deployment and ongoing support more predictable for staff and the service team.

02 / The work delivered

Paired each laptop with a 34-inch widescreen monitor and a USB-C docking station for one-cable connectivity

Why this mattered: Installing a system is not the end of the security job: visibility and control are needed while staff continue to use it.

03 / The work delivered

Imaged machines with the shire's standard build and migrated user data with minimal disruption

Why this mattered: Moving the workload or retiring obsolete dependencies reduces the amount of legacy infrastructure the business still has to operate.

04 / The work delivered

Collected all retired machines, performed secure data wiping, and donated viable units to a local charity

Why this mattered: A consistent device baseline makes deployment and ongoing support more predictable for staff and the service team.

05 / The work delivered

Documented the new fleet, warranty dates, and support process for the internal IT team

Why this mattered: The improvement must remain usable and supportable after handover, not depend on knowledge held only by the installer.

PROJECT 17 / BUSINESS RESULT

What changed for the business

40

new HP EliteBooks deployed with NBD support

34"

widescreen monitors and USB docks per workstation

0

old machines sent to landfill after secure data wipe

What we used — and its role

Ubiquiti / UniFi

Centrally managed switching, routing or wireless can be maintained as one office-network platform rather than as disconnected devices.

HP / Microsoft Surface

Business-class devices matched to staff roles create a more supportable endpoint estate than inconsistent personal or ageing computers.

The sales conversation

If your organisation recognises these same issues, start with the constraint rather than a product list: which part of the environment interrupts staff, exposes data or makes growth harder? We can review the current setup, identify dependencies and scope the relevant services before recommending a change.



A word from the stable

Old dependencies don't retire themselves.

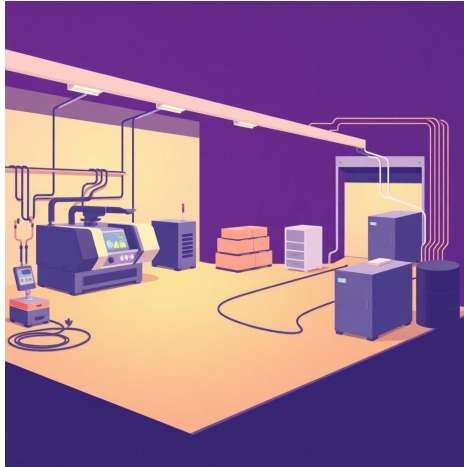
1300 904 635 | hello@uitg.com.au

PROJECT 18 / MANUFACTURING

Connected Rear Warehouse with Fibre

Fibre & warehouse connectivity

A manufacturing site needed to extend the network to a rear warehouse filled with CNC machines and CCTV cameras. Wireless was not an option due to heavy interference from plant equipment, so we ran a dedicated 300-metre fibre link with ducting, then tied it back to the office core and onward to the data centre.



The issues we needed to solve

- Rear warehouse had no reliable network connectivity for CNC machines and CCTV cameras
- Wireless links failed repeatedly due to electrical interference from machinery and metal racking
- 40 CCTV cameras needed stable bandwidth back to the office and data centre recording systems
- CNC machines required low-latency, consistent access to file servers and management systems
- The run crossed active yard and services, so proper ducting and protection were essential

PROJECT 18 / DELIVERY

What we did — and why

01 / The work delivered

Surveyed the 300-metre route and planned ducting to avoid existing services and vehicle traffic

Why this mattered: Starting with the actual site and workload reduces the risk of buying equipment that cannot solve the underlying problem.

02 / The work delivered

Installed underground ducting and pulled dedicated single-mode fibre from the office core to the warehouse

Why this mattered: Reliable connectivity is the foundation for the applications above it; changing software cannot repair an inadequate physical or network path.

03 / The work delivered

Terminated the fibre into a new core switch in the warehouse with redundant uplinks

Why this mattered: The business needs a path through equipment or connection failures rather than making one component a single point of interruption.

04 / The work delivered

Connected CNC machines and 40 CCTV cameras onto segmented VLANs with QoS priorities

Why this mattered: Guests, cameras and business systems have different trust levels, so they should not inherit unrestricted access to each other.

05 / The work delivered

Linked the warehouse core switch to the office core switch at 100 Gbps

Why this mattered: Reliable connectivity is the foundation for the applications above it; changing software cannot repair an inadequate physical or network path.

06 / The work delivered

Extended the connection via dark fibre at 100 Gbps from the office core to the data centre

Why this mattered: Reliable connectivity is the foundation for the applications above it; changing software cannot repair an inadequate physical or network path.

PROJECT 18 / BUSINESS RESULT

What changed for the business

300m fibre run with protected ducting	100Gbps core-to-core and dark fibre to data centre
40 CCTV cameras and CNC machines connected reliably	

The sales conversation

If your organisation recognises these same issues, start with the constraint rather than a product list: which part of the environment interrupts staff, exposes data or makes growth harder? We can review the current setup, identify dependencies and scope the relevant services before recommending a change.



A word from the stable

The right connection makes the rest of the office happier.

1300 904 635 | hello@uitg.com.au

PROJECT 19 / PROFESSIONAL SERVICES

Migrated 90 Servers to Cove Backup

Backup & disaster recovery

A business was backing up 90 servers across three racks of on-premise data centre space using an ageing backup platform with expensive licensing and growing storage costs. We moved the entire estate to Cove Backup, shifting disaster recovery to the cloud and reclaiming physical footprint.



The issues we needed to solve

- 90 servers protected by a legacy backup product with rising licence and maintenance costs
- On-premise backup storage consuming three full racks of data centre space
- Disaster recovery drills were slow, manual, and dependent on the same hardware being available
- Backup windows were creeping into business hours and impacting application performance
- No clear path to protect cloud workloads with the same policy framework

PROJECT 19 / DELIVERY

What we did — and why

01 / The work delivered

Audited every server, workload, and recovery objective to size the Cove Backup design

Why this mattered: Starting with the actual site and workload reduces the risk of buying equipment that cannot solve the underlying problem.

02 / The work delivered

Deployed Cove Backup agents across all 90 servers with consistent retention and scheduling policies

Why this mattered: A recoverable copy must exist independently of the production service; synchronising files alone is not a recovery strategy.

03 / The work delivered

Replicated backups to cloud storage to remove dependency on the local data centre for recovery

Why this mattered: The business needs a path through equipment or connection failures rather than making one component a single point of interruption.

04 / The work delivered

Configured cloud disaster recovery runbooks and tested failover procedures before go-live

Why this mattered: The business needs a path through equipment or connection failures rather than making one component a single point of interruption.

05 / The work delivered

Decommissioned the old backup hardware and reclaimed the three racks of data centre space

Why this mattered: A recoverable copy must exist independently of the production service; synchronising files alone is not a recovery strategy.

06 / The work delivered

Documented recovery times, roles, and escalation paths for the internal IT team

Why this mattered: The improvement must remain usable and supportable after handover, not depend on knowledge held only by the installer.

PROJECT 19 / BUSINESS RESULT

What changed for the business

\$40,000

saved per year in licence costs

3

data centre racks freed up

90

servers protected in Cove Backup

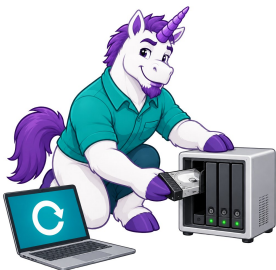
What we used — and its role

Cove Backup

Dedicated backup provides a recovery layer separate from production systems and day-to-day file access.

The sales conversation

If your organisation recognises these same issues, start with the constraint rather than a product list: which part of the environment interrupts staff, exposes data or makes growth harder? We can review the current setup, identify dependencies and scope the relevant services before recommending a change.



A word from the stable

Backups need a recovery plan, not just a hopeful nod.

1300 904 635 | hello@uitg.com.au

PROJECT 20 / ENTERPRISE

Migrated 1000 Users from On-Premise Exchange 2019 to Office 365

Email & collaboration migration

A large organisation was running Exchange 2019 on ageing on-premise hardware, struggling with remote access, mobile email, and the looming cost of a server refresh. We moved 1000 mailboxes to Office 365, unlocking Email, Teams, and OneDrive across the workforce.



The issues we needed to solve

- 1000 mailboxes tied to ageing Exchange 2019 servers facing a hardware refresh cycle
- Remote and mobile staff had a poor email experience without modern apps or MFA
- No central collaboration platform — file sharing relied on email attachments and network drives
- On-premise infrastructure created a single point of failure for business communication
- Compliance and retention policies were inconsistently applied across the organisation

PROJECT 20 / DELIVERY

What we did — and why

01 / The work delivered

Assessed the existing Exchange environment, mailbox sizes, and dependency on legacy add-ins

Why this mattered: Starting with the actual site and workload reduces the risk of buying equipment that cannot solve the underlying problem.

02 / The work delivered

Designed a hybrid migration approach with staged cutover waves to minimise disruption

Why this mattered: Moving the workload or retiring obsolete dependencies reduces the amount of legacy infrastructure the business still has to operate.

03 / The work delivered

Configured Microsoft 365 tenancy, identity synchronisation, and conditional access policies

Why this mattered: Passwords alone leave accounts exposed; additional access checks make stolen credentials less useful to an attacker.

04 / The work delivered

Migrated mailboxes in batches, validating sync, permissions, and client reconfiguration each wave

Why this mattered: Moving the workload or retiring obsolete dependencies reduces the amount of legacy infrastructure the business still has to operate.

05 / The work delivered

Rolled out Teams and OneDrive with training so staff could move off email attachments

Why this mattered: The improvement must remain usable and supportable after handover, not depend on knowledge held only by the installer.

06 / The work delivered

Decommissioned the on-premise Exchange 2019 servers once cutover and retention were verified

Why this mattered: Moving the workload or retiring obsolete dependencies reduces the amount of legacy infrastructure the business still has to operate.

PROJECT 20 / BUSINESS RESULT

What changed for the business

1000

users migrated to Office 365

0

on-premise Exchange servers remaining

24/7

email, Teams and OneDrive access from any device

What we used — and its role

Microsoft 365

Cloud email and collaboration reduce dependence on local mail servers and make access and administration consistent across devices.

SharePoint / Teams / OneDrive

Shared cloud workspaces separate business files and collaboration from a single office server or an individual computer.

The sales conversation

If your organisation recognises these same issues, start with the constraint rather than a product list: which part of the environment interrupts staff, exposes data or makes growth harder? We can review the current setup, identify dependencies and scope the relevant services before recommending a change.



A word from the stable

Old dependencies don't retire themselves.

1300 904 635 | hello@uitg.com.au

PROJECT 21 / INTERNATIONAL

Migrated 3000 Users from 15 Exchange 2013 Servers to Office 365

International email migration

An international business was running 15 on-premise Exchange 2013 servers across multiple regions, facing end-of-support risk, rising maintenance costs and a poor mobile email experience. We moved over 3000 user mailboxes to Office 365 in carefully planned waves across two months.



The issues we needed to solve

- 15 on-premise Exchange 2013 servers approaching end of support and costly to maintain
- 3000 mailboxes spread across multiple countries and time zones
- Mobile and remote staff struggled with legacy Outlook Web Access and inconsistent performance
- Complex coexistence requirements during the migration window
- Risk of email downtime affecting global operations and customer communication

PROJECT 21 / DELIVERY

What we did — and why

01 / The work delivered

Audited every Exchange server, mailbox size, distribution group and legacy dependency

Why this mattered: Starting with the actual site and workload reduces the risk of buying equipment that cannot solve the underlying problem.

02 / The work delivered

Designed a hybrid migration with staged waves based on region, department and mailbox size

Why this mattered: Moving the workload or retiring obsolete dependencies reduces the amount of legacy infrastructure the business still has to operate.

03 / The work delivered

Configured Microsoft 365 tenancy, directory synchronisation, conditional access and retention policies

Why this mattered: Passwords alone leave accounts exposed; additional access checks make stolen credentials less useful to an attacker.

04 / The work delivered

Migrated mailboxes in batches, validating sync, permissions and Outlook client reconfiguration each wave

Why this mattered: Moving the workload or retiring obsolete dependencies reduces the amount of legacy infrastructure the business still has to operate.

05 / The work delivered

Provided regional training and change management for Outlook, Teams and OneDrive

Why this mattered: The improvement must remain usable and supportable after handover, not depend on knowledge held only by the installer.

06 / The work delivered

Decommissioned all 15 Exchange 2013 servers once coexistence and retention were verified

Why this mattered: Moving the workload or retiring obsolete dependencies reduces the amount of legacy infrastructure the business still has to operate.

PROJECT 21 / BUSINESS RESULT

What changed for the business

3000+ user mailboxes migrated to Office 365	15 on-premise Exchange 2013 servers retired
2 month wave migration completed	0 mailboxes lost or corrupted

What we used — and its role

Microsoft 365

Cloud email and collaboration reduce dependence on local mail servers and make access and administration consistent across devices.

SharePoint / Teams / OneDrive

Shared cloud workspaces separate business files and collaboration from a single office server or an individual computer.

The sales conversation

If your organisation recognises these same issues, start with the constraint rather than a product list: which part of the environment interrupts staff, exposes data or makes growth harder? We can review the current setup, identify dependencies and scope the relevant services before recommending a change.



A word from the stable

Old dependencies don't retire themselves.

1300 904 635 | hello@uitg.com.au

PROJECT 22 / ENTERPRISE

Migrated 2000 Virtual Servers to Azure and Decommissioned On-Premise VMware

Azure migration & decommission

A large enterprise faced urgent VMware price rises and ageing on-premise infrastructure spread across three racks of physical hosts, switches, and routers. We migrated 2000 virtual servers to Microsoft Azure, consolidated the remaining office footprint to two WatchGuard firewalls, a core switch and a Metro Ethernet router, and completed the entire server migration within three months.



The issues we needed to solve

- 2000 virtual servers running on ageing VMware hardware facing a sharp licence cost increase
- Three racks of physical servers, networking gear and storage nearing end of life
- Urgent timeline driven by VMware pricing changes and unsupported infrastructure risk
- Complex application dependencies across workloads with limited documentation
- Need to maintain business continuity during a large-scale cloud migration

PROJECT 22 / DELIVERY

What we did — and why

01 / The work delivered

Discovered and catalogued every VM, dependency, owner and recovery requirement before migration

Why this mattered: Moving the workload or retiring obsolete dependencies reduces the amount of legacy infrastructure the business still has to operate.

02 / The work delivered

Designed Azure landing zones with proper networking, identity and governance from day one

Why this mattered: This workstream addressed the enterprise operation's need for a maintainable service rather than leaving the original limitation in place.

03 / The work delivered

Lifted and shifted compatible VMs while refactoring select workloads for cloud-native operation

Why this mattered: Moving the workload or retiring obsolete dependencies reduces the amount of legacy infrastructure the business still has to operate.

04 / The work delivered

Consolidated the on-premise edge to two WatchGuard firewalls, a core switch and a Metro Ethernet router

Why this mattered: Reliable connectivity is the foundation for the applications above it; changing software cannot repair an inadequate physical or network path.

05 / The work delivered

Executed migration in waves over three months with rollback plans and out-of-hours cutovers

Why this mattered: Moving the workload or retiring obsolete dependencies reduces the amount of legacy infrastructure the business still has to operate.

06 / The work delivered

Securely wiped all decommissioned physical servers and donated viable hardware to charity for learning and testing

Why this mattered: Moving the workload or retiring obsolete dependencies reduces the amount of legacy infrastructure the business still has to operate.

PROJECT 22 / BUSINESS RESULT

What changed for the business

2000

virtual servers migrated to Azure

3

racks of on-premise gear decommissioned

3

month migration window completed

What we used — and its role

WatchGuard

A managed firewall platform combines traffic control, secure access and, where deployed, SD-WAN policy in a consistent operating model.

VMware / Azure

A virtual or cloud compute platform separates business applications from the limitations of individual ageing on-premise servers.

The sales conversation

If your organisation recognises these same issues, start with the constraint rather than a product list: which part of the environment interrupts staff, exposes data or makes growth harder? We can review the current setup, identify dependencies and scope the relevant services before recommending a change.



A word from the stable

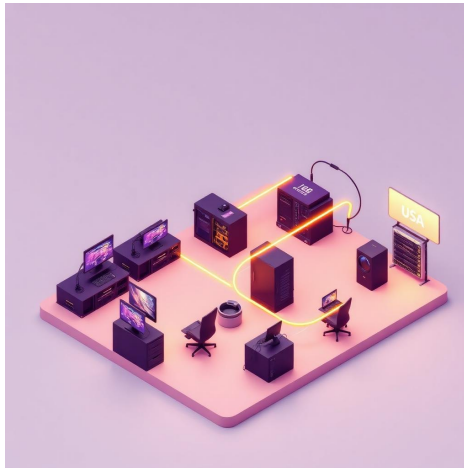
Old dependencies don't retire themselves.

1300 904 635 | hello@uitg.com.au

10 Gbps Wavelength to the USA for a 3D Graphics and Movie Studio

International wavelength

A 3D graphics and movie production company was moving terabytes of footage and renders to its USA office every day over a congested internet connection. We procured a dedicated 10 Gbps wavelength to the USA through Swoop and connected their Australian office directly to their American storage and network at line speed.



The issues we needed to solve

- Daily transfers of multiple terabytes of high-resolution footage, 3D assets and rendered frames to the USA office
- Existing internet connection was saturated, causing upload queues, missed deadlines and project delays
- Remote storage and network shares in the USA were unusable for real-time collaboration
- High-spec workstations could not leverage their 10 Gbps NICs because the upstream link was the bottleneck
- Public internet routing introduced latency, jitter and unpredictable performance for large file sync

PROJECT 23 / DELIVERY

What we did — and why

01 / The work delivered

Worked with Swoop, our partner ISP, to provision a dedicated 10 Gbps international wavelength from the studio to the USA

Why this mattered: This workstream addressed the media & entertainment operation's need for a maintainable service rather than leaving the original limitation in place.

02 / The work delivered

Connected the Australian office directly to the USA office's core network and storage environment at 10 Gbps

Why this mattered: This workstream addressed the media & entertainment operation's need for a maintainable service rather than leaving the original limitation in place.

03 / The work delivered

Upgraded the studio's core switching and workstation NICs to support full 10 Gbps end-to-end

Why this mattered: Reliable connectivity is the foundation for the applications above it; changing software cannot repair an inadequate physical or network path.

04 / The work delivered

Configured high-spec render workstations and storage arrays with 10 Gbps connections for fast upload of changes

Why this mattered: A consistent device baseline makes deployment and ongoing support more predictable for staff and the service team.

05 / The work delivered

Segmented production traffic from general office traffic so file transfers never impacted voice or cloud apps

Why this mattered: Guests, cameras and business systems have different trust levels, so they should not inherit unrestricted access to each other.

06 / The work delivered

Set up monitoring and alerting on the wavelength path, switch ports and storage throughput

Why this mattered: Installing a system is not the end of the security job: visibility and control are needed while staff continue to use it.

PROJECT 23 / BUSINESS RESULT

What changed for the business

10Gbps dedicated wavelength to the USA	TB/day transfers completed in minutes instead of hours
10Gbps workstation and storage connections end to end	Swoop partner ISP delivering the international wavelength

What we used — and its role

Swoop

The recorded carrier service provides the WAN connection; routing, wireless and user support remain separate design decisions.

The sales conversation

If your organisation recognises these same issues, start with the constraint rather than a product list: which part of the environment interrupts staff, exposes data or makes growth harder? We can review the current setup, identify dependencies and scope the relevant services before recommending a change.



A word from the stable

The right connection makes the rest of the office happier.

1300 904 635 | hello@uitg.com.au

PROJECT 24 / RETAIL

Customer Wireless Rollout for a Regional Shopping Centre

Public Wi-Fi

A medium regional shopping centre needed reliable customer wireless across all common areas, hallways, the food court and mall spaces. We deployed Ubiquiti access points and a Ubiquiti firewall, backed by a 1 Gbps NBN Enterprise Ethernet connection from Swoop, and now support more than 200 connected devices per day at peak.



The issues we needed to solve

- Patchy guest Wi-Fi that dropped out in food courts, hallways and near mall entrances
- Shoppers and tenants complaining about slow or unusable connections
- No central visibility into how many devices were online or where problems started
- Concern that an open guest network could expose centre management and retail systems
- Peak periods such as weekends and school holidays pushed the old connection past its limit

PROJECT 24 / DELIVERY

What we did — and why

01 / The work delivered

Conducted a site survey across the mall, food court, hallways and car park entry points

Why this mattered: Starting with the actual site and workload reduces the risk of buying equipment that cannot solve the underlying problem.

02 / The work delivered

Installed Ubiquiti wireless access points with overlapping coverage for seamless roaming

Why this mattered: Reliable connectivity is the foundation for the applications above it; changing software cannot repair an inadequate physical or network path.

03 / The work delivered

Deployed a Ubiquiti firewall to segment guest traffic from centre management and retail systems

Why this mattered: Guests, cameras and business systems have different trust levels, so they should not inherit unrestricted access to each other.

04 / The work delivered

Provisioned a 1 Gbps NBN Enterprise Ethernet connection from Swoop as the primary internet link

Why this mattered: Reliable connectivity is the foundation for the applications above it; changing software cannot repair an inadequate physical or network path.

05 / The work delivered

Configured separate VLANs for guests, centre staff and digital signage with bandwidth limits

Why this mattered: Guests, cameras and business systems have different trust levels, so they should not inherit unrestricted access to each other.

06 / The work delivered

Set up cloud-based monitoring so the centre team can see device counts, usage and uptime

Why this mattered: Installing a system is not the end of the security job: visibility and control are needed while staff continue to use it.

PROJECT 24 / BUSINESS RESULT

What changed for the business

200+ connected devices per day at peak	1Gbps NBN Enterprise Ethernet from Swoop
Full mall, food court and hallway coverage	0 guest complaints in the first month

What we used — and its role

Ubiquiti / UniFi

Centrally managed switching, routing or wireless can be maintained as one office-network platform rather than as disconnected devices.

Swoop

The recorded carrier service provides the WAN connection; routing, wireless and user support remain separate design decisions.

The sales conversation

If your organisation recognises these same issues, start with the constraint rather than a product list: which part of the environment interrupts staff, exposes data or makes growth harder? We can review the current setup, identify dependencies and scope the relevant services before recommending a change.



A word from the stable

A stronger signal beats shouting at the router.

1300 904 635 | hello@uitg.com.au

PROJECT 25 / CONSTRUCTION

30 Virtual Machines Migrated from VMware to Hyper-V for a Home Builder

Virtualisation & licensing savings

After a steep VMware licensing increase, a home builder asked us to move their entire virtual environment to Hyper-V. We migrated 30 virtual machines over three weeks, working in batches of 10 at night so no office, display home or site team lost a working day.



The issues we needed to solve

- A large VMware renewal increase made the existing virtualisation platform hard to justify
- 30 production virtual machines covering domain controllers, file, print, accounting, estimating and job management systems
- Sales offices and display homes rely on those systems during business hours, so daytime downtime was not an option
- Existing hosts and shared storage had to be reused rather than replaced
- No in-house team to run or validate a migration of this size

PROJECT 25 / DELIVERY

What we did — and why

01 / The work delivered

Audited all 30 virtual machines for dependencies, disk sizes, snapshots and application owners

Why this mattered: Starting with the actual site and workload reduces the risk of buying equipment that cannot solve the underlying problem.

02 / The work delivered

Grouped the estate into three batches of 10, ordering them so dependent systems moved together

Why this mattered: This workstream addressed the construction operation's need for a maintainable service rather than leaving the original limitation in place.

03 / The work delivered

Rebuilt the hosts as a Windows Server Hyper-V cluster using the existing hardware and shared storage

Why this mattered: This workstream addressed the construction operation's need for a maintainable service rather than leaving the original limitation in place.

04 / The work delivered

Converted and migrated each batch overnight, removing VMware tools and installing Hyper-V integration services

Why this mattered: Moving the workload or retiring obsolete dependencies reduces the amount of legacy infrastructure the business still has to operate.

05 / The work delivered

Tested boot, logon, application access, printing and backups after every batch before staff arrived

Why this mattered: A recoverable copy must exist independently of the production service; synchronising files alone is not a recovery strategy.

06 / The work delivered

Repointed Cove backups at the new Hyper-V hosts and ran restore tests during the project

Why this mattered: A recoverable copy must exist independently of the production service; synchronising files alone is not a recovery strategy.

07 / The work delivered

Decommissioned VMware licensing at the end of the three weeks and documented the new environment

Why this mattered: Correct licensing addresses entitlement and predictable administration, rather than leaving the organisation reliant on unsupported or inconsistent software access.

PROJECT 25 / BUSINESS RESULT

What changed for the business

30 virtual machines migrated to Hyper-V	3 weeks end to end, 10 machines per batch
0 business hours lost by staff	100% of VMware licensing costs removed

What we used — and its role

Cove Backup

Dedicated backup provides a recovery layer separate from production systems and day-to-day file access.

Hyper-V

Virtualisation consolidates server workloads and supports the recorded migration or cluster design without a separate physical machine for every application.

VMware / Azure

A virtual or cloud compute platform separates business applications from the limitations of individual ageing on-premise servers.

The sales conversation

If your organisation recognises these same issues, start with the constraint rather than a product list: which part of the environment interrupts staff, exposes data or makes growth harder? We can review the current setup, identify dependencies and scope the relevant services before recommending a change.



A word from the stable

Old dependencies don't retire themselves.

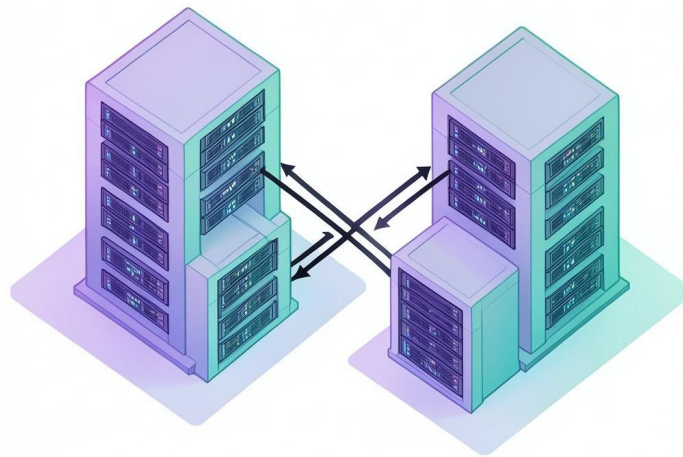
1300 904 635 | hello@uitg.com.au

PROJECT 26 / ENTERPRISE

Hyper-V Replication Across Two Next DC Data Centres

Disaster recovery & replication

An enterprise needed a resilient, geographically separated Hyper-V cluster with real-time replication between two Next DC facilities. We built a four-host, two-SAN environment connected by dedicated dark fibre and dual Dell switch stacks.



The issues we needed to solve

- Critical workloads running from a single data centre with no live disaster recovery site
- Recovery objectives demanded near-zero data loss and fast failover for business systems
- Storage replication between sites needed consistent, low-latency performance
- Network layer required redundancy and enough bandwidth for both production and replication traffic
- The design had to scale as the virtual machine estate grew

PROJECT 26 / DELIVERY

What we did — and why

01 / The work delivered

Designed an active-passive Hyper-V cluster split across two Next DC data centres

Why this mattered: This workstream addressed the enterprise operation's need for a maintainable service rather than leaving the original limitation in place.

02 / The work delivered

Deployed four Hyper-V hosts with two shared SAN arrays, one at each site

Why this mattered: This workstream addressed the enterprise operation's need for a maintainable service rather than leaving the original limitation in place.

03 / The work delivered

Installed dual Dell switch stacks at both sites for redundant core networking

Why this mattered: The business needs a path through equipment or connection failures rather than making one component a single point of interruption.

04 / The work delivered

Provisioned dedicated dark fibre between the two sites for private, low-latency replication

Why this mattered: The business needs a path through equipment or connection failures rather than making one component a single point of interruption.

05 / The work delivered

Configured Hyper-V Replica and cluster-aware updating for automated failover testing

Why this mattered: The business needs a path through equipment or connection failures rather than making one component a single point of interruption.

06 / The work delivered

Segmented production, management and replication traffic onto dedicated VLANs

Why this mattered: The business needs a path through equipment or connection failures rather than making one component a single point of interruption.

