FORTRA™

The Tripwire NERC CIP Solution Suite

A Tailored Suite of Products and Services to Automate NERC CIP Compliance

The North American Electric Reliability Corporation (NERC) maintains comprehensive reliability standards that define requirements for planning and operating the bulk electric system (BES). Among these are the Critical Infrastructure Protection (CIP) Cyber Security Standards, which specify a minimum set of controls and processes for power generation and transmission companies to follow to ensure the reliability and security of the North American power grid.

NERC registered entities need to be audit-ready at all times and must determine how to best address the frequently changing standard requirements. At the same time, the time-consuming, complex task of meeting NERC CIP compliance must not distract IT, Compliance and Operations staff from their primary focus: ensuring the reliability of the BES. Fortra's Tripwire NERC CIP Solution Suite helps meet those demands with a tailored package of products and expertise.

The top priority for those working in the power industry has always been reliability. However, with cyber incidents on the rise, the security of IT assets, along with OT assets as part of industrial control systems (ICS) on which the bulk electricity system depends, has become critical because a cybersecurity incident can result in loss of reliability and impact physical safety. Thus, Tripwire has the ability to manage both IT and OT assets as part of a more comprehensive NERC CIP cybersecurity program.

> *"We've been able to stay focused on our mission of delivering reliable energy and still achieve our NERC CIP compliance requirements through the use of Tripwire's tailored NERC CIP Solution Suite. They are committed to understanding our issues and have saved us incredible amounts of time and real dollars as well."*
>
> **—Southwestern US Energy Holding Company**

NERC CIP compliance requires registered entities to establish a set of controls and processes, continuously monitor those processes, and produce detailed evidence of these activities in an audit. But the cost of findings in an audit can be significant—in recent years, non-compliant registered entities have been assessed fines totaling over $150 million. Equally concerning is that such non-compliance leaves utilities more exposed to cyberattacks and more likely to experience service disruptions—putting the entire power grid at risk. The most drastic and recent example of which include Russia's use of Industroyer2 malware and BlackEnergy to dismantle Ukrainian substations and put Ukrainians in the dark.

The Tripwire NERC CIP Solution Suite helps registered entities pass their audit today and be more prepared for tomorrow's. Power companies can efficiently and confidently protect their assets from potential threats—malicious or unintended—and maintain reliability and compliance through:

- Continuous monitoring to continuously collect detailed status information on all your critical cyber assets and immediately detect any changes.

- Situational awareness to automatically aggregate and analyze your security data and alert on suspicious events or modifications that impact your compliance status.

- Risk management and efficient response through asset tag management to flexibly and easily tag your critical assets based on Impact Rating, associated BES System, Role, Owner, Location, etc., and have them automatically inherit the appropriate security control and classifications (e.g., daily vs. monthly scans, patch validation workflows, account enforcement policies, etc.).

- Audit-ready evidence to quickly generate reports and dashboards that fully document your compliance with security controls and processes by CIP requirements.

- Network visibility via active and passive means to identify not only the critical infrastructure assets being protected but potential threats that are acting maliciously or anomalously.

- Network defenses and remote access by synthesizing technologies from our partners. Tripwire is uniquely positioned to provide an end-to-cloud set of capabilities that enable deep packet inspection and blocking and secure remote access for difficult to visit infrastructure.

What is the Tripwire NERC CIP Solution Suite?

The Tripwire NERC CIP Solution Suite offers electric utilities a tailored package that helps automate and simplify NERC CIP compliance. It supplements standard Tripwire products with NERC CIP-specific extensions and content that includes tailored reports, dashboards, correlation rules, scripts, utilities, tools, and templates. Experienced NERC CIP consultants then deliver process assistance and training to help the power company reduce the amount of time and effort required to achieve compliance.

While the complete NERC CIP Solution Suite uses the functionality of Tripwire® Enterprise for Industrial Devices, Tripwire's Allowlisting solutions, Tripwire LogCenter®, Tripwire IP360™ and Tripwire's industrial visibility integrations, customers don't need all of these products to benefit from

the solution. Additionally, Tripwire can integrate with various third-party patch management, log management, SIEM, and GRC products that provide alerting and incident workflow.

Tripwire Enterprise for Industrial Devices

Tripwire Enterprise for Industrial Devices offers an industry-leading security configuration management (SCM) solution that automatically assesses, detects and assists in correcting file and configuration changes across critical IT and OT infrastructure to ensure NERC CIP compliance.

