SOLUTION BRIEF

Auto-Promotion of Expected Changes

Reduce your workload through automation

Highlights

Tripwire Enterprise supports multiple methods of automatically promoting expected changes:

- Promote-by-Reference
- Promote-by-Match
- Promote-by-Change Request
- Promote-by-Dynamic Software Reconciliation

Changes to configurations, files and file attributes across the IT infrastructure are just part of everyday life in enterprise organizations. But hidden within the large volume of daily changes can be a few unauthorized changes that impact the confidentiality, integrity or availability of a system. To protect critical systems and data, you need to detect every change, capture relevant details about each one, and use those details to determine if the change introduces security, compliance or availability risks.

With constant changes to files and configurations, how do you tell the difference between those that are "good" and "bad"? Or in a more pragmatic sense, between business as usual changes and those that spell trouble? That's what security configuration management (SCM), a critical security control, is supposed to do. Unfortunately, most SCM solutions determine that a change occurred—and stop there. Only a few capture the change in real time and with enough detail to show you who made it and exactly what was changed.

"True" SCM detects each change as it occurs and uses change intelligence to determine if a specific modification introduces security or compliance risks. File Integrity Manager, a core component of Tripwire® Enterprise, delivers this insight by combining Tripwire's industry-leading change detection with the intelligence to automatically filter out the expected ("known good"/business as usual) changes. This allows you to then focus entirely on the changes that are suspicious.

FOUNDATIONAL CONTROLS FOR
SECURITY, COMPLIANCE & IT OPERATIONS

Without automated intelligence determining if a change is expected you would need to manually review each and every one. While this might work for a small number of systems, in enterprise environments this approach would be unmanageable.

With Tripwire Enterprise, there are multiple methods of "approving" detected changes that are authorized by your organization and implemented exactly as intended. This is referred to as promoting a change. Promotion creates a new baseline that is an exact copy of the most recent change version.

Tripwire Enterprise supports multiple methods of promoting changes automatically through a feature called auto-promotion.

When using auto-promotion, modifications caused by software deployment or patching can be promoted automatically as "authorized" changes. This allows the user to focus on the remainder of detected changes that could be indicators of compromise (IoC).

To simplify the process of automatically promoting change, Tripwire Enterprise supports different methods. The following methods were designed to address specific business needs:

» Promote-by-Reference

» Promote-by-Match

» Promote-by-Change request

» Promote-by-Dynamic Software Reconciliation (DSR)

Promote-By-Reference

Promote-by-reference provides a method to promote detected changes on multiple systems if those changes match the current state of a reference system. The reference node is often referred to as a "gold build."

With this method, the "change-version" of elements will be promoted to "element-baseline" if the "change-version" of an element matches the "element-baseline" of the reference system.

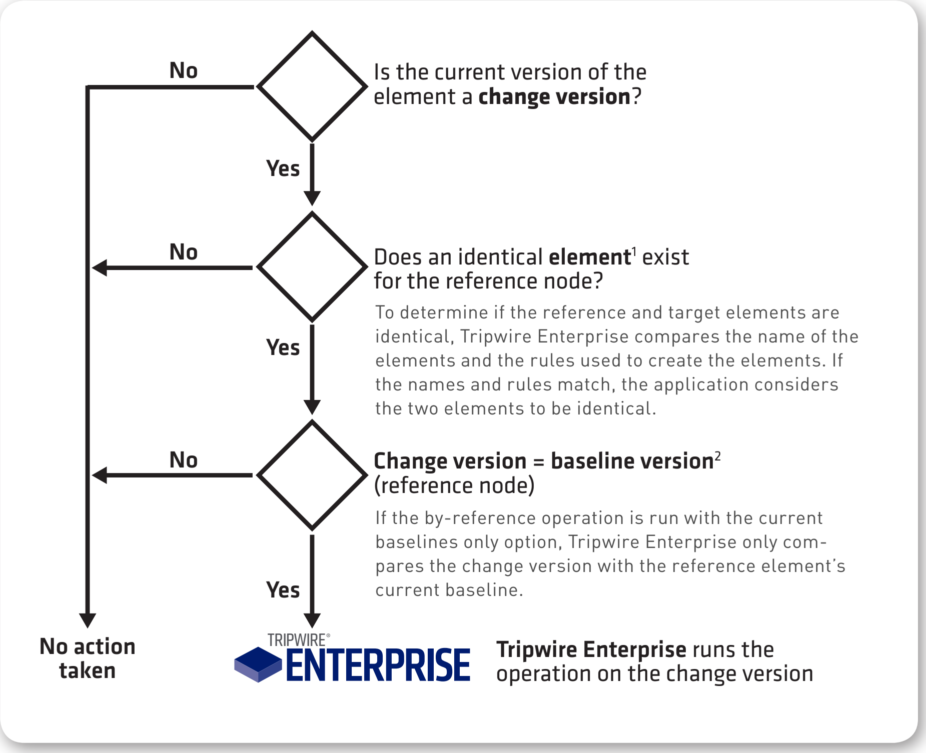
No
Is the current version of the element a **change version**?
Yes
No
Does an identical **element**[1] exist for the reference node?
To determine if the reference and target elements are identical, Tripwire Enterprise compares the name of the elements and the rules used to create the elements. If the names and rules match, the application considers the two elements to be identical.
Yes
No
Change version = baseline version[2] (reference node)
If the by-reference operation is run with the current baselines only option, Tripwire Enterprise only compares the change version with the reference element's current baseline.
Yes
No action taken
TRIPWIRE® ENTERPRISE
Tripwire Enterprise runs the operation on the change version

