SOLUTION BRIEF

Automating FISMA Compliance

Using Tripwire Security Configuration Management

Tripwire solutions have a history with government agencies, offering an 'iron-clad defense,' or foundation for a layered compliance and security strategy.

FISMA requires federal agencies, and by extension, the foundations, educational institutions, organizations that receive federal funds as well as the contractors that do business with them, to develop, document, and implement information security programs to protect the confidentiality, integrity and availability of the data and systems that support government operations and assets.

In meeting compliance, agencies and organizations subject to FISMA compliance really face a dual responsibility. First, is to meet FISMA requirements, by identifying and resolving risks, and performing ongoing assessment and testing. Second, is to be able to protect critical information security assets. This latter issue means being able to confidently share information and resources with trusted parties, and to be able to have confidence that those parties are providing appropriate levels of information protection.

In fact, the loss of privacy of employee and citizen data due to a security breach, and not knowing who is accessing systems and in what manner, are the top worries that keep federal managers up at night. While there has been marked improvement since the 2005 White House Office of Budget and Management (OMB) Annual Report to Congress on Implementation of FISMA, uneven implementation of security measures across the federal government continues, resulting in weaknesses that still must be corrected.

FISMA Reporting Challenges and Tedious Tasks

NIST is the doorway to information on what is required by the FISMA legislation. But understanding and reporting FISMA results each year can be a

tedious process, much in part because it is a complicated, manual process with ambiguous guidelines. Agencies use various methods to collect the required security data, using databases, spreadsheets and other documents. There is no streamlined way to integrate all of the data coming in from various sources and methods. As one agency head recently remarked, FISMA reporting is "spreadsheet chaos."

Audit preparation time is also consuming and expensive. This is mainly because FISMA requires enormous effort, budget and IT resources, all of which takes away from the agency's work on mission objectives. Funding is also an issue. OMB reported agencies spent approximately $5.5 billion in fiscal year 2006 to meet FISMA requirements. It is predicted that for agencies to comply with FISMA will require upwards of $27.9 billion between 2008 and 2012.

Barely Passing the Grade

According to the OMB, the overall grade on the annual report card has been stalled at D or D+ for the previous three years. In 2006, seven agencies improved their grades, six got worse and 10 remained the same.

However, making a passing grade doesn't mean your agency's data is now secure. In reality, FISMA does not require secure IT systems; it requires a process for assessing, testing and managing IT security. The annual grades are based largely on how good a job an agency is doing at inventorying, testing, certifying and accrediting its IT systems. To really secure systems, data and access, a new approach is needed that clarifies security requirements and uses automated solutions that manage configuration assessments.

High-Level Minimum Security Requirements

Since the release of Special Publication 800-53 Recommended Security Controls for Federal Information Systems, NIST has begun to promote an Information Security Automation Program (ISAP) to enable automation and standardization of technical security operations.

This evolution to the tactical objectives of ISAP focuses on the need to adopt automated solutions. This falls mainly into IT's lap, and that is a good thing. For it is within IT that Tripwire can provide the means to automate continuous testing and reporting of critical IT process controls, reduce manual processes, and continually provide a detailed audit and forensic trail that meets FISMA requirements. Industry experts agree: "Organizations should use compliance as an opportunity to implement technologies and processes that improve operational security as well as provide support for FISMA... compliance."1

Achieving compliance through good security practices is always more effective and efficient than achieving security through good compliance.

Automating FISMA Compliance with Tripwire Solutions

Achieving a known and trusted state is a challenging task for even the most technically adept and process-focused organizations. That's why more than 400 government agencies have adopted Tripwire software and service solutions to help simplify the task of automating compliance with an ever-growing number of compliance initiatives and requirements. Tripwire® Enterprise enables this process by combining file integrity monitoring with security configuration management.

Security Configuration Management

With security configuration management (SCM), Tripwire Enterprise can proactively test and assess systems against pre-configured, out-of-the-box policies. Tripwire leverages industry standards, specifically benchmarks from the Center for Internet Security (CIS), the National Institute of Standards and Technology (NIST), as well as the Defense Information Systems Agency (DISA). These benchmarks include tens of thousands of configuration assessments enabling automatic sustainable policy compliance testing for FISMA.