With Tripwire Enterprise, customers receive:

- Comprehensive change auditing that provides proof of changes with before and after images.

- Continuous monitoring of configuration hardening requirements to achieve and maintain compliance and strengthen assets for resilience to performance degradation and attack.

- Customized reports and dashboards grouped by NERC CIP requirement to document compliance and provide operational control.

- Tailored monitoring rules, which are selected based on the customer, provide the evidence to auditors that the standard requires—for example, active users and groups, installed applications, and password policies.

- Broad support for critical cyber assets, including file systems, applications, network devices, SCADA devices, HMI/RTU controllers and badge entry systems.
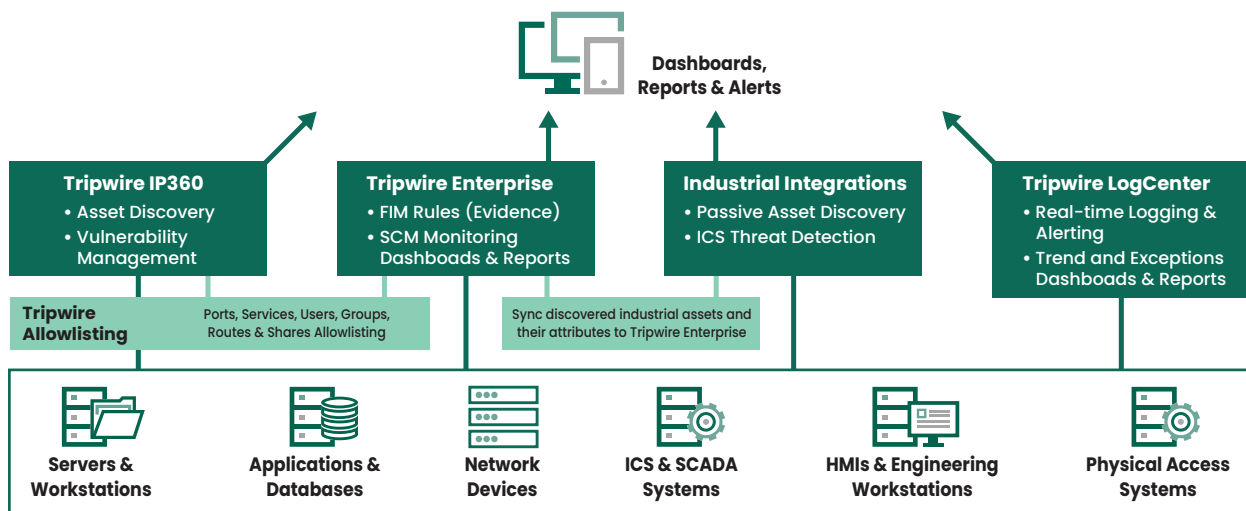
- Integrations into leading patch and update management tools and services and workflow management software, such SigmaFlow, that are optimized to help address the stringent requirements of NERC CIP standard 007-6-R2 Security Patch Management. Tripwire Enterprise Commander also offers a consistent, flexible and reliable way to retrieve rich information from Tripwire Enterprise.

Tripwire's Allowlisting Solutions

Allowlisting of baselines is an essential focus in any OT environment. With Tripwire's solutions, it automatically monitors changes being made across your network of devices, assets, and equipment. It also maintains a detailed history of these changes, reporting the "who" responsible for the change along with the "why." Reports listing these changes are then made available for your review in an easy to use interface.

Customers receive:

- A complete history of all changes made across customers' entire network.

- Granular details of each change, including the who, what, when, and why

- Automated generation of compliance reports

- Allowlist profiling that automates validation of system settings, including ports/services, local user accounts and software versions, on a per-device basis. For example, customers can ensure that only authorized network ports are in use on specific systems or that revoked user accounts are removed from critical systems.

- NERC CIP configuration policy tests that provide continuous awareness of compliance across a broad range of CIP requirements and significantly reduce the burden of preparing for an audit. They also provide relevant security and configuration information to operations staff—for example, where antivirus software or system logging have been disabled.

