ALERTENTERPRISE

SOLUTIONSHEET

AIRLINE PHYSICAL ACCESS GOVERNANCE AND CYBER-PHYSICAL SECURITY CONVERGENCE

The AlertEnterprise physical identity access governance and cyber-physical security convergence platform enables airlines to eliminate security silos, to deliver the most complete view of threats and vulnerabilities while providing a frictionless, safe and secure physical access experience for your workforce.

End-to-End Physical Access Lifecycle Management

WORKFORCE ENABLEMENT
Day 1 Productivity

- Rule-based, real-time automation 'hire-to-retire' of airline workforce badge & physical access management
  – Employees, contractors, corporate, crew, pilots
- 360-degree enterprise view and transparency of an identity's footprint
  – Access, trainings, validations, background checks
- Frictionless safe and secure physical access experience
  – Self-service requests, review and approvals for physical access and badge management

GOVERNANCE, SAFETY & COMPLIANCE
Safe and Secure Workspaces

- Proactive compliance – automated safety, security, training validation and background checks prior to badge and access grants for employees and non-employees
- Automated and continuous access/badge monitoring (including return) with area business owners
- Periodic reviews for regulatory compliance for critical areas and access creep mitigation
- Embedded automated enforcement controls for safety & security protocols for expiring:
  - Badge
  - Access
  - Passport
  - SIDA
  - Media Rooms
  - Photo
  - Training
  - Background Checks
  - Simulators
  - GDPR

SUSTAINABLE OPERATIONAL EXCELLENCE
Organic with Elasticity

- Fully automated integrations, complete data sync and integrity with internal and external systems
  – CASS, CLEAR, KCM, Airports, RapBack etc.
- Digital transformation of all internal and external facing security operations with uniformity and standardization
  – Authorized Signatories, RapBack Enrollment, Remote sites, Emergency Access, Citations, Vehicle Decals etc.
- Mobile footprint, photo updates, rebadging, jump seat allocations, physical keys management, passport validity monitoring and advance notifications

AIRLINE PHYSICAL IDENTITY ACCESS GOVERNANCE AND CYBER-PHYSICAL SECURITY CONVERGENCE

The cost to operate systems in existing silos is expensive and full of risk. AlertEnterprise delivers a single unifying platform with a dual-focused objective: 1) bridge the security gaps and 2) eliminate redundant spending.

ENTERPRISE GUARDIAN

PHYSICAL IDENTITY ACCESS MANAGEMENT

WORKFORCE ACCESS GOVERNANCE

- Real-time integration with HR, multiple PACS and IT / Business Systems
- Consolidated decentralized badge management across hubs
- Business partner onboarding, physical access governance
- Contractor access governance
- Self-service access requests
- Automated notification and re-issuance of expiring badge
- Removal of badge access on termination and risk indicators
- Full life-cycle visitor identity management in multi-tenant environment

IDENTITY INTELLIGENCE

WORKFORCE INTELLIGENCE

WORKFORCE INTELLIGENCE

- Identity intelligence to monitor insider threats
- Unified identity profile and risk score
- AI and Machine Learning behavior analytics
- Active policy enforcement for regulatory compliance

ENTERPRISE SENTRY

UNIFIED THREAT RESPONSE

CYBER-PHYSICAL SECURITY CONVERGENCE

- Unified dashboard across security systems (Video, PACS, Perimeter Intrusion Detection PID)
- Easy, controlled information sharing
- Mobile app for real-time, remote response
- Automated remediation scripts

SECURITY CONVERGENCE PLATFORM

INTEGRATION FRAMEWORK

IT Resources

SAP, workday., servicenow, Microsoft, ca, IBM, ArcSight, SailPoint, ORACLE

Physical Security

LENEL·S2, tyco, Johnson Controls, Genetec, Honeywell, SIEMENS, VANDERBILT, AMAG

OT Systems

Honeywell, Johnson Controls, SIEMENS, ABB, Rockwell Automation, Schneider Electric, GE, EMERSON

Types of Insider Threats

COMPROMISED / PAWN

Employees that don't know they're being compromised

MALICIOUS / EXPERT

Usually have legitimate user access to the system and willfully extract data or intellectual property

CARELESS

Employees that leave computer or terminal unlocked or otherwise violate cybersecurity best practices

