



TAKE CONTROL.



## LOG MANAGEMENT AND SIEM FOR SECURITY AND COMPLIANCE

As part of the Tripwire® VIA™ platform, 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.

Organizations of all sizes need to secure their valuable IT infrastructure and data and achieve compliance with regulations and standards. As security breaches continue to rise, this need has never been more critical. Log collection, retention and reporting are an accepted best practice for security and mandatory requirements of most regulatory policies. For years, though, log management solutions have generated a lot of noise without helping detect threats.

To reduce this noise and better identify threats, organizations began deploying SIEM solutions. These solutions offered a centralized view of threats, alerted on suspicious activities, and produced reports for security forensics or proof of compliance. Unfortunately, organizations purchased a specific SIEM based on the promise that it could help them detect potential breaches. At the time, few were able to manage their SIEM to improve security. Their solutions were simply too complex. So while they met compliance requirements, they did little to improve security. Now most organizations want a solution that meets their compliance needs, but also makes it easy to noticeably improve security.

Log and security event data together can significantly improve security by identifying critical threats before the damage is done—but only if the data is analyzed in the context of risk to the business. Tripwire Log Center provides

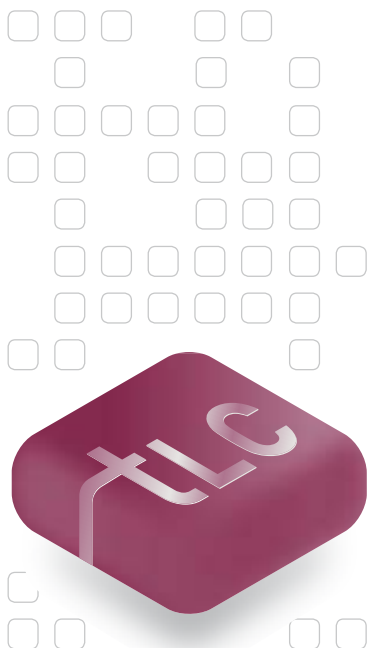
these capabilities with an easy-to-use, flexible and affordable log management and SIEM solution. You can install it within minutes and begin capturing log data and identifying events that threaten security.

### WHAT DISTINGUISHES TRIPWIRE LOG CENTER FROM OTHER SIEMs?

Tripwire Log Center differs from other SIEMs in many ways. Most notably is its ability as a Tripwire VIA solution to help you bring together the changes and events of interest that impact your security posture and affect your regulatory compliance. It also has other key differentiators that set it apart from other SIEMs.

#### » Centralized State-based Incident Detection.

As a Tripwire VIA solution, Tripwire Log Center joins forces with Tripwire Enterprise to provide visibility to your system configurations, their security posture and compliance status. Tripwire Log Center's log and security event management combines with Tripwire Enterprise's file integrity monitoring and compliance policy management to help you see the relationships between log activities and system changes. With this greater security context around events and changes of interest, you can better identify risk and prioritize your security efforts.



### » Simplified Security Intelligence

Tripwire Log Center lets you easily gain critical security intelligence. Its standards-based classification of log activity supports simple searches across platforms and devices that yield more comprehensive and accurate results. Use these valuable results for security forensic evidence or in compliance reports. Plus, easy-to-use, but advanced event correlation, dashboards and trending analysis give a quick, high-level view of your state of security. It also allows easy access to older forensic data because “active data” is not separated from “archived data.” This simplifies and reduces the cost of managing activity logs compared to the two-tiered data scheme that other log management solutions use.

### » An All-in-One Solution

Most SIEM products make you choose between strong log management and strong event management because these capabilities are typically offered as separate products or appliances. Tripwire Log Center was built from the ground up to include log and event management in single, integrated software solution that’s easy to use and deploy.

### » A Fit with Existing Workflow

Many enterprise organizations use additional systems to get real-time alerts on suspicious events. For example, they may have a SIEM in their Security Operations Center (SOC) or rely on a hosted SIEM. These systems often keep only a subset of the log data they collect and only for as long as needed. For this reason, organizations often require their compliance and operations departments to have a log management solution that serves as the trusted and primary collector of all logs.

