COLORTOKENS

Solution Brief

PROTECTING AIRPORTS FROM KNOWN AND UNKNOWN CYBER THREATS

Enabling airports to stay a step ahead of emerging cyber risks

Overview

Airports deal with millions of passengers and cargo movement every year and must be equipped to run all airport operations without interruptions or delays. To do so, airports adopt the latest in technology to streamline airline operations and to ensure the comfort and safety of the passengers. Though airports understand physical security well enough, they just can't afford to wait until their airport boarding, ticketing, baggage scanning, signage systems, or even worse, the air traffic control system becomes a victim of cyber-attack. The damage will be unthinkable, and catastrophic.

According to the European Aviation Safety Agency (EASA), aviation systems are bombarded with an average of one thousand attacks per month.

ColorTokens Xtended ZeroTrust Security Platform is a software-defined security solution, enabling airports to become proactive in their approach in improving security, at the same time simplifying their journey towards achieving the same. ColorTokens zero-trust architecture and intent-based security enables proactive security to workloads, application environments, endpoints and users in traditional and hybrid infrastructures against internal and external threats. ColorTokens technology is platform-agnostic and reduces the CAPEX and OPEX by consolidating point security and siloed networking products.

ColorTokens Airport Solution

With ColorTokens Xtended ZeroTrust Security Platform, airports can systematically equip themselves to enable proactive security against known and emerging cyber threats.

Benefits:

- Secure and centralized platform-independent solution for multi-vendor infrastructure
- Zero-trust network architecture to proactively defend airport systems from data breach, APT and other unknown cyber threats
- User and application endpoint security without additional hardware investment
- Security posture visualization across airport application environments, workloads, users and endpoints
- Signature-less endpoint security, to protect even unsupported/unpatched legacy terminals
- Fast deployment

Cybersecurity Challenges in Airports

- ***Reactive Security:*** Airports deal with hundreds of interconnected and inter-dependent systems, from airline ticketing, check-ins, and baggage handling systems to Airport Operations Control Center (AOCC), gate operations and so on. Airports have several point security products to monitor and remediate cyber threats. However, most of the systems and security strategy that is in place is reactive. Many airports deal with enormous amount of data from all these interconnected systems and utilize them for real-time decision making. The servers and applications handling data could be on-premise or on the cloud, or both, and airports may involve third-party vendors to manage technology, and eventually the security of these segments as well. This adds to the disjointed/siloed airport cybersecurity strategy, and the key decision makers do not have a unified view of the constantly changing security posture of the airport.
- ***Vulnerable Endpoints:*** Airports have thousands of endpoints and critical resources accessed by employees and third-party contractors

with different security clearance levels. Most of the endpoints, including flight ticketing, manned check-in workstations, POS terminals, e-boarding systems, parking systems, baggage handling, interconnected surveillance CCTV and digital signage systems are vulnerable to external and internal cyberthreats. The endpoints could be legacy systems or the ones running unpatched or unsupported operating system or application – eventually, these systems are not locked down or tamper-proof. Each of them poses a potential opportunity to a hacker trying to gain access to the multitude airport operations systems through a vulnerable endpoint and spread laterally. All these endpoints in airports are vulnerable to Advanced Persistent Threats (APT lateral threats), malware and ransomware, and it's just a matter of time before one of them gets infected, spreading the malicious code to other systems across the network.

- ***Threats from Within:*** Employee access to check-in and other endpoint terminals, and administrator access to critical database and application servers are still assigned ad hoc – making it difficult to track continuously when employees move across departments or exit the company. The attack from within the airport might come from a malicious employee tampering with the systems deliberately. The attack could also be from an employee unknowingly becoming a victim of a phishing attack, compromising his/her credentials to the attacker. Airports need to continuously educate and train their employees on cyber hygiene, which is time-consuming and expensive. Human errors, like a misconfiguration of an internal firewall, could leave critical database and application environments exposed and vulnerable.

> In 2017, Ukraine's Boryspil International Airport had to shut down parts of airport operations due to Petya/Not-Petya attack, and the LATAM Airlines Group came under WannaCry ransomware attack.

