BLACK BOX®

CASE STUDY
CYBERSECURITY

Strengthening Cyber Resilience Through Integrated Cybersecurity and IT Operations Modernization for India's Major Municipal Corporation

Overview

One of India's leading municipal corporations embarked on a strategic cybersecurity and IT operations modernization initiative to strengthen cyber resilience across its critical digital infrastructure. Supporting essential citizen services across multiple offices and a workforce of nearly 2 lakh employees, the organization required a unified security framework to improve visibility, governance, threat detection, and operational control across a highly distributed IT environment.

With 20,000+ IT assets and endpoints, the infrastructure demanded integrated cybersecurity capabilities, structured rollout governance, and sustained operational support. Black Box was selected to design, deploy, integrate, and support a comprehensive cybersecurity program while minimizing disruption to municipal operations.

Challenges

Managing cybersecurity across one of India's largest municipal IT environments posed major operational and technical challenges. Over time, security controls had evolved into multiple standalone tools, creating fragmented visibility and inconsistent processes across endpoints, applications, identities, and networks.

The organization aimed to build a unified security framework to improve monitoring, strengthen access controls, streamline vulnerability and patch management, enhance asset visibility, and meet evolving compliance needs.

Execution required coordination across departments and partners while addressing legacy systems, integration gaps, endpoint compatibility, and network readiness.

AT A GLANCE

CHALLENGES

- Limited visibility across users, endpoints, and assets
- Siloed security tools across the IT environment
- Manual patching and asset management processes
- Complex rollout across 200 distributed locations

SOLUTIONS

- Strategic cybersecurity partner across full lifecycle
- Integrated security across identity, network, endpoints
- Hybrid cloud, SaaS, and on-premises architecture
- Phased deployment with governance and support

RESULTS

- Strict six-month rollout delivered in two planned phases
- Visibility enabled across 20,000+ IT assets
- Monitoring strengthened across 20,000+ endpoints
- Patch deployment advanced across 25,000+ endpoints

BENEFITS

- Improved visibility across the security landscape
- Stronger identity, endpoint, and network security
- Enhanced governance and compliance readiness
- Scalable foundation for future digital services

Solutions

Black Box acted as a strategic cybersecurity partner, supporting the engagement from requirement definition and solution architecture to deployment, integration, transition, and ongoing support.

The engagement integrated multiple security capabilities across endpoint protection, network access control, identity and privileged access management, vulnerability assessment, patching, IT asset management, application monitoring, packet capture, directory services, and data protection.

Built on a hybrid architecture combining cloud, SaaS, and on-premises technologies, the solution integrated with existing systems while enabling centralized visibility across users, devices, applications, and critical IT assets.

A phased implementation covered discovery, design, readiness, deployment, testing, user acceptance, documentation, knowledge transfer, and rollout, supported by strong project governance.

Results

The phased implementation was delivered through two planned phases within a strict six-month timeline, strengthening cybersecurity visibility, governance, and operational resilience across a large municipal IT ecosystem.

Black Box enabled centralized visibility across 20,000+ IT assets and strengthened monitoring across 20,000+ endpoints, improving oversight, control, and faster issue detection. Patch deployment was advanced across 25,000+ endpoints, improving compliance readiness and reducing vulnerability exposure.

With a dedicated support team deployed for security operations, the organization gained sustained operational support to manage security tools, improve response coordination, and support ongoing cyber resilience.

Why Black Box?

Black Box delivered a large-scale cybersecurity program by combining consulting, systems integration, governance, and managed services. Using proven methods and close collaboration with technology partners, it unified diverse security tools into a cohesive ecosystem while minimizing disruption. The engagement highlights Black Box's ability to execute complex cybersecurity transformations for public-sector organizations with distributed infrastructure and critical digital services.

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.