SCM/FIM Overview

Agenda

Covering the following topics

- Tripwire Overview
- Tripwire Enterprise
- Change Detection: SCM/FIM
  - SCM Dashboards, Reporting, Policy Tests
- Use Cases:
  - Active Directory: GPO – Account Policy Changes
  - Firewalls & Network Devices
  - Servers & Filesystems
- Automated Workflows
- Integrations
- Extensions/Apps

A leader in security, compliance, and operational excellence

Foundational controls for security, compliance, and IT operations

Stable, growing public company in a chaotic industry

Relied on by thousands of customers since 1997

1000s
of successful customer deployments

20M
critical endpoints covered globally

92%
customer satisfaction

Trusted
by half the Fortune 500

F500

Why Tripwire?

Security Configuration Management & Integrity Monitoring from the Experts…it's in our DNA

The Importance of Baselines

- Everything Tripwire Enterprise does is based on the concept of establishing a baseline for an asset, then tracking changes against that baseline. This methodology allows effective state comparison, change management workflow, and policy compliance on top of FIM.
- Other solutions don't have baselines. Tracking and workflow are 'incident' or 'event' driven, rather than providing change management.

The Correct Workflows

- Tripwire has a long history of delivering change management workflows that work with tools like Dynamic Software Reconciliation to reduce the noise from business-as-usual changes.
- Other solutions focus on creating 'incidents' in their workflows but lack change reconciliation with the systems they're already using.

Comparing State; Providing Context

- Tripwire captures all change for forensic purposes including Good" v "Bad" and High-risk v low risk changes
- Tripwire links FIM Capability to Active Directory, making it more intelligent. Tightly integrated with compliance policies: Shows impact.
- Other solutions lack state comparison and have a limited understanding of change context (good vs bad, / high vs low risks.)

Don’t get fooled

Where other solutions are lacking

Basic SCM/FIM Capabilities

- Unable to detect changes on network devices
- Narrow built-in policies for FIM: applications, databases, web servers
- No concept of baselines / promoting changes to the baseline

Intelligence & Context

- Inability to compare state; understanding of the context around changes (good vs bad; high vs low risk)
- Lack of dynamic asset tagging / grouping; custom asset properties
- Inability to provide Change IQ. Can’t provide powerful decision tree capabilities enabling intelligent change and alert customization

Reconciliation & Remediation

- Restricted or no ability to reconcile changes, identify changes as business-as-usual
- No automation of change reconciliation; only manual review of incidents/changes
- Limited or no ability to prioritize remediation efforts

Ecosystem / Support / Integrations

- Primarily focused on data access governance or vulnerability management
- Inadequate platform support: no support for Oracle Enterprise Linux, SuSE, AIX, Solaris, Mac OS X and others.
- Small degree of integration and few threat intelligence partners

Tripwire is focused on three aspects of your business

Protecting your organization

» Foundational integrity controls
» Automated workflows
» Extensive integrations

Performing as expected

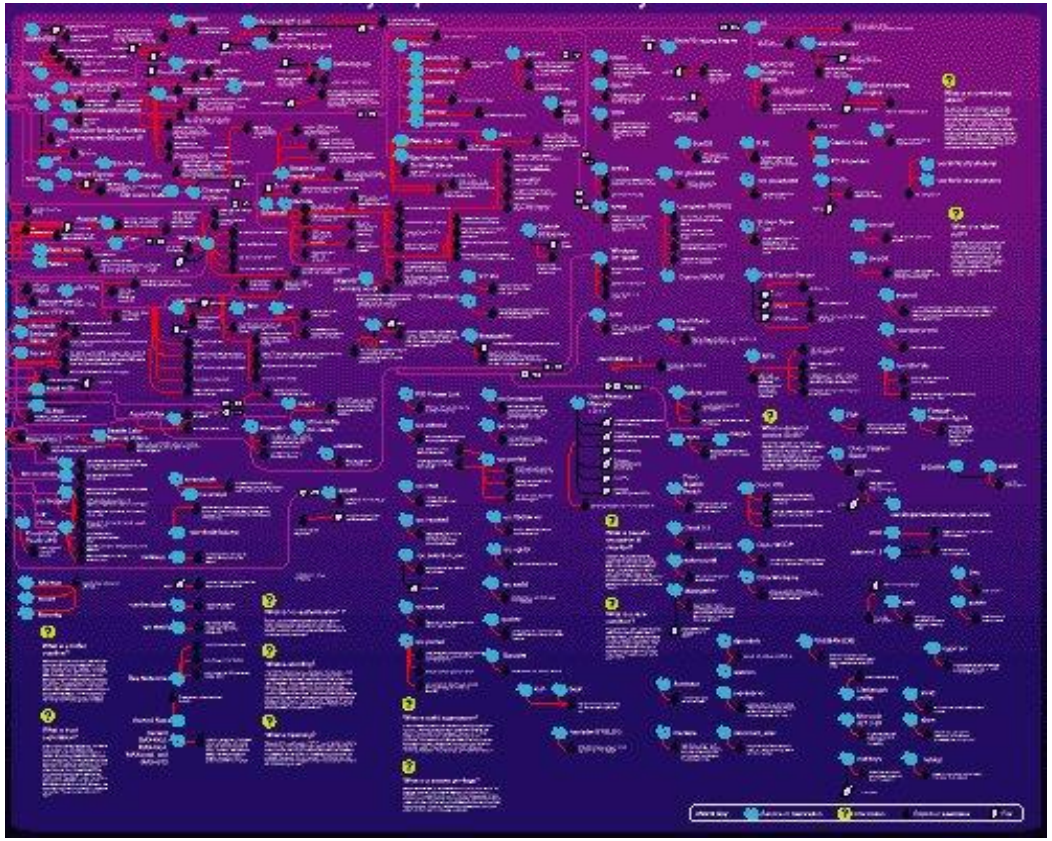
» Standard configurations
» Change audit and validation
» Improved uptime and MTTR

Proving compliance

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

The Devil in the Details

Finding the changes that matter



Snapshot: Files, Nodes, Assets, Servers, etc.

Integrity Monitoring

- Tripwire is the pioneer of File Integrity Monitoring and the capability to baseline systems and identify changes is our bread and butter
- Today, Tripwire can be used to ensure systems, applications, and other assets are not changing in suspicious, malicious, and unauthorized ways.
- Customers use integrity monitoring to better understand how their environment is changing, to take control of unplanned change, and to stay ahead of both auditors and attackers.

