



PRODUCT BRIEF

TRIPWIRE ENTERPRISE 8: PROTECT. DETECT. CORRECT.



The pressure on enterprises—in fact organizations of all types—to maintain a continuously compliant and secure IT infrastructure has not relented. If anything, the pressure from strengthened compliance and security initiatives in response to the increased frequency and complexity of threats continues to build. And IT still faces the same challenges: undetected changes to IT files and configurations that introduce risk and non-compliance, high volumes of change data that obscure the changes that actually need remediation, the need to maintain and prove compliance, and a disconnect between IT Security, Compliance, and Operations teams.

Tripwire Enterprise:

- Protects IT systems and critical data by assessing them against configuration standards, hardening guidelines and security best practices, and by prioritizing which fixes are most critical to address.
- Detects any changes to files or configurations in real time, whether significant or seemingly minor, and weights them according to risk or non-compliance level.
- Corrects integrity or compliance issues through an intuitive remediation workflow that supports multiple users and roles.

These integrated capabilities give IT security, compliance and operations an end-to-end security and compliance solution, and also provide practical way for them to work together and ensure critical issues don't get lost in the shuffle.

In addition, as a key solution in the Tripwire® VIA™ suite, Tripwire® Enterprise integrates with Tripwire® Log Center, a next-generation log and security event management solution. This combination delivers to IT centralized visibility into change, log and event data generated from across the entire IT infrastructure—along with intelligence to make better decisions faster, and automation that lets IT accomplish more than ever before. Simply put, the Tripwire VIA suite lets you take control of your IT infrastructure.

PROTECT: WITH COMPLIANCE POLICY MANAGER

As one of the first companies to help organizations meet their compliance demands, Tripwire has a depth of compliance expertise that's unmatched by almost any other. The Compliance Policy Manager in Tripwire Enterprise helps you meet the numerous security standards and regulations with which your organization must maintain continuous compliance, from PCI to SOX to DISA. Each policy assesses configurations against these standards, which are security best practices taken from over 20 different recognized sources such as the Center for Internet Security (CIS) or the National Institute of Standards and Technology (NIST). And with broad coverage for numerous platforms and devices—currently, over 250 policy/platform combinations—Tripwire Enterprise policies cover almost any asset in your IT infrastructure.

DETECT: WITH FILE INTEGRITY MANAGER

From the very beginning, the name "Tripwire" has been synonymous with file integrity monitoring. The File Integrity Manager in Tripwire Enterprise detects (in real time, or as frequently as required) changes to IT files and configurations on file servers, devices, databases, directories, virtual infrastructure and more. This broad coverage ensures you detect any change that occurs in your infrastructure.

At the same time, the File Integrity Manager maintains an ongoing "integrity baseline" that versions and tracks the known and trusted state of each file or configuration item. And with ChangeIQ™, IT can now easily distinguish between the changes that introduce risk or non-compliance and the tremendous volume of business-as-usual changes that occur every day on applications, platforms and databases.

CORRECT: WITH REMEDIATION MANAGER

IT operations teams put the bulk of their efforts into keeping systems and services available to internal and external customers. As it's proven that secure and compliant systems suffer fewer outages, IT security and compliance teams should have a direct line to IT operations.

Unfortunately, this is rarely the case. Security and compliance teams identify failing configurations, but they have no way to seamlessly pass those issues along to the responsible operations staff. Even when IT operations teams know about and want to remediate issues, firefighting and other priorities cause them to lose track of issues or run out of time to fix them. As a result, these issues get lost in the shuffle. For operations to avoid losing issues in this "IT black hole," they need workflow tools and automation.

Tripwire Enterprise provides these tools, with the new Remediation Manager module that lets various IT teams cross organization boundaries, provides a user interface that makes fixing failing configurations more manageable, and automates remediation of failing configurations.

