SEPIO

Zero Trust Hardware Access for Airports

Securing the physical foundation of aviation operations across IT, OT, IoT, and cyber-physical infrastructure

A Sepio white paper

Executive Summary

Airports are no longer only transportation hubs. They are highly connected cyber-physical environments where passenger processing, baggage handling, airside operations, building management, access control, video surveillance, retail, telecom, third-party services, and airport operations all depend on thousands of connected hardware assets.

A failure or compromise in one technology domain can quickly become an operational disruption across terminals, airlines, ground handlers, tenants, travelers, and critical airport services. For this reason, airport cybersecurity is not only about protecting data. It is about preserving operational continuity, safety, resilience, and trust.

Most airport cybersecurity programs already invest in endpoint security, network monitoring, identity, OT security, segmentation, and access control. Yet one foundational blind spot often remains: the organization may not be able to verify what a connected device truly is at the hardware level.

Traditional identifiers are not enough. MAC addresses can be spoofed. Hostnames can be misleading. Certificates may not represent the physical device itself. Agents are not always present, especially across OT, IoT, vendor-managed systems, and specialized airport infrastructure. Traffic analysis may be limited by encryption, segmentation, privacy requirements, and operational constraints. Asset inventories can quickly become outdated as airlines, contractors, tenants, vendors, and airport departments connect and move equipment across distributed sites.

Sepio's Zero Trust Hardware Access approach addresses this gap by extending trust verification to the hardware layer. Using patented AssetDNA technology and physical-layer intelligence, Sepio helps airports discover connected hardware assets, verify their true identity, validate whether they belong in a specific role or location, assess device risk, and support enforcement through existing security and operational workflows.

This gives airport security, IT, OT, engineering, and operations teams a more reliable foundation for cyber resilience. Instead of relying only on what a device claims to be, teams gain evidence of what the device truly is, where it is connected, whether it is expected, and what action should be taken.

The result is a stronger model for airport cyber resilience: one where trust begins before network access, before software identity, and before user activity. In a modern airport, Zero Trust must start at the hardware layer.

Trust starts at the hardware layer.

Airports cannot protect what they cannot accurately identify. Sepio extends Zero Trust beyond users, applications, and software agents to the connected hardware assets that keep airport operations moving.

Who This White Paper Is For

CISOs and Information Security leaders:

reduce unknown device risk, close hardware blind spots, and strengthen Zero Trust programs

OT and Engineering teams:

gain accurate visibility into devices supporting baggage systems, access control, CCTV, building management, airside operations, and critical facilities.

Digital Transformation leaders:

support smart airport initiatives without introducing unmanaged cyber-physical risk

Risk, compliance, and audit teams:

create evidence of asset discovery, device trust, segmentation readiness, and response workflows

See. Verify. Control.

Zero Trust Hardware Access enables airport teams to answer one of the most important security questions: should this physical device be trusted on this port, in this zone, performing this function, right now?

The Airport Cyber-Physical Reality

Airports operate at the intersection of passengers, safety, operations, tenants, airlines, vendors, and critical infrastructure.

Airports Are Connected Operational Ecosystems

Airport operations depend on a dense mix of IT, OT, IoT, and specialized cyber-physical systems. Some are owned by the airport authority. Others are operated by airlines, concessionaires, ground handlers, security contractors, building-system vendors, baggage-system integrators, telecom providers, and government agencies. This creates a constantly shifting environment where ownership, location, and trust are difficult to maintain with confidence.

Typical connected assets include passenger kiosks, check-in systems, baggage handling controllers, CCTV cameras, access control panels, biometrics readers, gate systems, building management controllers, lighting systems, HVAC, elevators, escalators, Wi-Fi infrastructure, network switches, VoIP phones, printers, digital displays, ruggedized OT workstations, servers, thin clients, and vendor-managed appliances.

This complexity is not a flaw. It is the reality of modern aviation. The challenge is that every connected asset becomes part of the airport's operational risk surface. When the device layer is not trusted, every control above it inherits uncertainty.

