



WHITE PAPER (TRIPWIRE)

Improve Your Cybersecurity Posture: NIST

**Continuous Monitoring Using Security Configuration
Management, Critical Change Control, Vulnerability
Management And Log Management**

There isn't an industry that hasn't been affected by cyber threats, and the broadcast industry is no exception. In April 2015, France's TV5Monde was attacked, resulting in eleven of its channels going dark and its social media outlets commandeered to display pro-Islamic State messages. This was preceded by an attack on WBOC in Salisbury, Maryland, where their Twitter account and website were hacked and the site's content also replaced with images supporting ISIS. While both examples were politically motivated, that's not to imply that's the only reason for an intruder to hack into a broadcaster—consider simply breaking the ability to broadcast, accessing customer (including credit card) information or stealing/ransoming intellectual property are other criminal MOs. Of particular concern is a disruption to the Emergency Alert System (EAS), especially during a coordinated physical attack—the results of which could be catastrophic public safety threats. This is a wake-up call to the broadcasting sector that it is not only vulnerable to disruptive cyber intrusions and attacks, but that those attacks could have a severe impact on society.

Consider threat vectors. While Internet Protocol-based (IP) services deliver huge benefits in being able to transfer content quickly across locations without feed lines and without using traditional fiber transport, there's inherent risk as IP platforms offer a vast range of threat vectors. Communication and media providers like broadcast, cable, wireless, wireline and satellite have increasingly adopted IP technology in their production operations and they all have websites, increasing their vulnerability. Protective measures that include people, process and technology must be implemented, maintained and, as attacks constantly evolve, continuously improved.

FCC Guidance

A working group (WG4) of the FCC's Communications Security, Reliability and Interoperability Council (CSRIC) initiative has issued basic security recommendations for operators, participants and manufacturers to better protect their systems, based on the National Institute of Standards and Technology (NIST) Cybersecurity Framework. The WG4 report provides common sense guidance based on recommendations from industry cybersecurity experts, narrowed down to what it means to broadcasters.

In this paper we summarize the NIST framework—reflecting on the most current FCC guidance—and addressing the goals and methods to achieve better cybersecurity. We then present options for automating these complex and burdensome processes using Fortra's solutions Tripwire® Enterprise, Tripwire IP360™ and Tripwire LogCenter®.

The result will be an action plan for your organization to start or enhance your current cybersecurity posture by leveraging the NIST Cybersecurity Framework.

WHAT IS NIST?

Mandated by the United States Federal Government in 2013 for their agencies, NIST is intended to offer guidance on how to minimize cyber risks to infrastructure and enhance the ability to respond effectively to a cyber event. The NIST guides are somewhat daunting, but they provide a complete description of how organizations can set up an IT system, define its risks and apply appropriate controls to address those threats. Furthermore, in an effort to make the guidance more accepted by the wide variety of organizations, the NIST guides are being re-written with guidance from civilian, military and intelligence communities. The FCC's initiative is an example.

As a result of President Obama's executive order in 2013, NIST also released its Cybersecurity Framework (CSF) for Improving Critical Infrastructure Cybersecurity. The framework is a voluntary, risk-based approach to cybersecurity that enables organizations of any nature to apply strong cybersecurity measures to secure critical infrastructure. The NIST CSF refers to other security standards such as NIST 800-53, COBIT 5 and ISO 27001. CSF does not provide templates on how to deploy the framework. The framework starts with functions organized by basic cybersecurity activities aligning with existing methodologies. The Framework provides a common taxonomy and mechanism for organizations to communicate their cybersecurity risk and plan.

How to Approach NIST with Tripwire

So how can security automation solutions such as Tripwire products help your organization? First let us give you an overview of the products, then a more specific solution example to see how Tripwire can help you support your alignment to the NIST Cybersecurity Framework.

Tripwire Endpoint Detection Response

Tripwire provides an integrated suite of solutions to deliver critical end point detection and response (EDR) capabilities. These include detecting security incidents, containing the incident at the endpoint, investigating security incidents and remediating endpoints.

Each solution from Tripwire or another security provider has core competencies in different areas in the information security space; integrating these competencies helps solve security and compliance problems. Gaining additional context from other solutions enables more informed and better decisions. Automation helps apply intelligence and delivers more effective security operations. Organizations can respond faster with precision while also driving security costs down. Tripwire's integrations with a wide array of vendors bring a range of benefits and use cases by distinct categories: Threat Intelligence, Network Security, Securing Industrial Control Systems (ICS), Analytics and Security Incident & Event Management (SIEM), IT Service Management (ITSM) and Integrated Access Management (IAM).