07 / The work delivered

Documented runbooks and tested failover and failback procedures before go-live

Why this mattered: The business needs a path through equipment or connection failures rather than making one component a single point of interruption.

PROJECT 26 / BUSINESS RESULT

What changed for the business

4 Hyper-V hosts across two data centres	2 SAN arrays with synchronous replication
2 Dell switch stacks for redundant core networking	Dedicated dark fibre link between Next DC sites
<15 min target failover time for critical VMs	

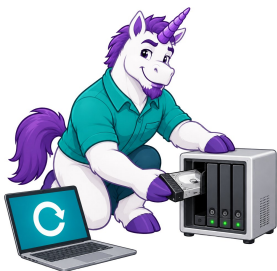
What we used — and its role

Hyper-V

Virtualisation consolidates server workloads and supports the recorded migration or cluster design without a separate physical machine for every application.

The sales conversation

If your organisation recognises these same issues, start with the constraint rather than a product list: which part of the environment interrupts staff, exposes data or makes growth harder? We can review the current setup, identify dependencies and scope the relevant services before recommending a change.



A word from the stable

Backups need a recovery plan, not just a hopeful nod.

1300 904 635 | hello@uitg.com.au

Free Passenger Wi-Fi at a Remote Airport via Bonded Starlink

Public Wi-Fi & remote connectivity

A remote regional airport had no reliable fixed-line internet and wanted to offer free passenger Wi-Fi in the terminal and apron areas. We delivered bonded Starlink backhaul, a WatchGuard firewall, and two Ubiquiti access points to cover travellers and staff.



The issues we needed to solve

- No usable fixed-line broadband or fibre at the remote airport location
- Passengers and pilots expected reliable internet while waiting for flights
- Public Wi-Fi had to be safely segregated from any airport operational systems
- Single Starlink dish alone could not guarantee consistent throughput during peak departures
- Equipment had to survive harsh weather, dust, and wide temperature swings on an airport roof

PROJECT 27 / DELIVERY

What we did — and why

01 / The work delivered

Installed two Starlink terminals on the terminal roof and bonded them into a single high-availability internet path

Why this mattered: Reliable connectivity is the foundation for the applications above it; changing software cannot repair an inadequate physical or network path.

02 / The work delivered

Deployed a WatchGuard firewall to inspect traffic, enforce content filtering, and separate guest Wi-Fi from operations

Why this mattered: Guests, cameras and business systems have different trust levels, so they should not inherit unrestricted access to each other.

03 / The work delivered

Mounted two outdoor-rated Ubiquiti access points to blanket the terminal, waiting area, and nearby apron

Why this mattered: This workstream addressed the aviation & transport operation's need for a maintainable service rather than leaving the original limitation in place.

04 / The work delivered

Configured a branded captive portal with simple terms of use for passengers

Why this mattered: This workstream addressed the aviation & transport operation's need for a maintainable service rather than leaving the original limitation in place.

05 / The work delivered

Built a separate secure SSID for airport staff and operations with restricted access to operational networks

Why this mattered: This workstream addressed the aviation & transport operation's need for a maintainable service rather than leaving the original limitation in place.

06 / The work delivered

Set up 24/7 monitoring and alerts so connectivity issues could be diagnosed before travellers noticed them

Why this mattered: Installing a system is not the end of the security job: visibility and control are needed while staff continue to use it.

PROJECT 27 / BUSINESS RESULT

What changed for the business

2x

bonded Starlink dishes for resilient backhaul

2

Ubiquiti access points covering terminal and apron

99.5%

terminal Wi-Fi availability since go-live

<50ms

average failover between Starlink links

What we used — and its role

WatchGuard

A managed firewall platform combines traffic control, secure access and, where deployed, SD-WAN policy in a consistent operating model.

Ubiquiti / UniFi

Centrally managed switching, routing or wireless can be maintained as one office-network platform rather than as disconnected devices.

Starlink

Satellite connectivity provides a practical connection option when usable terrestrial services are unavailable at a remote location.

The sales conversation

If your organisation recognises these same issues, start with the constraint rather than a product list: which part of the environment interrupts staff, exposes data or makes growth harder? We can review the current setup, identify dependencies and scope the relevant services before recommending a change.



A word from the stable

A stronger signal beats shouting at the router.

1300 904 635 | hello@uitg.com.au

PROJECT 28 / MANUFACTURING

Manufacturing Company Stopped Data Leaks with DLP in Days

Data loss prevention

A manufacturing company suspected sensitive drawings, pricing and customer lists were leaving the business. Within days of implementing Microsoft 365 Data Loss Prevention policies, the company discovered files being shared with competitors and unknown email addresses, and stopped further exfiltration before major damage occurred.



The issues we needed to solve

- Confidential product drawings and costing sheets were being shared outside the business without oversight
- Sales and customer lists were being emailed to personal accounts and competitor domains
- No visibility into which users were moving data, or whether sharing was accidental or malicious
- Legacy file shares and USB transfers made it impossible to track intellectual property
- Management feared the leaks had already cost them tenders and customer relationships

PROJECT 28 / DELIVERY

What we did — and why

01 / The work delivered

Rapidly scoped the Microsoft 365 tenant, file locations and email flow with the operations team

Why this mattered: This workstream addressed the manufacturing operation's need for a maintainable service rather than leaving the original limitation in place.

02 / The work delivered

Deployed Microsoft Purview Data Loss Prevention policies across Exchange, SharePoint and OneDrive

Why this mattered: Moving the workload or retiring obsolete dependencies reduces the amount of legacy infrastructure the business still has to operate.

03 / The work delivered

Created sensitive information types for product drawings, customer lists, pricing and contract terms

Why this mattered: This workstream addressed the manufacturing operation's need for a maintainable service rather than leaving the original limitation in place.

04 / The work delivered

Configured real-time policy tips so staff are warned before sending or sharing protected content

Why this mattered: This workstream addressed the manufacturing operation's need for a maintainable service rather than leaving the original limitation in place.

05 / The work delivered

Built automated alerts for security and leadership when high-risk sharing is detected

Why this mattered: This workstream addressed the manufacturing operation's need for a maintainable service rather than leaving the original limitation in place.

06 / The work delivered

Blocked external sharing of protected content while allowing approved, audited exceptions

Why this mattered: Starting with the actual site and workload reduces the risk of buying equipment that cannot solve the underlying problem.

07 / The work delivered

Trained staff on safe sharing practices and updated acceptable-use policy

Why this mattered: The improvement must remain usable and supportable after handover, not depend on knowledge held only by the installer.

PROJECT 28 / BUSINESS RESULT

What changed for the business

Days from deployment to first leak detected	100% visibility into protected data sharing
0 further leaks after policy enforcement	Competitor and unknown email domains flagged and blocked

What we used — and its role

Microsoft 365

Cloud email and collaboration reduce dependence on local mail servers and make access and administration consistent across devices.

SharePoint / Teams / OneDrive

Shared cloud workspaces separate business files and collaboration from a single office server or an individual computer.

The sales conversation

If your organisation recognises these same issues, start with the constraint rather than a product list: which part of the environment interrupts staff, exposes data or makes growth harder? We can review the current setup, identify dependencies and scope the relevant services before recommending a change.



A word from the stable

The horn is optional. Layered protection isn't.

1300 904 635 | hello@uitg.com.au

PROJECT 28 / QUESTIONS

A closer look at the solution

How quickly can DLP policies start protecting data?

Policies can be deployed and actively monitoring within hours. In this case the first concerning sharing activity was flagged within days, giving leadership immediate visibility into a problem they did not know they had.

Will DLP block legitimate customer or supplier communication?

No. We configure DLP with business rules, approved domains and exception workflows. Staff see policy tips before anything is blocked, and legitimate sharing can still happen with oversight.

What kind of data can DLP protect?

Microsoft Purview DLP can protect files, emails and chat messages containing intellectual property, customer lists, pricing, contracts, personally identifiable information, and more. We tune the rules to match what matters most to your business.

Can you help if we suspect data is already leaking?

Yes. We can audit your Microsoft 365 environment, review sharing and access logs, and deploy DLP quickly to contain the issue. Call 1300 904 635 or email hello@uitg.com.au for urgent assistance.

PROJECT 29 / CONSTRUCTION

Connected 3 Home Builder Offices with Dedicated Gigabit Air Fibre

Air fibre & point-to-point

A growing home builder had three offices on separate streets roughly 300 metres apart. Staff were juggling slow VPNs, USB drives and email attachments to share large plans, contracts and site photos between sites. We designed a dedicated gigabit air-fibre network linking all three buildings without trenching streets or waiting months for carrier fibre.



The issues we needed to solve

- Three offices on different streets with no direct, high-speed link between them
- Large construction plans, site photos and video files were painful to share across sites
- Staff relied on consumer-grade internet and VPNs that dropped during uploads
- Trenching dedicated fibre between sites was expensive, slow and disruptive to local traffic
- The builder needed a solution that could grow with more offices and display sites

PROJECT 29 / DELIVERY

What we did — and why

01 / The work delivered

Site survey with clear line-of-sight checks between all three rooftops

Why this mattered: Starting with the actual site and workload reduces the risk of buying equipment that cannot solve the underlying problem.

02 / The work delivered

Installed dedicated point-to-point air-fibre bridges delivering a full gigabit between buildings

Why this mattered: Reliable connectivity is the foundation for the applications above it; changing software cannot repair an inadequate physical or network path.

03 / The work delivered

Designed a ring-style topology so each office has a resilient path back to the others

Why this mattered: This workstream addressed the construction operation's need for a maintainable service rather than leaving the original limitation in place.

04 / The work delivered

Segmented traffic into VLANs for staff, guest Wi-Fi, voice and site-security cameras

Why this mattered: Guests, cameras and business systems have different trust levels, so they should not inherit unrestricted access to each other.

05 / The work delivered

Connected the linked network to a high-speed Swoop NBN Enterprise Ethernet breakout

Why this mattered: Reliable connectivity is the foundation for the applications above it; changing software cannot repair an inadequate physical or network path.

06 / The work delivered

Added centralised monitoring so link quality, uptime and bandwidth are visible in real time

Why this mattered: Installing a system is not the end of the security job: visibility and control are needed while staff continue to use it.

PROJECT 29 / BUSINESS RESULT

What changed for the business

1Gbps

dedicated air-fibre between offices

300m

approximate distance between sites

3

offices connected as one network

99.9%

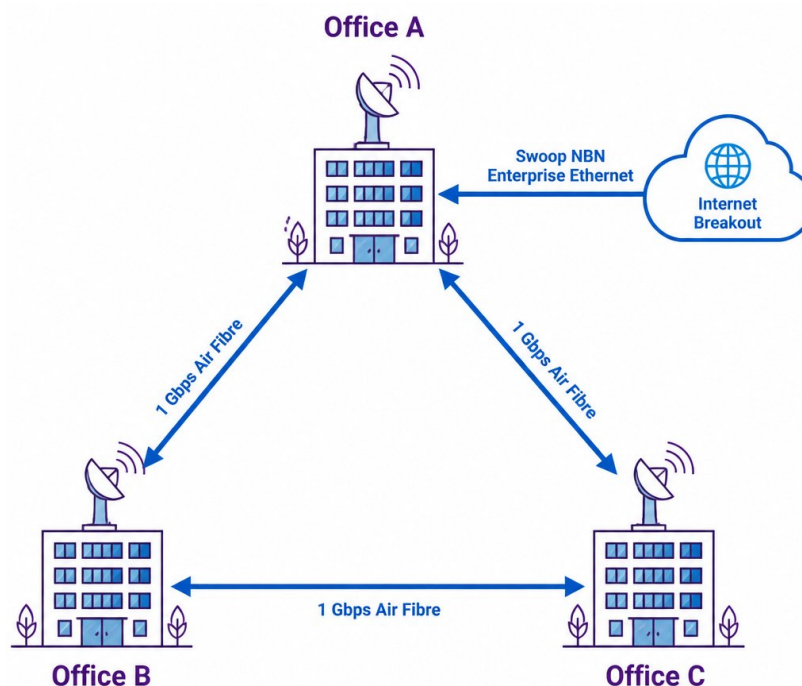
target uptime with ring topology

What we used — and its role

Swoop

The recorded carrier service provides the WAN connection; routing, wireless and user support remain separate design decisions.

Recorded project design



The sales conversation

If your organisation recognises these same issues, start with the constraint rather than a product list: which part of the environment interrupts staff, exposes data or makes growth harder? We can review the current setup, identify dependencies and scope the relevant services before recommending a change.



A word from the stable

The right connection makes the rest of the office happier.

1300 904 635 | hello@uitg.com.au

PROJECT 29 / QUESTIONS

A closer look at the solution

Is the air-fibre link a dedicated connection between our offices?

Yes. The link is a dedicated point-to-point air-fibre bridge installed on each rooftop. It does not share bandwidth with the public internet or neighbouring buildings, so the full gigabit is available between your sites at all times.

How long does an air-fibre installation like this take?

Most three-site deployments are surveyed, installed and tested within 4 to 6 weeks. The exact timeline depends on rooftop access, line-of-sight checks and any landlord approvals. We keep disruption to a minimum by doing the bulk of the work outside business hours where possible.

What happens if one link goes down?

We designed a ring-style topology, so each office has a resilient path back to the others. If one air-fibre link is blocked by weather or hardware fault, traffic automatically reroutes through the remaining link while we fix the issue.

Do you provide ongoing management and support?

Yes. The network is monitored 24/7 by our managed services team. We track link quality, uptime and bandwidth, apply firmware updates, and respond to alerts before they become problems. You also get local helpdesk support during business hours and after-hours escalation.

PROJECT 30 / CONSTRUCTION

Connected Display Homes to a Next DC Data Centre with Cisco Meraki SD-WAN

Meraki SD-WAN & display homes

A national home builder needed every display home to feel like a branch office: fast guest Wi-Fi for visitors, reliable internet for sales staff, and a secure tunnel back to the corporate data centre. We deployed Cisco Meraki access points and MX64 security appliances in each display home, using Swoop NBN or 5G as transport, and built a high-availability pair of Meraki MX200 security appliances at the Next DC data centre.



The issues we needed to solve

- Display homes are spread across many suburbs and regional centres, often with no existing business-grade internet
- Sales staff and demonstration devices needed consistent, secure access to CRM, pricing and document systems hosted in the data centre
- Visitors expect reliable guest Wi-Fi without seeing corporate network resources
- The data centre required a resilient, high-throughput head-end for dozens of upcoming display homes and branch offices
- Each site had to be deployable quickly so new display villages could open on schedule

PROJECT 30 / DELIVERY

What we did — and why

01 / The work delivered

Survey every display home for fixed-line availability and 5G signal quality, then order Swoop NBN or 5G backup as the primary transport

Why this mattered: Starting with the actual site and workload reduces the risk of buying equipment that cannot solve the underlying problem.

02 / The work delivered

Install Cisco Meraki indoor access points for visitor and staff Wi-Fi, with separate SSIDs and VLANs for guest, corporate and IoT traffic

Why this mattered: Guests, cameras and business systems have different trust levels, so they should not inherit unrestricted access to each other.

03 / The work delivered

Deploy Cisco Meraki MX64 security appliances with Auto VPN back to the data centre head-end

Why this mattered: This workstream addressed the construction operation's need for a maintainable service rather than leaving the original limitation in place.

04 / The work delivered

Build a high-availability pair of Cisco Meraki MX200 security appliances at Next DC with 1 Gbps Swoop fibre for resilient internet and inter-site routing

Why this mattered: Reliable connectivity is the foundation for the applications above it; changing software cannot repair an inadequate physical or network path.

05 / The work delivered

Configure cloud-based SD-WAN policies so business-critical traffic is prioritised and failover between NBN and 5G is automatic

Why this mattered: The business needs a path through equipment or connection failures rather than making one component a single point of interruption.

06 / The work delivered

Apply unified security policies across all sites from the Meraki dashboard, including content filtering, intrusion prevention and GeoIP restrictions

Why this mattered: This workstream addressed the construction operation's need for a maintainable service rather than leaving the original limitation in place.

07 / The work delivered

Document every site, hand over credentials, and train sales managers on basic troubleshooting

Why this mattered: The improvement must remain usable and supportable after handover, not depend on knowledge held only by the installer.

PROJECT 30 / BUSINESS RESULT

What changed for the business

100%

of display homes connected to the data centre

1Gbps

Swoop fibre at the Next DC data centre head-end

Sub-20ms

latency to corporate apps from any display home

Same day

turn-up possible for new villages

What we used — and its role

Cisco Meraki

Cloud management gives the support team a common view of the deployed network or camera estate without needing to visit each location.

Ubiquiti / UniFi

Centrally managed switching, routing or wireless can be maintained as one office-network platform rather than as disconnected devices.

Swoop

The recorded carrier service provides the WAN connection; routing, wireless and user support remain separate design decisions.

The sales conversation

If your organisation recognises these same issues, start with the constraint rather than a product list: which part of the environment interrupts staff, exposes data or makes growth harder? We can review the current setup, identify dependencies and scope the relevant services before recommending a change.



A word from the stable

The right connection makes the rest of the office happier.

1300 904 635 | hello@uitg.com.au

PROJECT 30 / QUESTIONS

A closer look at the solution

Why Cisco Meraki instead of other firewall or Wi-Fi brands?

Meraki gives us zero-touch deployment from a single cloud dashboard. We can ship an access point and MX64 to a new display home, plug it in, and the site is live within minutes. The same dashboard also manages the MX200 head-end pair at Next DC, so policies and firmware are consistent everywhere.

What happens if the fixed NBN link at a display home goes down?

Each Meraki MX64 is configured with an automatic failover path. If the Swoop NBN service drops, the appliance switches business traffic to the 5G backup and raises an alert. Guest Wi-Fi can also run over the backup so sales demonstrations keep working.

How do you keep visitor Wi-Fi separate from corporate systems?

We use separate SSIDs and VLANs for guest, corporate and IoT traffic. Guest traffic is tunnelled straight to the internet, while corporate traffic is routed through the Auto VPN tunnel back to the data centre. Firewall rules prevent cross-traffic between the networks.

Can this scale as the builder opens more display homes?

Yes. The Meraki cloud dashboard and the MX200 head-end pair at Next DC are sized to add new sites without re-engineering the core. New display homes simply become additional Auto VPN peers with the same standardised policies.

Remote Water Monitoring and Gate Control Over Starlink SD-WAN

Starlink SD-WAN & IoT

A small water corporation needed reliable connectivity at remote water sites to monitor flow with Meraki cameras and operate gates remotely. We delivered a Starlink-powered SD-WAN built on WatchGuard firewalls, with IP relays connecting gate controllers and cameras back to a central operations team.



The issues we needed to solve

- Remote water sites with no fixed-line internet or unreliable 4G coverage
- Need to view real-time water levels and flow via Meraki cameras
- Manual gate operations requiring staff to travel to each site
- SCADA and telemetry traffic needed secure, always-on connectivity
- Operations team required a single, centralised view of every site

PROJECT 31 / DELIVERY

What we did — and why

01 / The work delivered

Installed Starlink terminals at every remote water monitoring site for high-availability internet

Why this mattered: Installing a system is not the end of the security job: visibility and control are needed while staff continue to use it.

02 / The work delivered

Built a secure SD-WAN using WatchGuard firewalls with centralised management

Why this mattered: Reliable connectivity is the foundation for the applications above it; changing software cannot repair an inadequate physical or network path.

03 / The work delivered

Connected Meraki cameras overlooking channels and gates for visual water-level monitoring

Why this mattered: Installing a system is not the end of the security job: visibility and control are needed while staff continue to use it.

04 / The work delivered

Integrated IP relays to open and close water gates remotely from the operations centre

Why this mattered: This workstream addressed the water & utilities operation's need for a maintainable service rather than leaving the original limitation in place.

05 / The work delivered

Segregated camera, telemetry and management traffic across VLANs

Why this mattered: Guests, cameras and business systems have different trust levels, so they should not inherit unrestricted access to each other.

06 / The work delivered

Added 4G/5G failover where available to keep gates and cameras online during Starlink maintenance

Why this mattered: The business needs a path through equipment or connection failures rather than making one component a single point of interruption.

07 / The work delivered

Deployed centralised monitoring and alerting for link status, uptime and gate events

Why this mattered: Installing a system is not the end of the security job: visibility and control are needed while staff continue to use it.

PROJECT 31 / BUSINESS RESULT

What changed for the business

All sites connected via Starlink SD-WAN	24/7 remote visibility of water levels
Remote gate open/close control from office	WatchGuard firewall securing every site
Meraki cameras monitoring flow and gates	

What we used — and its role

WatchGuard

A managed firewall platform combines traffic control, secure access and, where deployed, SD-WAN policy in a consistent operating model.

Cisco Meraki

Cloud management gives the support team a common view of the deployed network or camera estate without needing to visit each location.

Starlink

Satellite connectivity provides a practical connection option when usable terrestrial services are unavailable at a remote location.

The sales conversation

If your organisation recognises these same issues, start with the constraint rather than a product list: which part of the environment interrupts staff, exposes data or makes growth harder? We can review the current setup, identify dependencies and scope the relevant services before recommending a change.



A word from the stable

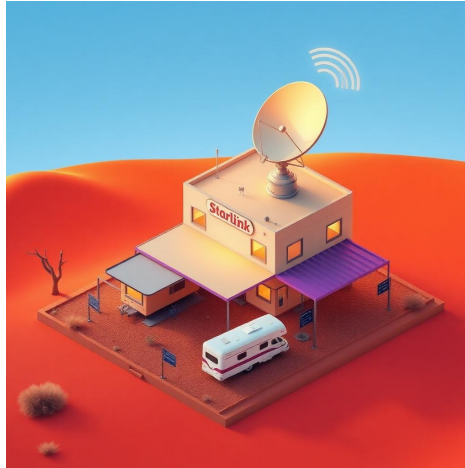
A stronger signal beats shouting at the router.

1300 904 635 | hello@uitg.com.au

Bonded Starlink and Guest Wi-Fi for an Outback Roadhouse

Remote connectivity & guest Wi-Fi

A remote desert roadhouse relied on poor NBN fixed wireless that dropped out during peak tourist season, leaving guests, staff and EFTPOS terminals offline. We installed bonded Starlink for resilient backhaul and built a separate guest Wi-Fi network with a branded captive portal.



The issues we needed to solve

- Poor NBN fixed wireless with frequent dropouts and low speeds during busy periods
- No mobile coverage for a reliable 4G/5G backup at the remote location
- EFTPOS, reservations, streaming and guest Wi-Fi all fighting for the same weak link
- Guests and staff sharing one network and one password created security concerns
- Peak tourist season regularly overloaded the connection and caused complaints

PROJECT 32 / DELIVERY

What we did — and why

01 / The work delivered

Installed two Starlink terminals and bonded them into a single high-availability internet path

Why this mattered: Reliable connectivity is the foundation for the applications above it; changing software cannot repair an inadequate physical or network path.

02 / The work delivered

Deployed a WatchGuard firewall to inspect traffic and separate guest, staff and payment networks

Why this mattered: Guests, cameras and business systems have different trust levels, so they should not inherit unrestricted access to each other.

03 / The work delivered

Installed outdoor-rated Ubiquiti access points across the roadhouse, fuel station and caravan area

Why this mattered: This workstream addressed the hospitality & tourism operation's need for a maintainable service rather than leaving the original limitation in place.

04 / The work delivered

Built a branded captive portal for guest Wi-Fi with fair-use limits and simple terms of use

Why this mattered: Guests, cameras and business systems have different trust levels, so they should not inherit unrestricted access to each other.

05 / The work delivered

Added 4G/5G failover where any mobile signal was available for extra resilience

Why this mattered: The business needs a path through equipment or connection failures rather than making one component a single point of interruption.

06 / The work delivered

Set up 24/7 monitoring and alerting so connectivity issues are caught before travellers notice

Why this mattered: Installing a system is not the end of the security job: visibility and control are needed while staff continue to use it.

PROJECT 32 / BUSINESS RESULT

What changed for the business

2x bonded Starlink dishes for resilient backhaul	99.5% roadhouse internet uptime since go-live
200+ guest devices per day at peak	<50ms average failover between Starlink links

What we used — and its role

WatchGuard

A managed firewall platform combines traffic control, secure access and, where deployed, SD-WAN policy in a consistent operating model.

Ubiquiti / UniFi

Centrally managed switching, routing or wireless can be maintained as one office-network platform rather than as disconnected devices.

Starlink

Satellite connectivity provides a practical connection option when usable terrestrial services are unavailable at a remote location.

The sales conversation

If your organisation recognises these same issues, start with the constraint rather than a product list: which part of the environment interrupts staff, exposes data or makes growth harder? We can review the current setup, identify dependencies and scope the relevant services before recommending a change.



A word from the stable

A stronger signal beats shouting at the router.

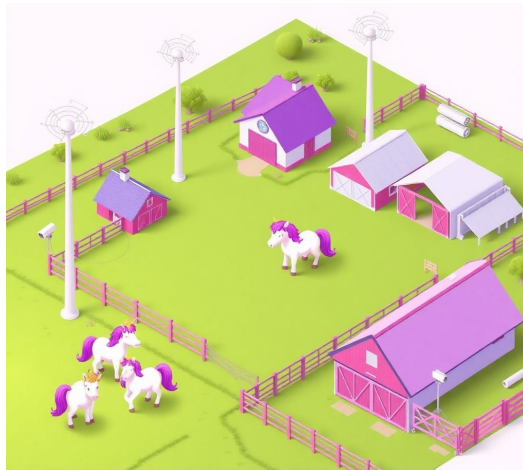
1300 904 635 | hello@uitg.com.au

PROJECT 33 / RURAL & AGRICULTURE

Farm-Wide Wi-Fi and Meraki Cameras for a Unicorn Farmer

Farm Wi-Fi & CCTV

A unicorn farmer needed reliable Wi-Fi across sprawling paddocks so every unicorn collar tracker could report its location in real time. We designed an outdoor wireless network with long-range access points and added Meraki cameras around barns, gates and yards so the farmer could check on the herd from anywhere.



The issues we needed to solve

- Large paddock areas with no usable Wi-Fi beyond the homestead
- Each unicorn wore a Wi-Fi tracker collar that needed constant connectivity
- Existing consumer router could not reach sheds, fences or the far paddocks
- Farmer needed visual monitoring of gates, yards and barns without driving to each location
- Outdoor hardware had to survive dust, rain, heat and curious animals

PROJECT 33 / DELIVERY

What we did — and why

01 / The work delivered

Paddock survey to map coverage zones, fence lines and animal movement paths

Why this mattered: Starting with the actual site and workload reduces the risk of buying equipment that cannot solve the underlying problem.

02 / The work delivered

Installed outdoor-rated Wi-Fi access points on high poles and existing sheds for long-range coverage

Why this mattered: This workstream addressed the rural & agriculture operation's need for a maintainable service rather than leaving the original limitation in place.

03 / The work delivered

Designed overlapping cells so unicorns and trackers stay connected as they move between paddocks

Why this mattered: This workstream addressed the rural & agriculture operation's need for a maintainable service rather than leaving the original limitation in place.

04 / The work delivered

Deployed Meraki cloud-managed cameras at barns, gates and yards with onboard storage

Why this mattered: Moving the workload or retiring obsolete dependencies reduces the amount of legacy infrastructure the business still has to operate.

05 / The work delivered

Segmented networks into staff, tracker, guest and camera VLANs for security

Why this mattered: Guests, cameras and business systems have different trust levels, so they should not inherit unrestricted access to each other.

06 / The work delivered

Added centralised monitoring and alerting for link quality, camera health and tracker connectivity

Why this mattered: Installing a system is not the end of the security job: visibility and control are needed while staff continue to use it.

PROJECT 33 / BUSINESS RESULT

What changed for the business

Full farm Wi-Fi coverage across paddocks	Live unicorn collar tracking
Meraki cameras covering barns and gates	24/7 visibility from any device

What we used — and its role

Cisco Meraki

Cloud management gives the support team a common view of the deployed network or camera estate without needing to visit each location.

The sales conversation

If your organisation recognises these same issues, start with the constraint rather than a product list: which part of the environment interrupts staff, exposes data or makes growth harder? We can review the current setup, identify dependencies and scope the relevant services before recommending a change.



