

CASE STUDY



CHALLENGE:

A rapidly expanding technology company based in London, UK, encountered critical security challenges, including a surge in cyberattacks due to reliance on cloud services and remote work, limited internal security expertise within their small IT team, and significant concerns about GDPR compliance given the sensitive customer data they managed.



SOLUTION:

The implementation of a Managed Detection and Response (MDR) solution across multiple locations in the United Kingdom addressed these challenges effectively. The MDR solution enabled:

- 24/7 threat monitoring
- advanced threat detection using AI and machine learning to identify and prioritize threats
- deployment of the MDR service using an RMM platform and bash scripting for Linux systems to support the client's needs
- and expert-led incident response
- The emphasis on collecting only meta-data ensured GDPR compliance and adherence to data sovereignty regulations



RESULTS:

The MDR solution delivered tangible outcomes, including malware infections, including through documented processes and incident reporting, a fortified overall security posture with enhanced vulnerability management and threat intelligence, and increased efficiency by freeing up internal IT resources for strategic initiatives.

CASE STUDY



KEY LEARNINGS:

This case highlights the effectiveness of MDR in addressing security challenges faced by European companies, particularly in the context of GDPR compliance and complex cyber threats. The combination of advanced technology with expert analysis proves crucial for comprehensive threat detection and response. The proactive adoption of compliance measures not only ensures regulatory adherence but also safeguards against potential fines and reputational damage. Ultimately, MDR emerges as a transformative solution, significantly improving security posture, reducing compliance burden, and enhancing operational efficiency.

- MDR can effectively address the security challenges of European companies facing GDPR compliance and complex cyber threats
- Combining advanced technology with expert analysis is crucial for comprehensive threat detection and response
- MDR can significantly improve security posture, reduce compliance burden, and enhance operational efficiency



LOOKING FORWARD:

We project a continual reinforcement of our client's security posture, sustained by the advantages of round-the-clock threat monitoring, advanced AI-driven threat detection, and expert-led incident response. Our proactive approach to GDPR compliance not only aligns with existing regulations but also serves as a proactive safeguard against evolving regulatory landscapes. Anticipating persistent gains in operational efficiency, we aim to free up internal resources for strategic initiatives that will foster innovation and drive sustained growth.