

PRODUCT BRIEF

TRIPWIRE LOG CENTER

HIGH PERFORMANCE LOG AND EVENT
MANAGEMENT FOR SECURITY AND COMPLIANCE



Enterprise organizations of all sizes need to achieve compliance with regulations and standards and to secure their IT infrastructure and the data it contains. As security breaches continue to rise, this need has never been more critical. Log collection, retention and reporting have become mandatory requirements of almost all regulatory policies and an accepted best practice. Enterprises are looking to implement these systems for the lowest cost and in the shortest possible time. But capturing and storing log data by itself does not make you more secure. Forward-thinking organizations realize this data represents a gold mine that, if properly accessed and analyzed in real time, can reduce security risk by identifying critical threats before the damage is done.

Tripwire® Log Center provides these capabilities with an easy-to-use, flexible and affordable solution that you can install within minutes to begin capturing log data. Tripwire's ultra-efficient log management solution provides everything you need to meet log compliance requirements. Its sophisticated security event management option adds the intelligence to identify the most critical threats, when they occur. And both capabilities are available as a single product that offers the industry's lowest total cost of ownership for an SIEM solution.

And as part of the Tripwire VIA suite of products, Tripwire Log Center offers out-of-the-box integration with Tripwire Enterprise to offer visibility beyond events. Tripwire Enterprise combines real-time change detection, comprehensive configuration auditing, continuous policy compliance management, and rapid configuration remediation in a single solution. By integrating these Tripwire solutions, you can correlate all suspicious events with changes to take control of threats across all events and changes.

WHAT DISTINGUISHES TRIPWIRE LOG CENTER FROM OTHER SIEM PRODUCTS?

- **Performance:** Tripwire Log Center delivers fast, efficient and affordable log management, with the ability to support tens of thousands of events per second. It achieves this high performance by writing the log data in its original format to highly compressed flat files. By comparison, many log management products must duplicate the data, storing raw log files in an archive and current data in a relational database for queries and reporting. This two-tiered data scheme is complex, expensive, and often results in older forensic data not being readily accessible.
Tripwire Log Center is unique in providing high-speed search, query and reporting functions directly from the flat file. With Tripwire Log Center, you get both unstructured search on raw text and fully structured reporting on normalized data, all without a SQL database. Because there is no separation between "active data" and "archived data," you benefit from significantly reduced costs and simplified log management.
- **Flexibility:** Tripwire Log Center offers its ultra-efficient log management capabilities as a software-based solution, so you can deploy it on your own low-cost hardware, consistent with your organization's standards. In addition, Tripwire Log Center software is modular, allowing you to locate functionality where you need it. This approach ensures you only pay for the capacity you need rather than purchasing special-purpose appliances in capacity increments that may exceed or fail to meet your needs.
- **Integration:** Most SIEM products make you choose between strong log management and strong event management capabilities. And typically these products are offered as two separate products that require two separate appliances. As a truly integrated solution, Tripwire Log Center was built from the ground up to include log and event management in single product.

Introduction

TRIPWIRE LOG CENTER MAKES COMPLIANCE EASY

Tripwire Log Center provides everything you need to meet the log compliance requirements of most regulatory policies. It captures all necessary log data and stores it in its original, raw format to ensure the integrity of the data for forensic analysis. And Tripwire Log Center's out-of-the-box reports for standard policies including PCI, SOX, GLBA and HIPAA automate the tasks of passing compliance audits.

TRIPWIRE LOG CENTER REDUCES SECURITY RISK

Tripwire Log Center extends the solution's log management capabilities to provide real-time event correlation and alerting through the Event Manager option. This makes Tripwire Log Center a fully functional security event manager, with the security console, complex correlation and real-time alerting supported by an event database to store all events of interest. It is this capability that adds real-time intelligence to the system and enables you to detect and react to security threats as they occur.

