WHITE PAPER

Security Fundamentals for Federal Agencies

Establish and Sustain the Four Essential Pillars of Federal Cybersecurity

FOUNDATIONAL CONTROLS FOR
SECURITY, COMPLIANCE & IT OPERATIONS

Cybersecurity experts are urging government agencies to protect their data with up-to-date, foundational security controls, and agencies are listening. But how can they determine where exactly to focus their efforts to maximize efficiency and ensure a strong security stance? This white paper details the four key components federal agencies need in order to establish and maintain a robust security posture.

The four pillars of an effective security strategy

- » Policy compliance
- » File integrity monitoring
- » Log management
- » Vulnerability management

Policy Compliance

Policy compliance is a broad term that can encompass different types of policies such as internal agency standards or widespread regulatory requirements. Regardless of which type or types of policies your agency must comply with, auditing will play a central role in the compliance process.

Audits are the methodology used to assess policy compliance. Even if your agency implements all the required controls and capabilities required by a policy, you can still fall into non-compliance by failing to achieve a demonstrable ability to measure your systems against that policy.

Differentiate compliance from controls

It's critical to understand the difference between the implementation of security controls and policy compliance itself. Following the directives of security controls (such as the CIS Controls, formeraly known as the Critical Security Controls) is just one set of actions that help agencies meet compliance. Policy compliance products and solutions that effectively make your control implementation efforts worthwhile possess one or more of the following capabilities:

Provide: Tools that directly provide a required control fall into this category. If an agency has a requirement for vulnerability assessment, the VA tool provides that control.

Validate: Some tools are specifically designed to measure whether another control is in place and configured correctly. These tools validate a control, but they don't provide it directly.

Support: There are definitely cases where a tool or capability doesn't fulfill all the requirements of a required control but makes the use of that control substantially easier or more effective.

Speaking in these terms—provide, validate, support—paves a clearer approach to compliance. Selection of a tool that provides one control doesn't necessarily guarantee validation, so it's important to ask how that control will be validated. At the same time, a powerful tool might not provide or validate, so it's important to assess how other controls are supported. It's important to avoid confusing the controls themselves with their validation.

How policy compliance adds value

Policy compliance tools should be focused on validation and justification for an auditor. Any new policy compliance tool should reduce the time spent preparing for audits by collecting data and delivering it in a usable format. In many cases, that's a report, but it might also include the ability to extract specific data as an auditor requests it. Use previous audits as a guide to determine how the tool might help. Tools should not actually make audits harder to pass.

Policy compliance can also be a budget driver. Return on investment for security is difficult because the outcomes are difficult to predict. Policy compliance is designed to pair a risk with a predictable outcome, usually a fine or other punitive measures. That creates an environment in which budget can be effectively allocated.

That predictable outcome can also be used to secure budget for tools and capabilities that have benefits beyond the specific policy. Compliance can be leveraged to justify budget.

Tripwire Enterprise

Tripwire® Enterprise is an integrated cybersecurity solution suite composed of three primary components: Tripwire File Integrity Manager, Tripwire Policy Manager and Tripwire Remediation Manager. Tripwire Policy Manager continuously assesses system changes and reports on your agency's compliance status with out-of-the-box compliance testing for FISMA, NERC, CIP, SOX, COBIT and many others.

Tripwire Enterprise benefits:

- » Supports over 1,000 policy and platform combinations
- » Reduces audit preparation time and cost with audit-ready reporting
- » Frequently updated to ensure you always have the coverage you need
- » Continuously compares your baseline configurations to policy standards
- » Protects your data with system hardening and compliance enforcement
- » Automates workflows via integrations with SIEMs and change management systems

File Integrity Monitoring

Each and every security breach correlates to a change within a system. That's why IT managers need to understand the importance of change management and file integrity monitoring (FIM). Agency environments require preventive and detective controls that identify change.

AI, machine learning and active threat hunting are certainly providing new tactics in the security industry, but the ability to pinpoint changes across your entire environment is where you'll find the most value.

