Enhancing NERC CIP Compliance with FileSure Defend

Introduction

As cyber threats against critical infrastructure intensify, regulatory bodies like the North American Electric Reliability Corporation (NERC) have established the Critical Infrastructure Protection (CIP) standards to safeguard the Bulk Electric System (BES) from evolving risks. These standards focus on key areas such as access control, perimeter security, incident response, and the protection of sensitive data.

FileSure Defend offers a robust security solution that provides kernel-level file auditing and protection. FileSure Defend operates outside the Windows security model and independently of native-Windows file access controls. This means that FileSure Defend can block file operations that would otherwise be allowed —even those initiated by administrators— effectively preventing ransomware and malware attacks. FileSure Defend provides an unprecedented degree of file access control. For example, FileSure Defend rules can allow specific users or groups to view files while preventing those files from being copied, renamed or deleted, and it will log any attempts to perform unauthorized file operations.

Importantly, NERC CIP focuses on monitoring critical cyber assets and security-relevant activities and does not require the auditing of all system files. FileSure Defend allows selectively auditing and protection of files essential to **NERC CIP** compliance, without overwhelming audit logs with unnecessary records.

By operating with its own rules model, FileSure Defend significantly enhances compliance with key NERC CIP standards.

NERC CIP Overview

NERC CIP standards create a comprehensive framework to secure the BES against cyber threats, making strict adherence crucial for operators of critical infrastructure. Failure to comply with NERC CIP standards can result not only in damages by bad actors, but also in substantial fines and penalties. FileSure Defend provides significant capability for protecting critical cyber assets required to comply with these NERC CIP standards: **CIP-003**, **CIP-004**, **CIP-005**, **CIP-007, CIP-010**, **CIP-011**, and **CIP-013**.

How FileSure Defend Supports NERC CIP Compliance

FileSure Defend goes well beyond native-Windows file access control and auditing mechanisms by offering granular rule-setting and providing comprehensive self-auditing features. FileSure Defend helps organizations meet the following key NERC CIP standards.

1. CIP-003: Security Management Controls

Purpose: To establish and maintain security management roles and responsibilities for protecting cyber assets.

How FileSure Defend Helps:
FileSure Defend allows organizations to explicitly define access control policies within its own console, independent of Windows rights management. This provides granular control over file access, ensuring that only authorized users have access to critical BES Cyber System Information (BCSI). Additionally, every policy change is recorded in FileSure Defend's internal audit log, creating a transparent history of access control adjustments.

By offering customizable access control mechanisms and maintaining detailed records of all policy changes, FileSure Defend supports compliance with CIP-003, ensuring that security management controls are well-documented and easily auditable.

2. CIP-004: Personnel & Training

Purpose: To ensure that only authorized, trained personnel have access to BES Cyber Systems.

How FileSure Defend Helps:
FileSure Defend's independence from native-Windows file auditing means that access control is centrally managed within its console, giving organizations direct oversight of who can access critical files. This enables compliance with CIP-004 by ensuring that only trained, authorized personnel are granted access to BES Cyber Systems.

In addition to controlling access, FileSure Defend's comprehensive audit logging tracks every action taken by personnel, recording both successful and failed attempts to access or modify files. This complete audit trail provides a clear record for compliance verification and post-incident analysis, demonstrating that access was permitted only to authorized individuals.

3. CIP-005: Electronic Security Perimeter

Purpose: To secure the electronic perimeter around critical cyber systems and ensure controlled access to BES Cyber Systems.

How FileSure Defend Helps:
FileSure Defend enables real-time monitoring and auditing of all file access events within the electronic security perimeter. By independently tracking file access attempts—both successful and unsuccessful—FileSure Defend ensures that unauthorized personnel cannot access critical systems, providing an additional layer of defense against potential breaches.

FileSure Defend enforces explicit access policies defined within its own console, outside the Windows security model. This allows for more secure and flexible management of access to critical cyber assets. All access events and policy changes are logged in FileSure Defend's internal audit system, providing a detailed record for post-event analysis and compliance reporting, which is essential for demonstrating compliance with CIP-005.

