BLACK BOX

CASE STUDY
CYBERSECURITY

How a Digital Financial Services Organisation Strengthened Cyber Resilience with XDR-Led Security Operations

Overview

A fast-growing digital financial services organization with an NBFC lending arm needed to strengthen cybersecurity operations as its endpoint, cloud, SaaS, identity, and data environments expanded. Existing security controls were present across multiple domains, but operated with limited integration, creating gaps in visibility, governance, and response coordination.

As the organization scaled digital lending operations, regulatory expectations under the DPDP Act, 2023 and the need for stronger cyber resilience became increasingly important. Black Box led a cybersecurity modernization programme centered on Trend Micro XDR, integrating endpoint, cloud, email, and data security capabilities into a connected operating model while maintaining business continuity.

Challenges

The organization's security environment included a mix of legacy and modern controls across endpoint, network, cloud, identity, and data domains. However, these tools were largely fragmented, requiring teams to review alerts and activity across multiple platforms. Limited centralized visibility slowed investigation, increased manual effort, and made it difficult to prioritize risks across distributed environments.

As digital adoption increased, the organization also needed stronger data governance, better oversight of cloud and SaaS activity, and improved alignment with regulatory requirements. The expanding estate highlighted the need for a more integrated, intelligence-driven security operations model.

AT A GLANCE

CHALLENGES

- Fragmented security across hybrid IT environments
- Limited visibility across distributed IT environments
- Manual investigations slowed incident response
- DPDP Act, 2023 compliance required stronger cyber governance

SOLUTIONS

- Trend Micro XDR enabled unified threat detection
- Integrated endpoint, cloud, email, and data security
- DLP strengthened sensitive data protection
- 24×7 SOC enabled continuous threat monitoring

RESULTS

- Unified XDR transformed security operations
- Endpoint coverage scaled from 50 to 1,200+ systems
- Correlated visibility improved threat investigations
- Stronger data governance and DPDP Act readiness

BENEFITS

- Reduced manual effort in security operations
- Improved visibility across hybrid IT environments
- Strengthened cyber resilience for digital growth
- Built a secure foundation for evolving compliance

Solutions

Black Box applied an integration-led, phased, and risk-based approach to modernize the organization's cybersecurity operations. Trend Micro XDR was implemented to correlate telemetry across endpoint, cloud, email, and data environments, enabling consolidated detection, investigation, and response workflows.

The solution connected endpoint protection, cloud and email security, data security, and DLP capabilities into a unified framework. Deployment followed a structured model covering discovery, solution design, proof of concept, implementation, optimization, knowledge transfer, and go-live support. Black Box also supported operationalization through its CERT-In empanelled 24×7 SOC capabilities, helping the client sustain continuous monitoring and response readiness.

Result

The implementation moved the organization from disconnected security controls to a coordinated XDR-driven operating model. Security teams gained correlated visibility across endpoint, cloud, email, and data environments, reducing investigation complexity and improving response effectiveness.

Endpoint coverage expanded from an initial deployment of approximately 50 systems to more than 1,200 endpoints, demonstrating the scalability of the architecture. Structured workflows reduced manual coordination, while data security and DLP capabilities strengthened oversight of sensitive information. The programme improved operational resilience, regulatory readiness, and cybersecurity alignment with the organization's digital growth priorities.

Why Black Box?

Black Box helped the organisation modernise its security operations through an integrated, XDR-led approach that unified visibility across endpoint, cloud, email, and data environments. Combining cybersecurity consulting, seamless technology integration, and CERT-In empanelled 24×7 SOC services, Black Box delivered a scalable security operating model that strengthened cyber resilience, improved governance, and supported the organisation's continued digital growth.

Black Box is a global leader in digital infrastructure solutions, delivering network and system integration, managed services, and technology products to Fortune 100 and top global enterprises. With a presence across the United States, Europe, India, Asia Pacific, the Middle East, and Latin America, Black Box serves businesses across financial services, technology, healthcare, retail, public services, and manufacturing.