

## PRODUCT BRIEF

# TRIPWIRE ENTERPRISE: TAKE CONTROL OF IT COMPLIANCE AND SECURITY



Enterprises and organizations of all types need to maintain a continuously compliant and secure IT infrastructure—all without sacrificing system or service availability or interrupting operational productivity. Depending on the industry, an IT group might be subject to IT compliance with one or more regulations or industry standards, such as PCI, NERC, SOX, FISMA, DISA and others. And organizations need to not only protect their IT infrastructures from theft or loss of sensitive personal or proprietary data, but they must also provide detailed evidence of how they protected it and demonstrate why they think these efforts will remain successful even as security issues rise.

Tripwire, with nearly 7000 customers and over 12 years developing customer-valued solutions for IT security and compliance automation takes its configuration control leadership to a new level with Tripwire® Enterprise. This latest release introduces new capabilities that help assess, detect and correct file, content and configuration changes across the entire infrastructure. New capabilities in Tripwire Enterprise, like ChangeIQ™ for the real-time assessment and prioritization of changes, and built-in integration with Tripwire Log Center for on-demand correlation of changes with log events data provide more visibility, intelligence and automation to Tripwire's industry-leading configuration control capabilities.

### FILE INTEGRITY MONITORING THAT FOCUSES ON THE CHANGES THAT MATTER

With today's incredibly dynamic IT environments, IT management faces change information overload. Tripwire's change auditing and detection technology has become so effective at monitoring files and configurations that it now provides complete visibility to every change in real-time, from content to permissions to minor file attributes. But until now, that technology couldn't easily determine if a given change introduced risk, or took the organization out of a compliant state. Because

IT organizations no longer have the time or resources to review and reconcile every detected change, automation and the ability to narrow focus to the changes that matter have become essential.

Tripwire Enterprise now offers ChangeIQ, built-in technologies that combine change detection with intelligent, real-time change assessment to automatically and immediately alert to critical changes—those that introduce the highest risk or take the IT infrastructure out of compliance. ChangeIQ can prioritize change and determine the change criticality of detected change in a number of different ways:

- Applying policy-filtering intelligence that compares changes to established policies, benchmarks and guidelines. Tripwire Enterprise prioritizes changes and evaluates their risk using policies like CIS, PCI, and NIST; internally developed policies; or even vendor hardening guidelines.
- Comparing each change against approved change tickets in a change management system (CMS).
- Customizable severity settings: Tripwire Enterprise allows users to quantify the for changes for numerous file and configuration aspects, and assigning a score based on the severity of a given change. For example, if a file of a "DLL" file type is added to a system, and if a permission change is also made, the combined score of these changes could indicate a significant security risk.
- Specifying conditional actions that can auto-promote or flag changes based on any number of different conditions or attributes.

When ChangeIQ determines that critical changes have occurred, Tripwire Enterprise can generate alerts and give one-click access to detailed remediation advice. That means changes get fixed before they result in full-blown security breaches or compliance failures. When changes don't fall into the critical category—the vast majority of detected changes—ChangeIQ can automatically promote them, saving IT staff countless hours manually

---

reviewing these changes or, worse, ignoring them because they're overwhelmed by the volume of changes.

By leveraging industry-recognized security standards with Tripwire's own deep expertise in how changes impact the IT infrastructure, Tripwire Enterprise provides the focus and intelligence needed to maintain continuous IT compliance and solid IT security.

### **ON-DEMAND, INSTANT INTEGRATION WITH TRIPWIRE LOG CENTER**

Tripwire Enterprise now provides built-in, on-demand integration with Tripwire® Log Center. This complete security information and event management (SIEM) solution provides ultra-efficient log processing and sophisticated event analysis in an enterprise-ready, standalone package. But unlike any other SIEM solution available today, Tripwire Log Center has out-of-the-box integration with Tripwire Enterprise, providing an immediate bridge between two critical compliance and security technologies. With this integration, Tripwire Enterprise users benefit from:

- The ability to review the node-specific log and event information behind a Tripwire Enterprise change alert provided by Tripwire Log Center in response to a Tripwire Enterprise change alert, without leaving the Tripwire Enterprise console or view.
- Freeform, plain-language event and message searches from within Tripwire Enterprise of any machine in the Tripwire Log Center database, to uncover trends and emerging threats.
- An intelligent log and event widget in Tripwire Enterprise's custom home pages to review real-time events of interest and gain greater situational awareness.
- Correlated log and security event data from Tripwire Log Center with change data from Tripwire Enterprise delivers unparalleled visibility into the changes in the entire IT infrastructure.

