



CASE STUDY

Texas's leading electric cooperative achieves NERC-CIP compliance using Securden Unified PAM

The largest electric cooperative in Texas, United States, deploys Securden Unified PAM to achieve robust access control for critical infrastructure, granular application control on endpoints, and automated service accounts management.

Company Profile

Based in Texas, this electric cooperative is one of the largest and oldest organizations specializing in power transmission and distribution, serving over 60 counties across the state. With more than 16 member organizations, the cooperative is responsible for supplying wholesale power to its member-owned distributors.

60+

COUNTIES SERVED

16+

MEMBER ORGANIZATIONS

Quick facts

INDUSTRY

Energy

LOCATION

Texas, USA

CHALLENGES FACED

- NERC-CIP compliance requirements
- Uncontrolled use of administrative rights
- Unexpected downtime caused by inefficient management of service accounts.
- Error prone and time intensive manual password management.

THE SOLUTION

Securden Unified PAM

RESULTS

- Demonstrated NERC-CIP compliance
- Eliminated admin rights from endpoints
- Enforced the principle of least privilege
- Streamlined privileged access
- Automated password management
- Improved helpdesk efficiency
- Eliminated unnecessary downtime



Committed to customer satisfaction, safety, and excellence, the cooperative strives to provide reliable service to all its customers.

The Challenge

The Texan electric cooperative works with the energy grid and handles numerous Information Technology (IT) and Operational Technology (OT) assets. These IT and OT systems are essential for the cooperative's business-critical operations. Member organizations control their OT machinery using their IT systems, for authentication.

Apart from service accounts, their IT systems contain other sensitive data and information like certificates, and admin account credentials that are spread across servers, and databases.

The North American Electric Reliability Corporation (NERC) classifies these cyber systems as part of the bulk electric systems (BES), along with the OT machinery. Given the nature of their work, the cooperative was required to ensure compliance with the NERC Critical Infrastructure Protection (CIP) standards.

The NERC-CIP guidelines establish strict standards for managing cyber systems, including tight access controls for critical systems, a robust electronic

security perimeter, configuration change management, and information protection.

The electric cooperative aimed to remove admin rights on endpoints to prevent users from making configuration changes to bulk electric systems. By controlling which applications users can run with admin rights, they can regulate who is authorized to make changes to configurations within the organization.

In addition to removing local administrator rights and managing application access privileges, NERC-CIP emphasizes the importance of enforcing password security measures, including automated password rotation throughout the organization for enhanced access control and management.

The co-operative was relying on manual password resets that proved unreliable from time to time.

“Periodic password changes were breaking things like services here and there. Rotating the password of service accounts was extremely stressful,”

VICE PRESIDENT OF INFORMATION SERVICES

The password changes for the service account were not properly propagated to dependent services, resulting in a stoppage of services. This often proved costly for the power distribution company that relies on the seamless functioning of its internal services.

The IT team also noticed a lack of visibility regarding the usage of admin privileges within their organization.

A comprehensive log that tracks 'who' performed 'what' actions and 'when' would offer essential oversight on privileged access.

“The lack of visibility into the use of admin rights and the access history of critical IT systems was hindering our progress with NERC-CIP. We expected the PAM solution to address this issue as well,”

VICE PRESIDENT OF INFORMATION SERVICES

With clear goals related to access controls, identity security, and restricting admin privileges, the IT team of the cooperative the cooperative's IT team began searching for an appropriate privileged access security solution.

Finding the Right Solution

When the IT team started looking for a PAM solution, they had list of critical considerations:

- ✓ Effective management of service accounts and their dependencies
- ✓ Eliminating local admin rights and enforcing just-in-time privilege elevation with robust application controls
- ✓ Complete activity tracking with clear and concise reporting for demonstrating compliance with NERC-CIP
- ✓ A scalable and robust PAM solution that can effectively manage their complex network of IT and OT devices while ensuring a quick implementation time.

Keeping these requirements in mind, the IT admin team started searching for a suitable PAM solution. When they found Securden Unified PAM, the IT team felt that it could potentially solve all their access governance problems.

The IT team at the electric co-operative was primarily looking for a solution to reliably manage privileged

access and eliminate admin rights to demonstrate compliance with NERC-CIP regulations. They discovered Securden Unified PAM, which offered a way to address their issues with unreliable service account password resets and streamline privileged access management.

“Instead of going with a separate solution for eliminating admin rights and a PAM solution, we decided to go with Securden Unified PAM, which has all the features to solve our problems and then some more,”

VICE PRESIDENT OF INFORMATION SERVICES

The Securden difference

With Securden, the energy co-operative transformed privileged access governance across all its member organizations and demonstrated compliance with NERC-CIP regulations.