Integrity monitoring is nothing new, but the core capabilities it utilizes have evolved dramatically in recent years. Change detection is FIM's central functionality, and the scope of your overall integrity management strategy can be even broader.

Shift to integrity management from basic FIM

FIM isn't just for files anymore. It now encompasses a wider range of tools and tactics that fall under the umbrella term "integrity management." Integrity management is composed of four basic steps:

Secure deployment: Ensure that the system's you're deploying meet risk acceptance criteria. First, establish those criteria so that you can measure the security performance of your servers, images and containers across all environments—be they on-premise, virtual or cloud.

Baseline deployed systems: If you don't have a solid baseline, you can't identify changes from it to understand how they affect the risk posture of your systems.

Monitor for change: Once your baseline is established, what process will your agency use to monitor that baseline for changes? Establish an explicit and rigorous change monitoring process that yields high visibility into your entire data ecosystem.

Act on important changes: Most changes don't require action, but you need a reconciliation process that separates the wheat from the chaff. IT managers must be able to quickly assess which changes impact risk and which changes are routine.

Integrity management's critical role

Applying the principles of integrity management helps agencies prevent, detect and investigate security incidents in their systems. The core capabilities of integrity management satisfy a variety of regulatory standards such as the National Institute of Standards and Technology's 800-53 governing security and privacy protocols (NIST 800-53).

NIST 800-53 requires stringent system information and integrity controls. It also calls for the use of "[…] integrity verification tools to detect unauthorized changes" on a number of organization-identified objects. This is included in control SI-07. While integrity verification is required for SI-07, the ability to detect and reconcile changes delivers validation of many other controls.

And while integrity management cannot "[…] create, enable, modify, disable and remove information system accounts in accordance with policy" as the AC-02 account management control calls for, it will provide the ability to capture every single one of those changes for investigation and audit.

Tripwire File Integrity Manager

Integrity management processes can generate staggering amounts of data, and IT professionals don't have the time to pour over that data to see what's relevant and what's merely digital noise. Available as a stand-alone solution or as part of the Tripwire Enterprise tool suite, Tripwire File Integrity Manager brings visibility and business context to the actionable data you need to focus on. Consider Tripwire File Integrity Manager to vastly improve your agency's integrity management.

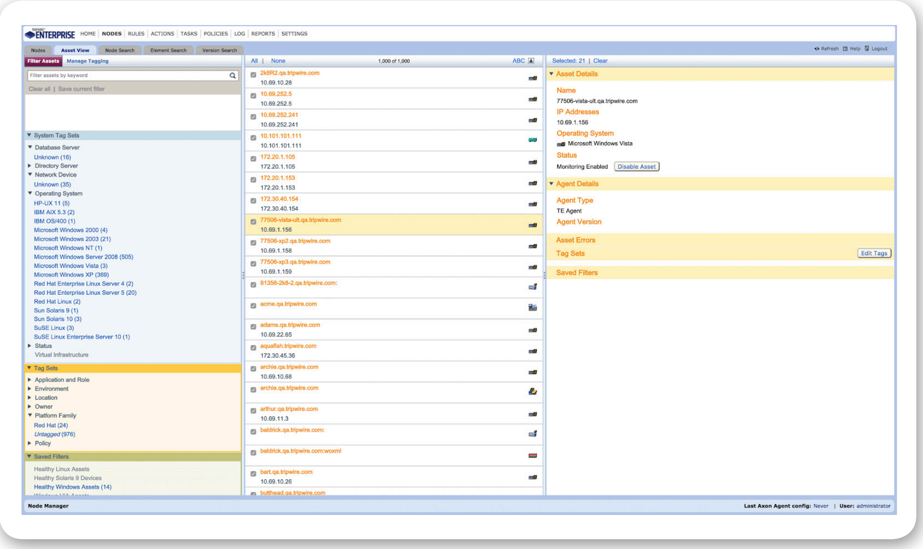
Tripwire File Integrity Manager benefits:

- Real-time change intelligence
- Change prioritization from low to high risk
- Automated reconfiguration for policy compliance
- Integration with change ticketing systems like ServiceNow
- Details pinpointing the "who, what and when" of pertinent events

Log Management

Government agencies must view log management within the context of security incident and event management (SIEM). The SIEM market evolved from collecting log data and correlating it with other data sources to deliver deeper analytical capabilities.

