Case Study

Strengthening Endpoints with Microsoft Defender for Endpoint

Microsoft

CUSTOMER OVERVIEW

A multinational law firm with headquarters based in London, UK with 30 offices, over 3000 staff and is a member of the 'Magic Circle'. It is one of the ten largest law firms in the world measured both by number of lawyers and revenue.

INDUSTRY

Law

EMPLOYEE COUNT

3000+

WEBSITE

N/A

satisnet
streamlining security management

SATISNET OVERVIEW

Satisnet are an established cyber security consultancy and MSSP with a pedigree in SIEM solutions established over the last 20 years. We do not offer a 'cookie cutter' approach to MSSP services, but partner and tailor our working practices to suit each customer. Satisnet recognises the need to identify compromises and associated impact within an organisation to improve the security of its IT infrastructure. Security should augment and strengthen an organisation, and we realise that security is not the sole business goal for a company or institution. Your organisation is looking for security solutions that drive business and institutional value among many other considerations. We strive to provide our customers with the answer to one critical question: 'What actions can be taken to truly improve your organisation and make its staff and security architecture better while allowing your organisation to perform its other core business functions?' Satisnet has several uniques as follows:

- **Community & Academic Focus** – We are committed to strengthening the entire security community working with leading universities, training initiatives and by contributing to open-source projects.
- **Cutting Edge Active Defense Technology** - A targeted attacker will easily bypass traditional security technologies. We focus on new defensive ideas and technologies.
- **Training Portal and Cyber Range** - We create real world practical training illustrating attacker and defender's viewpoint. We also offer access to an online cyber range environment which contains over 120+ different challenges ranging from network, active directory, host-based threat hunting, web application attacks, operating system security and forensics.
- **Cyber Security Automation** - Satisnet has been at the forefront of Security Orchestration and Automated Response for the last 8 years, applying automation and machine learning to all aspects of incident response and security operations.

BUSINESS NEEDS

Given the ongoing Coronavirus pandemic worldwide, there has been necessary need for enterprises to change working practices globally. During recent web meetings with the law firm, concerns were raised around security in these uncertain times. The requirement for remote working has become a business necessity and the securing of this has become a priority. Based on these findings, we recommended an initial focus on strengthening their users' endpoint computers and implementing DLP practices to ensure security standards are met by all users in the enterprise. This is vital for a Global Law firm to protect confidential data and their users from cyber attacks.

PRODUCTS/SOLUTION SELECTED

The law firm already had an existing standalone Endpoint Detection and Response (EDR) platform in place, but there was concern that it was not delivering much in terms of proactive monitoring and that it was not linked to any of the law firms' other security and infrastructure platforms – which are largely focused on Microsoft Azure. Satisnet conducted an audit of their existing EDR, and stress tested it against the latest MITRE ATT&CK breach simulations to understand the level of protection it was offering. We also configured a pilot of Microsoft Defender for Endpoint on 100+ employee machines and ran the same tests. The results were conclusive: Defender for Endpoint was clearly better at detection of attacks, with positive results when spotting tactics such as persistence and lateral movement.

The conclusion was to rollout Defender for Endpoint to the whole organisation and to also enable Azure Information Protection (AIP) within it to give advanced and automated Data Leakage Prevention (DLP).

RESULTING BENEFITS

The implementation of Defender for Endpoint has significantly secured and given improved visibility to support the new remote/distributed working model that the law firm now adopts, and they see this mode of working being the 'new norm' even after the pandemic is under control. Now using AIP, the Law firm can control their intellectual property even if it exits the organisation to - customers, partners or third-parties, ensuring only authorised parties maintain access.

Beyond EDR, areas where the law firm can rationalise and consolidate the raft of legacy security tools that they are using and of course paying for, something that traditional EDR's simply do not offer, the platform and associated modules give the following huge wins to the Law firm:

- **Vulnerability and Configuration Management** - This module is powerful and has threat intelligence/attack metrics built in, which replaces the need to buy vulnerability management solutions on Windows 10 devices.
- **Web Filtering** - Built-in free, compliments traditional web filtering and conducts it on the user device itself, so improving browser performance.
- **Advanced Threat Hunting** - Using KQL language security issues detected on a machine can quickly be investigated across the entire estate to spot other occurrences or potential hacker activity.

Integration with Azure and Office 365 ATP (MTP) – with linkage to O365 and Azure/AD – gives a huge advantage in detecting and analysing phishing-based attacks, which is the majority attack vector we see in SOCs.
With Defender for Endpoint integrated holistically with many of the other Azure security platforms the law firm was using: namely Outlook, cloud, and active directory, a joined-up view of security and the ability to perform cross-platform detection and response (XDR) was enabled.
The Law firm is now looking to implement Microsoft Cloud App Security (MCAS) as part of this XDR journey, protecting data and documents within SaaS environments also enabling user behaviour monitoring policies to be monitored and alerted on within the practice.

Microsoft

Microsoft Defender for Endpoint

Microsoft Azure Information Protection

Satisnet Ltd
Suite B, Building 210, The Village,
Butterfield Business Park,
Great Marlings, Luton,
Bedfordshire,
LU2 8DL

Tel: +44 (0) 1582 369330
Email: enquiry@satisnet.co.uk
Website: www.satisnet.co.uk

satisnet
streamlining security management