tripwire

FILE INTEGRITY MONITORING BUYER'S GUIDE

Compliance and Security for Virtual and Physical Environments

FOUNDATIONAL CONTROLS FOR
SECURITY, COMPLIANCE & IT OPERATIONS

What is File Integrity Monitoring?

In an IT network, a file can range from simple text file to a configuration script, and any change can compromise its integrity. A change to a single line item in a 100-line script could prove detrimental to the entire file or even operating system. For example, incorrectly assigning the wrong IP address to a startup script or a newly installed network printer could disrupt the network. Below are some examples of the type of configuration settings a file integrity monitoring solution detects and monitors:

- Registry Entries
- Configuration files and parameters
- .exe
- File and directory permissions
- Tables
- Indexes
- Stored procedures
- Rules
- Access control lists (ACLs)
- Adds/Deletes/Modifications
- Auditing/logging
- System files
- Web root
- Ports and services
- Protocols in use
- Remote access

File integrity monitoring (FIM) solutions, also called change auditing solutions, ensure the file for a server, device, hypervisor, application, or other element in the IT infrastructure remains in a known good state, even in the face of inevitable changes to these files. Ideally a FIM not only detects any changes to files, but also includes capabilities that help IT immediately remediate issues caused by improper change. The following sections describe the capabilities often available with file integrity monitoring solutions.

ESTABLISHES A BASELINE

When IT deploys a system/component into its technology infrastructure, it typically does so with the knowledge that the component is initially configured appropriately. A FIM solution captures the known good state of the entire system's IT configuration settings when it is deployed—or when it has been configured with recommended settings—and uses this state as a baseline configuration against which the solution can compare a later configuration. Many times this configuration state is referred to as a golden, compliance, or configuration baseline. A baseline-to-current-configuration comparison lets the solution immediately and automatically detect discrepancies caused by change.

Given the rapid deployment of virtual machines, an ideal file integrity monitoring solution would also include in the baseline the configurations of virtual environment elements. These elements include the physical server, hypervisor, each guest OS, and all applications and databases running on a guest OS.

ALERTS AND NOTIFIES I.T.

When the solution detects change, IT needs to determine whether or not the integrity of a file has been compromised and whether the change requires immediate attention. IT should have the ability to specify which devices and files are critical—and therefore require high-level, immediate attention—versus those that do not. For example the configuration file of an e-commerce site or a database populated with sensitive customer financial or medical data would warrant immediate attention, while configuration changes to non-critical systems could be given a "best effort" response.

Based on whether a system was viewed as critical or non-critical, the solution should be able to send alerts and notifications using a variety of methods to be sure IT receives them. For example, an email alert is worthless if the detected change disrupted email service. Other methods of notifying IT include an alert in the system tray, SNMP, CMD, SYSLOG, page, or within a management console. Early detection enables the administrator to quickly make any necessary corrections before downstream effects become critical.

Return to Table of Contents

What Gets Monitored?

File integrity monitoring solutions watch for changes to files associated with the servers, databases, routers, applications, and other devices and elements in the enterprise IT infrastructure. Files monitored may include registry files, configuration files, executables, file and directory permissions, tables, indexes, stored procedures, rules—the list goes on. In fact, the reality is today's IT infrastructure is far too complex to be monitored manually, even in smaller organizations.

File attributes being monitored may include hostname, username, ticket number, date and time stamp and operation type. This table provides an overview of the type of attributes these solutions may monitor.

Server File Systems	Databases	Network Devices	Directory Services	Hypervisors	Applications
Registry entries	Tables	Routing tables	Privileged group	Permissions	Web server keys
Configuration files	Indexes	Firewall rules	Group policy options	Firewall settings	System files
.exe	Stored procedures	Configuration files	RSoP	Auditing/logging	Logs
File permissions	Permission grants	ACLs		Access controls	Registry settings

This table provides a sampling of the type of IT configurations these solutions may monitor:

WINDOWS	UNIX
Access time	Access time
Creation time	Change time
Write time	Modify time
Size	Size
Package data	Package data
Read-only	ACL
DACL	User
SACL	Group
Group	Permissions
Owner	Growing
Growing	MD5
MD5	SHA-1
SHA-1	
Hidden flag	
Stream count	
Stream MD5	
Offline flag	
System flag	
Temp flag	
Compressed flag	
Archive flag	

Return to Table of Contents

A Checklist of Product Requirements

We've so far described what file integrity monitoring is and why it's needed. You've also learned what a FIM solution monitors and below are some must-haves for the solution you choose:

- Analyzes and prioritizes each detected change
- Helps reconcile authorized versus unauthorized change
- Helps determine if a change took systems out of compliance
- Provides assistance in remediation

Following are detailed checklists for what you should look for when evaluating any file integrity monitoring solution:

INTEGRITY VERIFICATION

The following requirements address how any file integrity monitoring solution should verify file and attribute integrity.

