



Utility Protects Servers and Data with Access Management

This major South Western Electric & Power Company serves more than 375,000 customers. As the electric and power provider enters its third century of operations, the company continues to find innovative ways to provide reliability, service and value to customers and the community.

CASE STUDY

The Business Challenge

A component of delivering reliable service includes ensuring security over the systems that manage energy. Several years ago, the utility company's Energy Management Services (EMS) group determined that they needed to ensure access controls to the servers that housed core applications and other sensitive data. The security of these applications and data were needed to not only reduce the risk of a security breach, but also as part of achieving FERC and NERC regulatory compliance, specifically around the Cyber Security Standards (CIP). In particular, the IT team wanted to enforce, down to the individual user level, exactly who was authorized to access which systems, when, and how, especially for privileged system users, such as system and database administrators. They also needed a much easier way to consolidate logs of the user access activity for management review and regulatory audits.

Effective Access Control

Like most IT environments, this utility provider uses a diverse mixture of both UNIX and Windows servers to run their business. Defining, managing, and enforcing authentication and authorization rules, automatically, across diverse IT platforms, located across multiple geographic locations, is a challenge. As well, manually provisioning new user entitlements to the various servers and removing the entitlements when they leave is time consuming and error prone.

An equally daunting access management challenge comes via the FERC and NERC regulations, specifically CIP-003 R5, CIP-005 R2, and CIP-007 R5. The intent of the NERC CIP Cyber Security Standards is to ensure that all entities responsible for the reliability of the Bulk Electric Systems in North America identify and protect Critical Cyber Assets that control or could impact the reliability of the Bulk Electric Systems.

To meet the CIPs compliance standards, organization must be able to prove that they have the controls in place for authorizing access by individuals to their servers. In particular, organizations need to focus on managing access to shared accounts (CIP-007, R5.2) Under CIPs, the organization is also required to provide an audit trail of the account usage, and must review the user activity logs at set intervals during the year.

Manual controls may be utilized in some cases, but it is very labor intensive to effectively manage and enforce these controls and create meaningful audit reports with the user activity logs decentralized across the various servers.



About FoxT

FoxT protects corporate assets with an enterprise access management solution that centrally enforces granular access entitlements, in real-time, across operating systems and business applications on any networked device. The ability to proactively administer, authenticate, authorize, and audit access across diverse platforms, down to the file and device level, enables organizations to greatly reduce compliance and audit costs, streamline IT security administration, and protect corporate value by mitigating the risk of insider fraud. Headquartered in Mountain View, California, FoxT serves Global 1000 customers in 32 countries. For more information - www.foxt.com or email sales@foxt.com.

Securing the IT Infrastructure

In 2007, the electric and power utility company decided to implement FoxT ServerControl solution to centralize the administration, authentication, authorization, and auditing of their access policies across their UNIX servers. Later, the organization added FoxT to their Windows servers to further centralize control over security policies. Interestingly, the system was actually implemented prior to the CIPS regulation, as a means to ensure security over their key energy management systems.

The FoxT solution is implemented to protect servers both in the Corporate and Energy Management Services business units.

The FoxT solution provides many benefits to the utility provider including:

- Ability to define and automatically enforce granular authorization and authentication access rights to improve security over sensitive data and applications; accounts are defined only on servers where they are needed.
- Simplifies overall IT management with consistent user roles, authorization, and authentication mechanisms across diverse servers
- Reduces the risk of insider fraud with controlled delegation of privileged accounts including keystroke logging
- Protects data in transit with encryption of network communications
- Simplifies NERC/CIPS regulatory compliance. The FoxT solution automatically consolidates the user activity logs from across the diverse servers and produces a variety of audit-friendly reports. The consolidated reporting also enables management to perform the required reviews of access controls and user activities much faster.
- Reduces the IT administration effort with centralized
 - System administrator provisioning & de-provisioning
 - Password management
 - SSH management

Summary

Using the FoxT solution, the South Western Electric and Power organization is able to improve the security of the servers that drive their core applications with centralized administration, authentication, authorization and audit capabilities. The ability to automatically control access across their diverse server domain not only provides greater protection of their corporate brand and equity, it also enables the utility provider to meet the CIPS standards with in the NERC regulations. With a centralized solution for administering their granular access control policies, the company is also able to reduce the effort it takes to both provision users and prepare for internal and regulatory audits, reducing the overall cost to manage IT systems.