MICROLAND®
Making digital happen

CASE STUDY

Microland Improved Infrastructure Security for a Leading UK-based Public Services Provider by Implementing Microsoft Defender for Endpoint (MDE) Solution for 11000+ Endpoints

Overview

The client is an FTSE Top 250 company known for delivering services to governments and other institutions serving the public or protecting vital national interests. Due to the nature of their business, it was imperative for the client to bolster their cybersecurity posture. They acknowledged the need for a more integrated and robust endpoint security solution to safeguard their extensive network of endpoints against evolving threats. The client sought the expertise of Microland, their trusted technology partner, to deploy the next-gen Antivirus (AV) Protection (SaaS) from Microsoft for their endpoints, replacing the existing Symantec Endpoint Protection (SEP) and proactively managing threats.

Challenges

The client faced multiple challenges related to its reliance on Symantec Endpoint Protection (SEP). The use of SEP left the company vulnerable to evolving cyber threats and malware attacks. The inadequacy of SEP's signature-based detection resulted in security incidents and compromised systems. The management of multiple security tools became complex and resource-intensive, straining IT resources and hampering operational efficiency. Additionally, the high licensing and maintenance costs associated with SEP and other fragmented security solutions further exacerbated the situation.

Additionally, SEP was not a user-friendly and a cost-effective antivirus protection solution. The client also faced challenges in establishing robust processes for monitoring security alerts and recommendations across its extensive network of over 11000 endpoints. These issues collectively emphasized the need for a comprehensive and efficient cybersecurity strategy to safeguard the client’s digital environment.

Solution

Microland, a Microsoft Solution Partner in Cloud Security, executed a comprehensive migration process to migrate the client's endpoints to MDE. Microland's security specialists managed the entire migration with precision, utilizing a strategic mix of technologies for seamless integration with the client’s existing infrastructure. We leveraged the following Microsoft services to implement real-time analysis and deliver enterprise-level protection for endpoints effectively with MDE.

- **Group Policy Objects (GPO) -** Used for centralized policy management and configuration of MDE across the client's extensive device network.

- **System Center Configuration Manager (SCCM) -** Employed for large-scale deployment of MDE agents to endpoints, ensuring efficient rollout and management.

- **Microsoft Intune -** Integrated for cloud-based management of MDE, enhancing flexibility and control over security policies for remote devices.

- **Azure ARC (For Servers) -** Overcoming challenges in onboarding servers to Defender, Microland selected Azure ARC for efficiently bringing servers into Defender using **Microsoft Defender for Cloud** plans.

Additionally, Microland conducted a thorough compatibility assessment, identifying potential conflicts, and implementing necessary adjustments for flawless MDE integration with the client's IT environment. Our cybersecurity experts provided comprehensive training to the client's IT staff and end-users, ensuring a smooth transition and optimal utilization of MDE's features.

Value Delivered

Improved security with next-gen protection against known and evolving cyber threats in real-time across multiple platforms. **11000** endpoints onboarded in **MDATP (Microsoft Defender Advanced Threat Protection)** are monitored on a daily basis.

Reduced complexity with a unified platform for endpoint protection, detection, and response, simplifying security and enhancing collaboration between security and IT teams.

Lower operational costs, with total estimated annual savings amounting to **$375K - a $300K reduction in license costs and a $75K reduction in people and maintenance costs.**

Enhanced user experience with reduced security risk