TRIPWIRE®
ENTERPRISE

# TRIPWIRE ENTERPRISE 8.4 DETECT. RESPOND. PREVENT.

◆ Tripwire has nearly two decades of experience in the security and compliance industry, with foundational technology essential for detecting cyber threats, rapid and real-time response, and prevention against future attacks. Tripwire Enterprise has kept over half of the Fortune 500 and many of the most sensitive networks in the world secure and compliant, with its capabilities fulfilling many security and policy compliance requirements. ◆


Tripwire® Enterprise is a security configuration management (SCM) suite that provides fully integrated solutions for policy, file integrity and remediation management. Organizations can use these solutions together for a full, end-to-end SCM solution, or use its file integrity monitoring or policy management solutions on their own to address today's pressing security and compliance challenges, while building a foundation that positions them to address tomorrow's. The suite lets IT security, compliance, and IT operations teams rapidly achieve a foundational level of security throughout their IT infrastructure by reducing the attack surface, increasing system integrity and delivering continuous compliance. Plus, because Tripwire Enterprise integrates with enterprise applications to automate workflow with additional security point solutions like SIEMs and change management tools, organizations can broaden their security worldview and gain even greater efficiencies.

A key IT enterprise security and compliance solution, Tripwire Enterprise supports a *detect, respond and prevent* strategy by:

- **Detection** of cyber threats and possible breach activity by highlighting possible indicators of compromise
- **Response** to deviations with high value, low volume alerts with guidance on what to do to return the system to a known secure state
- **Prevention** through adapting and prioritizing threats and change deviations to maintain a consistently hardened and objective view of overall security posture across all devices and systems

## HOW IT WORKS: TIGHTLY INTEGRATED CONTROLS

Tripwire Enterprise delivers four integrated capabilities that work in concert to create an enterprise-class SCM solution:

- **Tripwire File Integrity Manager (FIM)** is the world's first and best file integrity monitoring solution. It checks across large heterogeneous environments to provide threat detection and instant insight into configuration vulnerabilities while increasing operational efficiency by reducing configuration drift and unauthorized change. Tripwire's FIM can be used stand-alone to provide granular endpoint intelligence with rapid insight to security and compliance posture. If used in conjunction with Tripwire Policy Manager, it delivers change-triggered configuration assessment and other system configurable responses. This turns a "passive" configuration assessment into a dynamic, continuous, and real-time defensive solution that immediately detects deviations from expected, secure configuration standards and hardening guidelines.

- **Tripwire Policy Manager** establishes and maintains consistent compliance agent-based and agentless continuous configuration assessment against over 650+ combinations of platforms and security and compliance policies, standards, regulations and vendor guidelines. The Policy Manager also offers complete policy customization, waiver and exception management, automated remediation options, and prioritized policy scoring with thresholds, weights and severities. It does all this while providing auditors with evidence of compliance and making policy status highly visible and actionable for compliance teams.
- **Remediation Manager,** a value-add component of Tripwire Policy Manager, provides built-in guidance to IT security and compliance teams to repair drifted, misaligned security configurations while retaining role-based management, approvals and sign-offs for repairs. This helps operations teams more easily and efficiently know what failed and how to return systems into a production-ready state—and once they're in production, keep them there.
- **Investigation and Root Cause Drill-down** capabilities give IT Security and Operations teams the ability to rapidly and effectively investigate to determine root causes. Systems inevitably change as enterprises constantly revise and change their people, processes and technologies. Tripwire Enterprise can deliver granular drill-down, side-by-side comparisons, historic baselines and comparisons to quickly provide investigative teams what they need to know: what changed, when, by whom and how often, with "how" information.

## INDUSTRY-LEADING IT SECURITY AND COMPLIANCE CAPABILITIES

As part of an industry-leading security platform, Tripwire Enterprise can leverage these components to meet key IT security and compliance needs.

