AlertEnterprise!

WHITE PAPER

Seven Steps To A Superior Physical Identity and Access Management Solution

Enterprise-Class Physical Identity and Access Management Software

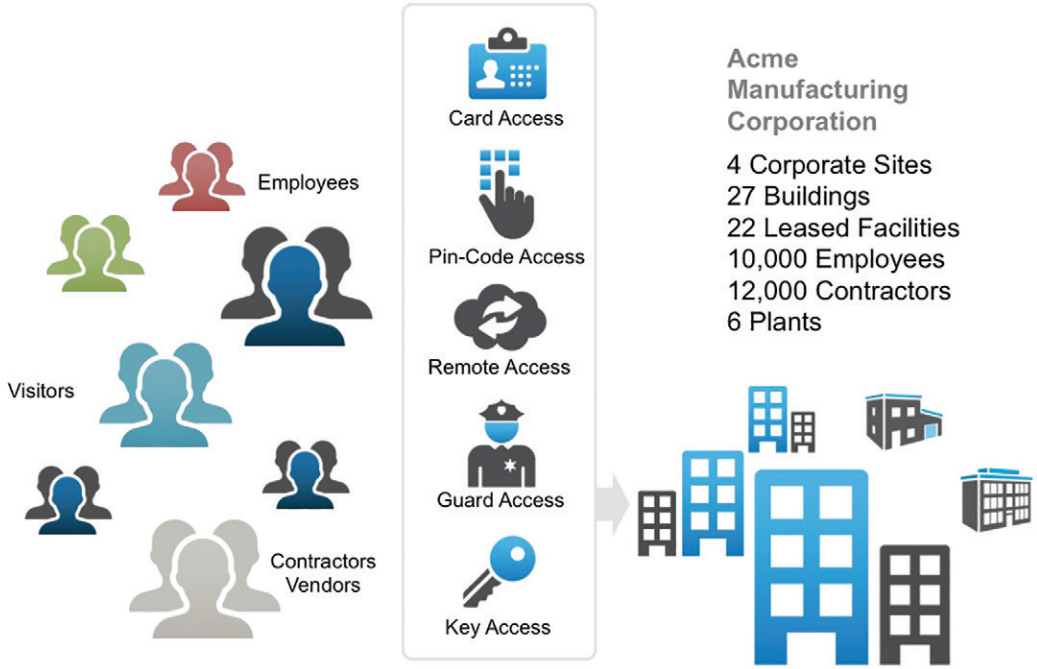
Seven Steps To A Superior Physical Identity and Access Management Solution

Enterprise-Class Physical Identity and Access Management Software

CONTENTS

Introduction

Today's instant economy requires that companies open up more of their business processes to external stakeholders. Employees, contractors, vendors, partners, service providers and visitors, all need access to particular assets, facilities and resources within the enterprise. But how much access is too much? And if granted, how much risk is the company taking? To ensure that commercial transactions and internal operations remain up and running at all times, successful and secure enterprises track the individuals in each of these classes as identities.



Enterprises are challenged with having to deal with many categories of identities who need access to a myriad of systems and resources that could be geographically dispersed across locations

Most organizations today rely on the corporate security department to manage policies on how much physical access to facilities zones and assets should be granted to each identity. Separately, the IT department manages access to the information systems. Regardless of the diligence of these departments, changes to the status of individuals is rarely correlated on a timely basis between the IT and physical security data silos. Full-time employees may leave the company, change jobs or move to new locations. Contractors may become permanent employees, complete their projects or be replaced. There is seldom an integrated and up-to-date profile on how much access has been granted and what happens when an individual's status, class or category changes.

The added dimension of constant change in the workforce, or the types of individuals needing short term temporary access makes it a lot harder to manage. Often times these processes are disjointed and decentralized making it impossible for business managers to know how much risk the organization is taking. Unbeknownst to managers granting access in one area of the company, they may potentially create huge risks in another part of the company.

