TRIPWIRE®
LOG CENTER

LOG INTELLIGENCE FOR SECURITY AND COMPLIANCE

◆ Given today's environment of sophisticated security threats, big data security intelligence solutions and regulatory compliance demands, the need for a *log intelligence* solution has become clear. ◆

As the number and sophistication of increasingly targeted cyber attacks continue to increase, organizations must sift through a deluge of log and event data to detect the signs of unauthorized activity. Organizations have taken two different approaches to examining this data with their SIEM solutions, but neither approach seems to have made any real improvements to security.

Many attempt to push all log and event data, plus all context metadata and even network traffic analysis, to a single SIEM solution, inundating it with useless data. Even if the SIEM could process the volume of data it receives, security teams often lack the resources or knowledge to build the complex chains of correlation rules that are required to filter out the noise and find relevant events.

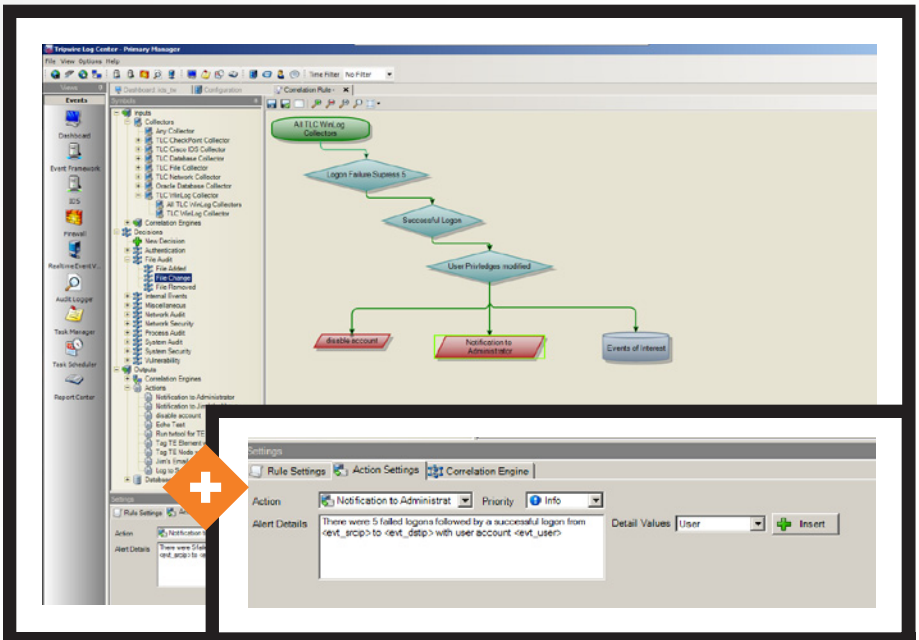
Yet others rely on log management products to collect, store, and forward device logs to the SIEM. Again, most of this data is also irrelevant, and the SIEM spends most of its processing capabilities examining the data to reach this conclusion.

Most organizations use log management solutions to meet regulatory requirements for log collection, retention and reporting. However, users traditionally send the logs through their SIEM to automate meeting the common regulatory requirement of reviewing those logs for specific types of activity. Yet even after investing in the necessary hardware, licensing, and development of correlation rules to process that data, many organizations lack confidence that the log management solution collected those logs completely, reliably and securely.

THE NEED FOR LOG INTELLIGENCE

Given today's environment of complex security threats, big data security intelligence solutions and regulatory compliance demands, the need for a log intelligence solution has emerged. This solution would:

- Offload much of the high-speed analysis and filtering of log and event data from the over-burdened and failing SIEMs of yesterday or the emerging and costly new security intelligence solutions to provide real-time, early breach detection.
- Give organizations confidence that they have met the basic log management requirements mandated in regulatory policies for complete, secure and reliable log collection.
- Improve security by leveraging the context of foundational security controls such as file integrity monitoring, vulnerability management and security configuration management.

