Alert Enterprise

Guardian PIAM for the Utilities Industry.

A GEN AI-powered enterprise-wide solution.

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.

Any breach or lapse in security governance, risk and compliance can be disastrous with potential loss of life, contracts, and revenue; as well as negative public perception, legal implications and even an impact on share value.

Alert Enterprise Guardian delivers GEN AI-powered enterprise-wide security, governance, compliance, policy enforcement, automation, and workforce management to the Utility and Critical Infrastructure sectors in a single platform. This makes physical and logical access and identity management a seamless part of business operations.

Key Challenges Faced by Utilities.

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 on NERC CIP trainings and ensuring access is removed instantly in order 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

Multiple access control, IT, HR, and Learning Management **Systems applications that don't talk to each other**

Decentralized Physical Access Control Systems **(PACS)**, with limited integration

Separate processes to assign and monitor access to its most delicate, high-risk areas, including generation and transmission

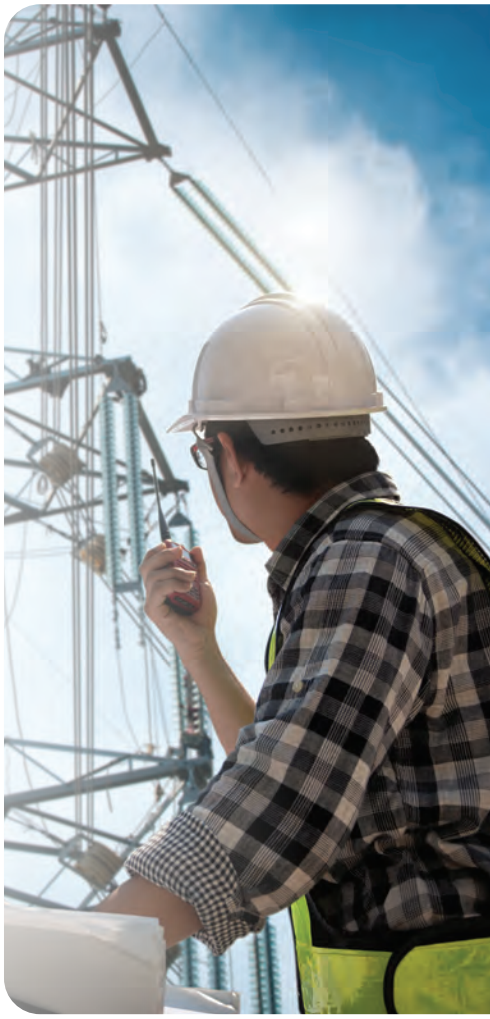
Large volumes of access **authorizations are conducted through email exchange,** leading to delays in authorizations, provisioning errors, and unrevoked access credentials

CONTACT US | LEARN MORE

The Alert Enterprise Solution.

Guardian for Utilities

Our Guardian solution 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.



- A 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
- Implementation of a single solution for cross-platform provisioning of access, and a solid pathway to staying CIP compliant with converged physical and logical systems

Measuring Your Return on Investment with Guardian.

75%+
of identity and access tickets processed can be automated

20%
Average Workforce Productivity Gain

MILLIONS
in Annual Total Savings/Cost Recovery

These figures are based on annual projections from an Alert Enterprise customer with 30,000+ employees.

CONTACT US | LEARN MORE

How Guardian Helps with NERC CIP Compliance.

CIP-001: Sabotage Reporting.

- **Correlation:** actively enforce sabotage procedures by intelligently connecting underlying physical and logical systems
- **Response:** act on single event or correlation of events that match sabotage characteristics through strict triggers and/or identification of abnormal events
- **SOC:** Security Operations Center interface to view events directly via live and archived video feeds, as well as monitoring the alarming condition across enterprise systems

CIP-002: Critical Cyber Asset Identification.

- Asset repository with configurable custom attributes to classify assets by types
- Asset workflow to trigger a request/approval and review processes on periodic basis by an asset owner
- Assets grouping by department or location for easy reporting
- Automated reconciliation from multiple source systems to help create and maintain asset catalogs on an automated basis

CIP-003: Security Management Controls.

- Policy and rule catalog to create policies around identities, systems, places or assets
- Automatic policy evaluation on a periodic basis
- Policy violation detected: automated workflows triggered with required notification and end-to-end audit

Guardian

NERC CIP COMPLIANCE

CIP-004: Personnel and Training.

- Training:
  - Check and approval before granting critical access
  - Expiry notification, access removal for expired training
- Background check validation for Temp worker access to critical locations

CIP-006: Physical Security of Critical Cyber Assets.

- Remove unwanted access during transfer or location changes by automating review
- Periodic Access Review for critical access by managers/area owners, auto access removal for denied access
- Immediate badge deactivation during HR termination or HOT termination
- Implement “Use it or Lose it” policies - auto badge deactivation if not used in 90 days
- Auto remove expired access / badges from cardholders
- Complete end-to-end audit for all actions, including: badge issuance, printing, access approvals, access review, etc.

CIP-008: Incident Reporting and Response Planning.

