DATASHEET

Tripwire Dynamic Software Reconciliation

Automation For Knowing "Good" Vs "Bad" Change

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.

Most enterprises experience massive amounts of system configuration change every day, and experience has shown that an average of 50% of system changes are simply additions, changes, or deletions considered "business as usual" (BAU) for your organization. The vast majority of these changes can be quickly accepted and promoted as "known good."

Tripwire® Dynamic Software Reconciliation (DSR) automates the verification and promotion of "known good"/BAU changes that are the result of software updates, upgrades and patches, saving IT organizations time, reducing human error and increasing efficiency. Tripwire DSR also works in concert with Tripwire Enterprise to deliver alert notifications and granular details needed for rapid response when unexpected, unauthorized or high-risk changes are detected.

Patch Tuesday Risk

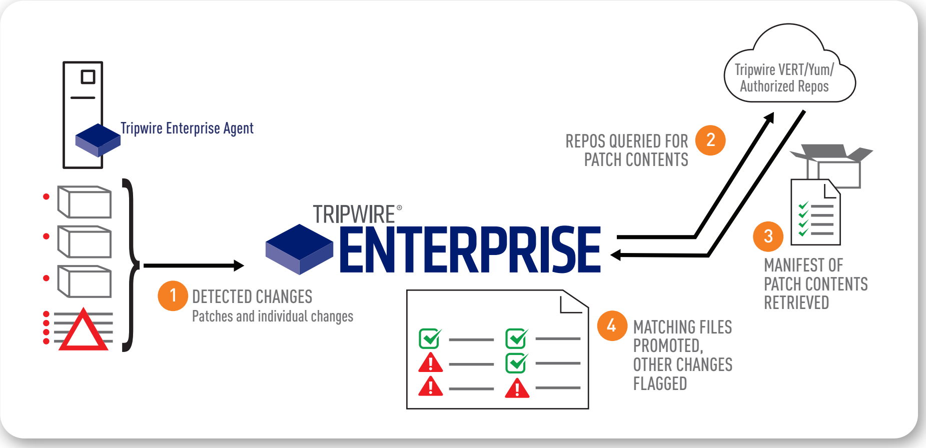
Patch Tuesday is perhaps the most anticipated—and feared—day of the month for many network administrators and security managers. Some may be glad to gain new protection against attacks on the vulnerabilities that have been found since the previous month's release. But many may also dread it due to the massive amount of work and time involved in rolling out often wide-reaching changes and dozens of patches to thousands of systems—many of them with very tight schedules for downtime. Some patches may cause regression errors or problems with other applications, and the reconciliation process can be difficult. Plus, it can be tedious to identify which change came from which sources in the event that real troubleshooting needs to occur in the workflow.

Tripwire Dynamic Software Reconciliation automates verification and promotion of upgrades, updates or patches from trusted sources. There are three categories of reconciliation sources currently available for automation:

- Tripwire VERT content reconciliation for Windows
- YUM repositories for verifying Unix patching and deployments
- Generic Software Module (GSM) allows you to define your own manifest or source which will be used for approving updates, changes, or even initial installations.

This could apply to a variety of changes needed such as from:

- Microsoft SCCM
- IBM Big Fix
- Adobe
- Java
- Microsoft SQL updates
- Anti-virus
- HP-UX (new)
- Other sources of your choosing


Tripwire Enterprise Agent
Tripwire VERT/Yum/ Authorized Repos
2 REPOS QUERIED FOR PATCH CONTENTS
TRIPWIRE® ENTERPRISE
3 MANIFEST OF PATCH CONTENTS RETRIEVED
1 DETECTED CHANGES
Patches and individual changes
4 MATCHING FILES PROMOTED, OTHER CHANGES FLAGGED

Tripwire Dynamic Software Reconciliation reduces workloads by identifying known good changes coming from legitimate patch sources. This increases confidence that automating the patch promotion process will only facilitate known good changes, and that potentially "bad" changes cannot sneak in during times that configurations are known to be changing (such as Patch Tuesdays).

Overview

Tripwire Dynamic Software Reconciliation solves these challenges by compiling a list of installed patches then it automatically queries Tripwire VERT, Linux YUM or repositories you authorize. It then fetches the file-level manifests to validate each patch, reliably verifying legitimate patches against authoritative sources to reduce business risk and improves operational efficiency for IT security and operations teams.

This validation also identifies any additional changes that are 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 patches have been applied.

Tripwire Enterprise integrated with Tripwire DSR adds increased automation and efficiency to reduce the workload surrounding verifying updates, upgrades, or patches:

- Reliable and authoritative validation of OS and software installation updates from the trusted sources
- Identifies and alerts on any other changes being made that are not part of a legitimate and verified patch
- Automates and optimizes system configuration changes and patch reconciliation

Tripwire Apps help you achieve a new level of scale and workflow efficiency with your Tripwire solution

- 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 resulting from software updates

Other Tripwire Apps

Tripwire State Analyzer

Matches hardened and secure configurations with allowlisting, including OS services, installed software, 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.

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 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 Enterprise Integration Framework

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

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