A word from the stable

The right connection makes the rest of the office happier.

1300 904 635 | hello@uitg.com.au

PROJECT 34 / HEALTHCARE

3CX Phone System Connecting 32 Healthcare Sites Across Australia

Voice & telephony

A healthcare provider with 16 sites in Western Australia, 14 in New South Wales and 2 in Victoria needed a single phone system to connect every clinic. We deployed a cloud-hosted 3CX platform with high-availability PABX, Swoop SIP trunking and softphones, cutting hardware costs and monthly call spend.



The issues we needed to solve

- 32 separate clinics across three states running inconsistent phone systems
- Major telco quote included roughly \$15,000 in hardware fees alone
- High monthly call costs, especially for interstate and mobile calls
- Staff could not transfer calls cleanly between states or work from home
- No centralised call queues, reporting, after-hours routing or voicemail

PROJECT 34 / DELIVERY

What we did — and why

01 / The work delivered

Deployed 3CX as a high-availability PABX hosted in Australian cloud infrastructure

Why this mattered: Communications need to follow how people work, with maintainable routing and extensions instead of the limitations of the old phone arrangement.

02 / The work delivered

Provisioned SIP trunks through Swoop for reliable, cost-effective calling

Why this mattered: Communications need to follow how people work, with maintainable routing and extensions instead of the limitations of the old phone arrangement.

03 / The work delivered

Configured auto-attendants, ring groups, call queues and after-hours voicemail

Why this mattered: Communications need to follow how people work, with maintainable routing and extensions instead of the limitations of the old phone arrangement.

04 / The work delivered

Rolled out softphones, mobile apps and desk phones so staff could answer from any site or home

Why this mattered: Communications need to follow how people work, with maintainable routing and extensions instead of the limitations of the old phone arrangement.

05 / The work delivered

Migrated existing numbers and managed staged cutovers to avoid disrupting clinics

Why this mattered: Moving the workload or retiring obsolete dependencies reduces the amount of legacy infrastructure the business still has to operate.

06 / The work delivered

Trained site managers and provided ongoing management, reporting and support

Why this mattered: The improvement must remain usable and supportable after handover, not depend on knowledge held only by the installer.

PROJECT 34 / BUSINESS RESULT

What changed for the business

32 healthcare sites connected across Australia	~\$15,000 saved in hardware fees vs major telco
~\$1,000 saved monthly in call costs	3 states connected — WA, NSW and Victoria
HA cloud-hosted PABX in Australia	

What we used — and its role

3CX

A software-based phone system supports central call routing and flexible extensions without preserving the old PBX operating model.

Swoop

The recorded carrier service provides the WAN connection; routing, wireless and user support remain separate design decisions.

The sales conversation

If your organisation recognises these same issues, start with the constraint rather than a product list: which part of the environment interrupts staff, exposes data or makes growth harder? We can review the current setup, identify dependencies and scope the relevant services before recommending a change.



A word from the stable

Good calls start with a properly connected office.

1300 904 635 | hello@uitg.com.au

PROJECT 34 / QUESTIONS

A closer look at the solution

Why did the healthcare provider choose 3CX over a traditional telco system?

The major telco solution required roughly \$15,000 in hardware fees and locked the provider into expensive call plans. 3CX delivered the same enterprise voice features in Australian cloud hosting with lower call costs and no proprietary hardware lock-in.

How do 32 clinics across three states stay connected on one system?

All sites register to the same cloud-hosted 3CX PABX over their existing internet connections. Staff can dial extensions between WA, NSW and Victoria, transfer calls between clinics, and use the same softphone app on their mobile or computer.

What happens if the internet at one clinic goes down?

Calls can be rerouted to mobile apps, other sites or voicemail automatically. Because the PABX is hosted in high-availability Australian cloud infrastructure, the core system keeps running even if an individual site loses connectivity.

Can you deploy a similar phone system for healthcare or multi-site businesses?

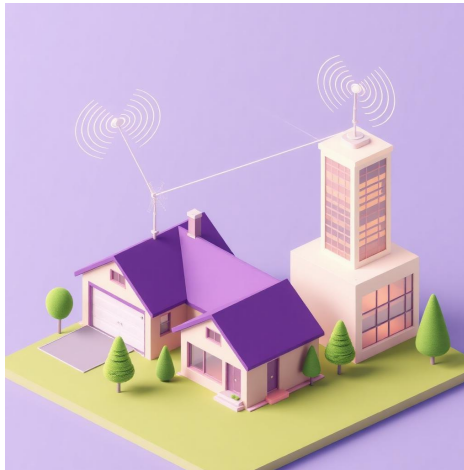
Yes. We service businesses all over Australia and design every 3CX deployment around your sites, compliance needs and call patterns. Call 1300 904 635 or email hello@uitg.com.au to scope a solution.

PROJECT 35 / PROFESSIONAL SERVICES

Point-to-Point Wireless Link from Manager's Home to Office

P2P wireless

A business manager needed reliable, high-speed access to office systems from home, but the NBN connection at his house was too slow and unstable for video calls, file sharing and cloud apps. We installed a dedicated point-to-point wireless bridge from the office roof to his home, bypassing the slow NBN entirely.



The issues we needed to solve

- Home NBN was too slow for video calls and cloud applications
- Frequent dropouts during important meetings and client calls
- Large files had to be downloaded overnight or brought in on USB
- VPN over the slow link was frustrating and often unusable
- No viable fibre or fixed-wireless upgrade path at the residence

PROJECT 35 / DELIVERY

What we did — and why

01 / The work delivered

Site survey with clear line-of-sight check between office and home rooftops

Why this mattered: Starting with the actual site and workload reduces the risk of buying equipment that cannot solve the underlying problem.

02 / The work delivered

Installed directional point-to-point wireless radios on both buildings

Why this mattered: Reliable connectivity is the foundation for the applications above it; changing software cannot repair an inadequate physical or network path.

03 / The work delivered

Configured a dedicated encrypted bridge separate from the public internet

Why this mattered: This workstream addressed the professional services operation's need for a maintainable service rather than leaving the original limitation in place.

04 / The work delivered

Integrated the home link into the office network with firewall segmentation

Why this mattered: Guests, cameras and business systems have different trust levels, so they should not inherit unrestricted access to each other.

05 / The work delivered

Added 4G/5G backup for resilience during severe weather events

Why this mattered: A recoverable copy must exist independently of the production service; synchronising files alone is not a recovery strategy.

06 / The work delivered

Set up monitoring and alerting on link quality, uptime and throughput

Why this mattered: Installing a system is not the end of the security job: visibility and control are needed while staff continue to use it.

PROJECT 35 / BUSINESS RESULT

What changed for the business

1Gbps dedicated wireless link between office and home	<5ms latency end to end
99.9% link uptime since install	Same day access to office files and systems

The sales conversation

If your organisation recognises these same issues, start with the constraint rather than a product list: which part of the environment interrupts staff, exposes data or makes growth harder? We can review the current setup, identify dependencies and scope the relevant services before recommending a change.



A word from the stable

A stronger signal beats shouting at the router.

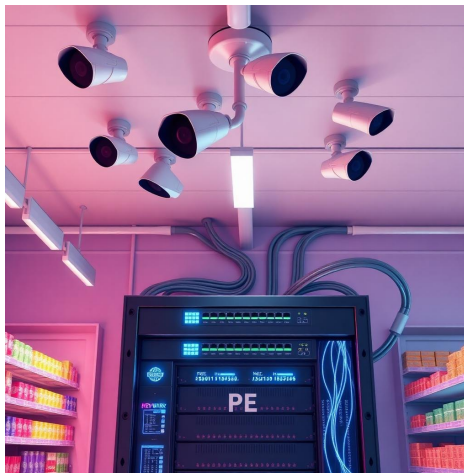
1300 904 635 | hello@uitg.com.au

PROJECT 36 / RETAIL

Data Cabling, Ubiquiti PoE Network and 40 Meraki Cameras for a Local Supermarket

CCTV & network cabling

A local supermarket needed a complete physical security and network overhaul. We ran structured data cabling throughout the store, installed Ubiquiti PoE switches to power the network, and deployed 40 Meraki cloud-managed cameras covering every aisle, entrance, loading dock and checkout.



The issues we needed to solve

- Old analogue CCTV with poor coverage and no remote access
- No structured cabling for tills, cameras, phones or Wi-Fi access points
- Checkout disputes and stock loss with no clear footage to review
- Loading dock and back-of-house blind spots
- Separate, unmanaged switches causing loops and dropped connections

PROJECT 36 / DELIVERY

What we did — and why

01 / The work delivered

Surveyed the store to design camera coverage and cable routes with no disruption to trading

Why this mattered: Starting with the actual site and workload reduces the risk of buying equipment that cannot solve the underlying problem.

02 / The work delivered

Ran CAT6 data cabling to every camera location, checkout, office and wireless access point

Why this mattered: Reliable connectivity is the foundation for the applications above it; changing software cannot repair an inadequate physical or network path.

03 / The work delivered

Installed Ubiquiti PoE switches to power cameras and access points from a central rack

Why this mattered: Reliable connectivity is the foundation for the applications above it; changing software cannot repair an inadequate physical or network path.

04 / The work delivered

Deployed 40 Meraki cloud-managed cameras with motion search, night vision and onboard storage

Why this mattered: Moving the workload or retiring obsolete dependencies reduces the amount of legacy infrastructure the business still has to operate.

05 / The work delivered

Segmented camera, staff, guest and POS traffic across secure VLANs

Why this mattered: Guests, cameras and business systems have different trust levels, so they should not inherit unrestricted access to each other.

06 / The work delivered

Configured cloud dashboard so managers can view live and recorded footage from any device

Why this mattered: Moving the workload or retiring obsolete dependencies reduces the amount of legacy infrastructure the business still has to operate.

PROJECT 36 / BUSINESS RESULT

What changed for the business

40 Meraki cameras covering every aisle and entrance	100% PoE-powered camera and access point network
Cloud centralised video management and remote access	Zero checkout blind spots after install

What we used — and its role

Cisco Meraki

Cloud management gives the support team a common view of the deployed network or camera estate without needing to visit each location.

Ubiquiti / UniFi

Centrally managed switching, routing or wireless can be maintained as one office-network platform rather than as disconnected devices.

The sales conversation

If your organisation recognises these same issues, start with the constraint rather than a product list: which part of the environment interrupts staff, exposes data or makes growth harder? We can review the current setup, identify dependencies and scope the relevant services before recommending a change.



A word from the stable

The horn is optional. Layered protection isn't.

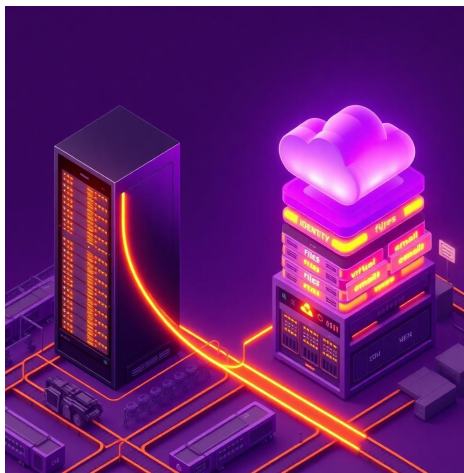
1300 904 635 | hello@uitg.com.au

PROJECT 37 / MANUFACTURING

Manufacturing Company Server-to-Cloud Migration with Azure and Microsoft 365

Cloud & infrastructure

A manufacturing company's on-premise servers were end of life and hosted Active Directory, file shares, Exchange, an accounting package and FileMaker. We moved the entire workload to the cloud with Entra ID, Azure Files, SharePoint, Office 365 Exchange Online, an Azure VM for FileMaker, and a 1 Gbps Swoop Enterprise Ethernet NBN link over a site-to-site VPN.



The issues we needed to solve

- Ageing on-premise servers running Active Directory, file shares, Exchange, accounting and FileMaker were end of life
- Risk of hardware failure halting production, payroll and order processing
- Remote staff and factory floor users struggled to access files and email reliably off-site
- No modern identity, device management or cloud backup in place
- Business needed high-availability connectivity between the factory and cloud resources

PROJECT 37 / DELIVERY

What we did — and why

01 / The work delivered

Migrated Active Directory and computers to Microsoft Entra ID with Intune/Endpoint Manager policies

Why this mattered: Moving the workload or retiring obsolete dependencies reduces the amount of legacy infrastructure the business still has to operate.

02 / The work delivered

Replaced on-premise file shares with Azure Files and SharePoint for document collaboration and permissions

Why this mattered: The improvement must remain usable and supportable after handover, not depend on knowledge held only by the installer.

03 / The work delivered

Moved Exchange to Office 365 Exchange Online with hybrid coexistence and staged mailbox cutover

Why this mattered: This workstream addressed the manufacturing operation's need for a maintainable service rather than leaving the original limitation in place.

04 / The work delivered

Hosted FileMaker in a dedicated Azure VM with backups, patching and monitored availability

Why this mattered: A recoverable copy must exist independently of the production service; synchronising files alone is not a recovery strategy.

05 / The work delivered

Configured a site-to-site VPN from the factory firewall to Azure for secure, low-latency access

Why this mattered: This workstream addressed the manufacturing operation's need for a maintainable service rather than leaving the original limitation in place.

06 / The work delivered

Installed a 1 Gbps Swoop Enterprise Ethernet NBN connection as the primary internet and cloud uplink

Why this mattered: Reliable connectivity is the foundation for the applications above it; changing software cannot repair an inadequate physical or network path.

07 / The work delivered

Retired the old physical servers once data, mail and applications were validated in the cloud

Why this mattered: Moving the workload or retiring obsolete dependencies reduces the amount of legacy infrastructure the business still has to operate.

PROJECT 37 / BUSINESS RESULT

What changed for the business

5 on-premise servers fully retired	1Gbps Swoop Enterprise Ethernet NBN to cloud
100% of staff on Entra ID and cloud email	Azure VM hosting FileMaker with managed backups

What we used — and its role

Microsoft 365

Cloud email and collaboration reduce dependence on local mail servers and make access and administration consistent across devices.

Intune / Autopilot

Policy-driven deployment helps standardise devices and reduces manual setup when a user receives a replacement computer.

SharePoint / Teams / OneDrive

Shared cloud workspaces separate business files and collaboration from a single office server or an individual computer.

Swoop

The recorded carrier service provides the WAN connection; routing, wireless and user support remain separate design decisions.

VMware / Azure

A virtual or cloud compute platform separates business applications from the limitations of individual ageing on-premise servers.

The sales conversation

If your organisation recognises these same issues, start with the constraint rather than a product list: which part of the environment interrupts staff, exposes data or makes growth harder? We can review the current setup, identify dependencies and scope the relevant services before recommending a change.



A word from the stable

Old dependencies don't retire themselves.

1300 904 635 | hello@uitg.com.au

Swoop Enterprise Ethernet NBN and Ubiquiti Upgrade for a Marketing Agency

Cloud connectivity

A local marketing agency was running its entire business in the cloud, but its standard NBN connection was too slow and the upload speed was choking large file transfers, video renders and client collaboration. We installed a 1 Gbps Swoop Enterprise Ethernet NBN service and rebuilt the office network with Ubiquiti wireless, a UniFi Cloud Gateway and managed switches.



The issues we needed to solve

- Standard NBN upload speed was too slow for cloud-based creative workflows
- Large video files, design assets and campaign uploads took hours or timed out
- Staff on Wi-Fi experienced dropouts and poor performance in meeting rooms
- Real-time client collaboration tools lagged and disrupted presentations
- No network visibility or traffic priority for business-critical cloud apps

PROJECT 38 / DELIVERY

What we did — and why

01 / The work delivered

Ordered and provisioned a 1 Gbps symmetrical Swoop Enterprise Ethernet NBN service

Why this mattered: Reliable connectivity is the foundation for the applications above it; changing software cannot repair an inadequate physical or network path.

02 / The work delivered

Installed a Ubiquiti UniFi Cloud Gateway as the core router and firewall

Why this mattered: Moving the workload or retiring obsolete dependencies reduces the amount of legacy infrastructure the business still has to operate.

03 / The work delivered

Replaced ageing switches with managed Ubiquiti PoE switches

Why this mattered: Reliable connectivity is the foundation for the applications above it; changing software cannot repair an inadequate physical or network path.

04 / The work delivered

Deployed ceiling-mounted Ubiquiti Wi-Fi 6 access points for full office coverage

Why this mattered: This workstream addressed the professional services operation's need for a maintainable service rather than leaving the original limitation in place.

05 / The work delivered

Configured VLANs and traffic shaping to prioritise creative cloud apps and video calls

Why this mattered: Guests, cameras and business systems have different trust levels, so they should not inherit unrestricted access to each other.

06 / The work delivered

Set up remote monitoring and alerting so issues are caught before staff notice them

Why this mattered: Installing a system is not the end of the security job: visibility and control are needed while staff continue to use it.

PROJECT 38 / BUSINESS RESULT

What changed for the business

1Gbps symmetrical Swoop Enterprise Ethernet NBN	Full office Ubiquiti Wi-Fi 6 coverage
10x+ faster upload speeds for large files	Cloud-ready network with app prioritisation

What we used — and its role

Ubiquiti / UniFi

Centrally managed switching, routing or wireless can be maintained as one office-network platform rather than as disconnected devices.

Swoop

The recorded carrier service provides the WAN connection; routing, wireless and user support remain separate design decisions.

The sales conversation

If your organisation recognises these same issues, start with the constraint rather than a product list: which part of the environment interrupts staff, exposes data or makes growth harder? We can review the current setup, identify dependencies and scope the relevant services before recommending a change.



A word from the stable

The right connection makes the rest of the office happier.

1300 904 635 | hello@uitg.com.au

PROJECT 38 / QUESTIONS

A closer look at the solution

Why did the marketing agency need Enterprise Ethernet NBN instead of standard NBN?

The agency lives entirely in the cloud. Standard NBN upload speeds were too slow for large video files, design assets and real-time collaboration. Swoop Enterprise Ethernet delivers symmetrical 1 Gbps speeds with consistent performance and business-grade SLA.

What Ubiquiti equipment was installed?

We deployed a Ubiquiti UniFi Cloud Gateway as the core router and firewall, managed Ubiquiti PoE switches, and Wi-Fi 6 access points across the office for reliable, high-density wireless coverage.

How does traffic prioritisation help a cloud-based business?

We configure VLANs and quality-of-service rules so creative cloud apps, video calls and file uploads get priority over streaming, guest devices and background traffic. This keeps the most important tools responsive even when the office is busy.

Can you deliver the same solution for other cloud-first businesses?

Yes. We service businesses all over Australia and design connectivity upgrades around your cloud stack, upload demands and office layout. Call 1300 904 635 or email hello@uitg.com.au to scope a solution.

PROJECT 39 / EDUCATION

School Saves \$2,000/Month by Switching to Swoop 1 Gbps Enterprise Ethernet NBN

Connectivity

A regional K-12 school was paying a major telco premium for slow, unreliable internet that could not keep up with cloud learning, video classrooms and admin systems. We migrated them to a 1 Gbps symmetrical Swoop Enterprise Ethernet NBN service, cut the monthly bill by \$2,000 and delivered the speed and uptime the school needed.



The issues we needed to solve

- Legacy contract with a big telco was costing thousands per month for underperforming internet
- Classrooms suffered buffering, dropped video lessons and slow cloud app performance
- Upload speeds were too slow for staff to sync files, submit reports and run online assessments
- Network dropped out during peak usage, disrupting teaching and administration
- No local support or escalation path when issues occurred during school hours

PROJECT 39 / DELIVERY

What we did — and why

01 / The work delivered

Audited the school's usage, user count and future cloud-learning roadmap

Why this mattered: Starting with the actual site and workload reduces the risk of buying equipment that cannot solve the underlying problem.

02 / The work delivered

Procured and provisioned a 1 Gbps symmetrical Swoop Enterprise Ethernet NBN service

Why this mattered: Reliable connectivity is the foundation for the applications above it; changing software cannot repair an inadequate physical or network path.

03 / The work delivered

Replaced the ageing firewall and core switch with business-grade managed hardware

Why this mattered: Reliable connectivity is the foundation for the applications above it; changing software cannot repair an inadequate physical or network path.

04 / The work delivered

Segmented staff, student and guest traffic with VLANs and content filtering

Why this mattered: Guests, cameras and business systems have different trust levels, so they should not inherit unrestricted access to each other.

05 / The work delivered

Configured quality-of-service rules to prioritise classroom video and cloud apps

Why this mattered: Moving the workload or retiring obsolete dependencies reduces the amount of legacy infrastructure the business still has to operate.

06 / The work delivered

Delivered ongoing monitoring, support and reporting through our managed service

Why this mattered: Installing a system is not the end of the security job: visibility and control are needed while staff continue to use it.

PROJECT 39 / BUSINESS RESULT

What changed for the business

\$2,000 saved every month on internet costs	\$24,000 estimated annual savings
1Gbps symmetrical Swoop Enterprise Ethernet NBN	99.9%+ business-grade uptime SLA
Local support and fast escalation	

What we used — and its role

Swoop

The recorded carrier service provides the WAN connection; routing, wireless and user support remain separate design decisions.

The sales conversation

If your organisation recognises these same issues, start with the constraint rather than a product list: which part of the environment interrupts staff, exposes data or makes growth harder? We can review the current setup, identify dependencies and scope the relevant services before recommending a change.



A word from the stable

The right connection makes the rest of the office happier.

1300 904 635 | hello@uitg.com.au

PROJECT 39 / QUESTIONS

A closer look at the solution

Why was the big telco so much more expensive?

Large carriers often charge premium rates for legacy contracts, bundled hardware and long minimum terms. Swoop's Enterprise Ethernet NBN is priced competitively for symmetrical, uncontended business-grade service, which is why we could cut the school's bill by \$2,000 a month while upgrading speed.

What is Swoop Enterprise Ethernet NBN?

It is a business-grade fibre service delivered over the NBN network with symmetrical upload and download speeds, committed bandwidth, static IP options and an SLA. For schools and offices running cloud apps and video, it is a major step up from standard NBN.

Did the school have downtime during the cutover?

No. We planned the migration around the school timetable, ran both services in parallel where possible, and cut over during a scheduled maintenance window so classes were not disrupted.

Can you do the same for other schools or education providers?

Yes. We work with schools, colleges and training providers across Australia. Call 1300 904 635 or email hello@uitg.com.au to review your current internet bill and see if a Swoop Enterprise Ethernet NBN migration can save money and improve performance.

PROJECT 40 / FINANCIAL SERVICES

Network Rebuild for a Financial Services Provider After Storm Damage

Ubiquiti network rebuild

A financial services provider's ageing network equipment was destroyed in a thunderstorm, leaving staff without internet, phones or access to cloud applications. We designed and installed a complete Ubiquiti network stack — four ceiling-mounted Wi-Fi 6 access points, new PoE switches, a UniFi Cloud Gateway, a 250 Mbps symmetrical Superloop FTTP NBN connection and a line-interactive UPS — restoring reliable, secure connectivity for the office and client meeting rooms.



The issues we needed to solve

- Legacy network gear was damaged by a thunderstorm and would not power back on
- No internet, VoIP phones or cloud app access for the entire office
- Old switches lacked PoE and could not support modern access points or phones
- Wi-Fi coverage was patchy, with dead zones in meeting rooms and client areas
- No UPS meant every power blip caused downtime and risked hardware damage
- The business needed a fast, secure rebuild with minimal disruption to client services

PROJECT 40 / DELIVERY

What we did — and why

01 / The work delivered

Installed four Ubiquiti Wi-Fi 6 access points for complete office and meeting-room coverage

Why this mattered: This workstream addressed the financial services operation's need for a maintainable service rather than leaving the original limitation in place.

02 / The work delivered

Replaced old switches with managed Ubiquiti PoE switches to power phones and access points

Why this mattered: Reliable connectivity is the foundation for the applications above it; changing software cannot repair an inadequate physical or network path.

03 / The work delivered

Deployed a Ubiquiti UniFi Cloud Gateway for routing, firewall and cloud-managed policies

Why this mattered: Moving the workload or retiring obsolete dependencies reduces the amount of legacy infrastructure the business still has to operate.

04 / The work delivered

Provisioned a 250 Mbps symmetrical Superloop FTTP NBN service with static IP addressing

Why this mattered: This workstream addressed the financial services operation's need for a maintainable service rather than leaving the original limitation in place.

05 / The work delivered

Installed a line-interactive UPS to protect the gateway, switches and NBN equipment from power events

Why this mattered: Reliable connectivity is the foundation for the applications above it; changing software cannot repair an inadequate physical or network path.

06 / The work delivered

Segmented staff, guest and voice traffic onto separate VLANs with firewall rules

Why this mattered: Guests, cameras and business systems have different trust levels, so they should not inherit unrestricted access to each other.

07 / The work delivered

Configured cloud-based monitoring and alerting so issues are visible before users notice them

Why this mattered: Installing a system is not the end of the security job: visibility and control are needed while staff continue to use it.

PROJECT 40 / BUSINESS RESULT

What changed for the business

4 Ubiquiti Wi-Fi 6 access points	250Mbps symmetrical Superloop FTTP
1 UniFi Cloud Gateway	1 UPS protecting core network
Same day core connectivity restored	Full office Wi-Fi and phone coverage

What we used — and its role

Ubiquiti / UniFi

Centrally managed switching, routing or wireless can be maintained as one office-network platform rather than as disconnected devices.

The sales conversation

If your organisation recognises these same issues, start with the constraint rather than a product list: which part of the environment interrupts staff, exposes data or makes growth harder? We can review the current setup, identify dependencies and scope the relevant services before recommending a change.



A word from the stable

The right connection makes the rest of the office happier.

1300 904 635 | hello@uitg.com.au

PROJECT 40 / QUESTIONS

A closer look at the solution

Why did you choose Ubiquiti for the rebuild?

Ubiquiti gives us enterprise-grade Wi-Fi, switching and routing in a single cloud-managed platform. It is fast to deploy, easy to monitor, and cost-effective for a small-to-medium office that still needs reliable, secure connectivity.

What does the UPS protect?

The UPS protects the UniFi Cloud Gateway, PoE switches and NBN termination equipment from power surges, brownouts and short outages. It keeps the network running through brief interruptions and allows a graceful shutdown if power is lost for longer.

How quickly was the office back online?

Core connectivity was restored the same day we installed the new equipment. Full Wi-Fi tuning, VLAN segmentation and phone integration were completed within 48 hours.

Is the new network secure enough for financial data?

Yes. We configured firewall policies, guest and voice VLANs, WPA3-Enterprise Wi-Fi where supported, automatic firmware updates, and cloud alerting. The setup aligns with the Essential Eight and can be hardened further for specific compliance requirements.

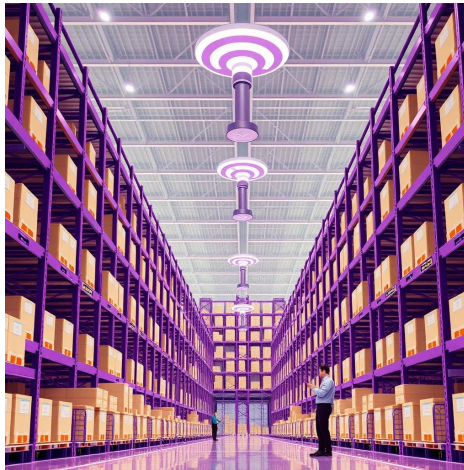
Can this solution scale if the business grows?

Absolutely. The Ubiquiti platform scales from a single office to multi-site deployments. Additional access points, switches and sites can be added to the same cloud controller without replacing the core design.

Wi-Fi 7 Upgrade for an MCG-Sized Warehouse

Wi-Fi 7 warehouse rollout

A distribution centre roughly the size of an MCG field had dead wireless zones between long racking aisles, pick scanners dropping connections, Wi-Fi Yealink phones cutting out, and tracking tags on pick bins losing their signal. We installed 89 Ubiquiti Wi-Fi 7 access points along every aisle, overhead and in pack/dispatch so operations now run smoothly from one end of the shed to the other.