Security Configuration Management

- Ensuring that systems are configured securely [and that they stay that way] is one of the most effective means of preventing successful cyber attacks.
- Tripwire helps customers identify insecure configurations and provides the guidance necessary to fix them.

Policy & Compliance Management

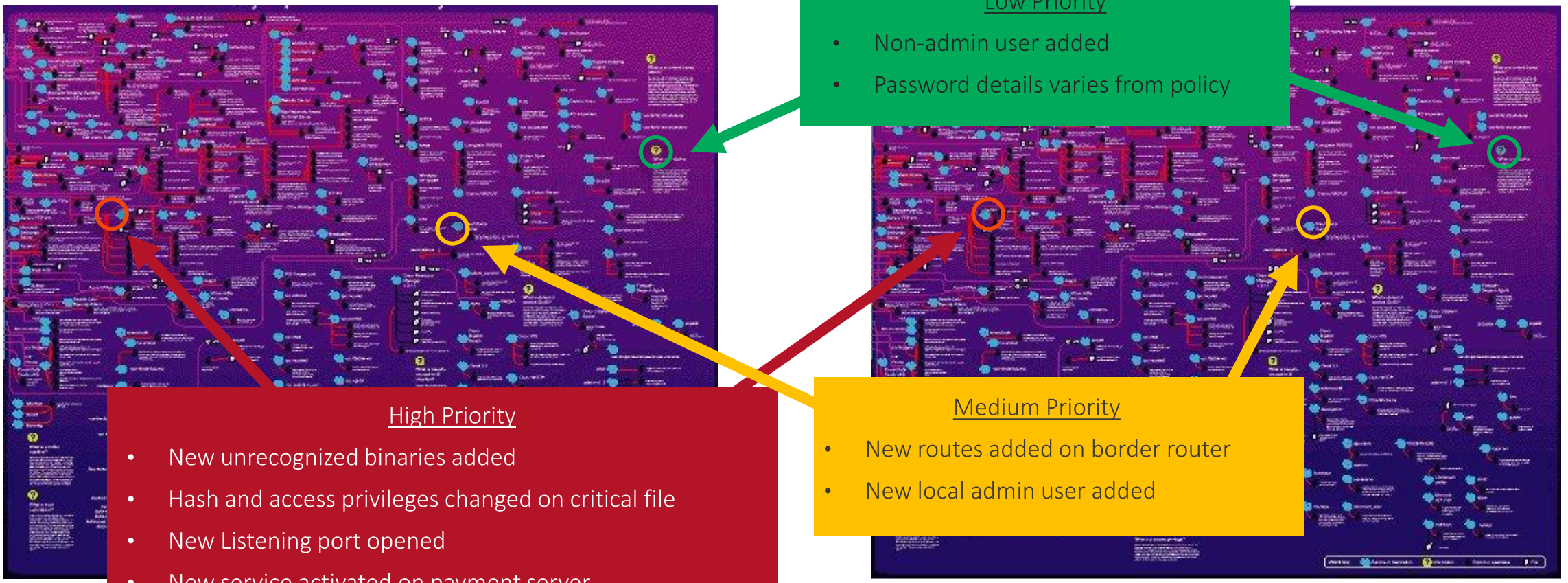
- Audit findings have a direct impact on the bottom line, and noncompliance with regulatory standards can draw the attention of auditors, attackers, and press alike.
- Staying ahead of compliance through continuous assessment is what Tripwire recommends and what Tripwire products can deliver.

The Devil in the Details *(3) Changes Occurred: Low, Medium, High*

Finding the changes that matter

Before

After



Low Priority

- Non-admin user added
- Password details varies from policy

High Priority

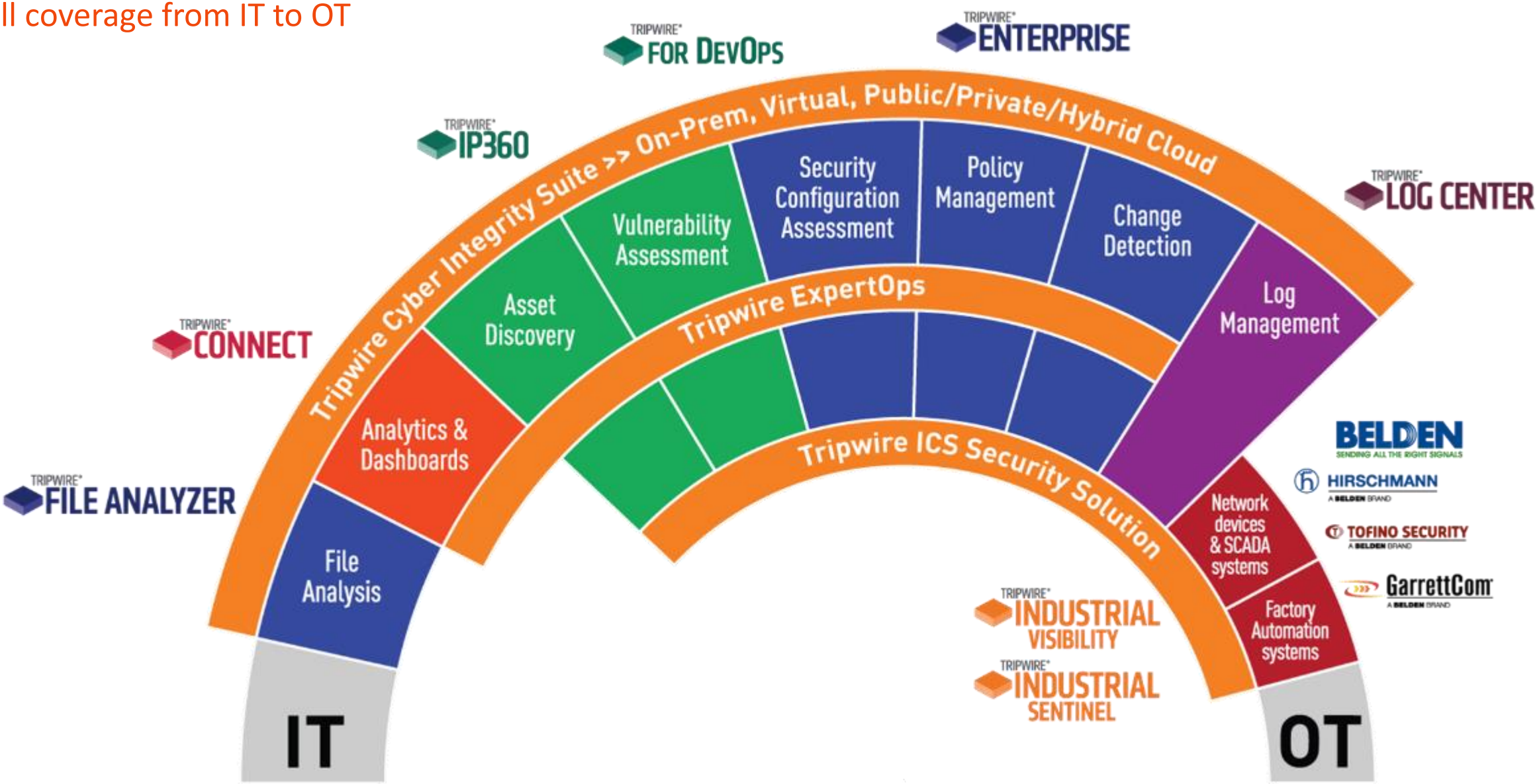
- New unrecognized binaries added
- Hash and access privileges changed on critical file
- New Listening port opened
- New service activated on payment server
- Logging disabled

