FORTRA™

SOLUTION BRIEF (TRIPWIRE)

Implementing FISMA SI-7

Tackle This Challenging Control to Improve Your FISMA Grade

To enhance your Federal Information Security Management Act (FISMA) compliance grade, you must implement one of the most challenging controls in NIST SP 800-53: the Controls, Family: System Information & Integrity (SI) 7 requirement. SI-7 states that organizations must employ automated and centrally managed integrity verification tools to detect unauthorized change. This level of visibility can be difficult enough to achieve, but SI-7 also requires organizations to incorporate the unauthorized changes they find into their incident response process and be ready to pass an audit trail demonstrating these capabilities.

Fortra's file integrity monitoring (FIM) solution Tripwire® Enterprise delivers the capabilities necessary to address this requirement by providing a deep understanding of all the changes occurring in your environment and, when desired, provides seamless integration into IT Service Management (ITSM) solutions to create a workflow for the smooth exchange of system change and security configuration state information with a wide variety of compliance, operations and reporting/analytics solutions. Fortra ITSM partners integrate with Tripwire Enterprise so that inventory can be shared with, and used within, the CMDB. ITSM partners include BMC Remedy, CA, Cherwell Software, HP Service Manager, IBM, Atlassian (JIRA), Landesk, Microsoft and ServiceNow.

As a premiere FIM provider, Tripwire's integrity management solution is an essential cybersecurity platform that enables federal departments and agencies to see with confidence, decide with confidence and operate with confidence, while meeting even the most stringent FISMA requirements such as SI-7.

ANALYST QUOTE

File integrity monitoring… driven in large part by compliance needs, is dominated by Tripwire.

—451 Research

Requirements of NIST SP 800-53 SI-7:

SI-7 Software and Information Integrity

Control:

a. Employ integrity verification tools to detect unauthorized changes to the following software, firmware, and information: [Assignment: organization-defined software, firmware, and information]; and

b. Take the following actions when unauthorized changes to the software, firmware, and information are detected: [Assignment: organization-defined actions].

Supplemental Guidance: Unauthorized changes to software, firmware, and information can occur due to errors or malicious activity. Software includes operating systems (with key internal components, such as kernels or drivers), middleware, and applications. Firmware interfaces include Unified Extensible Firmware Interface (UEFI) and Basic Input/Output System (BIOS). Information includes personally identifiable information and metadata that contains security and privacy attributes associated with information. Integrity-checking mechanisms—including parity checks, cyclical redundancy checks, cryptographic hashes, and associated tools—can automatically monitor the integrity of systems and hosted applications.

Control Enhancements:

1. Integrity Checks
2. Automated Notifications of Integrity Violations
3. Centrally Managed Integrity Tools
4. Tamper-evident Packaging
5. Automated Response to Integrity Violations
6. Cryptographic Protection
7. Integration of Detection and Response
8. Auditing Capability for Significant Events
9. Verify Boot Process
10. Protection of Boot Firmware
11. Confined Environments with Limited Privileges
12. Integrity Verification
13. Code Execution in Protected Environments
14. Binary or Machine Executable Code
15. Code Authentication
16. Time Limit on Process Execution Without Supervision
17. Runtime Application Self-Protection (RASP)

Tripwire's Response to SI-7

Tripwire, the leading provider of IT security and FISMA compliance automation solutions, can help your agency take control of a wide range of security and compliance challenges including SI-7. Tripwire has a trusted track record and reputation with FIM. Much of the Fortune 500 and nearly every federal Cabinet agency uses Tripwire solutions.

Tripwire Enterprise combines file and system integrity monitoring, compliance policy management, real-time analysis of detected change, and prescriptive remediation guidance to help IT organizations achieve and maintain compliance. It does this by immediately detecting file and configuration changes through real-time continuous file integrity monitoring. Tripwire also incorporates integrations to ITSM tools to identify authorized and unauthorized changes to system configuration components including those that introduce security risk or take systems out of compliance (security controls). Remediation guidance is provided for undesirable changes so IT and Security teams can fix issues quickly. Tripwire Incorporates apps and actions that allow admins to auto-promote other changes based on patch manifest matches, severity values and items deemed to be "business as usual" these action types simplify the implementation of a solid SI-7 focused tool.