This is part of the reason fields like user behavior analytics and big data analytics have seen so much rapid growth in recent years. Higher demand for analytics means agencies are struggling to deliver the right data and insights to the right destinations.



1,000 of 1,000

System Tag Sets
- Database Server
  - Unknown (16)
- Directory Server
- Network Device
  - Unknown (35)
- Operating System
  - HP-UX 11 (5)
  - IBM AIX 5.3 (2)
  - IBM OS/400 (1)
  - Microsoft Windows 2000 (4)
  - Microsoft Windows 2003 (21)
  - Microsoft Windows NT (1)
  - Microsoft Windows Server 2008 (505)
  - Microsoft Windows Vista (3)
  - Microsoft Windows XP (369)
  - Red Hat Enterprise Linux Server 4 (2)
  - Red Hat Enterprise Linux Server 5 (20)
  - Red Hat Linux (2)
  - Sun Solaris 9 (1)
  - Sun Solaris 10 (3)
  - SuSE Linux (3)
  - SuSE Linux Enterprise Server 10 (1)
- Status
- Virtual Infrastructure

Tag Sets
- Application and Role
- Environment
- Location
- Owner
- Platform Family
  - Red Hat (24)
  - *Untagged* (976)
- Policy

Saved Filters
- Healthy Linux Assets
- Healthy Solaris 9 Devices
- Healthy Windows Assets (14)

2k8R2.qa.tripwire.com
10.69.10.28
10.69.252.5
10.69.252.5
10.69.252.241
10.69.252.241
10.101.101.111
10.101.101.111
172.20.1.105
172.20.1.105
172.20.1.153
172.20.1.153
172.30.40.154
172.30.40.154
77506-vista-ult.qa.tripwire.com
10.69.1.156
77506-xp2.qa.tripwire.com
10.69.1.158
77506-xp3.qa.tripwire.com
10.69.1.159
81356-2k8-2.qa.tripwire.com:
acme.qa.tripwire.com
adams.qa.tripwire.com
10.69.22.65
aquafish.tripwire.com
172.30.45.36
archie.qa.tripwire.com
10.69.10.68
archie.qa.tripwire.com
arthur.qa.tripwire.com
10.69.11.3
baldrick.qa.tripwire.com:
baldrick.qa.tripwire.com:woxml
bart.qa.tripwire.com
10.69.10.26
butthead.qa.tripwire.com

Asset Details
Name
77506-vista-ult.qa.tripwire.com
IP Addresses
10.69.1.156
Operating System
Microsoft Windows Vista
Status
Monitoring Enabled
Agent Details
Agent Type
TE Agent
Agent Version
Asset Errors
Tag Sets
Saved Filters

Last Axon Agent config: Never | User: administrator

Fig. 1 Tripwire Enterprise provides both robust FIM and comprehensive policy compliance.

From a cost perspective, customers can find themselves paying for data that doesn't need to be in the SIEM or paying for log storage instead of analytics. These trends put pressure on federal IT professionals to spend more efficiently while strengthening the security of their log management practices.

Log management makes security visible

Security logging and analysis can help IT teams determine the location of attackers, identify malicious software and track activities on victim machines. "Even if the victims know that their systems have been compromised, without protected and complete logging records they are blind to the details of the attacks and to subsequent actions taken by the attackers," according to the Center for Internet Security (CIS).

"Without solid audit logs, an attack may go unnoticed indefinitely and particular damages done may be irreversible." If IT managers are not collecting, storing and analyzing log data for every asset in the organization, they will have significant gaps in their cyber situational awareness.

Log management simplifies compliance

It's compliance concerns—not security—that usually drive IT teams toward log management investments. The Federal Information Security Management Act is one of many regulations that requires log management components. In FISMA's case, log management is defined by NIST in SP 800-53.