Tripwire's Solutions

Tripwire Enterprise, Tripwire IP360 and Tripwire LogCenter are the core Tripwire solutions.

Tripwire Enterprise

Tripwire Enterprise consists of two primary functional capabilities: first, providing the ability to detect and filter authorized and unauthorized changes in critical files and configurations across your network, and second, the ability to assess and report whether your IT assets are configured in a manner compliant with your organization's adopted compliance policies (like FISMA).

File Integrity Monitoring is a key requirement of IT security. Subtle system changes associated with breaches, theft and all types of malicious behavior can activate a "tripwire" in monitored endpoints that then alerts the organization. Tripwire's best-of-breed File Integrity Monitoring detects critical changes to a system, determines who made the change and when, what actions occurred before or after, and if the change was authorized—exactly the type of information and detail necessary to identify new risks and threats.

Tripwire Policy Manager continually assesses IT control configurations against dozens of policies and standards (such as DISA STIGs, NIST/FISMA guidelines, PCI DSS, ISO,

and many others). Tripwire provides more than 650 out-of-the-box, customizable policies that instantly assess file and configuration settings on most operating systems and devices. Tripwire Policy Manager pinpoints efficiencies, speeds remediation and dramatically lowers the costs of proving compliance. This process of Security Configuration Management is one of the most important cybersecurity disciplines and is critical to any mature IT organization.

Tripwire IP360

Tripwire IP360 provides complete visibility into the enterprise network including all networked devices and their associated operating systems, applications and vulnerabilities. It's an ideal foundational control for effective security risk management. Tripwire IP360 uses advanced analytics and a unique quantitative scoring algorithm based on several factors—including the vulnerability score and business-relevant asset value—to prioritize the vulnerabilities for remediation. The result is actionable data that enables IT security teams to focus on the tasks that will quickly and effectively reduce overall network risk with the fewest possible resources. By employing the built-in integration between Tripwire Enterprise and Tripwire IP360, IT organizations can now enable EDR for the network, which provides the ability to automatically adjust security controls based on system changes and potential business impact thereby significantly reducing overall enterprise cyberthreat risk.

Tripwire LogCenter

Tripwire LogCenter is a log and event management product that provides enterprise-class log aggregation, event assessment and control. Tripwire LogCenter helps organizations comply with the NIST CSF (and other) requirements to maintain complete and accurate logs by providing agent-based, lossless capture and retention of logs—even in the face of network outages and other communication interruptions. Tripwire LogCenter event analysis further enables organizations to identify a coordinated attack across diverse devices, capture full log and forensic data, and inform system managers with dashboards, notifications and alerts. Its tight integration with Tripwire Enterprise enables customers to look at critical or suspicious changes to a device and then pivot to associated log events, and vice versa. Log investigation may be done right at the Tripwire Enterprise console to streamline

compliance and security efforts. In addition, Tripwire LogCenter can correlate on changes detected by Tripwire Enterprise based on authorization or impact to security policy. This real-time capability can cut the time to detect and investigate a security event from weeks or months to minutes.

The FISMA Solution

For an organization to meet NIST-prescribed guidance, there are a number of tasks and artifacts developed to determine system risk and the controls (system configuration, settings, utilities and tools) necessary to mediate the threats and vulnerabilities to that system. This is the essence of security, and it ties directly to authority to operate the system in a production setting. But secure setup of a system is not enough by itself. In addition to common threat vectors there is the risk of control failure itself. If a critical control is lost, how is that determined? What other controls can be put on the key control?

Risk and security management has been trying to grapple with this problem for a long time, and depending on the classification or categorization of the system, the solution can involve a lot of dedicated manpower to validate that system controls are effective and being maintained correctly.

This is why new NIST SP 800-37 focus has been changed towards the effort to develop controls and a plan to validate that controls are effective and operating as planned. Organizations must address risk and controls assessment for all systems in the manner prescribed by NIST; related tasks might include the assessment of overall system configuration results in a system categorization, and system component inventory and boundary information ("Categorize the information system and the information processed, stored, and transmitted by that system based on an impact analysis").

This is where Tripwire Enterprise, Tripwire IP360 and Tripwire LogCenter can provide both prescribed controls and a means to validate that overall controls are operating correctly.

Tripwire Enterprise can be used in this initial assessment task to gather configuration information about the devices on this system. That could include Windows, Unix and Linux Servers, network devices and databases like SQL Server or Oracle. To accomplish this, all devices would be scanned with rules to check file inventory and system configuration. Special rules can be used to baseline the state of custom

applications, including the application used to process and store sensitive information.