Tripwire Log Center can pass raw log data and events to additional systems for further analysis and investigations. This allows compliance and operations departments to autonomously collect and analyze log data and also send logs to an enterprise-wide SIEM or GRC tool.

### » Flexibility for Convenience and Cost-savings

Tripwire Log Center offers its efficient log management capabilities as a software-based solution. That lets you deploy it on your own low-cost hardware, consistent with your organization’s standards. Because Tripwire Log Center software is modular, you 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.

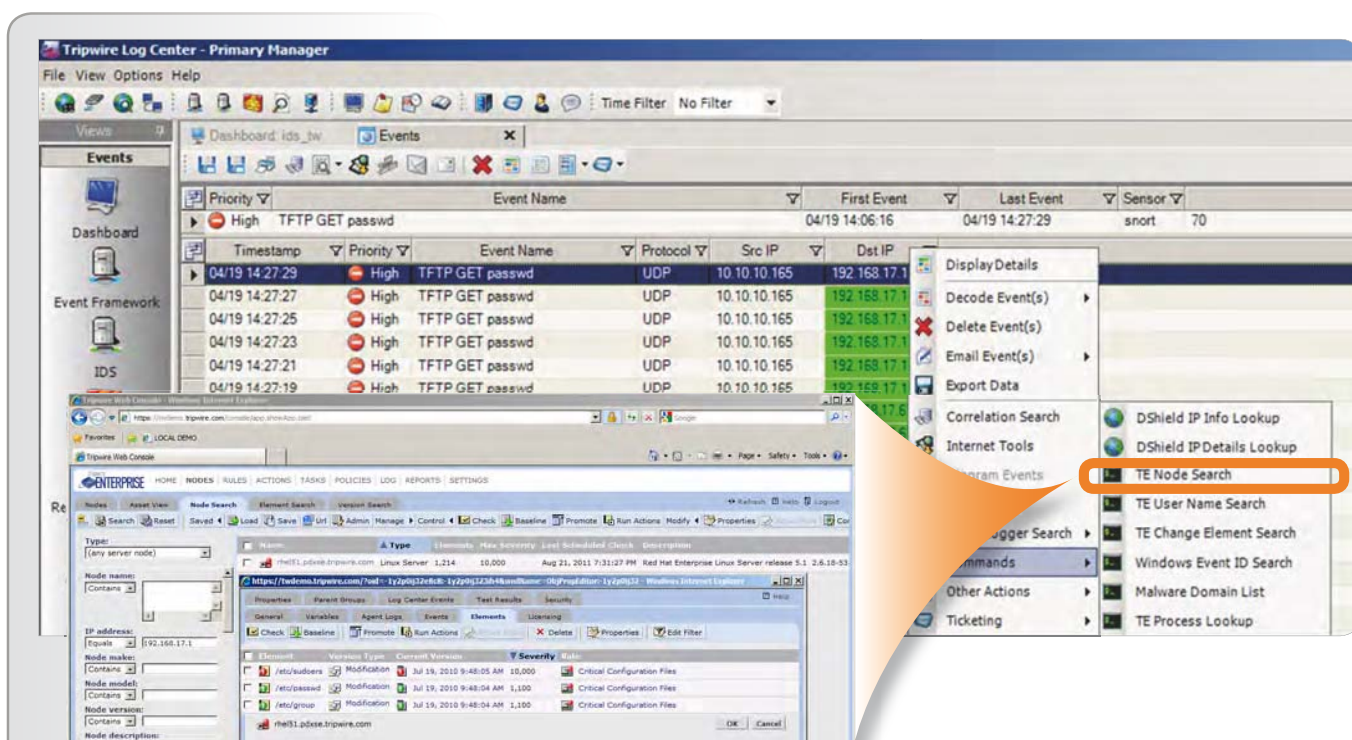


FIG. 1 Tight integration between Tripwire Log Center and Tripwire Enterprise automatically shows the relationship between an event of interest and an unexpected change to a critical file or impact policies.

# HOW CAN YOU USE TRIPWIRE LOG CENTER?

Organizations use Tripwire Log Center in several different ways. The most common use cases include detecting incidents or threats, generating evidence for security and compliance purposes, and adding risk and system state context by integrating it with Tripwire Enterprise.

