Tripwire Apps

Extend Tripwire Enterprise to unlock additional business value

Organizations continually look for new ways to unlock the value of Tripwire Enterprise, leveraging it as a hugely valuable strategic business tool.

Now you can extend your use of Tripwire Enterprise for better, faster and more cost effective cyberthreat protection and compliance.

Tripwire Apps help achieve a new level of scale and workflow efficiency with your Tripwire® Enterprise installation. Tripwire Apps deliver:

- Comprehensive connection with the most popular IT and security solutions, to collect data on your most critical systems for a single source of truth
- Advanced visibility and insight you need to track the current state of your environment
- Actionable reporting on approved—as well as unauthorized—endpoint settings
- Automatic change reconciliation of software updates to save time and resources

Tripwire Event Sender

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 to 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 or SNMP messaging. Now you are able to generate rich event data with business context, enabling better correlations and alerting workflows, to determine what requires immediate investigation.

Event Sender supports leading log intelligence and SIEM solutions such as Tripwire Log Center™, HP ArcSight, LogRhythm, IBM QRadar and Splunk.

Tripwire Enterprise Integration Framework

You have many complex systems to manage in your environment and sometimes those multiple "sources of truth" don't necessarily agree. Tripwire Enterprise Integration Framework (TEIF) provides an automated way for systems to directly integrate and communicate with each other.

TEIF can reconcile observed changes against approved changes, enabling you to promote those changes within Tripwire Enterprise. You can also update the status of the change ticket in prominent change ticketing systems such as BMC Remedy, ServiceNow, JIRA, Cherwell, CA Service Desk and IBM Flex.

Any changes not reconciled can be created as incident tickets for your security or operations team to investigate. Tripwire Enterprise provides full details of the unauthorized change, which can be attached to the ticket.

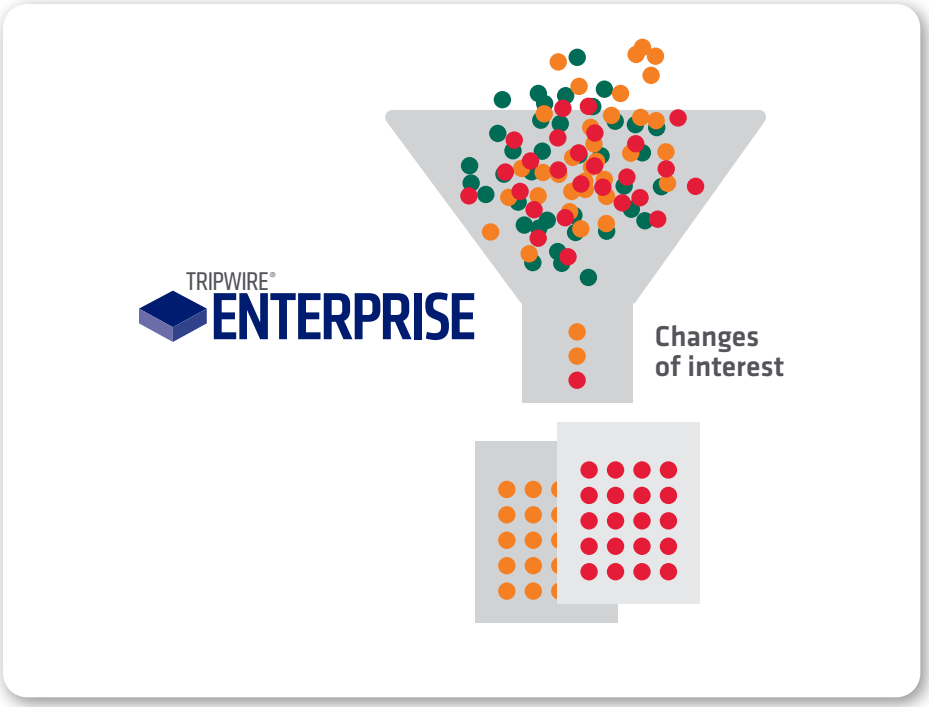

Fig. 1 Using Tripwire Enterprise Integration Framework you can easily prioritize, investigate and remediate suspicious changes.

Finally, TEIF can query your CMDB to retrieve metadata about in-scope assets such as business function or system owner, etc. and automatically apply corresponding asset tags within Tripwire Enterprise. In addition, with TEIF you can use data harvested directly from the node to update your CMDB's records for the corresponding asset to ensure that Tripwire Enterprise and your CMDB stay in close alignment.

Tripwire State Analyzer

Most compliance frameworks specify recommended or required settings such as rename administrator account or disable telnet, etc. Virtually all compliance tools report on discrepancies or gaps, yet it is also essential to continuously report on approved settings instead of just the unauthorized ones. This can be a significant challenge for many compliance tools.

The Tripwire State Analyzer app enables you to define a set of required or permitted system settings and when a system is examined, any settings that match your allowlist are enumerated. If a match is found, the report will include software package name, version and additional user-defined fields associated with the entry in the allowlist. If a setting does not match the allowlist, the report will include an exception, and an alert will show up in Tripwire Enterprise. You can also include the justification for a given setting in the same report to speed up the auditing process.

There are four scenarios supported by the Tripwire State Analyzer app: enabled network ports, running OS services, installed software, and active user accounts. Each of these scenarios has its own allowlist and supports its own independent workflow.

Tripwire Dynamic Software Reconciliation

Patch Tuesday is perhaps the most anticipated and feared day of the month for network administrators and security managers. They wait eagerly for the next round of patches, glad to gain some protection against attacks on the vulnerabilities that have been found since the previous month's release. They also dread it due to the massive amount of work and time involved in rolling out dozens of patches to thousands of systems. Some patches may cause regression errors or problems with other applications. Also, it is impossible to identify which change came from which source.