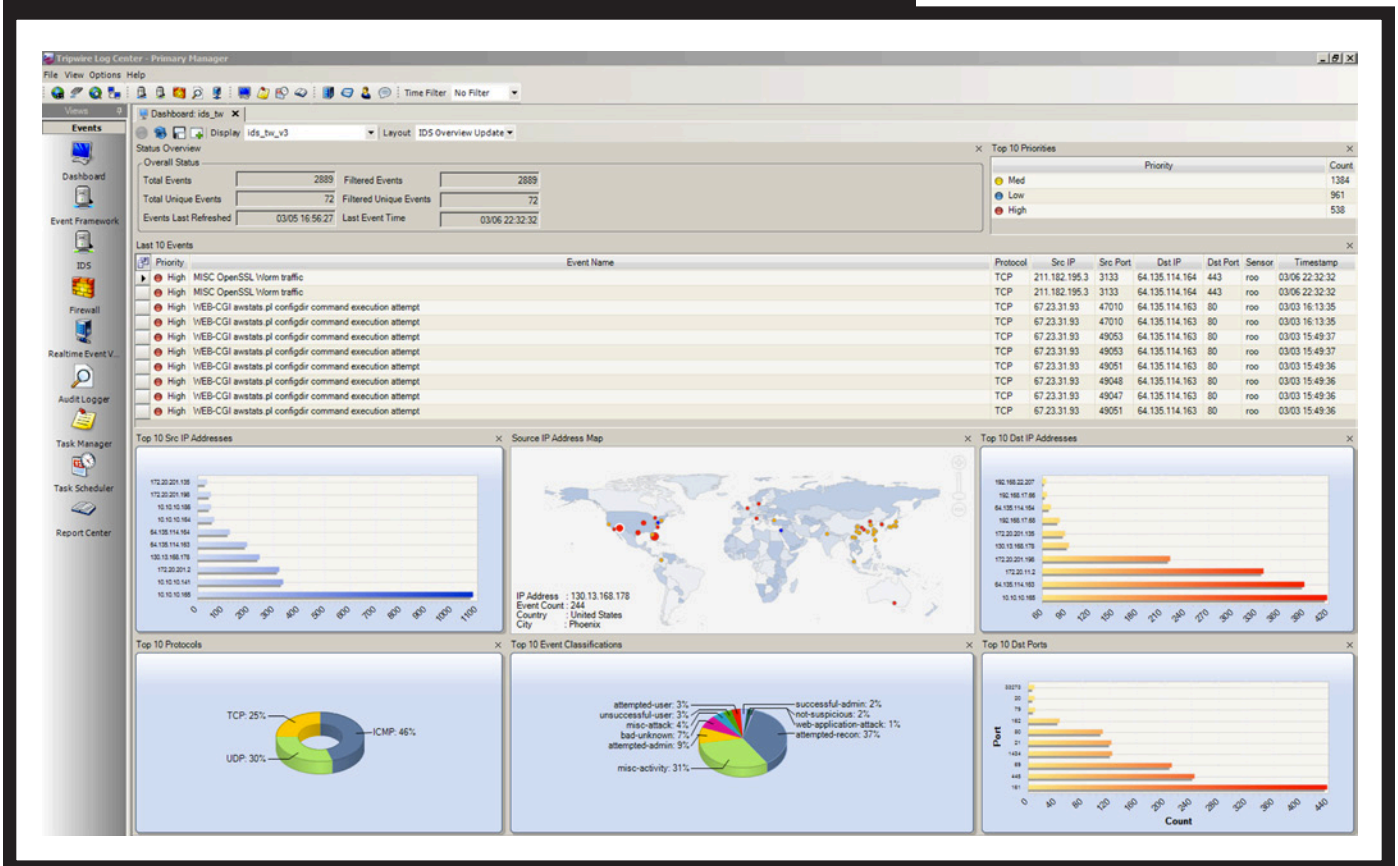


◆ **FIG. 1** *Tripwire Log Center lets you define complex combinations of events by easily creating correlation rules with a graphical drag and drop rule creator.*

» Prioritize security efforts based on the importance of an asset and the type of user associated with suspicious behaviors by incorporating both business and user context and information from other integrated security controls.

WHAT DISTINGUISHES TRIPWIRE LOG CENTER?