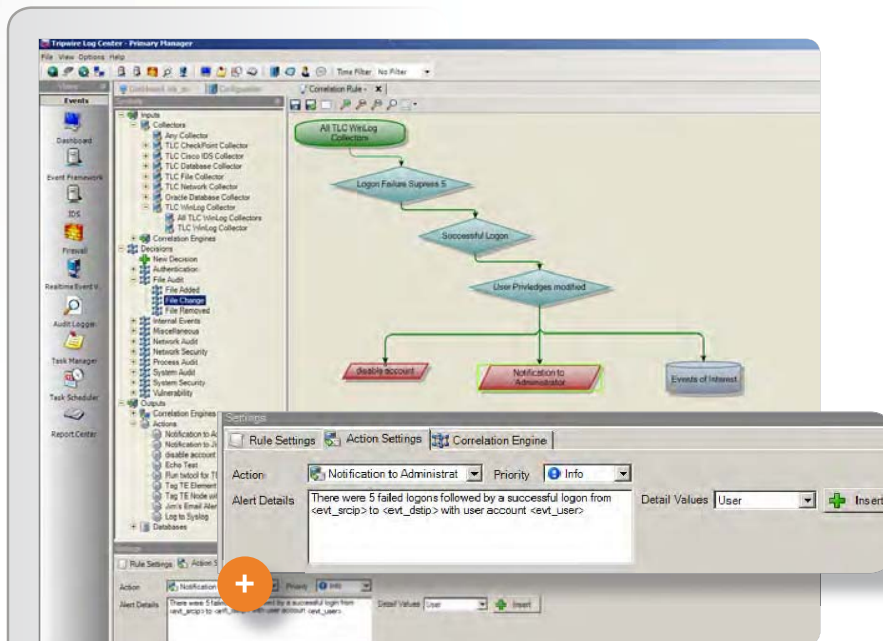


FIG. 2 Tripwire Log Center lets you define complex combinations of events by easily creating correlation rules with a graphical drag and drop rule creator.

## DETECT INCIDENTS AND THREATS

As a full SIEM, Tripwire Log Center supports incident and threat detection in several key ways. It lets you easily set up advanced correlation rules using drag and drop functionality to detect and alert on suspicious activity in real time.

You also see the security information you need at the required level of detail using flexible and customizable dashboards with drill-down capabilities. Use it to identify incidents with intelligent data visualization and trend analysis.

Plus, easily search across platforms and devices and obtain accurate and comprehensive results with standards-based classification of log messages. With Tripwire Log Center, you more quickly and easily see the events that threaten your organization most.



FIG. 3 Security dashboards and trending analysis views help you manage your security risks and dynamically drill down on areas requiring greater scrutiny.

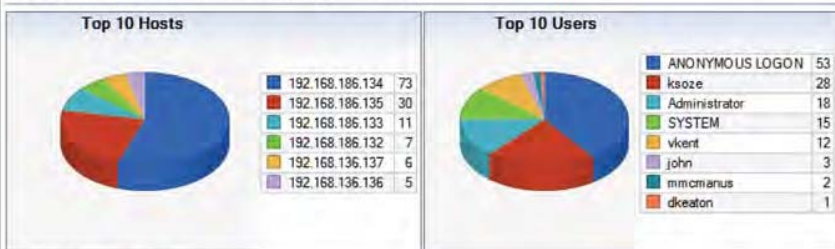


## PCI DSS v2.0 Requirement 10.2.1 User Overview Report

From: 2/19/2012 5:20:08 PM

To: 3/19/2012 5:20:08 PM

The following report provides an overview of the actions undertaken to be compliant with the Payment Card Industry Data Security Standard v2.0 Requirement 10.2.1 during the period of time listed above. This report displays an overview of successful user logon activity.



