AIRPORTS UNDER WATCH

Airports sit at the nexus of public infrastructure and national security, making them prime targets for cyberattacks. From ransomware to politically driven disruptions, they face a dynamic and increasingly sophisticated threat environment that's as complex as the systems they rely on.

The airport industry's cybersecurity challenge

Airports occupy a unique crossroads where critical infrastructure, public transit, and international borders all converge, making them an attractive target for hackers. According to a study covering the period from 2000 to January 2024, there were 54 documented cyberattacks against the aviation sector, with nearly two-thirds (35) targeting airports directly, and the rest against individual airlines.[‡] The threat is growing: Thales reported a 600% year-over-year increase in cyberattacks targeting aviation in 2024.[‡]

600%

year-over-year increase in ransomware attacks in the aviation sector

A cyberattack on an airport can result in delays and disruptions, both physical and logistical. Attacks can grind baggage handling to a halt, disrupt air traffic control, and rattle public trust in the safety of flying. With airports increasingly dependent on digital systems to keep operations running smoothly, strong cybersecurity is essential. Data must be well protected, and critical infrastructure kept up and running for the millions of people who rely on it every day.

The growing digital surface area

Airports operate on a complex web of digital systems, ranging from customer-facing apps and automated baggage handling to biometric scanners and a growing network of Internet of Things (IoT) devices, all working together behind the scenes. These technologies help keep operations running smoothly, but they also widen the door for emerging cyberthreats.

This growing complexity has dramatically expanded the airport attack surface. With so many interconnected systems operating across different functions, vulnerabilities can easily slip through the cracks. Gaining complete visibility across this environment is a significant challenge, and attackers are quick to exploit any blind spots. Cybercriminals and state-backed groups increasingly exploit these weak points to access networks, disrupt critical services, or exfiltrate sensitive data.

Grounded by ransomware

Ransomware attacks on airports are no longer hypothetical—they are happening frequently and causing more disruptive consequences. According to a 2025 study[‡], ransomware attacks on aviation infrastructure are on the rise, with threat actors increasingly targeting operational systems and administrative networks for maximum impact.

In 2024, Seattle-Tacoma International Airport was hit by a ransomware attack that exfiltrated data for sale and disabled baggage and ticketing systems. Just months later, airports across Malaysia experienced widespread disruption after being targeted by Qilin, a Russian-language cybercrime operation, prompting aviation authorities to issue urgent regional warnings.

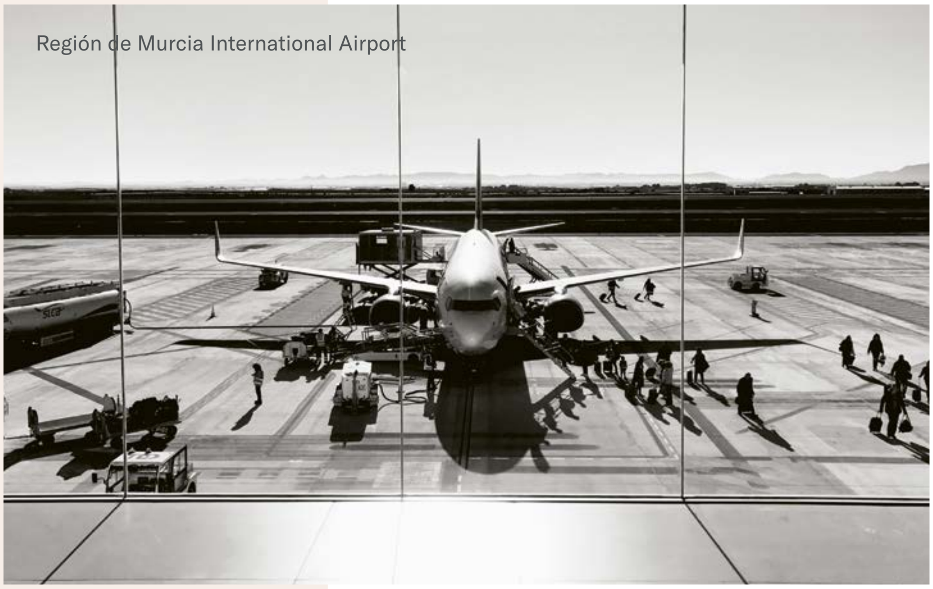
These incidents are prime examples of the ways ransomware can affect the full scope of airport operations: flights can be grounded, baggage handling systems disrupted, and passenger data compromised. In the cases above, these airports were forced to revert to manual check-ins and boarding processes, causing significant delays and and frustrating waiting passengers.