As a log intelligence solution, Tripwire Log Center offers a true alternative to how organizations have traditionally (and often unsuccessfully) attempted to meet their needs for early breach detection and compliance requirements for complete, secure and reliable log collection and automated log review. Here's what sets Tripwire Log Center apart from other solutions:



◆ **FIG. 2** *Security dashboards and trending analysis views help you manage your security risks and dynamically drill down on areas requiring greater scrutiny.*

» **Early Breach Detection.** As a Tripwire solution, Tripwire Log Center can join forces with Tripwire Enterprise and Tripwire IP360 to effectively identify and address suspicious activity on your high-value assets. Tripwire Enterprise analyzes and hardens system configurations, detects all system changes, shows which changes threaten security, and provides complete details about those changes. Tripwire IP360 determines if a device has any vulnerabilities (like an out-of-date patch), enabling you to react accordingly.

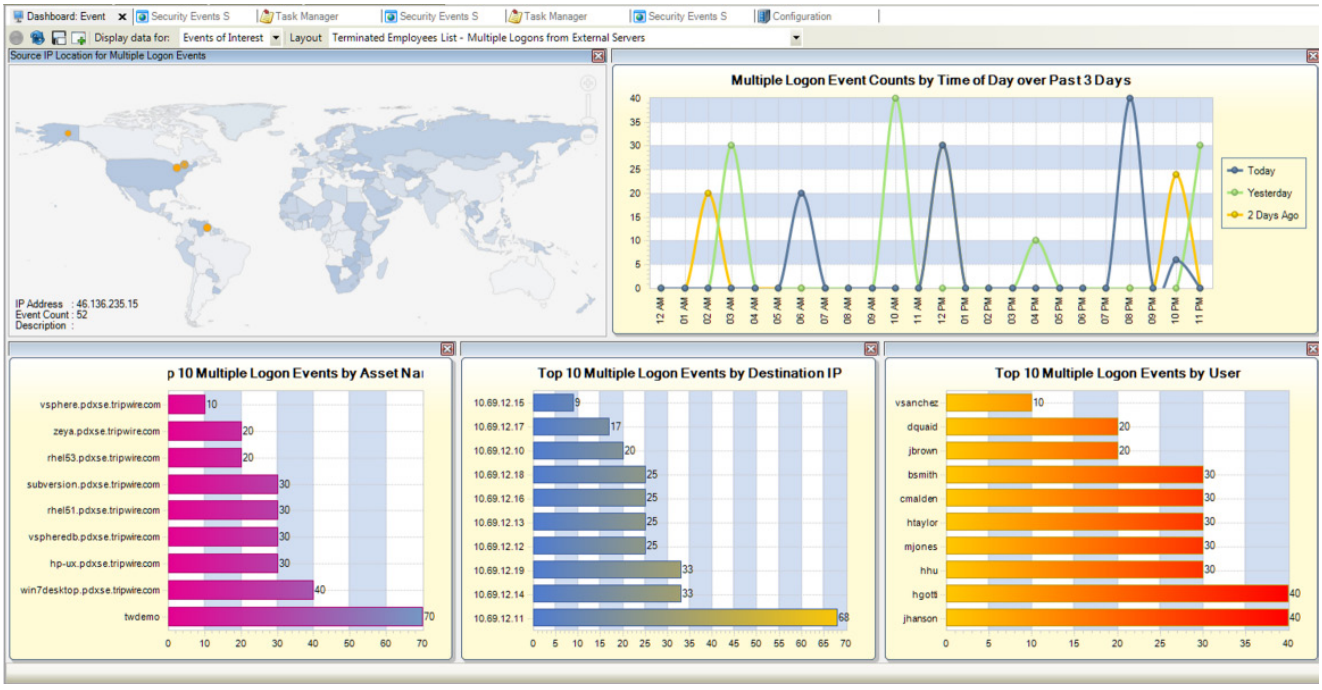
By adding Tripwire Log Center's log and security intelligence to these industry leading security solutions, you see the relationships between suspicious events, system changes, weak configurations and current vulnerabilities. That rich combination of information lets you better identify risk and prioritize your security efforts. For those using the SANS Top 20 as a security framework, Tripwire lets you protect critical infrastructure by correlating data and providing context from the first 4 controls.

