



Tripwire for Servers & Tripwire Manager

Configuration Audit and Control to Improve IT Security, Compliance, and Availability

DATASHEET

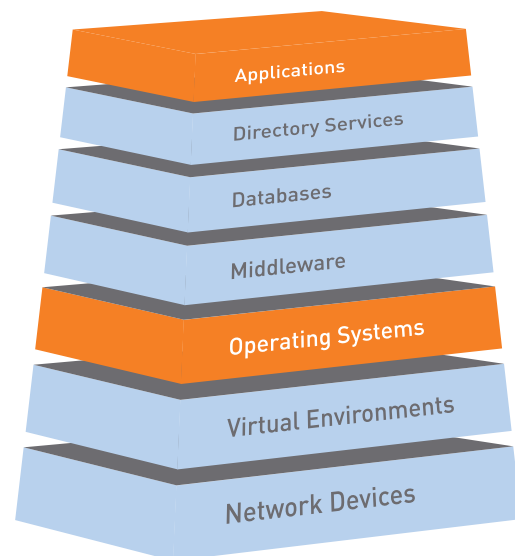
Unauthorized and undetected configuration change is the most significant threat to an enterprise's compliance status, security posture, and ability to deliver high quality IT services to customers, employees, and partners. High-performing IT organizations have gained control of change by instituting change management policies and enforcing them with configuration auditing and control. With strong internal controls in place, service outages decrease in frequency. "Firefighting" and volumes of unplanned work give way to greater focus on strategic initiatives. Security is strengthened—and preparation for compliance audits becomes almost simple. For many organizations, Tripwire® for Servers provides the configuration audit and control solution needed for their file systems.

Tripwire for Servers independently audits changes across a broad range of servers and desktops. It monitors and detects all changes to file systems, servers and desktops, including security settings, configuration parameters, and permissions. It provides a standalone solution—or when used with Tripwire® Manager, a single point of management control—for a wide range of platforms, including Windows, Linux, Solaris, HP-UX, and AIX, ensuring that all changes to servers and desktops are auditable, all changes are authorized, and all unauthorized changes are investigated.

Increased visibility into configuration changes on file servers and desktops enables staff to quickly reconcile changes with authorized change requests, and then focus remediation efforts on undesired changes. Tripwire for Servers identify what changed, who made the change, when, and how the change was made by comparing the current state of a system to a known and trusted baseline. Archives of current and past versions provide an audit trail and change history. It helps to

reduce unplanned work, provide auditable data to simplify IT audit preparation, and support service quality and security initiatives.

Tripwire Manager provides convenient, centralized management of your Tripwire for Servers installations. An enhanced GUI enables you to quickly verify system state, initiate integrity checks, receive notification of file system changes, and view changes prioritized by severity level. Tripwire Manager reports also provide a history of change, enabling you to easily meet audit and compliance requirements.



Tripwire for Servers Change Detection
Across the IT Infrastructure

DATASHEET

Tripwire For Servers Features & Benefits

Detects Undesired Change	Comprehensive monitoring of additions, deletions, and/or changes to file systems provides complete confidence in the integrity of your system. Detects and pinpoints what, where and when changes were made, allowing rapid remediation and restoration of systems to a known good state.
Event Log Correlation	Event logs are correlated with Tripwire integrity reports, improving system auditing by identifying who made a change for follow-up or data forensics. Enhances Tripwire for Servers functionality in supporting change management processes. Allows administrators to track all changes made by specific users.
Flexible Policy File Language, Including Wildcard Support	Policy file creation is easy and intuitive, allowing rapid application set-up and reduction of non-critical alerts. Policy file mechanics dramatically improved by not having to know every specific file type. Simpler policy creation process can result in fewer false positives and an improved “signal-to-noise” ratio.
Multiple Reporting and Alerting Functions	Information is provided how and where it’s needed, through email, syslog, SNMP traps, XML and HTML output and to the Tripwire Manager console. Five levels of reporting detail enable rapid discovery and remediation of the most critical files.
Integrated Command Execution (ICE)	Execution of custom command line scripts following specific integrity check results can be used for automatic restoration of known good backup files. Extends reporting and notification capabilities.
Broad Platform Support	Tripwire for Servers’ heterogenous support for any size IT environment—as well as full integration with Tripwire Manager—enables change monitoring and analysis across the enterprise.