SLOW POISON

Systems slowly moving outside of reasonable parameters

0-DAY INSIDERS

New personnel with little to no background information

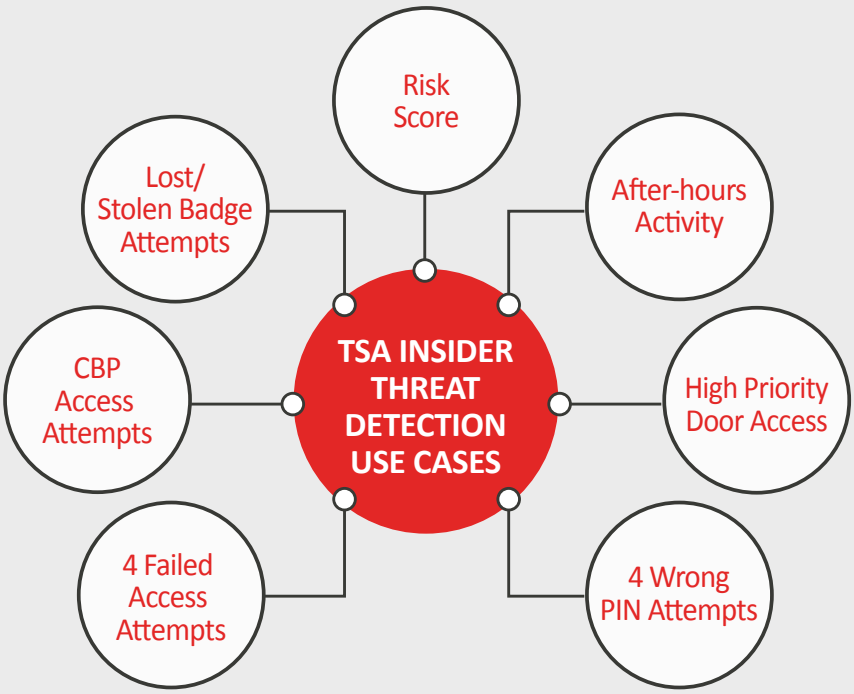
NEEDLE IN A HAYSTACK

Small incidents such as theft of IP or customer contact lists in a large volume of access pattern data that are difficult to detect

Airline employees are used to interacting with a workforce in constant flux, making it harder for permanent employees to question the presence of unfamiliar faces. This leads to situations where malicious insider threats can remain hidden in plain sight. Work environments that employ a large number of contractors and operate "multitenant" operations are always more susceptible to insider attack. An insider can swiftly cause devastation to airport infrastructure, leaving little trace of potential damage until the devastation manifests.

INSIDER THREAT PROTECTION WITH THE TRANSPORTATION SECURITY ADMINISTRATION (TSA) - LESSONS LEARNED

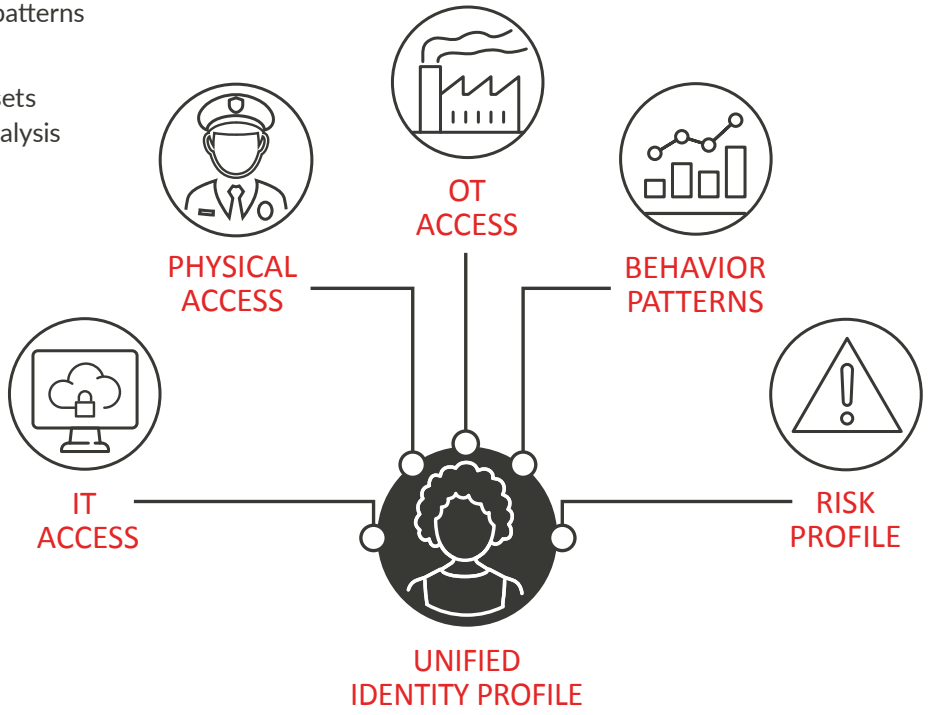
In 2014, AlertEnterprise participated in a pilot project with the TSA, deploying our converged cyber-physical platform to combat insider threats and deliver a unified threat response. The success of the pilot project revealed the power of real-time integration of cyber and physical security systems for identifying, correlating and mitigating insider threat related activity. Since then, AlertEnterprise has been selected and deployed at CATX and CAT1 airports across the globe.