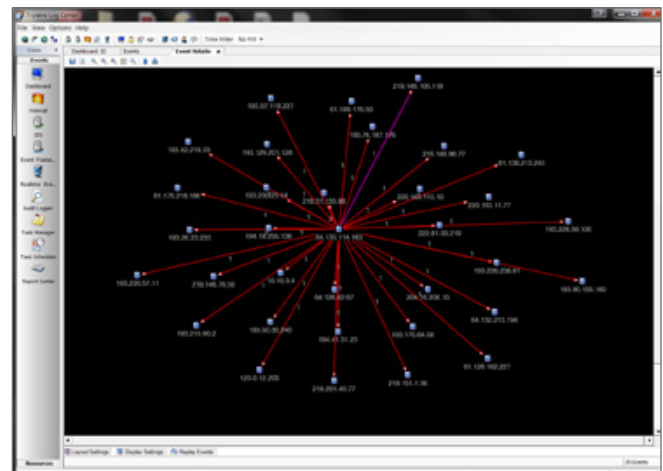
Both the Tripwire Log Center log and event management functions share the same console, data collectors and normalization rules. The user can easily switch back and forth between analyzing events of interest stored in the event data base and accessing the complete log history stored in the log files. In addition, you can purchase the full log and event management solution for about the same price that most other vendors charge for log management alone.

COMBINING TRIPWIRE SOLUTIONS OFFERS YOU MORE

To attain the broadest compliance coverage and maximum security control, take advantage of Tripwire VIA, an IT security and compliance suite that combines Tripwire Log Center with Tripwire Enterprise, the world's leading solution for configuration control. Like log management, file integrity monitoring is a mandatory requirement of most regulatory policies and is an accepted best practice. Tripwire Enterprise is a natural complement to Tripwire Log Center, allowing you to combine multiple real-time data sources—log information, change data and compliance status—and improve your ability to detect and act upon critical compliance and security threats, when they occur.



Total Visibility: Log Center shows all events across the IT infrastructure. Zoom in and drill into any suspicious activities for details.



Log Center captures every event making it easy to do deep forensics. Here is an example of an infrastructure map that shows a replay of an attack.

Tripwire Log Center Components

TRIPWIRE LOG CENTER COMPONENTS

Tripwire Log Center offers three main components—Log Manager, Event Manager and Log Concentrator.

Log Manager

Log Manager is a complete log compliance solution that collects, retains and reports on log data from countless IT infrastructure devices. When Log Manager collects log data, it compresses it, encrypts it and applies a checksum algorithm to ensure the integrity of the data before storing it as a flat file. With its fast Google-like indexing, Log Manager provides full reporting and complex query capabilities necessary for compliance reporting and forensic analysis. Log Manager also includes real-time, conditional alerting, so you'll know about suspicious activities immediately. You access all the features and functionality of Log Manager through a Log Center Console.

Event Manager

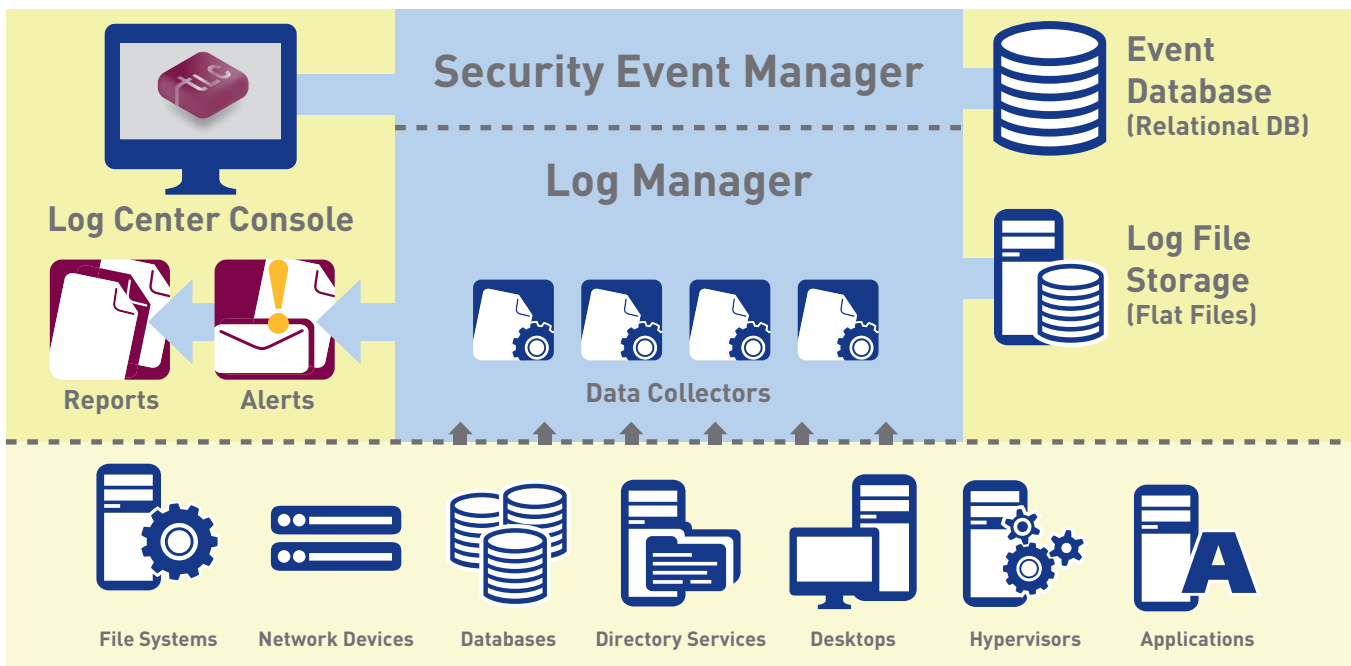
Event Manager uses the same code base and user interface as Log Manager to easily add security event management to your log management capabilities. The Event Manager enables the event database that stores alerts, events of interest and