The next step is to choose the correct security controls for the system based on the categorization for the system. This typically involves assessment with NIST 800-60 (Guide to Mapping Types of Information and Information Systems to Security Categorization) to help identify the risks to the system. It will also require a determination of special risks and controls unique to the system. However, in the end, this task will involve the selection of controls from the 18 control families found in NIST SP 800-53.

Tripwire Enterprise, Tripwire IP360 and Tripwire LogCenter all can assist in meeting NIST guidance by 1) providing a specific security controls as found in the 800-53 control families, 2) providing control assessment (continual monitoring), 3) file integrity validation, and 4) providing vulnerability management. Please refer to the NIST Tripwire Enterprise, Tripwire IP360 & Tripwire LogCenter Controls Matrix that follows.

The next step is to implement controls—when specific controls chosen are applied to the system. The result should be a report of all controls used in a system.

This is when Tripwire products are configured to perform as chosen controls (control and configuration monitoring), or as part of a management controls such as Contingency Planning (CP controls) which call for a method to validate system file integrity on backup devices and media, or Security Assessment and Authorization (CA controls), where Tripwire Enterprise is used as part of the auditors tools to validate the files have not changed and supports the SHA2 hash encryption algorithm. When Tripwire Enterprise is used to monitor for Technical or Operational controls, the user can choose to use an out-of-the-box policy, or develop their own monitoring rules. In either case, Tripwire Enterprise can provide reporting on all the controls it is monitoring on multiple platforms.

The next step is to Assess Security Controls. This work is typically when the first full assessment of a system is performed, and the controls which are not working are identified and put onto a tracking report.

Tripwire Enterprise's Policy Manager was designed for this step in the compliance process. Tripwire assessment policy for NIST (customized or used out of the box) then

provides the bulk of the required reporting, including an ability to track and report on failing configuration/controls in a “waiver” feature that tracks the authorization and remediation schedule for each control (POA&M=Tripwire Report). Tripwire technology continually assesses the state of the system controls and can be configured to alert security personnel when or if configuration or control is lost. The state of the control environment is determined with detailed reporting offering forensics and other relevant information.

The next step is to validate and authorize the system for production use. While this is defined as a specific task, it is really an ongoing process of evaluating risk and the present state of controls. And by using Tripwire Enterprise Policy Manager, security personnel and the system owner can maintain a “desktop” reporting feature that can show them the continual, near real-time status of controls and compliance at a glance.




The final step is to Monitor Security Controls. This typically involves an expensive effort to reassess changes to the system environment, frequent vulnerability scanning and alerting, ongoing security control assessment, taking ongoing remediation actions on system control failures or changes, making key updates, and reporting the combined information to authorities (such as FCC).

When a control fails, such as when a setting is changed that causes the system to be out of compliance, Tripwire Enterprise alerts the system administrator with information on how to fix most problems (remediation advice) and allows the Tripwire Enterprise operator to request a waiver which tracks the failure without affecting the NIST scoring. In addition, Tripwire IP360 offers ongoing vulnerability risk assessment and prioritization, which allows the operator to respond according to policy.

Conclusion

With solutions like Tripwire Enterprise, Tripwire IP360 and Tripwire LogCenter, organizations can make the challenge of becoming and maintaining a stronger cybersecurity posture as outlined in the NIST Cybersecurity Framework much easier and cost effective than trying to manage the requirements manually. As we’ve seen, Tripwire Enterprise and Tripwire LogCenter offer specific controls, control monitoring and management control capabilities. Additionally, Tripwire offers unique products that meet the very nature of “continuous monitoring” as defined by NIST 800-37. And this concept is not new to Tripwire—it has been the essence of the company since its formation.