The Remediation Manager:

- Automates remediation of up to 98 percent of failing configurations
- Lets users approve, manage and track remediation work orders through a separate and simplified user interface
- Executes detailed, accurate "best practice" scripts from the time-tested Remediation Advisor library, which takes the guesswork out of configuration repair
- Provides built-in role-based workflows so that different users can approve, defer, deny or execute remediation (and thus supports the separation of duties principle)
- Can be launched from a user's custom home page of Tripwire Enterprise so each user has just the remediation access they need
- Offers real-time status reporting (including color-coded flagging) on remediation work-order progress
- Generates a complete set of on-demand remediation reports that can be easily delivered to stakeholders

With the Remediation Manager, IT can automatically correct failed configuration tests to rapidly put systems into a policy-aligned, compliant state, whether in pre-deployment or production settings.

ADDITIONAL NEW FEATURES IN TRIPWIRE ENTERPRISE

The latest release of Tripwire Enterprise offers two additional features that users will appreciate. First, Tripwire Enterprise now supports the Security Content Automation Protocol (SCAP), the de-facto process for updating security content in security solutions used by the U.S. federal government. This latest release is certified as a SCAP compliant scanner for the Federal Desktop Core Configuration (FDCC).

Second, Tripwire Enterprise now has support for Windows 2008 R2 and RHEL 5.4 with real time data and data about who made changes.

Features and Benefits

SINGLE POINT OF CONTROL FOR ALL IT CONFIGURATIONS	Tripwire Enterprise provides centralized control of configurations across the entire physical and virtual IT infrastructure, including servers and devices, applications, and multiple platforms and operating systems.
FILE INTEGRITY MANAGER FOR SECURE DATA AND CONFIGURATIONS	Tripwire Enterprise's File Integrity Manager is the recognized best-of-breed solution for file integrity monitoring and real-time change auditing. File Integrity Manager establishes the secure, "known and trusted" baseline state that IT security has come to depend on.
COMPLIANCE POLICY MANAGER FOR FAST, AUDITABLE COMPLIANCE	The compliance policy management capabilities of Tripwire Enterprise test system configurations against over 250 policies that reflect security benchmarks from security leaders like CIS, industry standards like PCI, regulatory requirements like SOX, or your own internal security requirements.
REMEDIATION MANAGER FOR QUICK, EFFICIENT CONFIGURATION REPAIR	The new Remediation Manager add-on module automatically remediates up to 98 percent of failed configurations, saving IT tremendous time and effort.
ChangeIQ FOR INTELLIGENT REAL-TIME CHANGE ASSESSMENT	ChangeIQ capabilities intelligently assess changes in real time, determining whether they moved a system out of compliance, prioritizing remediation efforts and reducing overall risk.
BUILT-IN INTEGRATION WITH TRIPWIRE LOG CENTER THROUGH TRIPWIRE VIA	As part of the Tripwire VIA suite, Tripwire Enterprise integrates with Tripwire Log Center out of the box. The integration enables users to correlate change and event information to transform raw data into actionable knowledge. It also provides a centralized view of data center security.
WORKFLOW TOOLS FOR MANAGING FAILED CONFIGURATIONS	The Remediation Manager module provides role-based workflow tools that let users approve, deny, defer or execute remediation of failed configurations.
INTEGRATION WITH CHANGE MANAGEMENT SYSTEMS	Because Tripwire Enterprise integrates with leading Change Management System (CMS) solutions, as change happens Tripwire Enterprise automatically reconciles detected changes against change tickets and change requests.
VIRTUAL INFRASTRUCTURE MONITORING	Tripwire Enterprise integrates with VMware vCenter to provide control over virtual infrastructure (VI), auto-discovering new instances of VI and automatically monitoring and reporting on changes to VI.
SUPPORT FOR FASTER, EASIER AUDIT PREPARATION	Tripwire Enterprise dramatically reduces the time and effort for audit preparation by providing continuous, comprehensive IT infrastructure baselines along with real-time change detection and built-in intelligence to determine the impact of change.
SUPPORT FOR MAINTAINING A SECURE, COMPLIANT STATE	Tripwire Enterprise combines configuration assessment with real-time File Integrity Monitoring to detect, analyze and report on changes as they happen and keep configurations continually compliant. This immediate access to change information lets IT fix issues before they result in a major data breach, audit finding or long-term outage.
AUTOMATED IT COMPLIANCE PROCESS	Tripwire Enterprise automates compliance with the industry regulations and standards organizations are now subject to—from PCI, to NERC, SOX, FISMA, DISA and many others.
REPORTS AND DASHBOARDS FOR ENTERPRISE-WIDE VISIBILITY	Tripwire ships with numerous pre-defined reports that provide real-time scoring of compliance posture, including rate of change and other important trends. Report drilldowns, linking, and dashboards provide comprehensive overviews of security and compliance for any organizational level.

