oneAdvanced

CASE STUDY

Strengthening cybersecurity and delivering long-term savings for a major UK financial organisation

Industry

Financial Services

Project

Managed Cybersecurity Services

Introduction

For over a decade, we've had the privilege of partnering with a prominent UK financial services organisation, responsible for managing multi-billion pounds of assets. Our long-standing collaboration has enabled us to deliver a comprehensive range of managed services, including Service Desk, Asset Management, and Technical Service Engineers, providing reliable, high-quality support across their operations. As part of this partnership, we've also implemented managed cybersecurity services, working together to enhance their security posture, protect sensitive member data, and ensure uninterrupted service.

The Challenge

As a major financial services organisation, our customer is responsible for protecting customer data and maintaining service continuity. Managing such significant financial assets, they understand that a security breach could result in serious monetary and reputational damage, as well as significant consequences for its customers if they are unable to access the service.

The organisation recognised the need for a specialist partner to help navigate the dynamic nature of modern cyber risks. They required a robust, 24/7 security solution that could not only defend against current threats but also adapt to future challenges, ensuring their security posture remained strong and resilient.

The Solution

Building on our long-standing partnership, we developed a multi-faceted security strategy tailored to the customer's specific needs.

OUR APPROACH INCLUDED:

Managed Detection and Response (MDR): We implemented a comprehensive MDR solution providing 24/7, round-the-clock monitoring and response from our UK based Security Operations Centre (SOC). This proactive service ensures that potential threats are identified and neutralised immediately, minimising risk and providing the customer with complete peace of mind.

Consulting Information Security Manager (ISM): To provide strategic oversight, expert guidance, and security assurance, we introduced a dedicated ISM. The ISM acts as a focal point for all information security matters, engaging with OneAdvanced stakeholders and the customer's senior management, including their Board of Trustees. Key responsibilities include regular threat and risk reporting, guidance on emergent threats, vulnerability management, making corrective action plans, and chairing the monthly Security and Risk Board meeting.

Migration to Microsoft Sentinel: As part of our commitment to platform modernisation, we successfully migrated the customer from legacy tooling to a centralised Microsoft Sentinel deployment. We engineered this solution to a Gold-Standard architecture, utilising the proven Microsoft MSSP Tech Playbook for scalable, cross-tenant security management. This strategic move delivers advanced threat visibility and leverages the full depth of the integrated Microsoft Security Ecosystem. Crucially, we leveraged Azure Lighthouse to enable secure, delegated management, ensuring the customer retains full sovereign control and data autonomy within their tenant while meeting all UK regulatory and compliance requirements.

Continuous Service Improvement: We enhanced the customer's vulnerability management processes by implementing Armour Code to help coordinate various security tools. Furthermore, we managed the transition from their legacy antivirus to Microsoft Defender for Endpoint, further strengthening the Sentinel ecosystem and creating a more unified and effective security environment.

The Results

The implementation of this modernised security strategy has delivered significant and measurable benefits, strengthening the customer's defences and providing clear value.

KEY OUTCOMES INCLUDE:

Proactive Threat Detection and Immediate Response: The 24/7 MDR service ensures that potential threats are identified and contained rapidly, minimising risk and preventing incidents from escalating. This proactive approach significantly reduces the likelihood of disruption and supports uninterrupted service for customers.

Significant Cost Reduction: The strategic move to Microsoft Sentinel resulted in a 32% cost reduction over the 3 year term , optimising the customer's investment in cybersecurity whilst improving defences.

Strengthened Security Posture: The integrated solution, combining MDR, Sentinel, and Defender, provides a powerful and cohesive defence against advanced threats. This prevents downtime and ensures customers receive a seamless, uninterrupted service.

Compliance with Data Residency Protocols: The core security architecture was specifically engineered to uphold strict data residency protocols. By design, all security telemetry, log data, and operational artifacts are confined to the geographical boundaries explicitly chosen by the customer within their own Azure subscription settings. This deliberate configuration ensures the customer maintains complete sovereign ownership of their threat intelligence data and achieves full compliance with all relevant regulatory obligations.

