Zero Trust OT Cybersecurity Protection for Airports

Modern airports are complex ecosystems, integrating a vast array of interconnected systems that manage everything from air traffic control and baggage handling to passenger services and facility operations. The consequences of a successful cyberattack on an airport can range from significant operational disruptions and financial losses to severe safety risks and a profound impact on national security.

Airports face unique and escalating cybersecurity challenges due to their critical role in commerce, travel, and defense, and traditional IT solutions cannot protect the OT systems adequately:

Converged IT/OT Environments: The integration of IT systems (e.g., ticketing, administrative networks) with OT systems (e.g., air traffic management, runway lighting, HVAC, fuel systems, baggage handling) creates complex interdependencies and expands the attack surface. A breach in one domain can quickly impact the other, leading to widespread operational failures.

Legacy Systems and Proprietary Protocols: Many critical airport OT systems rely on aging infrastructure and proprietary protocols not designed with cybersecurity in mind. These systems often lack native security features, are difficult to patch, and can introduce significant vulnerabilities.

Extensive Third-Party Access: Airports frequently grant remote access to a multitude of third-party vendors, contractors, and service providers for maintenance, updates, and specialized services.

Insider Threats: Both malicious and accidental insider actions pose a significant risk. Employees, contractors, or even compromised credentials can lead to unauthorized access, data exfiltration, or operational sabotage.

These challenges underscore the urgent need for a robust, adaptive security solution that can protect airport operations from evolving cyber threats.

Figure 1 Airport OT Network

BlastShield™

Secure Remote Operations: Enables secure remote monitoring and control of airport operations, improving efficiency without compromising security.

Protection of Legacy Systems: Provides a "virtual air gap" for vulnerable legacy equipment that cannot be easily updated, mitigating the risk of exploitation.

Protection Against Advanced Threats: Network cloaking and passwordless MFA effectively counter sophisticated AI-driven reconnaissance and phishing.

Mitigation of Ransomware Attacks: Network segmentation and granular access control limit the spread of ransomware, minimizing disruption and data loss.

BlastShield™: Zero Trust OT Protection for Airports

BlastWave delivers a comprehensive Zero Trust security solution designed to address the unique complexities and vulnerabilities of airport OT environments. By implementing a "never trust, always verify" model, BlastWave makes hacking hopeless, ensuring the continuous availability, integrity, and safety of critical airport systems.

Network Cloaking:

BlastWave's core innovation is network cloaking, which creates a secure, invisible overlay network over your existing IT and OT infrastructure.

Problem Solved: Traditional networks are inherently visible, allowing attackers to easily scan for devices, open ports, and vulnerabilities. This reconnaissance is the first step in most cyberattacks.

How it Works: BlastWave leaves your existing network "as is" – no re-IPing or complex reconfigurations required. Instead, it creates a cryptographically enforced, secure overlay. All devices and services are assigned unique, internal overlay addresses that are hidden from the underlying "underlay" network. Only explicitly authorized and authenticated entities can even "see" these overlay addresses.

Airport Benefit: Imagine an attacker attempting to scan your airport's network. With BlastWave, they find nothing. No responses to pings, no visible ports, no discoverable devices. Your critical air traffic control systems, baggage handling networks, and facility controls become virtually undetectable to unauthorized eyes. This "virtual air gap" drastically shrinks your attack surface, eliminating the initial reconnaissance phase for adversaries and making it nearly impossible for them to map out your valuable assets.

Secure Remote Access

Remote access for vendors, technicians, and employees is essential for airport operations, but it's also a significant security risk, especially with traditional password-based methods.

Problem Solved: Passwords are a primary attack vector. They can be stolen, phished, or brute-forced, granting attackers easy entry into your network. Managing passwords for numerous third parties adds immense complexity and risk.

How it Works: BlastWave provides passwordless, cryptographically enforced secure remote access. Users and devices are authenticated based on trusted identities and policies, not shared secrets. Access is granted only after continuous verification of identity, device posture, and context.

Airport Benefit: Eliminate the burden and risk of passwords for all remote connections to your airport systems. Whether it's a maintenance contractor accessing a specific HVAC control system or an IT technician troubleshooting a server, their access is authenticated with robust, unphishable credentials. This significantly reduces the risk of compromised accounts, ensuring that only verified and authorized personnel can connect, and only to the specific resources they need.

Granular Microsegmentation

Once an attacker gains a foothold, their goal is often to move laterally across the network to reach high-value targets or spread malware. Flat networks enable this rapid propagation.

Problem Solved: Traditional networks often lack sufficient internal segmentation, allowing malware or compromised users to move freely once inside the perimeter. A breach in one system can quickly escalate into a widespread incident, impacting multiple critical airport functions.

How it Works: BlastWave enforces granular microsegmentation and strict policy enforcement within the secure overlay. Every device and every connection is explicitly authorized based on least privilege principles. If a piece of malware attempts to move from one compromised point to another unauthorized system, the connection is silently denied.

Airport Benefit: Contain threats at their source. If a single workstation or OT device becomes compromised, BlastWave's microsegmentation acts like a series of individual, air-gapped compartments. The malware is confined to that single segment, unable to spread laterally and wreak havoc across your entire airport network. This drastically limits the "blast radius" of any attack, protecting critical systems like air traffic control, baggage handling, and security infrastructure from cascading failures, ensuring operational resilience and safety.

The BlastWave Advantage for Airports

By combining network cloaking, secure remote access, and granular microsegmentation, BlastWave enables airports to achieve true digital independence. Make hacking hopeless.

v20260330

Prevent industrial cyberattacks, and ensure the world's critical infrastructure stays protected, productive, and profitable. Together we can build a resilient future for OT networks. Join the movement at **www.blastwave.com**

BlastWave
PREVENT
INDUSTRIAL
CYBERATTACKS