- **Tripwire Search by Hash API** provides API commands within the Tripwire Enterprise Data API. This command set API will let IT teams test systems being monitored by Tripwire Enterprise for bad file hash values in an automated way, using scripts or programs to leverage the Search by Hash API commands, and use large lists to search large numbers of assets.
- **Point-of-Sale (POS) Threat Content** is now available to protect Windows and Windows Embedded OS. These systems are especially vulnerable to digital tampering, malicious insiders, and RAM scraping, and once breached, privilege escalation and data exfiltration. Tripwire has released specialized content with tests for many of the most common attack changes that occur on POS.
- **Tripwire Asset View** helps organizations manage their Tripwire-monitored assets through their unique business lens by assigning tags that can reflect risk, priority, relevance and organizational alignment. Now Tripwire Enterprise can provision assets with pre-assigned asset tag files, shortening the time it takes to provision and have assets up, labeled and functioning. And now, Tripwire IP360 vulnerability assessments can deliver risk-prioritized asset tags to Tripwire Enterprise for increased risk visibility and remediation.
- **New Dashboards and Advanced Reporting** allows Tripwire Enterprise to track and display more detailed cyber threat monitoring and compliance reporting along with trending and customization. These new capabilities are field-proven and come from advanced work being done with Tripwire customers.
- **Tripwire Connect** is a new product from Tripwire that integrates with Tripwire Enterprise to deliver advanced, customizable— yet easy-to-use—reporting.

## ENTERPRISE SUPPORT

Tripwire Enterprise can operate with agents or agentlessly, and supports:

- All major OSes: Windows, Red Hat, SUSE, Solaris, MacOS, Debian, CentOS, etc.
- Many vendor-specific OSes: AIX, HP-UX, etc.
- Directory Services: Active Directory, LDAP, etc.
- Network Devices: Firewall, IPS and IDS configurations, routers, etc.
- Databases: Oracle, MS SQL, DB2, etc.

◆ Tripwire has taken its original host-based intrusion detection system, which could simply detect changes to files and folders, and expanded it into a robust file integrity monitoring (FIM) solution, able to monitor detailed system integrity: files, directories, registries, configuration parameters, DLLs, ports, services, protocols, etc. Enterprise integrations provide granular endpoint intelligence that supports threat detection, policy and audit compliance. Years have been spent honing Tripwire's ability to detect and judge change with policy and security risk prioritization and integration refinements to achieve high value, low volume change alerts. Tripwire Enterprise helps the largest enterprises manage system configuration integrity, security and compliance. ◆

## FEATURES AND BENEFITS

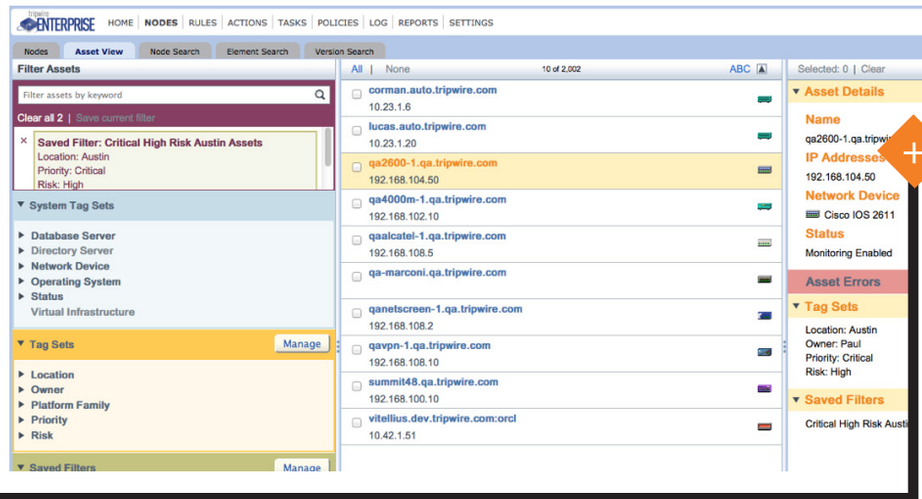
| | |
|---|---|
| **Increased threat detection for changes that indicate threats or breach activity.** | Tripwire Enterprise has a number of threat detection and response capabilities, with a new Search by Hash API, Point-of-Sale (POS) device protection, and integrated threat intelligence services in addition to our own integration for adaptive threat intelligence from Tripwire IP360. |
| **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. |
| **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. |
| **Robust Asset View capabilities** | Asset View lets you classify assets with business-relevant tags such as risk, priority, geographic location, regulatory policies, and more. Tripwire Enterprise's asset view capabilities now offer provisioning with an asset tag file, increased scale for large numbers of assets, and imported asset tagging from integration with Tripwire IP360, giving a sharper view of risk across the entire organization. |
| **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. |
| **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 (FIM) 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 processes** | 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. |
| **Tag Integration Framework to import metadata into Asset View** | The Tag Integration Framework lets you automatically bring metadata associated with assets in other IT systems into the Asset View as tags. That saves time tagging assets and quickly aligns your Tripwire-monitored assets with your business environment. |
| **Import Metadata from Existing Systems into Asset View with the Tag Integration Framework** | The Tag Integration Framework lets you automatically bring metadata associated with assets in other IT systems into the Asset View as tags. That saves time tagging assets and quickly aligns your Tripwire-monitored assets with your business environment. |


