PRODUCT BRIEF

# Tripwire Enterprise

## CONFIGURATION CONTROL FOR VIRTUAL AND PHYSICAL IT INFRASTRUCTURE

### COMPLETE CONFIGURATION CONTROL FOR THE PHYSICAL AND VIRTUAL INFRASTRUCTURE

Although the challenges IT faces in controlling configurations haven't substantially changed in the last year, the intensity of those challenges has certainly increased. More security breaches means IT must watch over configurations in the IT environment even more diligently. Compliance continues to be a major focus for IT, with most organizations being subject to an increasing number of complex regulations that require numerous IT controls. And as always, IT must ensure systems and services are available and performing at expected or guaranteed levels for the organization's internal and external customers. With this increased intensity comes the need for more comprehensive, immediate and continuous control of IT configurations and files in the physical and virtual IT infrastructure.

Version 7.6 of Tripwire® Enterprise helps IT tackle this challenge head-on, with a depth and breadth of coverage and support for change auditing and configuration assessment unmatched by any other configuration control solution. No other solution covers as many hardware platforms and components in the IT stack or offers as expansive a library of policies for compliance with regulations and standards as Tripwire Enterprise. Tripwire even integrates customer support with the Tripwire Enterprise software solution, so users can quickly get answers to critical technical questions and stay on top of the latest product updates and announcements. With Tripwire Enterprise, IT can ensure a constant, secure state of the technology infrastructure, achieve continuous compliance with critical regulations and standards, and gain confidence that their infrastructure can easily pass an audit.

### TRIPWIRE ENTERPRISE DELIVERS IMMEDIATE VALUE IN THREE EASY STEPS:

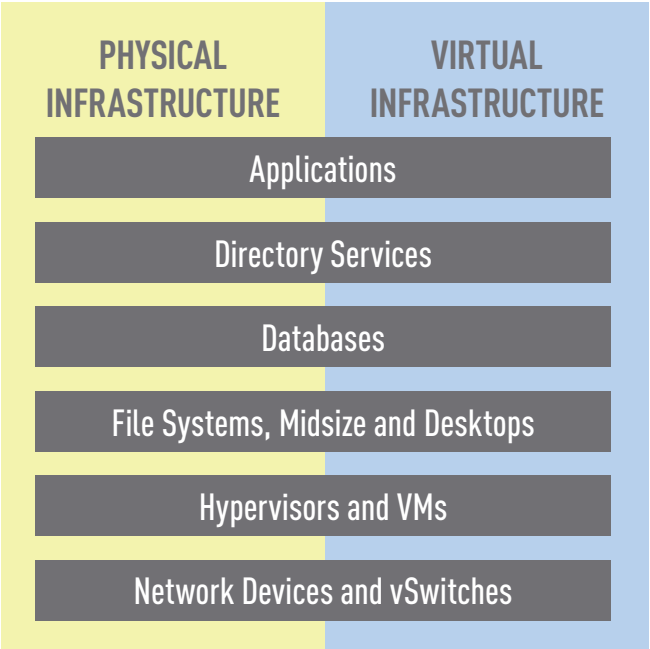
1. **Configuration Assessment.** Tripwire Enterprise proactively assesses current configuration settings against established internal policies and external industry benchmarks. The assessment produces a quantified enterprise-wide risk profile that allows IT to address vulnerabilities one-by-one across the IT infrastructure until the infrastructure moves into a known and trusted state.
2. **Change Auditing.** Once IT moves the infrastructure into a known and trusted state, Tripwire Enterprise helps them maintain it. Tripwire Enterprise detects all change across the entire IT infrastructure—applications, databases, servers, active directories, virtual environments, middleware and network devices—and alerts IT to any unauthorized or non-compliant change.
3. **Reporting and Remediation.** Tripwire Enterprise detects unauthorized or unplanned change and helps IT determine if that change took a configuration out of policy. Tripwire Enterprise also generates detailed reports, provides prescriptive steps to remediate failures, lets IT waive specific failures and automatically reconciles detected changes with leading enterprise management systems. Tripwire Enterprise even provides the ability to update a test with an out-of-policy value if that value reflects what the organization really needs.

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

# 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 configuration assessment and change audit 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 configuration assessment 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, Midsize and Desktops

**Tripwire Enterprise for File Systems, Midsize 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 architected to achieve configuration control across the enterprise with minimal impact on network bandwidth.

# Components (cont.), Platform Support and Specifications

## Tripwire Enterprise for VMware ESX

**Tripwire Enterprise for VMware ESX** 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 ESX 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 change auditing 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, MIDRANGE 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
- IBM i5/OS for AS400/iSeries

**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
- 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 ESX—SUPPORTED HYPERVISORS

- VMware ESX 3.0, 3.5 & ESXi

## 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

www.tripwire.com

## ABOUT TRIPWIRE

Tripwire is the leader in data center compliance and infrastructure management solutions, building confidence for IT across both virtual and physical infrastructures. Tripwire Enterprise and vWire software help over 6,500 enterprises worldwide meet their configuration auditing, file integrity monitoring, virtual infrastructure management and change auditing needs for IT operations, security and compliance. Tripwire is headquartered in Portland, Oregon, with offices worldwide. Tripwire can be found at www.tripwire.com, www.vwire.com, and @vwire on Twitter.

©2009 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. | TEPB7601