### **TRIPWIRE ENTERPRISE MEETS COMPLIANCE DEMANDS**

Tripwire Enterprise helps organizations achieve a secure, compliant state with real-time comparison of current configurations against standards and best practices captured in Tripwire Enterprise policies. These policies, developed and maintained by Tripwire's policy team of certified security professionals, test system configurations against security benchmarks like

those issued by the Center for Internet Security (CIS), industry standards like PCI and NERC, regulatory requirements like those in SOX, vendor security guidelines, and internal policies. Currently, Tripwire offers over 200 policies and has received over 30 certifications from CIS, the recognized authority on IT security, providing assurance that Tripwire can help any organization meet their compliance mandates.

Many products can identify settings that are out of compliance with a given policy; one or two of these can even do this with near real-time analysis. But the built-in, one-touch remediation advice delivered by Tripwire Enterprise helps IT correct misconfigurations quickly and with certainty. By providing a detailed punch-list of the actions to take to return a non-compliant setting to a compliant state, Tripwire Enterprise ensures IT is never more than a step away from returning to a secure, compliant and audit-ready state.

Tripwire Enterprise also produces on-demand or automated reports that provide immediate insight into compliance status. These reports can reveal overall or node-by-node compliance scores, the rate that changes occur, adherence to change processes and other critical information. Links within reports offer an easy way to gain more detailed specifics on the organization's security and compliance posture, while custom dashboards provide high-level overviews to provide upper management proof that IT is fully meeting the organization's security and compliance needs.

### **TRIPWIRE ENTERPRISE LETS IT OPERATIONS STAY ON TASK**

For IT operations, Tripwire Enterprise provides the means to keep tight control on configurations by eliminating the variances between staging and production environments or even between machines and devices, the variances that so often introduce security risks and decrease availability. When drift or failures do occur, IT can quickly pinpoint how and where they occurred, dramatically cutting mean time to repair and speeding system recovery.

In addition tripwire Enterprise lets IT operations continuously meet security and compliance mandates by providing dashboards and reports that demonstrate control without diverting their attention from the never-ending demands on their time. Evidence generated with Tripwire Enterprise makes audits painless, once again shortening the time required to prove compliance and eliminating the need to remediate audit findings.