Tripwire also offers Tripwire LogCenter®, a complete log and security event management solution that integrates with Tripwire Enterprise to deliver even greater control over IT infrastructure. For example, in addition to standard out of box change detection, side-by-side analysis and alerting in Tripwire Enterprise, changes discovered in Tripwire Enterprise are now matched to the footprint or "log events" surrounding the change right in the Tripwire Enterprise GUI. Tripwire Log Center contains normalization and correlation rules alongside reporting to validate SI-7 control policies right out of the box.

Tripwire IP360™, a leading vulnerability management solution, proactively discovers, profiles and assesses the vulnerability risk of all wired and wireless devices on an organization's network. Tripwire IP360 can quickly detect vulnerabilities and prioritize risk using business context data unique to your organization. Remediation of identified vulnerabilities is simplified through integrations with reporting and ticketing tools. Tripwire Enterprise uses vulnerability intelligence tags from Tripwire IP360 (vulnerability risk, specific vulnerabilities, specific applications, ease/impact of exploit, time endpoint was last scanned) to provide deeper security visibility and to further prioritize suspicious changes on critical endpoints.

Tripwire Advantages for FIM and FISMA

Tripwire has a solid reputation as a proven FIM provider. As matter of fact, it was specified as the industry standard in the original PCI standards. In addition to comprehensive and reliable file integrity monitoring capabilities, Tripwire Enterprise includes comprehensive policy compliance management capabilities with a library of over 2000 policy and OS combinations that enable proactive validation of the state of the IT infrastructure against internal and external best practices, security and compliance policies.

Here are some distinguishing features of Tripwire Enterprise's capabilities:

- Baselines endpoints and assesses systems against a known good configuration—provides differences between like systems.
- Real-time system change detection—assesses change in detail to include "when, what, where and who" information. Combined with Tripwire LogCenter or other SIEM tool and you will also have instant footprint data.

- Compliance and security policies— assesses your systems for their current secure/hardened state. Use our remediation guidance or auto-remediation workflows (where applicable) to bring your systems to a compliant state. Continuously monitor to ensure systems remain compliant, saving manpower and dollars by staying compliant.
- Reduces file system auditing resource usage by utilizing Tripwire Enterprise's built-in "event generator" on endpoints.
- Full role-based access control (RBAC) capabilities to allow permission-based login and tool usage—users can login and only use specific components of the tool they are authorized for. For instance, a Windows admins can log in to Tripwire Enterprise and only see the "windows assets" they are responsible for.
- As an Operations tool—many customers rely on Tripwire Enterprise to track change, so they can easily determine what went wrong when systems or applications are no longer functioning or when router changes block access to resources.
- As a Security tool—Tripwire solutions are regularly relied upon to monitor for and assess endpoints for deviations that are in line with cyberattacks and breaches.
- As a tool to assess Indicators of Compromise—Tripwire Enterprise hashes nearly everything and stores these values in its database. Users can search for known bad hashes or use our File Analytics tools to search local or SaaS-based partner databases for hash matches.
- As an isolation tool—Tripwire Enterprise can utilize "execution" actions to isolate systems that have known critical risks or contain malicious information.
- When combined, Tripwire State Analyzer and Tripwire Enterprise will alert when items that are not allowlisted (whitelisted) appear in your environment (services, applications, open ports, group memberships, routes and valid users).
- Combine our Ticketing Event Integration Framework (TEIF) with Tripwire Enterprise to assess change against ITSM tools such as Service Now, Remedy, Jira, Check-it and many others. This allows Tripwire Enterprise to auto-promote changes that have an approved status. It