Organizational Silos Create Risk

The majority of today's key business processes are automated. IT manages the underlying applications for these processes. Security practices relating to application and database access and authorization are tracked by IT security personnel. However, this tracking is rarely coordinated with physical security personnel who are tasked with protecting the facilities and physical assets and who are responsible for managing building access. Further, there is often a lag before status changes noted in HR systems are reflected in IT and physical security systems. Herein lies vulnerability.

Imagine a disgruntled employee in a two-week termination notice period. The employee may access the data center outside their normal hours and systematically download more information in one night, to an external drive, than they ever had in the prior two years. This often repeated scenario, can trigger potentially devastating damage to the company from loss of data, trade secrets or confidential information. Detecting such an event, much less preventing it, is very difficult without correlating the employee's activity across the information systems, the physical access control (badge access systems) and HR management systems.

Security Functions	The Need for Integration across IT and Physical Security
Physical Identity and Access	Single identity record, On-boarding / Off-boarding Access Approvals
Background Check & Training	Background check requires accessing information feeds and acting on the information contained Checking training system repositories to validate that required training has been completed
Policies	Threat conditions Compliance (FDA regulation, U.S. DEA Security Regulation)
Contractors / Vendors / Visitors	Security checks Escorted vs. un-escorted Access
Multi-Vendor Access Control Systems	Disparate PACS Varying access level
Badging and Security Operations	Various security policies and rules Expiration periods
Access Provisioning and Removal	Role-based access Instant termination
Access to Issued Assets	Provisioning access Tracking assets
Audit and Compliance	Audit reports Access certification Compliance mandates
Security Reports	Access behavior and patterns Insider threat Identity analytics

Table: List of commonly observed functions that would benefit from integrating Physical Security Functions with IT or OT

Today's top threats in the work place can be linked to a lack of integrated identity systems that extend across the enterprise.

The Need for a Holistic Identity Management Solution

Managing Security Across Many Stakeholders - Many enterprise functions, from HR to finance to parking, are tasked with ensuring security. However, few are enabled to do so, or feel that it is someone else's responsibility.

Examples of user/stakeholder functions that are generally impacted by security decisions

All these enterprise functions need to access a variety of systems to accomplish their tasks. Some of these systems are managed by IT, some are managed by Corporate Security, and others are managed by Operations. The systems have been established over time to efficiently perform the tasks for which they are responsible.

While each function may perform their own prescribed set of tasks very well, the systems may not be designed to interact with each other, particularly with regard to how much access and authorization to give a particular employee or contractor. The most effective mechanism for managing these decisions is an integrated individual profile from which responsible managers can holistically determine the combined level of risk inherent in each employee's assigned access and authorization levels. For example, does the entire building access given to the customer service representative allow entry to server rooms or inventory storage areas? Does access to the customer database authorize the representative to download customer data to a hard drive or print hard copy? Shouldn't these levels of access and authorization be coordinated across functions to suit specific job requirements?

The most effective mechanism for managing these decisions is an integrated individual profile from which responsible managers can holistically determine the combined level of risk inherent in each employee's assigned access and authorization levels.

Examples of infrastructure systems and resources to which access is being requested

Obviously, someone that is a visitor to an organization is not going to get carte blanche access to all the areas inside the corporate facilities. Similarly, we do not want to grant contractors who are on short term assignments, permanent access to facilities. Since many organizations deal with these actions manually, the policies within the same company about who can access what types of systems or facilities often vary from site to site. Policies not applied uniformly lead to higher risk.

Physical Identity and Access Management (PIAM)

Physical Identity and Access Management (PIAM) software has evolved to resolve these issues, delivering a solution that address the entire extended enterprise.