User Home Pages and Dashboards

Introducing Tripwire Enterprise 7.6

Tripwire Enterprise 7.6 delivers new features that help users interact with each other and with the Tripwire Support staff, manage alerts more easily, and gather more information more quickly from their Tripwire Enterprise implementation.

New or Enhanced in TE Version 7.6

- User Home Pages can now include ready-made widgets that interact with the Tripwire Customer Center, giving users real-time access to important Tripwire product and policy announcements, relevant forum discussions, and posts in the Tripwire developer's blog.
- Performance improvements that allow users to generate faster reports, especially when real-time or "who" user data is included in report definitions.
- User interface improvements include more manageable command bars and TE tabs that are easier to navigate.
- 64-bit support for select Tripwire Enterprise consoles allows users to take advantage of the improved memory optimization and client handling of 64-bit systems.
- Tripwire Enterprise 7.6 supports a number of new "real-time" agents capable of capturing detailed "who" information on detected changes, including Windows 2008 Server and Windows 2003 Server in both 32 and 64-bit agent versions, and Vista SP1 64-bit agents.

Visit the Tripwire Customer Center

Customize Your Home Page » Click here to get started

Alerts

Alert on: ... View All

- Node Error alert
Selected Node or Group: accounting01.hr.example.com
- 1 nodes have been newly discovered
0 remain in the Discovered Nodes
- Policy score change alert
Selected Node or Group: accounting01.hr.example.com
Selected Policy or Group: FSI Policy - Windows
- VI Node Change alert
Selected Node or Group: accounting01.hr.example.com

Change Reports

Name	Run	Browse To
Change Process Compliance	Run	View
Change Rat...	Sample	Run
Change Variance	Run	View
Changed Elements	Run	View

Explore Tripwire Customer Services

- Tripwire's Customer Services Group delivers trusted expertise in implementing a customized solution or in integrating Tripwire Enterprise with your change management systems and best practices. [Learn more](#)
- Tripwire's Remote Operations provide quick-start expertise to new customers, upgrade existing customers to new versions, or manage the day-to-day operations of Tripwire Enterprise implementations. [Learn more](#)
- Tripwire provides comprehensive training programs for all levels of Tripwire Enterprise users, through scheduled classes throughout North America and Europe or through on-site training programs. [Learn more](#)

Customer Center integration and customizable widgets provide useful, out-of-the-box functionality to user Home Pages.

PCI Dashboard

Linux PCI Compliance

Internal PCI Compliance = 7
Failing = 0

Linux PCI Result Summary

Failed Tests = 195
Passed Tests = 2,200

Windows PCI Compliance

Failing = 5
PCI Sample = 20

Change Process Compliance

Authorized = 4,000
Unauthorized = 1,000

Windows PCI Result Summary

Failed Tests = 312
Passed Tests = 5,200

PCI Virtual Infrastructure Scorecard

Failed Tests = 151
Passed Tests = 141

Tripwire Enterprise dashboards provide the real-time reports and alerts managers need to ensure continuous compliance.