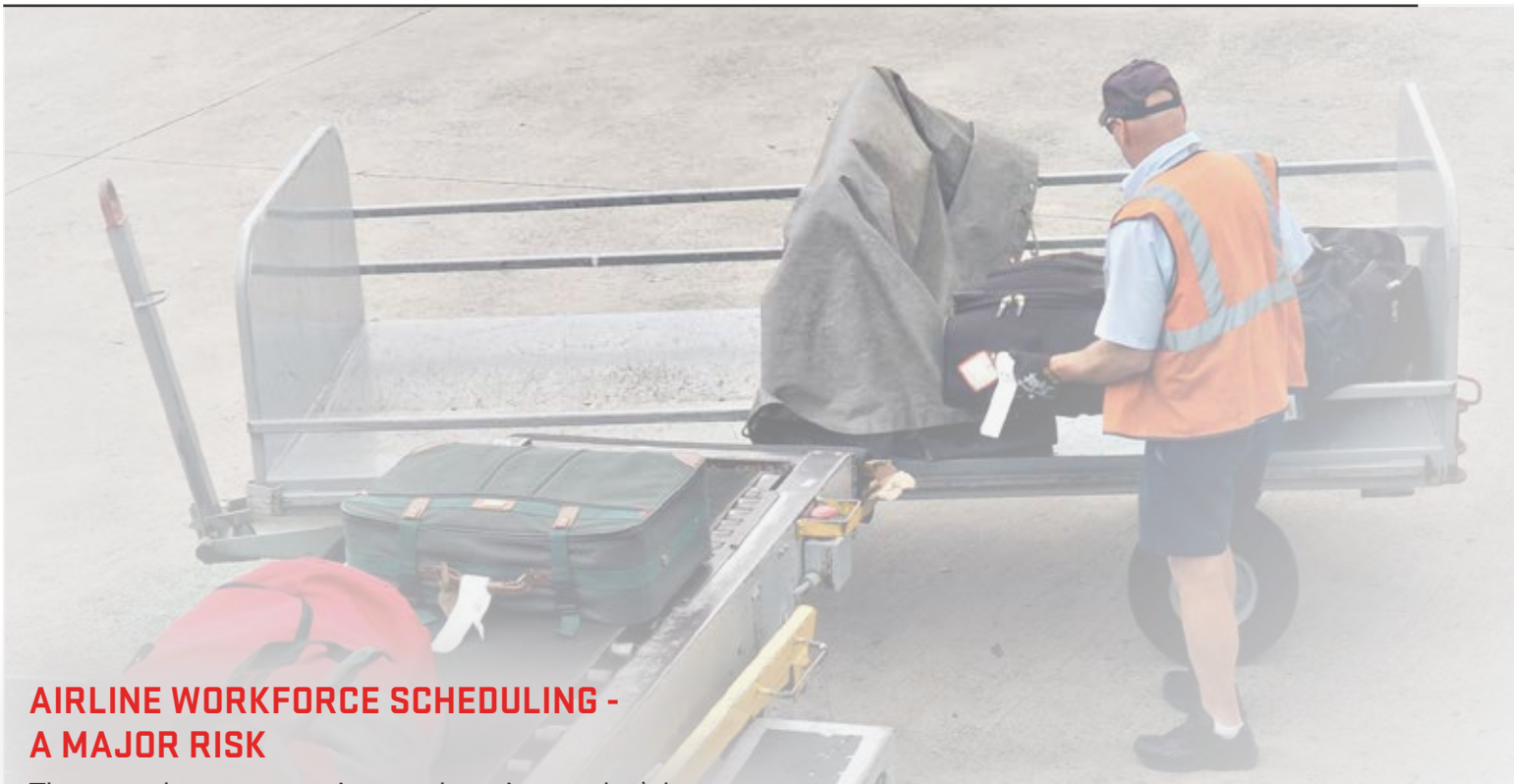
A UNIFIED IDENTITY PROFILE ENABLES INTELLIGENCE DECISION MAKING

A common digital identity for people and things is a starting point for provisioning airline system, data, network and physical access. Reduce the time and cost for detecting and resolving risk by automating threat protection across aviation IT, physical and operational systems from one place. AI and machine-learning Identity Intelligence technology automatically baseline identity profiles, allowing it to quickly sort through millions of events to detect behavior anomalies and trends for an effective response to potential malicious behavior and policy violations.

- Incorporate risk scoring and behavior patterns into an Identity profile