## READY TO DIG DEEPER?

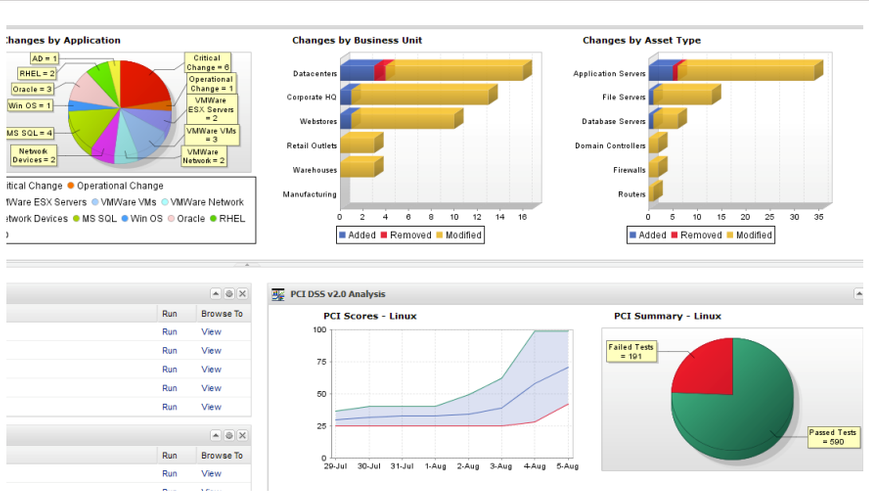
**Visit www.tripwire.com for the following datasheets**

- Tripwire File Integrity Manager
- Tripwire Policy Manager
- Tripwire Remediation Manager
- Tripwire Enterprise Report Catalog
- Tripwire Enterprise Platform Support
- Tripwire Connect

# FROM MACRO VIEWS TO MICRO DETAILS




**ORGANIZE AND MANAGE** *your assets in a way that reflects your business priorities*




**VIEW CHANGE AND CONFIGURATION** *from any perspective necessary*

| | | |
|---|---|---|
| | Header flags: Inherited ACE | Header flags: Inherited ACE |
| Group | iliad\None | iliad\None |
| Owner | BUILTIN\Administrators | BUILTIN\Administrators |
| Read-Only | false | false |
| SACL | Inherits Entries: true<br><br>Mandatory Label\Low Mandatory Level, Unsupported type: 17:<br>Specific rights:<br>List Folder / Read Data | Inherits Entries: true<br><br>Mandatory Label\Low Mandatory Level, Unsupp<br>Specific rights:<br>List Folder / Read Data |
| SHA-1 | d2b02ce1d4a7419a44aa2c30c012cddc394d8609 | da39a3ee5e6b4b0d3255bfef95601890afd80709 |
| Size | 20 | 0 |
| Stream Count | 1 | 1 |
| Stream SHA-1 | 2ccff934e001635915b9a76825f1d631c1392ea4 | 2ccff934e001635915b9a76825f1d631c1392ea4 |
| Type | File | File |

Insertion Deletion Change

**ZOOM INTO DETAILS** *that distinguish new threats from accidents and common*

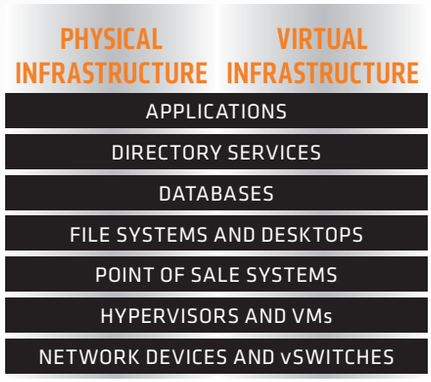
# REPORTS

◆ Tripwire Enterprise provides nearly 40 reports, with additional new dashboards and reports always being developed. More samples and a full Report Catalog are available on our 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

# 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 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 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.

## TRIPWIRE ENTERPRISE FOR POINT-OF-SALE (POS) DEVICES

Tripwire Enterprise secures POS devices against cyber threats, manages security and compliance policies for these devices, and provides IT Operations with alerts, notifications and response guidance when possible breach indicators or "indicators of compromise" are suspected to exist on these devices. Tripwire Enterprise agents can be run on supported POS device platforms, kiosks, some ATMS and other similar devices running Windows XP, 7, 8 and Windows Embedded OS.