The issues we needed to solve

- Warehouse floor is roughly the size of an MCG field with long metal racking aisles blocking signal
- Handheld pick scanners constantly dropped their Wi-Fi connection between aisles
- Wi-Fi Yealink phones cut out mid-call, slowing pack and dispatch coordination
- Tracking tags on pick bins failed to report location across large open areas
- Existing access points were consumer-grade, underpowered and poorly positioned
- Roaming between access points was slow, causing session drops and reconnection delays

PROJECT 41 / DELIVERY

What we did — and why

01 / The work delivered

Performed a full warehouse RF site survey mapping racking, aisles, pack/dispatch and high-density zones

Why this mattered: Starting with the actual site and workload reduces the risk of buying equipment that cannot solve the underlying problem.

02 / The work delivered

Installed 89 Ubiquiti Wi-Fi 7 access points — aisle-mounted, ceiling-mounted and pack/dispatch coverage

Why this mattered: Installing a system is not the end of the security job: visibility and control are needed while staff continue to use it.

03 / The work delivered

Designed overlapping cells with careful channel planning and power tuning for seamless roaming

Why this mattered: This workstream addressed the warehousing & logistics operation's need for a maintainable service rather than leaving the original limitation in place.

04 / The work delivered

Segmented networks into scanner, voice, tag tracking and guest VLANs for security and QoS

Why this mattered: Guests, cameras and business systems have different trust levels, so they should not inherit unrestricted access to each other.

05 / The work delivered

Enabled Wi-Fi 7 features for lower latency, better density handling and faster roaming

Why this mattered: This workstream addressed the warehousing & logistics operation's need for a maintainable service rather than leaving the original limitation in place.

06 / The work delivered

Configured cloud-based monitoring and alerting for access point health, client counts and interference

Why this mattered: Installing a system is not the end of the security job: visibility and control are needed while staff continue to use it.

PROJECT 41 / BUSINESS RESULT

What changed for the business

89 Ubiquiti Wi-Fi 7 access points installed	MCG-sized warehouse floor fully covered
100% of pick scanner aisles with stable connectivity	Stable Wi-Fi Yealink phone calls across the floor
Live pick-bin tracking tag location reporting	

What we used — and its role

Ubiquiti / UniFi

Centrally managed switching, routing or wireless can be maintained as one office-network platform rather than as disconnected devices.

The sales conversation

If your organisation recognises these same issues, start with the constraint rather than a product list: which part of the environment interrupts staff, exposes data or makes growth harder? We can review the current setup, identify dependencies and scope the relevant services before recommending a change.



A word from the stable

The right connection makes the rest of the office happier.

1300 904 635 | hello@uitg.com.au

PROJECT 41 / QUESTIONS

A closer look at the solution

Why did the warehouse need 89 access points for Wi-Fi 7 coverage?

A long, open, MCG-sized warehouse with metal racking creates signal shadows and dead zones. 89 carefully placed Wi-Fi 7 access points along aisles, ceilings and dispatch areas deliver overlapping coverage, high device density support and fast roaming for scanners, phones and tracking tags.

Will pick scanners work reliably after a Wi-Fi 7 warehouse upgrade?

Yes. The new design gives 100% aisle coverage with overlapping Wi-Fi 7 cells and fast roaming. Pick scanners now stay connected the full length of every aisle instead of dropping off when staff move between racks.

Do Wi-Fi Yealink phones work well on a warehouse Wi-Fi 7 network?

Yes. We place access points close to pack, dispatch and aisle endpoints and put voice traffic on its own VLAN with quality-of-service priority. Yealink Wi-Fi phones now hold calls clearly across the warehouse floor without cutting out mid-conversation.

Can tracking tags on pick bins be tracked accurately across a large warehouse?

Yes. With full Wi-Fi 7 coverage and dedicated tag-tracking VLANs, pick-bin tracking tags report location live across the entire MCG-sized floor. That lets staff find bins faster and improves inventory accuracy.

Can pick scanners, Wi-Fi phones and tracking tags all run on the same network?

Yes, but we segment them into separate VLANs with quality-of-service rules. That keeps voice calls clear, scanner traffic responsive, and tracking tag reports reliable even when hundreds of devices are connected at once.

What improvements does Wi-Fi 7 bring over older Wi-Fi for a warehouse?

Wi-Fi 7 offers lower latency, better performance in high-density environments, faster roaming between access points, and improved reliability in large open spaces. That means fewer dropped scanner sessions and clearer Wi-Fi phone calls for staff on the move.

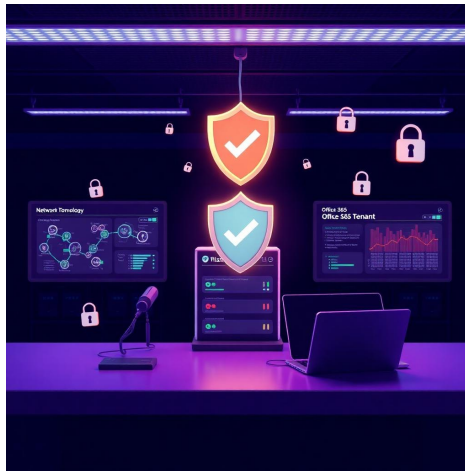
Do you support warehouses and distribution centres across Australia?

Yes. We service businesses all over Australia, from metro distribution centres to regional warehouses. Call 1300 904 635 or email hello@uitg.com.au to discuss a site survey and Wi-Fi design for your facility.

Attackers Caught Minutes After Guardz 24/7/365 MDR Deployment

Managed detection & response

A business suspected something was wrong on its network and in Office 365 but had no visibility into active threats. We deployed Guardz 24/7/365 MDR across servers and workstations and enabled Office 365 MDR for mailbox and identity monitoring. Within minutes the 24/7/365 Security Operations Center identified active attackers, isolated compromised endpoints and revoked malicious Office 365 sessions before data could be exfiltrated.



The issues we needed to solve

- Suspicious activity was occurring on the network and in Office 365 with no internal security team to investigate
- Existing antivirus had not flagged the intrusion, leaving attackers free to move laterally
- Unusual logins and mailbox rules hinted at Office 365 compromise but alerts were going unnoticed
- No 24/7 monitoring meant threats could operate overnight and on weekends
- The business needed rapid containment without disrupting day-to-day operations

PROJECT 42 / DELIVERY

What we did — and why

01 / The work delivered

Deployed Guardz 24/7/365 MDR protection across servers, workstations and Microsoft 365 for continuous monitoring

Why this mattered: Installing a system is not the end of the security job: visibility and control are needed while staff continue to use it.

02 / The work delivered

Enabled Office 365 MDR to monitor Entra ID sign-ins, mailbox rules, email forwarding and data access

Why this mattered: Installing a system is not the end of the security job: visibility and control are needed while staff continue to use it.

03 / The work delivered

Within minutes the 24/7/365 Security Operations Center confirmed active attacker behaviour and notified our team

Why this mattered: This workstream addressed the professional services operation's need for a maintainable service rather than leaving the original limitation in place.

04 / The work delivered

Isolated compromised endpoints from the network to stop lateral movement

Why this mattered: Guests, cameras and business systems have different trust levels, so they should not inherit unrestricted access to each other.

05 / The work delivered

Revoked malicious Office 365 sessions, forced password resets and enforced MFA

Why this mattered: Passwords alone leave accounts exposed; additional access checks make stolen credentials less useful to an attacker.

06 / The work delivered

Conducted a threat-hunt across the environment for persistence, backdoors and data access

Why this mattered: Installing a system is not the end of the security job: visibility and control are needed while staff continue to use it.

07 / The work delivered

Delivered a full incident report with hardening recommendations and ongoing MDR coverage

Why this mattered: This workstream addressed the professional services operation's need for a maintainable service rather than leaving the original limitation in place.

PROJECT 42 / BUSINESS RESULT

What changed for the business

Minutes from deployment to active-threat detection	100% of compromised endpoints isolated
0 data exfiltration incidents	24/7/365 SOC monitoring now in place
Full incident report and remediation roadmap delivered	

What we used — and its role

Guardz

Managed detection and response adds ongoing threat review and response beyond a one-off security installation.

Microsoft 365

Cloud email and collaboration reduce dependence on local mail servers and make access and administration consistent across devices.

The sales conversation

If your organisation recognises these same issues, start with the constraint rather than a product list: which part of the environment interrupts staff, exposes data or makes growth harder? We can review the current setup, identify dependencies and scope the relevant services before recommending a change.



A word from the stable

The horn is optional. Layered protection isn't.

1300 904 635 | hello@uitg.com.au

PROJECT 42 / QUESTIONS

A closer look at the solution

What is Guardz 24/7/365 MDR and how does it find attackers?

Guardz Managed Detection and Response continuously watches endpoints, identities, email and cloud activity for suspicious behaviour. When it detects an active threat, the 24/7/365 Security Operations Center investigates in real time and works with us to contain it.

How fast can Guardz 24/7/365 MDR detect an active attacker?

In this case the attackers were identified within minutes of the MDR deployment. Continuous monitoring and a 24/7 SOC mean threats are caught quickly instead of lingering undetected for weeks or months.

What does Office 365 MDR monitor?

Office 365 MDR watches Entra ID sign-ins, mailbox rules, email forwarding, data downloads, privileged account activity and unusual access patterns. It catches account takeovers, business email compromise and suspicious cloud behaviour.

Will deploying MDR disrupt our business?

No. Guardz MDR protection deploys quickly with minimal disruption. Containment actions such as isolating a compromised device can be performed surgically without taking the whole network offline.

Do you provide 24/7 incident response?

Yes. We combine Guardz MDR's 24/7/365 Security Operations Center with our own Australian-based support. Call 1300 904 635 or email hello@uitg.com.au to discuss MDR for your endpoints and Microsoft 365 environment.

PROJECT 43 / RURAL & AGRICULTURE

Starlink and Ubiquiti Wireless for a Remote Cattle Station

Rural connectivity

A remote cattle station lost all internet access when the local 3G network was shut down. The homestead, yards and outbuildings needed reliable connectivity for operations, safety and family communication. We installed Starlink as the primary link and four Ubiquiti outdoor access points to blanket the homestead and yard area with fast, stable Wi-Fi.



The issues we needed to solve

- 3G shutdown left the station with no usable internet at all
- Homestead, cattle yards, machinery shed and staff quarters all needed coverage
- Existing mobile coverage was patchy and insufficient for cloud apps and video calls
- Long distances and harsh outback conditions made a standard fixed-line service impossible
- Operations, weather monitoring and family communication all depended on getting connectivity back

PROJECT 43 / DELIVERY

What we did — and why

01 / The work delivered

Installed Starlink as the primary high-speed satellite internet connection

Why this mattered: Reliable connectivity is the foundation for the applications above it; changing software cannot repair an inadequate physical or network path.

02 / The work delivered

Ran four Ubiquiti outdoor wireless access points to cover the homestead, yards and outbuildings

Why this mattered: Reliable connectivity is the foundation for the applications above it; changing software cannot repair an inadequate physical or network path.

03 / The work delivered

Designed the wireless mesh to handle dust, heat and long open distances

Why this mattered: Reliable connectivity is the foundation for the applications above it; changing software cannot repair an inadequate physical or network path.

04 / The work delivered

Segmented networks for family, staff, operations and guest devices

Why this mattered: Guests, cameras and business systems have different trust levels, so they should not inherit unrestricted access to each other.

05 / The work delivered

Added a 4G failover path for critical operational traffic during Starlink maintenance

Why this mattered: The business needs a path through equipment or connection failures rather than making one component a single point of interruption.

06 / The work delivered

Configured remote monitoring so issues could be diagnosed without a long site visit

Why this mattered: Installing a system is not the end of the security job: visibility and control are needed while staff continue to use it.

PROJECT 43 / BUSINESS RESULT

What changed for the business

4 Ubiquiti access points covering homestead and yards	100+ Mbps download speeds via Starlink
24/7 connectivity for operations and safety systems	Same day remote support and diagnostics
Full coverage across the working station area	

What we used — and its role

Ubiquiti / UniFi

Centrally managed switching, routing or wireless can be maintained as one office-network platform rather than as disconnected devices.

Starlink

Satellite connectivity provides a practical connection option when usable terrestrial services are unavailable at a remote location.

The sales conversation

If your organisation recognises these same issues, start with the constraint rather than a product list: which part of the environment interrupts staff, exposes data or makes growth harder? We can review the current setup, identify dependencies and scope the relevant services before recommending a change.



A word from the stable

A stronger signal beats shouting at the router.

1300 904 635 | hello@uitg.com.au

PROJECT 43 / QUESTIONS

A closer look at the solution

Can Starlink really replace 3G or fixed-line internet in remote areas?

Yes. Starlink delivers high-speed, low-latency internet almost anywhere with a clear view of the sky. For properties that lost 3G or never had fixed-line options, it is often the best available connectivity solution.

How do you extend Starlink Wi-Fi across a large property?

We use outdoor-rated Ubiquiti access points linked back to the Starlink router. Depending on distances and layout, we run ethernet where possible or use point-to-point wireless links to reach distant sheds and yards.

Will the network handle dust, heat and storms?

Yes. We specify outdoor-rated, temperature-hardened equipment and mount it securely. Ubiquiti gear is widely used in rural and industrial environments and performs reliably in harsh Australian conditions.

What happens if Starlink goes down?

We can add a 4G or 5G failover path for critical devices and operational systems. While Starlink is very reliable, a failover ensures essential traffic keeps flowing even during maintenance or weather events.

Do you support rural properties and stations across Australia?

Yes. We service businesses all over Australia, including remote and regional properties. Call 1300 904 635 or email hello@uitg.com.au to discuss Starlink, rural wireless and backup connectivity for your location.

PROJECT 44 / MEDIA & ENTERTAINMENT

New Office 365, Entra AD and Endpoint Manager Environment for a Drone Data Company

Cloud migration & fitout

A drone data processing business demerged from its parent company and needed a completely new IT environment built from scratch. We delivered Office 365, Entra AD and Endpoint Manager for 200 users, procured 200 HP ZBook and EliteBook machines plus high-spec desktop workstations, installed dual WatchGuard firewalls in cluster, a 10 Gbps internet connection, Ubiquiti switching and Wi-Fi, and over 800 TB of Wasabi S3 object storage accessed through Lucid Link.



The issues we needed to solve

- Demerger required a brand-new IT environment with no dependency on the parent company's systems
- 200 users needed email, files, identity, devices and security policies provisioned quickly
- Drone data processing demanded extremely high-spec desktops with large curved displays and fast storage
- Over 800 TB of project data had to be migrated and made available without expensive cloud egress
- Engineers needed to collaborate on massive datasets from multiple offices as if files were local
- No existing firewalls, switches, wireless or internet service at the new premises

PROJECT 44 / DELIVERY

What we did — and why

01 / The work delivered

Built a new Entra ID tenant with custom domain, conditional access and MFA for all users

Why this mattered: Passwords alone leave accounts exposed; additional access checks make stolen credentials less useful to an attacker.

02 / The work delivered

Deployed Office 365 Exchange Online, SharePoint Online and Microsoft Teams for the 200-user workforce

Why this mattered: Moving the workload or retiring obsolete dependencies reduces the amount of legacy infrastructure the business still has to operate.

03 / The work delivered

Configured Microsoft Endpoint Manager (Intune) with autopilot, compliance policies, Wi-Fi certificates and required apps

Why this mattered: A consistent device baseline makes deployment and ongoing support more predictable for staff and the service team.

04 / The work delivered

Procured 200 HP ZBook and HP EliteBook laptops plus high-spec HP desktop workstations for drone data processing

Why this mattered: A consistent device baseline makes deployment and ongoing support more predictable for staff and the service team.

05 / The work delivered

Supplied 45-inch curved widescreens, USB-C docks, keyboards and mice for every workstation

Why this mattered: A consistent device baseline makes deployment and ongoing support more predictable for staff and the service team.

06 / The work delivered

Installed two WatchGuard firewalls in high-availability cluster with full traffic inspection and VPN

Why this mattered: This workstream addressed the media & entertainment operation's need for a maintainable service rather than leaving the original limitation in place.

07 / The work delivered

Delivered a 10 Gbps internet connection and a 10 Gbps aggregation switch linking all Ubiquiti access switches and firewalls

Why this mattered: Reliable connectivity is the foundation for the applications above it; changing software cannot repair an inadequate physical or network path.

08 / The work delivered

Deployed eight Ubiquiti Wi-Fi 6 access points across two building levels with seamless roaming

Why this mattered: This workstream addressed the media & entertainment operation's need for a maintainable service rather than leaving the original limitation in place.

09 / The work delivered

Migrated over 800 TB of drone imagery and project data into Wasabi S3 storage

Why this mattered: Moving the workload or retiring obsolete dependencies reduces the amount of legacy infrastructure the business still has to operate.

10 / The work delivered

Configured Lucid Link so editors and engineers can stream project files directly from object storage without local sync

Why this mattered: This workstream addressed the media & entertainment operation's need for a maintainable service rather than leaving the original limitation in place.

11 / The work delivered

Integrated Xero and Employment Hero with single sign-on where supported and provided secure access policies

Why this mattered: This workstream addressed the media & entertainment operation's need for a maintainable service rather than leaving the original limitation in place.

12 / The work delivered

Provided ongoing help desk support, asset management and monthly reporting through our managed service

Why this mattered: This workstream addressed the media & entertainment operation's need for a maintainable service rather than leaving the original limitation in place.

PROJECT 44 / BUSINESS RESULT

What changed for the business

200 users and machines migrated to the new environment	800TB+ project data stored in Wasabi S3 via Lucid Link
10Gbps internet and core aggregation switching	8 Ubiquiti access points across two levels
2 WatchGuard firewalls in HA cluster	45" curved widescreens at every drone data workstation

What we used — and its role

WatchGuard

A managed firewall platform combines traffic control, secure access and, where deployed, SD-WAN policy in a consistent operating model.

Ubiquiti / UniFi

Centrally managed switching, routing or wireless can be maintained as one office-network platform rather than as disconnected devices.

Microsoft 365

Cloud email and collaboration reduce dependence on local mail servers and make access and administration consistent across devices.

Intune / Autopilot

Policy-driven deployment helps standardise devices and reduces manual setup when a user receives a replacement computer.

SharePoint / Teams / OneDrive

Shared cloud workspaces separate business files and collaboration from a single office server or an individual computer.

Wasabi S3

Object storage provides a cloud destination for the recorded backup or file-data architecture, distinct from the users' local devices.

LucidLink

File streaming makes cloud-held project data accessible to applications without requiring a full local copy of every dataset first.

HP / Microsoft Surface

Business-class devices matched to staff roles create a more supportable endpoint estate than inconsistent personal or ageing computers.

The sales conversation

If your organisation recognises these same issues, start with the constraint rather than a product list: which part of the environment interrupts staff, exposes data or makes growth harder? We can review the current setup, identify dependencies and scope the relevant services before recommending a change.



A word from the stable

Old dependencies don't retire themselves.

1300 904 635 | hello@uitg.com.au

PROJECT 44 / QUESTIONS

A closer look at the solution

Why use Wasabi S3 instead of keeping everything in SharePoint?

Drone projects generate many terabytes of raw imagery, point clouds and video. SharePoint and OneDrive are not cost-effective or performant at that scale. Wasabi S3 provides predictable, low-cost object storage with no egress fees, and Lucid Link lets the team work with those files as if they were on a local drive.

What is Lucid Link and how does it help?

Lucid Link is a file streaming platform that connects creative and technical applications directly to cloud object storage. It means the drone team can open and edit multi-terabyte projects without waiting for full downloads or syncing everything locally.

How did you provision 200 machines so quickly?

We used Windows Autopilot and Microsoft Endpoint Manager. Devices were shipped from HP directly to users or staged in our workshop, then enrolled automatically with policies, apps, Wi-Fi certificates and printer mappings already applied.

Why two WatchGuard firewalls instead of one?

The firewalls run in a high-availability cluster. If one unit fails or needs maintenance, the second takes over automatically so the 200 users and critical drone data workflows stay online.

Can you support Xero and Employment Hero as part of managed services?

Yes. We help with identity setup, secure access policies, browser and app issues, and integration advice. For accounting and HR platform configuration we work alongside the customer's bookkeeper or payroll team.

PROJECT 45 / CONSTRUCTION

National Home Builder Turnaround After Malware Incident

Managed services & security

A malware incident exposed years of under-investment in a national home builder's IT. With 300 staff across seven offices, the problem extended well beyond infected computers: unmanaged personal devices, unreliable tape backups, ageing networks, non-compliant software, costly telephony and legacy data-centre infrastructure. Unicorn IT Group delivered a business-wide turnaround covering devices, security, backup, connectivity, cloud data, communications and ongoing support.



The issues we needed to solve

- Malware entered through sales staff's personal devices connecting to legacy company file shares, without central patching or device management. The legacy file shares were unsegmented.
- Years of under-investment left ageing servers, switches and even an old network hub in production.
- Seven offices relied on an expensive MPLS IPWAN, with older servers hosted at NEXTDC and ongoing data-centre overheads.
- Tape backups were unreliable and slow to restore, with no effective off-site disaster recovery arrangement.
- A major-telco hosted phone platform cost approximately \$10,000 each month.
- Microsoft software licensing was largely non-compliant, including pirated software.
- The 300-endpoint estate was outdated and inconsistent, mixing business equipment with personal machines.
- There was no formal data loss prevention, application control or modern endpoint protection.
- Legacy file shares and server dependencies complicated access to business files across the national operation.
- The print fleet included equipment around 20 years old, while business processes also needed modernisation.

- Display-home sales teams needed support outside a conventional office-only weekday service window.

PROJECT 45 / DELIVERY

What we did — and why

1. Removing the personal-device malware pathway

The issue

Sales staff used personal machines to reach legacy company file shares. Without central patching, security software or management on those devices, the business could not enforce a consistent security baseline. The recorded malware incident was traced to this access path.

The work delivered

Unicorn IT Group removed personal devices from the corporate network and replaced the endpoint estate with 300 business machines: HP Z Towers, HP ZBooks and Microsoft Surface laptops for the sales teams. The devices were enrolled, encrypted and centrally managed, with workstations for design and estimating, ZBooks for technical staff and Surface laptops for sales. This made device replacement part of the security response, rather than treating the infection as an isolated clean-up.

The change

The sales team retained portable access to its work on company-managed equipment. The documented personal-device route was removed and the business gained a consistent foundation for endpoint security and support.

2. Adding endpoint detection and managed response

The issue

The previous environment had no modern endpoint protection or formal application control. Replacing hardware alone would not address malicious software, unknown applications or the need to investigate suspicious activity.

The work delivered

We rolled out SentinelOne EDR, Guardz 24/7/365 managed detection and response, and basic application controls across the endpoint estate, alongside credential and MFA resets, legacy-share lockdown and monitoring. SentinelOne provides endpoint detection and response; Guardz adds managed threat monitoring and response. Application controls provide an additional restriction on software execution.

The change

Security moved from an unmanaged device-by-device position to a layered operating model. This is a description of the controls deployed, not a claim that future incidents are impossible or that a specific malware family was identified.

3. Protecting information and correcting licensing

The issue

Customer details, pricing and project information lacked formal data loss prevention. Microsoft licensing was largely non-compliant and included pirated software, creating a separate legal and operational problem alongside the malware incident.

The work delivered

We introduced Microsoft 365 DLP policies to protect those business data categories, conditional access and staff security awareness training, and moved the organisation to compliant Office 365 and Microsoft 365 licensing. Licensing remediation and data protection were treated as distinct requirements: legitimate software entitlement does not, by itself, prevent information leakage.

The change

The builder gained a legitimate licensing foundation and policy-based protection for sensitive business information. The published record does not specify individual licence quantities, DLP rules or an external compliance certification.

4. Replacing unreliable tape backups

The issue

Tape backups were unreliable and slow to restore, with no effective off-site disaster recovery arrangement. The incident highlighted why merely having a backup process was not enough when recovery depended on ageing media and manual handling.

The work delivered

We replaced tape with Cove Backup for endpoints, servers and Microsoft 365 data, including mailboxes, SharePoint and OneDrive. The longer brochure account records immutable off-site backup, daily monitoring and fortnightly restore testing with evidence. Cloud backup removed the reliance on couriering tapes and made off-site recovery part of the environment rather than a separate media-handling exercise.

The change

The replacement provided automated cloud backups and a more practical route to restores and recovery testing. The recorded testing cadence was fortnightly; individual restore times and recovery-point targets are not published, so no numerical recovery guarantee is asserted.

5. Rebuilding connectivity across seven offices

The issue

An expensive MPLS IPWAN connected the national office network. The legacy model was inflexible, while business users increasingly needed bandwidth for cloud applications, file access and modern communications.

The work delivered

We migrated the wide-area network to WatchGuard SD-WAN. Each office received at least 1 Gbps Swoop Broadband Enterprise Ethernet NBN, with 1000/400 FTTP backup connectivity. WatchGuard provided a common firewall and SD-WAN platform with automatic failover to the backup links.

The change

All seven offices moved to the new SD-WAN design with high-bandwidth primary services and backup connections. Swoop was the carrier for this historical project; the case study is not being rewritten to name a different provider used in current offers.

6. Refreshing switching and wireless inside the offices

The issue

The problems were not limited to internet connections. Ageing office switches and wireless infrastructure remained in service, and the refresh uncovered an old network hub still being used in production.

The work delivered

We replaced the old hub and refreshed office switching and wireless access points with Ubiquiti equipment. This addressed the local network underneath the new WAN and the new endpoint fleet, rather than leaving old internal equipment as a weak point in an otherwise upgraded environment.

The change

The offices gained modern switching and wireless to support staff devices and business services. Exact access-point counts, switch models, VLAN layouts and measured Wi-Fi coverage results are not recorded in the published case study.

7. Moving files away from legacy server dependencies

The issue

Business data depended on old file shares and hosted servers. Those shares were also involved in the personal-device malware pathway, so modernising file access formed part of both the infrastructure programme and the wider risk reduction.

The work delivered

We migrated file data to SharePoint and LucidLink, with Wasabi S3 object storage. The change moved file access away from the previous legacy-share model and aligned the data environment with the builder's modernised devices, Microsoft services and national connectivity.

The change

The business gained a cloud-based file environment and reduced reliance on the old hosted server estate. The record does not specify the volume of migrated data or the exact split of workloads between SharePoint and LucidLink.

8. Retiring virtual servers and data-centre racks

The issue

Older servers hosted at NEXTDC and two racks of equipment added infrastructure to operate and maintain. Keeping that legacy footprint after modernising business services would have preserved unnecessary dependencies.

The work delivered

As the environment was modernised, we decommissioned 18 virtual servers and removed two racks of equipment from the data centre. Server retirement was a separate deliverable from replacing user devices: it reduced the hosted infrastructure remaining behind the new workplace environment.

The change

The confirmed infrastructure result is 18 virtual servers retired and two racks removed. The published record does not include a data-centre invoice comparison, so rack removal is not converted into an invented monthly dollar saving.

9. Replacing the expensive hosted phone platform

The issue

The major-telco hosted phone system cost approximately \$10,000 per month. Communications therefore represented a material operating expense as well as another platform to modernise for a distributed sales and office workforce.

The work delivered

We moved the business to 3CX with Swoop SIP trunks. The replacement supported mobile apps, softphones and easier call routing, giving the business a different operating model from the previous hosted phone arrangement.

The change

The monthly bill fell to a small fraction of the previous approximately \$10,000 spend. A final monthly invoice is not included in the project record, so this edition does not claim an exact percentage saving, annual saving or payback period.

10. Replacing the ageing print fleet

The issue

The business was still using printers around 20 years old. This was another sign of under-investment and a separate operational issue that would not be solved by installing endpoint security or replacing internet connections.

The work delivered

We replaced the ageing printers with a managed Konica print fleet. Print was included in the wider workplace refresh so the builder's daily office requirements were addressed alongside laptops, desktop workstations, networks and communications.

The change

The organisation moved from ageing equipment to a managed print arrangement. Printer quantities, per-page rates and measured print-cost savings are not part of the published record and are not asserted here.

11. Improving business processes with Dynamics 365

The issue

A complete turnaround needed to support how the builder worked, not just replace technology. Business processes needed improvement as the company moved away from its under-invested legacy environment.

The work delivered

We worked with Dynamics Squared to introduce Dynamics 365 and improve business processes. This partner involvement complemented Unicorn IT Group's work on infrastructure, security, cloud data, devices and support.