- Translate large volumes of operational procedures information into event detection, pattern and anomaly recognition, and automatic scripted response actions
- Combine physical and logical events to correlate events and respond in unison to eliminate threats from multiple threat vectors
- Initiate sabotage reporting (CIP-001), system restorations, and activate cyber asset recovery plans
- Decrease response time and increase operational uptime

Badge and Access Management.

Alert Enterprise **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 Supervisor/HR or Security Administrators to trigger a new Identity creation process (as part of onboarding) and auto-provisioing 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.

Contractor/Temp-Worker Management.

Alert Enterprise 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.

The Guardian solution 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 offshift 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 Managment 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 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.

Alert Enterprise's 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 solution can be deployed as a Kiosk (selfservice) 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 solution 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.

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.

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 Watchlist, etc.

Establish Visitor Escort Compliance Requirements.

The VMS solution 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.

Compliance for Visitors.

In addition, Guardian PIAM delivers a seamless visitor management solution that revolutionizes the visitors experience for the Utilities industry.

- Workflow approval before granting critical site access
- Configurable workflow and notification, UI forms, badge template, and report & dashboard engine with auto report dispatch
- Necessary training validation
- Mandatory escort check-in with badge swipe
- Maximum number of visitors per escort
- Highlight and notify overstayed visitors
- Federal Criminal History and Watchlist check
- Auto ID verification at kiosk check-in
- Visitors tracking with Smart Badge
- Emergency notifications to checked-in visitors

CONTACT US | LEARN MORE

Customer Success Stories.

Northern Indiana Public Service Company (NIPSCO)

The Power of Automation.

With over 1.2 million customers and nearly 3,000 employees, Northern Indiana Public Service Company (NIPSCO) is one of Indiana's largest natural gas and electric organizations. Once inundated with error-prone, manual processes, this critical infrastructure organization needed an access control solution that could mitigate system inaccuracies, automate training, manage badging and improve auditing and reporting.

As the industry shifts from fossil fuels to renewable resources, utility organizations like NIPSCO are also expanding their physical footprint to accommodate remote stations – necessitating the demand for a united, enterprise-wide system.

Solution Chosen: Guardian PIAM.

With the Alert Enterprise Guardian Physical Identity and Access Management (PIAM) system, NIPSCO was able to move from manual to automated processes. Today, NIPSCO uses Guardian for badge management, access control, yearly training automation and maintaining CIP compliance.

Key Takeaways.

Guardian has helped streamline NIPSCO's access control and badging processes. Before implementation, new employees had to wait a couple of weeks to gain access to company facilities. With Guardian, they're granted immediate access to the places they need to be – and that access can be removed as quickly as it's given.

It has also helped significantly with regular auditing and reporting.

"The last few audits have done very, very well and Alert Enterprise has been a big part of that success story," said Jim Schmidt, CIP Compliance Systems Engineer for NIPSCO. "Our goal is to always have zero violations and we're very close to that. A lot of that success is due to Alert Enterprise."

> "The last few audits have done very, very well and Alert Enterprise has been a big part of that success story. Our goal is to always have zero violations and we're very close to that."
>
> **Jim Schmidt**
> **CIP Compliance Systems Engineer**
> **NIPSCO**

Customer Success Stories.

TXNM Energy
(formerly PNM Resources)

Compliance is Key.

TXNM Energy (formerly PNM Resources) has unique challenges exclusive to critical infrastructures, particularly when it comes to its diverse set of facilities that span both IT (company headquarters, administrative offices, etc.) and OT (industrial control facilities, substations, etc.).

Like other utility organizations, TXNM Energy is also heavily regulated by the North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP) standards. NERC CIP audits PNM Resources every three years, according to Gary Todd, Associate Director, Cyber Security, "If there's even one instance of noncompliance during that period, you don't pass. At a certain point, it became very clear that we needed to have automated access control."

Solution Chosen: Guardian PIAM.

After integrating with the organization's Active Directory, the Alert Enterprise Guardian Physical Identity and Access Management (PIAM) system enabled more efficient, secure access control across the entire organization. Automating processes also made it easier to meet CIP's strict compliance requirements.

Key Takeaways.

Because of their significance and connections within the critical infrastructure network, electric utility organizations are especially vulnerable to attacks – making the need for a strong physical access system paramount.

"With the substation attacks that were in the news this year and last year, physical access has taken on a whole new importance in our industry and will continue to be important," Todd said.

For TXNM Energy, the integration with Guardian has transformed manual, error-prone processes into smoother, automated systems that became a natural part of business.

"Not only did it help our security, but it changed the dynamic from the manual phone call / email process and the individual heroics that typically happen."

> "With the substation attacks that were in the news this year and last year, physical access has taken on a whole new importance in our industry and will continue to be important. Not only did Guardian PIAM help our security, it changed the dynamic from a manual phone call / email process and the individual heroics that typically happen."
>
> **Gary Todd**
> **Associate Director, Cyber Security**
> **TXNM Energy**

CONTACT US | LEARN MORE

Alert Enterprise

How Alert Enterprise 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

CONTACT US | LEARN MORE

© 2024 Alert Enterprise Inc. All rights reserved. Alert Enterprise, Guardian are trademarks of Alert Enterprise Inc. Other names and logos mentioned herein may be the trademarks of their respective owners.