vulnerability data and allows you to correlate those sources. It also provides near real-time views of current security events through the security dashboard and supports deep forensic analysis of that information. And Event Manager includes a security event ticketing system that ensures you prioritize and address high-priority security events.

Log Concentrator

You can deploy Log Concentrators to remote locations to collect, store and forward local log data. The Log Concentrator compresses and encrypts the log data for much more efficient, secure transmission. You can upload data to the Log Manager immediately or schedule upload for times when network traffic is low. You can also use Log Concentrators to distribute processing across multiple systems at high volume sites. In both cases, you get the same real-time, conditional alerting available as Log Manager. If your Tripwire Log Center installation includes event management, the Log Concentrator can also filter the stream of log data for events of interest and immediately transmit these events to the event database, even if the Log Concentrator is holding the compressed log data for later transmission.

Tripwire Log Center



The Log Manager component of Tripwire Log Center collects activity logs from anywhere in the IT infrastructure, compressing, encrypting, indexing and storing them quickly into flat files. Add the Event Manager to reduce security risk by getting near real-time dashboard visibility to security events and correlating events of interest, alerts and vulnerability data.

Tripwire Enterprise Integration

TRIPWIRE ENTERPRISE INTEGRATION

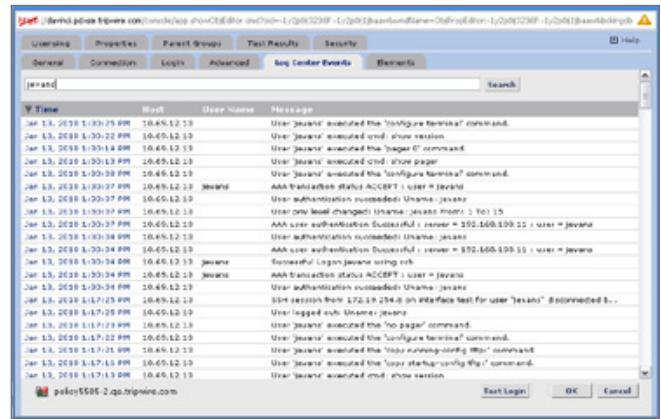
Tripwire offers the only integrated solution that lets you dynamically analyze your infrastructure so you have full visibility across events and changes. By integrating Tripwire Enterprise with Tripwire Log Center, organizations correlate events of interest with changes that impact IT policies to provide a complete view of all suspicious activities. With real-time alerting, rich dashboards and comprehensive archiving, you can protect your IT infrastructure with security-hardening standards and ensure immediate access to comprehensive audit histories.