Medium Priority

- New routes added on border router
- New local admin user added

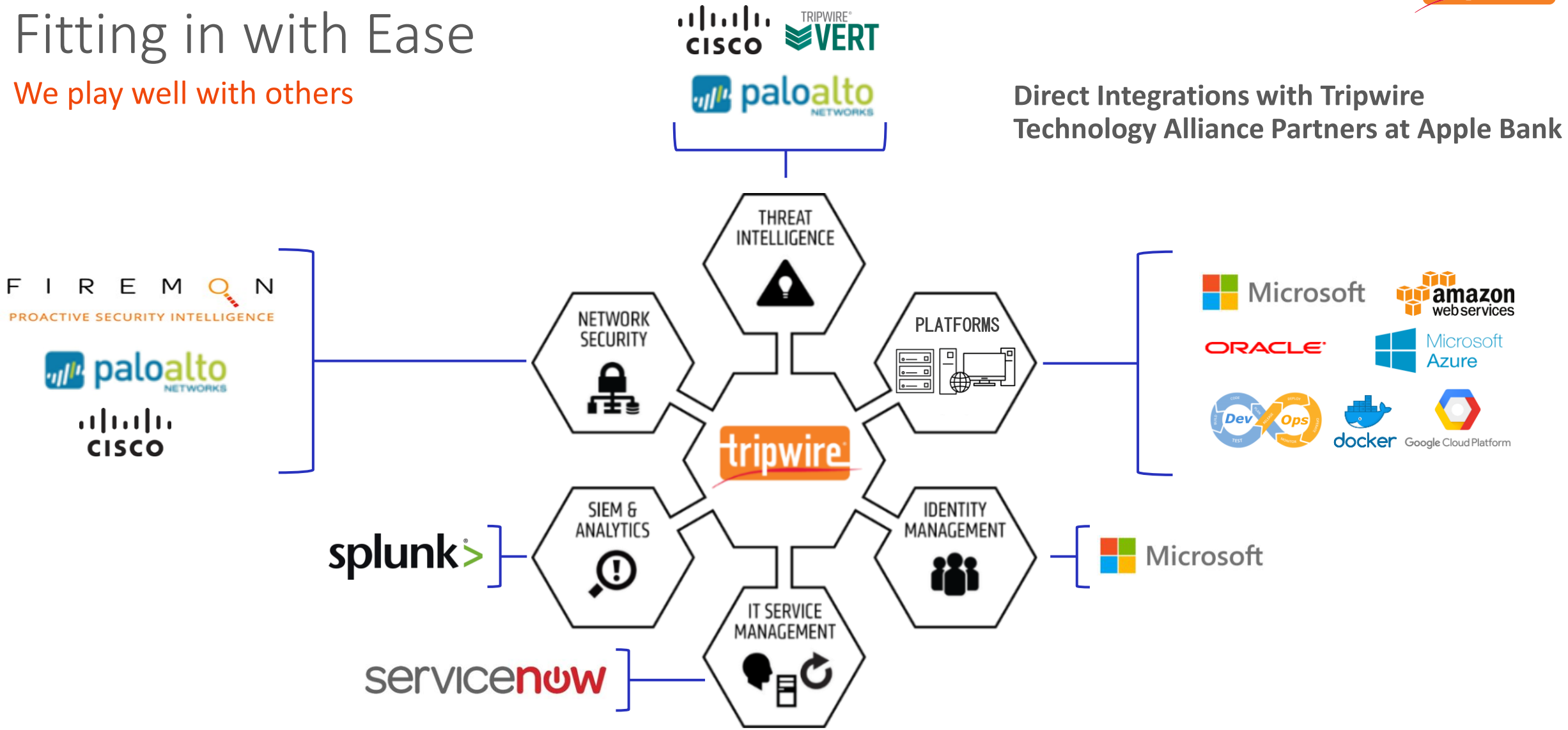
Tripwire's Cyber Integrity Solutions

Full coverage from IT to OT



Fitting in with Ease

We play well with others



Tripwire is the leader in Integrity Assurance

Robust Integrity monitoring and assurance, beyond traditional FIM and SCM

REAL-TIME DETECTION

Shortens the time it takes to catch and limit damage from threats, anomalies, and suspicious changes.

DEEP SYSTEM VISIBILITY

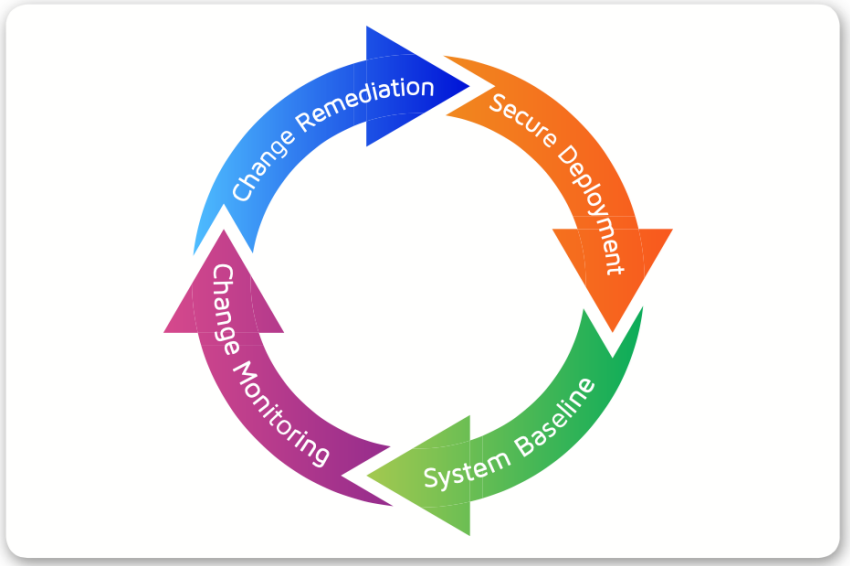
Gives you deep, unparalleled visibility into your security system state and know your security posture at all times.