- Direct addressal of several NERC CIP requirements:

  - CIP-007 R1: The solution monitors the state of ports and services

  - CIP-007 R2: The solution monitors the state of software versions and patches

  - CIP-007 R5.2 and CIP-004: The solution verifies that only approved accounts exist on systems

TRIPWIRE COVERAGE OF NERC CIP REQUIREMENTS

13 Standards & 44 Requirements – Tripwire Covers 23

	CIP-002 BES Cyber System Identification and Categorization	CIP-003 Security Management Controls	CIP-004 Training and Personnel Security	CIP-005 Electronic Security Perimeter	CIP-006 Physical Security of BES Cyber Systems	CIP-007 Systems Security Management	CIP-008 Incident Reporting and Response Planning	CIP-009 Recovery Plans for BES Cyber Systems	CIP-010 Configuration Change Management and Vulnerability Assessments	CIP-011 Information Protection	CIP-012 Control Center Communication Network	CIP-013 Supply Chain Management	CIP-014 Physical Security
1	BES Cyber System Identification	Cyber Security Policy for High/Medium Systems	Awareness	Electronic Security Perimeter	Physical Security Plan	Ports and Services	Cyber Security Incident Response Plan	Recovery Plan Specifications	Configuration Change Management	Information Protection	Physical & Logical Risk Mitigation for Data	Risk Management Plan	Transmission Station Physical Security
2	Regular Approval	Cyber Security Policy for Low Systems	Training	Interactive Remote Access Management	Visitor Control Program	Security Patch Management	Cyber Security Incident Response Plan Implementation and Testing	Recovery Plan Implementation and Testing	Configuration Monitoring	BES Cyber Asset Reuse and Disposal	Proof of Implementation	Proof of Implementation	Third Party Verification of Physical Security
3		Identification of Senior Manager	Personnel Risk Assessment Program		Maintenance and Testing Program	Malicious Code Prevention	Cyber Security Incident Response Plan Review, Update, Communication	Recovery Plan Review, Update and Communication	Vulnerability Assessments			CIP Senior Manager Approval	Primary Control Center
4		Delegation of Authority	Access Management Program			Security Event Monitoring			Transient Cyber Assets and Removable Media				Evaluate Potential Threats & Vulnerabilities
5			Access Revocation Program			System Access Controls							Physical Security Plan
6													Third Party Review of Plans

Tripwire LogCenter

Tripwire LogCenter is a complete log and event management solution that provides efficient log processing and sophisticated event analysis and alerting to meet NERC CIP log management requirements while providing access to data that helps organizations identify security events of interest and determine their root cause.

With Tripwire LogCenter, customers receive:

- Complete audit log capture and retention of all log events in a scalable solution.

- Customized reports and dashboards to document compliance and provide forensic analysis.

- Tailored logging and correlation rules to effectively and reliably collect and process log events for BES Cyber Assets such as SCADA devices and physical entry systems. This provides visibility across the environment and addresses security goals. For example, rules could be developed to provide effective logging retention across all systems or to ensure that revoked or unprivileged user accounts are no longer in use.

An advantage of using integrated Tripwire Enterprise and Tripwire LogCenter solutions is that they share data and components, providing a consistent view of your security posture that allows you to better identify the highest risk changes and events within your OT environment.

Tripwire IP360

Tripwire IP360 is a comprehensive vulnerability management solution that provides detailed assessments of a broad variety of asset classes in your environment and provides an ideal foundation for assessing every system on the network.

With Tripwire IP360, customers receive:

- Comprehensive asset discovery and profiling of all network-connected assets

- Industry-leading vulnerability assessment with coverage of the latest operating systems, applications and vulnerabilities

- Port scanning capabilities to aid in NERC CIP compliance

- Flexible risk-based reporting across all levels of the enterprise

Tripwire NERC CIP Coverage

Solutions are tailored to meet the exact needs of each customer, helping to meet as few as one to as many as 23 of the CIP requirements. Many of the CIP requirements are administrative or pertain to physical controls, but of those requirements involving technical controls, the Tripwire NERC CIP Solution Suite can help automate almost all of them.