File Integrity Monitoring (FIM)

Tripwire Enterprise monitors file integrity and file structures on information systems, including hardware, software, and network and security infrastructure, then provides detailed change information to enable agency staff to quickly pinpoint, analyze and recover from any undesirable change. In fact, Tripwire Enterpise delivers assurance that authorized changes are completed, and that unauthorized or ad hoc changes that circumvent policy are detected and immediately reported. With a verifiable audit trail, staff can then document every step to regulators which are provided in detailed reports to demonstrate

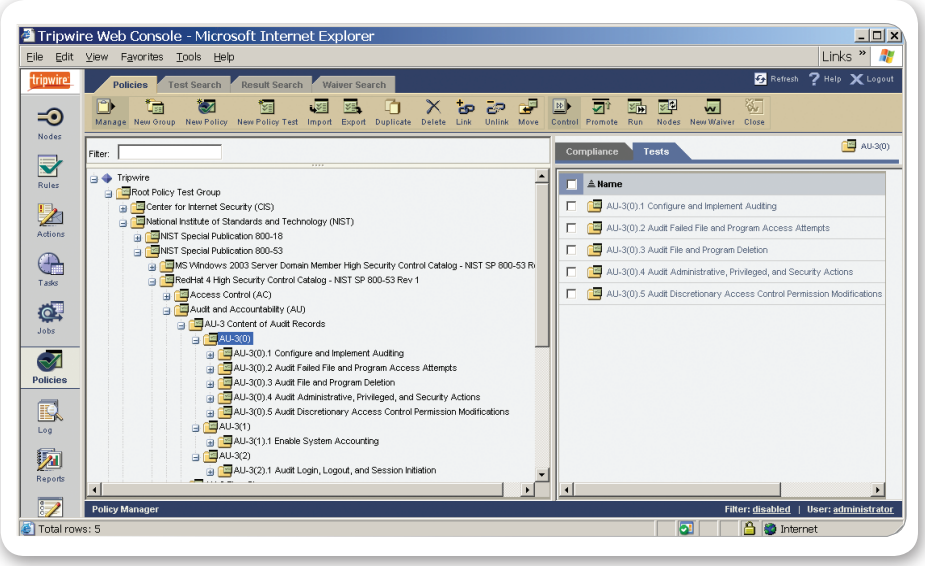


Fig. 1 Tripwire Enterprise console showing the selection of NIST SP 800-53A policy for Red Hat Enterprise Linux 4.

that changes to information systems can be detected, corrections verified, and changes explained.

The Ideal Combination for Automated Compliance

By combining SCM with FIM, Tripwire Enterprise assesses configurations across the data center to make certain they are within policy and compliant, ensuring systems achieve a known and trusted state. Tripwire Enterprise then maintains that known and trusted state by establishing a secure baseline and, through continuous change detection, monitors for deviations from it.

Benefits of Using Tripwire Enterprise for FISMA Compliance

Tripwire solutions have a long history with government agencies, offering an 'iron-clad defense', or foundation for a layered security strategy. This has enabled public sector IT staff to protect electronic government assets from loss, misuse, or unauthorized access and modification. Now, with SCM for FISMA-required policies, Tripwire offers an automated method for achieving and maintaining compliance. The value Tripwire Enterprise offers is immediate.

Reduce time and resources. Tripwire Enterprise gives you the evidence required to verify compliance with a single, verifiable audit trail. With Tripwire, you receive sophisticated, automated reporting required to complete audits, reducing the resources required to prepare for audits.

Maintain continuous compliance. Tripwire Enterprise exposes unauthorized changes through reconciliation with expected changes and allows IT staff to immediately identify any exceptions and trigger remediation of configurations that do not conform to policy.

Mitigate security risks. Tripwire Enterprise monitors and reports on every change made across the infrastructure regardless of source, detecting unauthorized change and non-conforming configurations to proactively discover and manage security and compliance exposure.

Tripwire Enterprise and the Specific NIST Controls

Tripwire Enterprise can facilitate compliance with many NIST controls right out of the box. With Tripwire you first assess configurations across the data center to make certain they are compliant. From information that is then continuously collected, you're able to generate needed reports and evidence that configurations are not unexpectedly changing, making your FISMA audit a quick task instead of a lengthy project.

Below are several examples of how Tripwire Enterprise meets the audit evidence required in NIST SP 800-53A.

Control Family: AU
Control Name: AU-3 Content of Audit Records

The NIST control AU-3 specifies that the subject system must produce audit records that contain sufficient information to establish what events occurred, the sources of the events, and the outcomes of the events.

Tripwire Enterprise provides a means to examine the audit trail settings of the subject system, as well monitoring those settings for change over time. If there is a configuration file, utility or method to examine an audit setting manually, those settings can be similarly checked by the Tripwire Policy Manager. Tripwire File Integrity Manager records when and who changed them from the baseline.

In Figure 1, Policy Manager in Tripwire Enterprise illustrates the selection of NIST SP 800-53A Policy for Red Hat Enterprise Linux 4. The open policy group illustrates the control family and the displays tests that have been created to help monitor this important control area. Tripwire's policy includes 11 tests that span both the base (0) area of the control and the enhanced controls (1) and (2). Depending on which assurance requirements of the subject system, Tripwire provides tests for either Low, Moderate and High baseline applications.

The base controls are fulfilled with the following tests:

» **Configure and Implement Auditing**
Pass indicates that auditing is enabled on a Red Hat system. This test was specified from the UNIX Security Checklist, V5R1.7 (15 July 2007), reference UNIX STIG: 3.16.