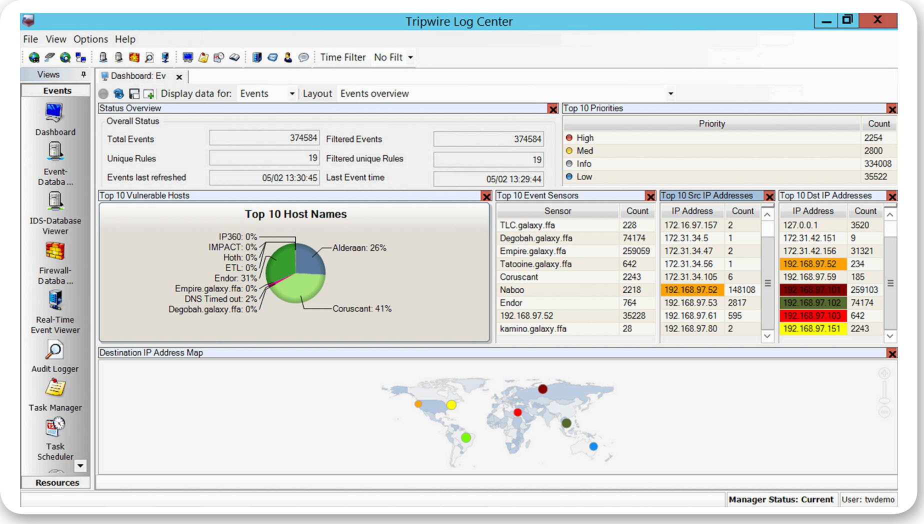
NIST 800-53 provides the most detailed exploration of log management requirements available, and it's certainly the most applicable to government agencies. NIST 800-53's requirements for logging are listed in the Audit and Accountability section and include defining a process for collecting logs, what log events need to be captured, what detail needs to be included in captured events as well as retention guidance and response processes.

Tripwire Log Center

The correlation engine in Tripwire Log Center® automatically identifies and responds to events of interest using a logical flow of one or more conditions. Actions can include creating a work ticket, sending a notification email, or running a command. Whether you collect logs strictly for regulatory compliance or to increase awareness of credible cyber threats, Tripwire Log Center ensures the process is secure and reliable.

Tripwire Log Center benefits:

- Reliable log collection, analysis and delivery
- Tight integration with your existing infrastructure
- Critical events highlighted on a customized dashboard
- Automated remediation and alerting with triggered scripts
- Reduced noise with pre-processed data prior to passing SIEM
- Quicker threat detection with a large library of correlation rules



Display data for: Events

Layout: Events overview

Status Overview

Overall Status

Total Events	374584	Filtered Events	374584
Unique Rules	19	Filtered unique Rules	19
Events last refreshed	05/02 13:30:45	Last Event time	05/02 13:29:44

Top 10 Priorities

Priority	Count
● High	2254
● Med	2800
● Info	334008
● Low	35522

Top 10 Vulnerable Hosts

Top 10 Event Sensors

Sensor	Count
TLC.galaxy.ffa	228
Degobah.galaxy.ffa	74174
Empire.galaxy.ffa	259059
Tatooine.galaxy.ffa	642
Coruscant	2243
Naboo	2218
Endor	764
192.168.97.52	35228
kamino.galaxy.ffa	28

Top 10 Src IP Addresses

IP Address	Count
172.16.97.157	2
172.31.34.5	1
172.31.34.47	2
172.31.34.56	1
172.31.34.105	6
192.168.97.52	148108
192.168.97.53	2817
192.168.97.61	595
192.168.97.80	2

Top 10 Dst IP Addresses

IP Address	Count
127.0.0.1	3520
172.31.42.151	9
172.31.42.156	31321
192.168.97.52	234
192.168.97.59	185
192.168.97.101	259103
192.168.97.102	74174
192.168.97.103	642
192.168.97.151	2243

Manager Status: Current | User: twdemo

Fig. 2 Tripwire Log Center provides reliable log collection, analysis and delivery.

