



# Change Detection and Reconciliation

## Apple Bank

# Tripwire is focused on three aspects of your business

## Performing as expected

- » Standard configurations
- » Change audit and validation
- » Improved uptime and MTTR



## Protecting your organization







- » Foundational integrity controls
- » Automated workflows
- » Extensive integrations

## Proving compliance

- » Extensive regulatory coverage
- » Continuous monitoring
- » Audit evidence and reports

# What gets monitored?

File integrity monitoring solutions watch for changes to files associated with the servers, databases, routers, applications, and other devices and elements in the enterprise IT infrastructure.

Server File Systems	Databases	Network Devices	Directory Services	Hypervisors	Applications
					
Registry entries	Tables	Routing tables	Privileged group	Permissions	Web server keys
Configuration files	Indexes	Firewall rules	Group policy options	Firewall settings	System files
.exe	Stored procedures	Configuration files	RSoP	Auditing/logging	Logs
File permissions	Permission grants	ACLs		Access controls	Registry settings

**Table 1:** File attributes being monitored may include hostname, username, ticket number, date and time stamp and operation type. This table provides an overview of the type of attributes these solutions may monitor.

WINDOWS	UNIX
Access time	Access time
Creation time	Change time
Write time	Modify time
Size	Size
Package data	Package data
Read-only	ACL
DACL	User
SACL	Group
Group	Permissions
Owner	Growing
Growing	MD5
MD5	SHA-1
SHA-1	
Hidden flag	
Stream count	
Stream MD5	
Offline flag	
System flag	
Temp flag	
Compressed flag	
Archive flag	

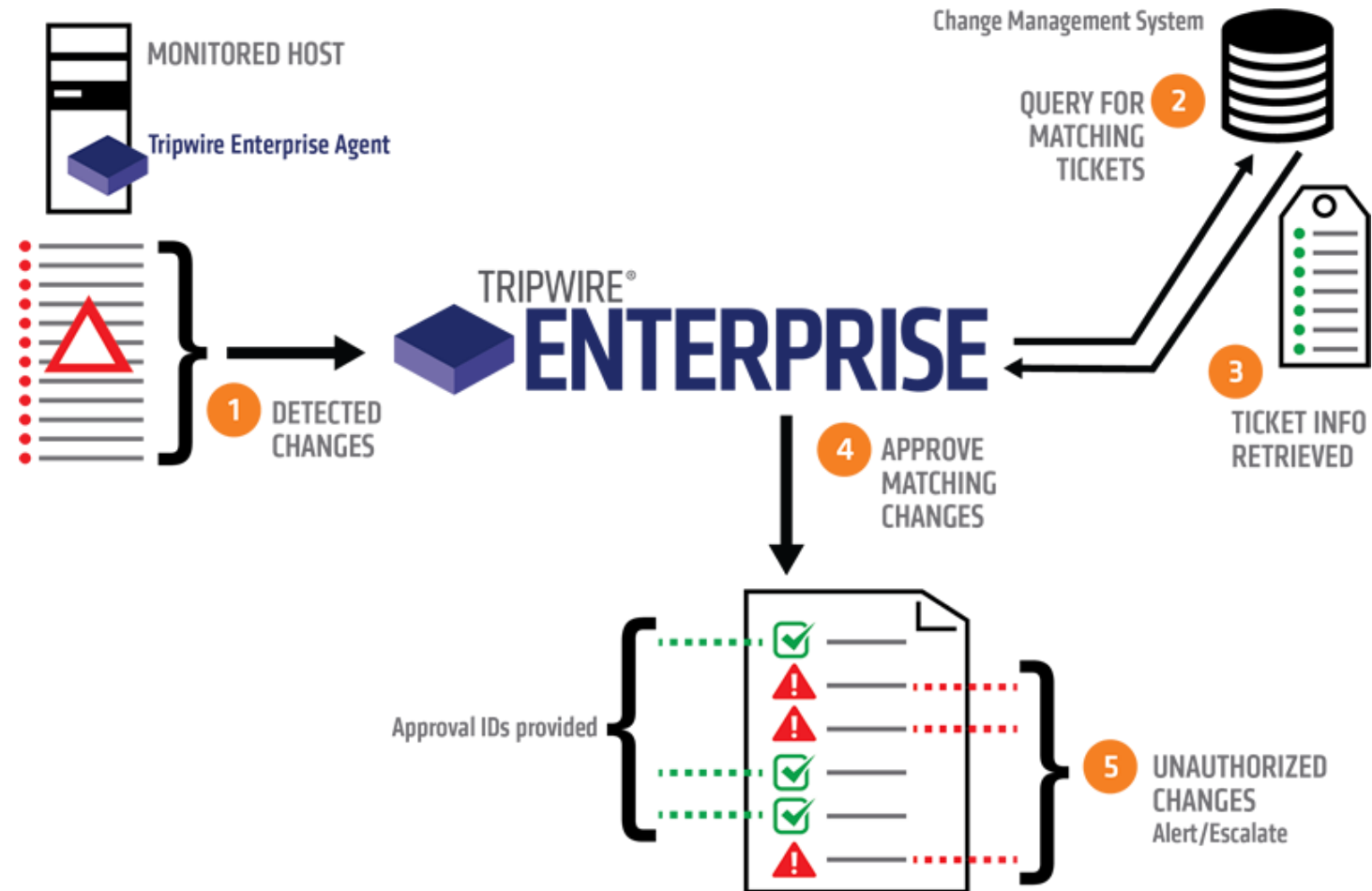
**Table 2:** This table provides a sampling of the type of IT configuration these solutions may monitor.