Tripwire Manager Features & Benefits

Graphical Policy Editor	The graphical policy editor, which is fully integrated into Tripwire Manager’s GUI, allows users to quickly and easily create and edit policy files for individual machines or groups without resorting to syntax editing.
Centralized Reporting	Reports from all Tripwire for Servers installations can be viewed and managed from a central console, saving administrative overhead. Filtering and/or sorting reports allows fast response to prioritized violations. Trends easily identified by viewing same-file violations across multiple machines.
Remote Management	Enterprise-wide management is fully enabled, assuring server integrity in all locations. Tripwire Manager is fully scalable, allowing control of thousands of installations through robust SSL connections.
Patch and Software Rollout Verification	Rapidly verifies the successful roll-out of identical patches and other software on multiple machines and Tripwire for Servers database updating is simplified and accelerated.
Replicate Integrity System Function	The Replicate Integrity System enables administrators to set up a server with a master version of an established “integrity system” (policy, configuration and authentication key files, and database) then distribute it to any number of Tripwire for Servers installations. Allows quick, easy and accurate comparisons and verifications of other systems to be made against this “golden baseline.”
Launch with Context	Enables Tripwire Manager to perform operations on designated agents upon its launch, providing greater integration into other IT frameworks such as EMS and security consoles.
Toolbar Application Launch	Provides customizable ability to execute external commands, providing a streamlined method of sending contextual integrity information to other applications (e.g. ticketing systems.)

DATASHEET

TRIPWIRE FOR SERVERS PLATFORM SUPPORT

- Compaq Tru64 UNIX 4.0F, 4.0G, 5.0A, 5.1, 5.1A & 5.1B
- FreeBSD 4.5, 4.6, 4.7, 4.10 & 5.3
- HP-UX 10.20, 11.0, 11i v1 & 11i v2
- IBM AIX 4.3.3, 5.1, 5.2 & 5.3
- Linux (kernel 2.2 and glibc 2.x, or higher)
- Red Hat Enterprise Linux 3 & 4 AS, WS & ES, 5
- Solaris (SPARC) 2.6, 7, 8, 9 & 10
- Solaris (x86/x64) 10
- Windows NT 4.0, 2000, 2003 & XP Pro
- Solaris (SPARC) 7, 8 & 9
- Windows NT 4.0, 2000, 2003, XP Pro & Vista
- Red Hat Enterprise Linux 3 & 4 AS, WS & ES, 5

UNIX SYSTEM PROPERTIES MONITORED

- File adds, deletes, modifications
- Event tracking for objects
- File permissions and properties—ignore, record and check
- Inode number, number of links
- Inode generation number
- ACL
- User id of owner, group id of owner
- File type, file size
- Device number of the disk on which the inode associated with the file is stored
- Device number of the device to which the inode points. Valid only for device objects.
- Number of blocks allocated
- Modification timestamp
- Inode creation/modification timestamp
- Growing/shrinking files—indicates that the file is expected to grow or shrink
- Flags: additional, operating system dependent, information about a file
- Access timestamp
- Hash checking: CRC-32, POSIX 1003.2 compliant 32-bit Cyclic Redundancy Check; MD5, the RSA Security Message Digest Algorithm; SHA, part of the SHS/SHA algorithm; HAVAL, a strong 128-bit signature algorithm

WINDOWS SYSTEM PROPERTIES MONITORED

- File adds, deletes, modifications
- Event tracking for objects
- Flags: archive, read-only, hidden, offline, temporary, system, compressed, directory
- Last access time
- Last write time
- Create time
- File type and size
- MS-DOS 8.3 name
- NTFS Compressed flag, NTFS Owner SID, NTFS Group SID, NTFS DACL, NTFS SACL
- SDC and size of SDC for this object
- Number of alternate data streams
- Hash checking: CRC-32, POSIX 1003.2 compliant 32-bit Cyclic Redundancy Check; MD5, the RSA Security Message Digest Algorithm; SHA, part of the SHS/SHA algorithm; HAVAL, a strong 128-bit signature algorithm

WINDOWS SYSTEM REGISTRY KEYS AND VALUES MONITORED

- Registry keys and values added, deleted or modified
- Event tracking for registry keys
- Owner SID
- Group SID
- DACL
- SACL
- Name of class
- Number of sub keys
- Maximum length of class name, sub key name and value name
- Number of values
- Maximum length of data for any value in a key
- Security descriptor control
- Size of security descriptor for this key
- Last write time
- Type of value data
- Length of value data
- Hash checking: CRC-32, POSIX 1003.2 compliant 32-bit Cyclic Redundancy Check; MD5, the RSA Security Message Digest Algorithm; SHA, part of the SHS/SHA algorithm; HAVAL, a strong 128-bit signature algorithm



ABOUT TRIPWIRE

Tripwire helps over 6,000 enterprises worldwide reduce security risk, attain compliance and increase operational efficiency throughout their virtual and physical environments. Using Tripwire's industry-leading configuration assessment and change auditing solutions, organizations successfully achieve and maintain IT configuration control. Tripwire is headquartered in Portland, Oregon, with offices worldwide.