Action Manager

Name	Type	Description
Attribute Conditional Action	Action Group	
Audit Trail Conditional Action	Action Group	
By Match Conditional Action	Action Group	
By Reference	Action Group	
Content Control	Action Group	
Custom Property	Action Group	
Element Name	Action Group	
List Action	Action Group	
Outside Change	Action Group	
Package Control	Action Group	
Promote to Baseline	Action Group	
Quiesce	Action Group	
SMP Action	Action Group	
SMP Action	Action Group	
Severity Rank	Action Group	

Create Action - Google Chrome

Select the action type to create:

- Attribute Conditional Action
- Audit Trail Conditional Action
- By Match Conditional Action
- By Reference
- Content Control
- Custom Property
- Element Name
- List Action
- Outside Change
- Package Control
- Promote to Baseline
- Quiesce
- SMP Action
- SMP Action
- Severity Rank

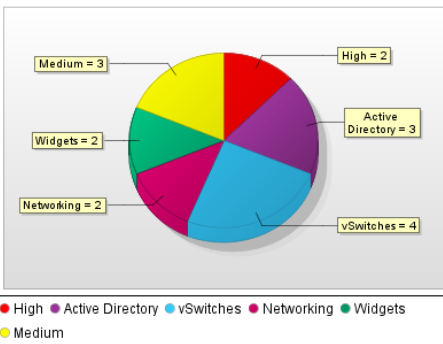
Selected type:

Tripwire Enterprise offers easy-to-use dialogs that simplify the creation and modification of actions, tasks, and rules.

Reports

ERP Changes By Severity

Date:	7/17/09 4:19 PM
Promotion Approval ID:	Not applied
Change window:	Not applied
Use strict package match:	No
Display criteria at end:	No
Element Exists:	Not applied
Nodes:	ERP, esx4se.pdxse.tripwire.com, onlinecollab.srv1.tripwire.com
Node name:	Not applied
Node Properties:	Not applied
Rules:	All
Rule name:	Not applied
Element name:	Not applied
Element Properties:	Not applied
Version Properties:	Demo Data Equals Yes
Change types:	Added, Modified, Removed
Severity range:	All
Current versions only:	No
Time range:	All time
Packages:	Not applied
Severity sections sort:	Severity, descending
Details table sort:	Count, descending
Details table (2nd) sort:	Name, descending



High Severity

Name	Type	Last Change Time	Count
DEMOSERVER.PDXSE.TRIPWIRE.COM	Windows Server	11/7/08 1:31 PM	2

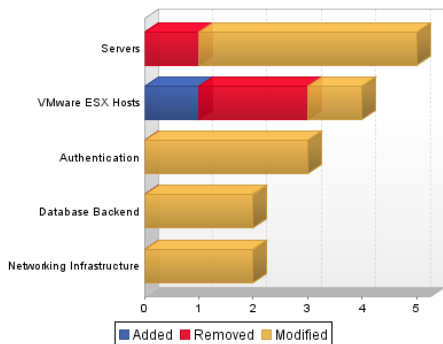
Severity Total: 2

Tripwire Enterprise provides nearly 40 reports, with additional under constant development. More samples and the full Report Catalog on the Tripwire website.

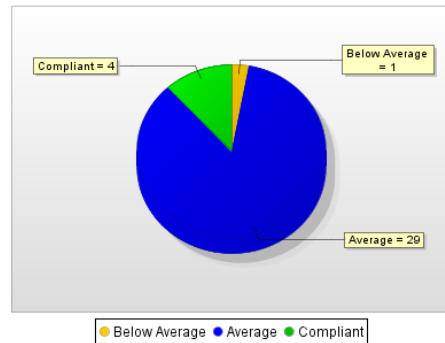
- Baseline Elements
- Change Process Compliance
- Change Rate
- Change Variance
- Change Window
- Changed Elements
- Changes by Node or Group
- Changes by Rule or Group
- Changes by Severity
- Compliance History
- Composite Changes
- Detailed Changes
- Detailed Test Inventory
- Detailed Test Results
- Detailed Waivers
- Device Inventory
- Elements
- Frequently Changed Elements
- Frequently Changed Nodes
- Inventory Changes
- Last Node Check Status
- Missing Elements
- Monitoring Policy
- Nodes with Changes
- Reference Node Variance
- Remediation Assessment
- Remediation Work Order Details
- Scoring
- Scoring History
- System Access Control
- System Log
- Task Report
- Test Result Summary
- Test Results by Node
- Unchanged Elements
- Unmonitored Nodes
- Unreconciled Change Aging
- User Roles All Object Types

