UNICORN IT GROUP

Cyber security and IT services

MANAGED DETECTION & RESPONSE | Professional Services

Attackers Caught Minutes After Huntress MDR Deployment

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

KEY RESULTS

Minutes	100%	0	24/7/365
from deployment to active-threat detection	of compromised endpoints isolated	data exfiltration incidents	SOC monitoring now in place

BEFORE

- 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

AFTER

- Minutes - from deployment to active-threat detection
- 100% - of compromised endpoints isolated
- 0 - data exfiltration incidents
- Deployed Huntress MDR agents to every server and workstation for continuous behavioural monitoring

"We knew something was wrong but had no idea where to look. Within minutes of the Huntress deployment the attackers were found, devices were isolated, and our Office 365 accounts were secured. It was the fastest response we have ever seen."

- Managing Director, professional services firm