

CASE STUDY:

Banking leader
achieves 90% greater
threat visibility and
50% lower SOC costs

INDUSTRY: BFSI

About the client

The client is a financial services organization that provides credit solutions to customers seeking to build or improve their credit history. As a subsidiary of a major financial group, the company operates within a highly regulated environment, managing sensitive customer and transactional data across cloud and on-premises systems. With operations supporting millions of accounts, the organization plays a critical role in providing accessible financial products while maintaining the highest standards of trust and compliance.

The client's challenge

The client's strategic goal was to reduce exposure across its hybrid environment while enhancing detection and response to advanced threats such as ransomware and credential-based attacks. Despite significant investment in traditional perimeter defenses, visibility across cloud, endpoint, and identity systems remained fragmented, leaving potential blind spots that could be exploited by threat actors.

To address these risks, the organization set out to implement a Zero Trust architecture and Extended Detection and Response (XDR) capability built on Microsoft's security technologies. This required consolidating legacy point solutions, integrating detection and response across identity, device, app, infrastructure, data, and network layers, and adopting a risk-based, contextual approach to security operations.

The company also sought to extend its security team through a co-sourced managed services model, maintaining in-house oversight while leveraging CyberProof's expertise for 24x7 monitoring, use case engineering, and automation. The objective was to create a unified and threat-led operational framework capable of continuously validating defenses, minimizing exposure windows, and improving operational efficiency.

Benefits



90% improvement in visibility:

Unified monitoring across Microsoft XDR and MDR environments provided end-to-end insight into threats, vulnerabilities, and attack surfaces, significantly enhancing ransomware resilience.



50% reduction in SOC operational costs:

Automation, playbook integration, and IaC-based deployment reduced manual workloads and optimized SOC team efficiency.



30-40% optimization in engineering capacity:

Retiring legacy infrastructure and consolidating technologies eliminated redundant workloads and freed staff to focus on higher-value security engineering.



Stronger control and collaboration:

Real-time dashboards, executive reporting, and a transparent co-sourced model enabled better risk-based decision-making and measurable exposure reduction.



The client's challenge

CyberProof partnered with the client and Microsoft to design and deploy a threat-led Extended Detection and Response (XDR) capability tightly integrated with the client's existing Managed Detection and Response (MDR) service. The initiative focused on improving visibility across the hybrid cloud environment, reducing exposure, and ensuring rapid response to ransomware and credential-based attacks.

Working collaboratively with Microsoft, CyberProof provisioned and operationalized a cloud-native architecture using the full Microsoft security stack – including Defender, Sentinel, and Purview – supported by CyberProof's service delivery platform. This unified operations model provided a single, transparent view of threats across identity, endpoint, application, network, and data layers, improving detection accuracy and accelerating containment.