- Visibility across IT, Physical and OT assets allowing for real-time usage pattern analysis
- PRA, background and training checks embedded into a risk score and profile leveraged for access control, granting and reporting activities
- Behavior patterns allow for actionable intelligence to minimize the risk profile to the environment



Identity Intelligence technology helps prevent airline insider threats by maintaining a risk profile for the internal and external workforce, tracking access to critical areas within airports and flight operations. Conducting upfront risk analysis reduces risk and cost, eliminates fraud and enhances security.

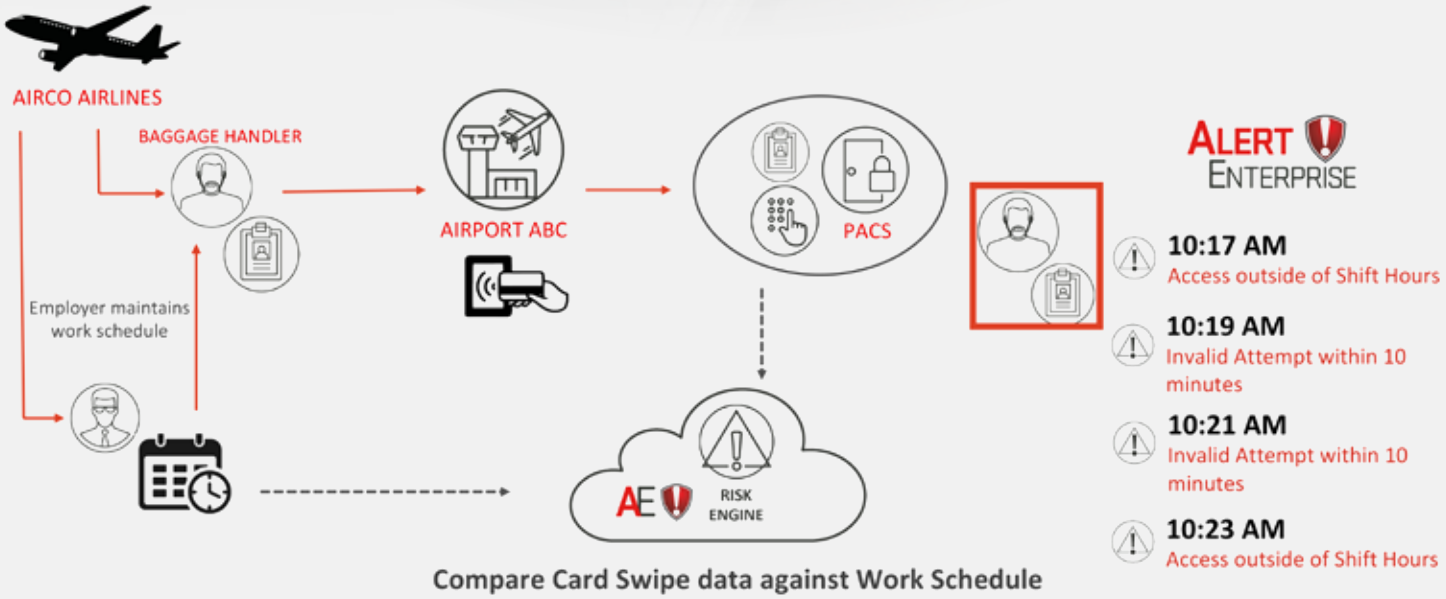


AIRLINE WORKFORCE SCHEDULING - A MAJOR RISK

There are three common issues when airports don't know airline workforce schedules