Integrating the Tripwire Enterprise with Tripwire Log Center also gives you the automated intelligence you need to find the changes that impact your policies without sifting through reams of security logs. Comprehensive change data is integrated right into the suite.

Tripwire Enterprise offers benefits beyond those offered by the integration. It offers policy compliance management to help you achieve and maintain continuous compliance with industry-based IT security policies like PCI, NERC, and HIPAA; security standards and vendor configuration best practices like NIST, CIS, FISMA; or your own internal standards. It also offers proven file integrity monitoring that assures security by detecting

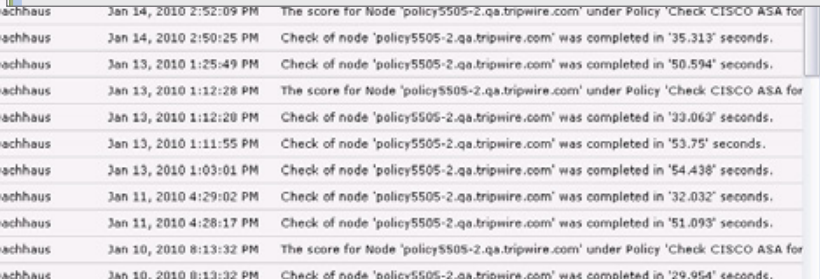
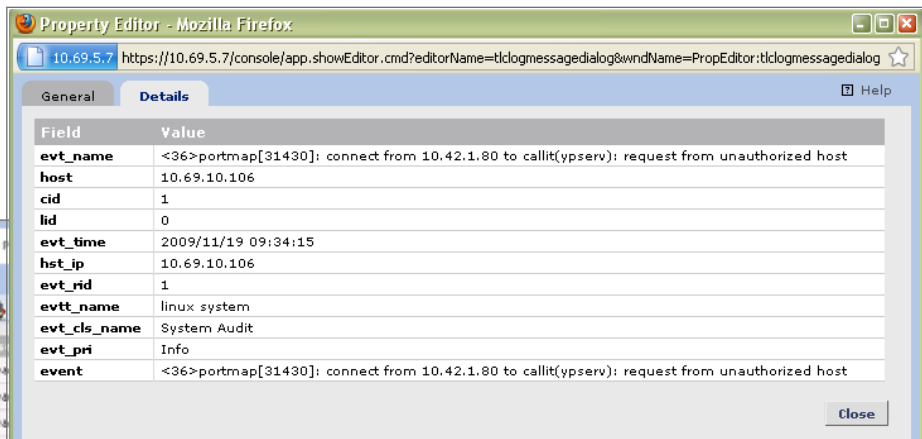
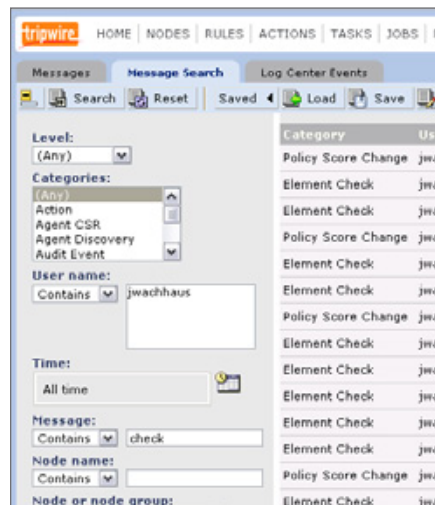
changes to files and configurations throughout physical and virtual infrastructures.

If your organization needs to take control of all events and changes across its entire IT infrastructure, combining Tripwire Log Center with Tripwire Enterprise provides real-time visibility into all threatening activities. With Tripwire, you see the full story of the events associated with unauthorized changes—both the events that led to the change and all the activities downstream impacted by that unexpected change.



By integrating Tripwire Enterprise with Log Center, organizations get visibility across all changes and events. Here a Tripwire Enterprise user sees all the events that surround a set of changes, providing a full context of all related activities.

Suspicious changes can be used to search for corresponding events from Log Center—directly from within Tripwire Enterprise. This means the Tripwire Enterprise user can quickly see all the events that surround a change, without ever leaving the Tripwire Enterprise interface.