ERP Changes By Group

Date:	7/17/09 3:34 PM
Promotion Approval ID:	Not applied
Change window:	Not applied
Use strict package match:	No
Display criteria at end:	No
Element Exists:	Not applied
Nodes:	Authentication, Database Backend, Networking Infrastructure, Servers, VMware ESX Hosts
Node name:	Not applied
Node Properties:	Not applied
Rules:	All
Rule name:	Not applied
Element name:	Not applied
Element Properties:	Not applied
Version Properties:	Demo Data Equals Yes
Change types:	Added, Modified, Removed
Severity range:	All
Current versions only:	No
Time range:	All time
Packages:	Not applied
Details table sort:	Total, descending
Details table (2nd) sort:	Name, ascending



NERC Scoring for Windows



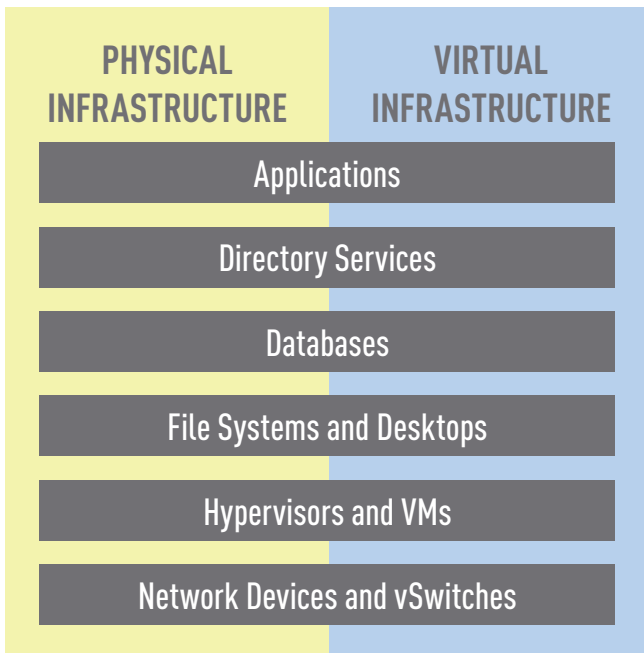
MS Windows Server 2003 DM - NERC v2

Compliant		
Node	Score	Waived Tests
WIN-COMPLIANCE2.PDXSE.TRIPWIRE.COM	77.19	0
WIN-COMPLIANCE3.PDXSE.TRIPWIRE.COM	77.19	0
WIN-COMPLIANCE4.PDXSE.TRIPWIRE.COM	77.19	0
WIN-COMPLIANCE5.PDXSE.TRIPWIRE.COM	77.19	0
Average		
Node	Score	Waived Tests

Components

BROAD, DEEP SUPPORT FOR COMPONENTS IN THE IT STACK

Whether IT needs to keep watch over mission-critical servers or the entire IT infrastructure—including virtualized environments and applications—Tripwire Enterprise provides the capability to assess, validate and enforce policies and detect all change, no matter the source. Tripwire supports the following components in the IT stack:



Tripwire Enterprise Across the IT Infrastructure

TRIPWIRE ENTERPRISE FOR APPLICATIONS

Mission-critical applications are at the top of the IT infrastructure and enable the daily activities like email, web-based applications, and other critical applications that keep organizations moving forward. Tripwire Enterprise for Applications provides compliance policy management and file integrity monitoring capabilities to help ensure that supported applications are configured properly for security, compliance, and optimal performance and availability. In addition to out-of-the-box policies for applications such as Microsoft Exchange and IIS server, Tripwire Enterprise lets IT easily create policies for other business applications, including custom applications.

