DATASHEET

Tripwire Enterprise & Tripwire LogCenter

Integrated for Unparalleled Cyberthreat Detection

The Tripwire Enterprise and Tripwire LogCenter integration provides unparalleled enterprise threat intelligence, giving rich context around changes and security events in your environment, right out of the box.

Tripwire provides out-of-the-box integration of Tripwire® Enterprise, a security configuration management solution, and Tripwire LogCenter®, a complete log management and SIEM solution. By joining these solutions, you can automatically correlate changes detected in Tripwire Enterprise with log and event data captured by Tripwire LogCenter.

Combined, they grant immediate visibility to file and configuration changes, along with information about the context in which those changes were made. This added risk context helps security professionals prioritize changes based on risk to the business.

By joining forces, Tripwire Enterprise and Tripwire LogCenter offer visible, actionable intelligence with several out-of-the-box, real-time integration points:

Change/Event Correlation Provides Change and Risk Context

Any SIEM can detect a security event. It's far more powerful when a SIEM can show you that there's a relationship between an event and an unexpected change to a critical file or setting. This reduces false positives and focuses your incident detection efforts on the events that actually matter.

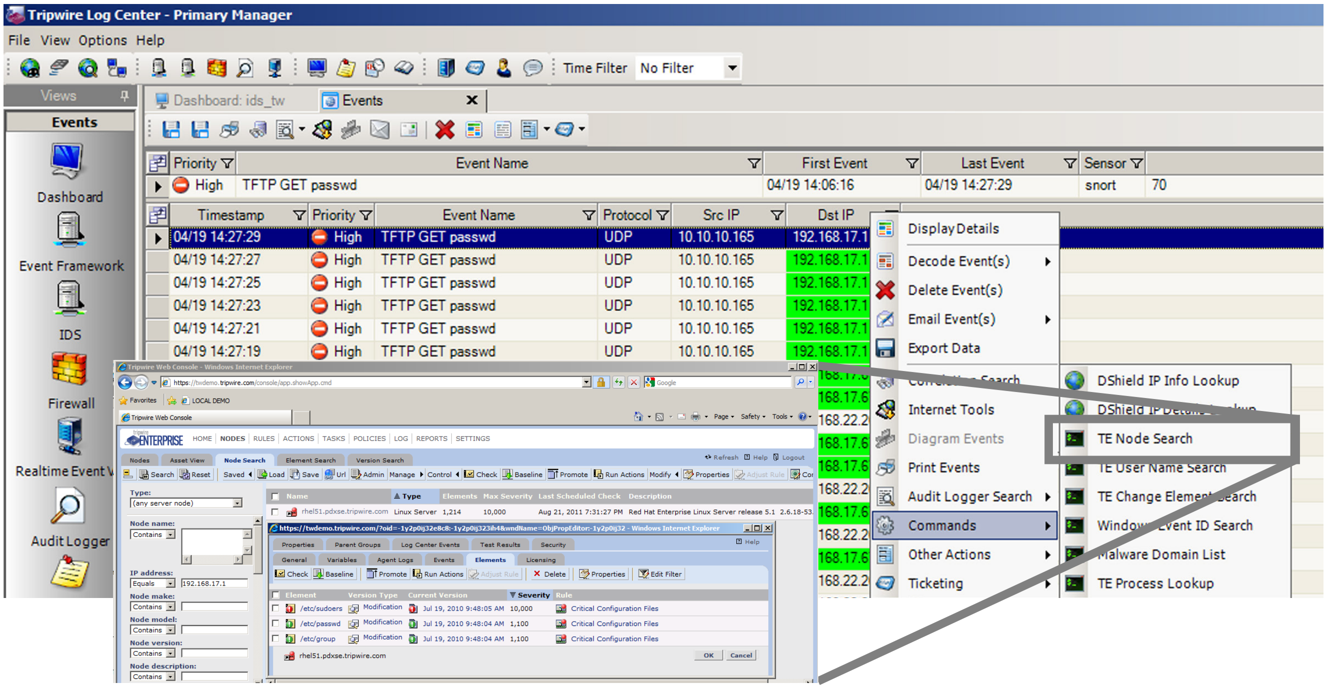
The out-of-the-box integration between Tripwire Enterprise and Tripwire LogCenter automatically correlates changes that impact policies with events detected by Tripwire LogCenter. By providing this real-time visibility into changes and their context through consoles and dashboards, it's far easier to identify impending threats.

