Threatscape

SECURITY CHALLENGES

In early 2020 Apex Fund Services (AFS), a financial services company experiencing rapid growth through acquisition, decided a strategic shift to digital transformation would be key in a cloud-first environment. Peter Kavanagh, then-CISO at AFS, attended a Microsoft Security Workshop hosted by Threatscape at Microsoft Ireland's headquarters in Dublin. While AFS were a long-time customer of Microsoft, this workshop was Peter's first encounter with Threatscape's dedicated Microsoft Security team.

Covid-19 compounded the need to accelerate AFS's digital transformation and cloud app adoption as all their employees now had to work remotely. Integrating acquisitions – ranging in size from a 50-user boutique financial services company to larger 1000+ user organisations with on-premises and hybrid infrastructures – added to the complexity. AFS struggled with the myriad of environments, security vendors, processes, and barriers to change that resulted from their ongoing acquisition strategy. The scarcity of skilled cyber security staff at a time of rapid development proved a further challenge.

They needed to choose a security platform, and quickly. AFS needed to not only select a platform to securely enable digital transformation, but also a trusted partner to take them on this journey. As an Azure consumer and advocate, Microsoft was a logical choice for them, but they did not understand the security offerings and capabilities within the M365 E5 licenses.

THREATSCAPE'S SOLUTION

Microsoft's account team and solutions specialists supported Threatscape in engaging with AFS, and we jointly illustrated the power of the Microsoft security platform.

The visibility, security, compliance, and control Microsoft 365 Defender offers proved a compelling business case, and in late 2021, AFS committed to purchasing M365 E5 across the board. At this stage they had grown from c3,000 users in early 2020 to 7,500 users with a projection, through further acquisition, to grow to c15,000 users in mid-2023.

To begin the process, we delivered our M365 Security Assessment to analyse AFS's Microsoft 365 environment and the AFS Azure Infrastructure from a security perspective.

We established a baseline across all aspects of security, including:

- Azure Active Directory, Conditional Access, Privileged Access, SSO
- Identity
- Application security
- Data Security
- Device Security

We examined AFS's security posture to identify gaps and produced a risk report and detailed roadmap highlighting the short, medium, and long-term improvements to further enhance their security, while illustrating how M365 E5 could address many of these gaps.

Using Azure Defender in the Azure Security Centre, we reviewed multiple AFS tenants. The purpose of the assessment was to:

- Review Azure subscription workload security
- Monitor for security alerts
- Identify security misconfiguration of resources already deployed
- Identify where security of resources could be improved during deployment

We also engaged one of our in-house Palo Alto Networks firewall specialists to extend the review to include firewall deployment and configuration in Azure, delivering incremental value to AFS.

The output illustrated security and compliance risks, misconfigurations, and recommendations on how to address risk and compliance using the M365 E5 security and compliance suite.

We now had to engage from a deployment perspective. This began with another security baseline assessment of their environment with our Overwatch for M365 Security service.

We looked at the security posture of AFS and provided a comprehensive report with a difference. We built a security and business impact register addressing Applications, Data, Devices, Identity, and Secure Score. Low business impact and high security risk changes were the low hanging fruit.

AFS migrated from legacy Symantec Endpoint Protection to Microsoft Defender for Endpoint (MDE) delivering quick technical wins and consolidation with Microsoft. With the adoption of MDE across the board, deployments have been simplified as MDE is built into the operating system.

ORGANISATIONAL BENEFITS

AFS quickly gained visibility across all devices regardless of their location. The TVM component of MDE now allows AFS to identify and help prioritise existing vulnerabilities on the devices, caused by misconfigurations and third-party software. In addition, Microsoft Information Protection (MIP) has now enabled AFS to identify where their data resides (Exchange, OneDrive, SharePoint and Teams) and which data types are being stored using the content explorer feature. With users collaborating across different systems and geographies, it is important to ensure AFS data is protected regardless of location. No other security vendor provides the level of security integration M365 E5 offers.

The story continues as we look to further deploy E5 security with a focus on quick business benefits and risk reduction. The roadmap includes deployment and configuration of Defender for Cloud Apps, Identities, O365 and Microsoft Sentinel to feed into their existing SOC service, adding additional automation for incident detection and response, and providing enhanced telemetry and alerting capabilities.

Overwatch for Microsoft Security 365 will now help AFS to maximise the value and benefits of their investment in M365 E5.

> **SIMPLIFY SECURITY WITHOUT COMPROMISE**
>
> The Threatscape team demonstrated deep knowledge and deployment experience, giving us confidence in our partner choice.
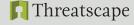>
> *– Peter Kavanagh CISO AFS*

Is your organisation struggling with securing your Microsoft environment? Our team of award-winning engineers have a wealth of expertise delivering a range of services from assessment through to deployment, with on-going consultation and training available as needed.

Why Choose Threatscape

We are the trusted security partner of enterprise clients who rely on us to secure critical IT assets in over 100 countries around the world. We are one of very few dedicated cyber security companies with a separate Microsoft Security Practice, and our expertise in this space is reflected in our status as a Microsoft Security Gold Partner and the Global Microsoft Security & Compliance Partner of the Year 2020/21.

Threatscape

Contact us today to find out how Threatscape can secure your digital environment.