» **Log Intelligence.** Tripwire Log Center satisfies multiple needs, helping reduce the workload and associated cost of SIEMs and security intelligence solutions by pre-filtering data and identifying anomalies and patterns known to be early indicators of breaches. This allows it to capture and store everything, but forward only actionable, relevant data to SOC staff and SIEMs, or newer security intelligence solution. It does all this while providing all the capabilities needed to meet the log management requirements included in most regulatory policies.

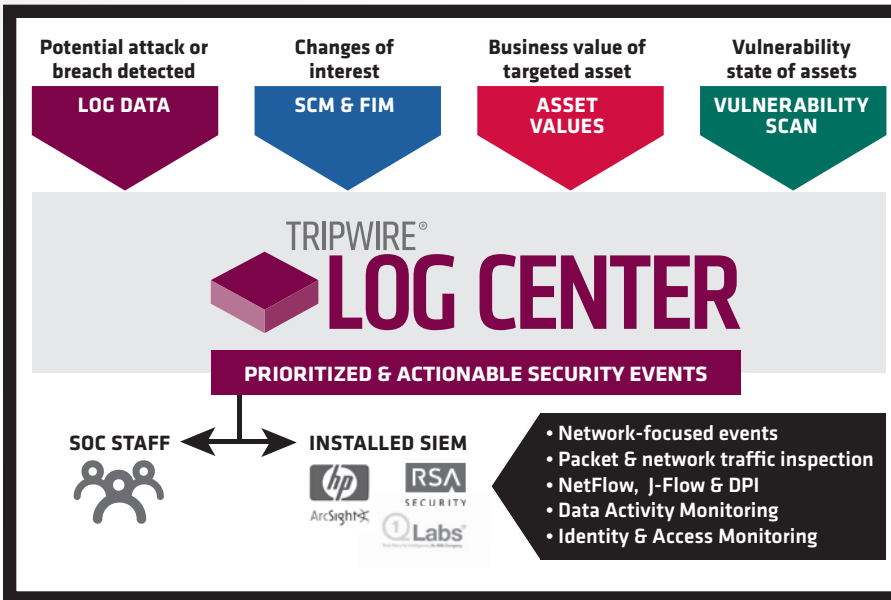
» **Complete, Reliable Log Collection.** Tripwire Log Center ensures that organizations meet regulatory requirements around complete, secure and reliable log collection. The agent used to collect and forward log data ensures that if a system, device or other asset goes down, you have 100 percent certainty that you've got all the data—even if an asset goes down. And we provide high levels of compression to reduce storage demands, while protecting those logs from alteration.

In addition, our Hyperlogging capability ensures that when logging gets turned off, whether accidentally or to cover the tracks of an attack, it immediately and automatically gets turned back on. With Tripwire Log Center, you don't have to purchase third party solutions to be confident that you've captured all of your log data.

» **Simplified Security Intelligence.** Tripwire Log Center makes it easy to gain critical security intelligence. Its



◆ **FIG. 3** *Obtain leading indicators of breach activity by adding business and user context to your incident detection efforts*



◆ **FIG. 4** *Tripwire Log Center provides secure and reliable log capture, sophisticated log analytics through its integration with other foundational security controls and lower cost of deployment of your existing SIEM.*

standards-based classification of log and event 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.

Tripwire Log Center also provides a drag-and-drop interface that lets you quickly and easily define correlation rules made up of complex combinations of events. When logs meet those rules, Tripwire Log Center flags them for quick review. This reduces the need for expertise and hard to come by resources to pare down log data to what is essential for review. Plus, you get an at-a-glance, high-level view of your state of security with the solution's advanced event correlation, dashboards and trending analysis.

With Tripwire Log Center, you can more easily access older forensic data because "active data" is not separated from "archived data." As a result, managing activity logs is easier and costs less compared to using the two-tiered data scheme of log management solutions. In comparison with security intelligence solutions that only hold onto and let you see a subset of log data for a small time period, Tripwire Log Center lets you see all your log data, no matter what time period you need to examine.