Operational Impact Is the Real Risk

Airport cybersecurity is not only about data loss. It is also about resilience, continuity, and safety-adjacent operations. A cyber incident can affect check-in, baggage sortation, flight information displays, passenger communications, parking, access control, physical security workflows, and the ability of teams to coordinate a response. The most damaging events may not compromise air traffic control or safety systems directly; they may still create large-scale disruption, manual workarounds, reputational damage, and cascading operational delays.

The New Airport Attack Surface

- → **Converged IT/OT environments:** Corporate networks, terminal systems, and operational networks often share dependencies even when segmented.
- → **Vendor and tenant ecosystems:** Third-party equipment is necessary, but it can reduce inventory accuracy and ownership clarity.
- → **Unmanaged and agentless assets:** Many airport systems cannot support endpoint agents, may run legacy software, or are maintained by external parties.
- → **Physical access realities:** Airports include public areas, restricted zones, remote facilities, gates, hangars, maintenance areas, and distributed infrastructure.
- → **Digital transformation:** Smart airport programs introduce sensors, automation, biometrics, mobile workflows, and data-driven operations that increase asset diversity.

What Makes Airport Environments Different

Airports combine the scale of a city, the uptime requirements of critical infrastructure, the distributed nature of a campus, and the accountability of regulated transportation. This means the security model must support thousands of assets across multiple operational domains while respecting safety, privacy, vendor maintenance windows, and continuous passenger service.

Some airport-specific risk factors include: public/restricted zones, tenants, airlines, ground handlers, concessionaires, maintenance vendors, and temporary connectivity.

> **“Airport security controls must improve trust without slowing operations.”**

Why Traditional Zero Trust Stops Too High in the Stack

Zero Trust must begin with verified hardware identity, not with an assumption that the device is what it claims to be.

Zero Trust Is Incomplete Without Hardware Trust

Zero Trust has transformed cybersecurity by requiring explicit verification of users, applications, access requests, and sessions (NIST SP 800-207 Zero Trust Architecture). However, many Zero Trust programs start at the software or identity layer. They assume that the device presenting an identity, certificate, MAC address, hostname, or agent is the device it claims to be. In airport environments, this assumption is risky.

A device may be unknown, unmanaged, misclassified, spoofed, repurposed, misplaced, compromised, or connected outside its authorized zone. Even well-managed environments can struggle when contractors connect temporary equipment, legacy OT assets cannot host agents, or third-party systems are integrated during construction, modernization, or expansion projects.

Why Software Identity Is Not Enough

→ **MAC and IP identifiers can be misleading:**
They support routing and management, but they do not prove true hardware identity.

→ **Agents are not universal:**
Many OT, IoT, and vendor-managed systems cannot run endpoint agents or cannot be modified without operational approval.

→ **Traffic inspection is increasingly constrained:**
Encrypted traffic, segmented networks, privacy concerns, and operational sensitivity can limit inspection-based visibility.

→ **CMDBs drift over time:**
Airport assets move, change ownership, are replaced, or are connected temporarily. Static records rarely remain authoritative.

→ **Vendor declarations require validation:**
Procurement and documentation can state what an asset should be; security teams still need evidence of what is actually connected.

The Trust Chain for Airport Assets

An airport trust chain should answer five questions before a device is allowed to operate without restrictions: What is it? Is that identity verified by physical-layer evidence? Where is it connected? Is it expected in that location and role? What should happen if it is unknown, risky, or out of policy?

From Visibility to Enforcement

Visibility alone does not reduce risk unless it supports action. Sepio connects discovery, verification, validation, risk scoring, and enforcement workflows so airport teams can move from asset awareness to operational control. The same verified identity that improves inventory can also guide NAC decisions, SIEM/SOAR playbooks, ticketing, segmentation validation, and incident response prioritization.