- ***Increasing Attack Surface:*** The number of connected endpoint terminals, digital signage and application environments, spread across a vast area of the airport, combined with the hundreds of Wi-Fi access points and thousands of passengers' mobile devices tethered to them provides a very large attack surface. Unlike other regulated industries like finance or healthcare, airport cyber security doesn't have a specific standard or compliance to adhere to. Many airports have adopted their own cyber security strategy that suits their day-to-day operating model. Executives of airports that oversee cyber security must deal with a plethora of security and monitoring products or depend on the skills of the personnel manning the security operations center (SOC). Though complex and time-consuming, it's a necessity to constantly assess the security posture and be notified of the risks to remediate with minimal disruption to airport operations and passenger convenience and safety.

ColorTokens Solution

ColorTokens Xtended ZeroTrust Security Platform helps key decision makers strengthen airport cybersecurity by taking a centralized and proactive approach. Airports no longer need to fight with siloed IT management products to ensure a uniform security posture across on-premise or multi-cloud data centers and distributed endpoints. ColorTokens offers airports the simplicity, flexibility and reliability required to achieve maximum security against known and unknown cyberattacks and helps them focus on improving other essential airport operations.

ColorTokens Xview - Visualize everything. Eliminate blind spots.

Without requiring disparate visualization tools, ColorTokens provides in-depth visibility of cross-segment traffic across the airport's on-premise or multi-cloud data center infrastructure, reducing operational headache. ColorTokens goes a step further in empowering cyber security personnel with residual risk metrics and contextual analytics to continuously assess and improve the security posture of the airport IT infrastructure.

This centralized granular visibility enables airports to visualize the communications happening in real-time among their critical application and database servers and identify suspicious incoming/outgoing connections.

ColorTokens Xshield for Workload Protection - Microsegment workloads in ZeroTrust Zones™

Airports run hundreds of applications. With ColorTokens, airports can implement a zero-trust network through secure micro-segmentation to separate their transactional, application development and passenger database environment in their multi-cloud, multi-vendor data center. ColorTokens enables fast, secure and logical segmentation without the need for additional investment on high-capacity internal firewalls. Network admins need not deal with time-consuming and error-prone VLAN/ACL configurations and thousands of firewall rules.

Airports can reduce the attack surface with ColorTokens secure micro-segmentation – limiting the propagation of APT lateral threats and other unauthorized access of critical resources from within or from outside the infrastructure. ColorTokens security automation ensures airports to have a uniform security posture, even when resources move across clouds or on-premise data centers. ColorTokens enables end-to-end encryption between terminals or resources, making the data communication tamper-proof.

ColorTokens Xprotect for Endpoint Detect and Response – Respond to the inevitable, rapidly.

ColorTokens protects all airport endpoints, critical assets and POS terminals from malware, ransomware and other unknown threats that eventually spawn a malicious process to infect the computer and spread laterally. ColorTokens takes a straightforward yet robust signature-less approach helping airport IT authorities worry less about legacy, unpatched and unsupported endpoints. ColorTokens provides exceptional security by locking down check-in kiosks, baggage handling terminals, building and video management systems, airport operational control center, back office systems and so on, without the need for multiple anti-virus tools, signature updates and patch management headache – also saves costs on expensive cyber training for employees. ColorTokens goes a step ahead in protecting these systems even if they are offline.

Conclusion

The number of security incidents are on the rise, year over year – upwards of 50,000+ security incidents and 2,000+ data breaches, according to Verizon's 2018 Data Breach Investigations Report. Owing to the frequency and sophistication of cyber-attacks, airports need to rethink their existing reactive security strategies, and embrace a holistic, proactive approach. The journey to better security is accomplished through simpler operational complexity. Colortokens provides a unified and platform-agnostic security solution that will scale along with the rapidly changing airport digitalization projects, while reducing the operational complexity. ColorTokens Xtended ZeroTrust Security Platform empowers airports to stay a step ahead of emerging cyber risks.

colortokens.com
sales@colortokens.com