NEXTLABS

SOLUTION BRIEF

NERC and FERC Cyber Security

Identify, control and audit the flow of critical cyber assets, to ensure confidentiality and demonstrate NERC and FERC compliance

SOLUTION HIGHLIGHTS

- Identify over- or under-privileged cyber assets, to help organizations tighten security over critical functions or data.
- Protect information, policies and procedures associated with critical cyber assets, by identifying and implementing electronic access controls.
- Continuously monitor electronic access to critical cyber assets.
- Automate information-handling procedures to protect information assets by reducing user errors and compliance violations.
- Create an information security barrier around critical cyber assets with broad communication control across e-mail, voice, and video communications.

OVERVIEW

The NERC (North American Electric Reliability Corporation) is a self-regulatory body responsible for ensuring energy industry compliance with Critical Infrastructure Protection (CIP) standards. These rules require organizations that deliver bulk electricity to the North American electrical power grid ("Responsible Entities") to identify and protect critical cyber assets. FERC (Federal Energy Regulatory Commission) oversees the power industry, but gives NERC the responsibility for maintaining and complying with CIP standards.

Bulk power suppliers must define methods, processes, and procedures for securing critical cyber assets, as well as the non-critical cyber assets within the electronic security perimeter. "Cyber assets" are loosely defined as all "programmable electronic devices and communication networks including hardware, software, and data.

THE SOLUTION

NextLabs' NERC Cyber-security Compliance Solution provides persistent protection and reporting over critical information asset access and usage to support NERC-CIP compliance.

The solution provides integrated data protection combining a suite of applications with a compre-hensive set of best practice policy libraries and reports required to support NERC-CIP and FERC requirements. Policy sets can be easily customized to the environment or used as templates to create new policies.

The solution combines multi-channel communications control, information rights management, virtual information barriers, and host-based data loss prevention technologies with application, document, and device control capability. It performs real-time policy evaluation on or off the network. This comprehensive approach improves compliance and mitigates information risk.

A set of unique integrated user assistants can alert and educate end-users of any risky information activities, and support CIP training requirements by guiding them toward safe information handling procedures. Policy Assistants automate many tasks like encryption, tagging, & approval, ensuring safe handling and compliance. This is the only available solution that controls information sharing across communication, and collaboration channels.

The solution protects the critical infrastructure of the Responsible Entity while ensuring safe internal and external collaboration among employees by automating safe handling of critical information assets, and ensuring proper access to and protection of critical applications and data. It scales to meet the information. protection requirements for Responsible Entities and integrates seamlessly with Supervisory Control and Data Acquisition systems and all applications. It is easy to use and maintain.

Requirements Addressed by NextLabs'Compliance Solution for NERC-CIP

NERC-CIP RELIABILITY STANDARD	REQUIREMENTS
CIP-002-1 Identification of Critical Cyber Assets	R1 Critical Asset Identification Method
	R2 Critical Asset Identification
	R3 Critical Cyber Asset Identification
CIP-002-1 Security Management Controls	R1 Cyber Security Policy
	R3 Exceptions
	R4 Information Protection
	R5 Access Control
	R6 Change Control & Configuration Management
CIP-004-1 Personnel and Training	R1 – R4
CIP-005-1 Electronic Security Perimeter	**R1** Electronic Perimeters
	R2 Electronic Access Controls
	R3 Monitoring Electronic Access
	R4 Cyber Vulnerability Assessment
	R5 Doc Review & Maintenance
CIP-007-1 Systems Security Management	**R1** Test Procedures
	R2 Ports and Services
	R3 Security Patch Mgmt
	R4 Malicious Software Prevention
	R5 Account Management
	R6 Security Status Monitoring
	R7 Disposal or Deployment
	R8 Cyber Vulnerability Assessment
	R9 Doc Review & Maintenance
CIP-008-1 Incident Reporting & Response Planning	**R1** Cyber Security Incident Response Plan
	R2 Cyber Security Incident Documentation
CIP-008-1 Recovery Plans for Critical Cyber Assets	**R4** Backup and Restore
	R5 Testing Backup Media

Proactive Remediation without Costly Administrator Support

When the risk of a policy violation occurs, e-mail users are automatically prompted to take action to fix the error, in real time, with all activity logged for central auditing. IT administrators are not required to understand each user's intent or authorized recipients for resolution.

Automated Workflow to Reduce Risks

Pre-built Policy Assistants integrate transparently at the desktop to alert and educate users of policy violations, highlight errors, and provide remediation that prevents data loss, without slowing productivity.

Companies can now optimize productivity with safe e-mail communications while avoiding data loss or inadvertent disclosures that damage business integrity, and compromise client confidence.

THE SOLUTION INCLUDES BEST PRACTICE POLICY APPLICATIONS

The solution includes a comprehensive set of best practice policy libraries and reports required to support NERC and FERC require-ments. The solution can:

Assessments and Identification

- Analyze information risk based on industry best practices, regulatory requirements, access, and activity data, to identify high risks to prioritize and focus remediation projects.
- Identify over- or under-privileged cyber assets, to tighten security over critical functions or data.

Monitoring and Enforcing Security over Cyber Assets

- Protect information, policies, and procedures associated with critical cyber assets, by identifying and implementing electronic access controls within the electronic security perimeter.

Monitor electronic access to critical Cyber Assets

- Prevent insider data loss in real-time on endpoints, servers, and mobile devices, to help end users protect data and eliminate manual remediation.
- Automate information-handling procedures to protect information assets by reducing user errors and compliance violations.
- Controlling who can communicate with whom and what data can be sent to which partner or customer.

Managing, Reporting and Documenting of Cyber Assets

- Centralize management of fine-grained role or rule-based authorization based on policy to manage authorizations across multiple application data and cyber assets.
- Report on remediation of policy violations in the access or use of cyber assets, to support documen-tation of incidents.

- Analyze access and usage of data and applications across systems, and use reporting tools to simplify incident investigation and document policies and procedures

SOLUTION DEPLOYMENT: HOW TO GET STARTED TODAY

NextLabs implements the Solution by using expert product knowledge and a services best practices methodology. NextLabs can also assist clients with identifying their controlled data, as well as defining information control policies.

Step 1: Requirements Gathering

NextLabs works with you to understand your infrastructure, and security and policy requirements.

Step 2: Risk Assessment

We help you to discover and identify your current risks to help prioritize Solution requirements.

Step 3: Policy Configuration

Policies are designed and electronically codified using NextLabs' suite of Information Risk Management software, along with any custom Policy Assistant automation.

Step 4: Install Policy Enforcers

Policy Enforcers are deployed across applications and systems, if applicable to requirements.

Step 5: Knowledge Transfer

NextLabs will conduct knowledge transfer training to ensure your team possesses the expertise to appropriately maintain and manage the solution.

ABOUT NEXTLABS

NextLabs®, Inc. provides data-centric security software to protect business critical data and applications. Our patented dynamic authorization technology and industry leading attribute-based policy platform helps enterprises identify and protect sensitive data, monitor and control access to the data, and prevent regulatory violations – whether in the cloud or on premises. The software automates enforcement of security controls and compliance policies to enable secure information sharing across the extended enterprise. NextLabs has some of the largest global enterprises as customers and has strategic relationships with industry leaders such as SAP, Siemens, Microsoft, and IBM. For more information on NextLabs, please visit http://www.nextlabs.com.

NEXTLABS