- Integrations to leading network security, access control and workflow and service management vendors, such as Cisco, ForeScout and ServiceNow, for complete asset visibility and rapid response to vulnerabilities and exposures

- Integration with Tripwire Enterprise, and through that, a complete history of changes made to assets

Industrial Solutions

Tripwire has integrations with asset discovery and inventory solutions that provide anomalous behavior detection, security assessments, and vulnerability management of OT devices to highlight potential threats and protect sensitive industrial assets. The integration with Tripwire Enterprise allows the user to combine data from an OT visibility and security solution with the integrity and compliance data on IT assets in Tripwire Enterprise. The benefit of this partnership is allowing for a unified view and reporting of both IT and OT assets.
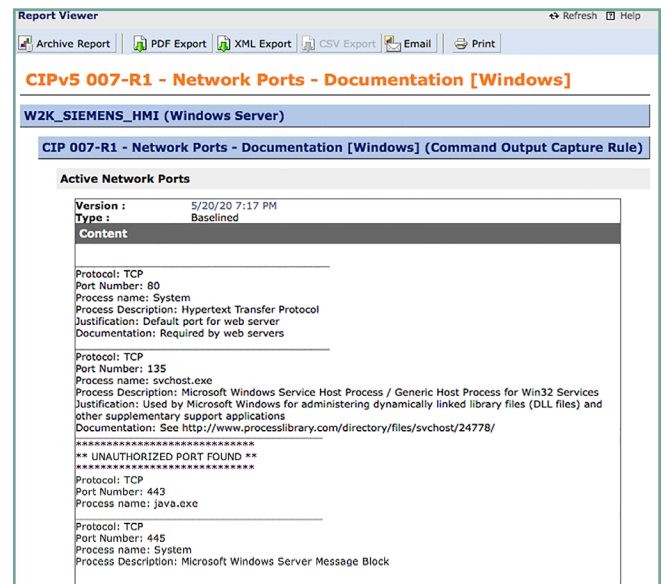
Tripwire Enterprise element content reports meet the CIP 007 R1 requirement to document the current status and justification for all ports and services on all BES Cyber Assets.

To further decipher the flood of data produced by your IIoT devices, Tripwire LogCenter has well defined content and configurations which enable you to aggregate all alerts and display them in actionable reports and dashboards with the same solutions that integrate into Tripwire Enterprise. You are immediately informed of critical events such as firmware uploads, configuration changes and baseline deviations, and can have follow-on alerts generated from Tripwire LogCenter to better understand the correlation of a sequence of events that bear further scrutiny.

Tripwire combines solutions like Tripwire Enterprise, Allowlisting, and Tripwire IP360 to act as an additional control to identify misconfigured devices or potential security incidents, identify ports or specific hardware and firmware versions, establish and track patch sources and more to satisfy NERC CIP requirements.

Experienced NERC CIP Consultants

To ensure effective tailoring and deployment of Tripwire products to the specific environment for the electric utility company, Tripwire's NERC CIP solution provides consulting from Tripwire Professional Services.

These NERC-experienced consultants will work with an organization to:

- Develop best practices around discovery methods and discuss the company's classification/taxonomy process to ensure that Tripwire accurately reflects how they view and manage their business.

- Review the reports and dashboards that auditors will require and tailor monitoring rules and reports that operators, managers, executives and compliance program staff will use to manage and report on security compliance programs.

- Provide specialized training on using Tripwire products to perform forensic analysis and determining the risks associated with hacking or a breach. This permits companies to perform more comprehensive root cause analysis, which in turn helps with compliance and remediation.

Addressing the Toughest CIPs

Some NERC CIP requirements are tougher than others. CIP–007 and CIP-010 are among the toughest. For CIP-007, Tripwire's Allowlisting can save years of personnel time by monitoring and documenting the status of all ports and services on each critical cyber asset. For CIP-010, Tripwire products can provide current status of compliance plus an audit record of configuration changes and vulnerability exposures.

Tripwire NERC CIP Solution Integrates to Secure ICS

Tripwire partners with several leading technology and solution providers in the NERC compliance space to provide a complete compliance solution. These joint solutions automate and simplify NERC CIP compliance and technology challenges in the power and utility industry. Tripwire supports 23 of the requirements and our partners complete the rest.

NERC CIP partners include AlertEnterprise, Archer Security Group, Belden GarrettCom and Tofino Security, Curricula, ICF International, NovaTech, PAS, RedSeal, Rkneal, SigmaFlow, The Anfield Group, WhiteScope, FoxGuard Solutions, and WizNucleus.