EXTENSIVE APP INTEGRATIONS

Closes the gap between IT and security by integrating with both teams' existing toolsets.

AUTOMATED COMPLIANCE

Out-of-the-box platforms and policies enforce regulatory compliance standards.



TRIPWIRE® ENTERPRISE

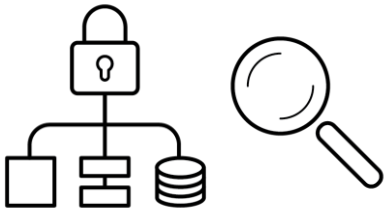
Tripwire Enterprise:

Winner of Two SC Media Awards in 2019

BEST RISK MANAGEMENT / REGULATORY COMPLIANCE SOLUTION

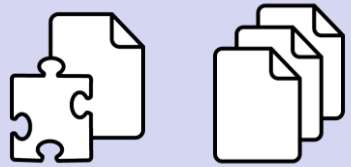
REGULATORY COMPLIANCE TOOLS AND SOLUTIONS

Tripwire Enterprise Policy Management Solution



Scope

- Asset Tagging
- Smart Node Groups
- World's Largest Policy Library

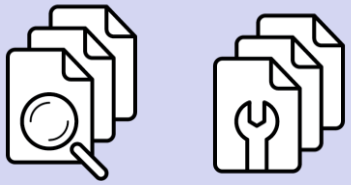


Baseline

- Establish initial baselines for assets
- Detect changes from the baseline
- Monitor the elements for included policies

Measure

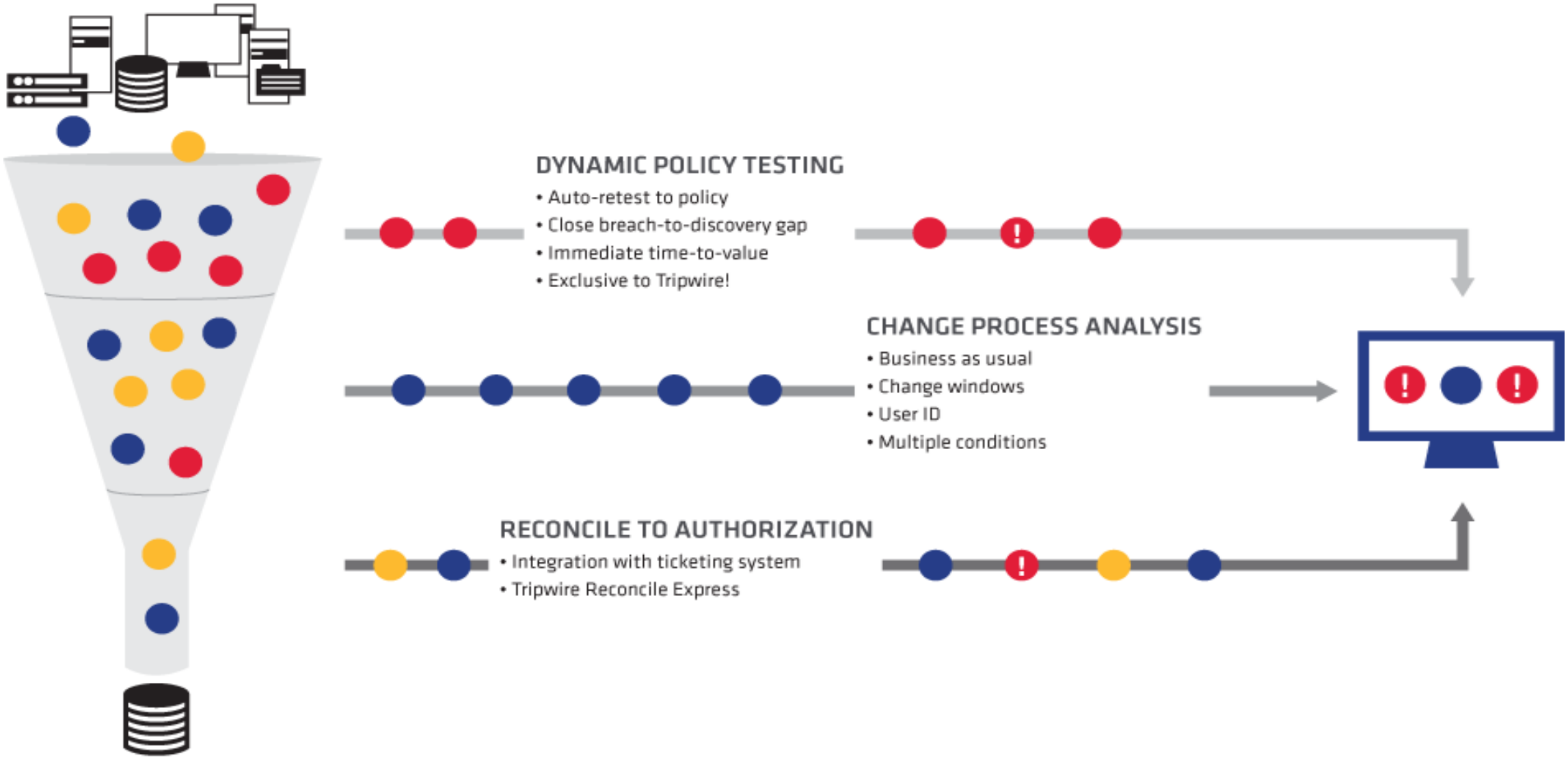
- View deviations from baseline
- Report on policy compliance
- Proactively alert on changes
- Policy compliance dashboards



Remediate

- Detailed change data, including who made a change
- Remediation guidance included

Change Detection and Integrity Monitoring



With Tripwire Security Configuration Management

You Always Know…

Current System State

- Baselining Systems Tells You What You Currently Have
- Files, Registry, Database Configurations, Network Devices, Active Directory

Desired System State

- Security Policies Can Define Your Desired State
- Industry Standard Hardening, Compliance, Self-Created

How To Transition From Current To Desired State

- Compare Your State To Desired and Correct Differences
- Assessment, Deviations, Variance, Remediation, Automation

When Desired State Changes

- Agent and Agentless Change Detection
- Scheduled Scanning & Real Time

Why Things Changed?