The change

Dynamics 365 became part of the modernisation programme. Specific modules, integrations, workflow designs and quantified productivity gains are not identified in the published project record.

12. Making ongoing support fit the sales operation

The issue

A national home builder's sales activity does not stop when a conventional weekday office closes. Display-home staff needed a support arrangement that reflected weekend trading, while seven offices and 300 staff needed a managed service beyond the immediate incident.

The work delivered

We onboarded the business to fully managed IT support with a project-specific 7am–7pm weekday service window and weekend cover for display-home sales teams. This connected the transformation to ongoing service ownership rather than leaving the builder with a collection of one-off upgrades. The longer programme account also records a managed-service SLA, monthly reporting and documented, monitored infrastructure.

The change

The organisation gained support aligned to its office and sales operations. These were this client's service arrangements, not a statement of Unicorn IT Group's standard office hours or a promise that every current plan includes the same support window.

PROJECT 45 / BUSINESS RESULT

What changed for the business

300 HP and Surface endpoints deployed	7 offices connected over SD-WAN
18 virtual servers decommissioned	2 racks data-centre equipment removed
1 Gbps+ primary connectivity per office	1000/400 FTTP backup links
3CX replaced the ~\$10,000/month phone service	7am-7pm weekday support plus weekend sales cover

What we used — and its role

SentinelOne

Endpoint detection and response helps identify suspicious activity on computers and supports investigation and containment.

Guardz

Managed detection and response adds ongoing threat review and response beyond a one-off security installation.

WatchGuard

A managed firewall platform combines traffic control, secure access and, where deployed, SD-WAN policy in a consistent operating model.

Ubiquiti / UniFi

Centrally managed switching, routing or wireless can be maintained as one office-network platform rather than as disconnected devices.

Microsoft 365

Cloud email and collaboration reduce dependence on local mail servers and make access and administration consistent across devices.

SharePoint / Teams / OneDrive

Shared cloud workspaces separate business files and collaboration from a single office server or an individual computer.

Cove Backup

Dedicated backup provides a recovery layer separate from production systems and day-to-day file access.

Wasabi S3

Object storage provides a cloud destination for the recorded backup or file-data architecture, distinct from the users' local devices.

LucidLink

File streaming makes cloud-held project data accessible to applications without requiring a full local copy of every dataset first.

3CX

A software-based phone system supports central call routing and flexible extensions without preserving the old PBX operating model.

Swoop

The recorded carrier service provides the WAN connection; routing, wireless and user support remain separate design decisions.

HP / Microsoft Surface

Business-class devices matched to staff roles create a more supportable endpoint estate than inconsistent personal or ageing computers.

Konica / managed print

A managed print platform brings device support and print administration into a maintainable workplace service.

Dynamics 365

Business applications address operational workflows alongside the infrastructure and security improvements.

The sales conversation

If your organisation recognises these same issues, start with the constraint rather than a product list: which part of the environment interrupts staff, exposes data or makes growth harder? We can review the current setup, identify dependencies and scope the relevant services before recommending a change.



A word from the stable

The horn is optional. Layered protection isn't.

1300 904 635 | hello@uitg.com.au

PROJECT 45 / QUESTIONS

A closer look at the solution

Was this only a malware clean-up?

No. The incident exposed wider problems with personal-device access, ageing equipment, backups, licensing, data protection, connectivity, phones and support. The project addressed those underlying issues as a business-wide modernisation programme.

What equipment replaced the personal and ageing machines?

The documented rollout comprised 300 HP Z Towers, HP ZBooks and Microsoft Surface laptops, with portable Surface devices for sales teams. Personal devices were removed from the corporate network.

Which security controls were deployed?

SentinelOne EDR, Guardz 24/7/365 MDR, basic application controls and Microsoft 365 DLP policies. Microsoft licensing was also remediated. This case study does not claim a particular malware family, forensic finding or compliance certification.

Which carrier connected the offices?

This project used Swoop Broadband Enterprise Ethernet NBN at at least 1 Gbps per site, plus 1000/400 FTTP backup links, with WatchGuard SD-WAN replacing MPLS IPWAN.

What replaced the tape backups and file shares?

Cove Backup replaced tape for endpoints, servers and Microsoft 365 data, with immutable off-site storage, daily monitoring and fortnightly restore testing recorded in the programme account. File data moved to SharePoint and LucidLink with Wasabi S3 object storage. These are separate functions: cloud file access is not a substitute for backup.

How much did the new phone system save?

The old service cost approximately \$10,000 each month. 3CX with Swoop SIP trunks reduced it to a small fraction. The exact new monthly bill is not published, so no precise percentage or annual dollar saving is claimed.

Were all the old servers kept?

No. Eighteen virtual servers were decommissioned and two racks of equipment removed from the data centre as part of the modernisation.

Are the 7am-7pm hours standard for every client?

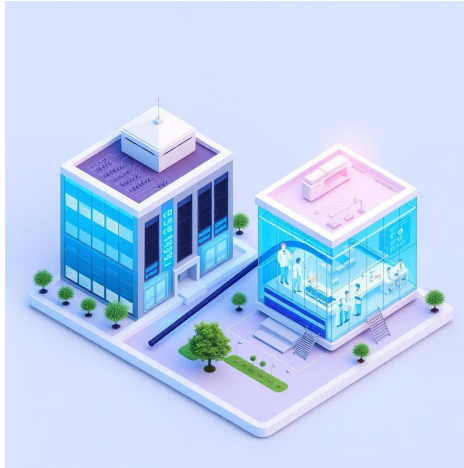
No. Weekday 7am-7pm support and weekend display-home cover describe this client's arrangement. Current support coverage and after-hours requirements are scoped separately for each business.

PROJECT 46 / HEALTHCARE & RESEARCH

100 Gbps Dark Fibre Link for Medical Research Campus

Dark Fibre

A medical research institute opened a second premise while its compute and storage servers remained in the original building. Staff needed seamless, low-latency access to large genomic and imaging datasets from the new site.



The issues we needed to solve

- New research premise had no local servers; all compute and storage sat in the original building
- Researchers needed to move multi-terabyte imaging and genomic datasets between sites daily
- Standard internet and VPN links were too slow and introduced unacceptable latency for real-time analysis
- Any outage would halt time-sensitive clinical trials and collaborative research

PROJECT 46 / DELIVERY

What we did — and why

01 / The work delivered

Surveyed both premises and the street route to confirm dark fibre path feasibility

Why this mattered: Starting with the actual site and workload reduces the risk of buying equipment that cannot solve the underlying problem.

02 / The work delivered

Procured and lit a dedicated dark fibre pair between the two buildings

Why this mattered: Reliable connectivity is the foundation for the applications above it; changing software cannot repair an inadequate physical or network path.

03 / The work delivered

Terminated 100 Gbps coherent optics at each end with redundant switch stacks

Why this mattered: The business needs a path through equipment or connection failures rather than making one component a single point of interruption.

04 / The work delivered

Configured layer-2 extension so the new premise appears on the same network segment as the original data centre

Why this mattered: Guests, cameras and business systems have different trust levels, so they should not inherit unrestricted access to each other.

05 / The work delivered

Added diverse physical routing and automatic failover to protect against fibre cuts

Why this mattered: The business needs a path through equipment or connection failures rather than making one component a single point of interruption.

PROJECT 46 / BUSINESS RESULT

What changed for the business

100Gbps dedicated dark fibre link	<1ms latency between premises
2 buildings on one logical LAN	0 shared internet dependency
24/7 research access to central storage	

The sales conversation

If your organisation recognises these same issues, start with the constraint rather than a product list: which part of the environment interrupts staff, exposes data or makes growth harder? We can review the current setup, identify dependencies and scope the relevant services before recommending a change.



A word from the stable

The right connection makes the rest of the office happier.

1300 904 635 | hello@uitg.com.au

PROJECT 46 / QUESTIONS

A closer look at the solution

Why dark fibre instead of leased Ethernet?

Dark fibre gives the research institute full control over the optics and bandwidth. A single 100 Gbps wave can be upgraded to 400 Gbps later by swapping transceivers, without renegotiating carrier contracts.

How do you keep the link running if the fibre is cut?

We designed the path with physically diverse entry points and core routing, and the edge switches support automatic failover to a backup path within milliseconds.

Can researchers access servers as if they were local?

Yes. The link is presented as a layer-2 extension, so the new premise is on the same IP subnet as the original data centre. Storage mounts, RDP and analysis tools behave exactly as they would on a local LAN.

Is 100 Gbps really needed for a research site?

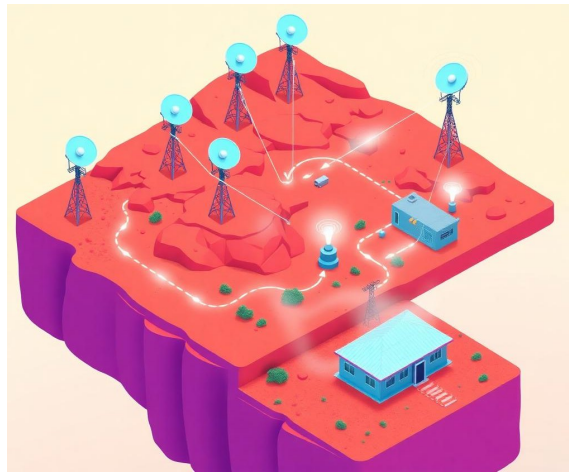
For medical imaging, genomics and large collaborative datasets, 100 Gbps removes the wait time when moving files and allows multiple researchers to work concurrently without contention.

PROJECT 47 / MINING & RESOURCES

6-Hop Solar Microwave Network Delivers 100 Mbps Fibre to Remote Mine Site

Wireless backhaul

Before Starlink existed, a remote Western Australian mine site was stuck on a 2 Mbps/2 Mbps satellite link. We designed and built a six-hop solar-powered microwave network to a Tom Price business with a 100 Mbps fibre connection, connecting the mine to its head office for the first time at real broadband speeds. The big-T telco wanted \$4.6 million to run fibre; our solution was built for \$69,000 excluding the existing Tom Price connection supplied by the mining company.



The issues we needed to solve

- Remote mine site limited to 2 Mbps/2 Mbps satellite with high latency and poor reliability
- Major telco quoted \$4.6 million to install a dedicated fibre run
- No commercial power available at relay sites across the six-hop path
- Harsh Pilbara environment with extreme heat, dust and cyclone exposure
- Need for centralised monitoring and rapid fault response across all outdoor sites

PROJECT 47 / DELIVERY

What we did — and why

01 / The work delivered

Surveyed the terrain and designed a six-hop microwave path from the mine site to a Tom Price business with existing fibre

Why this mattered: Starting with the actual site and workload reduces the risk of buying equipment that cannot solve the underlying problem.

02 / The work delivered

Built six solar-powered relay sites with battery backup, industrial enclosures and microwave dishes

Why this mattered: A recoverable copy must exist independently of the production service; synchronising files alone is not a recovery strategy.

03 / The work delivered

Specified cyclone-rated towers, mounts and grounding to survive extreme weather

Why this mattered: This workstream addressed the mining & resources operation's need for a maintainable service rather than leaving the original limitation in place.

04 / The work delivered

Tuned links for 100 Mbps symmetrical throughput with low latency and high availability

Why this mattered: The business needs a path through equipment or connection failures rather than making one component a single point of interruption.

05 / The work delivered

Deployed centralised monitoring for solar/battery health, link quality, temperature and uptime

Why this mattered: Installing a system is not the end of the security job: visibility and control are needed while staff continue to use it.

06 / The work delivered

Documented the network architecture and trained local staff on basic troubleshooting

Why this mattered: The improvement must remain usable and supportable after handover, not depend on knowledge held only by the installer.

PROJECT 47 / BUSINESS RESULT

What changed for the business

100 Mbps fibre-speed connection to head office	\$69k build cost vs \$4.6M telco quote
6 hops solar-powered microwave relay sites	Cyclone rated towers, mounts and enclosures

The sales conversation

If your organisation recognises these same issues, start with the constraint rather than a product list: which part of the environment interrupts staff, exposes data or makes growth harder? We can review the current setup, identify dependencies and scope the relevant services before recommending a change.



A word from the stable

A stronger signal beats shouting at the router.

1300 904 635 | hello@uitg.com.au

PROJECT 47 / QUESTIONS

A closer look at the solution

Why microwave instead of satellite or fibre?

At the time, Starlink was not available and satellite was limited to 2 Mbps/2 Mbps with high latency. Fibre was technically ideal but the telco quote was \$4.6 million. Microwave gave us fibre-like speed for a fraction of the cost.

How did you power the relay sites?

Each hop runs on a solar array with battery storage in an industrial enclosure. The design accounts for cloudy days and high temperatures so the radios stay online overnight and through poor weather.

Can the network survive a cyclone?

Yes. Towers, mounts, grounding and enclosures were specified and installed to cyclone ratings for the region. The microwave dishes are also rated for the wind loads expected in the Pilbara.

How is the network monitored?

We use centralised monitoring for link uptime, signal strength, latency, solar input, battery voltage and enclosure temperature. Alerts go to our support team so issues are caught before users notice them.

Could this be upgraded now that Starlink is available?

Absolutely. Many remote sites today use Starlink as primary or backup connectivity. For this site, the microwave network was the right solution at the time and can still serve as a resilient backup path.

PROJECT 48 / NOT-FOR-PROFIT

Secure Public Wi-Fi Rolled Out Across 4 Employment Services Offices in Hobart

Public wireless

An employment services provider wanted to offer free public Wi-Fi to job seekers and visitors at its four Hobart offices, but needed the network to be secure and protected against misuse. We deployed Ubiquiti UniFi wireless access points and UniFi Cloud Gateway at each office, with a separate Swoop FTTP NBN service at 250/100 Mbps dedicated to guest traffic, plus content and application filtering to keep the service safe and appropriate.



The issues we needed to solve

- Job seekers and visitors had no way to get online at the offices to search for jobs, complete applications and attend video interviews
- Public Wi-Fi had to be completely isolated from the provider's staff and client-data networks
- Content and application filtering was required to prevent misuse, inappropriate content and bandwidth abuse
- Guest traffic could not be allowed to compete with or touch the corporate internet connections
- Four offices across Hobart needed a consistent, centrally managed solution

PROJECT 48 / DELIVERY

What we did — and why

01 / The work delivered

Installed Ubiquiti UniFi wireless access points at all four offices with a dedicated guest SSID and captive portal

Why this mattered: Guests, cameras and business systems have different trust levels, so they should not inherit unrestricted access to each other.

02 / The work delivered

Deployed a UniFi Cloud Gateway at each site to handle routing, firewalling and guest network isolation

Why this mattered: Guests, cameras and business systems have different trust levels, so they should not inherit unrestricted access to each other.

03 / The work delivered

Provisioned a separate Swoop FTTP NBN service at 250/100 Mbps per office dedicated purely to public Wi-Fi

Why this mattered: This workstream addressed the not-for-profit operation's need for a maintainable service rather than leaving the original limitation in place.

04 / The work delivered

Configured VLANs and firewall rules so guest devices can reach the internet only — never the internal network

Why this mattered: Guests, cameras and business systems have different trust levels, so they should not inherit unrestricted access to each other.

05 / The work delivered

Enabled content and application filtering to block malicious, adult and high-abuse traffic categories, with bandwidth limits per user

Why this mattered: Reliable connectivity is the foundation for the applications above it; changing software cannot repair an inadequate physical or network path.

06 / The work delivered

Centralised management in UniFi so all four sites are monitored and updated from one dashboard

Why this mattered: Installing a system is not the end of the security job: visibility and control are needed while staff continue to use it.

PROJECT 48 / BUSINESS RESULT

What changed for the business

4 sites

offices with secure public Wi-Fi across Hobart

250/100

Mbps dedicated Swoop FTTP NBN per office

100%

guest traffic isolated from internal systems

1 pane

central UniFi management for every site

What we used — and its role

Ubiquiti / UniFi

Centrally managed switching, routing or wireless can be maintained as one office-network platform rather than as disconnected devices.

Swoop

The recorded carrier service provides the WAN connection; routing, wireless and user support remain separate design decisions.

The sales conversation

If your organisation recognises these same issues, start with the constraint rather than a product list: which part of the environment interrupts staff, exposes data or makes growth harder? We can review the current setup, identify dependencies and scope the relevant services before recommending a change.



A word from the stable

The right connection makes the rest of the office happier.

1300 904 635 | hello@uitg.com.au

PROJECT 48 / QUESTIONS

A closer look at the solution

Why a separate NBN service instead of sharing the office connection?

A dedicated Swoop FTTP NBN service at 250/100 Mbps means guest traffic can never slow down or interfere with the corporate connection, and it adds a clean physical separation between public users and business systems.

How is the guest network kept away from staff systems?

Guest devices sit on their own VLAN behind the UniFi Cloud Gateway. Firewall rules allow internet access only, so there is no path from the public Wi-Fi to staff computers, servers or client data.

What does content and application filtering block?

We filter malicious sites, adult content and known abuse categories, and we can restrict high-bandwidth or peer-to-peer applications. This keeps the service safe, appropriate and fair for everyone using it.

Can visitors just connect, or is there a sign-in?

Visitors connect through a captive portal with the provider's branding and an acceptable-use policy they must accept before getting online. Time and bandwidth limits can be applied per session if needed.

How are all four offices managed?

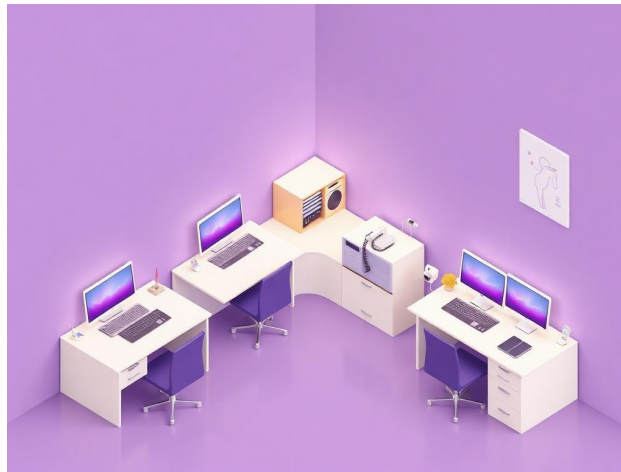
Every access point and gateway is adopted into a single UniFi management console. We monitor uptime, apply firmware updates and adjust filtering policies centrally, so all four sites stay consistent.

PROJECT 49 / REAL ESTATE

Small Real Estate Agency Moves to Fully Cloud Managed IT on the Silver Plan

Managed services

A boutique real estate agency with five staff needed everything handled — support, phones, Wi-Fi, devices and security — without hiring IT. We put them on our Silver managed services plan with 3CX hosted PABX, Ubiquiti wireless and cloud gateway, five MacBooks, forty widescreen monitors across the office and listing displays, four Meraki security cameras, and a fully cloud-based setup on Swoop 500/200 FTTP NBN.



The issues we needed to solve

- Five staff relying on ad-hoc IT with no monitoring, patching or backup in place
- Phone system was an expensive legacy PABX with no mobile or remote working support
- Office Wi-Fi was a consumer router that couldn't cope with listing uploads and video calls
- No security cameras covering the office, front of house or server/comms area
- The agency wanted to be 100% cloud — no on-premise servers to maintain or break

PROJECT 49 / DELIVERY

What we did — and why

01 / The work delivered

Onboarded all five users onto the Silver managed services plan — unlimited support, proactive monitoring, patching and security included

Why this mattered: Installing a system is not the end of the security job: visibility and control are needed while staff continue to use it.

02 / The work delivered

Replaced the legacy PABX with 3CX hosted PABX — desk phones, mobile apps and voicemail-to-email for agents on the road

Why this mattered: Communications need to follow how people work, with maintainable routing and extensions instead of the limitations of the old phone arrangement.

03 / The work delivered

Installed a Ubiquiti UniFi Cloud Gateway and wireless access point for fast, centrally managed office Wi-Fi

Why this mattered: Reliable connectivity is the foundation for the applications above it; changing software cannot repair an inadequate physical or network path.

04 / The work delivered

Supplied and configured five Apple MacBooks enrolled in MDM, with forty widescreen monitors deployed across desks and window listing displays

Why this mattered: Installing a system is not the end of the security job: visibility and control are needed while staff continue to use it.

05 / The work delivered

Installed four Cisco Meraki security cameras covering entry, office floor, comms area and rear access, with cloud recording and alerts

Why this mattered: Moving the workload or retiring obsolete dependencies reduces the amount of legacy infrastructure the business still has to operate.

06 / The work delivered

Moved email, files and line-of-business apps fully into the cloud — no on-premise servers — connected over Swoop 500/200 FTTP NBN

Why this mattered: Moving the workload or retiring obsolete dependencies reduces the amount of legacy infrastructure the business still has to operate.

PROJECT 49 / BUSINESS RESULT

What changed for the business

5 users fully managed on the Silver plan	500/200 Mbps Swoop FTTP NBN connection
40 widescreen monitors across the office	0 servers on-premise — 100% cloud based

What we used — and its role

Cisco Meraki

Cloud management gives the support team a common view of the deployed network or camera estate without needing to visit each location.

Ubiquiti / UniFi

Centrally managed switching, routing or wireless can be maintained as one office-network platform rather than as disconnected devices.

3CX

A software-based phone system supports central call routing and flexible extensions without preserving the old PBX operating model.

Swoop

The recorded carrier service provides the WAN connection; routing, wireless and user support remain separate design decisions.

The sales conversation

If your organisation recognises these same issues, start with the constraint rather than a product list: which part of the environment interrupts staff, exposes data or makes growth harder? We can review the current setup, identify dependencies and scope the relevant services before recommending a change.



A word from the stable

Less IT drama. More getting on with the day.

1300 904 635 | hello@uitg.com.au

PROJECT 49 / QUESTIONS

A closer look at the solution

What does the Silver plan include for a small office like this?

Silver includes unlimited remote support, Microsoft 365 management, proactive monitoring and patching, Office 365 backup, SentinelOne endpoint security, Guardz 24/7/365 MDR and email protection — everything a five-person office needs to stay secure and productive.

Why 3CX hosted PABX instead of keeping the old phone system?

3CX hosted PABX removes the on-premise phone box entirely. Agents take calls on desk phones, laptops or mobile apps with one number, and features like voicemail-to-email and call queues are included — ideal for agents out at inspections.

Why MacBooks for a real estate agency?

The team preferred macOS, and MacBooks suit mobile agents. We enrol them in MDM so every device is encrypted, patched and configured with the agency's apps before it's handed over.

How are the cameras managed?

The four Meraki cameras record to the cloud and are managed from the Meraki dashboard. We get alerts for motion after hours, and footage can be reviewed from anywhere without a recorder on site.

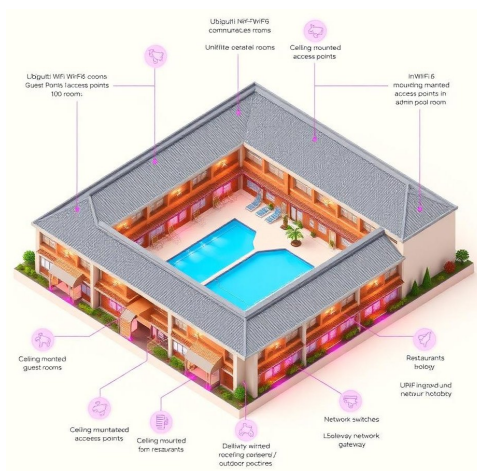
Is 500/200 FTTP enough for a five-person office?

Easily. The Swoop 500/200 FTTP NBN service handles cloud file sync, video calls, 3CX voice and listing uploads with headroom to spare, and Enterprise Ethernet is available if they ever outgrow it.

New Motel Delivers Fast Guest Wi-Fi Across 100 Rooms

Guest Wi-Fi

A new 100-room motel needed reliable, fast Wi-Fi in every room and across all guest areas from day one. We designed the network during construction, pre-wiring each room with four network ports back to four comms rooms, then connected every comms room by fibre to a central admin room with Swoop 1 Gbps fibre, Ubiquiti aggregation switches and a UniFi gateway. Each room received an in-wall Wi-Fi 6 access point, with ceiling access points in hallways, lobby, restaurant and outdoor pool and games areas.



The issues we needed to solve

- 100 rooms needed strong, consistent Wi-Fi for streaming, video calls and smart devices
- Guest areas including pool, games area, restaurant, check-in and hallways needed coverage too
- The network had to be designed before walls were closed up, with cabling back to multiple comms rooms
- Four comms rooms needed to be linked to a central admin room with high-capacity fibre backhaul
- The solution needed to be easy to manage and support as the motel grew

PROJECT 50 / DELIVERY

What we did — and why

01 / The work delivered

Worked with the builder during construction to pre-wire every room with four network ports back to the nearest comms room

Why this mattered: This workstream addressed the hospitality & tourism operation's need for a maintainable service rather than leaving the original limitation in place.

02 / The work delivered

Installed four comms rooms with Ubiquiti UniFi switches, each connected by fibre to the central admin comms room

Why this mattered: Reliable connectivity is the foundation for the applications above it; changing software cannot repair an inadequate physical or network path.

03 / The work delivered

Provisioned Swoop 1 Gbps fibre internet to the central admin room for high-speed, symmetrical backhaul

Why this mattered: Reliable connectivity is the foundation for the applications above it; changing software cannot repair an inadequate physical or network path.

04 / The work delivered

Installed a Ubiquiti aggregation switch and UniFi gateway at the central admin room for routing and central management

Why this mattered: Reliable connectivity is the foundation for the applications above it; changing software cannot repair an inadequate physical or network path.

05 / The work delivered

Fitted every guest room with an in-wall Ubiquiti Wi-Fi 6 access point for strong, room-specific coverage

Why this mattered: Guests, cameras and business systems have different trust levels, so they should not inherit unrestricted access to each other.

06 / The work delivered

Added ceiling-mounted access points in hallways, lobby, check-in, restaurant and outdoor pool and games areas

Why this mattered: This workstream addressed the hospitality & tourism operation's need for a maintainable service rather than leaving the original limitation in place.

07 / The work delivered

Set up separate guest and staff networks with bandwidth shaping and captive portal for a professional guest experience

Why this mattered: Guests, cameras and business systems have different trust levels, so they should not inherit unrestricted access to each other.

PROJECT 50 / BUSINESS RESULT

What changed for the business

100 rooms with dedicated in-wall Wi-Fi 6 access points	4 comms rooms fibre-linked to central admin
1 Gbps Swoop symmetrical fibre backhaul	100% guest area Wi-Fi coverage

What we used — and its role

Ubiquiti / UniFi

Centrally managed switching, routing or wireless can be maintained as one office-network platform rather than as disconnected devices.

Swoop

The recorded carrier service provides the WAN connection; routing, wireless and user support remain separate design decisions.

The sales conversation

If your organisation recognises these same issues, start with the constraint rather than a product list: which part of the environment interrupts staff, exposes data or makes growth harder? We can review the current setup, identify dependencies and scope the relevant services before recommending a change.



A word from the stable

The right connection makes the rest of the office happier.

1300 904 635 | hello@uitg.com.au

PROJECT 50 / QUESTIONS

A closer look at the solution

Why pre-wire every room during construction?

Pre-wiring during construction is far cheaper and cleaner than retrofitting later. Four ports per room gives flexibility for in-wall Wi-Fi, smart TVs, phones, future upgrades and any room layout changes without reopening walls.

How are the four comms rooms connected?

Each comms room has a UniFi switch and is connected back to the central admin comms room by fibre. This gives high-speed, low-latency links between every room block and the main internet gateway.

What access points were used?

We used in-wall Ubiquiti Wi-Fi 6 access points in every room for strong, localised coverage, plus ceiling-mounted access points in hallways, lobby, restaurant, check-in and outdoor areas like the pool and games area.

How is guest traffic managed?

Guest and staff networks are separated by VLANs. The UniFi gateway handles routing, firewalling and bandwidth shaping, with a captive portal for a branded guest sign-in experience.

Can this design scale if the motel adds more rooms or buildings?

Yes. The fibre-linked comms room architecture and 1 Gbps Swoop backhaul make it straightforward to add new room blocks, additional access points and higher internet speeds as needed.