Rely on Tripwire for NERC CIP Compliance

As a recognized leader in solutions for IT security and compliance, Tripwire has significant experience helping customers automate compliance for numerous standards across almost any device, platform and system. Tripwire has helped registered entities achieve and maintain NERC
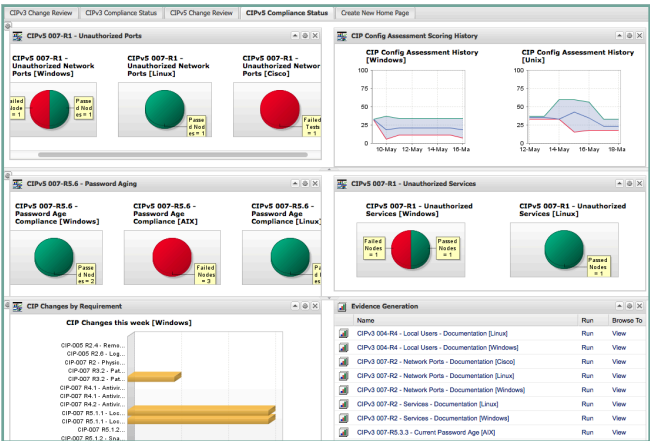
The Tripwire Enterprise NERC CIP dashboard provides a quick view of overall compliance status.

CIP compliance since 2008—experience that has allowed Tripwire to develop a team of consultants well versed in NERC CIP compliance and NERC CIP-specific content now embedded in the NERC CIP Solution Suite.

With the Tripwire NERC CIP Solution Suite, electric utilities have a comprehensive solution—from products, to customized extensions and content and expert consulting—to help them automate and simplify NERC CIP compliance. By meeting NERC CIP compliance, these companies secure their IT/OT systems against inadvertent misuse and intentional, malicious attacks. In turn, these secure systems help companies ensure the reliability of North America's bulk electric system.

With the NERC CIP Solution Suite, power companies can automate and simplify their NERC CIP compliance demands by taking advantage of Tripwire's:

- Asset discovery
- Continuous monitoring
- Automated assessment
- Audit-ready evidence
- NERC-experienced consultants

HOW TRIPWIRE CAN HELP

CIP-002-5: Cyber Security — BES Cyber System Identification and Categorization

CIP-002 R1: BES Cyber System Identification	Tripwire IP360 can help identify and track the critical cyber assets that are in scope. Tripwire can discover all assets in assigned IP scope using TCP and UDP protocols. Discovery of all assets allows for further classification and interrogation.

CIP-003-6: Cyber Security — Security Management Controls

CIP-003 R1: Cyber Security Policy for High/Medium Systems	R1.2.3	Tripwire validates and monitors security settings and related configurations to ensure that monitoring of dial-up services and features has been implemented.
CIP-003 R2: Cyber Security Plans for Low Impact BCS	R1.2.4	Tripwire reports through Tripwire Enterprise and Tripwire LogCenter can provide excellent forensic details to assist in the investigation/analysis of an Incident or in the preparation/evaluation of an IOC report.
	A-2	Where physical access systems are accessible or send logs to Tripwire, these products can provide evidence of proper configuration and use.
	A-3	Tripwire can provide supporting evidence of properly configured access control and detect non-compliance access through logs.
	A-4	Tripwire can provide valuable data about an environment as part of incident response.

CIP-004-5 Cyber Security — Training & Personnel Security

CIP-004 R4: Access Management Program	Tripwire Enterprise and Tripwire LogCenter are used to verify account and access control settings on systems and networks via logs and configuration changes.	
	R4.3	Tripwire's Allowlisting can verify only approved accounts exist on systems, as codified in an authorized user allowlist.
CIP-004 R5: Access Revocation Program	R5.4	Standard monitoring access logs comes out of the box with Tripwire LogCenter; access controls are monitored by Tripwire Enterprise, and tailored rules can be created to search for access control logs that match lists of former employees to validate that access and activity by the former employees has been stopped.
		Tripwire's Allowlisting can verify only approved accounts exist on systems, as codified in an authorized user allowlist.
	R5.5	Tripwire can help ensure that shared accounts have suitable controls, and that passwords have been changed according to stated policies.