» **Business and User Context.** Tags from the Asset View in Tripwire Enterprise can be used to categorize your assets by business context. This lets you identify assets in ways such as those most critical to your business. In addition, Tripwire Log Center integrates with Active Directory, which the majority of organizations use to monitor user access. Because of this integration, you can monitor specific users and user groups based on user attributes like entitlements, groups, and roles.

Combining business and user context lets you more easily monitor assets and users that together may warrant a closer watch—for example, your highest value assets to which contractors have access. Further prioritize risk by correlating suspicious events from Tripwire Log Center with threatening changes detected by Tripwire Enterprise and vulnerabilities identified by Tripwire IP360.

» **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 security intelligence solution or SIEM in their Security Operations Center (SOC) or rely on a hosted solution. 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 provides a secure and reliable way to capture logs, and can pass raw log data, but can also pass only the actionable event data to additional systems for further analysis and investigations. This allows compliance and operations departments to autonomously collect and analyze log data and also send pre-processed logs to an enterprise-wide security intelligence solution or GRC tool. Plus, with its Active Directory integration, Tripwire Log Center seamlessly gathers user entitlement, groups, roles and other attributes that already exist in

your Active Directory environment to help you more accurately detect suspicious activities.

HOW CAN YOU USE TRIPWIRE LOG CENTER?

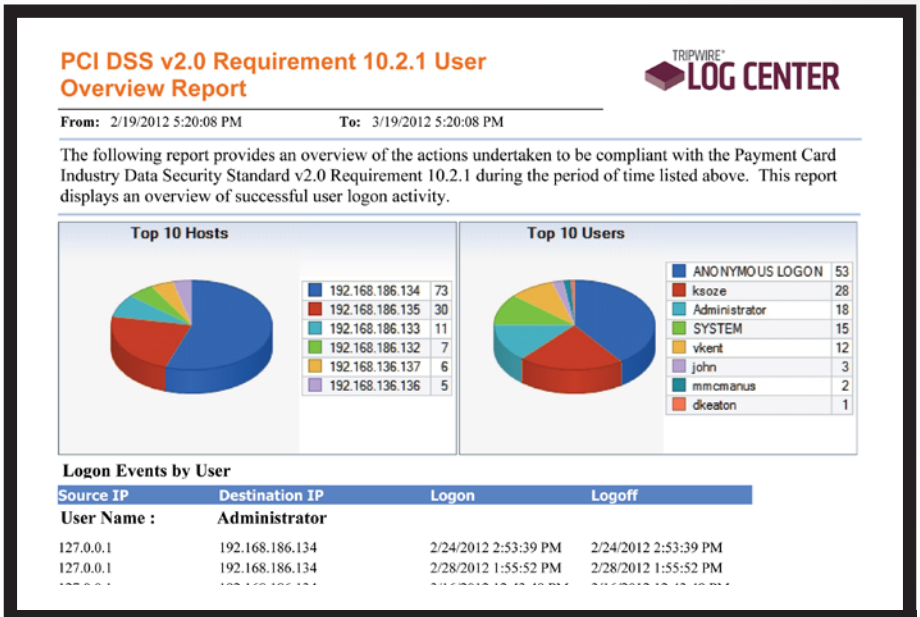
Because of Tripwire Log Center's log intelligence and flexibility in integrating with other solutions, it can be used in a variety of ways.

