CyberProof®
A UST Company

CASE STUDY:

Managed XDR services for a large banking organization

INDUSTRY: BFSI

cyberproof.com

Client background

The client, a subsidiary of a large corporation, offers credit-building credit cards to clients with a limited or uneven credit history.

Client challenge

The strategic goal of the client was to effectively detect advanced attacks such as ransomware and significantly decrease risk. The client decided to leverage the capabilities offered by Microsoft technologies to move away from a traditional perimeter-based approach – and adopt a Zero Trust approach. Their goal was to make risk-based, context-driven decisions rooted in Identity, Device, App, Infrastructure, Network and Data. They also wanted to work in a hybrid model to extend their security operations team using a managed security services provider to operate and manage the tools they required to deliver these capabilities.

The client initially had been considering various point products but changed direction with CyberProof and Microsoft support, because they were interested in having a single security vendor support the Extended Detection & Response (XDR) capability that they wanted to deploy.

Benefits

- 90% increase in visibility into threats, vulnerabilities, and environments – improving the customer's ransomware resiliency
- Custom reporting using Microsoft tools, so insights into security posture can be shared with senior leadership
- 50% reduction in day-to-day SOC operational costs; including optimizing SOC team activities
- 30–40% reduction in engineering staff (due to the elimination of legacy infrastructure)
- 20-30% optimization of infrastructure and cloud consumption, as newly deployed cloud solutions are SaaS - reducing costs
- Consolidation of IT productions

Our solution

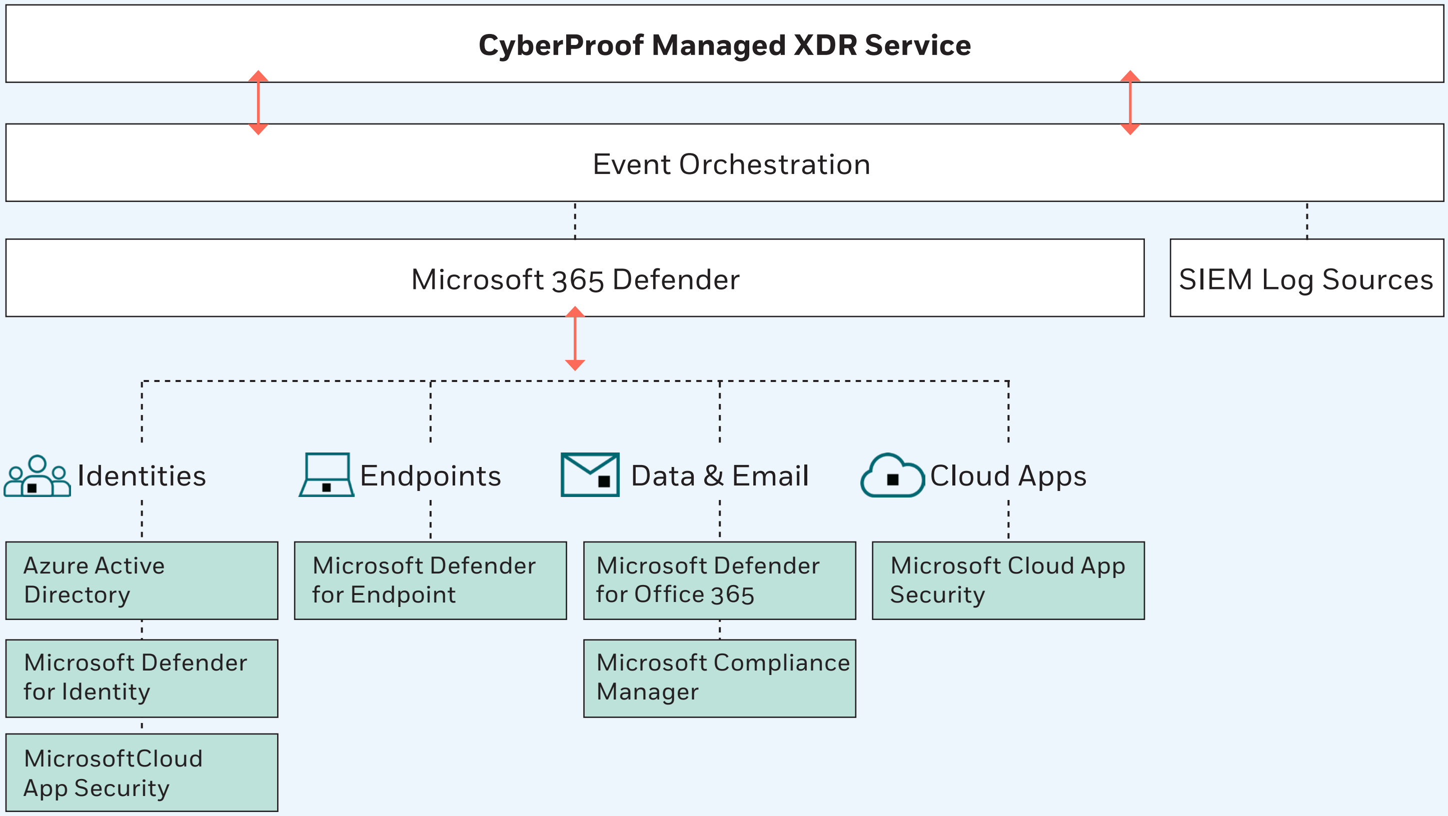
CyberProof worked together with Microsoft to provision and deploy the Microsoft XDR capability and integrate it with the customer's current Managed Detection & Response (MDR) service with CyberProof. This was done by leveraging the CyberProof Defense Center (CDC) platform, which supports collaborative, real-time security operations for all stakeholders through orchestration and smart automation including: alert enrichment, incident prioritization, playbook-led responses, and seamless chatops communication.