Vulnerability Management

Vulnerability management is fundamentally about risk reduction presented by vulnerabilities within a system environment. Executive Order 13800 delineates the importance of assessing vulnerabilities: "Known but unmitigated vulnerabilities are among the highest cybersecurity risks faced by executive departments and agencies."

Vulnerability management and compliance

It's important to consider that meeting compliance doesn't always ensure that your vulnerability management program is adequately robust. Passing an audit is not the same as reducing vulnerability risk. If compliance is part of your organization's drive for vulnerability assessment tools, achieving clarity on the objectives can help you avoid barriers to success down the road.

Vulnerability management and compliance should work hand in hand. For example, if you're part of the Department of Defense and subject to Command Cyber Readiness Inspection (CCRI) audits, then a vulnerability assessment tool is a key component in audit preparation. Understanding which assets are on the network, their vulnerabilities, and which to fix first is a crucial part of CCRI preparation.

Vulnerability management is a process

The process of reducing risk from vulnerabilities is just that: a process. There are tools that make that process substantially more efficient, but they don't replace the need for the process or the people to run it.

It's entirely possible to create a complex workflow diagram for vulnerability management, but at its core, there are really three steps:

Discover: You have to start by deploying a solution that can pinpoint the vulnerabilities you have, and by extension all of the assets on which you might find those vulnerabilities. The output of discovery is some kind of inventory of assets and vulnerabilities.

Report: In order to take action on that inventory, organizations need reporting tools. A simple report might just be a list of vulnerabilities found, but in most cases, there needs to be some scoring method of prioritization for both the vulnerability and the sensitivity of the asset on which it resides.

Remediate: Many vulnerability management programs stop with the first two of these three steps and count themselves as successful, but unless meaningful remediation is part of the equation, you haven't accomplished the core objective of reduction of risk. The challenge is that remediation, whether through applying a patch or some other step, is the most complicated step. The key question to answer is how you can connect the prioritized reporting of vulnerabilities to the most successful workflow in your organization.

Tripwire IP360

Tripwire IP360™ serves as a complete vulnerability management toolkit for federal agencies. It automatically scores risks to help you address significant vulnerabilities right away, allowing you to take a look at the granular details around each risk. It uses a unique fingerprinting method to produce a comprehensive asset inventory and identify vulnerabilities across each and every endpoint connected to your network. When you apply Tripwire IP360 to your environment, you can expect to reduce risk scores by more than 50 percent.

Tripwire IP360 benefits:

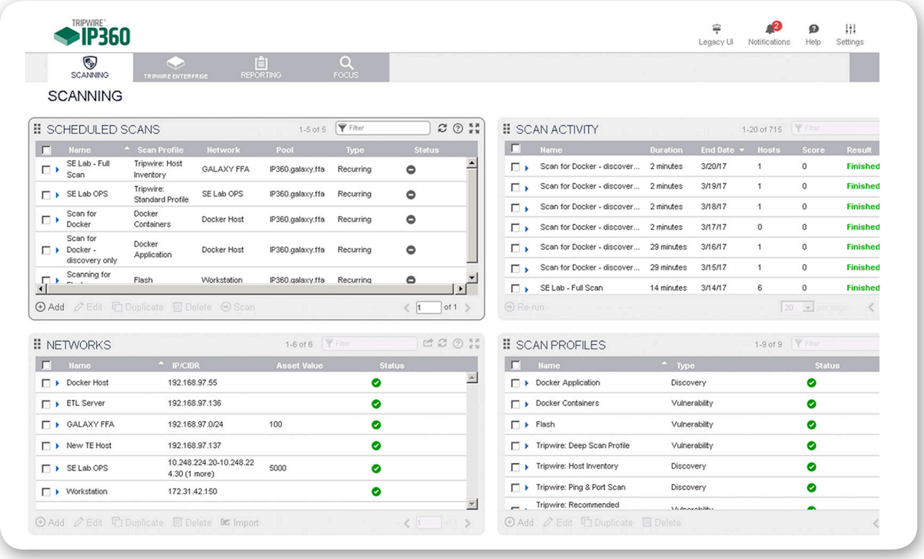
- » Faster vulnerability scans with fewer false positives
- » Combines agent-based and agentless scanning results
- » Supports on-premises, cloud and hybrid environments
- » Efficient and accurate vulnerability scoring and prioritization
- » Open APIs enable integration with help desk and asset management
- » Minimizes manual efforts through integration with your existing toolsets