NIST TRIPWIRE ENTERPRISE, TRIPWIRE IP360 & TRIPWIRE LOGCENTER CONTROLS MATRIX

NIST 800-53A Control Family	Control Type	Tripwire Response*	Provides and/or Supports and/or Validates	Tripwire Enterprise Policy Compliance Management	Tripwire Enterprise File Integrity Monitoring	Tripwire IP360 Vulnerability Management	Tripwire Log Center Audit Log/ Event Analysis
Access Control (AC)	Technical		Provides Supports Validates	Tripwire Enterprise can be used for assessment of the many operating system settings that support many of the AC controls including AC-2 Account management, AC-6 Least Privilege, and AC-7 Unsuccessful login attempts	Tripwire Enterprise can be used to continually monitor and validate that files have not been changed on servers, devices or particular applications or data files. This is often important for AC control of mobile users and remote access devices. (e.g. AC-19)		Tripwire Log Center can be used as the control specified AC-2(4) which specifies that the organization must employ automated mechanism for auditing access control events, including remote access AC-17.
Audit and Accountability (AU)	Technical		Provides Supports Validates	Tripwire Enterprise is used to assess AU controls which are called for in the description of applicable controls. These include AU-4, Audit of Storage Capacity, AU-5, Response to Failure as well as settings called for, example: AU-2(4) Audit Privileged Functions and AU-9 Protection of Audit Information	Tripwire Enterprise File Integrity Monitoring (FIM) can be used to assist in Audit and Accountability of files that should not change or should be compared between systems to be identical. Unexpected change alerts can signal breach or malicious behavior.	Tripwire IP360 directly provides AU-06(5) controls with our proprietary advanced threat intelligence integrations by bringing vulnerability intelligence into a single pane of glass with other critical data.	Tripwire Log Center can be used as a core audit control - working to specifically meet requirements of AU-2 thru AU-12. Tripwire Log Center also provides analytical capabilities to compare audit trails.
Security Assessment and Authorization (CA)	Management		Validates Supports		Tripwire Enterprise is often used as a continual monitoring Audit tool to validate files and reports have not changed between compliance audits. Tripwire Enterprise supports the CA-2(i) control by use of approved encryption hash algorithms SHA2 for this function.	Tripwire IP360 can support CA-08 control policies with vulnerability exposure.	





* The overall Tripwire response rating is based on the following criteria:

- How much Tripwire enables the key intention behind the control
- Greater weight to “provides functionality” for the control
- The number of sub-requirements responded to
- Harvey balls represent the amount of Tripwire response to the control requirement (25/50/75/100%)

NIST TRIPWIRE ENTERPRISE, TRIPWIRE IP360 & TRIPWIRE LOGCENTER CONTROLS MATRIX

NIST 800-53A Control Family	Control Type	Tripwire Response*	Provides and/or Supports and/or Validates	Tripwire Enterprise Policy Compliance Management	Tripwire Enterprise File Integrity Monitoring	Tripwire IP360 Vulnerability Management	Tripwire Log Center Audit Log/ Event Analysis
Configuration Management (CM)	Operational		Validates Supports	Tripwire Enterprise supports verification of key security settings such as CM-5 which calls for Audit Access Restriction enforcement, and CM-7 which calls for "Least Functionality." Tripwire Enterprise verifies these settings within the operating system, and assures that common attackable services are disabled.	Tripwire Enterprise FIM is a best practice control for obtaining the essential baseline configuration called for in the CM control set. Once this baseline is obtained, Tripwire Enterprise can be configured to watch specific applications for change meeting the requirements around CM.		Tripwire Log Center can be used to automate and enforce access restrictions on audit logs as well as supporting the auditing for change is access restriction changes - example CM-5(1-2)
Contingency Planning (CP)	Operational		Supports		Tripwire Enterprise is often used to support file integrity operations for Contingency programs, being able to validate the files on contingency systems (CP-2) and backups (CP-9).		
Identification and Authentication (IA)	Technical		Validates, Supports	Tripwire Enterprise supports the Authentication settings are correctly set, such as IA-5 or IA-9 Authenticator management controls, and IA-7, Cryptographic module configuration.	Because many operating systems use files to maintain identification and authentication information for users, devices and other controls, the Tripwire Enterprise file integrity monitoring of these files can be a pivotal monitoring control to the unauthorized escalation of privilege.		



NIST TRIPWIRE ENTERPRISE, TRIPWIRE IP360 & TRIPWIRE LOGCENTER CONTROLS MATRIX

NIST 800-53A Control Family	Control Type	Tripwire Response*	Provides and/or Supports and/or Validates	Tripwire Enterprise Policy Compliance Management	Tripwire Enterprise File Integrity Monitoring	Tripwire IP360 Vulnerability Management	Tripwire Log Center Audit Log/ Event Analysis
Incident Response (IR)	Operational		Provides Validates Supports	Tripwire Enterprise supports key and recommended Incident monitoring settings are maintained and in accordance with NIST and NSA recommendations, such as IR-5.	Tripwire Enterprise FIM is also used as a manner to verify and detect network device changes to the configuration files that control most routers.	Tripwire IP360 can support the enforcement of customer defined IR-06(2) control policies and procedures by monitoring for vulnerability exposure	Tripwire Log Center can provide tracking of security events including incidents. Tripwire Log Center also provides for method of collection and correlation of incident information to help forensic type analysis.
Maintenance (MA)	Operational		Validates Supports	Tripwire Enterprise policy supports the validation of key controls in Maintenance settings such as MA-3 which calls for certain diagnostic application services disabled, or settings for remote administration.	Tripwire Enterprise is often used to support the verification of no change to key files and systems for the support of maintenance activities performed by remote access, and can be set to inform system owners of all change to systems during a maintenance phase.		
Media Protection (MP)	Operational		Validates Supports	Tripwire Enterprise policy supports the validation of restrictive access settings and audit controls within most operating systems to support controls such as MP-2 Media Access.			Tripwire Log Center performs audit of media storage areas and audit of attempted access and granted access.
Physical and Environmental (PE)	Operational		Validates Supports			Tripwire IP360 and can support the enforcement of customer defined PE-03(6) control policies and procedures by monitoring for vulnerability exposure for penetration testing.	