### Logon Events by User

Source IP	Destination IP	Logon	Logoff
<b>User Name : Administrator</b>			
127.0.0.1	192.168.186.134	2/24/2012 2:53:39 PM	2/24/2012 2:53:39 PM
127.0.0.1	192.168.186.134	2/28/2012 1:55:52 PM	2/28/2012 1:55:52 PM
127.0.0.1	192.168.186.134	3/16/2012 12:43:49 PM	3/16/2012 12:43:49 PM

FIG. 4 Tripwire Log Center helps quickly and efficiently prove compliance with out-of-the box reports

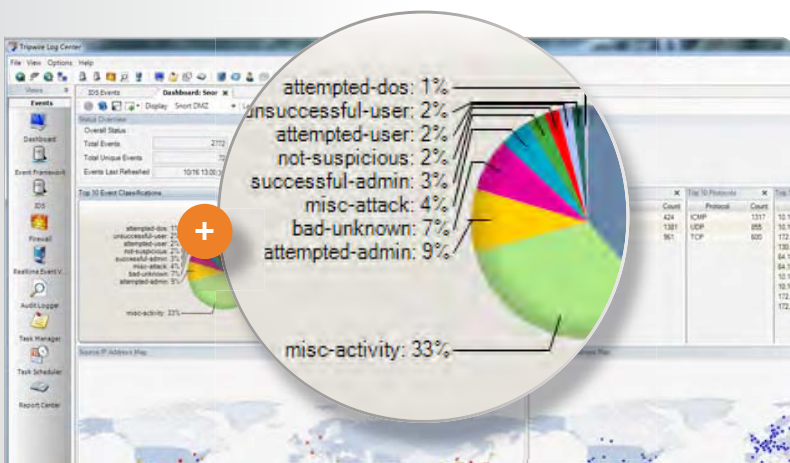


FIG. 5 Tripwire Log Center allows users to create customized dashboards.

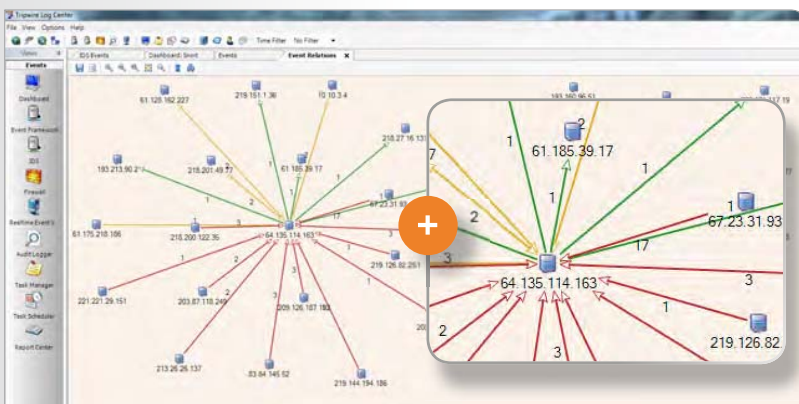


FIG. 6 Event relationship diagram displaying color-coded links between the nodes, showing the highest priority events that flowed over each link.

## GENERATE EVIDENCE FOR SECURITY AND COMPLIANCE

Tripwire Log Center provides everything you need to meet the log compliance requirements of most regulatory policies and industry standards, including the Payment Card Industry Data Security Standard (PCI DSS). It aggregates and archives all log sources—from network devices to servers, operating systems, applications, and more.

Tripwire Log Center also provides efficient access to raw log data for your own security forensic investigations. Plus, it lets you share that data with other SIEMs and GRC tools. That meets log compliance requirements and helps those systems better detect incidents by eliminating false positives.

With standards-based event classification, you more easily build complex, accurate reports based on cross-platform and -device queries. Efficient and tamper-proof log data storage further ensures the integrity of the data for forensic investigations.

## ADD RISK CONTEXT TO EVENTS BY INTEGRATING WITH TRIPWIRE ENTERPRISE

Tripwire Log Center helps reduce the noise of the volumes of log activity and events that organizations generate each day. As a Tripwire VIA solution, it lets you correlate events of interest with suspicious changes identified by Tripwire Enterprise, the gold standard solution for change data.

Tripwire Log Center further helps you identify and prioritize security risk by forwarding log and event data aggregated from additional security controls to other SIEMs or GRC solutions. For example, it can forward events from controls like intrusion-detection systems (IDS), file integrity monitoring (FIM) solutions, and security configuration management (SCM) solutions.