CIP-005-5 Cyber Security — Electronic Security Perimeter(s)

CIP-005 R1: **Electronic Security Perimeter**	**R1.1**	Tripwire IP360 combined with professional services use of Tripwire discovery tools can help identify and track the cyber assets that are in scope.
CIP-005 R2: Interactive Remote Access Management	**Tripwire Change Auditing and Configuration Assessment/reporting will track settings associated with authenticated access control for remote use.**	
	R2.2	Tripwire validates and monitors security settings and configurations made to ensure strong authentication by external interactive users.

CIP-006-5 Cyber Security — Physical Security of BES Cyber Systems

CIP-006 R1: **Physical Security Plan**	**R1.4**	Tripwire can facilitate monitoring of physical access and other environmental monitoring systems through automated collection and analysis of these device logs by Tripwire LogCenter.
	R1.5	Tripwire can facilitate monitoring of physical access and other environmental monitoring systems by analyzing the logs collected, utilizing custom correlation rules to alert on unauthorized access attempts.
	R1.6	Tripwire can facilitate monitoring of physical access and other environmental monitoring systems through automated collection and analysis of these device logs by Tripwire LogCenter.
	R1.7	Tripwire can facilitate monitoring of physical access and other environmental monitoring systems by analyzing the logs collected, utilizing custom correlation rules to alert on unauthorized access attempts.
	R10	In the case where physical access restrictions are not used, Tripwire Enterprise can validate that alternative logical controls are in place as required. Tripwire LogCenter can be used to centrally gather logs from components and issue an alarm for failures.
CIP-006 R2: **Visitor Control Program**	**R2.3**	Log retention for the required periods can be assured through Tripwire's log management and archiving capabilities.

CIP-007-5 Cyber Security — Systems Security Management

CIP-007 R1: **Ports and Services**	**Tripwire's Allowlisting can monitor ports and services and compare current state against a tailored set of customer-specific approved port and services, alerting when monitoring detects a variance.**	
	R1.1	Tripwire's Allowlisting can monitor ports and services and compare current state against a tailored set of customer-specific approved port and services, alerting when monitoring detects a variance.
	R1.2	Tripwire can detect whether removable media has been connected to a monitored system, providing timely alerting of potential violations.
CIP-007 R2: **Security Patch Management**	**Tripwire's Allowlisting can identify software versions and installed patches and compare current state against a tailored set of customer-specific approved software versions and patches, alerting when there is a variance on specific BCAs.**	
	R2.2	Tripwire IP360's vulnerability assessment capabilities can identify any necessary patches that should be installed on a broad range of BCA systems based on vendor recommendations. The vulnerability database is typically updated every week.
	R2.3	Tripwire detects when patches are implemented and will record this information for later review and analysis.
CIP-007 R3: **Malicious Code Prevention**	**Tripwire can scan for anti-virus and malware products installed through tailored change auditing rules. Logs can be watched to find specific malware events and allow the Tripwire operator to examine the device for incident information.**	
	R3.1	Tripwire's FIM monitoring can detect the introduction of unapproved/unauthorized files on a given system.
	R3.3	Tripwire checks for security settings and configurations to validate anti-virus and malware prevention is enabled and updated appropriately.
CIP-007 R4: **Security Event Monitoring**	**Tripwire can scan logs for account management activity and configuration settings for changes to account privilege, alerting as appropriate.**	
	R4.1	Tripwire LogCenter rules can capture successful and unsuccessful logins for all monitored hosts, and provide alerting as desired.
	R4.2	Tripwire LogCenter rules can detect and alert when a BCA stops logging activity, thus providing alerting on continuous 24x7 basis.
	R4.3	Log retention for the required periods can be assured through Tripwire's log management and archiving capabilities.
	R4.4	Log retention for the required periods can be assured through Tripwire's log management and archiving capabilities.

CIP-007 R5: System Access Controls	**Tripwire can scan logs for account management activity and configuration settings for changes to account privilege, alerting as appropriate.**	
	R5.1	Tripwire can scan logs for account management activity and configuration settings to ensure authentication is enforced, alerting as appropriate.
	R5.2	Tripwire's Allowlisting can verify only approved accounts exist on systems, as codified in an authorized user allowlist.
	R5.4	Tripwire can ensure that default accounts are disabled and/or passwords are changed where required, and activity logging can provide alerting on inappropriate use of such accounts.
	R5.5	Tripwire can verify configuration settings for passwords and other security settings to meet and maintain compliance requirements.
	R5.6	Tripwire can verify configuration settings for passwords and other security settings to meet and maintain compliance requirements.
	R5.7	Tripwire can verify configuration settings for passwords and other security settings to meet and maintain compliance requirements, and provide alerting when success/failure thresholds are exceeded.

