

Empowering Security Operations to Identify Critical Threats

A security breach is inevitable and often starts with a successful phishing attempt against an unsuspecting employee. Once the attackers gain access to that employee's credentials, they can remain hidden in an organisation's infrastructure for weeks, maybe months - watching, waiting, and learning.

Securely monitor every endpoint across **15,000 devices in 160 countries**, delivering a **unified endpoint management and security platform**.

Client Requirement

An education organisation required a unified security ecosystem to detect, respond to, and recover from these threats – fast - to prevent attacks from damaging the business. They needed visibility into an increasingly complex IT estate to **securely monitor every endpoint across 15,000 devices in 160 countries, delivering a unified endpoint management and security platform.**

Challenge

Most of toolsets that the client were using were configured 'out of the box' without any customisation or line of site that linked the products together. **With these tools not being activity monitored or reviewed, this left alerts open for weeks** as there was not a central or over-arching security authority managing these alerts.

Project Overview

CoreAzure, supported by Methods, was chosen as the domain expert supplier to deliver the cyber security and Microsoft consultancy programme. The project kicked off with an analysis of the client's existing Microsoft technology estate against the perceived cyber security risk posture to:



Provide the client with a view of the current landscape



Provide a roadmap of activities to address their current security risks by utilising the Microsoft product set

When applied appropriately, Microsoft 365 and Azure enterprise threat protection products share security signals and correlate alerts across all products into an attack timeline, and automate many aspects of the investigation and remediation processes.

Results

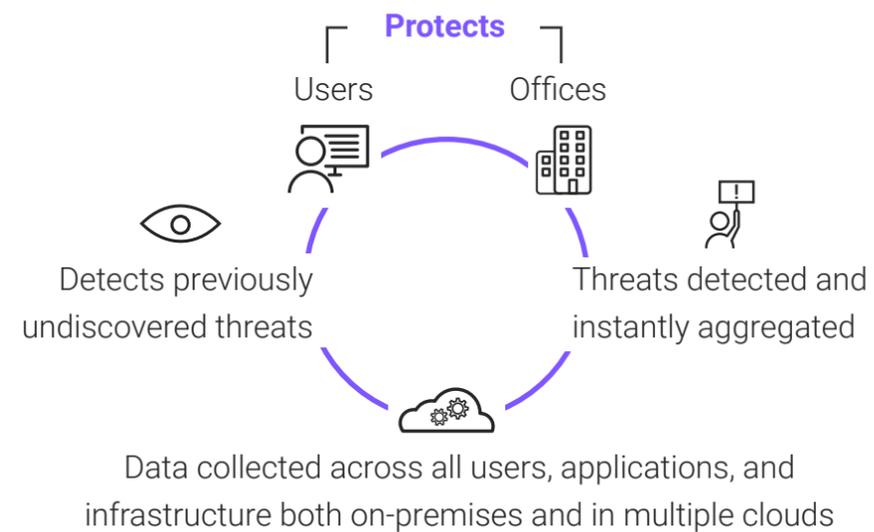
The programme used operational workflows to deliver security orchestration and remediation (SOAR) capabilities. This allowed a sequence of tasks to be executed without human intervention, using Machine Learning to streamline incident response processes by automating time-consuming, manual tasks whilst eliminating gaps inherent with standalone solutions, in the most demanding IT environments. As a result, the client's teams are free to focus on more complex and interesting security challenges.

Working through the roadmap, we implemented a fully configured environment capable of monitoring and reacting to threats and breaches from outside, reducing the residual risk to the organisation. Through capitalising on opportunities to optimise the environment, our client was able to maximise and streamline the usage of their Microsoft licencing estate.

Next Steps

Today we continue to analyse the client's technology estate against perceived cyber security risk posture. Once our first iteration of work was complete, we went on to design the ingestion of the Next Generation Firewall platforms and distributed web gateways.

Embracing a direct to-cloud security stack



We provide the client with a holistic view of their current threat landscape to address their current security risks by continually expanding upon and harnessing the full extent of the Microsoft Enterprise Security and Mobility suite they have invested in.

The enterprise threat protection products we have implemented share complex security signals and correlate alerts across all products into an attack timeline and automate many aspects of the investigation and remediation processes.

In addition, we are embarking on the next phase of implementation of a fully consolidated, unified cloud-based monitoring solution, combining and maximising system availability, performance and security event information across the client's entire hybrid IT estate.

About CoreAzure

CoreAzure is a leading Microsoft Cloud specialist and an established Microsoft UK Gold Partner providing cutting edge technical consulting, architecture and design, build, migration and support services to help organisations maximise their investment in Microsoft technologies.

You can find out further information on our cyber security offering, as well as how we can develop and implement a pragmatic and proportionate Remediation Assignment Plan in a matter of days, at methods.co.uk/what-we-do/cyber-security



methods  CoreAzure



London | Birmingham | Bristol | Cardiff | Chelmsford | Edinburgh | Manchester | Sheffield

 Info@methods.co.uk

 020 7240 1121

 www.methods.co.uk