## TRIPWIRE ENTERPRISE FOR VIRTUALIZED ENVIRONMENTS

Tripwire Enterprise works in virtualized environments—private, public and hybrid clouds. The Tripwire Enterprise Console can operate as a virtual machine, and its agents can monitor any supported virtualized endpoint. This includes delivering protection for cyber threats in virtualized/cloud environments, system integrity monitoring, application of security and compliance policies, real time alerts and notifications, dashboards and reporting. Tripwire Enterprise also works with provisioning tools such as Puppet, Chef, Ansible and others. Supported cloud environments include Microsoft Azure, Amazon Web Services (AWS), Verizon Terremark and various FedRAMP-approved environments. Tripwire Enterprise is also in use with a

number of Managed Service Providers (MSPs/MSSPs). Tripwire Enterprise supports VMware, Microsoft Hyper-V and Red Hat Enterprise. Additional support is under constant development.

### 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.

# PLATFORM SUPPORT & SPECIFICATIONS

## TRIPWIRE ENTERPRISE CONSOLE—SUPPORTED PLATFORMS AND BROWSERS

- Windows, Red Hat Enterprise Linux, SUSE Linux Enterprise
- Firefox, Internet Explorer

## TRIPWIRE ENTERPRISE FOR APPLICATIONS—SUPPORTED APPLICATIONS

- Microsoft IIS
- Microsoft Exchange 2010 & 2013

## TRIPWIRE ENTERPRISE FOR DIRECTORY SERVICES—SUPPORTED APPLICATIONS

- Windows Active Directory

## TRIPWIRE ENTERPRISE FOR FILE SYSTEMS AND DESKTOPS—SPECIFICATIONS

**Agent platform support**

- AIX
- CentOS
- Debian
- HP-UX
- Mac OS X
- Oracle Enterprise Linux
- Red Hat Desktop Linux
- Red Hat Enterprise Linux
- Solaris SPARC, x86 & x64
- SUSE Linux Enterprise Server
- Windows Server 2003, 2008 & 2012
- Windows Desktops, incl. XP, Vista & 7

**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**

- Hyper-V
- Red Hat Enterprise Virtualization
- VMware ESX & ESXi
- VMware vSphere

**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

**Agentless support for file systems**

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

## TRIPWIRE ENTERPRISE FOR VMWARE—SUPPORTED HYPERVISORS

- VMware ESX & ESXi
- vCenter Server

# PLATFORM SUPPORT & SPECIFICATIONS (CONT.)

## TRIPWIRE ENTERPRISE FOR NETWORK DEVICES—SUPPORTED VENDORS & DEVICES

- Cisco IOS, CatOS, PIX OS & ASA
- Cisco VPN 3000 Series Concentrator
- Cisco Catalyst 1900/2820 Switch
- Alcatel OmniSwitch
- Bluecoat
- Extreme
- F5 BigIP
- Foundry FastIron & ServerIron
- HP ProCurve Series
- Juniper M/T Series
- Marconi ForeThought
- NetScreen
- Nokia IPSO
- Other devices using the included Universal Device Kit

**Agentless support for file systems**

- POSIX-compliant operating systems

## TRIPWIRE ENTERPRISE FOR POINT OF SALE (POS) DEVICES—SUPPORTED OSes

- Windows 7 & 8 Embedded*

## TRIPWIRE ENTERPRISE FOR DATABASES—SPECIFICATIONS

### ORACLE 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 2005, 2008 & 2012

**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 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)

Visit www.tripwire.com for detailed platform version support *Tripwire supports the TE Agent on Windows Embedded 7 Standard, Windows Embedded 8 Standard platforms. Because of the modular and customizable nature of these platforms, we strongly recommend testing the agent in your particular Windows Embedded configuration. Tripwire may not be able to support your configuration of embedded Windows. Some capabilities of the agent and security content might require configuration changes to your Windows system. In certain cases, you may want to engage with Tripwire Professional Services to assist with your deployment.

tripwire®

◆ Tripwire is a leading provider of advanced threat, security and compliance solutions that enable enterprises, service providers and government agencies to confidently detect, prevent and respond to cybersecurity threats. Tripwire solutions are based on high-fidelity asset visibility and deep endpoint intelligence combined with business-context, and enable security automation through enterprise integration. Tripwire's portfolio of enterprise-class security solutions includes configuration and policy management, file integrity monitoring, vulnerability management and log intelligence. Learn more at tripwire.com. ◆

**SECURITY NEWS, TRENDS AND INSIGHTS AT TRIPWIRE.COM/BLOG ◆ FOLLOW US @TRIPWIREINC ON TWITTER**



TEPB84a 201509