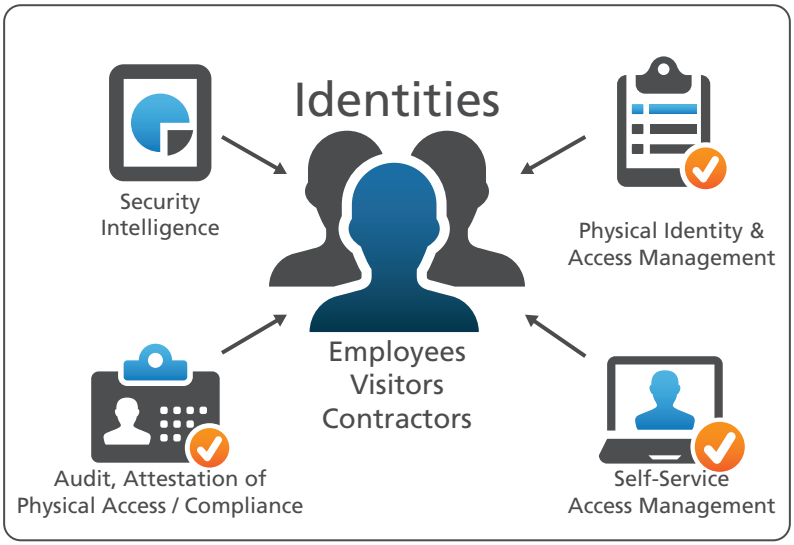


Figure 2 - update image
Physical Identity Management Software must deliver capabilities beyond just onboarding and offboarding

Modern and effective PIAM software must be comprised of four key building blocks:

- Basic PIAM Capabilities - Converged Logical-Physical Onboarding Offboarding
- Self-Service Access Request Handling – extending the capabilities across the enterprise
- Access Certification and Audit of Access Granted – Is it still relevant and still secure
- Identity Intelligence – learning access patterns over time and identifying anomalies

Basic PIAM Capabilities

Immediate benefits can be gained from linking the most obviously siloed sources of identity information. For example, connecting the Human Resources Management System (HR) with the Physical Access Control Systems (PACS) can deliver immediate integration value and allow managers to make more informed decisions related to the extent of facility or corporate access based on job role, function and relevance.

Another important opportunity is to link the Physical Access Control System with IT network directory structures that track who has access to corporate applications and resources such as network access, email, messaging, databases, etc. Some examples of these are LDAP – Lightweight Directory Access Protocol and AD - Active Directory. Creating this additional connection can deliver visibility into an individual's role in the organization, their job function, the amount of facility access they need to get their job done, and finally the amount of system or application access and authorization they need so that they can not only operate efficiently, but also adhere to security guidelines

Consider this authentic scenario. An insurance company employee enters the company facilities via the main lobby, takes the elevator to his floor and "badges in" to get access through the main door at that level. He then proceeds to his desk and signs into the company network to access his email etc. At the same time, someone else is using the same access credentials remotely via a VPN (Virtual Private Network) connection. Of course he cannot possibly be present locally and connected remotely at the same time. A converged PIAM can detect the external intrusion. The power of security convergence, is most evident with the realization that certain threats can only be detected when viewed across more than one domain (e.g. IT Security and Physical Security).

The old-fashioned practice of sending separate access requests to each department (e.g. IT Security and Physical Security), and then waiting for what seems like an eternity, before each department responds leads to dead periods during which productivity and planning are disrupted and security exists in limbo

Self Service Access Request Handling

The old-fashioned practice of sending separate access requests to each department (e.g. IT Security and Physical Security), and then waiting for what seems like an eternity, before each department responds leads to dead periods during which productivity and planning are disrupted and security exists in limbo. Sometimes requests for supporting information stay in those departments and never get back to the requestor creating additional delays. Self-Service capabilities distribute the tedious task of collecting the information related to the request back to the requestors. This ensures that all required information is collected. The requestor receives acknowledgement followed by confirmation and security functions can focus, instead, on assessing risk and closing security gaps. Automated workflow capabilities allow approving managers to get notified so they can quickly approve access and get their staff productive right away. Fast and secure.