Bi-Directional Context Enables Forensic Discovery and Investigation

Quickly find vulnerabilities, respond to attacks and recover from breaches. The integration between Tripwire Enterprise and Tripwire LogCenter provides contextual controls that give you unprecedented levels of visibility and intelligence. For example, in Tripwire Enterprise you can investigate suspicious activity on a server, device or other IT asset by seeing related security events from Tripwire LogCenter—all without leaving the console you work from most. Similarly, from Tripwire LogCenter you can view the Tripwire Enterprise asset associated with an event of interest to inspect potentially related changes detected on that asset.

Global Event Search Reveals Trends and Threats

Save time by obtaining more accurate and comprehensive results from your queries. Identify unexpected threat patterns faster. In Tripwire Enterprise you can now execute standards-based queries against log and event information captured by Tripwire LogCenter. This can provide hard evidence of a threat to back up a gut suspicion. It can also reveal an anomaly that may indicate the seeds


Tripwire Log Center - Primary Manager
File View Options Help
Time Filter No Filter
Views
Events
Dashboard
Event Framework
IDS
Firewall
Realtime Event V
Audit Logger
Dashboard: ids_tw
Events
Display Details
Decode Event(s)
Delete Event(s)
Email Event(s)
Export Data
Correlation Search
Internet Tools
Diagram Events
Print Events
Audit Logger Search
Commands
Other Actions
Ticketing
DShield IP Info Lookup
DShield IP Details Lookup
TE Node Search
TE User Name Search
TE Change Element Search
Windows Event ID Search
Malware Domain List
TE Process Lookup
Tripwire Web Console - Windows Internet Explorer
https://twdemo.tripwire.com/console/app.showApp.cmd
Google
Favorites
LOCAL DEMO
Tripwire Web Console
Page Safety Tools
tripwire ENTERPRISE
HOME NODES RULES ACTIONS TASKS POLICIES LOG REPORTS SETTINGS
Nodes Asset View Node Search Element Search Version Search
Refresh Help Logout
Search Reset Saved Load Save Url Admin Manage Control Check Baseline Promote Run Actions Modify Properties Adjust Rule
https://twdemo.tripwire.com/?oid=-1y2p0ij32e8c8:-1y2p0ij323ih4&wndName=ObjPropEditor:-1y2p0ij32 - Windows Internet Explorer
Properties Parent Groups Log Center Events Test Results Security
General Variables Agent Logs Events Elements Licensing
Help
Check Baseline Promote Run Actions Adjust Rule Delete Properties Edit Filter
OK Cancel

Priority	Event Name	First Event	Last Event	Sensor	
High	TFTP GET passwd	04/19 14:06:16	04/19 14:27:29	snort	70

Timestamp	Priority	Event Name	Protocol	Src IP	Dst IP
04/19 14:27:29	High	TFTP GET passwd	UDP	10.10.10.165	192.168.17.1
04/19 14:27:27	High	TFTP GET passwd	UDP	10.10.10.165	192.168.17.1
04/19 14:27:25	High	TFTP GET passwd	UDP	10.10.10.165	192.168.17.1
04/19 14:27:23	High	TFTP GET passwd	UDP	10.10.10.165	192.168.17.1
04/19 14:27:21	High	TFTP GET passwd	UDP	10.10.10.165	192.168.17.1
04/19 14:27:19	High	TFTP GET passwd	UDP	10.10.10.165	192.168.17.1

Type: (any server node)
Node name: Contains
IP address: Equals 192.168.17.1
Node make: Contains
Node model: Contains
Node version: Contains
Node description: Contains

Name	Type	Elements	Max Severity	Last Scheduled Check	Description
rhel51.pdxse.tripwire.com	Linux Server	1,214	10,000	Aug 21, 2011 7:31:27 PM	Red Hat Enterprise Linux Server release 5.1 2.6.18-53.

Element	Version Type	Current Version	Severity	Rule
/etc/sudoers	Modification	Jul 19, 2010 9:48:05 AM	10,000	Critical Configuration Files
/etc/passwd	Modification	Jul 19, 2010 9:48:04 AM	1,100	Critical Configuration Files
/etc/group	Modification	Jul 19, 2010 9:48:04 AM	1,100	Critical Configuration Files

rhel51.pdxse.tripwire.com

Fig. 1 Tight integration between Tripwire LogCenter and Tripwire Enterprise automatically shows the relationship between an event of interest and an unexpected change to a critical file or that impacts policies.

of a coordinated attack. For example, you can query for all files changed by a specific user or for "portmap scanning" messages that can reveal an external threat.