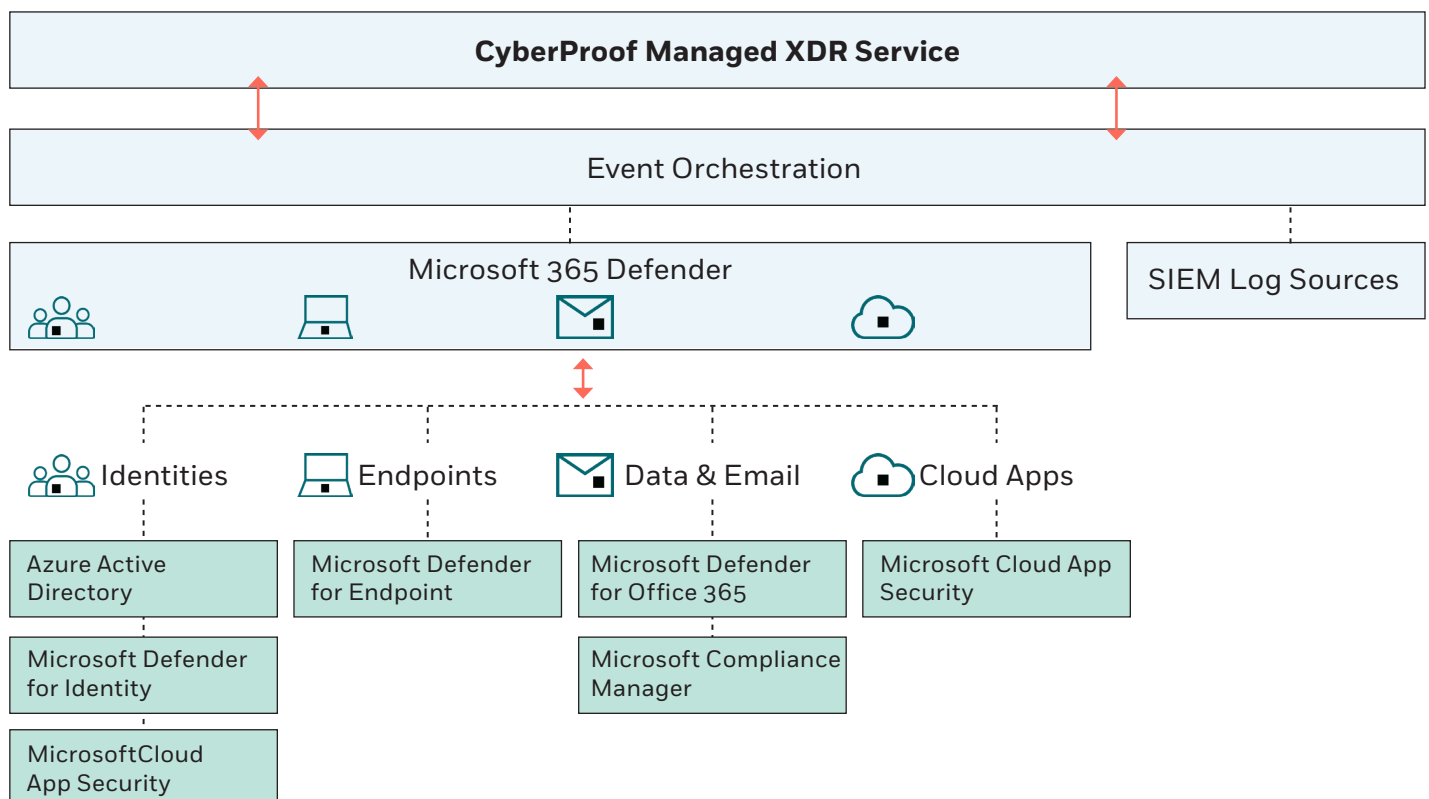
The service delivery platform delivered real-time collaboration and automation, using playbook-led response, enrichment, and orchestration to streamline

analyst workflows. Integrated ChatOps functionality enabled seamless communication between the client's SOC and CyberProof's global operations teams, while custom dashboards provided executive-level visibility into security posture and ongoing exposure reduction.

To ensure efficient onboarding and scalability, CyberProof employed Infrastructure as Code (IaC) methodologies, automating up to 95% of the transition from legacy systems to the next-generation SOC. This automation dramatically reduced deployment time, minimized configuration errors, and provided reusable templates to support continuous improvement.

Finally, the program was structured as a co-sourced operating model, enabling the client's internal team to retain control over strategic functions while leveraging CyberProof's 24x7 monitoring, threat intelligence, and detection engineering expertise. The result was a modern, cost-optimized, and continuously improving cyber defense ecosystem aligned to the organization's risk and regulatory priorities

MICROSOFT DEFENDER TO COVER FULL STACK SECURITY



About CyberProof

CyberProof, a UST company, delivers better security operations and drives superior experiences for enterprise customers. Our cloud-first, AI-powered approach to security delivers industry-leading services to drive real business results. We believe that working closely with our customers and partners through a 'better security, together' services model jointly empowers us to defend against the greatest of threats. See: www.cyberproof.com.

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