TRIPWIRE ENTERPRISE FOR DIRECTORY SERVICES

Tripwire Enterprise for Directory Services provides independent compliance policy management for LDAP-compliant directory server objects and attributes, such as LDAP schema, password settings, user permissions, network resources, group updates, and security policies. Tripwire bases these assessments on CIS, NIST, DISA, FISMA, NERC, FDCC and other industry standards and regulations to help ensure organizations get their directory servers into a secure and compliant state. The component accelerates its deployment with pre-configured Active Directory, Sun Java System Directory Server and Novell eDirectory default settings that can be fully customized to specific enterprise environments.

TRIPWIRE ENTERPRISE FOR DATABASES

Tripwire Enterprise for Databases works in conjunction with Tripwire's File Systems component to help organizations get their Oracle, Microsoft and IBM database servers into secure, continually high-performing states. Tripwire does this by assessing configurations of schema objects, application and configuration files, security and configuration parameters, access settings, and user roles and permissions against CIS, PCI and NIST guidelines for security. Once IT gets the database server into a known and trusted state, it keeps it there by ensuring all subsequent configuration changes are detected.

TRIPWIRE ENTERPRISE FOR FILE SYSTEMS AND DESKTOPS

Tripwire Enterprise for File Systems and Desktops assesses the configurations of physical and virtual server and desktop file systems, including security settings, configuration parameters, and permissions. Tripwire bases its policies on settings recommended by respected organizations such as CIS and NIST. When followed by Tripwire's tunable change detection, IT has a single solution that ensures visibility and accountability for all configuration control activity on a wide range of platforms. And Tripwire's agents are designed to achieve configuration control across the enterprise with minimal impact on network bandwidth.

Components (cont.), Platform Support and Specifications

TRIPWIRE ENTERPRISE FOR VMWARE

Tripwire Enterprise for VMware provides visibility across the VMware virtual infrastructure, enabling continuous configuration control of virtual environments. This component provides out-of-the-box assessment tests for hypervisors, virtual containers, and vSwitches based on CIS security policies, DISA Security Technical Implementation Guides (STIGs), and VMware's Infrastructure 3 Security Hardening guide. The included VirtualCenter integration auto-populates the same hierarchy of VirtualCenters, Clusters, Data Centers, Folders, Resource Pools and hypervisors from VMware into Tripwire Enterprise, which enables auto-discovery, monitoring and reporting of changes among and within newly-created virtual infrastructure objects.

TRIPWIRE ENTERPRISE FOR NETWORK DEVICES

Tripwire Enterprise for Network Devices assesses configuration settings of the broadest range of network devices in the industry, including any device running a POSIX-compliant operating system. By testing configurations against industry-proven settings and then following up with continuous file integrity monitoring that identifies out-of-compliance changes, this component helps organizations achieve and maintain continuous compliance with security, regulatory, and operational measures. In addition, Tripwire generates an audit trail of all configuration control activities, so proving compliance in an audit is greatly simplified.

TRIPWIRE ENTERPRISE CONSOLE SUPPORT

Platforms

- Solaris, Windows, Red Hat Enterprise Linux, SUSE Linux Enterprise

Web Browsers

- Firefox, Netscape, Internet Explorer

TRIPWIRE ENTERPRISE FOR APPLICATIONS—SUPPORTED APPLICATIONS

- Microsoft IIS
- Microsoft Exchange Server 2003
- Oracle Database 10g

TRIPWIRE ENTERPRISE FOR DIRECTORY SERVICES—SUPPORTED APPLICATIONS

- Windows Active Directory
- Sun Java System Directory Server
- Novell eDirectory
- LDAP v2 & v3

TRIPWIRE ENTERPRISE FOR DATABASES—SPECIFICATIONS

Oracle 9i, 10g & 11g

Schema Objects

- Functions
- Indexes
- Procedures
- Tables
- Triggers
- Views
- Packages and package bodies
- Sequences
- Stored outlines
- Synonyms
- Types and type bodies
- Libraries
- Database Links
- Clusters

Database Objects

- Directories
- Tablespace

Security

- System Privileges
- Object Privileges
- Audit Parameters

Access Settings

- Users
- Profiles
- Roles

Software Files

(using file system monitoring rules)