Tripwire LogCenter "Event Widget" Displays Real-Time Information

Save time finding security incidents and out-of-compliance status. A Tripwire LogCenter event widget can now be placed in Tripwire Enterprise dashboards (Fig. 1) to provide real-time event information from Tripwire LogCenter for monitored servers, applications and devices. Status updates to these events are made in Tripwire Enterprise and then updated in Tripwire LogCenter upon synchronization.

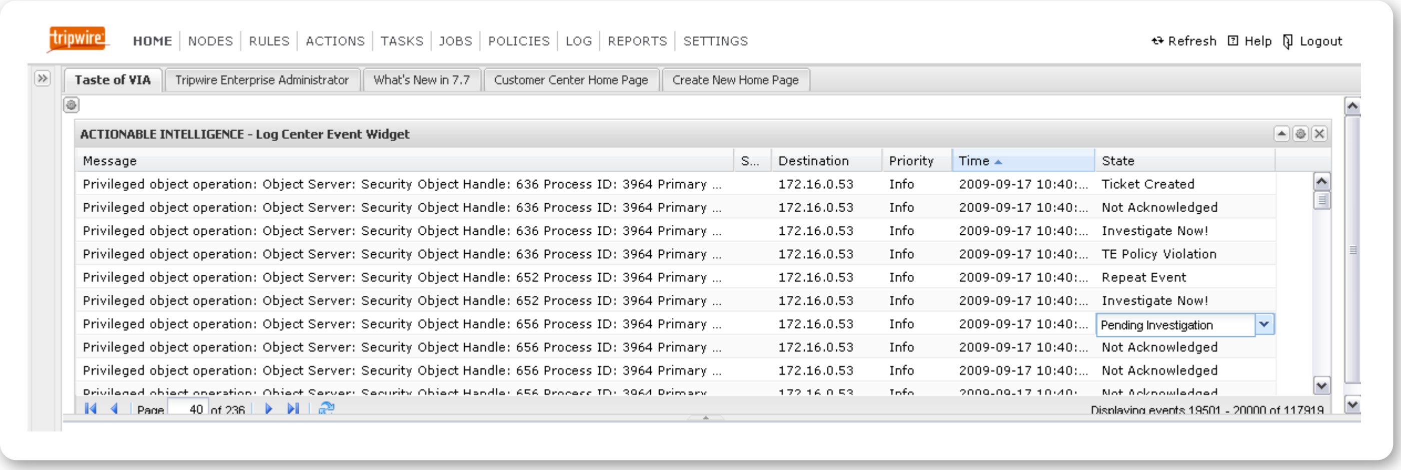
Plus, Tripwire Enterprise and Tripwire LogCenter continue monitoring the infrastructure to protect critical files and systems, detect incidents at the speed of change, and remediate issues before damage is done.

The Tripwire Enterprise and Tripwire LogCenter Integration in Action

Tripwire Enterprise indicates that a file share's configuration settings have been changed to allow anyone to access critical data anonymously. Whenever someone accesses this file share, Tripwire LogCenter sends you an alert. Clearly there's a problem. To fix the problem, you return the configuration to its previously known and trusted state using automated remediation in Tripwire Enterprise. In this case, it fixes the configuration setting so that it prohibits guests and unauthorized users from accessing the files. and requires each user to authenticate to view the material. The next time an unauthorized user or perpetrator tries to login to the system, access is denied. Problem solved.

Hyperlogging Rapidly Re-Enables Critical Logs That Have Been Disabled

Reduce the risk associated with gaps in logging coverage and satisfy requirements for logging continuity. Hyperlogging rapidly and automatically re-enables logging of critical logs that have been disabled—an action hackers or malicious insiders often take to cover their tracks. Tripwire Enterprise detects when logging systems in Tripwire LogCenter have been disabled and immediately re-enables them. It also provides reports to auditors and real-time alerts of compliance violations.