- Deep Change Inspection
- Who, What, When, Where, Detailed Content, Change Management Processes

Are Changes Good or Bad?

- Sources Of Truth
- Change Windows, Patch Reconciliation, BAU, CMDB Reconciliation, Threat Intel

How To Respond and Share

- Inspect, Take Action, Report
- Historical Changes, Remediation / Mitigation Guidance, Audit Ready, Change Dashboards

What Makes FIM “true” FIM?

File Integrity Manager is true FIM

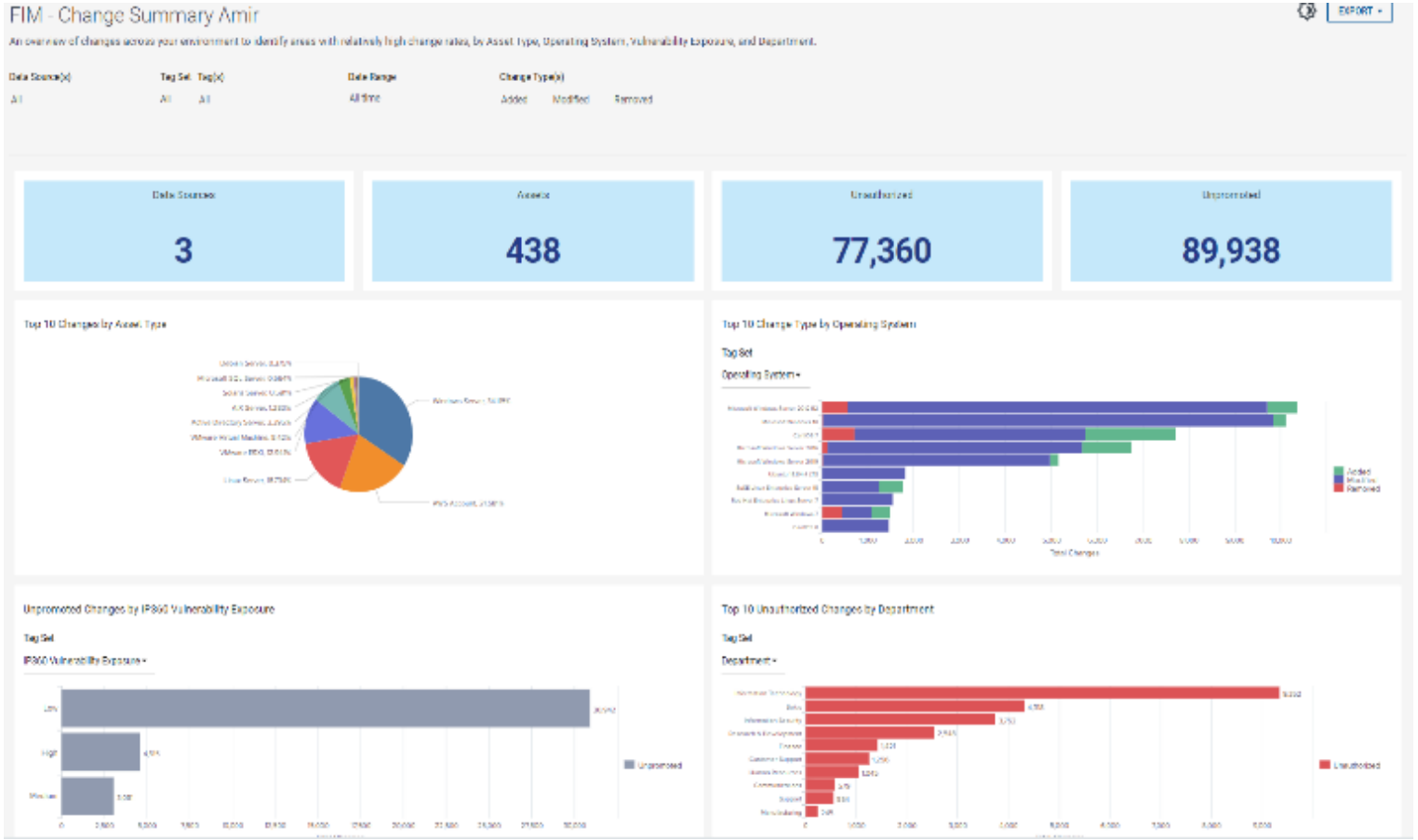
- True FIM detects change by first establishing a highly detailed baseline version of each monitored file or configuration in a known and trusted state
- Using real-time monitoring, it detects change to any aspect of the file or configuration and captures these in subsequent versions
- Versions provide critical before-and-after views that show exactly who made the change, what changed, and more.
- True FIM also applies change intelligence to each change to determine if it impacts integrity (for example, rules that determine if the change takes a configuration out of policy or is one that is typically associated with an attack)

FIM – Change Summary

An overview of changes across your environment to identify areas with relatively high change rates

Questions answered:

- Do certain asset types have more system changes than others?
- Which asset groups have the most unauthorized change in my environment?



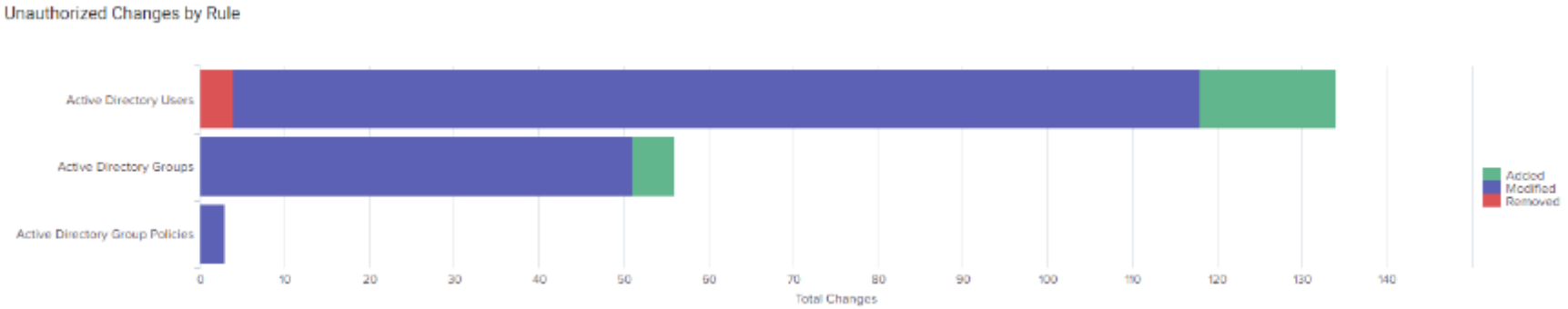
Change Dashboards & Reporting - AD

FIM – Unauthorized Changes

An Overview of Changes to Active Directory Users, Groups and Group Policies.

