ALERTENTERPRISE

WHITEPAPER

How a Major Utility Company Achieved Zero Compliance Violations

[1+1+1 = 0]

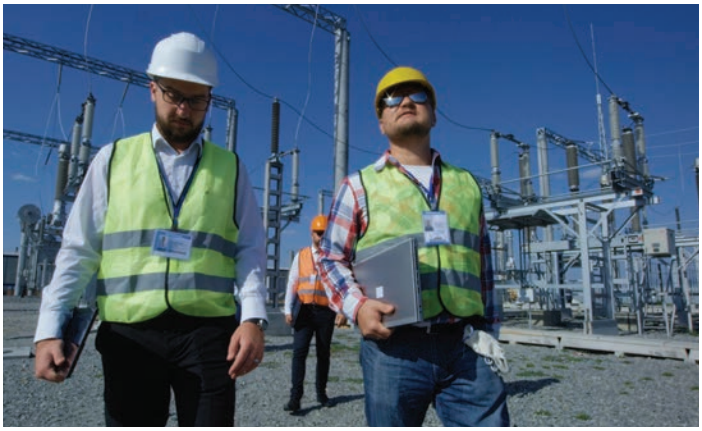
CONVERGING IT, OT AND PHYSICAL SECURITY FOR CONTINUOUS NERC-CIP COMPLIANCE AND ENTERPRISE SECURITY.

More than a decade ago, the North American Electric Reliability Corporation (NERC) approved Critical Infrastructure Protection (CIP) standards CIP-001 through CIP-009, designed to provide new and improved regulatory accountability. NERC-CIP basically carries two primary purposes. The first is to provide a cyber-security framework to identify critical cyber assets and the second is to protect those assets. Critical assets, as defined by the standards, are those systems, equipment or facilities that if affected by destruction or otherwise would be detrimental to the reliability or operability of the Bulk Electric System (BES). For companies in the public utility, gas, water and other critical sectors, staying current with regulations and recordkeeping for safety, security and access has been an insurmountable challenge to overcome. Since the mandate hit the books, companies have struggled with compliance—many failing to resolve how to effectively comply with the three most critical areas of the NERC-CIP standards: CIP-001 (Sabotage Reporting), CIP-002 (Critical Cyber Asset Identification) and CIP-004 (Insider Threat).

AlertEnterprise Inc. has successfully worked with companies across the utility and critical infrastructure spectrum to address and resolve all areas of NERC-CIP compliance. The following is a current, real-world example of how technology helped one of our high-profile customers achieve the ultimate goal: continuous compliance and zero violations.

The Utility Customer Profile

With thousands of natural gas and electric customers spread across almost one third-of the state, the Utility understood the risk of data theft and NERC-imposed fines. Their goal was to unify its enterprise Identity and Access Management (IAM) to meet NERC-CIP requirements, with an integrated access and reporting mechanism across IT, Physical Access and Control Systems/SCADA). The Utility approached the potential pain points of NERC-CIP head on—access to physical and logical systems; controls; documentation; onboarding, off-boarding, terminations; and more—using AlertEnterprise technology to automate compliance and bridge the gap between physical and logical systems.



Since working with AlertEnterprise, the Utility company has obtained continuous compliance and zero violations—an attainable and sustainable goal—all with a unified enterprise IAM software platform.

Challenges of the Utility Customer

The client had these familiar challenges:

- *Multiple access control, IT, HR and Learning Management Systems applications that didn't talk to each other*
- *Decentralized Physical Access Control Systems (PACS), some legacy, with limited integration*
- *Separate processes to assign and monitor access to its most delicate, high-risk areas, including generation and transmission*
- *Mounting access authorizations conducted through email exchange, leading to delays in authorizations, provisioning errors and unrevoked access credentials*
- *Reliance on hand-tracked authorizations—on massive spreadsheets—for CIP compliance*

As you could imagine, or have experienced, CIP compliance tasks were becoming unmanageable for the Utility company, and it was difficult to perform quarterly access reviews. Manual access checks were spotty and tedious and 24-hour revocation became a concern, as well as establishing good internal controls by personnel to revoke access.

Technology from AlertEnterprise Automates Compliance

With a vision of centralized access, the Utility customer turned to AlertEnterprise and its proven IAM solutions. They successfully centralized management of all identity lifecycle for employees and contractors; established a central identity repository for contractors; and increased user access management functionality and credential levels through a single platform. They were able to achieve this vision:

- *Elevate critical business processes around identity and access management/governance in an integrated solution*
- *Attain the highest levels of compliance with audit/ regulatory and reporting requirements holistically*
- *Drive the entire access management equation to end-to-end automation and integration*
- *Implement a single solution for cross platform provisioning of access and a solid pathway to staying CIP compliant with converged physical and logical systems*

To safeguard vulnerabilities in an entity's systems requires an automated risk management solution, especially as regulations continue to develop. The expansion of NERC compliance monitoring self-certifications, audits and spot-checks continue to grow in size and scope. Along with this expansion, we've continued to observe an increase in the amount of documentation required by NERC-CIP. Utilities are far from mastering these requirements and struggle to do so with traditional compliance methods, especially with newly proposed NERC-CIP standards on track for approval in 2020.

AlertEnterprise Delivers

- *Highly flexible governance platform to manage employee, contractors and visitors for IT, Physical and OT access*
- *Mapping of critical and cyber assets to IT security controls and PACS*
- *Powerful data modeling 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 SP800-53, ISO 27000, SOX and other regulations*

About AlertEnterprise

AlertEnterprise hides 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.

The AlertEnterprise Suite of Solutions

- Enterprise Guardian - Physical Identity and Access Management Software
- Enterprise Visitor Identity Management Software
- Enterprise Sentry - Cyber|Physical|OT Unified Security
- Identity Intelligence Technology

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 on-boarding/off-boarding 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

What Utilities Need to Know

The key mandates of NERC-CIP require a deep understanding of risk to critical assets, in addition to effective and continual monitoring of access. A simple mistake in understanding monitoring of access has resulted in millions of dollars in theft, in addition to NERC and FERC imposed fines. If you require any information on this topic, contact AlertEnterprise today at ***510.440.0840*** *or* ***info@alertenterprise.com****.*

ALERTENTERPRISE