DETECT INCIDENTS AND THREATS SOONER

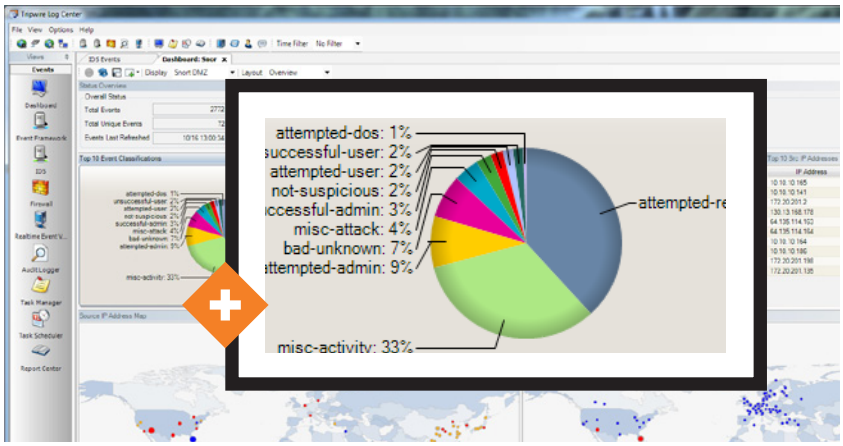
Tripwire Log Center supports early threat detection in several key ways. It collects data from devices, servers, applications and automated security processes and forwards only the actionable, relevant data to the security intelligence solution or security teams. That not only improves security, but also reduces the costs of processing that data with a security intelligence solution. You easily set up advanced correlation rules that review this data to detect and alert on suspicious activity around your high-value assets.

When used with Tripwire Enterprise, Tripwire Log Center lets you even create rules that detect and alert on suspicious events related to changes that affect the security and compliance state of your systems. And the integration provides an additional layer of business and user context. Further, when used with IP360, you add vulnerability data to this context.

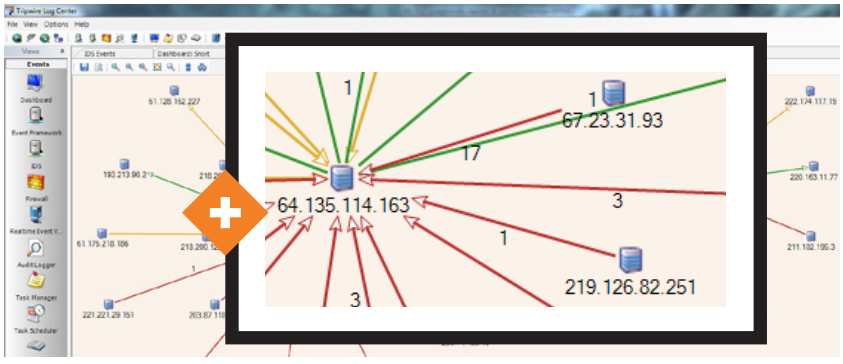
You also see security information at the detail you need with flexible and customizable dashboards that have drill-down capabilities. Use it to identify incidents with intelligent data visualization and trend analysis. Easily search across platforms and devices and obtain accurate and comprehensive results with standards-based classification of log messages and events.



◆ **FIG. 5** *With out-of-the box reports, Tripwire Log Center helps quickly and efficiently prove compliance.*



◆ **FIG. 6** *Tripwire Log Center allows users to create customized dashboards.*



◆ **FIG. 7** *Event relationship diagram displaying color-coded links between the nodes, showing the highest priority events that flowed over each link.*

With Tripwire Log Center, you more quickly and easily see the events that threaten your organization most.

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 a pre-defined set of report templates that automatically provide the evidence they require. It aggregates and archives all log sources—from network devices to servers, operating systems, applications, and more.

It also provides efficient access to raw log data for your own security investigations and 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.

GAIN SYSTEM STATE INTELLIGENCE

Integrating Tripwire Log Center with Tripwire Enterprise and Tripwire IP360 arms you with valuable security and business context around activity on your systems so you can prioritize and address the threats that matter most.

For example, monitor, detect and alert upon anomalous activity occurring around your highest value assets. Do this by using Tripwire Enterprise Asset view to tag and classify assets based on criteria such as their criticality, risk, business impact, geographic locations and departments. Then filter the highest value assets based on their tags and use that information when building correlation rules in Tripwire Log Center. Further prioritize these threats by examining suspicious activity based on user entitlement with the Active Directory integration or by using IP360 to determine which targeted assets are vulnerable due to out-of-date patches.

By prioritizing threats according to who they're associated with, their impact on your most critical assets, and how vulnerable they are, you can quickly execute the most effective response.