Questions answered:

How many Total Unauthorized Changes have been Added, Modified, and or Removed?



RED - Number of REMOVED Elements.
BLUE - Number of MODIFICATIONS
GREEN - Number of Added Elements

FIM – Unauthorized Changes %

How many Unauthorized Changes have been Added, Modified, and or Removed. And Total Change Count

Rule Type	Rule Name	Last Element Check Date	Added	Modified	Removed	Total Changes	Unauthorized Change %
Active Directory Rule	Active Directory Users		16	114	4	134	56.7%
Active Directory Rule	Active Directory Groups		5	51	0	56	48.2%
Active Directory Rule	Active Directory Group Policies		0	3	0	3	0.0%

Change Dashboards & Reporting AD

Attribute	Jan 12, 2021 10:31:27 AM	May 22, 2021 2:00:08 AM
member	CN=Administrator,CN=Users,DC=tripwire,DC=local CN=svc_ip360_scan,OU=Service Accounts,OU=Tripwire,DC=tripwire,DC=local CN=svc_teadmon,OU=Service Accounts,OU=Tripwire,DC=tripwire,DC=local	CN=Administrator,CN=Users,DC=tripwire,DC=local CN=John Salmi,CN=Users,DC=tripwire,DC=local CN=svc_ip360_scan,OU=Service Accounts,OU=Tripwire,DC=[illegible]wire,DC=local CN=svc_teadmon,OU=Service Accounts,OU=Tripwire,DC=trip[illegible]e,DC=local
memberOf	CN=Administrators,CN=Builtin,DC=tripwire,DC=local CN=Denied RODC Password Replication Group,CN=Users,DC=tripwire,DC=local	CN=Administrators,CN=Builtin,DC=tripwire,DC=local CN=Denied RODC Password Replication Group,CN=Users,DC[illegible]ripwire,DC=local

FIM – Change Details
WHO CHANGED it?

Change Type	Changed By
Modified	TRIPWIRE\twireadmn
Modified	NA\twireadmn
Modified	NA\twireadmn
Added	NA\twireadmn
Modified	NA\twireadmn

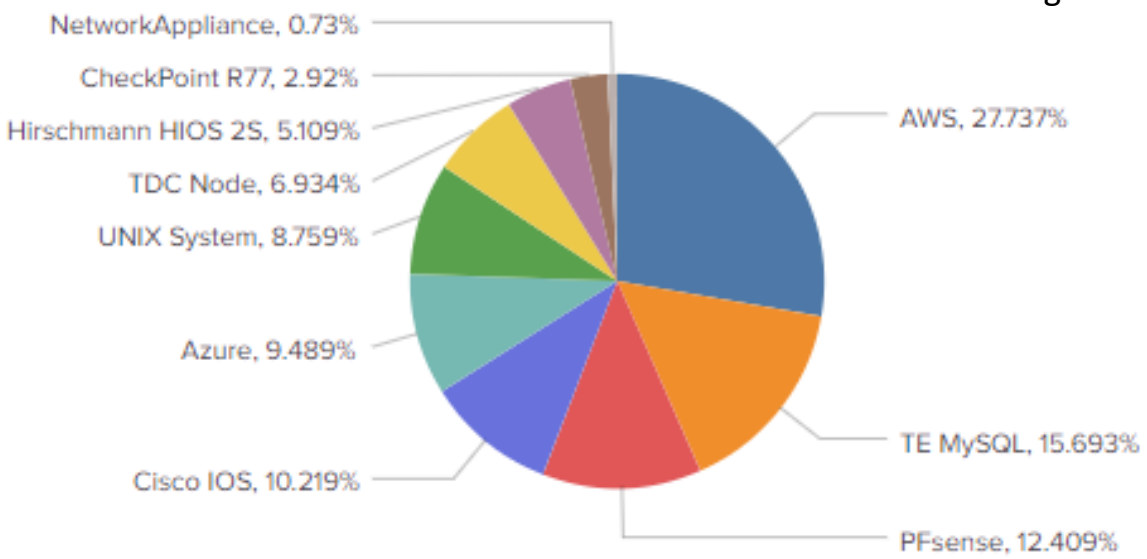
FIM – Change Details
WHAT CHANGED?

Detailed Changes by Element

Data Source	Asset Name	Element Name
TE SE Demo Lab	dc01.tripwire.local	CN=Domain Admins,CN=Users,DC=tripwire,DC=local
TE SE Demo Lab	dc02.na.tripwire.local	CN=LinuxNonRootUsers,OU=Security Groups,OU=Tripwire,DC=na,DC=tripwire,DC=local
TE SE Demo Lab	dc02.na.tripwire.local	CN=LinuxRootUsers,OU=Security Groups,OU=Tripwire,DC=na,DC=tripwire,DC=local
TE SE Demo Lab	dc02.na.tripwire.local	CN=Splunk Read Only Users,OU=Security Groups,OU=Tripwire,DC=na,DC=tripwire,DC=local
TE SE Demo Lab	dc02.na.tripwire.local	CN=TE Custom SE Admin User Group,OU=Security Groups,OU=Tripwire,DC=na,DC=tripwire,DC=local