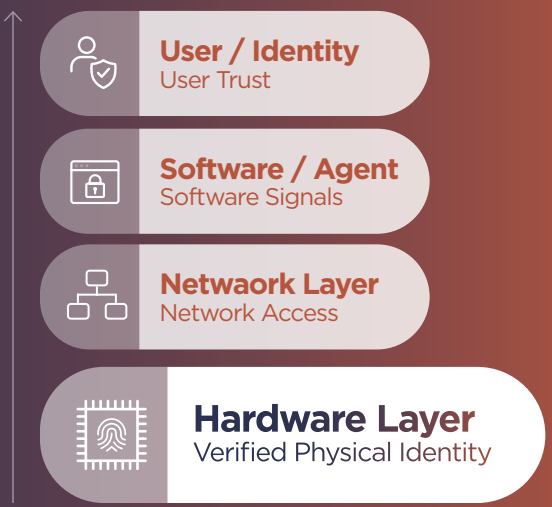
Zero Trust Hardware Access.

A security model that validates physical device identity before trust is granted - extending Zero Trust down to the hardware layer.

Verify the device

Validate its role

Trust only what is proven



SEPIO

The Hardware Blind Spot in Airport Environments

3

The most dangerous asset is often the one your tools do not truly recognize.

Where Blind Spots Appear

Airport networks contain many assets that are difficult to identify through conventional methods. Some are agentless. Some are vendor-managed. Some sit behind gateways. Some are dormant until a process starts. Some appear as generic Linux, Windows, or embedded devices. Some are intentionally deceptive. Some are simply connected in the wrong place.

These blind spots matter because airport operations depend on physical devices that bridge cyber and operational processes. If the device identity is wrong, then policy, segmentation, risk scoring, and response can also be wrong.

Common Airport Hardware Risk Scenarios

Scenario	Airport Context	Sepio Contribution
Rogue Device in Restricted Zone	An unauthorized device is connected to a port in an operations area or equipment room.	Detect true device identity and location; trigger alert, ticket, or block workflow.
Misidentified Physical Security Device	A device appears legitimate based on MAC/vendor data but does not match expected hardware characteristics.	Validate actual identity against AssetDNA and expected role.
Vendor Device Outside Policy	A third-party device is connected for maintenance, integration, or monitoring without proper authorization.	Highlight ownership, location, and policy mismatch for review.
Dormant / Shadow Asset	An asset exists in the environment but is not visible in current security tools or is no longer actively managed.	Surface asset presence and usage history for remediation.
Endpoint Coverage Gap	A workstation or specialized endpoint is connected without expected EDR/NAC posture.	Provide “show me what is connected but not protected” workflows.
Hardware Identity Spoofing	A device claims to be a trusted type but physically behaves like another class of device.	Expose identity mismatch using physical-layer evidence.

Why Hardware Deception Is Different

Many tools classify devices based on software, network behavior, traffic signatures, vendor prefixes, or self-reported data. These signals are useful, but they can be incomplete or manipulated. Hardware-level validation adds a different layer of evidence. It helps security teams detect when a device's claimed identity does not align with its physical characteristics and location.

The Operational Cost of Unverified Devices

→ **Security teams** spend time reconciling conflicting data from CMDB, NAC, EDR, OT monitoring, and network tools.

→ **OT and engineering teams** face delays when unknown devices must be physically traced across terminals, closets, and operational zones.

→ **Incident response teams** may not know which systems are truly affected when a threat emerges.

→ **Compliance teams** lack defensible evidence that all connected assets have been discovered, validated, and governed.

→ **Digital transformation programs** can slow down when new devices cannot be trusted quickly and safely.

The Sepio Zero Trust Hardware Access Framework

Discover, verify, validate, score, and enforce trust at the physical layer.

The Five Pillars of Zero Trust Hardware Access

1 Discover

Identify connected hardware assets across IT, OT, IoT, and cyber-physical environments - including unmanaged, unknown, dormant, and misclassified devices.

2 Verify

Use Sepio AssetDNA technology to establish true device identity based on physical-layer intelligence rather than relying only on self-reported software or network attributes.

