ALERTENTERPRISE

Use Case Scenarios for Utility Corporations.

Utilities are critical infrastructures with complex security requirements. New sophisticated threats that live in both cyber and physical domains stand poised and ready to attack, with potential ongoing risk to IT, Operational Technology (OT), and Physical Security.

AlertEnterprise delivers enterprise-wide security, governance, compliance, policy enforcement, automation and workforce management to the Utility and Critical Infrastructure sectors 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 ERP, 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 our suite of solutions, organizations can achieve:

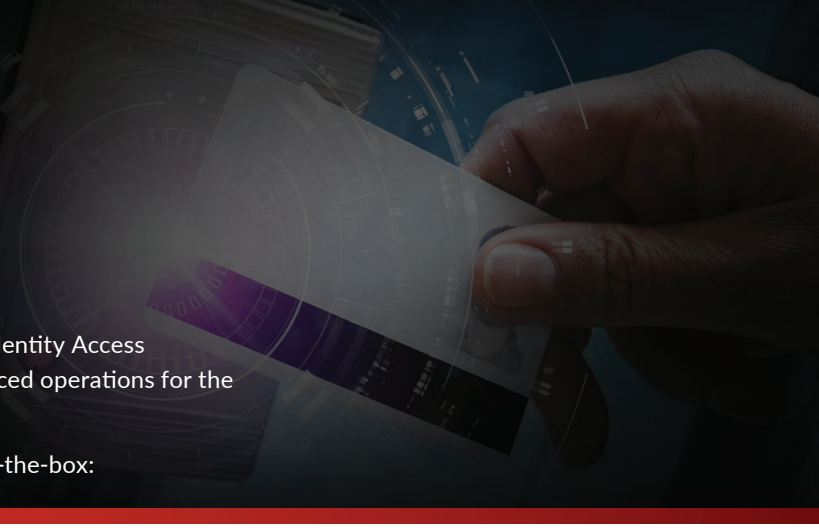
- Highly flexible governance platform to manage employees, contractors and visitors for IT, Physical and OT access
- Mapping of critical and cyber assets to IT security controls and Physical Access Control Systems (PACS)
- Powerful data modelling to bring to light potential compliance violations and control system risks, as well as IT security gaps before a potential NERC violation
- Automation of assessments for NERC-CIP, NIST SP 800-53, ISO 27000, SOX and other regulations
- Elevated critical business processes around identity and access management/governance in an integrated solution
- Implement a single solution for cross-platform provisioning of access, and a solid pathway to staying CIP compliant with converged physical and logical systems

Challenges.

Following are the most common challenges faced by Utilities providers:

- Disjointed manual processes to assign and monitor building access to its most high-risk areas, including generation and transmission
- Reliance on hand-tracked authorizations and periodic access reviews – on massive spreadsheets – for CIP compliance
- No assurance of immediate access removal for employee/contractors at termination
- Tracking expired NERC CIP trainings and ensuring access is removed instantly, to stay in compliance
- Ensuring unused contractor badges are terminated to avoid misuse
- The manual contractor onboarding process takes too much time and is error prone
- There isn't a good process to manage metal keys and their approvals

Badge and Access Management.



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 Building Access from Hire-to-Retire.

Real-time integration of 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 Policies.

The transfer and job change events are also automated and access is adjusted per the new job profile.

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 (NERC CIP & non-CIP) and critical assets (BES & BCSI), which empowers the system users and managers to view/request additional access for themselves or others as required. Once the access is requested, the configurable workflow helps to capture necessary approvals electronically and once approved, the access is auto-provisioned in the PACS.

Guardian can be configured to deactivate a badge after a configurable number of days of inactivity. Users can request activation via a self-service portal when needed.

Guardian also natively integrates with ServiceNow ticket management systems to automate building access tickets as required.

Contractor / Temp-Worker Management.

AlertEnterprise Guardian provides an automated workflow to onboard a contractor including necessary approvals, background checks and badge issuance and printing.

Guardian provides all necessary controls for cardholders including defining supervisor, unique contractor numbers, access approvals and regular periodic audits. The contractor's badges get automatically deactivated on termination, contract expiry or inactivity.

Anomaly Detection.

Guardian monitors all Operational Systems (Energy Management Systems, Transmission Systems, Protective Relays, etc.) which enables the security personnel to correlate staff entry into sensitive locations with work-order issuance and prior access patterns.

AI-powered anomaly detection, like badge swipe at off-shift hours, piggybacking, and multiple access denied attempts, can be enabled for critical resources to reduce the risk from insiders.

Automated Periodic Access Review (Report Generation).

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.

A built-in Periodic Access Review process allows Area Owners and Manager/Supervisors to review their employees/contractors and assigned access areas on a periodic basis. Once the access is approved or denied, Guardian instantly provisions the change in the PACS system and maintains complete audit of the review decisions and changes made in the user's access.

Guardian integrates with 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.

Enforcement of NERC CIP Compliance Standards.

Guardian integrates with compliance applications like SAP GRC to include monitoring of NERC and NERC CIP controls, as well as state or local Public Utility Commission guidelines.

Guardian actively performs weekly configurable analysis of training/certification data, from Learning Management systems, to identify users whose certification has either expired or will expire within a specified number of days. This triggers an automatic notification sent to the identified users and the CIP manager.

Similarly, the solution performs scheduled checks/real time policy enforcement of Personal Risk Assessment (PRA) information and identifies users whose PRAs will expire within a configurable, specified number of days. This triggers an automatic notification sent to the identified users and HR/Security Admins to take necessary action.

Syncing Across Multiple PACS.

Guardian connects with multiple Physical Access Control Systems (PACS) to manage physical access to facilities, substations, control rooms and power generation stations - 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.

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 which allows the hosts to notify visitors to provide the required information for access to critical sites.

Audit All Visitor Logs.

The VMS maintains the logs of all the visitors entering and exiting both NERC and non-NERC facilities. This provides the ability to conduct an audit of the logs and enhance search capabilities. Per NERC CIP compliance standards, the visitor logs must be retained for at least 14 months from the date of access.

Establish Visitor Escort Compliance Requirements.

VMS enforces NERC CIP compliance standards when the visitor is requesting access to NERC facilities. The solution checks for the NERC escorts and their certification and PRA status. The access request form lists the expected time to check out as a mandatory field, in addition to other fields that are listed as mandatory in NERC logbook.

The solution triggers escalation emails to escort a visitor 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 Visitor Screening.

Upon visitor registration, the VMS performs an automated background check, using the visitor's ID or driver's license information, against a set of watch lists, including among others BOLO and do-not-enter. If access is requested for NERC sites, the solution will also check for the required certification and PRA prior to granting access.

The automated check can also be made against Federal Crime History, terrorism watch list, etc.

Identify and Notify All Visitors in the Facility.

The VMS provides a single interface for accurately identifying all the visitors in a facility and notifying them in case of an emergency.

How AlertEnterprise Leverages Technology So Utilities 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

TO LEARN MORE, PLEASE REFERENCE THESE ADDITIONAL RESOURCES:

- AlertEnterprise Security Convergence for Utilities
- NIST National Cybersecurity Center of Excellence IAM Utilities Guide
- Security Convergence for Utilities & Critical Infrastructures
- Cyber-Physical Security Considerations for the Electricity Sub-Sector

ALERTENTERPRISE

SOLUTIONSHEET | ALERTENTERPRISE.COM