Change Dashboards & Reporting Network Devices

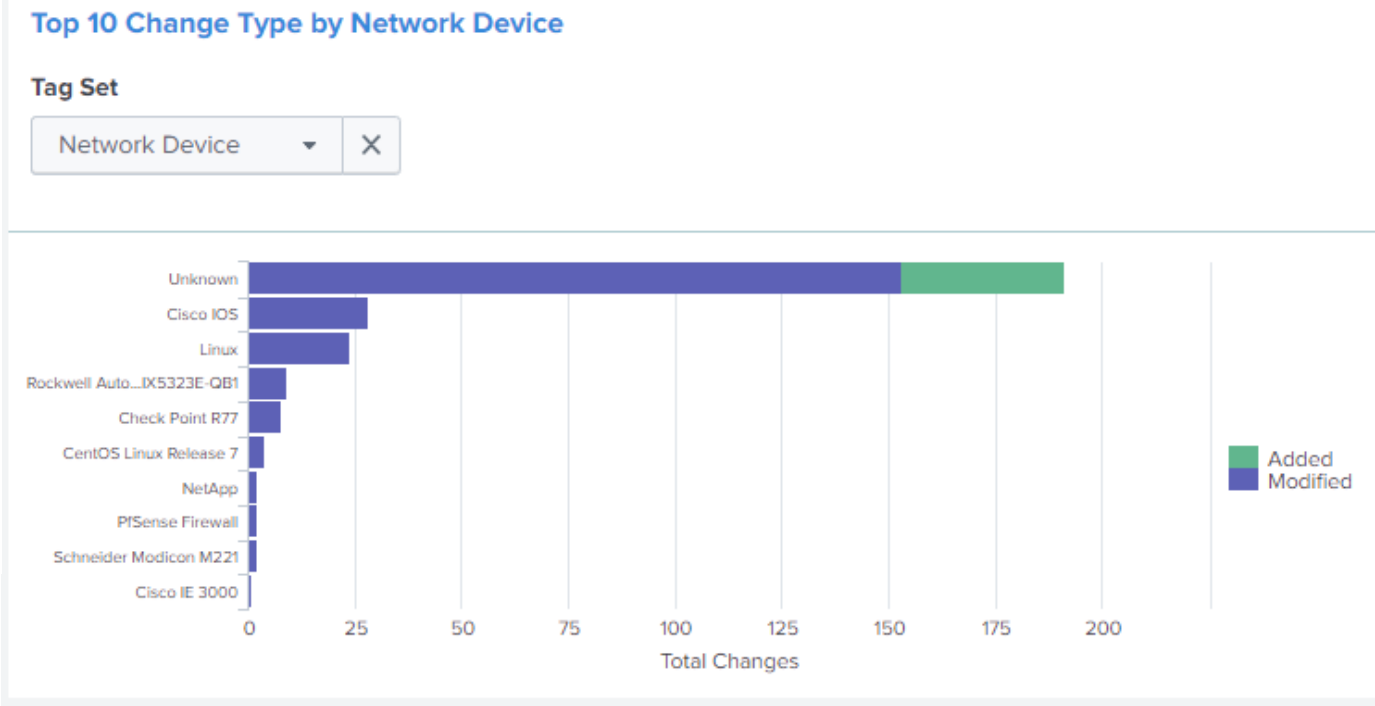
Top 10 Changes by Asset Type



FIM – Unauthorized Changes %

Percent of Changes to devices by Asset Network devices tag sets.

Top 10 Change Type by Network Device



1.Device Setup
1.1 General Settings 2
1.1.1 Ensure 'Login Banner' Is Set
1.1.2 Ensure 'Enable Log on High DP Load' Is Enabled
1.2 Management Interface Settings 2
1.2.3 Ensure HTTP and telnet Options Are Disabled for the Management Interface 2
1.2.3.1 Verify That Telnet Option Is Disabled for the Management Interface
1.2.3.2 Verify That HTTP Option Is Disabled for the Management Interface
1.3 Minimum Password Requirements 11
1.3. 1 Ensure 'Minimum Password Complexity' Is Enabled
1.3. 2 Ensure 'Minimum Length' Is Greater than or Equal to 12
1.3. 3 Ensure 'Prevent Password Reuse Limit' Is Set to 24 or More
1.3. 4 Ensure 'Required Password Change Period' Is Less than or Equa

1 Management Plane 47
1.1 Local Authentication, Authorization and Accounting (AAA) 12
1.1. 1 Enable 'aaa new-model'
1.1. 2 Enable 'aaa authentication login'
1.1. 3 Enable 'aaa authentication enable default'
1.1. 4 Set 'login authentication' for 'line con 0'
1.1. 5 Set 'Login Authentication for 'line tty'
1.1. 6 Set 'login authentication for 'line vty'
1.1. 7 Set 'login authentication' for 'ip http'
1.1. 8 Set 'aaa accounting' to Log All Privileged Use Commands Using 'commands 15'
1.1. 9 Set 'aaa accounting Connection'
1.11.1.11 Set 'aaa accounting Network'
1.1.12 Set 'aaa accounting System'

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: Provides a sampling of the type of IT configuration these solutions may monitor.

Beyond FIM: Policy Compliance Management

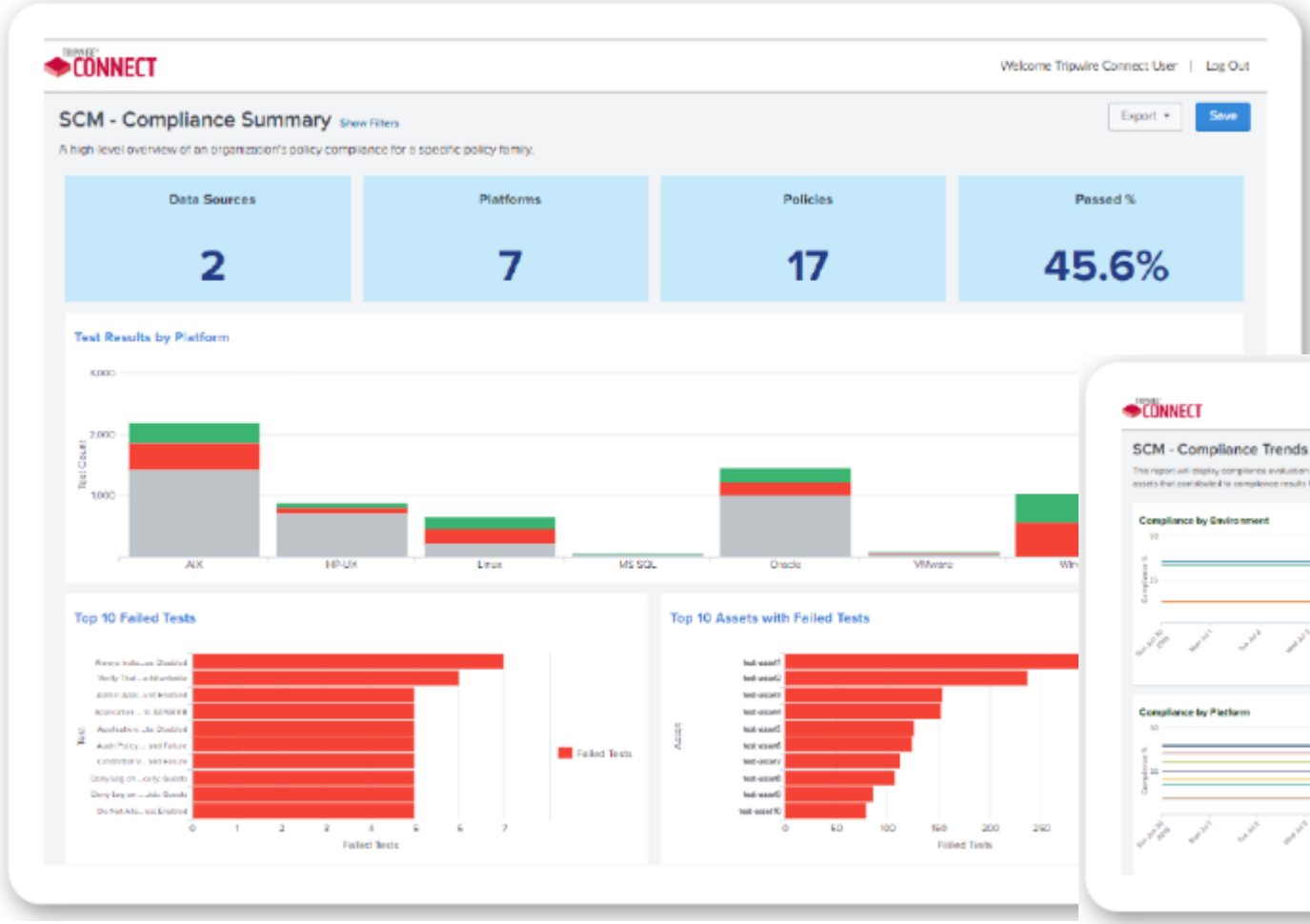
Compliance policy management ensures the integrity of your IT configurations by proactively comparing them against internal policies or external policies for standards, regulations and security best practices.