CyberProof supported the client throughout the transition, including the implementation and operational phases. Working together with Microsoft, CyberProof built a new cloud-native architecture integrating the Microsoft security stack – while consolidating the existing tech stack and gaining significant cost efficiencies.

CyberProof's XDR deployment for the client and ongoing service integration with the MDR solution is fully scalable and provides continuous improvement:

- The CDC provides a "single pane of glass" collaboration platform that allows the client and CyberProof cyber professionals to accelerate incident detection and response utilizing the Microsoft XDR security stack.
- CyberProof leverages Infrastructure as Code (IaaC) for onboarding services, dramatically reducing the transition time from legacy to next-gen SOC, automating up to 95% of onboarding tasks by treating the configuration and set-up as code. Once a template is developed, it can be re-used for repetitive tasks - thereby introducing great efficiencies.

MICROSOFT DEFENDER TO COVER FULL STACK SECURITY


CyberProof Managed XDR Service
Event Orchestration
Microsoft 365 Defender
SIEM Log Sources
Identities
Endpoints
Data & Email
Cloud Apps
Azure Active Directory
Microsoft Defender for Identity
MicrosoftCloud App Security
Microsoft Defender for Endpoint
Microsoft Defender for Office 365
Microsoft Compliance Manager
Microsoft Cloud App Security

CyberProof®
A UST Company

About CyberProof

CyberProof, a UST company, helps our clients transform their security to a cost-effective, cloud-native technology architecture. Our next-generation Managed Detection & Response (MDR) service is built to support large, complex enterprises by combining expert human and virtual analysts. Our services are enabled by our purpose-built platform, the CyberProof Defense Center – enabling us to be more agile, collaborate better, and deliver powerful analytics. Our integrated security services include Threat Intelligence, Threat Hunting, and Vulnerability Management. Our experts innovate to meet our clients' needs with custom use cases, integrations, and automations. For more information, visit www.cyberproof.com.

Barcelona | California | London | Singapore | Tel Aviv | Trivandrum

cyberproof.com