3 Validate

Compare verified identity against expected role, location, ownership, function, policy, and business context.

4 Score

Prioritize risk using asset context, device type, exposure, vulnerabilities, behavior, location, and trust status.

5 Enforce

Support action through policies, alerts, tickets, integrations, blocking workflows, and response playbooks.

What Sepio Does Differently

→ **Physical-layer device intelligence:**
Sepio helps identify what a device truly is, not only what it reports through software or network attributes.

→ **Trafficless approach:**
Sepio does not require traffic monitoring or packet inspection to deliver core device identity and visibility value, thus making it encryption-independent and protocol-agnostic.

→ **No special hardware probes or taps:**
Sepio is designed to reduce deployment friction in complex, distributed environments.

→ **Location-aware asset context:**
Sepio helps locate where assets are connected, supporting faster investigation and remediation.

→ **Policy and integration-ready:**
Verified hardware identity can support NAC, SIEM, SOAR, CMDB, ITSM, and XDR workflows.

→ **Scalable to large campuses:**
Suitable for distributed terminal, airside, landside, and remote facility environments.

Zero Trust Hardware Access in Practice

In practice, Sepio helps airport teams move from "we think this is a device" to "we have evidence of what this device is, where it is, whether it is expected, and what action should be taken." This is a fundamental shift from inventory management to trust enforcement.

Airport Use Cases

From terminals and baggage halls to SOC workflows and smart airport programs.

Use Case 1

Unknown and Unmanaged Asset Discovery

Airport teams need continuous awareness of assets connected across landside and airside networks. Sepio helps surface devices that are not in CMDB, not covered by endpoint controls, not expected in a zone, or not properly classified.

→ **Business value:** reduces shadow asset risk and supports more accurate asset governance.

→ **Operational value:** shortens time to locate and investigate unknown devices.

Use Case 2

Rogue Device Mitigation in Operational Zones

Equipment rooms, baggage areas, gates, maintenance zones, and vendor areas can all include network access points. Sepio helps identify suspicious or unauthorized hardware and provides the context needed for response teams to act quickly.

→ **Business value:** supports operational continuity and reduces exposure to unauthorized connectivity.

→ **Operational value:** provides physical location context and policy-driven escalation.

Use Case 3

Baggage Handling and Building Systems Visibility

Baggage handling systems, HVAC, lighting, elevators, escalators, and other facility systems are critical to passenger flow. Many include specialized controllers and vendor-managed devices that may not fit traditional endpoint security models. Sepio helps create a verified asset view without requiring intrusive traffic inspection.

Use Case 4

Access Control, and Physical Security Infrastructure

Physical security systems are themselves cyber assets. Cameras, recorders, access panels, biometric readers, intercoms, and display systems should be continuously verified against expected identity, location, ownership, and policy.

Use Case 5

Endpoint Coverage Gap Analysis

Airport security leaders often need to know which connected assets do not have expected controls such as EDR, NAC posture, or configuration coverage. Sepio can support an asset-centric workflow: identify what is connected, validate what it is, compare against expected controls, and route gaps to the right team.

Use Case 6

Third-Party and Tenant Asset Governance

Airports depend on tenants, airlines, retailers, government agencies, and vendors. Sepio can help provide a neutral, evidence-based view of connected hardware assets and reduce dependency on manual declarations or periodic surveys.

Use Case 7

Incident Response and Forensic Readiness

When a threat is detected, response teams need to know what devices exist, where they are connected, what they are, whether they moved, and what business process they support. Sepio helps create a verified asset context that can improve triage and reduce investigation time

Architecture and Integration Model

A practical model for airport deployment without inline dependencies, traffic inspection, or operational disruption.

Deployment Principles for Airports

→ **Non-disruptive by design:**
Avoid adding inline dependencies to operational networks.

→ **Trafficless discovery:**
Reduce privacy, bandwidth, and inspection constraints by not relying on packet monitoring for core identity value.