INTEGRITY VERIFICATION	Y / N
Can automatically check for changes to file/directory contents.	
Can automatically check for changes to file/directory permissions.	
Can automatically check for changes to file/directory time/date stamps.	
Can automatically check for changes to file/directory names.	
Can automatically check for changes to file/directory ownership.	
Can automatically check for additions/modifications/deletions to Windows registry keys.	
Can check for file content changes using cyclic redundancy checking and/or digital signature checking.	
Supports multiple hashing algorithms (e.g. MD5, SHA).	
Can automatically detect changes to access control lists.	
Can monitor security identifier and descriptor.	
Ability to correlate event audit logs to determine which user made a change.	
Ability to detect changes to server file systems.	
Ability to detect changes to databases.	
Ability to detect changes to network devices.	
Ability to detect changes to directory services file systems.	
Ability to detect changes to hypervisor file systems.	
Ability to detect changes to virtual workloads.	
Ability to detect changes to virtual network devices (vSwitches).	
Ability to detect changes to application file systems.	
Ability to archive new versions of configurations as changes are detected and baseline configurations evolve.	
Examines parts of configuration file that apply to a compliance policy (internal and external) and compares the actual to the expected.	
Ability to reconcile detected changes with change tickets in a Change Management System (CMS) or a list of approved changes.	
Ability to analyze changes in real time to determine if they impact file integrity based on conditions under which change was made, type of change made and user-specified severity of a change.	

Return to Table of Contents

Operational Requirements

The following requirements address how any file integrity monitoring solution is managed and supported from a user perspective.

OPERATIONAL REQUIREMENTS	Y / N
Ability to generate a baseline of a server(s) so that integrity is based on a known good state.	
Ability to create a single baseline that can be distributed to a group of servers to verify differences from baseline (i.e. configuration verification).	
Execution of commands based on integrity violations.	
Policy files can be remotely distributed via a console to one or more machines.	
Policy templates are available from vendor.	
Files and directories can be grouped together in policy template (rule blocks).	
Specify severity level to individual files and/or directories.	
Supports file directory recursion.	
Console can view status of machines.	
Console can group agents.	
Ability to have monitoring (view-only) only consoles available for defined users.	
Templates can utilize wildcards or variables (to encompass minor differences in file system contents between systems).	
Can operate through firewall (ports opened).	
Works well in low bandwidth connections.	
Can update snapshot database from console.	
Ability to easily and quickly update multiple baselines at once, in cases where routine maintenance and/or changes cause integrity violations.	

OPERATIONAL REQUIREMENTS	Y / N
Ability to automatically promote baseline.	
Ability to auto-promote changes when real-time analysis of change indicates they are inconsequential or beneficial.	
Management console that is cross platform (i.e. Windows and Unix).	
Management console can detect status of agents.	
Allows users to quickly compare two versions and quickly isolate changes or differences between versions.	
Agents operate on Windows , Linux and Unix.	
Can change agent passphrases from console.	
Transfer only delta change information for each scan (after the first), not all configuration data each time	
Scalability to address requirements of both individual departments and entire enterprise worldwide.	
Ability to provide users access from anywhere to a single location which allows them to view, search, and compare configurations.	
Provides immediate access to detailed change information.	
Arrange and manage monitored components in a number of ways including by location, device type, and responsibility.	
Enables explanations, descriptions, or labels to be annotated to any version by users.	
Provides authorized users the ability to establish one specific version as a trusted configuration for each system.	
Provides standard sets of defaults and templates for each operating environment	

Return to Table of Contents

Security and Control Requirements

The following requirements address security requirements that any file integrity monitoring solution should include.

SECURITY AND CONTROL	Y / N
Establish levels of access and control for specific groups of users.	
Assigns established access and control to particular groups of devices.	
Provides secure communication between devices and database.	
Increases ability to audit the network by placing relevant change information in one central repository	
Informs authorized persons of when, how and who made changes.	
Provides proof to management that various departments are in compliance with set security policies.	
Enables compliance with security and regulatory requirements (e.g. CIS, PCI, ISO, SOX, FISMA, FDCC, FFIEC, NERC, HIPAA, JSOX, GLBA, etc.)	
Reports devices that don't meet established operational or regulatory policies.	
Analyzes changes in real time to determine if they introduce risk based on conditions under which change was made, type of change made and user-specified severity of a change.	
Default policy templates to automatically check detected changes against internal or external policies.	
Console has auditing facilities.	
Communication link between agent and console is secure (SSL).	
Ability to verify agent security and pass phrases.	

Return to Table of Contents

Enterprise Management Integration Requirements

The following requirements address integration requirements that any file integrity monitoring solution should include.

INTEGRATION	Y / N
Command line interfaces and or API to allow for custom integration.	
Launch in context commands to provide the ability to launch and take actions from other EMS systems.	
Interface launch commands (toolbar actions) to provide one click actions.	
Integration or links to change ticketing systems (e.g. HP OpenView, BMC Remedy, Peregrine, Tivoli) to correlate and match requested change tickets to actual changes.	
Integrates with security information and event management (SIEM) solutions to provide log management capabilities and correlate change and compliance status information with security event information from a single point of control.	
Ability to create tickets and/or incidents in change management system based upon integrity violations.	
Integration into virtual management console to keep inventory information consistent and help secure virtual environments.	