4. CIP-007: System Security Management

Purpose: To ensure secure configurations, patch management, and vulnerability mitigation.

How FileSure Defend Helps:
FileSure Defend's kernel-level control allows it to block file operations that would otherwise be allowed under Windows—preventing ransomware or malware attacks, even when initiated by administrators. This capability greatly enhances system security and prevents unauthorized file modifications.

By enforcing file access policies at the kernel level, FileSure ensures that unauthorized users cannot modify or access critical system files. It also logs and audits all file and system changes, supporting compliance with patch management and configuration requirements under CIP-007.

5. CIP-010: Configuration Change Management and Vulnerability Assessments

Purpose: To ensure that configuration changes are properly tracked and vulnerabilities are assessed regularly.

How FileSure Defend Helps:
FileSure records every configuration change in real-time, maintaining a complete and accurate audit trail of file and system modifications. This helps organizations comply with CIP-010 by preventing unauthorized changes and enabling prompt responses to potential vulnerabilities.

By continuously auditing and protecting critical files and configurations, FileSure supports ongoing vulnerability assessments, ensuring that potential risks are identified and mitigated before they can impact the BES.

6. CIP-011: Information Protection

Purpose: To protect the confidentiality, integrity, and availability of BES Cyber System Information (BCSI).

How FileSure Defend Helps:
FileSure's access control mechanisms, which operate independently of Windows, ensure that only authorized personnel can access or modify sensitive BCSI. By monitoring and logging all access attempts, FileSure creates a complete audit trail, demonstrating compliance with CIP-011's information protection requirements.

7. CIP-013: Supply Chain Risk Management

Purpose: To manage the risks introduced by third-party vendors and external software or services.

How FileSure Defend Helps:
FileSure provides visibility into file changes made by third-party vendors or software, tracking all modifications in its audit log. This helps organizations detect and prevent unauthorized or malicious changes introduced through the supply chain. Additionally, FileSure blocks unauthorized executables from being written to the system, minimizing the risk of supply chain vulnerabilities.

Protecting Audit Logs: An Essential Component of Compliance

A critical aspect of NERC CIP compliance is the protection of audit logs themselves. These logs provide essential evidence of security events, access attempts, and configuration changes—making them a target for tampering. If audit logs are altered or deleted, it can compromise the organization's ability to prove compliance, detect incidents, or respond effectively.

FileSure Defend enhances compliance by protecting both the audit logs and the console used to manage policies:

- **Access Control for the Console**: FileSure Defend allows organizations to control access to its console using its own rules model, ensuring that only authorized personnel can view or modify security policies, logs, or settings. This prevents unauthorized users from tampering with critical configurations or accessing sensitive data.
- **Protection of Audit Logs**: FileSure Defend can protect access to its audit logs, ensuring that they remain secure from unauthorized access or modification. By leveraging explicit access rules, only designated personnel can access the logs, and any attempts to alter or delete these logs can be blocked and recorded. This ensures that audit trails remain intact and tamper-proof, providing a reliable and verifiable record for compliance audits.

The ability to protect both the security console and audit logs helps organizations ensure the integrity and reliability of their logging systems, a crucial aspect of demonstrating compliance with NERC CIP standards.

Conclusion

As cyber threats continue to evolve, critical infrastructure operators must stay ahead by adhering to stringent NERC CIP standards. FileSure Defend provides robust, independent file auditing, monitoring, and access control mechanisms that strengthen compliance across multiple CIP standards, including CIP-003, CIP-004, CIP-005, CIP-007, CIP-010, CIP-011, and CIP-013.

By offering comprehensive auditing, real-time monitoring, the ability to block ransomware or malware—even malware introduced by administrators—and customizable access controls, FileSure Defend helps organizations protect critical systems and maintain compliance with the highest cybersecurity standards. For more information on how FileSure Defend can support your NERC CIP compliance efforts, contact us today.