# TRIPWIRE LOG CENTER COMPONENTS

Tripwire Log Center offers its key capabilities through the Tripwire Log Center Manager. These capabilities include log management, event management and log concentration.

## LOG MANAGEMENT

Tripwire Log Center offers a complete log compliance solution that collects, retains and reports on log data from countless IT infrastructure devices. When it collects log data, it compresses, encrypts, and applies a checksum to the data to ensure its integrity. It then stores the data as a flat file.

With its fast indexing and standards-based event classification, each manager provides the ability to perform complex queries easily and accurately and to deliver full, cross-platform reports for compliance reporting and forensic analysis. Each manager also includes real-time, conditional alerting, so you know about suspicious activities immediately. You access all the features and functionality of a Tripwire Log Center Manager through a Log Center Console

## EVENT MANAGEMENT

Because Tripwire Log Center is an all-in-one log management and SIEM solution, you access the event management capabilities through the Log Center Console. This means that security analysts can search across archived logs or respond to a dashboard alert from a single management interface.

Tripwire Log Center's event management capabilities include an 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. It even supports deep forensic analysis of that information. Plus, the Tripwire Log Center Manager provides a security event ticketing system so you can prioritize responses to security events.

## SECONDARY LOG CENTER MANAGER

Sometimes you may wish to collect, store and forward log data from remote locations or distribute processing across multiple systems when you have high-volume sites. In both cases, you can deploy secondary managers to serve as log aggregators. In this role, secondary managers compress and encrypt the log data for highly efficient, secure transmission. You can upload data to a central, primary manager immediately, or schedule upload for times when network traffic is low.

When using log aggregators, you get the same real-time, conditional alerting that a centralized, primary manager offers. Plus, you can filter the stream of log data for events of interest and immediately transmit them to the event database—even if the manager doing the log concentration is holding the compressed log data for later transmission.



**FIG. 7** Tripwire Log Center collects activity logs from anywhere in the IT infrastructure, compressing, encrypting, indexing and storing them quickly into flat files. Plus, Tripwire Log Center's security event management capabilities helps reduce security risk by getting near real-time dashboard visibility to security events and correlating events of interest, alerts and vulnerability data.

## TRIPWIRE LOG CENTER FEATURES AND BENEFITS

FEATURE	BENEFIT
Intelligent Security Event Management	Provides state-based incident detection and better analysis by correlating change, event and vulnerability data. This provides visibility into the events that introduce security risk.
Security Dashboard and Event Views	Helps you better manage your security risks and dynamically drill down on areas requiring greater scrutiny through a centralized, customizable dashboard view of alerts, events and vulnerabilities.
Drag-and-Drop Correlation Rule Creator	Lets you define complex combinations of events that you need to be alerted on by easily creating and customizing correlation rules with a graphical, drag and drop rule creator.
Event Flow Visualization	Helps you pinpoint the parts of your IT infrastructure affected by a particular incident by automatically generating a graphical event relationship diagram. Shows how an attack entered and infiltrated the network by supporting replay of events.
Conditional Alerting	Delivers immediate notification of suspicious activity with real-time alerting based on complex sequences of events.
Compliance and Management Reports	Supports your compliance auditing or management needs with simple and customizable reports to visualize log and event information.
Device and Application Support	Offers comprehensive support for almost any device and application in your data center with pre-defined normalization rules for the devices and applications most organizations use.
Log and Event Management in One Solution	Reduces complexity, costs, training time and set-up time by offering log and event management capabilities in a single solution.
Accurate and Comprehensive Correlation Searches	Lets you easily perform sophisticated searches across all event data using standards-based event classification and provides accurate and comprehensive results. Use these results to meet your security forensics or compliance needs.
Event Collection	Provides for your event collection needs with a unique architecture that supports a sustained capture rate of tens of thousands of events per second (EPS).
Deep Forensic Analysis	Allows quick investigation of suspicious incidents and attacks, including their root cause, impact and ongoing effects. It does this with easy search capabilities that yield accurate, comprehensive results.
Security Event Ticketing System	Supports prioritizing and tracking incident response by letting you generate event tickets.
Affordable and Extensible Solution	Lets you pay only 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. Reduces costs by letting you install a software-only log and event management solution on your own hardware, sized for the log volume needed for each location.

