ALERTENTERPRISE

Use Case Scenarios for Finance Organizations.

Banks and financial institutions have sensitive information and assets associated with their customers, and any breach or lapse in security can be disastrous with revenue loss, higher operating costs and a damaged reputation heading the list of potentially negative consequences. These institutions are also subjected to industry regulations and oversight by government agencies which requires strict documentation and reporting standards.

AlertEnterprise delivers enterprise-wide security, governance, compliance, policy enforcement, automation and workforce management to the Financial sector in a single platform that makes physical and logical access and identity management a seamless part of business operations.

The AlertEnterprise Solution.

AlertEnterprise removes the complexity of integration across CRM, GRC, IAM and Security applications. We identify and uncover blended threats that exist across IT applications, Physical Access Control Systems, and Industrial Controls to deliver holistic prevention of fraud, theft and acts of sabotage. With the suite of solutions, organizations can achieve:

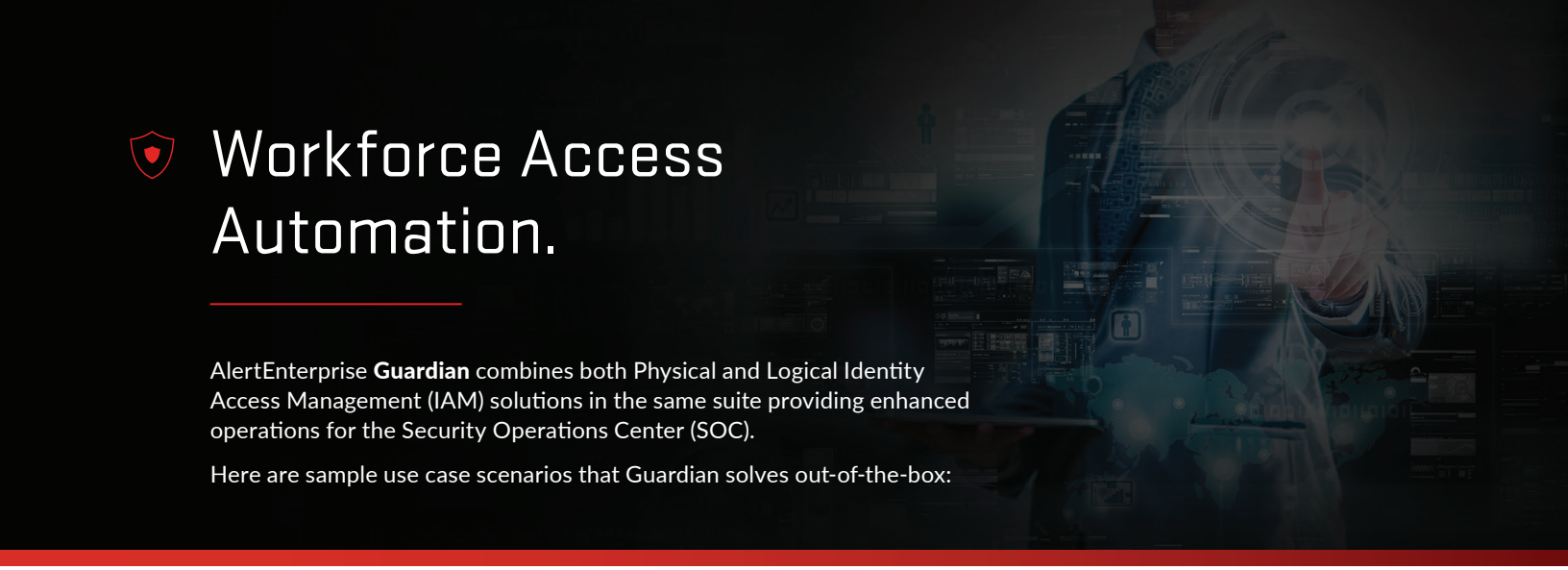
- Highly flexible governance platform to manage employees, contractors and visitors for IT, Physical and OT access
- Mapping of critical and cyber assets to IT security controls and Physical Access Control Systems (PACS)
- Powerful data modelling to bring to light potential compliance violations and control system risks, as well as IT security gaps, before a potential security violation
- Adherence regulations and automate controls for NIST, ISO/IEC 27001, SOX and data privacy needs
- Elevated critical business processes around identity and access management/governance in an integrated solution
- Implement a single solution for cross platform provisioning of access with converged physical and logical systems

Challenges.

The following are the most common challenges faced by Finance institutions:

- Tedious onboarding process leading to delayed access provisioning on day one
- Lack of automation resulting in manual and late termination, which leads to orphaned access and active unused cards
- Alarms fatigue and noise around false positives and duplicate events
- Access authorizations lack automated workflows leading to SOD violations, unauthorized access, and unrevoked access credentials
- Inefficient security policy enforcement and regulatory controls leading to poor audit quality and missed timelines
- Lack of segregation of duties resulting in access abuse and security loopholes
- Vulnerability to insider threats by both current and disgruntled users with no audit trail or security reviews
- Visitor management fails to provide timely service and smooth check-in experience impacting customer satisfaction
- Multiple parts of the organization (IT, HR, Learning Management System, etc.) are either siloed or fragmented, creating communication gaps

Workforce Access Automation.



AlertEnterprise **Guardian** combines both Physical and Logical Identity Access Management (IAM) solutions in the same suite providing enhanced operations for the Security Operations Center (SOC).

Here are sample use case scenarios that Guardian solves out-of-the-box:

Automated Onboarding and Offboarding.