Fig. 1 Promote-by-Reference

By creating an "action" of the type "promote-by-reference," this method can then be used, and the "action" will be added to a "task" or to a "rule." Once this is completed, the action will be executed at the end of the task, or after the rule runs.

Use Case for Promote-By-Reference

The promote-by-reference method can be used to promote a number of changes across multiple systems caused by the deployment of software.

The reference system can be a system in the preproduction environment that has the latest software installed.

If you are using a repository for OS packages and/or software, you might want to refer to the auto-promotion method "Promote by Dynamic Software Reconciliation" later in this document.

Promote-By-Match

This method provides a way to promote changes detected across multiple systems if the changes match the criteria specified within a file referred to as a "match-file."

A match file can either be a UTF-8 encoded text file or an XML file containing the output of a "Detailed Change Report."

Running this report against a system that has detected changes creates "Detailed Change Report" XML output. The change information stored in the file is used to promote detected changes that match the file in other systems.

By creating an "action" of the type "promote-by-match" and adding this "action" to a "task" or to a "rule," this method can be used. The action will be executed at the end of the task or after the rule runs.

Use Case for Promote-By-Match

Because this method uses a file containing criteria for promotions, it can be created from a reference system, which is monitored by a different Tripwire Enterprise console.

Promote-by-Match: Matching strategies defined by match-file format

Matching Strategy	Match file contains a list of...	An operation runs if...
Element name	...element name	...a current version represents an element with a name that matches an entry in the match file.
Element name and hash value	...element names and associated hash values	...a current version represents an element with a name, change type and hash value (optional) that matches an entry in the match file.
Rule name	...rule names	...a current version represents a monitored object that was identified by a rule listed in the match file.

If the same Tripwire Enterprise console manages both the reference system and the target systems, the promote-by-reference method is recommended as it doesn't require the tasks to create a match file.

Another use case for this function can be to use a match file generated by another tool. An example of this would be if a match file was created by converting a manifest file.

Promote-By-Change Request

This method provides a way to auto-promote changes of multiple systems if the change and date/time stamp matches a change request in a change management (CM) system like ServiceNow, Remedy, JIRA or others.

CM systems help verify that changes made to a system were authorized and performed properly, and this integration enables Tripwire Enterprise to query a CM system to verify that the changes it detected were properly planned and authorized. In other words, this feature determines if the right changes were made to the right system, at the right time, and by the right person.

Additionally, unexpected changes found by Tripwire Enterprise generate incident tickets in the CM system, which then notifies the proper channels of a change management process violation or a possible security event. For example, Tripwire Enterprise detects a system change that has no ticket in the CM system or finds that additional changes were made that weren't authorized on the ticket.

Use Case for Promote-By-Change Request

This method is more likely to be used for changes other than software deployment and patching (see Promote-by-Reference and Promote-by-Dynamic Software Reconciliation). One example is applying a new Windows (domain) policy to multiple servers that will cause changes in security settings, permission changes on objects, etc.

Note: Promote-By-Change Request requires an additional software license and professional services engagement.

Promote-By-Dynamic Software Reconciliation

Tripwire's Dynamic Software Reconciliation (DSR) app automates the verification and promotion of expected ("known good"/business as usual) changes that are the result of software deployment, updates, upgrades and patches.