After implementing Securden Unified PAM, the organization noticed significant improvements in privileged access security, operational efficiency, and the ability to achieve and demonstrate compliance.

1 Robust Security

Securden Unified PAM enabled the co-operative to adopt secure, just-in-time remote access to IT assets, enforce best practices for password management, and implement multi-factor authentication. As a result, the energy co-operative significantly enhanced their overall cybersecurity posture.

“We were struggling with manual processes for access management and activity tracking. With Securden's PAM solution, we (IT team) were able to automate password management, control remote access, and improve the overall security of the organization,”

VICE PRESIDENT OF INFORMATION SERVICES

2 Improved Operational Efficiency & Productivity

Automated periodic password resets, dependency management, dynamic application control policies, and role-based access control have significantly improved the operational efficiency and productivity of the energy cooperative. Securden assisted the IT team in achieving greater efficiency by eliminating redundant and repetitive manual tasks through effective automation.

3 Achieve and Demonstrate Compliance

Securden Unified PAM provided important security controls that helped them demonstrate compliance with NERC-CIP regulatory requirements such as:

- ✓ Data encryption when stationary and when in-transit
- ✓ Implementing password security best practices
- ✓ Enforcing the principle of least privilege
- ✓ Secure remote access for internal users and third parties
- ✓ MFA for remote access to bulk electric systems
- ✓ Separation of administrative duties and change management
- ✓ Revoking access permissions from leaving employees
- ✓ Granting and revoking access privileges based on job roles
- ✓ Activity tracking and access history of bulk electric systems

With dependable password rotation and effective dependency management, Securden assisted the energy co-operative in streamlining their IT and OT communication. By implementing automation and workflows to replace manual tasks, Securden enhanced the efficiency of the IT helpdesk and minimized the potential for human errors. Additionally, the comprehensive reporting features provided by Securden Unified PAM enabled the IT team to easily demonstrate compliance with NERC-CIP requirements.

“Securden made it incredibly easy to demonstrate compliance with specific NERC-CIP requirements,”

VICE PRESIDENT OF INFORMATION SERVICES

4 Complete Control over Admin Rights

Using Securden their IT team was able to eliminate and restrict admin rights from user accounts in the organization. They successfully enforced application access controls through policies. With control over admin rights and application access, the IT team was able to restrict users from performing administrative changes and control 'who' has the permissions to run 'what' applications and with 'what' privileges, achieving change management.

5 Enhanced Visibility

Securden Unified PAM records every activity related to privileged access as audit trails. The IT administrator can export meaningful reports that can provide visibility over privileged access and use of admin rights to the IT administrator. The IT administrator made use of these reports to create better control policies which helped improve the operational efficiency of the entire workforce, creating a workflow for continuous optimization.

After using the product extensively, the electric co-operative is very satisfied with the capabilities and reliability provided by Unified PAM. They plan to expand its usage across their member organizations soon.

“Securden is stable, better priced, and has more features than most of the solutions available in the market.”

VICE PRESIDENT OF INFORMATION SERVICES

60+

COUNTIES SERVED

16+

MEMBER ORGANIZATIONS

NERC-CIP

DEMONSTRATED

0

ADMIN RIGHTS ON
ENDPOINTS

“

Securden's product and services are very good. The pricing is very affordable for a solid product that is scalable for small companies to very large enterprises. Their support has been really great, from evaluation till now.

VICE PRESIDENT OF INFORMATION SERVICES



About Securden

Securden is a leading provider of privileged access governance solutions that holistically combines the principle of least privilege with other critical security principles such as zero-trust and provide visibility into privileged activities to continuously monitor cyber risk to effectively prevent cyberattacks, malware & ransomware propagation, and insider exploitation.

With simplicity and robustness in its core design, Securden offers a refreshing and intuitive panel of controls to govern privileged access across cloud, physical, and virtual environments.

Here is a quick list of Securden's offerings:

- Password Vault for Enterprises
- Endpoint Privilege Manager
- Vendor Privileged Access Management
- Unified PAM
- UnifiedPAM forMSPs

The products have been built to be extremely scalable and secure. Securden is trusted by small businesses and large enterprises such as large banking and financial services, manufacturing companies, government agencies, healthcare organizations, managed IT service providers, educational institutions, and security service provider. To learn more, visit www.securden.com

Achieving NERC-CIP compliance using Securden Unified PAM

The largest electric cooperative in Texas, United States, deploys Securden Unified PAM to achieve robust access control for critical infrastructure.

[REQUEST A DEMO](#)