COLLECT LOGS RELIABLY AND SECURELY

One of the biggest challenges organizations face when meeting compliance or trying to determine root cause of an attack is the possibility that the required data has been lost, or was never collected. Concerns over data loss often compel organizations to purchase additional software solutions that help ensure all data gets captured. In addition, many systems get overwhelmed by the amount of data they need to capture and manage.

Tripwire Log Center's advanced log collector collects all of your logs in a secure, reliable way, eliminating the need to purchase third party software. Plus Tripwire's Hyperlogging capability ensures that even when attackers attempt to cover their tracks by turning off logging on the systems they attack, it's automatically turned back on before any data gets lost. For compliance purposes, this is a must.

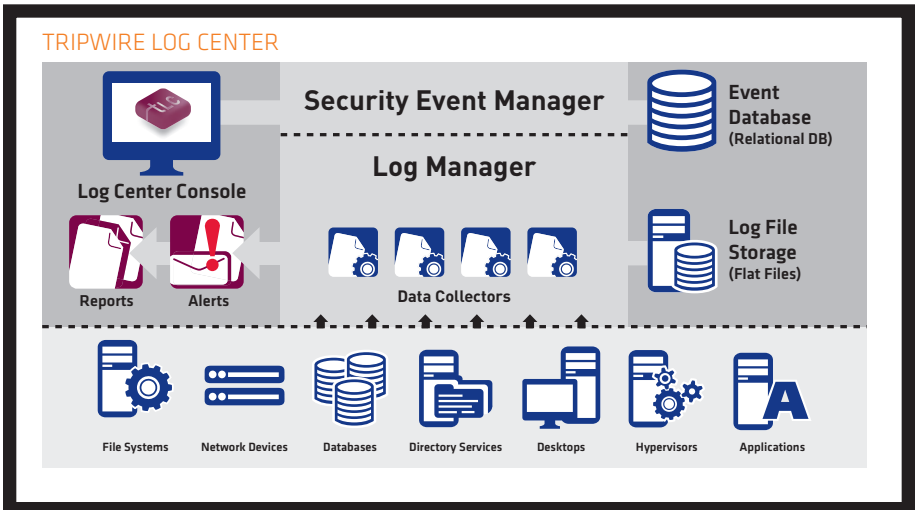


FIG. 8 *Tripwire Log Center collects activity logs from anywhere in the IT infrastructure, compressing, encrypting, indexing and storing them quickly into flat files. Plus, Tripwire Log Center reduces security risk by providing near real-time dashboard visibility to security events and correlating events of interest, alerts and vulnerability data.*

TRIPWIRE LOG CENTER FEATURES AND BENEFITS

FEATURE	BENEFIT
Log Intelligence	Through integrated Tripwire solutions, combines details of suspicious events with both in-depth knowledge of system state from Tripwire Enterprise and known vulnerabilities from Tripwire IP360 to deliver system state intelligence. That lets you better prioritize security threats based on the real risks they pose to your essential business functions. Provides state-based incident detection and better analysis by correlating change, event and vulnerability data through the integrated solutions. This provides greater visibility into possible security events..
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.
Business Context	Lets you identify suspicious activity based on the criticality, risk and business impact of your most valued assets by leveraging Asset View tags in Tripwire Enterprise.
User Context	Integrates with Active Directory to provide the context of user entitlement, groups, roles and other attributes that already exist in your Active Directory environment so that you can more accurately detect suspicious activities.
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.
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 for security investigations or to meet your compliance needs.
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.
Advanced Log Collector and Event Collection	Provides for your event collection needs with an advanced log collector that reliably and securely collects and forwards log data. Uses a unique architecture that supports a sustained capture rate of tens of thousands of events per second (EPS).
Security Event Ticketing System	Supports prioritizing and tracking incident response by letting you generate event tickets.

Tripwire is a leading global provider of risk-based security and compliance management solutions that enable organizations to effectively connect security to the business. Tripwire delivers foundational security controls like security configuration management, file integrity monitoring, log and event management, vulnerability management, and security business intelligence with performance reporting and visualization.

LEARN MORE AT WWW.TRIPWIRE.COM OR FOLLOW US @TRIPWIREINC ON TWITTER.

TLCPB701r 201307