NIST TRIPWIRE ENTERPRISE, TRIPWIRE IP360 & TRIPWIRE LOGCENTER CONTROLS MATRIX

NIST 800-53A Control Family	Control Type	Tripwire Response*	Provides and/or Supports and/or Validates	Tripwire Enterprise Policy Compliance Management	Tripwire Enterprise File Integrity Monitoring	Tripwire IP360 Vulnerability Management	Tripwire Log Center Audit Log/ Event Analysis
Planning (PL)	Management		Supports		Tripwire Enterprise, can support the enforcement of customer defined PL-08(i) control policies and procedures by monitoring for user account attribute changes, system access, and system change.	Tripwire IP360 and Tripwire Configuration Compliance Manager can support the enforcement of customer defined PL-08(i) control policies and procedures by monitoring for vulnerability exposure.	Tripwire Log Center can support the enforcement of customer defined PL-08(i) control policies and procedures by monitoring for user account attribute changes, system access, system change, and log / event data.
Personnel Security (PS)	Operational		Validates Supports	Tripwire Enterprise can support PS-05 control policies with critical system change and system access data on monitored hosts			Tripwire Log Center contains out of the box tests, rules, and reporting to validate PS-05 control policies
Risk Assessment (RA)	Management			Tripwire Enterprise, Tripwire Log Center, Tripwire IP360 and Tripwire Configuration Compliance Manager (CCM) can support the enforcement of customer defined RA-03 control policies and procedures by monitoring for user account attribute changes, system access, system change, vulnerability exposure, and log/event data		Tripwire IP360 can directly provide RA-05 controls by monitoring for the vulnerability exposure of a system	

NIST TRIPWIRE ENTERPRISE, TRIPWIRE IP360 & TRIPWIRE LOGCENTER CONTROLS MATRIX

NIST 800-53A Control Family	Control Type	Tripwire Response*	Provides and/or Supports and/or Validates	Tripwire Enterprise Policy Compliance Management	Tripwire Enterprise File Integrity Monitoring	Tripwire IP360 Vulnerability Management	Tripwire Log Center Audit Log/ Event Analysis
System and Services Acquisition (SA)	Management		Provides Validates Supports	Tripwire Enterprise, Tripwire Log Center, and Tripwire Configuration Compliance Manager can support the enforcement of customer defined SA-04(1, 2, 5, 8) control policies and procedures by monitoring for user account attribute changes, system access, system change, log and event data		Tripwire IP360 and can support the enforcement of customer defined SA-09 (1), SA 11(2), SA 11 (6), SA 12(7), SA 15(2,4,5) control policies and procedures by monitoring vulnerability exposure	Tripwire Enterprise, Tripwire Log Center, and Tripwire Configuration Compliance Manager can support the enforcement of customer defined SA-04(1,2, 5,8) control policies and procedures by monitoring for user account attribute changes, system access, system change, log and event data
System an Communications Protection (SC)	Technical			Tripwire Enterprise provides policy that support verification of security settings that support SC family protections. These include SC-3 controls on security functions of the OS, SC-4 which protect secure shared resources, and SC-7 which include hardened network and routing methods.	Tripwire Enterprise FIM can be used to assist in the continual monitoring of security configuration of any applications. Assuring that applications remain in a secure, operational state that protects confidentiality, integrity and availability.		
System and Information Integrity (SI)	Operational		Provides, Validates, Supports	Tripwire Enterprise policy support SI Family controls such as SI-9, the support of information input restrictions controls.	Tripwire Enterprise FIM supports the monitoring of SI Family controls through the verification of configuration files for SPAM protection, Error handling and other key files that should not change until needed.	Tripwire IP360 can support the enforcement of customer defined SI-02(1-3) control policies and procedures by monitoring for the vulnerability exposure	
Program Management (PM)	Management	N/A					



Fortra.com

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.