PROJECT 51 / MANUFACTURING

Industrial Estate Connected with P2P Wireless and Bonded SHDSL Before NBN

P2P wireless & SHDSL

Before NBN and Starlink existed, a customer moving into a brand new industrial estate had no copper, no ADSL and no fibre. The incumbent telco quoted \$400,000 to install fibre. Instead, we built a point-to-point wireless link to a friendly neighbouring building and bonded two SHDSL connections to deliver 40 Mbps symmetrical for \$500 per month. The wireless link is still in place today, upgraded to air fibre, while the SHDSL lines have been replaced with a 1 Gbps FTTP NBN connection.



The issues we needed to solve

- New industrial estate had no NBN, no copper phone lines and no ADSL available
- The incumbent telco quoted \$400,000 to run fibre to the building
- The business needed reliable, symmetrical internet for cloud apps, email and file sharing from day one
- No viable fixed-line options existed beyond expensive legacy technology
- The solution had to be affordable and upgradeable as infrastructure improved

PROJECT 51 / DELIVERY

What we did — and why

01 / The work delivered

Surveyed neighbouring buildings and identified one with existing SHDSL and connectivity willing to share access and close to telephone exchange

Why this mattered: Starting with the actual site and workload reduces the risk of buying equipment that cannot solve the underlying problem.

02 / The work delivered

Designed and installed a point-to-point wireless link from the friendly building to the customer's roof

Why this mattered: Reliable connectivity is the foundation for the applications above it; changing software cannot repair an inadequate physical or network path.

03 / The work delivered

Provisioned two SHDSL services and bonded them into a single 40 Mbps symmetrical pipe

Why this mattered: This workstream addressed the manufacturing operation's need for a maintainable service rather than leaving the original limitation in place.

04 / The work delivered

Configured failover so traffic could use either SHDSL line or the wireless path if one failed

Why this mattered: The business needs a path through equipment or connection failures rather than making one component a single point of interruption.

05 / The work delivered

Monitored latency, packet loss and uptime remotely to keep the hybrid link stable

Why this mattered: Installing a system is not the end of the security job: visibility and control are needed while staff continue to use it.

06 / The work delivered

Upgraded the wireless link to air fibre as the technology matured, and later replaced the SHDSL pair with a 1 Gbps FTTP NBN service when it became available

Why this mattered: Reliable connectivity is the foundation for the applications above it; changing software cannot repair an inadequate physical or network path.

PROJECT 51 / BUSINESS RESULT

What changed for the business

\$400k avoided fibre install cost	40/40 Mbps symmetrical bonded SHDSL
\$500/mo monthly connectivity cost	1 Gbps current FTTP NBN upgrade
Still running P2P wireless link upgraded to air fibre	

The sales conversation

If your organisation recognises these same issues, start with the constraint rather than a product list: which part of the environment interrupts staff, exposes data or makes growth harder? We can review the current setup, identify dependencies and scope the relevant services before recommending a change.



A word from the stable

A stronger signal beats shouting at the router.

1300 904 635 | hello@uitg.com.au

PROJECT 51 / QUESTIONS

A closer look at the solution

What is SHDSL and why was it used?

SHDSL (Single-Pair High-Speed Digital Subscriber Line) is a symmetrical copper-line technology that delivers dedicated upload and download speeds over existing copper. With no NBN or fibre available, two SHDSL lines were bonded to create a 40 Mbps symmetrical connection at a fraction of the fibre build cost.

How did the point-to-point wireless link work?

We installed a point-to-point wireless bridge on the customer's roof and on a nearby building that already had fibre internet. The wireless link carried the customer's traffic to and from that building's connection, bypassing the need for a direct fibre run to the estate.

Was the connection reliable enough for business use?

Yes. The bonded SHDSL pair provided the primary path, while the wireless link acted as both a secondary path and a way to reach the upstream fibre. We monitored the link continuously and engineered failover so the business stayed online even if one path had issues.

What happened when NBN became available?

The office could only get FTTN at roughly 20 Mbps or lower, which was not good enough. We kept the upgraded air-fibre wireless link in service and added a 1 Gbps FTTP NBN connection through the same friendly-building arrangement, replacing the bonded SHDSL pair.

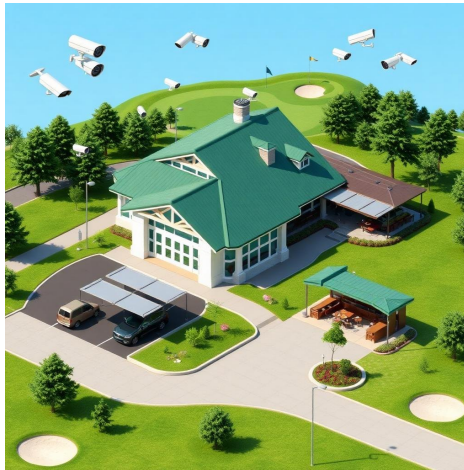
Could this approach work for other industrial estates today?

Absolutely. Where fibre builds are expensive or delayed, point-to-point wireless, air fibre, bonded copper or a mix of links can deliver reliable business-grade connectivity much faster and cheaper than waiting for trenching.

95 Meraki Cameras Secure an Exclusive Golf Course

CCTV & Security

An exclusive golf course wanted comprehensive video coverage across its buildings, clubhouse, parking area, gate, gardening sheds, driveway, driving range booths, bar, tills and restaurant. We installed 95 Cisco Meraki cloud-managed cameras, including longer-range models overlooking the course, giving management and security a single dashboard for live monitoring, playback and alerts.



The issues we needed to solve

- Large property with multiple buildings and outdoor areas needing consistent coverage
- Clubhouse, bar, restaurant and tills required discrete indoor cameras for staff and patron safety
- Parking lot, driveway and main gate needed clear vehicle and visitor visibility day and night
- Gardening sheds and maintenance areas had no security or monitoring
- Driving range booths and surrounding fairways needed longer-range coverage without installing a separate DVR system

PROJECT 52 / DELIVERY

What we did — and why

01 / The work delivered

Surveyed the entire course to identify blind spots, lighting conditions and cable routes

Why this mattered: Starting with the actual site and workload reduces the risk of buying equipment that cannot solve the underlying problem.

02 / The work delivered

Installed 95 Cisco Meraki MV cameras across the clubhouse, bar, restaurant, tills, parking, gate, sheds, driveway and driving range booths

Why this mattered: Coverage and controlled access make surveillance useful to the operation, rather than simply increasing the number of cameras.

03 / The work delivered

Deployed longer-range Meraki cameras on poles to cover fairways and the driving range

Why this mattered: Coverage and controlled access make surveillance useful to the operation, rather than simply increasing the number of cameras.

04 / The work delivered

Used Meraki PoE switches to power and connect every camera back to a central cloud dashboard

Why this mattered: Reliable connectivity is the foundation for the applications above it; changing software cannot repair an inadequate physical or network path.

05 / The work delivered

Configured motion alerts, onboard storage and retention policies tailored to each camera location

Why this mattered: Coverage and controlled access make surveillance useful to the operation, rather than simply increasing the number of cameras.

06 / The work delivered

Isolated camera traffic on a secure VLAN with firewall rules and bandwidth shaping

Why this mattered: Guests, cameras and business systems have different trust levels, so they should not inherit unrestricted access to each other.

PROJECT 52 / BUSINESS RESULT

What changed for the business

95 Meraki cameras covering the entire property	100% coverage of buildings, parking, gate and driving range
Cloud central dashboard for live and recorded footage	30 days onboard video retention

What we used — and its role

Cisco Meraki

Cloud management gives the support team a common view of the deployed network or camera estate without needing to visit each location.

The sales conversation

If your organisation recognises these same issues, start with the constraint rather than a product list: which part of the environment interrupts staff, exposes data or makes growth harder? We can review the current setup, identify dependencies and scope the relevant services before recommending a change.



A word from the stable

The horn is optional. Layered protection isn't.

1300 904 635 | hello@uitg.com.au

PROJECT 52 / QUESTIONS

A closer look at the solution

Why Cisco Meraki cameras for a golf course?

Meraki MV cameras are cloud-managed, so there is no need for on-premise NVRs or DVRs. Each camera stores footage onboard and streams to a central dashboard, making it easy to monitor the clubhouse, bar, parking, gate, sheds, driving range and fairways from one screen.

How are indoor areas like the bar and restaurant handled?

We installed discreet indoor Meraki cameras above tills, the bar and dining areas. These help protect staff, deter theft, resolve disputes and give managers visibility during busy periods without being intrusive.

Can the cameras cover large outdoor areas like the driving range?

Yes. We used longer-range Meraki cameras mounted on poles to cover the driving range booths and surrounding fairways. The lenses and positioning were chosen to give clear visibility at distance while minimising the number of cameras needed.

How is the camera network kept secure?

Camera traffic runs on a dedicated VLAN with strict firewall rules and bandwidth shaping. Access to the Meraki dashboard is protected by multi-factor authentication and role-based permissions, so only authorised managers and security staff can view footage.

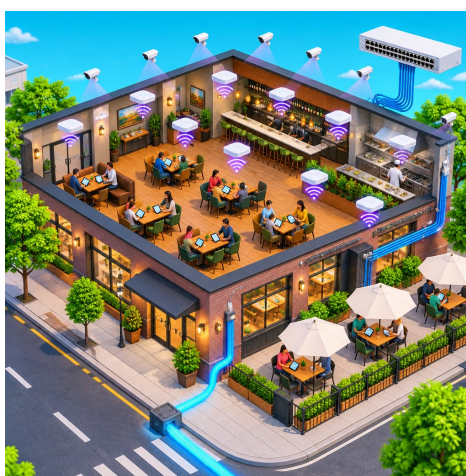
What happens if the internet goes down?

Each Meraki camera stores video onboard, so recording continues even if internet connectivity is interrupted. Once connectivity returns, the cameras sync back to the dashboard and alerts resume.

Restaurant Fixed Poor Wi-Fi Coverage for Guest Wireless and Tablet Ordering

Guest Wi-Fi & POS

A restaurant wanted to offer guest wireless to diners and switch to wireless tablets for table ordering, but poor Wi-Fi coverage made both unreliable. We installed eight Cisco Meraki wireless access points, a Cisco Meraki 48-port switch and 18 Meraki cameras, connected the POS terminals, and upgraded the venue to a Vocus 1000/400 Mbps FTTP NBN service.



The issues we needed to solve

- Guest wireless coverage was poor, with dropouts in the dining room, bar and outdoor patio
- Wait staff could not rely on wireless tablets for table ordering because connections kept dropping
- The existing network had no wired capacity to support access points, POS terminals and cameras together
- The venue had almost no camera coverage across the dining room, bar, entrances and kitchen
- The old internet connection was too slow to handle guest Wi-Fi, tablet ordering, POS transactions and cloud backups at once

PROJECT 53 / DELIVERY

What we did — and why

01 / The work delivered

Performed a wireless site survey of the dining room, bar, kitchen and outdoor patio to map dead zones and place access points

Why this mattered: Starting with the actual site and workload reduces the risk of buying equipment that cannot solve the underlying problem.

02 / The work delivered

Installed eight Cisco Meraki cloud-managed wireless access points for seamless whole-of-venue coverage

Why this mattered: Reliable connectivity is the foundation for the applications above it; changing software cannot repair an inadequate physical or network path.

03 / The work delivered

Deployed a Cisco Meraki 48-port PoE switch to power and connect the access points, cameras and POS terminals

Why this mattered: Reliable connectivity is the foundation for the applications above it; changing software cannot repair an inadequate physical or network path.

04 / The work delivered

Installed 18 Meraki cloud-managed cameras covering the dining room, bar, entrances, kitchen and back-of-house

Why this mattered: Moving the workload or retiring obsolete dependencies reduces the amount of legacy infrastructure the business still has to operate.

05 / The work delivered

Connected the POS terminals to the new switched network for reliable, fast transactions

Why this mattered: Reliable connectivity is the foundation for the applications above it; changing software cannot repair an inadequate physical or network path.

06 / The work delivered

Provisioned a Vocus 1000/400 Mbps FTTP NBN service with separate VLANs for guest wireless, POS, cameras and staff systems

Why this mattered: Guests, cameras and business systems have different trust levels, so they should not inherit unrestricted access to each other.

07 / The work delivered

Configured a capped, isolated guest Wi-Fi network so diners get fast internet without touching business systems

Why this mattered: Guests, cameras and business systems have different trust levels, so they should not inherit unrestricted access to each other.

PROJECT 53 / BUSINESS RESULT

What changed for the business

8 Meraki access points covering the whole venue	18 Meraki cameras protecting the venue
1000/400 Mbps Vocus FTTP NBN connection	100% tablet ordering coverage across dining, bar and patio
1 cloud dashboard for Wi-Fi, switching and cameras	

What we used — and its role

Cisco Meraki

Cloud management gives the support team a common view of the deployed network or camera estate without needing to visit each location.

Vocus

The recorded carrier service provides internet or private inter-site capacity; the speed and connection type are specific to this project.

The sales conversation

If your organisation recognises these same issues, start with the constraint rather than a product list: which part of the environment interrupts staff, exposes data or makes growth harder? We can review the current setup, identify dependencies and scope the relevant services before recommending a change.



A word from the stable

A stronger signal beats shouting at the router.

1300 904 635 | hello@uitg.com.au

PROJECT 53 / QUESTIONS

A closer look at the solution

Why Cisco Meraki access points for a restaurant?

Meraki access points are cloud-managed, so coverage, guest networks and interference are tuned from one dashboard instead of by climbing a ladder. With eight points placed from a proper site survey, diners and wait staff get a strong signal everywhere from the dining room to the outdoor patio.

How does guest Wi-Fi stay separate from the POS and business systems?

Guest wireless runs on its own isolated VLAN with bandwidth caps, so diners can stream and browse freely without ever touching the POS terminals, tablets, cameras or back-office systems. The Meraki dashboard keeps every network visible in one place.

Why did the restaurant need a 48-port switch?

Eight access points, 18 cameras and multiple POS terminals all need reliable wired connections. A Meraki 48-port PoE switch powers them all over a single cable each and gives us remote visibility of every port, so a fault can be diagnosed without a site visit.

What did the Vocus 1000/400 FTTP NBN connection change?

The venue now has 1000 Mbps down and 400 Mbps up on a full fibre connection. Guest Wi-Fi, tablet ordering, cloud POS transactions, camera streaming and off-site backups all run at once without anyone noticing, and the extra upload speed keeps cloud backups and camera sync quick.

Do the cameras keep recording if the internet drops?

Yes. Meraki cameras store footage onboard, so recording continues during any outage. Once the connection returns, they sync back to the cloud dashboard automatically.

PROJECT 54 / SPORTS & RECREATION

Local Cricket Club Recovered from a Business Email Compromise and Modernised Its IT

Security & Microsoft 365

A local cricket club was running the office on old POP3 email that kept losing messages, had invoices redirected by a compromised account, malware on the office PC, and no multi-factor authentication. Unicorn IT Group replaced the legacy setup with Microsoft 365, Teams-based file storage, four Intune-managed machines, endpoint protection, secure Xero access, email filtering with business email compromise protection, phishing training, Office 365 backup, MFA, and a complete Meraki network with guest Wi-Fi and CCTV across the clubhouse, bar, oval gate and oval.



The issues we needed to solve

- POP3 email constantly losing messages and failing to sync across the committee's phones and laptops
- A hacked email account was used to redirect supplier invoices, putting club funds at risk
- Malware was found on the ageing office machine, with no central endpoint protection or patching
- No multi-factor authentication on any cloud accounts, including the bookkeeper's Xero login
- Sensitive club documents stored on personal USB drives and scattered inboxes instead of one secure place
- No guest Wi-Fi, forcing visitors and game-day streamers onto the same network as club systems
- No CCTV covering the bar, clubhouse, oval gate or oval areas

PROJECT 54 / DELIVERY

What we did — and why

01 / The work delivered

Migrated the club from legacy POP3 email to Microsoft 365 Exchange Online, Teams and SharePoint/OneDrive

Why this mattered: Moving the workload or retiring obsolete dependencies reduces the amount of legacy infrastructure the business still has to operate.

02 / The work delivered

Procured four new Windows laptops, joined them to Microsoft Entra ID and Intune for policies, patching and remote management

Why this mattered: Installing a system is not the end of the security job: visibility and control are needed while staff continue to use it.

03 / The work delivered

Deployed SentinelOne and Guardz for endpoint detection, response and 24/7 threat monitoring

Why this mattered: Installing a system is not the end of the security job: visibility and control are needed while staff continue to use it.

04 / The work delivered

Configured Xero with multi-factor authentication and secured the associated email account

Why this mattered: Passwords alone leave accounts exposed; additional access checks make stolen credentials less useful to an attacker.

05 / The work delivered

Implemented business email compromise protection, anti-phishing and malware filtering for all club mail

Why this mattered: This workstream addressed the sports & recreation operation's need for a maintainable service rather than leaving the original limitation in place.

06 / The work delivered

Ran phishing awareness training for committee members, staff and volunteers

Why this mattered: The improvement must remain usable and supportable after handover, not depend on knowledge held only by the installer.

07 / The work delivered

Enabled Microsoft 365 backup with point-in-time recovery for mail, Teams and OneDrive data

Why this mattered: A recoverable copy must exist independently of the production service; synchronising files alone is not a recovery strategy.

08 / The work delivered

Rolled out MFA across Office 365, Xero and any other cloud services used by the club

Why this mattered: Passwords alone leave accounts exposed; additional access checks make stolen credentials less useful to an attacker.

09 / The work delivered

Installed Cisco Meraki Wi-Fi, switching and a firewall, with a separate guest network for members and game-day streaming

Why this mattered: Guests, cameras and business systems have different trust levels, so they should not inherit unrestricted access to each other.

10 / The work delivered

Deployed Meraki cloud-managed cameras covering the bar, clubhouse, oval gate and oval areas with remote access for keyholders

Why this mattered: Moving the workload or retiring obsolete dependencies reduces the amount of legacy infrastructure the business still has to operate.

11 / The work delivered

Provisioned a Swoop 200/100 Mbps NBN service to support guest streaming and third-party game-day camera setups

Why this mattered: Guests, cameras and business systems have different trust levels, so they should not inherit unrestricted access to each other.

PROJECT 54 / BUSINESS RESULT

What changed for the business

0 invoice redirect or email compromise incidents since cutover	4 new Intune-managed, protected endpoints
100% MFA coverage on Office 365 and Xero	24/7 endpoint monitoring via Guardz and SentinelOne
Covered bar, clubhouse, oval gate and oval with Meraki cameras	200/100 Mbps Swoop NBN for game-day streaming and guests

What we used — and its role

SentinelOne

Endpoint detection and response helps identify suspicious activity on computers and supports investigation and containment.

Guardz

Managed detection and response adds ongoing threat review and response beyond a one-off security installation.

Cisco Meraki

Cloud management gives the support team a common view of the deployed network or camera estate without needing to visit each location.

Microsoft 365

Cloud email and collaboration reduce dependence on local mail servers and make access and administration consistent across devices.

Intune / Autopilot

Policy-driven deployment helps standardise devices and reduces manual setup when a user receives a replacement computer.

SharePoint / Teams / OneDrive

Shared cloud workspaces separate business files and collaboration from a single office server or an individual computer.

Swoop

The recorded carrier service provides the WAN connection; routing, wireless and user support remain separate design decisions.

The sales conversation

If your organisation recognises these same issues, start with the constraint rather than a product list: which part of the environment interrupts staff, exposes data or makes growth harder? We can review the current setup, identify dependencies and scope the relevant services before recommending a change.



A word from the stable

Old dependencies don't retire themselves.

1300 904 635 | hello@uitg.com.au

PROJECT 54 / QUESTIONS

A closer look at the solution

Why was POP3 causing emails to go missing?

POP3 typically downloads email to a single device and removes it from the server. If a phone, laptop or old Outlook profile downloaded messages and the device failed, those emails were gone. Moving to Microsoft 365 keeps every message in the cloud and synced across all devices.

How did the club stop invoice redirection?

We reset all credentials, enabled MFA, added business email compromise protection that flags suspicious payment changes, and trained staff to verify bank details by phone. The old POP3 account was disabled and replaced with monitored Microsoft 365 mailboxes.

What is Intune and why join the new machines to it?

Microsoft Intune is cloud-based device management. It enforces security policies, keeps Windows and apps patched, encrypts disks, and lets us remotely support or wipe a machine if it is lost or compromised. This replaces the old habit of unmanaged personal computers.

Why does Office 365 need separate backup?

Microsoft protects its infrastructure, but it does not keep unlimited backups of your data. Accidental deletes, ransomware, or a malicious insider can still wipe club files and emails. Our Cove/Syncro backup captures mail, Teams and OneDrive data with point-in-time recovery.

How is the guest Wi-Fi kept separate from club systems?

The Meraki firewall and wireless controller create isolated VLANs. The guest network can reach the internet and game-day streaming services but cannot see club printers, files, Xero, or the camera network.

Can committee members view the cameras from home?

Yes. Authorised committee members and keyholders can open the Meraki dashboard or app to view live and recorded footage from the bar, clubhouse, oval gate and oval cameras, using MFA-protected accounts.

PROJECT 55 / VETERINARY & ANIMAL CARE

Local Vet Clinic Moved Into a Brand-New Building with a Complete IT Fit-out

New clinic fit-out

A local veterinary clinic relocated to a brand-new purpose-built building and needed everything installed from scratch — data cabling, Wi-Fi, cameras, network, internet, phones, and all new computers. Unicorn IT Group delivered the cabling, Ubiquiti switching, a UniFi Cloud Gateway, guest wireless, Swoop 1 Gbps/1 Gbps NBN Enterprise Ethernet, 14 new Windows machines, a 3CX cloud phone system with 14 extensions, and Microsoft Endpoint Manager zero-touch deployment so staff could sign in and work immediately. We layered on Guardz threat monitoring, MFA across every app, and a serverless Microsoft Teams setup for files and collaboration.



The issues we needed to solve

- New building had no data cabling, network equipment, or internet connection
- Old clinic relied on a mix of personal and ageing computers with no standard configuration
- No centralised device management, patching, or security visibility
- Staff needed to be productive from day one without lengthy manual setup
- Client and staff Wi-Fi had to be kept separate from clinic systems and cameras
- No on-premise servers were wanted; files and records needed to live in the cloud
- MFA and endpoint protection had to cover every user and app from the start
- The old on-premise phone system could not move to the new building and lacked modern features such as call queues and mobile answering

PROJECT 55 / DELIVERY

What we did — and why

01 / The work delivered

Installed certified data cabling throughout reception, consult rooms, treatment areas, staff spaces and kennels

Why this mattered: Reliable connectivity is the foundation for the applications above it; changing software cannot repair an inadequate physical or network path.

02 / The work delivered

Deployed Ubiquiti switching and a UniFi Cloud Gateway for routing, VLANs and centralised network management

Why this mattered: Guests, cameras and business systems have different trust levels, so they should not inherit unrestricted access to each other.

03 / The work delivered

Configured a separate guest wireless network isolated from clinic systems and cameras

Why this mattered: Guests, cameras and business systems have different trust levels, so they should not inherit unrestricted access to each other.

04 / The work delivered

Provisioned Swoop 1 Gbps symmetrical NBN Enterprise Ethernet for reliable cloud and telehealth connectivity

Why this mattered: Reliable connectivity is the foundation for the applications above it; changing software cannot repair an inadequate physical or network path.

05 / The work delivered

Installed Meraki cloud-managed cameras covering reception, treatment areas, kennels and external entries

Why this mattered: Moving the workload or retiring obsolete dependencies reduces the amount of legacy infrastructure the business still has to operate.

06 / The work delivered

Procured 14 new Windows laptops and desktops matched to reception, vet, nurse and admin roles

Why this mattered: A consistent device baseline makes deployment and ongoing support more predictable for staff and the service team.

07 / The work delivered

Enrolled every machine into Microsoft Endpoint Manager with Autopilot deployment profiles and security baselines

Why this mattered: A consistent device baseline makes deployment and ongoing support more predictable for staff and the service team.

08 / The work delivered

Shipped devices so staff could unbox, connect to Wi-Fi, sign in once, and have apps, printers and policies ready automatically

Why this mattered: Communications need to follow how people work, with maintainable routing and extensions instead of the limitations of the old phone arrangement.

09 / The work delivered

Deployed Guardz for 24/7 endpoint threat monitoring and response

Why this mattered: Installing a system is not the end of the security job: visibility and control are needed while staff continue to use it.

10 / The work delivered

Enabled multi-factor authentication on Microsoft 365, Xero, practice management software and any other cloud apps

Why this mattered: Passwords alone leave accounts exposed; additional access checks make stolen credentials less useful to an attacker.

11 / The work delivered

Moved all files, records and collaboration into Microsoft Teams and SharePoint with no on-premise servers

Why this mattered: Moving the workload or retiring obsolete dependencies reduces the amount of legacy infrastructure the business still has to operate.

12 / The work delivered

Configured point-in-time Microsoft 365 backup to protect mail, Teams and OneDrive data

Why this mattered: A recoverable copy must exist independently of the production service; synchronising files alone is not a recovery strategy.

13 / The work delivered

Deployed a 3CX cloud PBX with 14 extensions, desk phones, call queues, voicemail-to-email, and 3CX mobile/softphone apps for vets on call

Why this mattered: Communications need to follow how people work, with maintainable routing and extensions instead of the limitations of the old phone arrangement.

PROJECT 55 / BUSINESS RESULT

What changed for the business

14 new machines deployed with zero-touch setup	14 3CX cloud phone extensions deployed
1 Gbps symmetrical Swoop Enterprise Ethernet	0 on-premise servers needed
100% MFA coverage across clinic apps	24/7 endpoint monitoring via Guardz
Day 1 staff productive after unboxing and signing in	

What we used — and its role

Guardz

Managed detection and response adds ongoing threat review and response beyond a one-off security installation.

Cisco Meraki

Cloud management gives the support team a common view of the deployed network or camera estate without needing to visit each location.

Ubiquiti / UniFi

Centrally managed switching, routing or wireless can be maintained as one office-network platform rather than as disconnected devices.

Microsoft 365

Cloud email and collaboration reduce dependence on local mail servers and make access and administration consistent across devices.

Intune / Autopilot

Policy-driven deployment helps standardise devices and reduces manual setup when a user receives a replacement computer.

SharePoint / Teams / OneDrive

Shared cloud workspaces separate business files and collaboration from a single office server or an individual computer.

3CX

A software-based phone system supports central call routing and flexible extensions without preserving the old PBX operating model.

Swoop

The recorded carrier service provides the WAN connection; routing, wireless and user support remain separate design decisions.

The sales conversation

If your organisation recognises these same issues, start with the constraint rather than a product list: which part of the environment interrupts staff, exposes data or makes growth harder? We can review the current setup, identify dependencies and scope the relevant services before recommending a change.



A word from the stable

Old dependencies don't retire themselves.

1300 904 635 | hello@uitg.com.au

PROJECT 55 / QUESTIONS

A closer look at the solution

What does zero-touch deployment mean for the vet clinic?

Each new computer was enrolled in Microsoft Endpoint Manager before delivery. Staff opened the box, connected to Wi-Fi, signed in with their Microsoft 365 account, and the device automatically installed the practice management app, printer drivers, security policies and Guardz. No manual imaging or IT visit was needed.

Why was a separate guest wireless network important?

Clients and visitors use guest Wi-Fi, while clinic computers, phones, cameras and payment terminals stay on a secure internal network. VLANs and firewall rules prevent guests from reaching clinical systems, protecting patient data and payment information.

How are the Meraki cameras used?

Cloud-managed cameras cover reception, treatment areas, kennels and external entrances. Authorised managers can view live and recorded footage from a phone or browser, with footage stored onboard and access protected by MFA.

Why did the clinic move to Teams instead of keeping a server?

With no on-premise server to maintain, patch or replace, the clinic reduces cost and risk. Files, schedules and collaboration live in Microsoft Teams and SharePoint, accessible securely from any clinic computer or approved device.

How is patient and practice data backed up?

Microsoft 365 data is protected with point-in-time backup covering Exchange Online, Teams and OneDrive. Even though Microsoft hosts the service, this gives the clinic the ability to recover from accidental deletion, ransomware or malicious changes.

What happens if a device is lost or stolen?

Because every machine is managed by Endpoint Manager, we can remotely lock or wipe it, reset the user's passwords, and revoke sessions. Encryption and conditional access policies also prevent unauthorised access to clinic data.