Access Certification and Audit of Access Granted

The adage that the one constant you can count on is change, is particularly true when it comes to employees and contractors in the enterprise. It is important to review security prior to access being granted. However, it is equally important to ask the questions during all phases of the employee or contractor lifecycle. This is to ensure they still need the access previously requested and to validate that it is not in conflict with security policies.

Periodic access certification has been an audit mainstay in the IT application segment. This has not been the case when it comes to decisions regarding Physical Access Control. Access Certification in a converged context can be very helpful in deciding how much access and authorization to grant or how much access and authorization should be blocked to employees who have had job changes.

Identity Intelligence

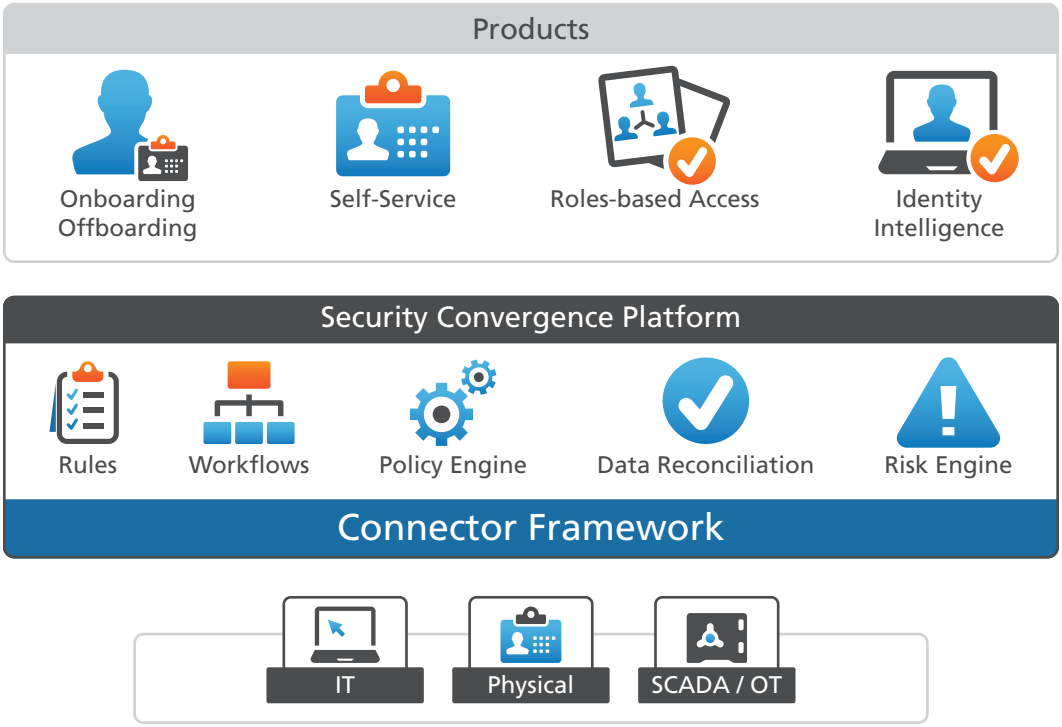
The combined categories of employees, contractors, vendors and visitors that have been granted access to the organization at any given instant in time make up the badged population. It is important for security managers to know how large the badged population is, what risks they pose to the enterprise and how to mitigate the risk.

Identity Intelligence software can rely on machine learning and the deployment of rules. For example, John Q is a control room worker who has been following a steady shift pattern of working Monday through Friday, nine to five. He suddenly starts showing up at midnight on a Saturday and uses his work badge to access a secure area. The deviation from the pattern of nine to five on weekdays and the exception to the rules that people with John's role should not be accessing a room that stores the critical assets sets off a series of alerts to various stakeholders including security personnel.