→ **Segment-aware operation:**
Work across segmented environments while preserving operational boundaries.

→ **Integration-first workflow:**
Feed verified hardware identity into existing SOC, ITSM, NAC, CMDB, and XDR processes.

→ **Evidence-based trust:**
Use physical-layer device intelligence as a source of truth for hardware-level validation.

Reference Integration Patterns

Integration Area	Airport Need	How Sepio Supports It
CMDB / Asset Inventory	Maintain accurate asset records across terminals, facilities, and third parties.	Enrich inventory with verified identity, location, and hardware context.
NAC / Network Enforcement	Apply access policies based on trusted device identity.	Support allow/block or quarantine decisions based on verified device trust.
SIEM / SOAR	Prioritize and automate response.	Send events and context for playbooks, alerts, and investigation.
ITSM / Ticketing	Operationalize remediation.	Create tickets with device type, location, owner, and recommended action.
XDR / EDR	Find assets outside endpoint coverage.	Identify connected endpoints and devices that lack expected controls.
OT and Engineering Systems	Protect operational continuity.	Provide non-intrusive visibility into OT-adjacent hardware assets.

Data Model for Airport Device Trust

A hardware-aware trust model should include verified identity, asset class, connection point, network zone, physical location, owner, expected role, security coverage, known vulnerabilities, observed history, risk indicators, and enforcement status. Sepio brings the physical-layer identity component that many existing data models lack

Regulatory and Resilience Alignment

Align hardware-level trust with aviation cyber resilience, segmentation, access control, monitoring, and risk-based remediation.

Supporting Aviation Cybersecurity Expectations

Cybersecurity expectations for aviation, as outlined in ICAO Aviation Cybersecurity Strategy, ACI airport cybersecurity guidance, EASA Part-IS, NIS2, NIST CSF 2.0, NIST SP 800-207, IEC 62443, ISO/IEC 27001, and NIST SP 800-161, increasingly emphasize resilience, segmentation, access controls, continuous monitoring, and timely patching or risk-based remediation. These goals all depend on knowing which assets exist, where they are, whether they are critical, and whether they are trusted. Sepio strengthens these foundations by providing verified hardware identity and location-aware asset context.

Mapping Sepio to Common Airport Cybersecurity Objectives

Objective	Airport Security Requirement	Sepio Alignment
Asset Discovery	Maintain a complete and current view of connected IT, OT, IoT, and cyber-physical assets.	Discovers and classifies assets using hardware-level intelligence.
Segmentation Readiness	Know which assets belong in each network zone and detect out-of-policy devices.	Validates device identity and location against policy expectations
Access Control	Prevent unauthorized access to critical cyber systems.	Supports trust-based allow, block, quarantine, and escalation workflows.
Continuous Monitoring	Detect anomalies and changes that may affect critical operations.	Maintains continuous visibility into connected hardware and identity changes.
Risk-Based Remediation	Prioritize based on criticality, exposure, and real risk.	Adds device identity, location, and trust evidence to risk scoring.
Audit Evidence	Demonstrate governance over connected assets and control gaps.	Creates defensible hardware-level asset records and event history.

Why Hardware Verification Improves Compliance Workflows

Compliance programs often require evidence. A list of expected assets is useful, but it is not the same as continuous validation of what is actually connected. Hardware-level verification helps security and audit teams demonstrate that inventory, access decisions, segmentation, and remediation workflows are grounded in observed device truth.

A 30-Day Action Plan for Airport Teams

A practical starting point for discovery, validation, and hardware-level Zero Trust

Days 1-10 Establish the Baseline

→ **Identify priority airport zones:** SOC-managed networks, baggage systems, physical security systems, building management, terminal operations, and remote facilities.

→ **Create a baseline of connected hardware assets** and compare against CMDB, NAC, EDR, OT monitoring, and vendor records.

→ **Identify unmanaged,** unknown, dormant, duplicate, and misclassified devices.

