

Tripwire Enterprise Components

Enterprise/FS—*for Servers*

Enterprise/DT—*for Desktops*

Enterprise/ND—*for Network Devices*

Tripwire® Enterprise/Server is the independent engine that provides a single point of management control for auditing change across heterogeneous desktops, servers, routers, switches, firewalls, and load balancers. This solution for detecting, reconciling and reporting change supports three components, covering the enterprise infrastructure. Enterprise/FS and Enterprise/DT detect file system changes on servers and desktops, while Enterprise/ND monitors a broad selection of network devices and enables agentless monitoring of any POSIX-compliant operating system.

TRIPWIRE ENTERPRISE COMPONENT FEATURES AND BENEFITS

ENTERPRISE/FS & ENTERPRISE/DT

INTELLIGENT AGENT-BASED SERVER MONITORING	Locally-installed agents with enhanced feature sets take advantage of local processing power, a cached baseline database, and correlated package analysis, allowing change auditing with lower impact on network bandwidth.
FILE CHANGE MONITORING	Detection and logging of file additions/deletions as well as modifications to file content, permissions and attributes, enables rapid recovery from service and security issues resulting from undesired change. File contents can optionally be archived.
DIRECTORY CHANGE MONITORING	Changes to directories' permissions and attributes—as well as additions or deletions to subdirectories—are detected and logged.
CORRELATED OPERATING SYSTEM PACKAGE ANALYSIS	Detection and analysis of file system change enables matching to software packages, allowing for instant acceptance or rejection of change information as well as fast identification of causes of file system changes.
AGENTLESS MONITORING OF UNIX SERVERS	Available for any POSIX-compliant operating system, allows for limited monitoring of locked-down or currently unsupported platforms
DEFAULT RULES	Rules for popular file system configurations are included to enable fast and easy set-up and increases manageability at enterprise levels.
EASY RULE CREATION AND EDITING	Administration is simplified and false positives reduced through simple definition of expected file changes.
COMMAND EXECUTION ACTION	Enables flexible, automated response to any specified baseline deviation and increases integration with third-party backup systems.
ALTERNATIVE DATA STREAM CHANGE MONITORING	Detection and logging of changes, additions and deletions to Windows alternative data streams can prevent effects of hidden and/or malicious configuration data.



• TRIPWIRE ENTERPRISE COMPONENT FEATURES AND BENEFITS, CONT.

ENTERPRISE/ND	MULTI-VENDOR SUPPORT	Support for a variety of network devices from a broad array of vendors centralizes change auditing across heterogeneous environments and increases policy compliance through uniform device management.
	CONFORMANCE CHECKING	Identification and reporting of all device configurations differing from designated baselines—or missing specific configuration settings—increases audit compliance and network security.
	AAA INTEGRATION	Correlation of TACACS+ and RADIUS data answers when, how, and by whom changes were made.
	DEVICE LIST IMPORT	Enables device list import from other systems, minimizing manual entry and data entry errors.
COMMON TO ALL COMPONENTS	HIERARCHICAL GROUPING	Logical arrangement of nodes (by location, type, etc.) increases staff efficiencies by presenting the network in an intuitive, natural fashion to best fit the unique needs of any organization.
	REFERENCE NODE BASELINE	Enables checking for deviations on multiple nodes from any reference node, providing flexible difference reporting and rapid remediation.
	EVENT-DRIVEN AND PERIODIC CHANGE DETECTION	Inspections triggered by real-time SNMP events (e.g. node access) enable immediate notification of configuration changes. Scheduled inspections deter circumvention of established change control practices.
	CORRELATED CHANGE REPORTING	Archives information documenting when, what, how, who and even why changes were made, which increases auditability and security.
	VERSION HISTORY	Automatic archiving of change history eliminates manual record-keeping, reduces mean time to repair (MTTR), and satisfies audit requirements.
	VERSION COMPARISON	Side-by-side, color-coded comparison of any two node elements clearly highlights changes made.
	CHANGE NOTIFICATION	Change alerting ensures the immediate communication of the right information to the right person.
	WEB SERVICES API	Ability to integrate Tripwire functionality into other applications and third party tools allows extensive customization and increases leverage of existing software resources.

• SPECIFICATIONS

TRIPWIRE ENTERPRISE AGENT PLATFORM SUPPORT FOR TRIPWIRE ENTERPRISE/FS

- Solaris (SPARC) 8, 9 & 10
- Windows 2000 Server, SP2
- Windows 2003 Server
- HP-UX 11.0, 11i v1 & 11i v2
- AIX 5.1, 5.2 & 5.3
- Red Hat Enterprise Linux 3 & 4
- SUSE LINUX Enterprise Server 9

TRIPWIRE ENTERPRISE AGENT PLATFORM SUPPORT FOR TRIPWIRE ENTERPRISE/DT

- Windows 2000 Professional, SP2
- Windows XP Professional
- Red Hat Desktop 3 & 4

TRIPWIRE ENTERPRISE AGENTLESS SUPPORT FOR FILE SYSTEMS

- POSIX-compliant operating systems (through Tripwire Enterprise/ND)

TRIPWIRE ENTERPRISE/ND SUPPORTED VENDORS & DEVICES INCLUDE

- Cisco IOS, CatOS and PIX OS
- Cisco VPN 3000 Series Concentrator
- Alcatel OmniSwitch 6xxx/7xxx/8xxx
- Check Point Nokia IPSO Systems
- Extreme
- F5 BigIP
- Foundry
- HP ProCurve Series
- ISS Nokia IPSO Systems
- Juniper M/T Series
- Marconi ForeThought
- NetScreen
- Nokia IPSO OS
- Nortel Alteon & Passport

UNIX SYSTEM PROPERTIES MONITORED

- File additions, removals, modifications
- Audit tracking
- File existence
- File permissions
- Access Control List (ACL)
- Installation package data
- User id of owner, group id of owner
- File or directory type and file size
- Access, modification and change timestamp
- Hash checking—MD5, the RSA Security Message Digest Algorithm; and SHA-1, part of the SHS/SHA algorithm

WINDOWS SYSTEM PROPERTIES MONITORED

- File additions, removals, modifications
- Registry keys and values
- Event tracking
- Flags—archive, hidden, offline, temporary, system, compressed
- Access, write and create time
- Installation package data
- File or directory type and file size
- Owner, Group, DACL, SACL, read-only
- Number and hashes of alternate data streams
- Hash checking—MD5, the RSA Security Message Digest Algorithm; and SHA-1, part of the SHS/SHA algorithm

Please refer to the Tripwire Web site for complete details and updated information on supported platforms, devices, versions, and complete system requirements.



www.tripwire.com
 US TOLL FREE: 1.800.TRIPWIRE MAIN: 503.276.7500 FAX: 503.223.0182
 326 SW Broadway, 3rd Floor Portland, OR 97205 USA