Tracking Non-Standard Behavior (NSB) delivers additional value-added capabilities like monitoring for insider threat, badge utilization, repeatedly violation of rules, and space utilization are all excellent reasons to deploy Identity Intelligence.

It is important for security managers to know how large the badged population is, what risks they pose to the enterprise and how to mitigate the risk

AlertEnterprise - Delivering the most innovative PIAM Solution



Guardian Physical PIAM Software Delivers IT-OT-Physical Security Convergence

AlertEnterprise has developed innovative software technology that incorporates all four of the described components of Physical Identity and Access Management. Guardian Physical™ from AlertEnterprise centralizes the administration and management of identities related to Employees, Contractors and Visitors within the enterprise and automatically links them to the Physical Access Control Systems. By combining the decisions on the amount of system access and authorization with the extent of physical area access improves security, reduces organizational risk and lowers the cost of operations for corporate and enterprise security. AlertEnterprise uniquely delivers this capability across IT, Physical Security and OT (Operational Technology that encompasses SCADA Industrial Control Systems as well).

Guardian Physical™ from AlertEnterprise centralizes the administration & management of identities related to Employees, Contractors and Visitors within the enterprise and automatically links them to the Physical Access Control Systems.

Seven Steps to an Effective PIAM Strategy

In addition to taking stock of all the existing applications and systems that need to be integrated, there is the organization challenge of bridging cultural gaps across various departmental entities within the same organization. Many of these entities, until now, did not have to consider the impact of security decisions on other departments.

AlertEnterprise has developed a seven-step approach to streamline the process of deploying Physical Identity and Access Management. Each step is a unique capability that differentiates AlertEnterprise from all other providers in the market.

The following outlines the seven step approach:

- Step 1: Use the most Streamlined IT-Physical Access Control Integration Solution
- Step 2: Extend Identity Management and Identity Governance beyond IT
- Step 3: Leverage Built-In Compliance and Active Policy Enforcement
- Step 4: Plan for Enterprise Scalability and Global Deployment
- Step 5: Enable IT-OT Convergence to Protect Critical Infrastructure
- Step 6: Build Risk Intelligence Right into Your Process
- Step 7: Select Cyber-Aware PIAM Software

A brief description of each step follows

STEP 1: Use the most Streamlined IT-Physical Access Control Integration Solution

The AlertEnterprise solution delivers a bundle of features that set us apart from other vendors. These features include a comprehensive Corporate Badging solution that leverages our dynamic connector framework for real-time integration with multiple Physical Access Control Systems (PACS) such as Lenel, Honeywell, Tyco Software House CCURE, AMAG, and many others. Additionally, full integration with IT applications from Microsoft, SAP, Oracle and many others delivers reliable and secure data transfer with HR, Identity Management, Directory Services (Active Directory, LDAP, etc.). OT integration enables access assignment and monitoring across various SCADA / Industrial Control Systems, providing complete IT-OT-Physical convergence.

AlertEnterprise also can provide full control of the target PACS systems including such actions as Create Badge, Disable Badge, Print Badge, and as well as badge design functionality. Additional capabilities of assigning roles-based area access and door-by-door access authorization, regardless of the PACS vendor make the AlertEnterprise PIAM a powerful tool for operational security.

AlertEnterprise PIAM capabilities include:

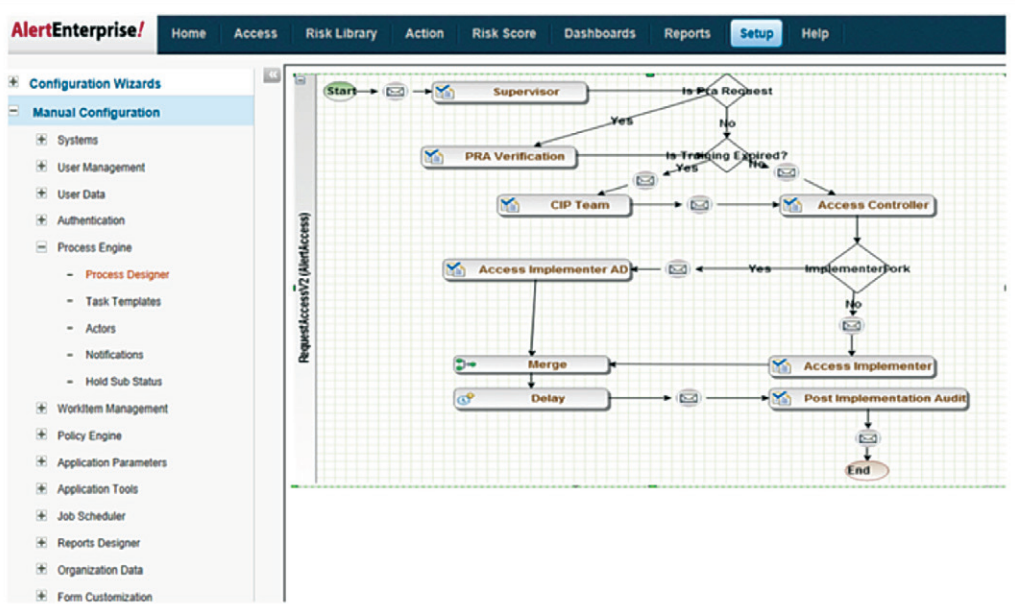
- Support for all major Access Control vendors
- Built-in integration with Directory Services like AD and LDAP
- Perfect integration with enterprise applications like HR, IAM and others

STEP 2: Extend Identity Management and Identity Governance beyond IT

AlertEnterprise enables corporations to manage identities for employees, contractors and visitors, while providing complete identity governance capabilities, together with management of IT and OT roles, and Physical Access Authorizations. A full identity lifecycle can be managed, along with role-based access assignments, workflow automation, access certifications and transaction authorizations. Unified "Area Administrator", User Self-Service and Delegated Administration views further enhance the feature set.

Key capabilities include:

- Common Identity for Logical and Physical identities
- Identity Lifecycle Management with Automated Workflow
- Access Certification and Authorization – Logical and Physical
- Contractor Management and Visitor Management Capabilities
- IT roles, OT roles and Physical Access Authorizations



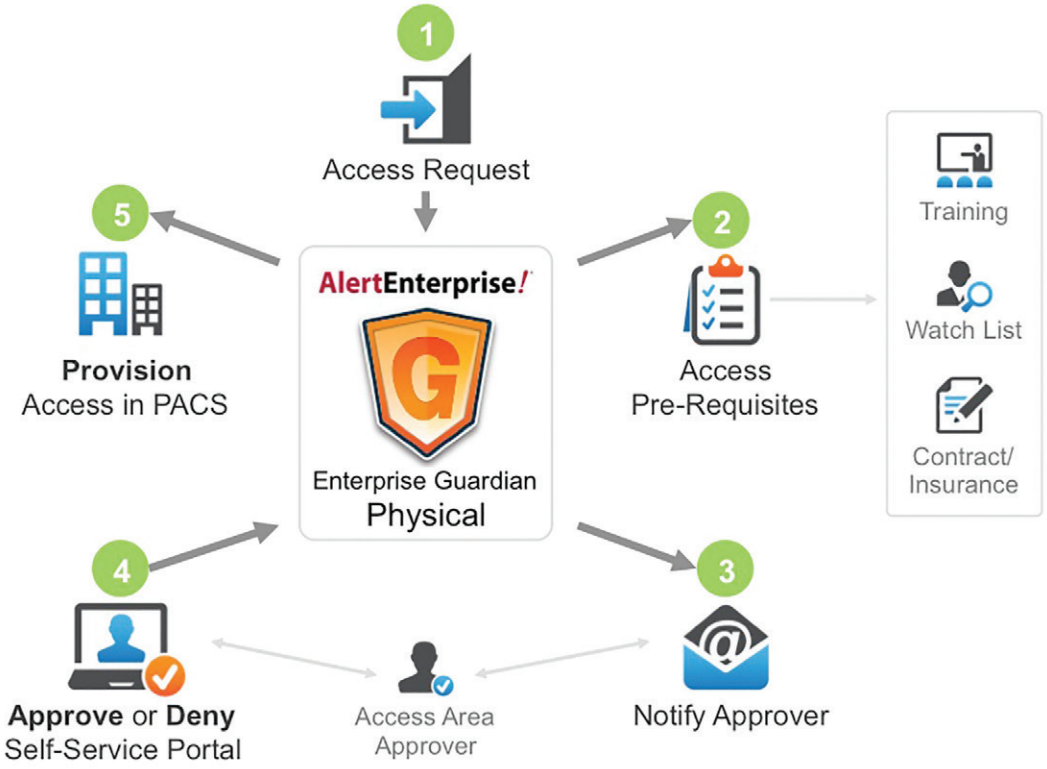
Automated Workflow allows security and departmental managers to quickly approve or deny requests while actively enforcing company policies