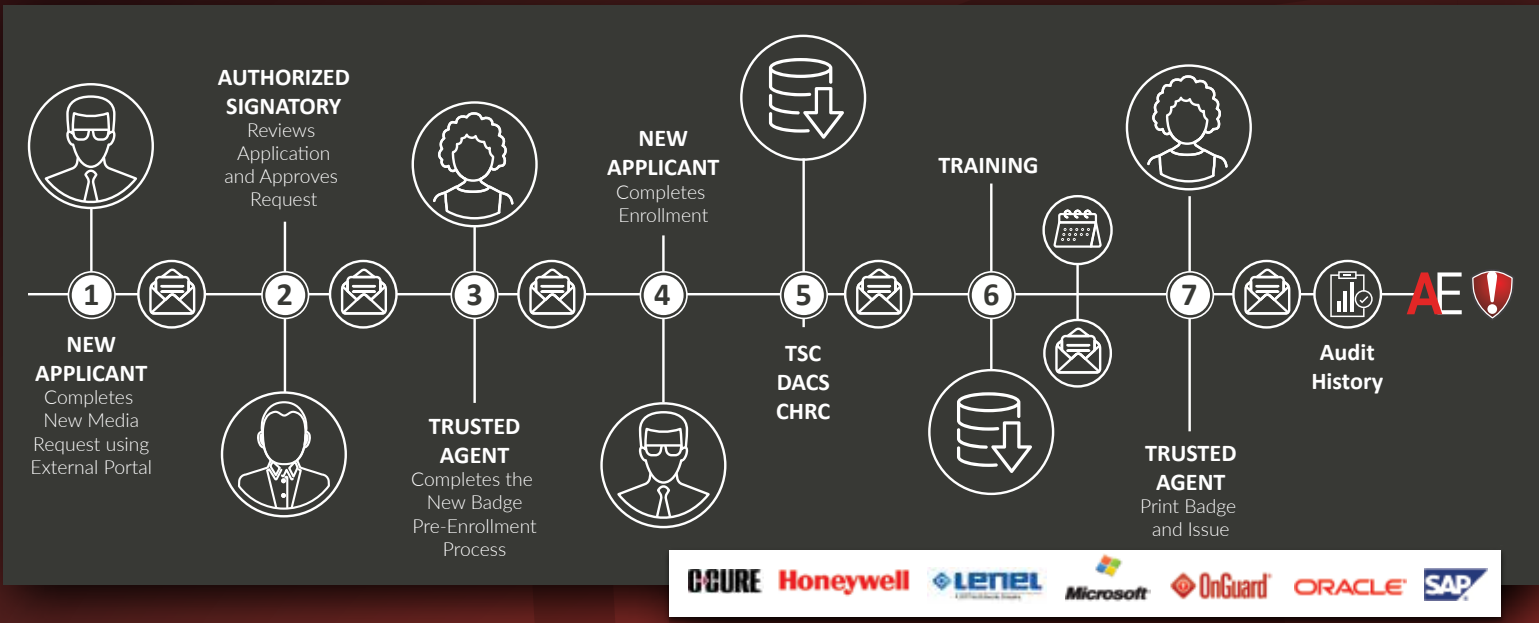
1. Default is to grant 24/7/365 access
2. Rogue employees can access areas (e.g. SIDA/Baggage) outside of their shift hours
3. Neither Airlines nor Airports have any visibility to the risks

Airlines and airports can reduce the risk with converged security that delivers real-time integration between IT work schedule applications and physical access controls systems.



Hire-to-Retire Identity and Credential Lifecycle Management

AlertEnterprise automates the entire onboarding / offboarding process starting with the pre-enrollment risk analysis that provide a high degree of automating for the vetting process.



AlertEnterprise Features Summary

- Streamline and automate the entire lifecycle management from request to return of all airline assets (ID Badges, Keys, Laptops, etc.), physical and digital access using an online portal and AE's Guardian workflow engine.
- Integrations with various HR, ERP, and IT applications like to offer a "single pane of glass" view of each identity, the "time and place" access provisioned to that identity, and how that access is being used along with reports of any violations or abnormalities.
- Continual vetting using integrations with various international, federal, state, and local digital repositories to determine credit history, criminal activity, policy and regulatory violations, and misconduct.
- Identity Intelligence compares behavior to a normalized dataset to calculate a dynamic Risk Score which indicates the evolving threat each insider poses to the airline, airport, or organization.
- Automatically trigger incident response SOPs with situational intelligence.

AlertEnterprise

INFO@ALERTENTERPRISE.COM
ALERTENTERPRISE.COM