Supply chain and third-party threats

Airports rely on a vast network of third-party vendors and outsourced services. External providers manage everything from IT support and baggage handling to catering and maintenance, creating a complex supply chain. A vulnerability in a single component or piece of software can ripple across the entire airport ecosystem. Attackers increasingly exploit these often fragile relationships, targeting suppliers with weaker security postures to access their partner's more fortified environments.

In July 2024, a global IT outage caused by a faulty CrowdStrike software update disrupted operations at Delta Airlines, highlighting how a single point of failure can have severe consequences. While not a cyberattack, the incident caused flight delays and cancellations at major airports worldwide, underscoring the reliance airports have on their digital partners to maintain full continuity.

Airports are attractive targets for hackers due to their convergence of critical infrastructure, public transit, and international borders



Región de Murcia International Airport

The Collins Aerospace Cyberattack

In late 2025, Collins Aerospace, a major aviation technology supplier, experienced a ransomware attack directed at its MUSE check-in, boarding and baggage management system. The attack, attributed to a British individual, caused multi-day disruption to several European airports. Collins Aerospace, a subsidiary of RTX, provides check-in and operational software directly to airlines, rather than to airports themselves.

While the incident affected airport passengers, it did not originate within those airports' own IT systems. Instead, it exposed how interdependent modern air travel has become, with the failure of a single third-party supplier able to impact airline operations across multiple countries.

The disruption of the Collins Aerospace attack is yet another reminder about the power of robust security protocol, which can protect organizations from potentially cascading effects. Tools such as ThreatLocker® Allowlisting and Ringfencing™ ensure critical systems can operate securely even when a partner's network is compromised. The next breach could come from anywhere in the supply chain, so adopting a Zero Trust architecture is a practical path to operational resilience.

Tackling operational technology vulnerabilities

Behind the high-tech terminals and digital check-in kiosks, many of the systems that keep airports running are decades old. Operational technology (OT), such as runway lighting controls, baggage handling machinery, HVAC systems, and even radar and communications infrastructure, often runs on legacy software that predates modern cybersecurity standards. These systems were built for mechanical reliability, not to defend against ransomware, remote access, or lateral movement by savvy threat actors.

Because many OT systems are isolated from regular IT monitoring, vulnerabilities can go undetected for years. Patching is often difficult, either because systems are proprietary or because downtime isn't an option in a 24/7 operational environment. As a result, attackers who gain access through modern entry points—such as phishing emails, a third-party's compromised laptop, or exposed application programming interfaces (APIs)—can sometimes pivot into these older, unguarded layers of airport infrastructure. Attacking OT, especially industrial control systems (ICS), can lead to serious consequences, as shown by a simulated attack that compromised environmental and safety-critical systems at an airport.

Resilience in the air: the road ahead

As cyberthreats become increasingly aggressive, it's time for airports to adopt modern cybersecurity practices, just as they have done with modern technologies to streamline operations and enhance the passenger experience. One of the most effective ways to achieve this is through a Zero Trust security model, whereby no user, device, or system is automatically trusted, regardless of whether it's inside or outside the network perimeter.

By enforcing strict access controls and software allowlisting, airports can reduce the risk of lateral movement and limit the damage from any breach. It's a proactive strategy that better reflects the reality of today's threat landscape, especially for environments that juggle a mix of legacy technology and modern digital systems.

NEXT PAGE

Cyber Hero Frontline sat down with two of Heathrow's senior technology leaders to explore how their roles intersect to keep one of the U.K.'s most critical gateways safe.