Examples of Change Details and What You Can do With Them

Change Feature	Benefit
Monitor for changes with over 65 attributes of a file or configuration to consider with attributes like file hash values (MD5, SHAH-1, etc.)	Deep understanding drives more accurate remediation
Version tracking to view each version of a file/configuration over a period of time.	Historical understanding provides better decision making and delivers audit-ready evidence
Ability to detect users making changes, without requiring native OS auditing.	Removes complexity of detecting changes
Ability to monitor any device with SSH or Telnet capabilities	Not complex and cumbersome since it's agentless and discovers difficult protocols
Scales to cover the entire IT stack (virtualization, cloud, physical/virtual servers/desktops, applications (databases, directory services, web applications, Exchange), network devices (routers, switches, firewalls and any other device that can utilize SSH).	Comprehensive coverage assures broad and deep security
Using the Tripwire Dynamic Software Reconciliation app, matches patch changes to patch manifests.	Quickly zero in on changes that aren't associated with patch activity during the patch window
Understand good vs bad changes based on context from the change management process and their potential impact on security.	Minimize false positives, focus on the true problems
Automatically monitor changes on newly installed applications	Gain real-time change insights
Whitelist users, ports, services and applications and alert/take action on unauthorized matches	Comprehensive and fast detection of potential threats
Kill unauthorized processes and uninstall unapproved applications. Isolate endpoints	Enforce integrity requirements and enhances security
Easily view side-by-side comparisons	Quick assessment of changes delivering faster remediation
Offers key insight into change events over a period of time	Gain better intelligence to make better decisions
Offers key insights into the vulnerability risks on assets	Better and faster risk assessments allow users to see what vulnerabilities exist on systems known to also have critical changes. Are changes related to a successful exploit?

also allows IT organizations to utilize Tripwire Enterprise to close out approved CRs or create new incidents when unapproved changes occur.

- Add the Tripwire Dynamic Software Reconciliation app to give Tripwire Enterprise the ability to assess all changes during maintenance windows against patch manifests to determine valid “patch related” change. Tripwire Enterprise then promotes patch related changes with no need of reconciliation.
- Combine Event Sender with Tripwire Enterprise to provide “event” specific format and expanded context to your SIEM tool of choice.

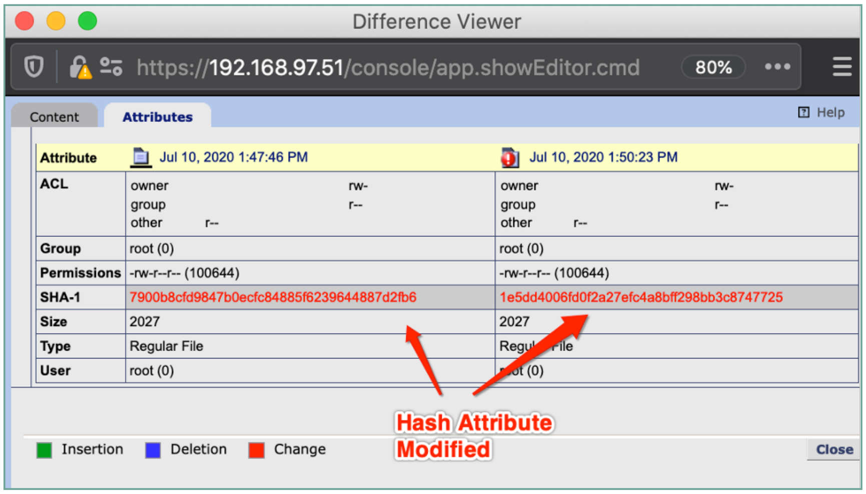
Tripwire provides truly continuous compliance monitoring by detecting changes that impact security parameters as they occur, in contrast to typical periodic full scans of endpoints. Tripwire’s approach reduces the audit performance impact on target systems and the network through the use of a built-In “event generator,” while allowing organizations to monitor and maintain compliance over time—even as change occurs.

BASIC SECURITY HYGIENE: FILE INTEGRITY MONITORING

Not only is FIM required for FISMA compliance, but it’s also foundational to security. The current best practices in cybersecurity assume you have been breached and that an intruder is on your network. The intruder’s objective is to become familiar with your network and assets then strike at an opportunistic time. In order to do this, the intruder must make changes to carry out his mission by moving around, conducting reconnaissance, increasing his privileges and doing damage such as stealing data or denying services. These actions require him to make changes that Tripwire can detect: inserting an executable, altering security configuration files, adjusting the OS and access rights, etc. Continuous monitoring of files and configurations can detect and stop these malicious attempts. This is core to security practices.

Tripwire integrates with a wide range of solutions to extend the insight on the change, which results in enhanced security and optimized processes. Tripwire integrates with SIEM providers to deliver more context around the events they are collecting for investigation. Tripwire integrates with ITSM solutions for closed-loop change control. To increase security, Tripwire integrates with File Analytic feeds and sandboxing technologies to gain additional insight or validation on the potential threat. Tripwire can detect and take action on zero-day malware attacks in real time.