STEP 3: Leverage Built-In Compliance and Active Policy Enforcement

A built-in controls repository houses controls for compliance with multiple regulations and company policies. Automatic verification of training and background certification allows rules to be enforced. In the event requirements are not met, physical access can be automatically revoked. Compliance and Active Policy Enforcement features enable organizations to meet regulatory requirements easily. In addition, organizations can now easily enable roles-based and individual user-based access to critical assets based on user profile attributes.

Key capabilities include:

- Regulatory compliance requirements
- Validate Training and Certification Systems
- Roles-Based Access to Critical Assets – dynamic update upon role change



Automated notifications allows the software to ascertain if requested access meets regulatory compliance or company policy requirements, and then notify security managers.

STEP 4: Plan for Enterprise Scalability and Global Deployment

AlertEnterprise software solutions have been designed to scale to hundreds of thousands for users for large enterprises and government applications. A major government agency uses our software worldwide to globalize their deployment, cover eighteen time zones across the globe and unify security policies across 200 countries. Our solution is fully scalable, and supports geographically dispersed deployments.

High availability as well as enterprise fail-over and backup capabilities rely on the most flexible technology architecture for an enterprise-class platform. Database, operating system and other component technologies are interchangeable and can support specific requirements that organizations may choose mandate.

Key capabilities include:

- PACS Globalization
- Aggregated Reporting
- Powerful yet flexible technology platform

STEP 5: Enable IT-OT Convergence to Protect Critical Infrastructure

Recent incidents such as the Target Corporation data breach and the PG&E substation physical attack have underlined the need for holistic security to close the gaps between IT and physical security of critical assets. AlertEnterprise enables organizations to fully integrate their IT systems with OT, not only for unified provisioning but also for monitoring and correlation of blended threats. Through our solution, IT and OT administrators can easily define and enforce these policies.

AlertEnterprise enables organizations to fully integrate their IT systems with OT, not only for unified provisioning but also for monitoring and correlation of blended threats. Through our solution, IT and OT administrators can easily define and enforce these policies

AlertEnterprise delivers role-based and user-based access:

- Roles that should have corporate access and authorizations
- Roles that should have sensitive area access and authorizations
- Roles that have OT system Access – combined with IT Access

STEP 6: Build Risk Intelligence Right into Your Process

Purpose-built Risk Analytics and Risk Management features provide capabilities not available in traditional badging solutions. AlertEnterprise can leverage user attributes, access patterns, and policy violations to calculate risk scores for individual users. Our solution automatically detects anomalies and sends alerts on exceptions. Combined with customizable reports and dashboards, and a dynamic reports designer, enterprises can leverage this capability to address hard-to-find insider threat vectors and indicators of compromise.