→ **Map high-risk assets** to physical locations, owners, business processes, and network zones.

Days 11-20 Validate Trust and Policy Fit

- → **Define expected hardware profiles by zone and function:** cameras, access control, kiosks, baggage systems, controllers, servers, endpoints, printers, and network equipment.
- → **Flag identity mismatches,** unexpected devices, and assets connected outside approved locations.
- → **Prioritize risk** based on operational criticality, exposure, device trust, known vulnerabilities, and ownership clarity.
- → **Create remediation playbooks** with IT, OT, engineering, SOC, and vendor teams.

Days 21-30 Operationalize Enforcement

- → **Integrate verified device context** into SIEM, SOAR, ITSM, CMDB, NAC, and XDR workflows.
- → **Implement policy-based escalation** for unknown, unauthorized, or high-risk hardware assets.
- → **Validate segmentation** by confirming that expected device types are present in the expected network zones.
- → **Build executive dashboards** for risk reduction, asset coverage, unknown device trends, and remediation status.

Expected 30-day outcome.

Airport teams should be able to identify critical blind spots, validate device trust in priority zones, reduce unknown hardware risk, and establish repeatable workflows for enforcement and remediation.

Maturity Model and Readiness Questions

Measure progress from inventory to hardware-level trust enforcement

Level	State	Typical Condition	Next Step
1	**Manual Inventory**	Asset records depend on spreadsheets, vendor reports, and periodic audits.	Automate discovery and reconcile records.
2	**Network Visibility**	Teams can see many connected assets but classification is inconsistent.	Add hardware-level verification.
3	**Verified Identity**	Device identity is validated using physical-layer evidence and location context.	Connect identity to policy and risk.
4	**Risk-Based Control**	Unknown or risky devices trigger alerts, tickets, and response workflows.	Automate enforcement through integrations.
5	**Continuous Hardware Trust**	Trust is continuously verified and used across SOC, IT, OT, compliance, and transformation programs.	Optimize policy, metrics, and resilience reporting.

Readiness Questions for Airport Leaders

- → Can we identify every connected hardware asset across priority terminal, airside, landside, and facility networks?
- → Can we verify device identity beyond MAC address, hostname, IP, and self-reported information?
- → Do we know where each critical device is physically connected?
- → Can we detect a device that claims to be one thing but physically appears to be another?
- → Can we identify devices that lack expected endpoint, NAC, or monitoring coverage?
- → Can we validate that baggage, CCTV, access control, and building systems are connected only where expected?
- → Can we give incident responders a verified list of impacted assets within minutes?
- → Can we provide auditors with evidence that connected assets are continuously governed?
- → Can our Zero Trust program make decisions based on verified hardware identity?
- → Can we support smart airport innovation without increasing unmanaged device risk?

KPIs to Track

Conclusion

The future of airport cybersecurity depends on trusted device truth.

Airports are becoming smarter, more automated, and more connected. That transformation improves passenger experience and operational efficiency, but it also increases dependency on physical devices that must be trusted. Traditional visibility, endpoint security, network monitoring, and access control remain important. But without verified hardware identity, the security stack is still making trust decisions on an incomplete foundation.

Sepio's Zero Trust Hardware Access approach gives airports a way to extend Zero Trust down to the physical layer. By discovering, verifying, validating, scoring, and enforcing trust for connected hardware assets, airport teams can close a foundational blind spot and strengthen resilience across IT, OT, IoT, and cyber-physical systems.

The Sepio message for airports

Secure the airport from the hardware layer up. Verify every device. Trust only what is proven. Act before blind spots become disruption.

About Sepio

Sepio is the leader in Zero Trust Hardware Access. Sepio enables organizations to see, verify, and control connected hardware assets using patented AssetDNA technology based on physical-layer intelligence. The platform helps enterprises and critical infrastructure organizations close hardware-based blind spots, reduce rogue and unmanaged device risk, and extend Zero Trust principles down to the device level without requiring traffic inspection or special hardware probes.

SEPIO