How does the 3CX phone system help the clinic?

The 3CX cloud PBX gives the clinic 14 extensions, call queues for reception and triage, voicemail-to-email, and mobile/softphone apps so vets can answer calls from anywhere. Because it runs in the cloud, there is no on-premise phone server to maintain or replace.

PROJECT 56 / HEALTHCARE

New Doctor Surgery Opens with Full Cloud-First IT Setup

Medical practice fit-out

A brand-new GP clinic with three doctors and one receptionist needed a complete, secure, cloud-first office before opening day. We delivered new computers, Microsoft 365 with MFA and backup, SharePoint for files and policies, cloud-managed applications, a 3CX phone system, 500/200 Mbps FTTP NBN, Meraki cameras, switches, wireless and gateway, plus Guardz endpoint monitoring — all with no on-premise server.



The issues we needed to solve

- Brand-new surgery with no data cabling, network equipment, internet connection or computers
- Three GPs and one receptionist needed to see patients from day one with zero IT delays
- Medical records and practice data had to stay secure and accessible only to authorised staff
- No internal IT person; the solution had to be fully managed and supportable remotely
- Phones, appointment reminders and after-hours call handling needed to work immediately
- Patient Wi-Fi had to be isolated from practice computers, printers and cameras
- Essential cybersecurity — MFA, backups and endpoint protection — had to be built in from day one

PROJECT 56 / DELIVERY

What we did — and why

01 / The work delivered

Installed certified structured data cabling to reception, three consult rooms, the admin area and waiting room

Why this mattered: Reliable connectivity is the foundation for the applications above it; changing software cannot repair an inadequate physical or network path.

02 / The work delivered

Deployed Meraki cloud-managed switches, wireless access points and a security gateway with centralised dashboard

Why this mattered: Reliable connectivity is the foundation for the applications above it; changing software cannot repair an inadequate physical or network path.

03 / The work delivered

Created isolated VLANs for practice systems, patient Wi-Fi, printers and cameras

Why this mattered: Guests, cameras and business systems have different trust levels, so they should not inherit unrestricted access to each other.

04 / The work delivered

Provisioned 500/200 Mbps FTTP NBN with static IP and automatic 4G failover for always-on connectivity

Why this mattered: The business needs a path through equipment or connection failures rather than making one component a single point of interruption.

05 / The work delivered

Supplied and configured five new Windows desktops and laptops matched to doctor, nurse and reception roles

Why this mattered: A consistent device baseline makes deployment and ongoing support more predictable for staff and the service team.

06 / The work delivered

Enrolled every device into Microsoft Endpoint Manager with Autopilot deployment profiles, disk encryption and security baselines

Why this mattered: A consistent device baseline makes deployment and ongoing support more predictable for staff and the service team.

07 / The work delivered

Deployed Microsoft 365 Business Premium with Exchange Online, SharePoint and Teams for email, files and collaboration

Why this mattered: Moving the workload or retiring obsolete dependencies reduces the amount of legacy infrastructure the business still has to operate.

08 / The work delivered

Built a SharePoint document library for policies, templates, compliance records and staff onboarding materials

Why this mattered: The improvement must remain usable and supportable after handover, not depend on knowledge held only by the installer.

09 / The work delivered

Configured Guardz 24/7 endpoint threat monitoring and response across every computer

Why this mattered: Installing a system is not the end of the security job: visibility and control are needed while staff continue to use it.

10 / The work delivered

Enforced multi-factor authentication across Microsoft 365, practice management software and all other cloud apps

Why this mattered: Passwords alone leave accounts exposed; additional access checks make stolen credentials less useful to an attacker.

11 / The work delivered

Deployed immutable Office 365 backup covering mail, Teams, OneDrive and SharePoint data

Why this mattered: A recoverable copy must exist independently of the production service; synchronising files alone is not a recovery strategy.

12 / The work delivered

Installed Meraki cloud cameras covering reception, waiting room and entry points with role-restricted access

Why this mattered: Moving the workload or retiring obsolete dependencies reduces the amount of legacy infrastructure the business still has to operate.

13 / The work delivered

Deployed a hosted 3CX phone system with five extensions, IVR, call queues, voicemail-to-email and mobile softphones for after-hours doctors

Why this mattered: Communications need to follow how people work, with maintainable routing and extensions instead of the limitations of the old phone arrangement.

14 / The work delivered

Delivered user training and a simple runbook for reception and clinical staff

Why this mattered: The improvement must remain usable and supportable after handover, not depend on knowledge held only by the installer.

PROJECT 56 / BUSINESS RESULT

What changed for the business

5 new computers ready before opening day	500/200 Mbps FTTP NBN with 4G failover
5 3CX phone extensions with mobile apps	0 on-premise servers to maintain
100% MFA coverage across practice apps	24/7 endpoint monitoring via Guardz
Day 1 patient bookings and calls flowing	

What we used — and its role

Guardz

Managed detection and response adds ongoing threat review and response beyond a one-off security installation.

Cisco Meraki

Cloud management gives the support team a common view of the deployed network or camera estate without needing to visit each location.

Microsoft 365

Cloud email and collaboration reduce dependence on local mail servers and make access and administration consistent across devices.

Intune / Autopilot

Policy-driven deployment helps standardise devices and reduces manual setup when a user receives a replacement computer.

SharePoint / Teams / OneDrive

Shared cloud workspaces separate business files and collaboration from a single office server or an individual computer.

3CX

A software-based phone system supports central call routing and flexible extensions without preserving the old PBX operating model.

The sales conversation

If your organisation recognises these same issues, start with the constraint rather than a product list: which part of the environment interrupts staff, exposes data or makes growth harder? We can review the current setup, identify dependencies and scope the relevant services before recommending a change.



A word from the stable

Old dependencies don't retire themselves.

1300 904 635 | hello@uitg.com.au

PROJECT 56 / QUESTIONS

A closer look at the solution

What does cloud-first mean for a small doctor surgery?

It means email, files, collaboration and phone calls run from secure cloud services instead of an on-premise server. The surgery gets lower upfront cost, automatic updates, remote access for authorised staff, and no server to maintain, patch or replace.

Why is patient Wi-Fi kept separate from practice systems?

Meraki VLANs and firewall rules isolate the guest network. Patients can browse the internet, but their devices cannot reach practice computers, printers, cameras or the practice management system. This protects patient data and payment information.

How does the 3CX phone system help the surgery?

The hosted 3CX PBX gives the surgery five extensions, a professional greeting, call queues for reception, voicemail-to-email, and mobile softphones so doctors can answer after-hours calls from their own phones. Because it runs in the cloud, there is no phone server in the comms room.

Why does Microsoft 365 need separate backup?

Microsoft keeps the service running, but it does not provide unlimited protection against accidental deletion, ransomware or malicious changes. Our Office 365 backup captures Exchange, Teams, OneDrive and SharePoint data with point-in-time recovery.

What happens if a doctor's laptop is lost or stolen?

Because every device is managed by Endpoint Manager, we can remotely lock or wipe it, reset the user's passwords and revoke active sessions. Disk encryption and conditional access policies also prevent unauthorised access to practice data.

PROJECT 57 / MINING & RESOURCES

30 km Haul Road CCTV and Fibre Network for a Mine Site

Haul-road CCTV & fibre

A mining company had no visibility along its 30 km haul road, so operations could not confirm road conditions, traffic or safety incidents in real time. As part of a broader communications upgrade running fibre from the wharf to the mine and camp, we partnered with a fibre installer to extend fibre the full length of the haul road and build 35 solar-powered CCTV towers. Every tower switch was connected directly back to the fibre backbone — no wireless backhaul was used because the terrain was too hilly, and the fibre was being installed anyway.



The issues we needed to solve

- No CCTV coverage along a 30 km haul road, making real-time safety and traffic monitoring impossible
- Haul road conditions, dust, vehicle movements and wildlife could not be checked before dispatching heavy equipment
- No reliable power or communications infrastructure along the remote road corridor
- Wireless backhaul was not viable due to hilly terrain and line-of-sight issues between towers
- Existing fibre project only covered the wharf-to-camp and wharf-to-mine links, not the haul road itself
- The solution had to survive extreme temperatures, dust storms and limited maintenance access

PROJECT 57 / DELIVERY

What we did — and why

01 / The work delivered

Worked with a certified fibre installer to extend the comms fibre run the full 30 km alongside the haul road

Why this mattered: Reliable connectivity is the foundation for the applications above it; changing software cannot repair an inadequate physical or network path.

02 / The work delivered

Built 35 small towers and huts at regular intervals, each with solar panels, battery backup and a weatherproof cabinet

Why this mattered: A recoverable copy must exist independently of the production service; synchronising files alone is not a recovery strategy.

03 / The work delivered

Installed ruggedised network switches and 90+ fibre terminations inside the huts, with every switch connected directly back to the fibre backbone

Why this mattered: Reliable connectivity is the foundation for the applications above it; changing software cannot repair an inadequate physical or network path.

04 / The work delivered

Mounted pan-tilt-zoom CCTV cameras on every tower and patched each camera through the local switch to the fibre network

Why this mattered: Installing a system is not the end of the security job: visibility and control are needed while staff continue to use it.

05 / The work delivered

Connected the haul-road network back to the mine's control room and camp operations centre

Why this mattered: This workstream addressed the mining & resources operation's need for a maintainable service rather than leaving the original limitation in place.

06 / The work delivered

Configured remote monitoring so operators can view any camera, check switch and fibre health and receive fault alerts from one dashboard

Why this mattered: Installing a system is not the end of the security job: visibility and control are needed while staff continue to use it.

PROJECT 57 / BUSINESS RESULT

What changed for the business

30km fibre-backed haul road covered	35 solar-powered CCTV towers and huts
90+ fibre terminations across the towers	24/7 visibility of road conditions and traffic
0 wireless links used — all fibre-connected	

The sales conversation

If your organisation recognises these same issues, start with the constraint rather than a product list: which part of the environment interrupts staff, exposes data or makes growth harder? We can review the current setup, identify dependencies and scope the relevant services before recommending a change.



A word from the stable

The right connection makes the rest of the office happier.

1300 904 635 | hello@uitg.com.au

PROJECT 57 / QUESTIONS

A closer look at the solution

Why run fibre along the haul road instead of using wireless or 4G?

A fibre run was already being installed from the wharf to the mine and camp as part of a communications upgrade, so extending it along the haul road gave us high-bandwidth, low-latency, reliable backhaul without relying on patchy cellular coverage or fighting the hilly terrain for wireless line-of-sight. It also keeps camera feeds off the public internet.

Were the CCTV towers connected wirelessly back to the operations centre?

No. Every tower has a ruggedised network switch that is connected directly back to the fibre backbone running the length of the haul road. Wireless backhaul was not used because the hills along the road blocked line-of-sight and the fibre was being installed anyway.

How many fibre terminations were installed across the project?

We installed at least 90 fibre terminations across the 35 towers and huts, providing enough capacity for cameras, switches and future expansion without adding new field splice points.

How are the CCTV towers powered in such a remote location?

Each of the 35 towers has its own solar panel array and battery backup housed in a weatherproof hut. The cameras, switches and fibre termination equipment run entirely off-grid, with batteries sized to keep everything operating through dust storms and short periods of low sunlight.

What can mine operators see and control from the operations centre?

Operators can view live and recorded footage from every camera, remotely pan, tilt and zoom, check switch and fibre health, and receive automatic alerts if a camera, hut or link goes offline. This gives the control room full situational awareness of the 30 km road from one screen.

Can this design be reused for other remote haul roads or pipelines?

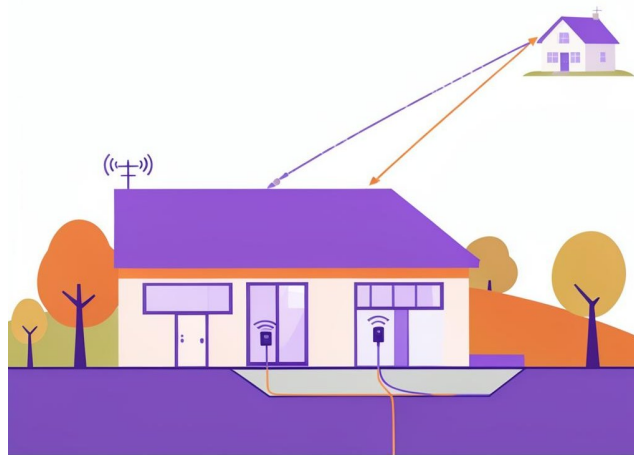
Yes. The solar-powered tower and fibre-hut design is ideal for any long linear corridor where trenching power and communications is impractical, including haul roads, pipelines, conveyor belts and remote airstrips. We design each deployment around local sunlight, dust conditions and distance to the nearest fibre backbone.

PROJECT 58 / VETERINARY

Regional Vet Clinic Upgraded to Swoop Enterprise Ethernet and Ubiquiti

Regional connectivity

A regional veterinary practice was running cloud practice management software, diagnostic imaging and VoIP phones over a slow, unreliable connection. Staff were dropping calls and waiting minutes for X-rays to upload. We installed Swoop Enterprise Ethernet 250/250 at the clinic, a Ubiquiti Cloud Gateway and wireless access points, and a point-to-point wireless link to the vet's home office.



The issues we needed to solve

- Cloud practice-management software timing out on a slow regional broadband connection
- X-ray and diagnostic image uploads taking several minutes and often failing
- VoIP calls dropping during consultations and after-hours emergency calls
- Unreliable Wi-Fi coverage in treatment rooms, consult rooms and reception
- The principal vet needed to work from a home office but the house had its own poor connection
- No failover, so any internet outage stopped appointments, billing and telemedicine

PROJECT 58 / DELIVERY

What we did — and why

01 / The work delivered

Installed Swoop Enterprise Ethernet 250 Mbps symmetrical fibre at the clinic with a business SLA

Why this mattered: Reliable connectivity is the foundation for the applications above it; changing software cannot repair an inadequate physical or network path.

02 / The work delivered

Deployed a Ubiquiti Cloud Gateway with traffic shaping to prioritise practice software, VoIP and imaging traffic

Why this mattered: Moving the workload or retiring obsolete dependencies reduces the amount of legacy infrastructure the business still has to operate.

03 / The work delivered

Installed Ubiquiti wireless access points to give full coverage across consult rooms, treatment areas and reception

Why this mattered: Reliable connectivity is the foundation for the applications above it; changing software cannot repair an inadequate physical or network path.

04 / The work delivered

Built a dedicated point-to-point wireless link from the clinic roof to the vet's home office using Ubiquiti airMAX

Why this mattered: Reliable connectivity is the foundation for the applications above it; changing software cannot repair an inadequate physical or network path.

05 / The work delivered

Configured separate staff, guest and device networks to keep clinical systems isolated

Why this mattered: Guests, cameras and business systems have different trust levels, so they should not inherit unrestricted access to each other.

06 / The work delivered

Added automatic 4G failover so the clinic stays online during fibre faults

Why this mattered: The business needs a path through equipment or connection failures rather than making one component a single point of interruption.

07 / The work delivered

Documented the network and handed over simple guest and staff Wi-Fi access

Why this mattered: Guests, cameras and business systems have different trust levels, so they should not inherit unrestricted access to each other.

PROJECT 58 / BUSINESS RESULT

What changed for the business

250/250 Mbps symmetrical Swoop Enterprise Ethernet	Seconds for X-ray and image uploads instead of minutes
100% clinic and home office coverage	24/7 practice phone system stays online

What we used — and its role

Ubiquiti / UniFi

Centrally managed switching, routing or wireless can be maintained as one office-network platform rather than as disconnected devices.

Swoop

The recorded carrier service provides the WAN connection; routing, wireless and user support remain separate design decisions.

The sales conversation

If your organisation recognises these same issues, start with the constraint rather than a product list: which part of the environment interrupts staff, exposes data or makes growth harder? We can review the current setup, identify dependencies and scope the relevant services before recommending a change.



A word from the stable

The right connection makes the rest of the office happier.

1300 904 635 | hello@uitg.com.au

PROJECT 58 / QUESTIONS

A closer look at the solution

Why Swoop Enterprise Ethernet instead of standard NBN?

Standard NBN in the region was contended and asymmetric, which meant uploads were too slow for diagnostic images and video calls. Swoop Enterprise Ethernet gave the clinic a dedicated, symmetrical 250/250 Mbps business fibre link with an SLA and local support.

How is the vet's home office connected to the clinic?

We installed a Ubiquiti point-to-point wireless bridge from the clinic roof to the home office. It uses the clinic's fast fibre connection, so the home office gets reliable internet for after-hours consults and admin work without paying for a second business line.

Is the Wi-Fi secure for staff and clients?

Yes. We set up separate networks for staff, guest devices and clinic equipment. Clinical systems are isolated from guest Wi-Fi, and the Ubiquiti gateway applies firewall rules and traffic shaping to keep priority traffic smooth.

What happens if the fibre goes down?

The Ubiquiti gateway is configured with automatic 4G failover. If the primary Swoop fibre link fails, the clinic switches to 4G within seconds, keeping phones, payments and cloud software online.

Did you replace the existing practice phones?

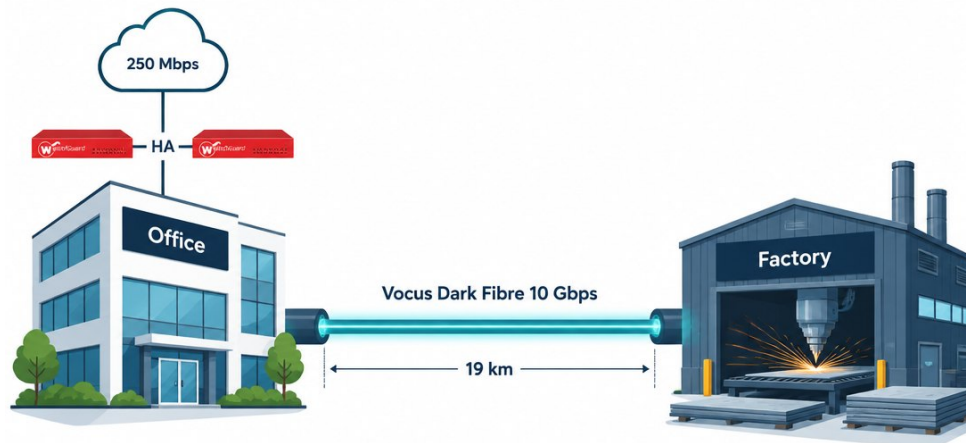
The clinic kept its existing handsets and phone system, but they now run over the stable fibre connection instead of the old flaky broadband. Calls are prioritised on the network so they no longer drop mid-consultation.

PROJECT 59 / MANUFACTURING

Dark Fibre Links a Laser Steel Factory 19 km From Its Office

Dark fibre & WAN

A laser steel cutting factory and its head office were 19 km apart and connected only by a slow VPN over NBN. Large production files, CAD/CAM downloads and server access at the factory dragged, and there was no line of sight for a wireless link. We provisioned a dedicated Vocus dark fibre path between the sites and upgraded the office internet to 250 Mbps with WatchGuard firewalls in high availability.



The issues we needed to solve

- Factory and head office 19 km apart with no line-of-sight path for wireless
- VPN over NBN was too slow for large laser cutting and CNC file downloads
- Production machines pulled files from office servers, causing delays and re-work
- Office relied on a single internet connection with no firewall redundancy
- Production stoppages whenever the VPN dropped or the NBN link congested

PROJECT 59 / DELIVERY

What we did — and why

01 / The work delivered

Surveyed the route and coordinated with Vocus to provision dedicated dark fibre between office and factory

Why this mattered: Starting with the actual site and workload reduces the risk of buying equipment that cannot solve the underlying problem.

02 / The work delivered

Delivered a private 10 Gbps layer-2 link between the two sites with no contention

Why this mattered: This workstream addressed the manufacturing operation's need for a maintainable service rather than leaving the original limitation in place.

03 / The work delivered

Upgraded the office to 250 Mbps symmetrical Vocus internet for cloud and remote access

Why this mattered: Moving the workload or retiring obsolete dependencies reduces the amount of legacy infrastructure the business still has to operate.

04 / The work delivered

Installed a WatchGuard firewall pair in active/passive high availability at the office

Why this mattered: The business needs a path through equipment or connection failures rather than making one component a single point of interruption.

05 / The work delivered

Segregated factory machine, office and guest traffic onto separate VLANs

Why this mattered: Guests, cameras and business systems have different trust levels, so they should not inherit unrestricted access to each other.

06 / The work delivered

Added monitoring and alerting on both the dark fibre link and internet connection

Why this mattered: Installing a system is not the end of the security job: visibility and control are needed while staff continue to use it.

PROJECT 59 / BUSINESS RESULT

What changed for the business

10Gbps dedicated dark fibre between sites	19km private fibre span
250Mbps symmetrical office internet	HA WatchGuard firewall pair
Near-zero production file wait times	

What we used — and its role

WatchGuard

A managed firewall platform combines traffic control, secure access and, where deployed, SD-WAN policy in a consistent operating model.

Vocus

The recorded carrier service provides internet or private inter-site capacity; the speed and connection type are specific to this project.

The sales conversation

If your organisation recognises these same issues, start with the constraint rather than a product list: which part of the environment interrupts staff, exposes data or makes growth harder? We can review the current setup, identify dependencies and scope the relevant services before recommending a change.



A word from the stable

The right connection makes the rest of the office happier.

1300 904 635 | hello@uitg.com.au

PROJECT 59 / QUESTIONS

A closer look at the solution

Why dark fibre instead of a faster internet VPN?

A VPN over the public internet shares bandwidth with every other user and adds encryption and routing overhead. A dedicated dark fibre link gives the business a private, uncontended 10 Gbps path between two sites with predictable latency and no internet congestion.

What does 'no line of sight' mean for connectivity options?

Line of sight is needed for many point-to-point wireless technologies. Hills, buildings and vegetation blocked any wireless path here, so a cabled fibre solution was the only reliable way to deliver high bandwidth between the two sites.

How does the factory benefit from 10 Gbps back to the office?

Laser and CNC machines download large cutting files, nesting patterns and job files from servers in the office. At 10 Gbps those transfers complete almost instantly, so machines spend less time waiting and more time cutting.

What is the advantage of WatchGuard firewalls in high availability?

Two WatchGuard firewalls run as a clustered pair. If one unit fails, the other takes over automatically, keeping internet access, site-to-site routing and security enforcement online without manual intervention.

Can the factory still operate if the office internet goes down?

Yes. The dark fibre link is independent of the office internet connection. Even if the office loses its 250 Mbps internet link, the factory still has full-speed access to office servers through the private fibre path.

PROJECT 60 / LEGAL

Legal Firm IT Upgrade: 1.8 TB File Server Moved to Microsoft Teams

Full IT modernisation

A law firm was running 1.8 TB of matter files on an ageing on-premises file server, with printers scanning to network folders and desktops joined to a local domain. We migrated everything to Microsoft Teams and SharePoint, integrated the Konica Minolta printers to scan straight into client folders, decommissioned the server, rebuilt every computer into Microsoft Entra ID with Intune, upgraded the internet to 500/500 Mbps NBN Enterprise Ethernet from Swoop, and installed a full Cisco Meraki network with 16 cameras.



The issues we needed to solve

- 1.8 TB of matter files, precedents and scanned documents locked on a single ageing file server
- Konica Minolta printers scanning only to on-premises network folders, with staff manually filing every document
- All desktops and laptops joined to a local Active Directory domain with no modern device management
- Slow, asymmetric internet that could not support cloud file access or Teams for the whole firm
- Flat network with unmanaged switches, an end-of-life firewall and patchy Wi-Fi through the tenancy
- No CCTV coverage of reception, stairwells or the carpark despite client confidentiality obligations

PROJECT 60 / DELIVERY

What we did — and why

01 / The work delivered

Mapped the full file structure and matter numbering, then designed matching Teams and SharePoint document libraries

Why this mattered: Starting with the actual site and workload reduces the risk of buying equipment that cannot solve the underlying problem.

02 / The work delivered

Migrated 1.8 TB in staged passes with delta syncs, so staff kept working until the final weekend cutover

Why this mattered: Moving the workload or retiring obsolete dependencies reduces the amount of legacy infrastructure the business still has to operate.

03 / The work delivered

Configured OneDrive and Teams file sync with retention and versioning on every matter library

Why this mattered: Moving the workload or retiring obsolete dependencies reduces the amount of legacy infrastructure the business still has to operate.

04 / The work delivered

Integrated the Konica Minolta multifunction devices to scan directly into the correct client folder in SharePoint from the printer panel

Why this mattered: Moving the workload or retiring obsolete dependencies reduces the amount of legacy infrastructure the business still has to operate.

05 / The work delivered

Decommissioned and removed the file server and domain controller once all data and printing was verified in the cloud

Why this mattered: Moving the workload or retiring obsolete dependencies reduces the amount of legacy infrastructure the business still has to operate.

06 / The work delivered

Rebuilt every computer and joined it to Microsoft Entra ID, enrolled in Intune with compliance, encryption and app deployment policies

Why this mattered: A consistent device baseline makes deployment and ongoing support more predictable for staff and the service team.

07 / The work delivered

Upgraded the internet to 500/500 Mbps NBN Enterprise Ethernet from Swoop, our partner ISP, with an SLA

Why this mattered: Reliable connectivity is the foundation for the applications above it; changing software cannot repair an inadequate physical or network path.

08 / The work delivered

Installed a Cisco Meraki firewall, Meraki switches and Meraki access points for full cloud-managed networking and Wi-Fi

Why this mattered: Reliable connectivity is the foundation for the applications above it; changing software cannot repair an inadequate physical or network path.

09 / The work delivered

Deployed 16 Meraki cameras covering reception, corridors, stairwells and the carpark with cloud video retention

Why this mattered: Moving the workload or retiring obsolete dependencies reduces the amount of legacy infrastructure the business still has to operate.

PROJECT 60 / BUSINESS RESULT

What changed for the business

1.8TB of matter files migrated to Teams and SharePoint	0 on-premises servers remaining
500/500 Mbps symmetrical Enterprise Ethernet	16 Meraki cameras across the office and carpark
100% of devices in Entra ID and Intune	

What we used — and its role

Cisco Meraki

Cloud management gives the support team a common view of the deployed network or camera estate without needing to visit each location.

Intune / Autopilot

Policy-driven deployment helps standardise devices and reduces manual setup when a user receives a replacement computer.

SharePoint / Teams / OneDrive

Shared cloud workspaces separate business files and collaboration from a single office server or an individual computer.

Swoop

The recorded carrier service provides the WAN connection; routing, wireless and user support remain separate design decisions.

Konica / managed print

A managed print platform brings device support and print administration into a maintainable workplace service.

The sales conversation

If your organisation recognises these same issues, start with the constraint rather than a product list: which part of the environment interrupts staff, exposes data or makes growth harder? We can review the current setup, identify dependencies and scope the relevant services before recommending a change.



A word from the stable

Old dependencies don't retire themselves.

1300 904 635 | hello@uitg.com.au

PROJECT 60 / QUESTIONS

A closer look at the solution

How do the printers scan straight into client folders?

The Konica Minolta multifunction devices are integrated with SharePoint, so staff choose the client or matter destination on the printer panel and the scan lands directly in the correct folder in Teams. There is no scan-to-email step and no manual filing afterwards.

Was there downtime while 1.8 TB was migrated?

No. The bulk of the data was copied in staged passes over several weeks while staff kept using the server. The final delta sync and cutover ran over a weekend, and the firm started Monday working entirely from Teams.

Why remove the file server instead of keeping it as a backup?

Once files are in SharePoint with versioning, retention and cloud backup, an on-premises server adds cost, patching and risk without adding protection. Removing it also let us retire the local domain and move to Entra ID and Intune.

What changed for staff after the Entra ID and Intune rebuild?

Each machine was rebuilt clean and now signs in with the same Microsoft 365 account used for email and Teams. Devices are encrypted, patched and configured automatically, and a replacement laptop can be shipped to a lawyer and set itself up without a technician touching it.

Why 500/500 Mbps symmetrical internet for a small office?

Cloud file access, large document uploads, scanning to SharePoint, Teams calls and cloud camera footage all depend on upload speed, which ordinary broadband does not provide. Enterprise Ethernet delivers matched upload and download with a service level agreement.