## ServiceNow - Tripwire TEIF – Tripwire Enterprise Integration Framework

Automated way for systems to directly integrate and communicate with each other.

### Benefits

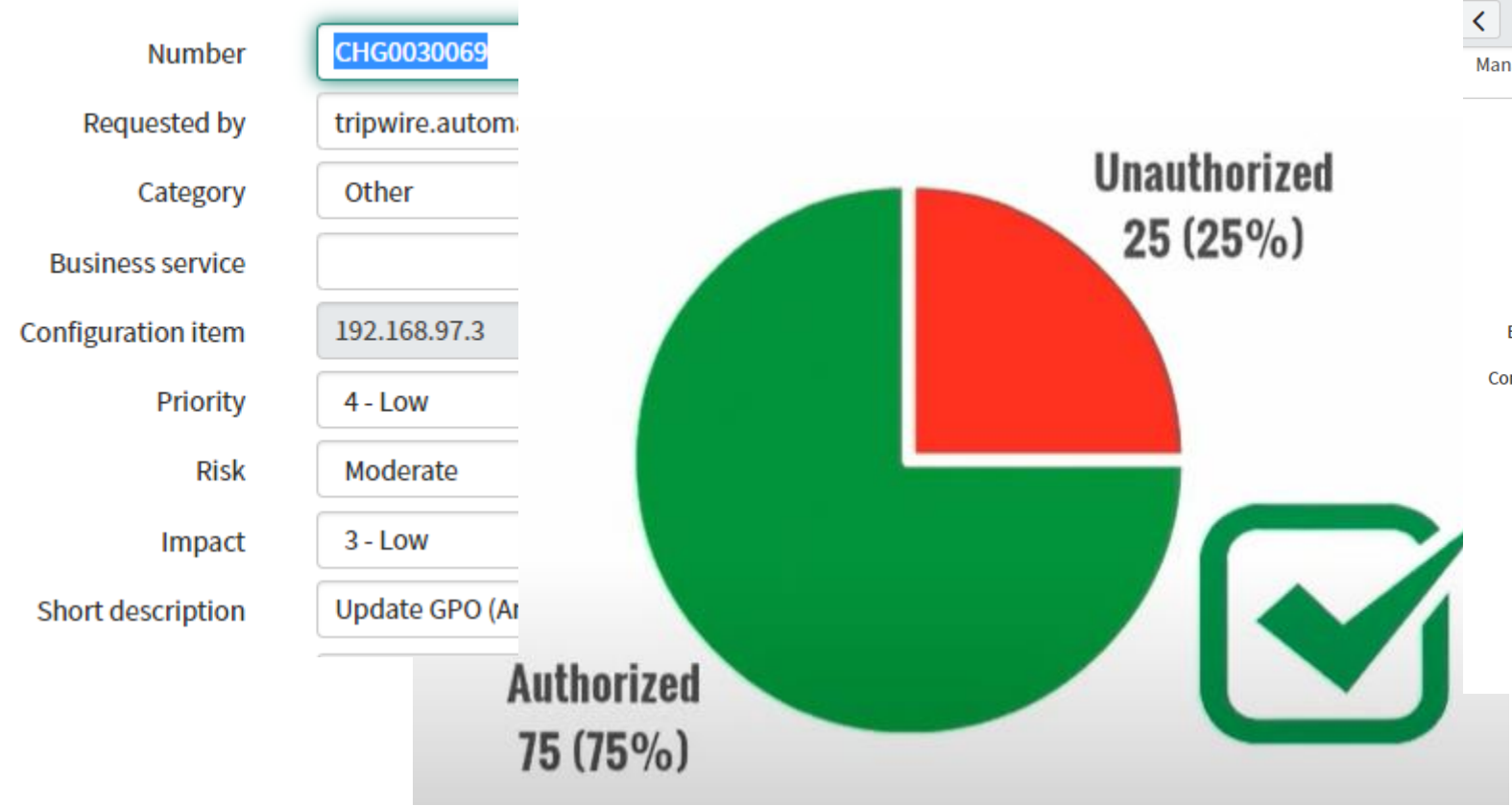
- Automatic promotion of approved changes
- Incident creation for unreconciled changes