Real-time integration of Enterprise Guardian with leading HR systems allows Supervisors/HR or Security Administrators to trigger a new Identity creation process (as part of onboarding) and auto-provisioning of access levels based on their role, location and access policies.

Similarly, the HR/Admins can initiate a "User Termination" workflow as part of the employee offboarding process. This triggers automated removal of identities and access levels across all connected systems.

Access Management.

Guardian integrates across various enterprise applications, physical facilities and critical assets. This empowers the system users and managers to view/request access for themselves or others in the organization, and audit if the same access was granted via an established standard.

Admins/Users can create a new request (via a self-service portal) to add/remove specific access, either for themselves or others. These requests are sent for single or multi-step approval and auto-provisioning (once approved) based on the security needs. Contractor user access review is performed on a quarterly basis or as required by compliance. Guardian can be configured to deactivate a badge after a configurable number of days of inactivity.

Asset Governance.

The Guardian platform provides Asset Inventory Management for various asset types like metal keys, gate openers or other high valued assets, that can be assigned to individual employees.

The self-service portal (with SSO/AD) is fully capable of requesting assets, and the necessary approval process can be configured to record approvals and the chain-of-custody, end-to-end lifecycle of these assets.

Report Generation.

Multiple compliance standards require both physical and logical access to be reviewed every 90 days. AlertEnterprise Guardian is capable of generating reports required for periodic reviews (daily, weekly, monthly, etc.) and ad-hoc reviews consisting of identities that are active, inactive and pending for approval, training, etc.

Guardian integrates with other IT, HR, Cybersecurity, Learning Management and Ticket Management systems to generate reports that provide a unified view of threats across the enterprise, and deploy rules-based solutions to prevent malicious acts, sabotage, terrorism and cyber threats.

Anomaly Detection with AI.

Guardian tracks employees' requests to access a new facility or area for themselves or another person, which enables the security personnel to correlate staff entry into sensitive locations with business reasons and prior access patterns.

AI-powered anomaly detection, like a badge swipe at off-shift hours, piggybacking and multiple access denied attempts, can be enabled for critical resources to reduce the risk from insiders. By enabling convergence between physical and logical security systems, the solution can gather and provide security intelligence from a number of sources and systems.

The AI policy engine also helps in detecting noise/duplicate alarms and provides only the qualified alarms for security teams to address. The alarm response dashboard can be an external application like ServiceNow, Splunk or others. The connector framework will help push these qualified alarms to any system.

Enforcement of Compliance Standards.

Finance institutions must adhere to a gold standard audit for SOX and access security. Guardian integration with compliance applications, like SAP GRC, makes the audit easier and follows the required process for FDIC adherence, including background checks on identities at set intervals.

Similar governance can be performed on a need basis for contractors or temporary employees, with automatic alerts sent when there is a change in status for individuals, the ability to track the approvals and revocations.

For access requests and approvals, Guardian automatically checks security policies and documents compliance with requirements that verify who approved access to which facilities and for what duration of time. It also enforces the Segregation of Duties (SOD) which avoids access requests being self-approved.

Syncing Across Multiple PACS.

Guardian connects with multiple Physical Access Control Systems (PACS) to manage physical access to critical facilities - from one place. It takes the guesswork out of approving access to physical locations or applications based on specific roles within the organization.

This enables the security staff to remove physical access to systems and facilities with a single click and invoke mitigating controls like additional video surveillance or proximity tracking.

Visitor Management System.

AlertEnterprise Visitor Management System (VMS) provides Corporate Security with enhanced control of visitor access and enforces security standards. All of the platform features related to workflow, notification, compliance and PACS integration, are available for visitor scenarios as well.

Following are the common use-cases which are available out-of-the-box:

Streamline Visitor Registration Process.

The VMS can be deployed as a Kiosk (self-service) or Lobby (managed service) setup. The visitor registration process can be streamlined by providing a pre-registration workflow and enhanced by integrating with local or federal banned lists.

Access points are managed and locations are secured in a granular manner using a centralized management process. The solution provides front desk and security teams with streamlined, robust and secure processes for validating a visitor's identity.

Audit All Visitor Logs.

The VMS maintains logs that report on who visited a facility, who approved their visit, how long they stayed and which areas within the facility visitors were allowed to access. This provides the ability to conduct an audit and enhance search capabilities.

Establish Visitor Escort Compliance Requirements.

VMS enforces strict compliance standards when the visitor is requesting access to critical facilities. The access request form lists the expected time to check out as a mandatory field.

The solution triggers escalation emails when the visitor is not checked out after a certain number of hours (configurable). If the visitor is not checked out after 24 hours (configurable), VMS triggers an email to ESOC.

Automate Background Checks.

Upon visitor registration, VMS performs an automated background check, using the visitor's ID or driver's license information, against a set of watch lists (BOLO, do-not-enter, etc.).

Identify and Notify All Visitors in the Facility.

The VMS solution provides a single interface for accurately identifying all the visitors in a facility and notifying them in-case of an emergency. This offers a holistic view of building occupancy at any given time.

How AlertEnterprise Leverages Technology So Finance Organizations Can Maintain Continuous Compliance.

- Extends access management and risk analysis beyond IT applications to include physical access control systems
- Creates a unified access and reporting mechanism across applications in all domains (IT, Physical Access Control Systems/ SCADA)
- Establishes an all-encompassing strategy for onboarding/offboarding related to access management, managing contractor access as well as validation of certification and background checks
- Offers holistic business alignment for security risk and compliance posture alignment

ALERTENTERPRISE

SOLUTIONSHEET | ALERTENTERPRISE.COM