---

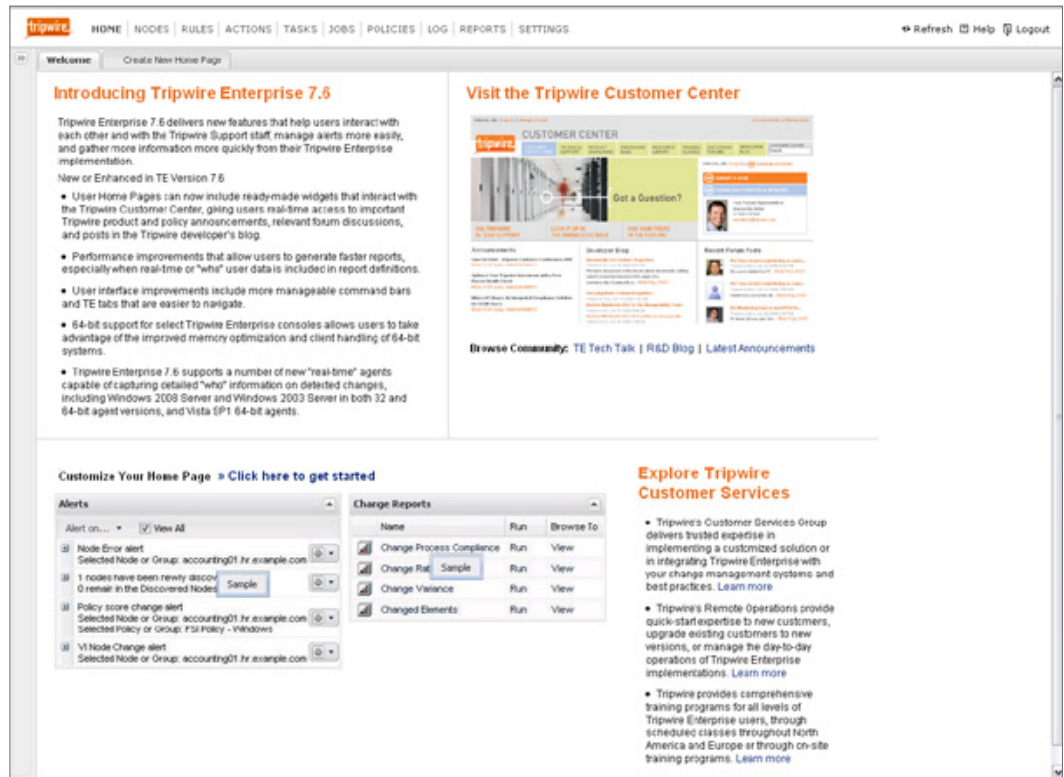
## Features and Benefits

---

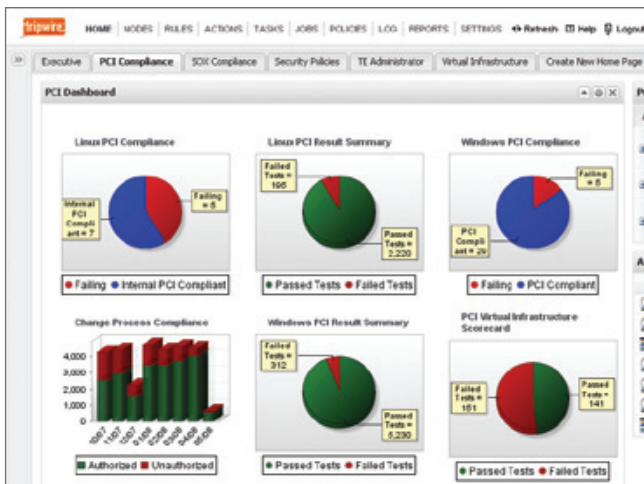
SINGLE POINT OF CONTROL FOR ALL IT CONFIGURATIONS	Tripwire Enterprise provides centralized control of configurations across the entire physical and virtual IT infrastructure, including servers, devices, applications, and multiple platforms and operating systems.
ChangeIQ PROVIDES INTELLIGENT REAL-TIME 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	The out-of-the box integration of Tripwire Enterprise with Tripwire Log Center supports correlation between change and event information, transforming raw data into actionable knowledge and providing a tightly integrated view of data center security.
POLICY ASSESSMENTS FOR ACHIEVING COMPLIANCE	Tripwire Enterprise's Compliance Policy Management tests system configurations against over 200 policies that quantify the standards of security leaders like CIS, industry standards like PCI, regulatory requirements like SOX, and even your own internal security requirements.
BUILT-IN REMEDIATION ADVICE	With a single touch, Tripwire Enterprise generates a punch list of remediation actions needed to rapidly return drifted or out-of-bounds configurations to a secure, compliant state.
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 compliance policy management with real-time File Integrity Monitoring to detect, analyze and report on changes as they happen and keep configurations continuously 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 IT compliance posture, including rate of change and other important trends. Report drilldowns, linking, and dashboards provide comprehensive overviews of security and compliance needed at any level in the organization.

---

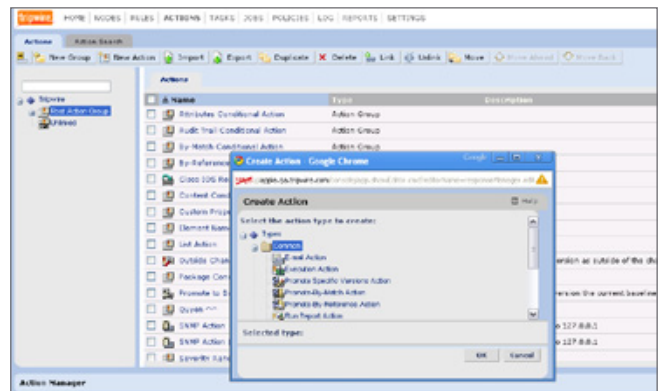
# User Home Pages and Dashboards



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



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

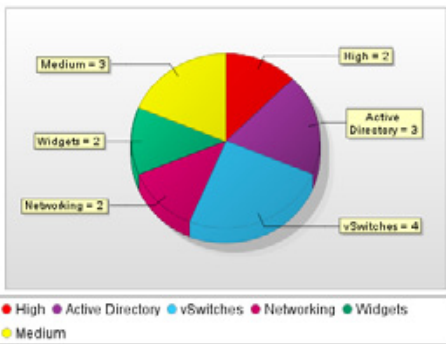


Tripwire Enterprise offers easy-to-use dialogs that simplify the creation and modification of actions, tasks, and rules.