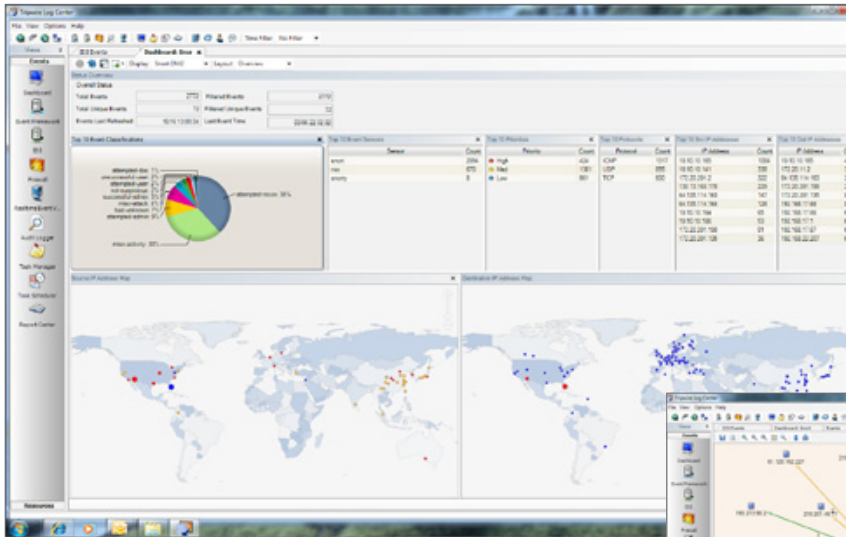
Features and Benefits

LOG MANAGER FEATURES AND BENEFITS	
ULTRA-EFFICIENT LOG MANAGEMENT	Tripwire Log Center's unique architecture enables it to run on standard Windows servers and capture tens of thousands of events per second (EPS).
REAL-TIME, ADVANCED CONDITIONAL ALERTING	Tripwire Log Center provides real-time alerting that can be based on complex sequences of events from multiple sources, ensuring you receive immediate notification of suspicious activity—functionality typically found only in security event manager solutions. Alerts can be sent via email, Syslog, scripts or directly to the console.
COMPLIANCE REPORTS	Log Manager includes out-of-the box reports for standard policies including PCI, SOX, GLBA and HIPAA.
EFFICIENT, CONVENIENT LOG STORAGE	When Tripwire Log Center captures logs, it compresses them (at up to 25:1 ratio) encrypts and then stores them to a flat file, so you can use standard storage mediums like SAN and NAS. Because active log data is the same as archived log data, Tripwire Log Center avoids a two-tiered data architecture.
BROAD LOG FORMAT SUPPORT	Tripwire Log Center supports all popular log transmission protocols (Syslog UDP/TCP, SNMP v1-3, database, Windows WMI, Cisco SDEE, SQL, FTP, SFTP, File Copy, and CheckPoint OPSEC) so you can immediately start collecting logs from virtually any source.
BROAD DEVICE AND APPLICATION SUPPORT	Tripwire Log Center ships with pre-defined normalization rules for all of the devices and applications present in most organizations (see list below). Additional devices can be quickly added by Tripwire when needed, or you can easily create your own rules using the regular expressions format.
DYNAMIC LOG SCHEMA	Unlike other products, Tripwire Log Center applies normalization rules on raw log data after it is captured, not before, so you don't need to know the log schema to capture a new device log. Later, when generating reports and queries, you can dynamically add to or edit the schema to support the log format.
POWERFUL SEARCH CAPABILITIES	Freeform Google-like text searches let you quickly access forensic evidence and search for events from the raw log data.
SQL-LIKE QUERIES AND REPORTS	Tripwire Log Center lets you query log data using SQL-like requests and generate formatted reports that normalize and present just the log data you request—all without requiring an SQL database.
EVENT MANAGER FEATURES AND BENEFITS	
SOPHISTICATED SECURITY EVENT MANAGEMENT	Event Manager lets you correlate alert, event and vulnerability data to gain visibility to the events that introduce security risk.
EVENT DATABASE	With the event management option, Tripwire Log Center provides the support to create and use the event database, storing current events of interest for quick display, analysis and drill-downs. MySQL and Microsoft SQL databases are supported. Filtered event data can be collected from all Log Managers or Log Concentrators throughout the enterprise.
SECURITY DASHBOARD AND EVENT VIEWS	Tripwire Log Center gives you a centralized, dashboard view of the alerts, events and vulnerabilities in your infrastructure to help you better manage your security risks and dynamically drill down on areas requiring greater scrutiny.
FULL CORRELATION SEARCH	You can perform sophisticated queries and search across all data stored in the event database.
DEEP FORENSIC ANALYSIS	Tripwire Log Center gives security analysts the tools to track the organization's security status and then quickly investigate suspicious incidents for their potential cause, impact and ongoing effects. When current security events raise questions about past incidents, analysts can just as easily access data from the flat log files as they can the data stored in the event database.