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

- » Microsoft TechNet reconciliation for Windows hot fixes

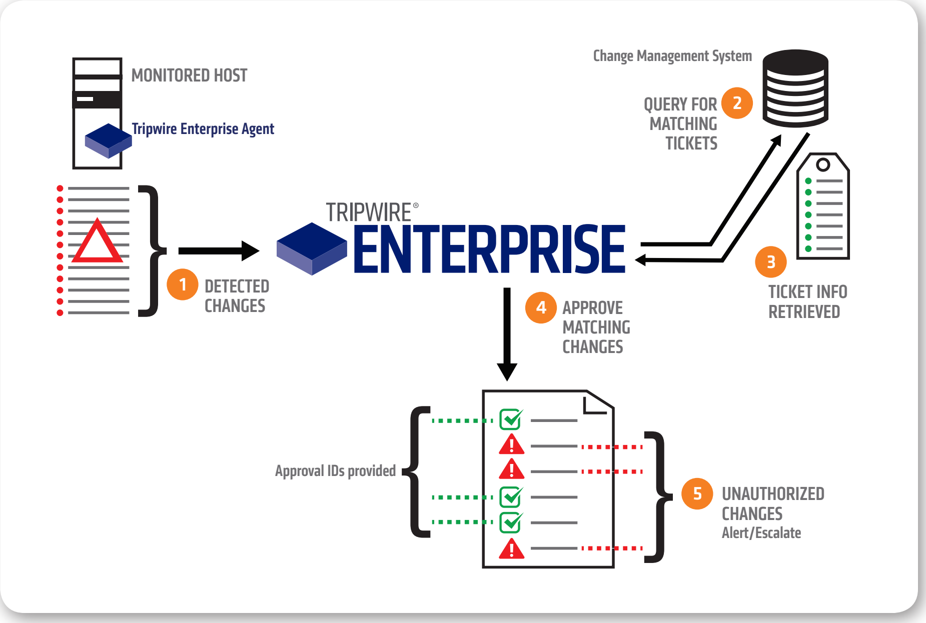

Fig 2. Promote-By-Change Request automates system integrations with Service Desk products like ServiceNow, Remedy, Cherwell and others, for facilitating greater workflow efficiencies within IT security and operations.

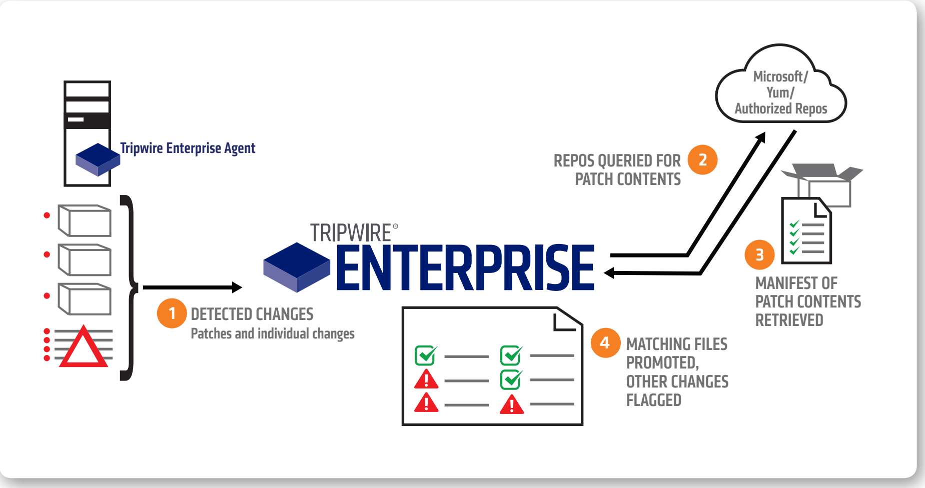
Tripwire Enterprise Agent
TRIPWIRE®
ENTERPRISE
1 DETECTED CHANGES
Patches and individual changes
REPOS QUERIED FOR PATCH CONTENTS 2
Microsoft/ Yum/ Authorized Repos
3 MANIFEST OF PATCH CONTENTS RETRIEVED
4 MATCHING FILES PROMOTED, OTHER CHANGES FLAGGED

Fig 3. Promote-By-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).

- YUM Repositories for verifying Unix patching and deployments
- Generic Software Module (GSM), which allows you to define your own manifest or source and is used for approving updates, changes, or even initial installations

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

- Microsoft System Center Configuration Manager (SCCM)
- IBM BigFix
- Adobe
- Java
- Microsoft SQL updates
- Anti-virus
- Other sources of your choosing

This validation also identifies any additional changes that are not part of the approved patch. Dynamic Software Reconciliation offers an automated way to optimize patch reconciliation and minimize the pain of dealing with hundreds of changes detected on each system after patches have been applied.

Use Case for Promote-By-Dynamic Software Reconciliation

This method is recommended to auto-promote detected changes caused by updates, upgrades and patches where the changes can be matched with a manifest from a repository. This method can also be used to auto-promote any change due to initial software deployment as long as the manifest is defined in a repository.

Note: Promote-by-Dynamic Software Reconciliation requires an additional software license and professional services engagement.

Which Methods of Auto-Promotion Are Right for You?

Depending on your current processes and use of CM systems and patch/software repositories, it's possible to use a combination of all four methods. Using any of these auto-promotion methods will immediately increase the value of your SCM solution by drastically reducing the change analysis workload and making it easier to detect and respond to unwanted changes, which can have a security or compliance impact.

Ask your Tripwire representative for more information or to discuss which methods are the best fit for your organization.

Tripwire is the trusted leader for establishing a strong cybersecurity foundation. Partnering with Fortune 500 enterprises, industrial organizations and government agencies, Tripwire protects the integrity of mission-critical systems spanning physical, virtual, cloud and DevOps environments. Tripwire's award-winning portfolio delivers top critical security controls, including asset discovery, secure configuration management, vulnerability management and log management. As the pioneers of file integrity monitoring (FIM), Tripwire's expertise is built on a 20+ year history of innovation helping organizations discover, minimize and monitor their attack surfaces. **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