CIP-008-5 Cyber Security — Incident Reporting and Response Planning

CIP-008 R1: Cyber Security Incident Response Plan	R1.2	Tripwire reporting on logs, events, configuration and change detection would help to create IOC reports that could be part of an ISAC response document.

CIP-009-5 Cyber Security — Recovery Plans for BES Cyber Systems

CIP-009 R1: Recovery Plan Specifications	R1.3	Tripwire products can be customized to create baselines for products and devices configuration. These may be called for and used for recovery steps taken after incidents of system attack or failure.
	R1.4	Tripwire products can be customized to create baselines for products and devices configuration. These may be called for and used for recovery steps taken after incidents of system attack or failure.
	R1.5	Tripwire products can be used to collect and aggregate logs and event information from a variety of sources. This information can be stored and later used for recovery steps taken after incidents of system attack or failure.
CIP-009 R2: Recovery Plan Implementation and Testing	**Tripwire products can be customized to create baselines for products and devices configuration. These may be called for and used for recovery steps taken after incidents of system attack or failure.**	
	R2.2	Tripwire products can be used to collect baselines, logs and event information from a variety of sources. This information can be stored and later used for recovery steps taken after incidents of system attack or failure.

CIP-010-14 Cyber Security — Configuration Change Management and Vulnerability Assessments

CIP-010 R1: Configuration Change Management	**Tripwire can monitor all the details required for the CIP baseline, including security configuration details. Any change to the baseline can be reported on for daily compliance activities, as well as for meeting audit requests.**	
	R1.1	Tripwire provides out of the box monitoring and reporting capability for the five key points of baseline monitoring.
	R1.2	Tripwire has out of the box features for documenting deviations from the baseline as well as documenting authorization of those changes.
	R1.3	The Tripwire solution has built-in workflows for updating the baseline, as well as supports reporting on the updates to the baseline.
	R1.4	The Tripwire solution is easily extended to monitor CIP-005 and 7 security configurations, and showing whether there was any change.
	R1.5	Tripwire allows for easily documenting baseline changes of test systems before changes are made in production.
	R1.6	Although Tripwire does not provide a change ticketing system or enforce review processes, Tripwire can be used to confirm the correct configuration of any tools used to meet this requirement.

CIP-010 R2: Configuration Monitoring		**Tripwire's core functionality offers exceptional change detection and investigation capabilities.**
	R2.1	Tripwire Enterprise's core functionality offers exceptional change detection and investigation capabilities.
CIP-010 R3: Vulnerability Assessments		**Tripwire IP360 offers excellent vulnerability assessment and reporting across a broad variety of asset types.**
	R3.1	Tripwire IP360 offers excellent vulnerability assessment and reporting across a broad variety of asset types.
	R3.2	Tripwire IP360 offers excellent vulnerability assessment and reporting across a broad variety of asset types. Controls exist to minimize the potential for adverse effects during a scan.
	R3.3	Tripwire IP360 offers excellent vulnerability assessment and reporting across a broad variety of asset types. Controls exist to minimize the potential for adverse effects during a scan. Tripwire Enterprise can be used to ensure the test environment is equivalent to the target PCA.
	R3.4	Tripwire reporting helps document assessment results and provide usable content for mitigation plans.
CIP-010 R4: Transient Cyber Assets and Removable Media	R4	Tripwire Enterprise supports the requirements for configuration management on TCAs, as well as usage of removable media.

CIP-011-1 Cyber Security — Information Protection

CIP-011 R1: Information Protection		**Tripwire can be used to 1) generate evidence for audit of BCA for file system access controls, and 2) identify files used for evidence of compliance, monitoring them for change and retention (according to requirements and reported for auditors and compliance officials).**
	R1.2	Tripwire Change Auditing feature can be custom configured to assess if an application or operating system is configured for secure data transmission, storage or event logging—itself logging when these settings are changed or suppressed. This feature could support the appropriate management of BES information protection.

Schedule Your Demo Today

Let us take you through a demo of the Tripwire NERC CIP Solution Suite and answer any of your questions.

Visit tripwire.com/demo

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.

FORTRA™

Fortra.com