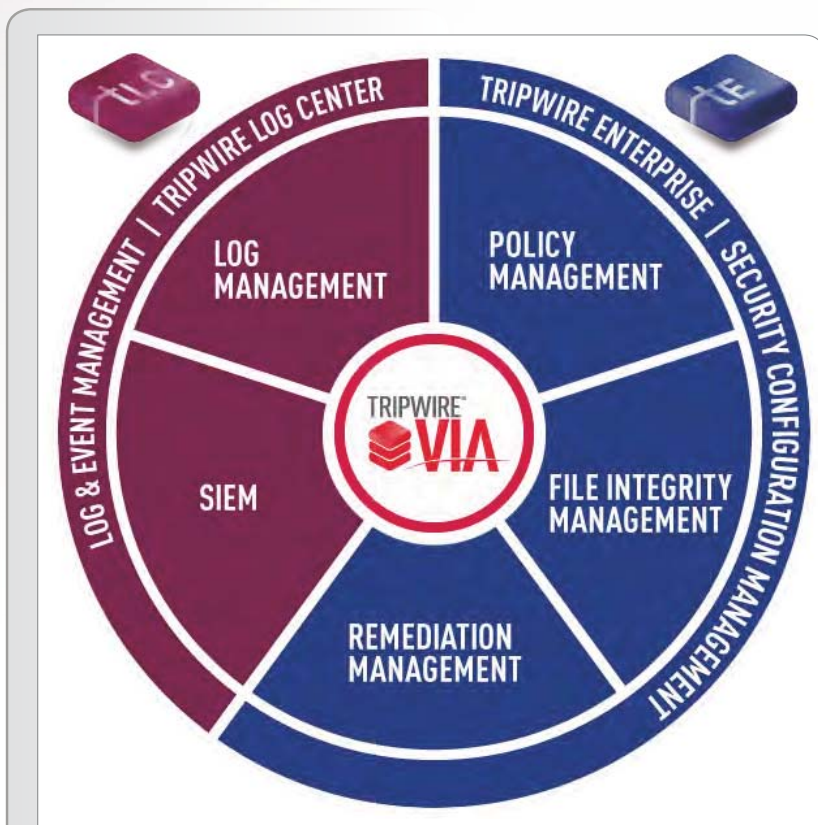


FIG. 8 Tripwire VIA solutions include Tripwire Log Center for log management and SIEM and Tripwire Enterprise for policy management, file integrity monitoring, and remediation management. With Tripwire VIA you can analyze all events of interest and important changes across your organization to get real-time visibility into all threatening activities.

### WANT TO LEARN MORE?

For more information on how Tripwire Log Center will benefit you, please visit [www.tripwire.com](http://www.tripwire.com) to download videos, white papers, and solution briefs, or to request a demo. You can also view a complete list of system requirements and supported devices and applications.

## High-performance Log and Event Management from Tripwire

Tripwire Log Center provides everything you need to meet your log management requirements through sophisticated log compliance and security event management in an integrated, easy-to-deploy solution. Combine Tripwire Log Center with Tripwire Enterprise to broaden compliance coverage and reduce security risk by increasing visibility, intelligence and automation.





✚ Tripwire is a leading global provider of IT security and compliance solutions for enterprises, government agencies and service providers who need to protect their sensitive data on critical infrastructure from breaches, vulnerabilities, and threats. Thousands of customers rely on Tripwire's critical security controls like security configuration management, file integrity monitoring, log and event management. The Tripwire® VIA™ platform of integrated controls provides unprecedented visibility and intelligence into business risk while automating complex and manual tasks, enabling organizations to better achieve continuous compliance, mitigate business risk and help ensure operational control. ✚

LEARN MORE AT [WWW.TRIPWIRE.COM](http://WWW.TRIPWIRE.COM) OR FOLLOW US @TRIPWIREINC ON TWITTER.