Reporting and Alerting Requirements

The following requirements address reporting and alerting functionality that any file integrity monitoring solution should include.

REPORTING AND ALERTING	Y / N
Product has multiple levels of reporting.	
Provides executive level summary reports/dashboards.	
Reports can be sent via email.	
Reports can be sent as a SNMP trap.	
Reports can be sent to syslog.	
Reports can be printed.	
Reports can be archived locally.	
Reports clearly denote severity levels of integrity violations.	
Reports can be filtered and searchable.	
Reports can be exported to other applications (CSV, XML or HTML format).	
Reports can be created on demand.	
Reports can easily be customized.	
Sends alerts to a Web Console, Network Consoles, email and pagers whenever a high-priority file, content or configuration change is detected.	

REPORTING AND ALERTING	Y / N
Alerts users when configurations change and introduce risk or non-compliance, and provides details on what change was made and who made the change.	
Alerts can be based on complex combinations of events using Boolean algebra (i.e. criteria sets)	
Provides a single source of change information.	
Specifies the relative significance of a change according to the monitoring rules for a system component.	
Enables searches of configuration histories and audit logs for specified content using a variety of search criteria and filters.	
Allows searching to be predefined or saved for future use by all users.	
Identifies all devices whose configurations differ from their designated baselines, or either contain or are missing specified configuration settings.	
Audit logging that provides a change control record for all change activity by recording detected changes, added and deleted devices, modified user accounts, etc.	
Console can send alert when agent connections are lost.	
Can differentiate authorized vs. unauthorized changes based on change window, who made the change, what the change was, etc.	
Provides a role-based and customizable user interface.	

Return to Table of Contents

Beyond FIM: Policy Compliance Management

Compliance policy management ensures the integrity of your IT configurations by proactively comparing them against internal policies or external policies for standards, regulations and security best practices. By proactively identifying misconfiguration risks and providing prescriptive remediation guidance, policy compliance management enables a rapid return to a known and trusted state.

When compliance policy management and file integrity monitoring capabilities are combine, you gain complete configuration control and continuous compliance. You get the initial confidence that systems are configured in a known and trusted state, and confidence that by monitoring for and detecting any improper change they'll maintain that state.

COMPLIANCE POLICY MANAGEMENT REQUIREMENTS

Superior file integrity monitoring—FIM that includes compliance policy management—requires not only the detection and reporting of unauthorized changes, specific types of changes, changes made under certain conditions and user-specified severity of changes. It must also perform an assessment of how an existing—or just changed—configuration compares with established organizational and regulatory guidelines. Capabilities to look for are provided in this final checklist.

COMPLIANCE POLICY MANAGEMENT	Y / N
Ability to compare an asset's configuration state against a pre-defined policy to determine whether or not the configuration is compliant.	
Seamlessly integrates with file integrity monitoring data to immediately reassess upon detected changes (continuous compliance).	
Vendor supplied policy templates.	
Supports Center for Internet Security (CIS) benchmarks out-of-the-box.	
Supports security standards (NIST, DISA, VMware, ISO 27001) out-of-the-box.	
Supports regulatory requirements (PCI, SOX, FISMA, FDCC, NERC, COBIT) out-of-the-box.	
Supports operational/performance policies out-of-the-box for business-critical applications.	
Ability to easily modify standard policies to conform to unique organizational needs.	
Capture and automate own organizational (internal) policies.	
Ability to assess all the same platforms on which you are tracking changes, i.e. operating systems, network devices, data bases, directory servers, etc.	
Provides out-of-the-box remediation guidance to help fix non-compliant configurations.	
Ability to systematically waive policy tests to seamlessly integrate into compliance processes and requirements.	
Ability to detect and ignore files that are in a policy, but are not on the monitored system.	
Ability to run assess configurations against existing data without requiring a rescan.	
Ability to use same scan data in multiple, different policy checks without requiring a rescan.	
Provides proof to management that various departments are in compliance with set security policies.	
Ability to report "policy scorecards" to summarize the compliance status of a device.	
Ability to assign different weights to different tests that comprise a policy scorecard.	
Ability to ignore certain tests for certain periods of time (i.e. support for policy waivers).	
Ability to report on current policy waivers in effect and their expiration dates.	

Return to Table of Contents

Tripwire is the trusted leader for establishing a strong cybersecurity foundation. Partnering with Fortune 500 enterprises, industrial organizations and government agencies, Tripwire protects the integrity of mission-critical systems spanning physical, virtual, cloud and DevOps environments. Tripwire's award-winning portfolio delivers top critical security controls, including asset discovery, secure configuration management, vulnerability management and log management. As the pioneers of file integrity monitoring (FIM), Tripwire's expertise is built on a 20+ year history of innovation helping organizations discover, minimize and monitor their attack surfaces. **Learn more at** tripwire.com

***The State of Security*: News, trends and insights at** tripwire.com/blog
Connect with us on LinkedIn, Twitter **and** Facebook

BRFIMBG1j 1506