Tripwire Event Sender

Enrich Your SIEM with Compliance, Scoring and Change Data

Organizations have continually found new ways to unlock the value of Tripwire Enterprise, adding additional leverage to a valuable strategic business solution. And now you can extend Tripwire Enterprise to achieve better, faster and more cost effective cyberthreat protection and compliance.

Tripwire apps are now available to all customers, and new ones are constantly under development. The apps can help you achieve a new level of scale and workflow efficiency with your Tripwire Enterprise installation. See the back of this datasheet for descriptions of our offerings

Many security and operations teams leverage SIEMs to track the state of their environment and alert on security and operational issues. While this may be an effective way to gain that single view of your environment, objective compliance results and file integrity data such as who made the change, exact before and after differences in files or configurations, the severity of change, or even visibility into your most critical assets is not available from SIEMs. As a result, it is difficult to make effective risk-based decisions without complete data.

Tripwire® Event Sender sends rich compliance, scoring and change data from Tripwire Enterprise to SIEMs via syslog messaging. Now you can generate pre-processed and correlated event data that includes business context delivered to your SIEM for faster and more informative automated alerts and workflows. This level of detail provided to your SIEM will help to determine prioritized investigation and remediation, saving time.

Overall enterprise compliance and endpoint change detection data can improve SIEM results. Examples of data that Tripwire Event Sender can share with your SIEM include:

» Specific compliance test pass/fail reports, showing how business compliance goals are or are not being met, with details to use to correct

» Endpoint configuration "drift"—what changes were made, baseline comparison of before and after differences, who made the changes, when and how—for faster resolution and forensic value

» Prioritized criticality of a given change, passed to a SIEM with all the supporting details available enables more rapid response to resolve

Tripwire Event Sender supports leading SIEMs such as Tripwire Log Center™, HP ArcSight, LogRythm, IBM QRadar and Splunk.

FOUNDATIONAL CONTROLS FOR
SECURITY, COMPLIANCE & IT OPS

Tripwire apps help you achieve a new level of scale and workflow efficiency with your Tripwire Enterprise installation:

» Connect with the most popular IT and security solutions to collect data on your most critical systems for a single source of truth

» Reduce the friction between your data and the visibility and insight you need to track the current state of your environment

» Report on approved as well as unauthorized endpoint settings

» Save time and resources by automatically reconciling changes that result from software updates
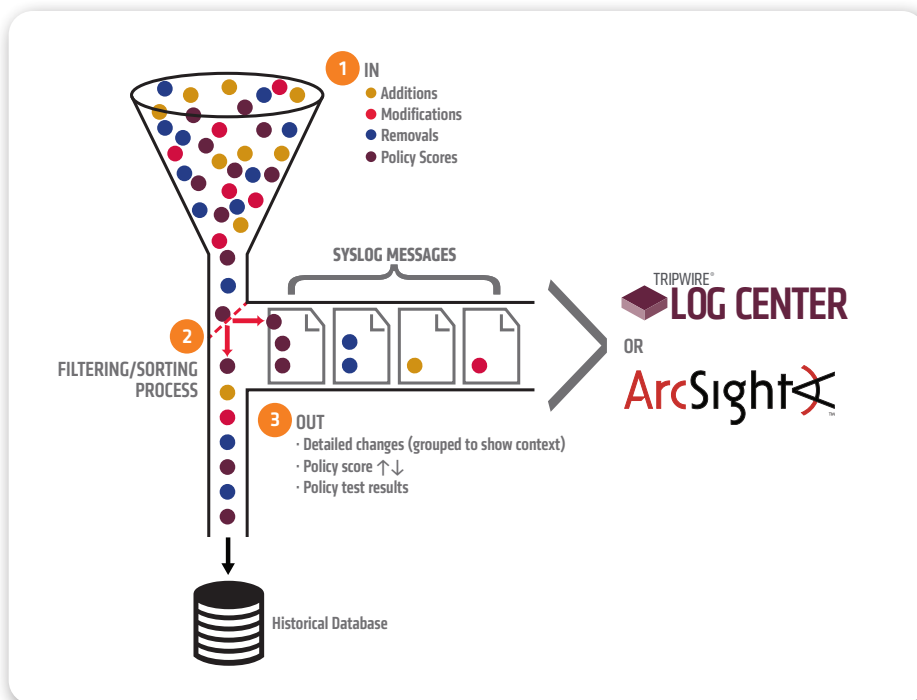
Other Available Apps

Tripwire Enterprise Integration Framework

Automates system integrations with Service Desk products like ServiceNow, Remedy, and Cherwell and others, for facilitating greater workflow efficiencies within IT security and operations.

Tripwire State Analyzer

Matches hardened and secure configurations with allowlisting including OS services, installed software, and enabled ports, and active user accounts, alerting on exceptions. This automation can keep exception alerting to just the detection of threats or "changes of interest" that may require investigation.

1 IN
- Additions
- Modifications
- Removals
- Policy Scores

SYSLOG MESSAGES

2 FILTERING/SORTING PROCESS

TRIPWIRE® LOG CENTER
OR
ArcSight

3 OUT
· Detailed changes (grouped to show context)
· Policy score ↑↓
· Policy test results

Historical Database

Tripwire Event Sender sends compliance, scoring, and change data to other systems such as SIEMs and enterprise reporting products, giving overall security ecosystem visibility for the enterprise.

Tripwire Dynamic Software Reconciliation

Reduces workload by identifying known good changes from legitimate patch sources, increasing confidence that automating the patch promotion process will only facilitate known good changes, and potentially "bad" changes cannot sneak in during times that configurations are known to be changing (such as Patch Tuesdays).

Tripwire Enterprise Commander

Cross-platform command line interface for Tripwire Enterprise, allowing unlimited integration and workflow possibilities. This facility delivers the greatest flexibility and customization to our customers.

tripwire®

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