BLACK BOX

CASE STUDY
AIRPORTS

Strengthening Global VoIP Security for a Leading International Airline

Overview

The airline is a long-standing premium customer operating across 50+ international destinations, relying on a sophisticated VoIP ecosystem for reservations, customer support, and remote staff connectivity. High call volumes and a geographically dispersed workforce made uninterrupted, secure voice infrastructure critical. As global traffic grew, VoIP threats escalated. Attackers targeted weak extensions, attempted credential theft, and exploited the IVR for fraudulent premium-rate callbacks, putting finances, operations, and customer trust at risk.

Black Box, the airline's trusted telecom partner, collaborated with Assertion to deliver a swift, targeted response.

Challenges

The airline's environment revealed multiple vulnerabilities that cybercriminals quickly exploited. Internet-facing SBCs supporting remote workforces were attacked within minutes of going live. In one month alone, attackers attempted millions of SIP registrations to locate valid extensions, with over fifty targeted through brute-force attempts, increasing the risk of takeover and disruption.

In early 2022, unauthorized access to the IVR platform enabled a premium-rate call-back scam, inflating international charges before detection. At the airline's global scale, such anomalies could easily go unnoticed. These incidents highlighted major security gaps. The airline needed real-time threat tracking, toll-fraud detection, and stronger protection for remote agents - capabilities that manual monitoring and periodic audits could not provide.

AT A GLANCE

CHALLENGES

- Persistent VoIP attacks across its remote-worker network
- Nearly 5.6 million hostile registration attempts targeting remote extensions
- Over 50 extensions subjected to active brute-force attempts
- A large toll-fraud incident where attackers exploited the IVR system
- High operational risk due to distributed call centers, remote agents, and internet-facing SBCs

SOLUTIONS

- Rapid deployment of a cloud-based Proof of Concept using Assertion® SecureVoice™
- Real-time analysis of SIP messages and calls to detect extension harvesting, spoofing attempts, and toll fraud
- Automated collection of threat intelligence, identification of malicious IP churn, and continuous call monitoring
- SBC telemetry to uncover suspicious call patterns and ongoing attacks

RESULTS

- Full visibility into past and ongoing attacks, enabling immediate containment
- Prevention of toll-fraud losses and reduced exposure to IVR callback scams
- Restoration of customer trust after repeated VoIP breaches
- Successful PoC leading to a formal procurement request within two months
- Renewed long-term engagement with the airline and stronger VoIP security offerings

BENEFITS

- 24x7 monitoring and real-time detection across all remote-worker VoIP channels
- Protection against extension takeover, eavesdropping, and data exfiltration
- Verified calling to reduce identity theft and improve call answer rates
- Policy-driven mitigation that preserves uptime and business continuity
- A reusable VoIP security model for other enterprises with similar risks

Solutions

Black Box saw the situation as an opportunity to rebuild confidence and introduce a more resilient voice-security model. Working with Assertion, the team deployed a no-obligation 30-day Proof of Concept for Assertion® SecureVoice™. The cloud-based model allowed near-instant activation without altering the airline's core systems.

SecureVoice™ examined every SIP message and phone call in real time, identifying active attacks, spoofing attempts, and suspicious calling routines. It collected actionable threat intelligence and established clear evidence of hostile activity. The platform also worked closely with the airline's SBC footprint to uncover malicious patterns that had previously gone undetected.

This approach gave the airline round-the-clock visibility into its VoIP traffic for the first time. It showed how toll-fraud attempts, remote-extension probing, and credential-harvesting campaigns unfolded at each stage. Assertion provided hands-on support throughout the PoC, customizing thresholds, tuning detections, and offering insight into attacker behavior.

The results were immediate and convincing. Within two months, the airline moved forward with a formal procurement process, marking a rare outcome for a government-linked organization.

Results

The strengthened monitoring structure drastically reduced the airline's exposure to VoIP threats. SecureVoice™ blocked ongoing extension attacks, flagged suspicious call origins, and prevented further toll-fraud activity. IVR call-back risks were contained, and operational teams gained the clarity required to act quickly on emerging issues.

The PoC also helped restore faith in Black Box's ability to safeguard the airline's communication infrastructure. The renewed partnership set the foundation for a long-term security roadmap, positioning Black Box as a leading advisor on voice-security strategy.

Why Black Box?

Black Box offered deep industry experience, a strong local presence, and the ability to respond decisively during a high-pressure situation. Our partnership with Assertion combined telecom expertise with advanced real-time VoIP security analytics.

The airline benefited from a single accountable technical partner who delivered a fast PoC rollout, provided clear visibility into ongoing threats, enabled rapid mitigation of live attacks, and established a scalable defense model. This collaboration reaffirmed our role as a trusted provider capable of safeguarding mission-critical communications in complex and globally distributed environments.

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.