Features and Benefits (cont'd)

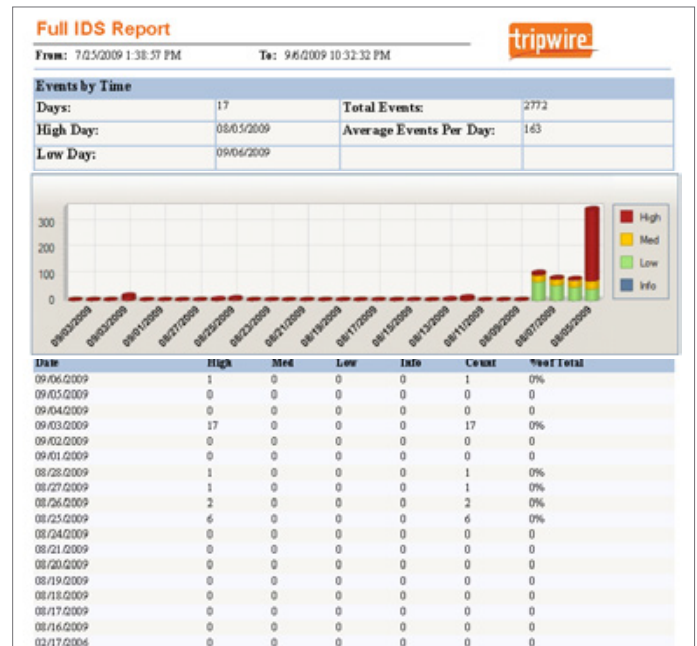
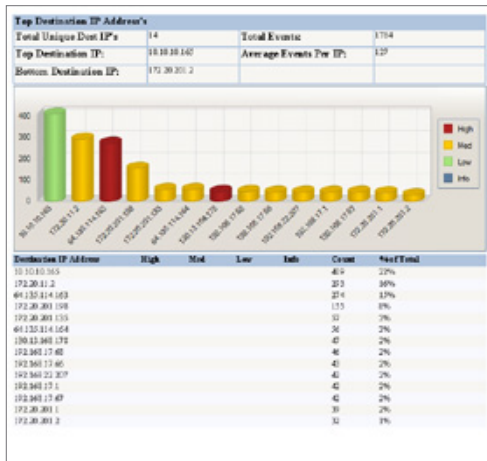
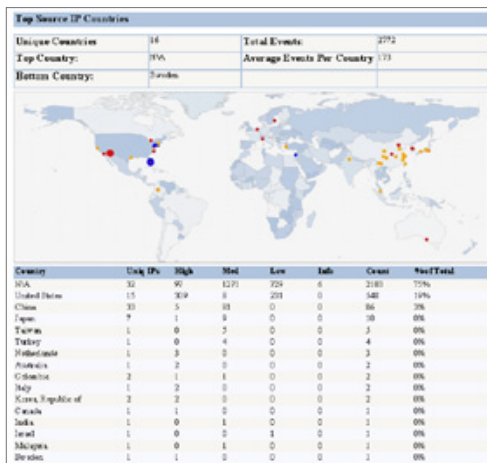
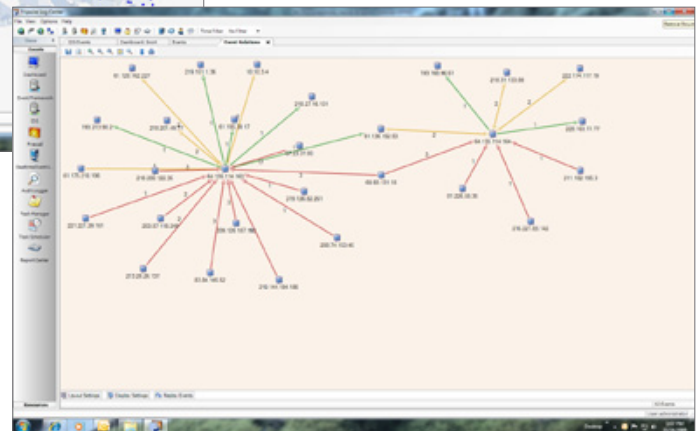
EVENT MANAGER FEATURES AND BENEFITS (CONT'D)	
DRAG AND DROP CORRELATION RULE CREATOR	Tripwire Log Center includes a graphical, drag and drop rule creator that lets you easily create and customize correlation rules to identify the complex combinations of events that you need to be alerted to.
EVENT FLOW VISUALIZATION	Event Manager can automatically generate a graphical event relationship diagram, giving you an additional forensic tool for pinpointing which parts of the IT infrastructure are being affected by a particular incident. You can also replay events to see how an attack entered and dispersed through the network.
SECURITY EVENT TICKETING SYSTEM	From within Tripwire Log Center, you can generate event tickets so that you can prioritize and track incident response.
OVERALL FEATURES AND BENEFITS	
LOG AND EVENT MANAGEMENT IN ONE SOLUTION	Tripwire Log Center is an advanced log and event manager in a single solution that shares log collectors, consoles, reporting, correlation rules, and more. This single solution approach also reduces costs, training time, and set-up time. Your users can easily alternate between accessing event data and accessing raw log data.
AFFORDABLE AND SCALABLE SOLUTION	As a software-only solution, you install Tripwire Log Center where you need it, on your own hardware, sized for the log volume at each location. And you pay just for the volume of log data you need on an enterprise basis, rather than purchasing appliances that are only offered in expensive and large, pre-set increments.
OUT-OF-THE BOX COMPLIANCE REPORTS	Tripwire Log Center ships with the reports you need most to easily meet log management requirements of regulations such as PCI, SOX, GLBA and HIPAA.
EASY-TO-USE CONSOLE	The Tripwire Log Center console is the graphical user interface for controlling Tripwire Log Center. The Console provides role-based authorization, and you can allow users to see all or just their part of the log and event data. You can deploy as many consoles as you need; each console can seamlessly connect to any Tripwire Log Manager, Log and Event Manager or Log Concentrator within the network.
LOCATION SEPARATION	Tripwire Log Center allows you to limit access to log data based on location, type or function. This setup is ideal for multi-divisional organizations or service providers that support multiple clients; they simply install a single Tripwire solution and give individual users secure access to only their data.