# Tripwire TEIF – Tripwire Enterprise Integration Framework

Automate the reconciliation process between Tripwire Enterprise and ServiceNow to identify **UNAUTHORIZED CHANGES**

And create a new ServiceNow **Incident** Requests for those changes.



INC0010163

Manage Attachments (1): Tripwire Detailed Changes Report -... [rename] [download]

Number

INC0010163

Contact

\* Caller

Category

Software

Im

Subcategory

-- None --

Urg

Business service

Pri

Configuration item

Unknown

Assignment g

\* Short description

Tripwire detected potentially unauthorized changes for Application

Description

Potentially unauthorized changes include:  
C:\Program Files\Tripwire\Tripwire Log Center Manager\Data\,vdb4.txt  
C:\Program Files\Tripwire\Tripwire Log Center Manager  
C:\Program Files\Tripwire\Tripwire Log Center Manager\Data  
C:\Program Files\Tripwire\Tripwire Log Center Manager\Data\d\,a,b - Copy (2).txt  
C:\Program Files\Tripwire\Tripwire Log Center Manager\Data\d\,a,b - Copy - Copy.txt

Record all changes for improved MTTR and Forensics

# Tripwire TEIF – Tripwire Enterprise Integration Framework

AB Group Policy Object

Scope

Details

Settings

Delegation

Status

Domain:

galaxy.ffa

Owner:

Domain Admins (GALAXY\Domain Admins)

Created:

8/3/2021 9:06:29 PM

Modified:

8/13/2021 9:50:04 AM

User version:

0 (AD), 0 (SYSVOL)

Computer version:

0 (AD), 0 (SYSVOL)

Unique ID:

{A6D58634-EB08-4D8B-B8EC-391672F8C626}

GPO Status:

Enabled

All settings disabled

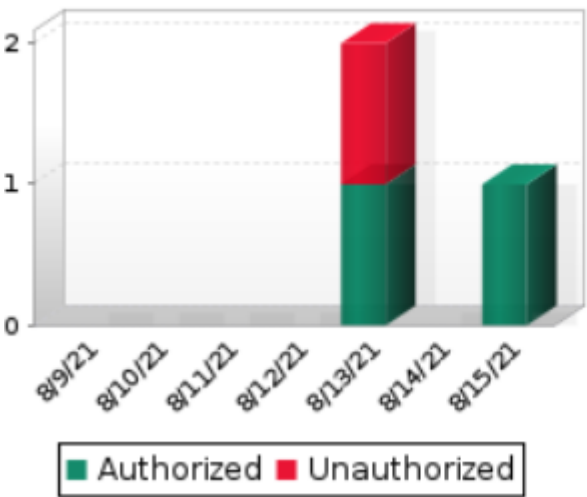
Computer configuration settings disabled

Enabled

User configuration settings disabled

Comment:

Application Changes - Reconciled versus Unreconciled



- a. Change from our baseline
- b. Who made that change?
- c. What changed?
- d. When was it changed.
- e. What System had the change

Changed Elements with Approval ID					
Node: AD (Active Directory Server)					
Date	Element	Change Type	Attributes	Users	Promotion Approval ID
8/4/21 11:50 AM	CN={66E5E921-B7BC-498C-A21D-8118B9E2703D},CN=Policies,CN=System,DC=galaxy,DC=ffa	Modified	groupPolicyMD5	GALAXY\tdemo	CHG0030068

# Tripwire TEIF – Tripwire Enterprise Integration Framework

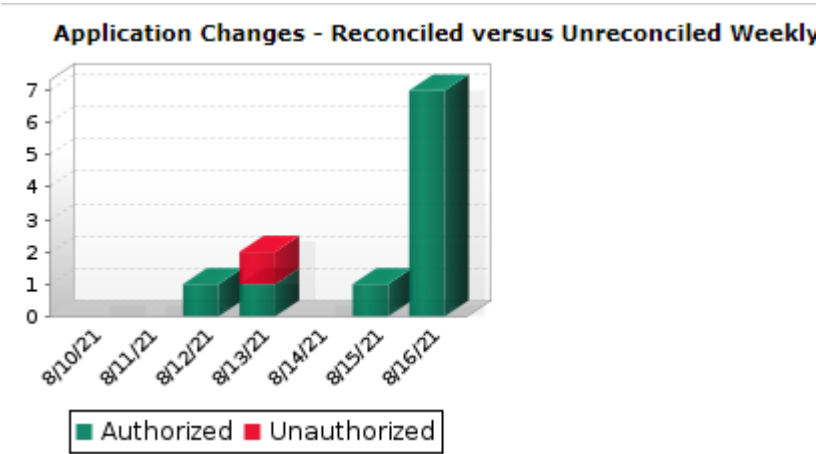
Since a change Ticket was created for the AD and Windows 10 systems the Promotion Approval ID has been updated. Instead of manually updating the changes that have occurred on the system.. The TEIF integration does that on a scheduled bases.

Node: AD (Active Directory Server)					
Date	Element	Change Type	Attributes	Users	Promotion Approval ID
8/16/21 1:57 PM	CN={A6D58634-EB08-4D8B-B8EC-391672F8C626},CN=Policies,CN=System,DC=galaxy,DC=ffa	Modified	groupPolicyMD5	GALAXY\twdemo	CHG0030068
8/16/21 12:25 PM	CN={A6D58634-EB08-4D8B-B8EC-391672F8C626},CN=Policies,CN=System,DC=galaxy,DC=ffa	Modified	groupPolicyMD5	GALAXY\twdemo	CHG0030068
Node: Stingray (Windows Server)					
Date	Element	Change Type	Attributes	Users	Promotion Approval ID
8/16/21 1:32 PM	C:\Program Files\Tripwire\Tripwire Log Center Manager\Data\A\Changed File.txt	Modified	SHA-256, Size	STINGRAY\agerges	CHG0030067
8/16/21 12:27 PM	C:\Program Files\Tripwire\Tripwire Log Center Manager\Data\A\Changed File.txt	Modified	SHA-256, Size	STINGRAY\agerges	CHG0030067

Who made that change?

Tripwire TEIF – Tripwire Enterprise Integration Framework

For Network device, we see that a change occurred, and an incident ticket was created.



General | Content | Attributes | Log | Properties

Date: Aug 16, 2021 1:57:51 PM

Element: snmp-server Information

Type: Current Baseline

Exists: Yes

Default Severity: None

Change window: Inside window

Approval ID: INC0010181

Comment: Promoted by twintegrations on 8/16/21 1:57 PM  
---  
Notification via integration ->

8/16/21 11:51 AM	snmp-server Information	Modified	MD5	<div><div>GeneralContentAttr</div><div>New VersionExport</div><div>no snmp-server location no snmp-server contact snmp-server community *****</div></div>	INC0010181
8/16/21 11:36 AM	snmp-server Information	Modified	MD5		INC0010181
8/16/21 11:19 AM	snmp-server Information	Modified	MD5		INC0010180