These advantages are why many FISMA customers are committed to Tripwire. Tripwire’s distinct value of deep and real time understanding of systems and changes sets the company apart from the others. Remove your SI-7 requirement struggles with Tripwire and achieve FISMA compliance with a worthy grade.



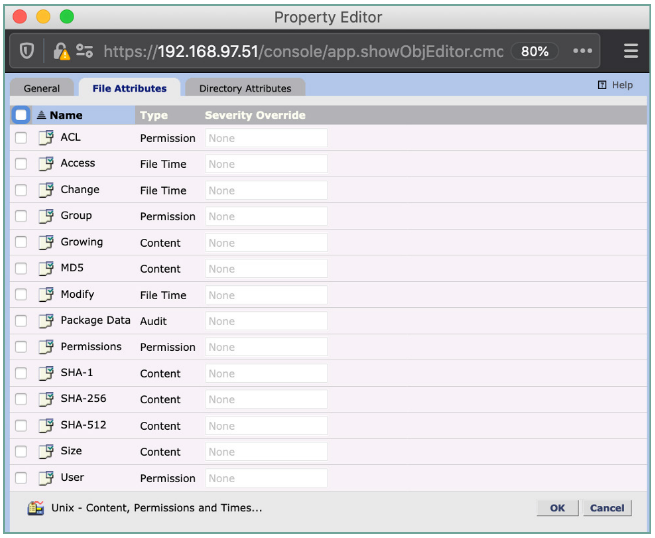
Attribute	Jul 10, 2020 1:47:46 PM	Jul 10, 2020 1:50:23 PM
ACL	owner rw- group r-- other r--	owner rw- group r-- other r--
Group	root (0)	root (0)
Permissions	-rw-r--r-- (100644)	-rw-r--r-- (100644)
SHA-1	7900b8cfd9847b0ecfc84885f6239644887d2fb6	1e5dd4006fd0f2a27efc4a8bff298bb3c8747725
Size	2027	2027
Type	Regular File	Regular File
User	root (0)	root (0)

Side-By-Side Attribute Differences—Making a comparison with side-by-side attributes allows a quick assessment of changes, and highlights what’s different to determine if it’s a potential risk. Here we see change to baselined file attributes of security control (/etc/login.defs)

As a premiere FIM provider, Tripwire has expanded on this core competency to deliver advanced enterprise-class solutions that include configuration and policy management, file integrity monitoring, vulnerability management, log management, and reporting and analytics. Tripwire is the choice for security, FISMA compliance and operations needs.

Conclusion

FIM goes beyond SI-7 compliance. FIM is basic security hygiene that all organizations should have to track malicious activity. FIM is critical for IT operations to keep systems up and optimal with the key insight to correct and restore. Remember bad users don't just enter a network and reside on a wire—in short order, bad-users end up on an exploited endpoint.



□	Name	Type	Severity Override
□	ACL	Permission	None
□	Access	File Time	None
□	Change	File Time	None
□	Group	Permission	None
□	Growing	Content	None
□	MD5	Content	None
□	Modify	File Time	None
□	Package Data	Audit	None
□	Permissions	Permission	None
□	SHA-1	Content	None
□	SHA-256	Content	None
□	SHA-512	Content	None
□	Size	Content	None
□	User	Permission	None

Unix - Content, Permissions and Times...

Windows File and Directory Attributes—A comprehensive list of file attributes provides a deeper and better understanding of system integrity.

Additional Tripwire Enterprise Capabilities

- CyberCrime detection, control, and monitoring
- MITRE ATT&CK detection, control, and monitoring
- Create a baseline of the systems
- Monitor the device inventory (s/w, h/w, f/w) for changes
- Monitor the configuration settings for various devices
- Monitor ports, protocols and services
- Monitor critical file systems
- Monitor account management
- Monitor password management
- Monitor Audit Log security
- Monitor log content/configuration
- Monitor for malicious code/spam
- Monitor registry settings
- Provide/Monitor anti-virus state: Installed, running, and up to date
- Provide/Monitor specifications on computers registered in the domain
- Provide/Monitor specifications on users registered in the Domain
- Provide/Monitor a list of installed software on ESX, Linux, Solaris and Windows
- Provide/Monitor a listing of the last password set date for computers
- Provide/Monitor a listing of the last password set date for users
- Full policy remediation guidance
- Full policy auto-remediation workflow and editor
- Asset Tagging profiler and editor

FORTRA™

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.