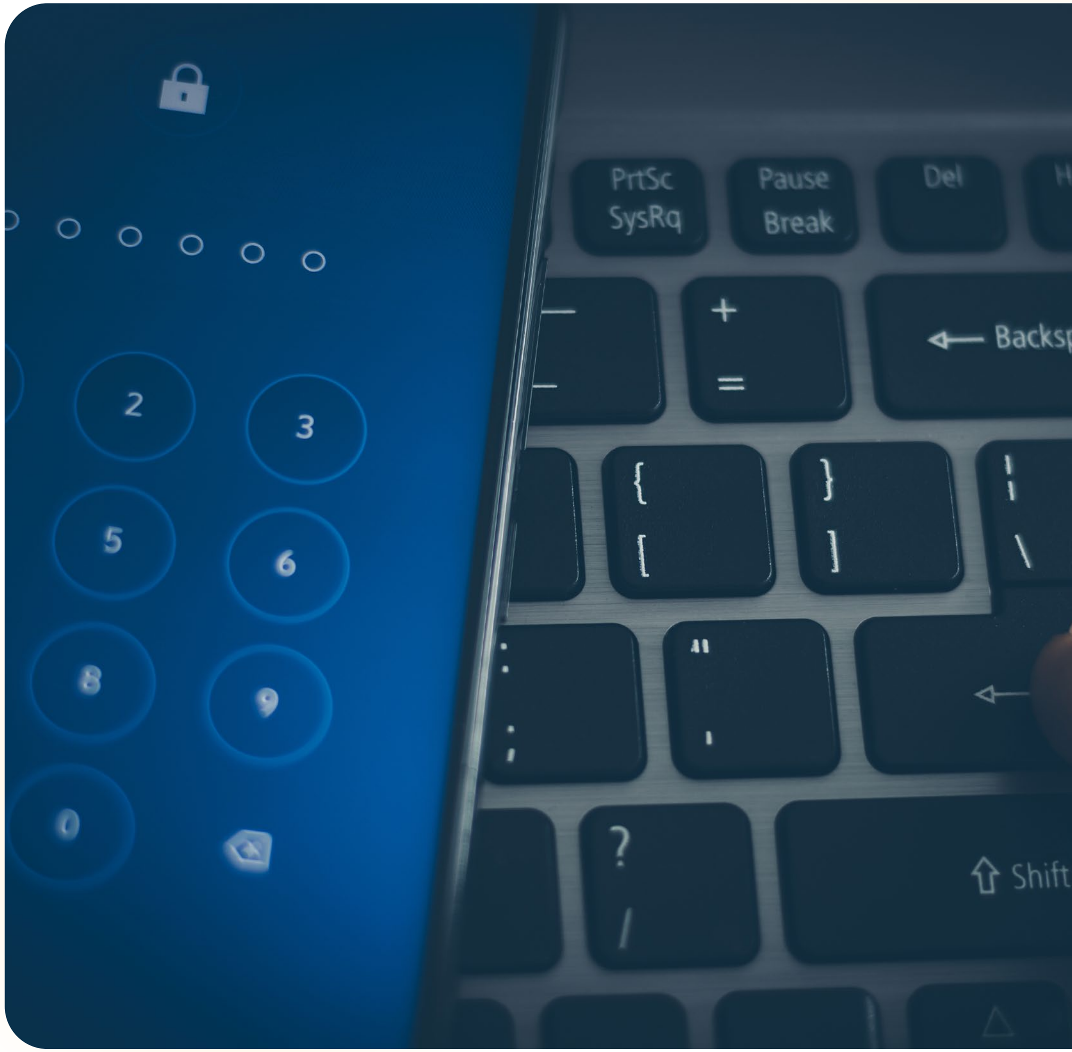
Crucially, this architecture does not impede security operations. Our SOC maintains continuous, highly secure access to manage the environment and perform threat hunting via Azure Lighthouse. This model utilises secure, delegated resource management, allowing our analysts to operate within our customer's tenant without ever moving or storing their sensitive data outside of defined sovereign boundaries.

Enhanced Peace of Mind: With continuous MDR monitoring and a dedicated Information Security Manager, the customer's leadership team can be confident that their organisation and its members are protected around the clock.

"Our long-standing partnership with this organisation has been instrumental in delivering a robust cybersecurity strategy that not only protects their customers' sensitive data but also ensures the continuity of their critical services. By leveraging our expertise in managed detection and response, strategic security guidance, and modernised security platforms, we've significantly strengthened their security posture while achieving substantial cost savings. This collaborative approach has given them the peace of mind that comes with knowing their organisation is secure, resilient, and well-prepared for the evolving cyber threat landscape."

**Matthew Cracknell, Head of Security Operations,
OneAdvanced IT Services.**

Our partnership continues to evolve, with ongoing improvements and enhancements being made not only to their cybersecurity services but to all the managed services we provide. This collaborative approach ensures the organisation remains secure, resilient, and prepared for the future.



oneAdvanced

Powering the world of work

OneAdvanced IT Services is an award-winning managed service provider, delivering innovative, secure, and scalable solutions with export support, tailored to organisations' unique challenges. Our end-to-end IT services are designed to enhance productivity, optimise costs, and support critical infrastructures, all while ensuring compliance and security. Backed by a commitment to continuous improvement, we deliver purpose-driven solutions that create meaningful results for the sectors and communities we serve.

Get in touch

☎ +44(0) 330 343 4000 www.oneadvanced.com ✉ hello@oneadvanced.com