Key capabilities include:

- Risk Scoring – attributes
- Access Behavior Monitoring - Anomaly Detection
- High Risk Individual Accessing High Risk area

STEP 7: Select Cyber-Aware PIAM Software

As organizations focus cybersecurity measures on protecting their network perimeters, attackers are starting to test new and previously untapped vulnerabilities in corporate armor. This often includes cyberattacks on Physical Access Control System components, and even video surveillance / CCTV systems. The next era of the hybrid attack is here and it is imperative to address the blended threats that exist across the silos of IT, OT (Operational Technology – SCADA, ICS and IoT) and Physical Security. Consequently, enterprises are increasingly concerned about their PACS being vulnerable to cyberattacks.

Key capabilities include: Enforcing best-practice cyber protection policies for the underlying computer systems that run the physical security automation systems

- Monitoring PACS privileged user or administrator activity
- Alerting on unauthorized configuration changes
- Alerting on creation of badges or identities in the PACS backend database bypassing standard procedures

AlertEnterprise can leverage user attributes, access patterns, and policy violations to calculate risk scores for individual users. Our solution automatically detects anomalies and sends alerts on exceptions

Additional Steps

Implementing a converged logical and physical security solution can be a complex task with many moving parts. It is important to select a solution that can address ALL of the seven steps outlined above. Having a solution that will scale to the needs of the enterprise is key to future proofing your security.

Key features

- Manage security risk to systems, facilities, areas, critical assets and people
- Establish an authoritative source for enterprise identities both LOGICAL and PHYSICAL
- Integrate and rationalize identities across HR, Directory Services and Badging Systems
- Map enterprise roles to physical area access and enforce policies
- Enable simultaneous common operation across PACS from multiple vendors

Benefits

- Eliminate gaps between logical and physical identities by establishing authoritative common identities
- Scale to meet enterprise needs across time zones and geographies
- Automate physical security controls required by various industry regulations
- Reduce cost and reduce risk by eliminating overlap of function
- Extend useful life of existing systems and enhancing overall security

Added Benefits - Enterprise Consolidation of Physical Access Control

Many large enterprises, multinational corporations and government institutions operate multiple facilities that include owned buildings, leased properties and plant operations that extend across cities, states and countries.

Many of these facilities operate Physical Access Control Systems that were procured over long periods of time, owned by landlords, or acquired as a result of company mergers.

Alert Enterprise's Guardian Physical solution establishes a common operating environment and extends all the benefits of common identity management across multiple PACS, buildings and geographies. It uniquely leverages all existing Access Control systems by accounting for limits on the number of users a system can support and by converting native systems to completely scalable enterprise systems with common provisioning and reporting across systems and multiple vendors.

About AlertEnterprise

AlertEnterprise, based in Silicon Valley, uniquely delivers Information Technology and Operational Technology (IT-OT) Convergence for Corporate and Critical Infrastructure protection. AlertEnterprise uniquely eliminates silos and uncovers blended threats across IT Security, Physical Access Controls and Industrial Control Systems for true prevention of insider threat, fraud, theft, sabotage and acts of terrorism. AlertEnterprise delivers Enterprise IAM, industry-specific Operational Compliance Management, as well as Situational Awareness with continuous monitoring and incident management for effective response to critical threats and protection of critical infrastructure for various sectors including pharmaceutical/healthcare, utilities, oil and gas, airports, federal agencies, and many other industries.

With the AlertEnterprise incident management capability, an organization is provided with complete situational intelligence so that seemingly innocent events when correlated across IT, physical and operational domains, can be simultaneously uncovered and resolved. With AlertEnterprise, organizations can leverage their existing IT systems, physical access control systems whilst managing security, risk and compliance for business applications, enhancing security and reducing risk from complex processes like onboarding and offboarding.

AlertEnterprise!
4350 Starboard Drive
Fremont, CA 94538
P: 510.440.0840
F: 510.440.0841
info@alertenterprise.com
www.alertenterprise.com