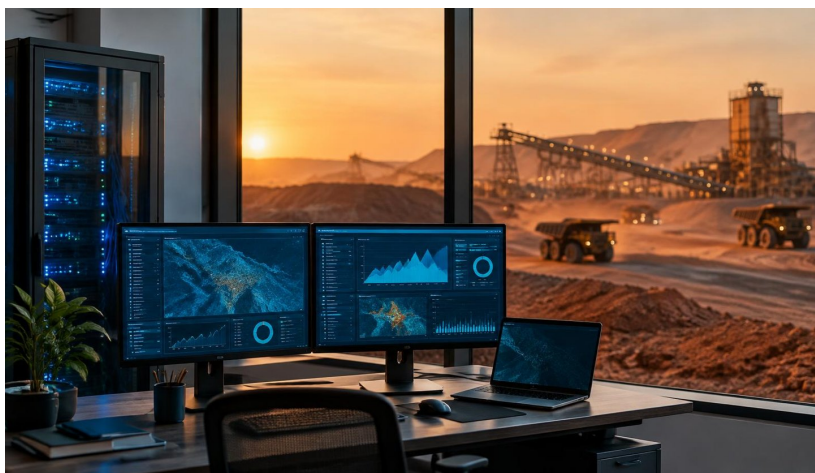
Where are the cameras and who can view them?

The 16 Meraki cameras cover reception, public corridors, stairwells and the carpark only, not private offices or meeting rooms. Footage is retained in the Meraki cloud and access is limited to nominated firm staff.

Mining Company Migrated 1200 Users from Exchange 2013 to Office 365

Enterprise email migration

A mining company was running 1200 users across 15 on-premise Exchange 2013 servers at its head office and mine sites, with no mobile email, no multi-factor authentication and servers that had long passed end of support. We migrated all 1200 mailboxes to Office 365 in two months, wave by wave, with no email downtime and no impact on 24/7 mine operations.



The issues we needed to solve

- 15 ageing Exchange 2013 servers supporting 1200 users across head office, mine sites and remote camps
- Exchange 2013 was out of support, with no security updates and rising hardware and licence risk
- Remote and fly-in fly-out staff had no reliable mobile email and poor Outlook Web Access
- No multi-factor authentication or conditional access on a environment used by contractors and vendors
- Mailboxes of 20 GB or more, slow mail flow between sites and frequent database white-space problems
- Continuous mine operations meant there was no maintenance window in which email could go offline

PROJECT 61 / DELIVERY

What we did — and why

01 / The work delivered

Audited every mailbox, database, transport rule, shared mailbox, resource and third-party application dependency

Why this mattered: Starting with the actual site and workload reduces the risk of buying equipment that cannot solve the underlying problem.

02 / The work delivered

Designed a hybrid Exchange deployment so on-premise and cloud mailboxes could coexist during the migration

Why this mattered: Moving the workload or retiring obsolete dependencies reduces the amount of legacy infrastructure the business still has to operate.

03 / The work delivered

Built the Microsoft 365 tenancy with Entra ID connect, single sign-on, MFA and conditional access before any mailbox moved

Why this mattered: Passwords alone leave accounts exposed; additional access checks make stolen credentials less useful to an attacker.

04 / The work delivered

Sequenced migration waves by site, shift pattern and business criticality so no operation lost email at handover

Why this mattered: The improvement must remain usable and supportable after handover, not depend on knowledge held only by the installer.

05 / The work delivered

Throttled migration bandwidth to protect satellite and microwave links serving remote mine sites

Why this mattered: Reliable connectivity is the foundation for the applications above it; changing software cannot repair an inadequate physical or network path.

06 / The work delivered

Migrated mailboxes in staged batches with delta syncs, then cut over Outlook, mobile and Teams access per wave

Why this mattered: Moving the workload or retiring obsolete dependencies reduces the amount of legacy infrastructure the business still has to operate.

07 / The work delivered

Trained site administrators and super users on Outlook, OneDrive, Teams and shared mailboxes in each wave

Why this mattered: The improvement must remain usable and supportable after handover, not depend on knowledge held only by the installer.

08 / The work delivered

Decommissioned all 15 Exchange 2013 servers once mail flow, journaling and retention were verified in the cloud

Why this mattered: Moving the workload or retiring obsolete dependencies reduces the amount of legacy infrastructure the business still has to operate.

PROJECT 61 / BUSINESS RESULT

What changed for the business

1200 users migrated from Exchange 2013 to Office 365	2 month migration completed across all sites
0 email downtime during the migration	15 on-premise Exchange 2013 servers retired
100% of accounts protected by MFA and conditional access	

What we used — and its role

Microsoft 365

Cloud email and collaboration reduce dependence on local mail servers and make access and administration consistent across devices.

SharePoint / Teams / OneDrive

Shared cloud workspaces separate business files and collaboration from a single office server or an individual computer.

The sales conversation

If your organisation recognises these same issues, start with the constraint rather than a product list: which part of the environment interrupts staff, exposes data or makes growth harder? We can review the current setup, identify dependencies and scope the relevant services before recommending a change.



A word from the stable

Old dependencies don't retire themselves.

1300 904 635 | hello@uitg.com.au

PROJECT 61 / QUESTIONS

A closer look at the solution

How did you migrate 1200 mailboxes without any email downtime?

A hybrid deployment keeps on-premise and cloud mailboxes talking to each other throughout the project. Mail flow never stops, users on the old system and users in Office 365 can email each other normally, and each mailbox is moved individually with a delta sync so only the final cutover moment is brief.

Why was two months the right timeframe?

With 1200 users spread across sites and shift rosters, the migration had to be planned around operational cycles rather than pushed through as one big cutover. Staged waves of 80 to 150 users per weekend gave support time to help people with Outlook profiles and mobile devices, and let the team prove each site before moving on.

What was the biggest risk with remote mine sites?

Bandwidth. Satellite and microwave links at remote sites have limited capacity and high latency, and a mailbox migration can saturate them. We throttled the migration traffic, scheduled larger mailboxes overnight, and confirmed the site links stayed within their committed rates throughout.

What happened to the old Exchange servers afterwards?

Once all mailboxes, shared mailboxes, resource bookings, journaling and retention policies were verified in Office 365, the 15 Exchange 2013 servers were shut down, the data securely wiped, and the hardware retired or reused. That removed a whole unsupported platform from the environment.

What security came with the move?

Every account was brought under single sign-on with multi-factor authentication and conditional access, so sign-ins from unknown devices or unusual locations are challenged. Mailbox auditing, anti-phishing policies and data loss prevention were enabled from the first wave rather than bolted on later.

Did staff need retraining?

Light training, yes. Email behaves the same in Outlook, but file sharing changes from attachments to OneDrive and Teams links. Each wave included short site briefings, a quick reference card and priority help desk cover for the first few days.

Print Publisher Gets 1 Gbps Swoop FTTP and Moves from POP3 to Office 365

Connectivity & Microsoft 365

A local print publisher was losing hours every day to slow internet and still collecting email over POP3, which pulled each message onto one computer and left nothing on a server. We installed a 1 Gbps / 400 Mbps Swoop fibre to the premises (FTTP) service and migrated the whole business from POP3 to Office 365, so mail, files and calendars are now identical on every device.



The issues we needed to solve

- A standard NBN connection too slow for uploading high-resolution artwork, proofs and press-ready files to clients
- Crippled upload speed meant large jobs took hours to send, and staff were planning production around file transfers
- POP3 email downloaded each message to whichever desktop collected it, so nothing appeared on phones, laptops or a second screen
- Mailboxes stored in local desktop files with no backup, so a failed computer would take years of customer orders with it
- No shared calendar, contacts or address book — job deadlines and courier collections were tracked verbally
- No multi-factor authentication on the business's only customer-facing channel
- No practical way to work away from the office or send large files without a portable drive

PROJECT 62 / DELIVERY

What we did — and why

01 / The work delivered

Surveyed the premises, confirmed fibre to the premises availability and quoted the upgrade through Swoop, our partner ISP

Why this mattered: Starting with the actual site and workload reduces the risk of buying equipment that cannot solve the underlying problem.

02 / The work delivered

Provisioned and installed a 1 Gbps download / 400 Mbps upload Swoop FTTP business fibre service with a service level agreement

Why this mattered: Reliable connectivity is the foundation for the applications above it; changing software cannot repair an inadequate physical or network path.

03 / The work delivered

Terminated the fibre at the optical network terminal in the comms cabinet, replaced the ageing router with a managed firewall and re-terminated the patch panel

Why this mattered: Installing a system is not the end of the security job: visibility and control are needed while staff continue to use it.

04 / The work delivered

Built a Microsoft 365 tenancy on the publisher's existing domain with shared mailboxes, a shared job calendar and a single enquiries address

Why this mattered: This workstream addressed the media & entertainment operation's need for a maintainable service rather than leaving the original limitation in place.

05 / The work delivered

Migrated mail out of the POP3 desktop stores and into Exchange Online mailboxes so every device reads the same mailbox

Why this mattered: Moving the workload or retiring obsolete dependencies reduces the amount of legacy infrastructure the business still has to operate.

06 / The work delivered

Enabled Outlook, mobile mail and Outlook on the web with multi-factor authentication and modern sign-in

Why this mattered: Passwords alone leave accounts exposed; additional access checks make stolen credentials less useful to an attacker.

07 / The work delivered

Turned on OneDrive and SharePoint for artwork, templates and customer records, replacing attachment-based file sharing

Why this mattered: Moving the workload or retiring obsolete dependencies reduces the amount of legacy infrastructure the business still has to operate.

08 / The work delivered

Enabled Microsoft 365 backup so mail, OneDrive and SharePoint can be restored independently of Microsoft

Why this mattered: A recoverable copy must exist independently of the production service; synchronising files alone is not a recovery strategy.

09 / The work delivered

Trained the team on Outlook, shared calendars and file links, then retired the POP3 accounts once mail flow was verified

Why this mattered: The improvement must remain usable and supportable after handover, not depend on knowledge held only by the installer.

PROJECT 62 / BUSINESS RESULT

What changed for the business

1Gbps download / 400 Mbps upload Swoop FTTP fibre	100% of mailboxes moved from POP3 to Office 365
0 messages left stranded on a single desktop	100% of accounts protected by multi-factor authentication
Daily backups of mail, OneDrive and SharePoint	

What we used — and its role

Microsoft 365

Cloud email and collaboration reduce dependence on local mail servers and make access and administration consistent across devices.

SharePoint / Teams / OneDrive

Shared cloud workspaces separate business files and collaboration from a single office server or an individual computer.

Swoop

The recorded carrier service provides the WAN connection; routing, wireless and user support remain separate design decisions.

The sales conversation

If your organisation recognises these same issues, start with the constraint rather than a product list: which part of the environment interrupts staff, exposes data or makes growth harder? We can review the current setup, identify dependencies and scope the relevant services before recommending a change.



A word from the stable

The right connection makes the rest of the office happier.

1300 904 635 | hello@uitg.com.au

PROJECT 62 / QUESTIONS

A closer look at the solution

What was wrong with POP3 email?

POP3 downloads each message onto whichever computer collects it and usually removes it from the server. Two people cannot see the same inbox, phones show nothing useful, and a failed PC destroys the mail with it. Office 365 keeps one copy in the cloud and syncs every device against it.

Why 1 Gbps down and 400 Mbps up?

Business fibre is commonly sold asymmetrically, and 400 Mbps upload is still many times faster than a standard NBN upload — enough for artwork, proof and press-file hand-offs without paying for symmetrical capacity the publisher does not need yet. If volumes grow we can step the service up without re-cabling the premises.

Did email go offline during the migration?

No. The Microsoft 365 mailboxes were built alongside the existing POP3 accounts and the historic mail imported into them, then the domain's mail routing was switched over once everything was verified. The cutover ran outside business hours and the team arrived to the same addresses, now in Outlook and on their phones.

What happened to years of old POP3 mail?

It was exported from the desktop stores and imported into the matching Office 365 mailboxes. Old orders, quotes and proofs are now searchable in Outlook instead of buried in a data file on one machine that nobody could back up.

What did the faster connection actually change day to day?

High-resolution artwork that used to take an hour to send now uploads in minutes, cloud quoting and prepress tools respond instantly, and video calls with clients no longer stall when someone else is transferring a file. Upload-bound jobs stopped being scheduled around the connection.

Doesn't Microsoft back up Office 365?

Microsoft keeps the platform running, but it does not give you a simple way back from a deleted mailbox, an overwritten file or a compromised account. We enabled a daily backup of mail, OneDrive and SharePoint so items can be restored independently.

Hyper-V and Synology Cluster Replicated Across Two NEXTDC Datacentres

Private cloud & disaster recovery

A client holding close to 900 TB of business-critical data needed enterprise resilience without losing control of their own infrastructure. We designed and built a two-site private cloud: Hyper-V compute clusters and Synology storage clusters in two NEXTDC datacentres, replicated for automatic failover, wired together with dark fibre to the client's office, and backed up over an express route to Wasabi using Veeam Backup & Replication. The office runs on Vocus 2 Gbps / 2 Gbps symmetrical fibre internet, sized for the traffic a two-site private cloud generates.



The issues we needed to solve

- Nearly 900 TB of live client data with no tolerance for loss or extended outage
- Existing on-premises servers with no failover — one hardware failure would take the business down
- No disaster recovery site: a fire, flood or extended power outage at the office would stop all systems
- Backup jobs running over the shared internet connection were slow and competed with staff traffic
- Office internet capacity was nowhere near the size needed to work against clusters holding that much data
- A single path between the office and any hosted infrastructure meant one cut cable would isolate the site
- No centralised switching or security fabric across sites, making management and segmentation difficult

PROJECT 63 / DELIVERY

What we did — and why

01 / The work delivered

Racked and configured a Hyper-V cluster of 4 servers in each of two NEXTDC datacentres, with clustered storage and live failover between nodes

Why this mattered: The business needs a path through equipment or connection failures rather than making one component a single point of interruption.

02 / The work delivered

Deployed 4 Synology storage appliances in each datacentre as a replicated storage cluster, hosting close to 900 TB across the pair

Why this mattered: The business needs a path through equipment or connection failures rather than making one component a single point of interruption.

03 / The work delivered

Provisioned dark fibre from the client's office to each datacentre, so the office has two physically diverse paths and the datacentres stay connected to each other if one link fails

Why this mattered: Reliable connectivity is the foundation for the applications above it; changing software cannot repair an inadequate physical or network path.

04 / The work delivered

Installed Cisco Meraki switching and Meraki firewalls across all three sites, cloud-managed from a single dashboard with consistent security policies

Why this mattered: Reliable connectivity is the foundation for the applications above it; changing software cannot repair an inadequate physical or network path.

05 / The work delivered

Provisioned Vocus 2 Gbps / 2 Gbps symmetrical fibre internet to the office, giving staff full-speed access to the hosted clusters with headroom for cloud services and outbound traffic

Why this mattered: Reliable connectivity is the foundation for the applications above it; changing software cannot repair an inadequate physical or network path.

06 / The work delivered

Configured continuous replication between the two clusters so workloads fail over automatically if a datacentre or cluster node goes down

Why this mattered: The business needs a path through equipment or connection failures rather than making one component a single point of interruption.

07 / The work delivered

Built an express route to Wasabi for backup storage, keeping backup traffic off the internet connection and the LAN

Why this mattered: A recoverable copy must exist independently of the production service; synchronising files alone is not a recovery strategy.

08 / The work delivered

Deployed Veeam Backup & Replication to protect the clusters, with backups landing in Wasabi and regular restore testing built into the schedule

Why this mattered: The business needs a path through equipment or connection failures rather than making one component a single point of interruption.

09 / The work delivered

Tested failover by taking nodes and links offline deliberately, proving the surviving cluster carries the load before handover

Why this mattered: The business needs a path through equipment or connection failures rather than making one component a single point of interruption.

PROJECT 63 / BUSINESS RESULT

What changed for the business

900TB of client data protected across two datacentres	2 NEXTDC datacentres with automatic failover
4+4 Hyper-V hosts and Synology appliances per site	2Gbps symmetrical Vocus fibre internet to the office
3 diverse dark fibre paths joining office and datacentres	Veeam backups to Wasabi over a dedicated express route

What we used — and its role

Cisco Meraki

Cloud management gives the support team a common view of the deployed network or camera estate without needing to visit each location.

Veeam Backup & Replication

Backup and replication address different recovery needs: retained copies of data and availability of virtual workloads.

Wasabi S3

Object storage provides a cloud destination for the recorded backup or file-data architecture, distinct from the users' local devices.

Vocus

The recorded carrier service provides internet or private inter-site capacity; the speed and connection type are specific to this project.

Hyper-V

Virtualisation consolidates server workloads and supports the recorded migration or cluster design without a separate physical machine for every application.

Synology

Shared storage supports the recorded server and data architecture; replication and backup must still be designed as separate protections.

The sales conversation

If your organisation recognises these same issues, start with the constraint rather than a product list: which part of the environment interrupts staff, exposes data or makes growth harder? We can review the current setup, identify dependencies and scope the relevant services before recommending a change.



A word from the stable

Backups need a recovery plan, not just a hopeful nod.

1300 904 635 | hello@uitg.com.au

PROJECT 63 / QUESTIONS

A closer look at the solution

Why build in two datacentres instead of moving to public cloud?

At nearly 900 TB, public cloud storage and egress costs were significant, and the client wanted predictable performance and full control of their data. Two colocation sites with replication deliver cloud-style resilience on hardware the client owns, at a fixed monthly cost.

What happens if one datacentre goes offline?

The clusters replicate continuously, so the surviving site takes over the workloads automatically. We proved this before handover by deliberately taking nodes and links offline — services kept running on the second cluster with no data loss.

Why dark fibre to the office?

Dark fibre gives the office a dedicated, uncontended path to each datacentre with effectively unlimited capacity. Because there is a fibre path to each site plus a path between the datacentres themselves, losing any single link still leaves every location connected.

What does the Vocus 2 Gbps / 2 Gbps internet service do?

The dark fibre paths carry traffic privately between the office and the datacentres. The Vocus service is the office's connection to the public internet, cloud platforms and the outside world. At 2 Gbps symmetrical, uploading is as fast as downloading, so staff can work from hosted applications all day and still push large datasets out without the connection becoming the bottleneck.

How is the environment backed up?

Veeam Backup & Replication protects the virtual machines and storage, sending backup copies to Wasabi over an express route so backup traffic never touches the office internet connection. Restores are tested on a schedule, not just assumed to work.

Why Meraki across three sites?

Cisco Meraki switching and firewalls are managed from one cloud dashboard, so a policy change, a new network segment or a firmware update applies consistently across the office and both datacentres without anyone driving between sites.

Can this grow beyond 900 TB?

Yes. Both the Hyper-V compute and the Synology storage scale by adding nodes to the existing clusters, and the dark fibre paths have the headroom to carry far more replication and user traffic than they do today.

PROJECT 64 / HEALTHCARE

New Doctor Surgery in Perth Fitted Out and Placed on Gold Managed Services

Medical practice fit-out

A brand-new medical practice in Perth had eight consulting rooms, 18 staff and an opening date, but no cabling, network, phones or computers. We fitted the surgery out end to end — structured data cabling to every room, Cisco Meraki routing, switching, wireless and guest wireless, Vocus 1 Gbps / 1 Gbps symmetrical fibre internet, 18 desktops and monitors, Office 365 for the whole team and a hosted 3CX phone system — then placed the practice on our Gold Managed Services plan so the environment stays monitored, patched and protected long after opening day.



The issues we needed to solve

- Brand-new tenancy with no data cabling, network, internet service, phones or computers, and a fixed opening date to work back from
- Eight consulting rooms plus reception and the back office each needed a wired data point for clinical and administrative systems
- 18 staff with no shared calendar, mailboxes or file storage — and no IT staff of their own
- Patients and visitors needed wireless, but it could not sit on the same network as clinical systems
- No phone system, so the practice could not take bookings or transfer calls between consulting rooms
- Clinical and administrative data had to be secure, backed up and recoverable, with no room or appetite for an on-premise server
- The practice wanted a support partner in place from day one rather than finding one after the first outage

PROJECT 64 / DELIVERY

What we did — and why

01 / The work delivered

Walked the new premises with the practice manager and marked up data points for all eight consulting rooms, reception and the back-office positions

Why this mattered: Starting with the actual site and workload reduces the risk of buying equipment that cannot solve the underlying problem.

02 / The work delivered

Ran structured Cat6 data cabling to every position, terminated at a patch panel inside a lockable wall cabinet and tested every drop end to end

Why this mattered: Installing a system is not the end of the security job: visibility and control are needed while staff continue to use it.

03 / The work delivered

Installed a Cisco Meraki MX security appliance as the practice router, with Meraki switching and Meraki wireless access points, all managed from a single cloud dashboard

Why this mattered: Reliable connectivity is the foundation for the applications above it; changing software cannot repair an inadequate physical or network path.

04 / The work delivered

Configured separate networks for clinical systems, staff and a guest wireless SSID for patients, with the guest network isolated from practice data

Why this mattered: Guests, cameras and business systems have different trust levels, so they should not inherit unrestricted access to each other.

05 / The work delivered

Provisioned Vocus 1 Gbps / 1 Gbps symmetrical fibre internet with a service level agreement, sized for cloud clinical systems, video consults and file transfers

Why this mattered: Reliable connectivity is the foundation for the applications above it; changing software cannot repair an inadequate physical or network path.

06 / The work delivered

Supplied and configured 18 desktops and monitors, imaged and enrolled in Intune with clinical software, printers and OneDrive mapped before delivery

Why this mattered: Starting with the actual site and workload reduces the risk of buying equipment that cannot solve the underlying problem.

07 / The work delivered

Built Office 365 for all 18 staff with shared mailboxes and a practice calendar, OneDrive and SharePoint for files, and multi-factor authentication enforced on every account

Why this mattered: Passwords alone leave accounts exposed; additional access checks make stolen credentials less useful to an attacker.

08 / The work delivered

Deployed a hosted 3CX phone system with an extension in each consulting room and at reception, an IVR greeting, a call queue, voicemail-to-email and mobile apps for after-hours cover

Why this mattered: Communications need to follow how people work, with maintainable routing and extensions instead of the limitations of the old phone arrangement.

09 / The work delivered

Enabled Microsoft 365 backup so mail, OneDrive and SharePoint can be restored independently of Microsoft

Why this mattered: A recoverable copy must exist independently of the production service; synchronising files alone is not a recovery strategy.

10 / The work delivered

Surveyed wireless coverage in every consulting room and the waiting area, then tuned channels and transmit power so a room tablet or laptop never drops mid-consultation

Why this mattered: Starting with the actual site and workload reduces the risk of buying equipment that cannot solve the underlying problem.

11 / The work delivered

Placed the practice on the Gold Managed Services plan — proactive monitoring and patching, SentinelOne Complete endpoint protection, Guardz 24/7/365 MDR across servers, workstations and Microsoft 365, Intune device management, email signature management, IT governance and roadmap, and strategic quarterly reviews

Why this mattered: Installing a system is not the end of the security job: visibility and control are needed while staff continue to use it.

12 / The work delivered

Commissioned and documented everything — network diagram, IP plan, asset register and admin credentials — then trained reception and the principals before handover

Why this mattered: The improvement must remain usable and supportable after handover, not depend on knowledge held only by the installer.

PROJECT 64 / BUSINESS RESULT

What changed for the business

8 consulting rooms cabled, wired and signed off before opening day	18 desktops, monitors and mailboxes delivered ready to work
1Gbps symmetrical Vocus fibre internet to the surgery	3 separate networks: clinical, staff and patient guest wireless
24/7 monitoring and MDR under the Gold Managed Services plan	0 on-premise servers needed to run the practice

What we used — and its role

SentinelOne

Endpoint detection and response helps identify suspicious activity on computers and supports investigation and containment.

Guardz

Managed detection and response adds ongoing threat review and response beyond a one-off security installation.

Cisco Meraki

Cloud management gives the support team a common view of the deployed network or camera estate without needing to visit each location.

Microsoft 365

Cloud email and collaboration reduce dependence on local mail servers and make access and administration consistent across devices.

Intune / Autopilot

Policy-driven deployment helps standardise devices and reduces manual setup when a user receives a replacement computer.

SharePoint / Teams / OneDrive

Shared cloud workspaces separate business files and collaboration from a single office server or an individual computer.

3CX

A software-based phone system supports central call routing and flexible extensions without preserving the old PBX operating model.

Vocus

The recorded carrier service provides internet or private inter-site capacity; the speed and connection type are specific to this project.

The sales conversation

If your organisation recognises these same issues, start with the constraint rather than a product list: which part of the environment interrupts staff, exposes data or makes growth harder? We can review the current setup, identify dependencies and scope the relevant services before recommending a change.



A word from the stable

Less IT drama. More getting on with the day.

1300 904 635 | hello@uitg.com.au

PROJECT 64 / QUESTIONS

A closer look at the solution

What did the office fit-out actually include?

Everything the surgery needed to trade on day one: data cabling to all eight consulting rooms and the back office, a comms cabinet with patching and switching, a Meraki router and firewalls, wireless and guest wireless, the Vocus fibre internet connection, 18 desktops with monitors, Office 365 mailboxes and shared files for all 18 staff, and a hosted 3CX phone system. It was designed, installed, tested and documented as one project with a single point of accountability.

Why Cisco Meraki for a single-site practice?

Meraki is cloud-managed, so the router, switches and access points are configured, updated and monitored from one online dashboard rather than by someone plugging a laptop into a box in the comms room. That suits a practice with no IT staff: changes happen remotely, alerts reach us before the practice notices a problem, and every device is accounted for in the same place.

Why 1 Gbps / 1 Gbps symmetrical fibre?

A modern surgery is upload-heavy. Clinical systems, pathology and imaging files, cloud backups, video consults and phone calls all leave the building constantly. Symmetrical fibre means uploading is as fast as downloading, so a consult-room workstation sending a large file does not slow the whole practice, and the service comes with a carrier service level agreement rather than best-efforts home broadband.

Why keep guest wireless separate from the practice network?

Patients and visitors bring their own devices, and there is no way to know what is on them. Putting that traffic on its own network means a guest device can never reach clinical systems or file storage. The practice can also change the patient Wi-Fi password without locking staff out of anything.

How does a 3CX phone system work in a surgery?

3CX is a hosted PBX, so the phone system runs from the cloud instead of from a box in the comms room. Reception gets a call queue and a professional greeting, each consulting room gets an extension that can be dialled directly, voicemail arrives as email, and the principals can take calls on the mobile app when the practice is closed. Adding or moving an extension is a settings change, not a visit.

What does the Gold Managed Services plan cover for this practice?

Gold includes everything in Silver — proactive monitoring and patching, SentinelOne Complete endpoint protection with EDR, Guardz 24/7/365 MDR across servers, workstations and Microsoft 365, Intune device management, Microsoft 365 backup and email signature management, with unlimited remote support — plus web and DNS hosting, documented IT governance and a roadmap, and strategic quarterly reviews. Because it is a per-user plan, all 18 staff are covered on the same tier.

How does this help with patient data and privacy obligations?

A practice holds personal information it has to protect, and the controls that matter most are the unglamorous ones: multi-factor authentication on every account, devices patched and monitored continuously, 24/7 threat detection that can act at three in the morning, daily backups of Microsoft 365, and a documented record of who has access to what. All of that sits inside the plan rather than depending on someone remembering to do it.

Could the practice add a second site or more rooms later?

Yes. Meraki organisations are designed for multiple sites under one dashboard, so a second location inherits the same security policies and monitoring, and new consulting rooms are additional data drops and access points rather than a redesign. The Vocus fibre service and the per-user Gold plan both scale in the same way.

Let's make your IT the quiet part of the day



Start with a practical review

- Tell us what is unreliable, expensive, exposed or getting in the way.
- We review the current environment and the dependencies that matter.
- You receive a scoped recommendation for the services and delivery work needed.

Unicorn IT Group

1300 904 635

hello@uitg.com.au

unicornitgroup.com

Suite 122, 8 Collingwood St, Osborne Park WA 6017

Office: Mon-Fri 7:30am-5:30pm AWST. Monitoring: 24/7/365.

Current plan inclusions and rates: unicornitgroup.com/pricing. Historical project details in this booklet are not a current quote.