



# Discover How a Major U.S. Airport Strengthened Its Cybersecurity Posture for Enhanced Visibility and Resilience

## Overview

As one of the busiest international airports in the United States, this aviation leader plays a vital role in domestic and global air travel. With four runways and three major terminals, the airport supports millions of passengers each year and serves as a key hub for American Airlines as well as numerous global carriers. However, rapid digitalization brought new cybersecurity risks. The airport's newly established IT infrastructure lacked real-time visibility, making it vulnerable to advanced threats and undetected vulnerabilities.

To build a more resilient and proactive security environment, the airport turned to Black Box. By implementing a robust cybersecurity architecture, including extended detection and response (XDR), round-the-clock monitoring, and VMaaS, Black Box helped transform fragmented security operations into a unified, intelligent defense framework tailored to aviation demands.

## Challenges

The airport was undergoing a digital transformation to modernize operations, enhance passenger experience, and support critical services. However, the new environment introduced complex cybersecurity challenges. The IT infrastructure lacked continuous monitoring and advanced threat detection capabilities, which increased the risk of sophisticated cyberattacks.

Additionally, there were no centralized mechanisms to assess, prioritize, or remediate vulnerabilities, leaving essential systems exposed. The customer needed a solution that could not only monitor threats in real time but also provide proactive advisories and reduce the incident response time. Without a unified strategy, maintaining resilience across such a vast and sensitive environment was becoming increasingly difficult.

## AT A GLANCE

### CHALLENGES

- Gaps in real-time threat visibility due to evolving digital infrastructure
- No centralized security monitoring or rapid incident response capabilities
- Limited vulnerability insight exposing critical systems to risk
- Lack of a scalable cybersecurity framework for airport-wide protection

### SOLUTIONS

- Implementation of a Splunk-based XDR platform for intelligent threat detection
- 24x7 monitoring and management delivered through the Black Box SOC in Plano, Texas
- Deployment of Vulnerability Management-as-a-Service (VMaaS) for comprehensive visibility
- Integration of threat intelligence for early detection and rapid response

### RESULTS

- Unified and strengthened cybersecurity posture across airport systems
- Reduced mean time to detect and respond to threats
- Increased visibility into vulnerabilities and improved patch prioritization
- Enhanced operational resilience with proactive risk mitigation strategies

### BENEFITS

- Always-on cybersecurity monitoring and faster response times
- Improved protection of mission-critical airport infrastructure
- Proactive threat management and lower attack surface
- Scalable and future-ready security foundation for continued digital expansion



## Solutions

To address these critical challenges, the airport partnered with Black Box to implement a comprehensive cybersecurity solution. At the core was a next-generation, Splunk-based XDR platform that delivered intelligent threat detection, incident correlation, and automated responses. All monitoring and management services were delivered via the Black Box Security Operations Center (SOC) in Plano, Texas, ensuring expert support and 24x7 coverage. In parallel, Black Box deployed a Vulnerability Management-as-a-Service (VMaaS) platform, enabling full visibility across the airport's digital infrastructure, allowing the team to proactively detect, assess, and resolve vulnerabilities.

By combining advanced technology with real-time threat intelligence and continuous oversight, Black Box created a cohesive and scalable cybersecurity posture aligned with the operational needs of a major airport.

## Why Black Box?

This transformation highlights why global enterprises, especially those in critical infrastructure sectors, choose Black Box as their cybersecurity partner. Black Box brings together best-in-class security platforms, 24x7 managed services, and deep domain expertise to build intelligent, scalable, and high-performance defenses.

For this international airport, Black Box delivered more than technology; they provided strategic assurance, operational reliability, and a proactive cybersecurity ecosystem. With a clear focus on outcomes, industry best practices, and long-term readiness, Black Box continues to empower organizations to lead securely in an increasingly digital and threat-prone world.

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.

## Results

The solution delivered immediate improvements across the airport's cybersecurity environment. Threat detection was significantly strengthened through the implementation of XDR services, providing broader visibility and faster response. The addition of vulnerability management capabilities allowed the team to detect and address security gaps with greater accuracy. Continuous threat advisories helped the organization stay ahead of risks, while integrated threat intelligence optimized detection workflows. With 24x7 monitoring and expert analysis, incident response times were reduced, and overall resilience across systems was enhanced.