Microsoft SQL Server 2000 & 2005

Schema Objects

- Tables
- Indexes
- Triggers
- Views
- Stored Procedures
- Functions
- User-defined types

Database Objects

- Configuration Parameters
- Databases

Security & Access Settings

- Logins
- Server Roles
- Database Users
- Database Roles

Software Files

(using file system monitoring rules)

IBM DB2 UDB Version 8.2 & 9.5

Schema Objects

- Functions
- Aliases
- Indexes
- Packages
- Procedures
- Schemas
- Schema Groups
- Sequences
- Tables
- Triggers
- User Defined Types
- Variables
- Views

Database Objects

- Bufferpool
- Configuration Parameter
- Database Partition Group
- Event Monitor
- Histogram Template
- Service Class
- Tablespace
- Threshold
- Work Action Set
- Work Class Set
- Workload

Security

- Audit Policy
- Security Label Component

Security Access Settings

- Groups
- Roles
- Users

Software Files

(using file system monitoring rules)

Platform Support and Specifications (cont.)

TRIPWIRE ENTERPRISE FOR FILE SYSTEMS AND DESKTOPS—SPECIFICATIONS

Agent platform support

- Solaris (SPARC) 8, 9 & 10
- Solaris (x86) 10
- Windows 2000 Server
- Windows Server 2003 (incl. x64 Editions)
- Windows Server 2008 (incl. Core and x64)
- Windows XP x86 and Professional
- Windows 2000 Professional
- Windows Vista (incl. x86 and x64)
- HP-UX 11i v1, v2 & v3 (11i v2 & v3 on Itanium)
- AIX 5.2, 5.3 & 6.1
- Red Hat Enterprise Linux 3, 4 & 5 AS, ES & WS
- Red Hat Desktop Linux 3, 4 & 5
- SUSE Linux Enterprise Server 9 & 10
- Oracle Enterprise Linux 4 & 5
- CentOS 4.2
- Fedora Core 5 through 10

UNIX system properties monitored

- File adds, deletes, modifications
- Audit tracking
- File existence
- ACL (Access Control List)
- Installation package data
- User ID of owner, group ID of owner
- File and directory type, and file size
- Access, modification and change timestamp
- Growing attribute

Virtual environment support

- VMware ESX 3.0, 3.5 & ESXi
- VMware vSphere 4.0
- Solaris Zones

Agentless support for file systems

- POSIX-compliant operating systems (through Tripwire Enterprise for Network Devices node)

Windows system properties monitored

- File adds, deletes, modifications
- Registry keys and values
- Event tracking
- Installation package data
- Flags: archive, hidden, offline, temporary, system, compressed
- Access, write and create time
- File and directory type, and file size
- Owner, Group, DACL, SACL, read-only
- Number and hashes of alternate data streams
- Growing attribute

TRIPWIRE ENTERPRISE FOR VMware—SUPPORTED HYPERVISORS

- VMware ESX 3.0, 3.5 & ESXi
- VMware vSphere 4.0

TRIPWIRE ENTERPRISE FOR NETWORK DEVICES—SUPPORTED VENDORS & DEVICES

- Cisco IOS, CatOS & PIX OS
- Cisco VPN 3000 Series Concentrator
- Cisco Catalyst 1900/2820 Switch
- 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
- Other devices using the included Universal Device Kit

Agentless support for file systems

- POSIX-compliant operating systems



ABOUT TRIPWIRE

Tripwire is a leading global provider of IT security and compliance automation solutions that help businesses and government agencies take control of their entire IT infrastructure. Thousands of customers rely on Tripwire's integrated solutions to help protect sensitive data, prove compliance and prevent outages. Tripwire® VIA™, the comprehensive suite of industry-leading file integrity, policy compliance and log and security event management solutions, is the way organizations can proactively achieve continuous compliance, mitigate risk and improve operational control through Visibility, Intelligence and Automation. Learn more at www.tripwire.com and @TripwireInc on Twitter.