Control Family: AC (Access Control)
Control Name: AC-7 Unsuccessful Login Attempts

The NIST Control AC-7 specifies that the subject system must enforce a limited number of consecutive invalid attempts during specific time period (defined by the agency).

In Figure 2, the Tripwire Enterprise policy tests are exposed for this NIST Control family, customized for the Solaris 10 environment. In this platform, the testable controls will support Low, Moderate and High baseline assurance.

These tests are:

» **Verify /etc/default/login contains 'RETRIES=5' or less**
Pass indicates that the system configuration is set to count for 5 unsuccessful login attempts. This test was specified from CIS Solaris 10 Benchmark (Section 6.15, v. 2.1.1).

» **Verify /etc/security/policy.conf contains 'LOCK_AFTER_RETRIES=YES'**
Pass indicates that the system will lock the account until released by an administrator when the maximum unsuccessful attempts is exceeded. This test was specified from UNIX Security checklist (GEN000460) V5R1.7 (15 July 2007) and references UNIX STIG: 3.16.

Control Family: CM (Configuration Management)
Control Name: CM-4 Monitoring Configuration Changes

The organization monitors changes to the information system and conducts security impact analyses to determine the effects of the changes.

Tripwire Enterprise continuously monitors configuration changes across the

entire data center as often as needed. It also provides robust, flexible reporting with rules already defined and tuned, covering the OS in an intelligent manner. When integrated with an enterprise management system as part of the change management process, Tripwire detects when someone circumvents security systems and processes designed for production system. Such detection allows IT to do the appropriate impact analysis and better manage security testing.

Tripwire Enterprise provides reporting to help monitor configuration changes. An example of Tripwire coverage for CM-4 is in the NIST SP 800-53A the Changes by Severity report. This report shows the total number of changes detected on selected monitored systems that fall within a specified range of severity levels, helping operations staff identify changes that have the potential to adversely introduce security risk and impact service quality.

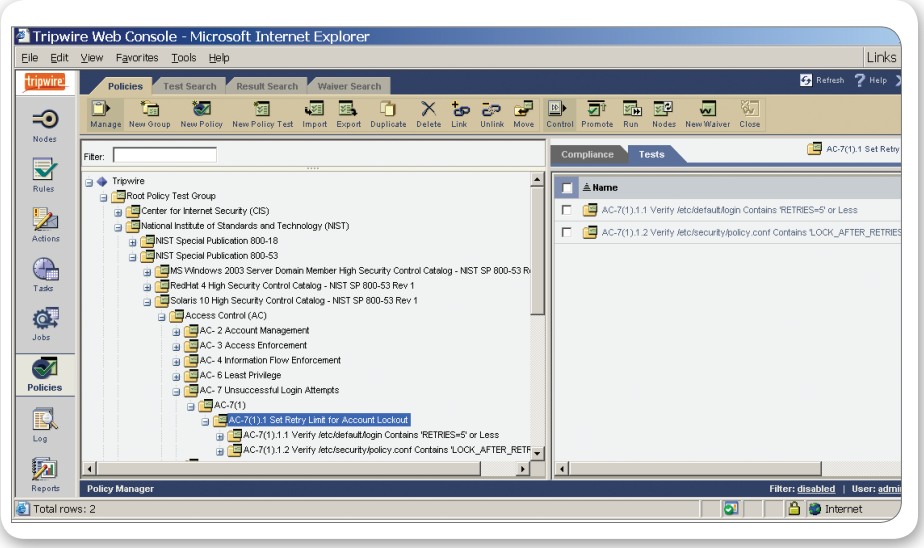
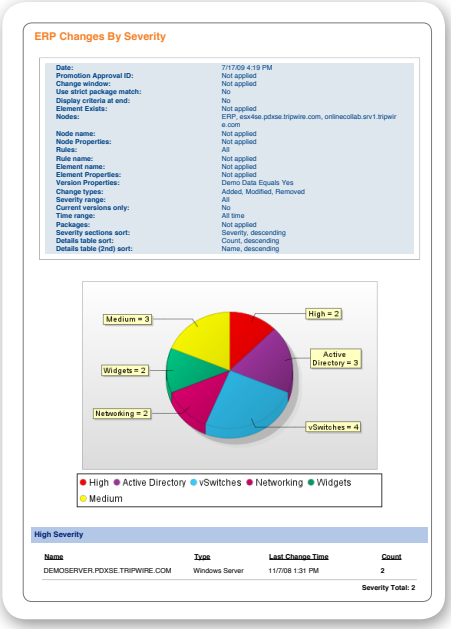


Fig. 2 Policy tests are exposed for the NIST "Access Control" family, customized for the Solaris 10 environment.

Fig. 3 The "Changes by Severity" report provides an example of coverage by Tripwire Enterprise of the NIST SP 800-53A CM-4 "Monitoring Configuration Changes" control.



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