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).

Microsoft Defender for Endpoint

Microsoft Azure Information Protection

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.

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