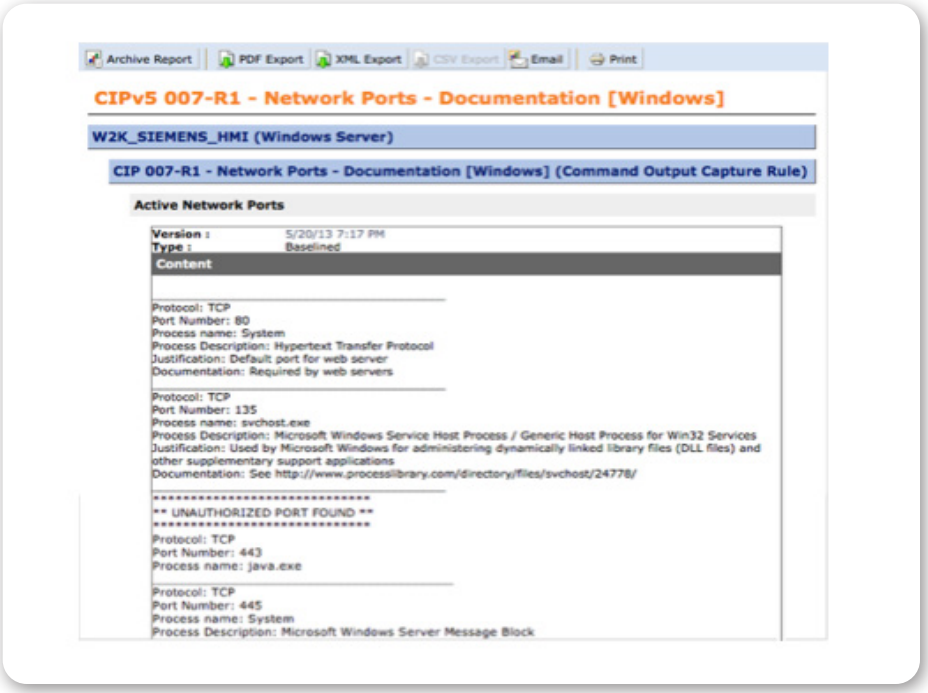

Fig. 2 Report on approved as well as unauthorized system settings, regardless of type, using the Tripwire State Analyzer app.

Tripwire Dynamic Software Reconciliation (DSR) solves these challenges by compiling a list of installed patches, then querying MS TechNet and YUM repositories for Linux and fetching the file-level manifests for each patch. These manifests are then used to promote changes, which offers a reliable and authoritative source to identify all legitimate changes. That also identifies any additional changes made to the system that were not part of the approved patch. Tripwire DSR offers an automated way to optimize your patch reconciliation and minimize the pain of dealing with hundreds of changes detected on each system after Windows patches have been applied.

Tripwire Enterprise Commander

Many enterprise applications lack a native command line interface. This can be a challenge if you want to automate and integrate basic operations, which is a necessary function in most enterprise IT environments.

Tripwire Enterprise Commander is a cross-platform CLI for Tripwire Enterprise that allows unlimited integration and workflow possibilities. It offers a consistent and reliable way to retrieve rich information from Tripwire Enterprise, in as flexible a manner as possible.

By leveraging TE Commander you can also make changes and trigger actions within Tripwire Enterprise. Actions include scanning a host, adding or updating an asset tag, or disabling a node as part of a decommissioning process—all without direct user interaction.

Tripwire Password Manager

Tripwire Password Manager acts as an information broker between a privileged access management (PAM) solution and Tripwire Enterprise or Tripwire IP360™. Tripwire Password Manager maximizes your PAM investment by integrating it with your Tripwire solution. This allows you to retrieve credentials from the PAM, eliminating the need to manage scan credentials within Tripwire Enterprise or Tripwire IP360 directly.

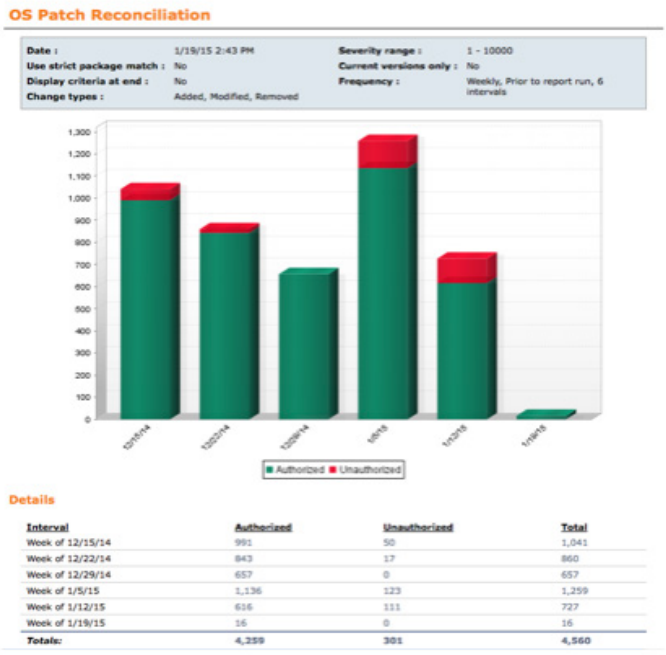

Fig. 3 Tripwire Dynamic Software Reconciliation rapidly brings to light any additional changes made to a system.

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