Reports and Dashboards



(Above) Tripwire Log Center allows users to create customized dashboards.

(Below) Event relationship diagram displaying color-coded links between the nodes, showing the highest priority events that flowed over each link.



(Left and Above) A Tripwire Log Center IDS Report, providing the status of all IDS events during a user-determined time frame.

Supported Devices, Applications and System Requirements

SUPPORTED DEVICES AND APPLICATIONS

Firewall and VPNs

- ARKOON Firewalls
- Avenail Firewalls
- Check Point Firewall-1
- Cisco ASA
- Cisco Linksys VPN Router
- Cisco PIX® Security Appliance
- Cisco VPN Series Concentrator
- CyberGuard Firewalls
- Fortinet FortiGate Firewalls
- GnatBox Firewalls
- InGate Firewalls
- Juniper Netscreen Firewalls
- Juniper SSL VPN
- Netscreen
- Windows XP Firewall
- Microsoft® ISA
- MonoWall
- RapidStream Firewalls
- Secure Firewall (Sidewinder)
- SecureSoft Firewalls
- SunScreen Firewalls
- Symantec Enterprise Firewall™ / Raptor Firewall
- WatchGuard Firebox Firewalls
- WELF

Vulnerability Management

- Retina REM Console
- GFI Network Security Scanner
- Harris STAT
- Internet Scanner
- Nessus Scanner
- NMap

System Monitoring

- Apple Mac OS X
- Cisco Security Agent (CSA)
- Debian GNU/Linux
- Free BSD
- IBM iSeries (AS400)
- Microsoft® Windows Server 2000
- Microsoft® Windows Server 2003
- Microsoft® Windows Server 2008
- Microsoft® Windows Vista
- Microsoft® Windows XP
- Novell SUSE Linux
- Snare for Windows
- Linux
- OpenBSD
- Red Hat Enterprise Linux
- Red Hat Fedora Core Linux
- Sun Solaris™
- SonicWALL Firewalls
- Tripwire for Servers
- Tripwire Enterprise
- Ubuntu Linux

Web Servers

- Apache HTTP Server
- Microsoft® Internet Information Server (IIS)
- Snare IIS

Database

- Microsoft SQL Server
- Oracle Database

Email

- Microsoft Exchange Server

Applications

- Courier POP3
- Microsoft® DHCP
- Microsoft® Proxy Logs
- glFTPd
- IPFilter Firewall
- IPTables Firewall
- NcFTPd
- Postfix
- Pure-FTPd
- Sendmail
- VSFTPD
- Nagios
- Qmail
- Snare Apache
- VMware ESX
- WU-FTPd

Intrusion Detection/Prevention Systems

- Cisco IDS/IPS
- Dragon HIDS
- Fortinet Fortigate IDS/IPS
- RealSecure Network Sensor
- Proventia (NetworkICE)
- McAfee® IntruShield®
- Snort IDS
- Sourcefire IDS
- Symantec Intruder Alert™
- TippingPoint IPS
- Third Brigade

Multi-Function Appliance (UTM)

- FortiGate™ Antivirus Firewall

AntiVirus Systems

- SourceFire Clam Antivirus
- Symantec AntiVirus Corporate Edition
- Fortinet FortiGate Antivirus
- McAfee® VirusScan Enterprise
- McAfee® Orchestrator (ePO)

Routers and Switches

- 3COM Firewalls
- Cisco Catalyst Switch
- Cisco IOS Router
- Linksys
- DLink
- Enterasys Routers
- Enterasys Switches
- HP ProCurve Network Switches
- HP SAN Switch
- Netopia Router
- Nortel Connectivity
- Nortel Switch
- TopLayer AppSwitch
- ZyXEL

Wireless

- Aruba Wireless
- Cisco Wireless

SYSTEM REQUIREMENTS

Recommended requirements for a mid-size installation are as follows:

Log Manager

- CPU: Single Quad-Core Intel® Xeon® processor or equivalent
- Memory: 4GB + 2MB per device
- Disk: 500GB 7.2K RPM SATA Drive; recommend additional to enable a RAID Configuration
- Operating System: Microsoft Windows 2003 64-bit; Microsoft Windows 2008 64-bit
- Other Software: Microsoft .NET Framework version 3.5

Log and Event Manager

- CPU: Single Quad-Core Intel Xeon processor or equivalent
- Memory: 4GB + 2MB per device
- Disk: 500GB 7.2K RPM SATA Drive; recommend additional to enable a RAID Configuration
- Operating System: Microsoft Windows 2003 64-bit; Microsoft Windows 2008 64-bit
- Other Software: Microsoft .NET Framework version 3.5
- Databases: MySQL v5.1 or later; MS-SQL (non-express versions)

Log Concentrator

For medium to high volume log data collection, system requirements are the same as for the Log Manager. For low volumes, minimum requirements are 1GB memory, 100GB disk space, Windows 2003 32-bit, and .NET Framework version 3.5.

Log Center Console

- Memory: 2GB or better
- Disk: Minimum of 100MB free space
- Operating System: Windows 2003 – All Versions; Windows 2008 – All versions; Windows XP, Vista & 7 – All non-home versions
- Other Software: Microsoft .NET Framework version 3.5

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 tripwire.com.