Summary

Many federal agencies find themselves in need of a substantial security overhaul. They need advanced tools and techniques to keep up with both the rapid proliferation of cyberattacks and the requirements of regulatory frameworks meant to stop them. File integrity monitoring, log management, policy compliance and vulnerability management are the four security fundamentals your agency must address, and Tripwire products offer the out-of-the-box coverage federal agencies require.

Request a Demo

Let us take you through a demo of Tripwire's security and vulnerability management products and services customized to your specific IT security and compliance needs. Visit **tripwire.com/contact/request-demo/**



SCANNING

SCHEDULED SCANS 1-5 of 5

☐	Name	Scan Profile	Network	Pool	Type	Status
☐	SE Lab - Full Scan	Tripwire: Host Inventory	GALAXY FFA	IP360.galaxy.ffa	Recurring	⊖
☐	SE Lab OPS	Tripwire: Standard Profile	SE Lab OPS	IP360.galaxy.ffa	Recurring	⊖
☐	Scan for Docker	Docker Containers	Docker Host	IP360.galaxy.ffa	Recurring	⊖
☐	Scan for Docker - discovery only	Docker Application	Docker Host	IP360.galaxy.ffa	Recurring	⊖
☐	Scanning for	Flash	Workstation	IP360.galaxy.ffa	Recurring	⊖

SCAN ACTIVITY 1-20 of 715

☐	Name	Duration	End Date	Hosts	Score	Result
☐	Scan for Docker - discover...	2 minutes	3/20/17	1	0	Finished
☐	Scan for Docker - discover...	2 minutes	3/19/17	1	0	Finished
☐	Scan for Docker - discover...	2 minutes	3/18/17	1	0	Finished
☐	Scan for Docker - discover...	2 minutes	3/17/17	0	0	Finished
☐	Scan for Docker - discover...	29 minutes	3/16/17	1	0	Finished
☐	Scan for Docker - discover...	29 minutes	3/15/17	1	0	Finished
☐	SE Lab - Full Scan	14 minutes	3/14/17	6	0	Finished

NETWORKS 1-6 of 6

☐	Name	IP/CIDR	Asset Value	Status
☐	Docker Host	192.168.97.55		✓
☐	ETL Server	192.168.97.136		✓
☐	GALAXY FFA	192.168.97.0/24	100	✓
☐	New TE Host	192.168.97.137		✓
☐	SE Lab OPS	10.248.224.20-10.248.224.30 (1 more)	5000	✓
☐	Workstation	172.31.42.150		✓

SCAN PROFILES 1-9 of 9

☐	Name	Type	Status
☐	Docker Application	Discovery	✓
☐	Docker Containers	Vulnerability	✓
☐	Flash	Vulnerability	✓
☐	Tripwire: Deep Scan Profile	Vulnerability	✓
☐	Tripwire: Host Inventory	Discovery	✓
☐	Tripwire: Ping & Port Scan	Discovery	✓
☐	Tripwire: Recommended	Vulnerability	✓

Fig. 3 Tripwire IP360 is a complete vulnerability management solution for agencies of any size.

Tripwire is a leading provider of security, compliance and IT operations solutions for enterprises, industrial organizations, service providers and government agencies. Tripwire solutions are based on high-fidelity asset visibility and deep endpoint intelligence combined with business context; together these solutions integrate and automate security and IT operations. Tripwire's portfolio of enterprise-class solutions includes configuration and policy management, file integrity monitoring, vulnerability management, log management, and reporting and analytics. **Learn more at** tripwire.com

The State of Security: Security News, Trends and Insights at tripwire.com/blog
Follow us on Twitter @TripwireInc » **Watch us at** youtube.com/TripwireInc