# 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, onlincollab.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

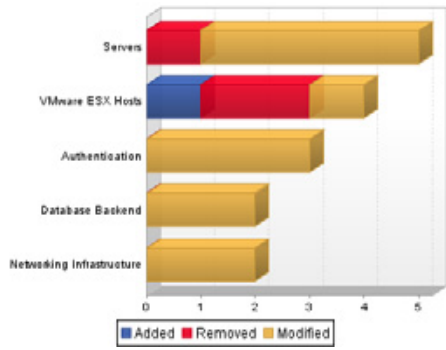
Severity Total: 2

Tripwire Enterprise provides over 30 reports, with additional reports under constant development. More samples and the full Report Catalog on the Tripwire website.

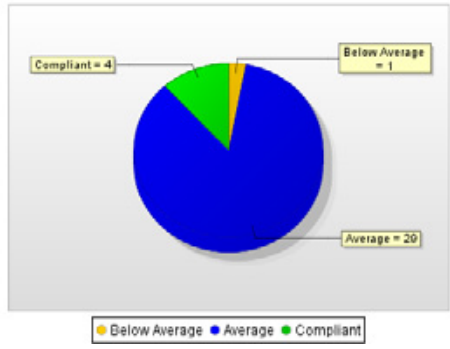
- Baseline Elements
- Change Process Compliance
- Change Rate
- Change Variance
- Change Window
- Changed Elements
- Changes by Node or Group
- Changes by Rule or Group
- Changes by Severity
- Compliance History
- Composite Changes
- Detailed Changes
- Detailed Test Inventory
- Detailed Test Results
- 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
- 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

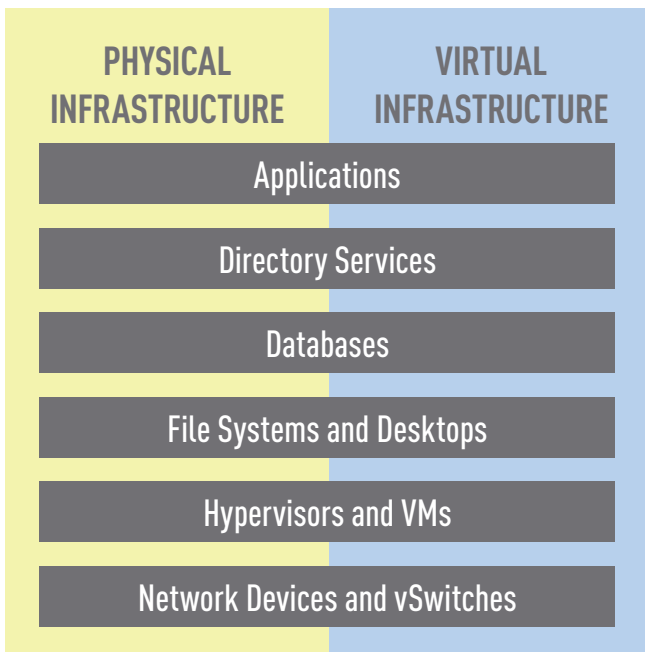
  

Average		
Node	Score	Waived Tests
www.tripwire.com	76.54	0

## 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

## Take Control with Tripwire VIA

We all know that changes, breaches, audits and outages happen. Tripwire VIA™ solutions have something in common: they let you take control of these situations by giving visibility across the entire infrastructure, providing intelligence to help you make better decisions faster, and automating repetitive and manual tasks. The IT Security and Compliance Automation suite of Tripwire VIA includes Tripwire Enterprise for configuration control and Tripwire Log Center for log and event management. Combine both solutions to minimize your total cost of ownership and take control of your entire IT infrastructure—all from a single, trusted vendor.



### ABOUT TRIPWIRE

Tripwire is the leading global provider of IT security and compliance automation solutions that help businesses and government agencies take control of their entire IT infrastructure. Over 7,000 customers in more than 86 countries rely on Tripwire's integrated solutions. Tripwire VIA™, the comprehensive suite of industry-leading file integrity, policy compliance and log and event management solutions, is the way organizations proactively prove continuous compliance, mitigate risk, and achieve operational control through Visibility, Intelligence and Automation. Learn more at [www.tripwire.com](http://www.tripwire.com).

©2010 Tripwire, Inc. | Tripwire is a registered trademark of Tripwire, Inc. All other product and company names are property of their respective owners. All rights reserved. | TEPB7701a



867.1191  
[sales@nexustech.com.ph](mailto:sales@nexustech.com.ph)  
[www.nexustech.com.ph](http://www.nexustech.com.ph)