ACTIONABLE INTELLIGENCE - Log Center Event Widget

Message	S...	Destination	Priority	Time	State
Privileged object operation: Object Server: Security Object Handle: 636 Process ID: 3964 Primary ...		172.16.0.53	Info	2009-09-17 10:40:...	Ticket Created
Privileged object operation: Object Server: Security Object Handle: 636 Process ID: 3964 Primary ...		172.16.0.53	Info	2009-09-17 10:40:...	Not Acknowledged
Privileged object operation: Object Server: Security Object Handle: 636 Process ID: 3964 Primary ...		172.16.0.53	Info	2009-09-17 10:40:...	Investigate Now!
Privileged object operation: Object Server: Security Object Handle: 636 Process ID: 3964 Primary ...		172.16.0.53	Info	2009-09-17 10:40:...	TE Policy Violation
Privileged object operation: Object Server: Security Object Handle: 652 Process ID: 3964 Primary ...		172.16.0.53	Info	2009-09-17 10:40:...	Repeat Event
Privileged object operation: Object Server: Security Object Handle: 652 Process ID: 3964 Primary ...		172.16.0.53	Info	2009-09-17 10:40:...	Investigate Now!
Privileged object operation: Object Server: Security Object Handle: 656 Process ID: 3964 Primary ...		172.16.0.53	Info	2009-09-17 10:40:...	Pending Investigation
Privileged object operation: Object Server: Security Object Handle: 656 Process ID: 3964 Primary ...		172.16.0.53	Info	2009-09-17 10:40:...	Not Acknowledged
Privileged object operation: Object Server: Security Object Handle: 656 Process ID: 3964 Primary ...		172.16.0.53	Info	2009-09-17 10:40:...	Not Acknowledged
Privileged object operation: Object Server: Security Object Handle: 656 Process ID: 3964 Primary		172.16.0.53	Info	2009-09-17 10:40:	Not Acknowledged

Page 40 of 236

Displaying events 19501 - 20000 of 117919

Fig. 2 The integration of Tripwire Enterprise and Tripwire LogCenter lets you correlate detailed system configuration state and change data with log and event data.

Tripwire Enterprise Agents Deliver Instant Log Data

Enable deep logging on different systems without difficult, manual efforts. The integration helps you meet this longstanding log management need much more easily. Take advantage of Tripwire Enterprise agents that are already deployed to immediately send detailed system state, change and configuration information to Tripwire LogCenter. If you're an existing Tripwire Enterprise user, you can obtain this instant logging capability with a simple console upgrade if your deployed agents are version 7.5 or higher.

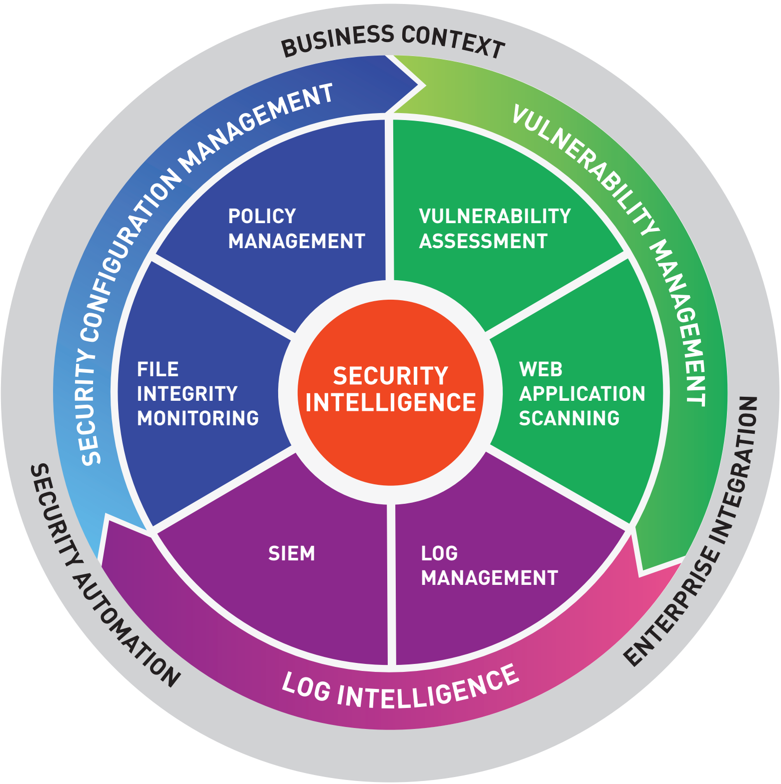


Fig. 3 Tripwire solutions include Tripwire LogCenter for log and event management, Tripwire Enterprise for security configuration management and Tripwire IP360™ for vulnerability management. With Tripwire you gain system state intelligence that lets you prioritize risk and protect your high value, mission-critical assets.

Tripwire is the trusted leader for establishing a strong cybersecurity foundation. We protect the world's leading organizations against the most damaging cyberattacks, keeping pace with rapidly changing tech complexities to defend against ever-evolving threats for more than 20 years. On-site and in the cloud, our diverse portfolio of solutions find, monitor and mitigate risks to organizations' digital infrastructure—all without disrupting day-to-day operations or productivity. Think of us as the invisible line that keeps systems safe. **Learn more at tripwire.com**

***The State of Security*: News, trends and insights at tripwire.com/blog**
Connect with us on LinkedIn, Twitter and Facebook