COMPLIANCE POLICY MANAGEMENT REQUIREMENTS

- Superior file integrity monitoring—FIM that includes compliance policy management—requires not only the detection and reporting of unauthorized changes, specific types of changes, changes made under certain conditions and user-specified severity of changes
- It must also perform an assessment of how an existing—or just changed—configuration compares with established organizational and regulatory guidelines
- **Tripwire's robust library includes ~1,000 policies geared towards measuring adherence against standards, regulations and security best practices**

COMPLIANCE POLICY MANAGEMENT	Y / N
Ability to compare an asset's configuration state against a pre-defined policy to determine whether or not the configuration is compliant.	
Seamlessly integrates with file integrity monitoring data to immediately reassess upon detected changes (continuous compliance).	
Vendor supplied policy templates.	
Supports Center for Internet Security (CIS) benchmarks out-of-the-box.	
Supports security standards (NIST, DISA, VMware, ISO 27001) out-of-the-box.	
Supports regulatory requirements (PCI, SOX, FISMA, FDCC, NERC, COBIT) out-of-the-box.	
Supports operational/performance policies out-of-the-box for business-critical applications.	
Ability to easily modify standard policies to conform to unique organizational needs.	
Capture and automate own organizational (internal) policies.	
Ability to assess all the same platforms on which you are tracking changes, i.e. operating systems, network devices, data bases, directory servers, etc.	
Provides out-of-the-box remediation guidance to help fix non-compliant configurations.	
Ability to systematically waive policy tests to seamlessly integrate into compliance processes and requirements.	
Ability to detect and ignore files that are in a policy, but are not on the monitored system.	
Ability to run assess configurations against existing data without requiring a rescan.	
Ability to use same scan data in multiple, different policy checks without requiring a rescan.	
Provides proof to management that various departments are in compliance with set security policies.	
Ability to report "policy scorecards" to summarize the compliance status of a device.	
Ability to assign different weights to different tests that comprise a policy scorecard.	
Ability to ignore certain tests for certain periods of time (i.e. support for policy waivers).	
Ability to report on current policy waivers in effect and their expiration dates.	

SCM Dashboards & Reporting



SCM – Compliance Summary

High-level overview of an organization's policy compliance for specific policy family

Questions answered:

- Which policy platform has the highest number of failed policy tests?
- Which policy tests have the most failures in my environment?
- What are the top 10 assets with failed policy tests?

SCM – Compliance Trends

This report displays trends of historical policy compliance across the environment or groups of assets.

Questions answered:

» Has my overall policy compliance improved or gotten worse over time?

» Has my compliance for a specific policy improved or gotten worse over time?

SCM Policy Tests - Change to Policy Configurations

Test Details

Policy Name	MS Windows Server 2019 DC - CIS v1.1.0 Level 1	**Asset Compliance Score**	
Asset Name	dc01.tripwire.local	**91.3%**	
Data Source	TE SE Demo Lab		

Policy Test Name	Windows Firewall Domain - Display Notifications: No	**Policy Test Result**	Passed
Has Waiver	No	**Waiver Name**	[NA]

Policy Test Description

This test verifies that 'Display a notification' in the firewall domain profile is set to no. Disabling this feature will notify and ask permission of the user whenever an application wishes to connect to the network.

Policy Test Remediation

To remediate failure of this policy test, configure the Windows Firewall to prohibit notifications

Modifying the security options policy:

1. Select a group policy object to edit within the **Microsoft Management Console**.
2. Browse to **Computer Configuration > [Policies] > Windows Settings > Security Settings > Windows Firewall with Advanced Security > Windows Firewall with Advanced Security**.
3. In the right panel click **Windows Firewall Properties**, select **Domain Profile** tab.
4. In the **Settings** panel, click **Customize...** button.
5. In the **Display a notification:** combo box of the **Firewall settings** panel, select **No**, and then click **OK** button twice.
6. Run the **gpupdate** command to apply the change.

Note:

- To perform this procedure you must be a domain administrator.
- Tests may continue to fail until the domain refreshes the setting configured above.
- When you change a security setting and click **OK**, that setting will take effect in the next refresh of settings, or after reboot.
- The security settings are refreshed every **90 minutes on a workstation or server** and every **5 minutes on a domain controller** . The settings are also refreshed every 16 hours, whether or not there are any changes.

Element Name	HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\WindowsFirewall\DomainProfile\DisableNotifications	**Last Element Check Date**	[NA]	**Element Result**
Expected Value				
If an element version has no content, the condition should:Fail Regular expression: /\((\d+)\)/ (Flags:Case Insensitive) Display Notification Equals 1				Passed
Observed Value				
Display Notification=1				

SCM – Compliance Tests

Policy tests include CIS, NIST, MITRE ATT&CK, SOX and many more.

Questions answered:

- Has my overall policy compliance improved or gotten worse over time?
- Has my compliance for a specific policy improved or gotten worse over time?
- Policy tests are available for Active Director, File Systems, Network Devices. 0ver 1000 combinations.
- Test will show Passed or Failed with a detailed step by Step Remediation Instructions.

Tripwire Enterprise Product Extensions/Apps

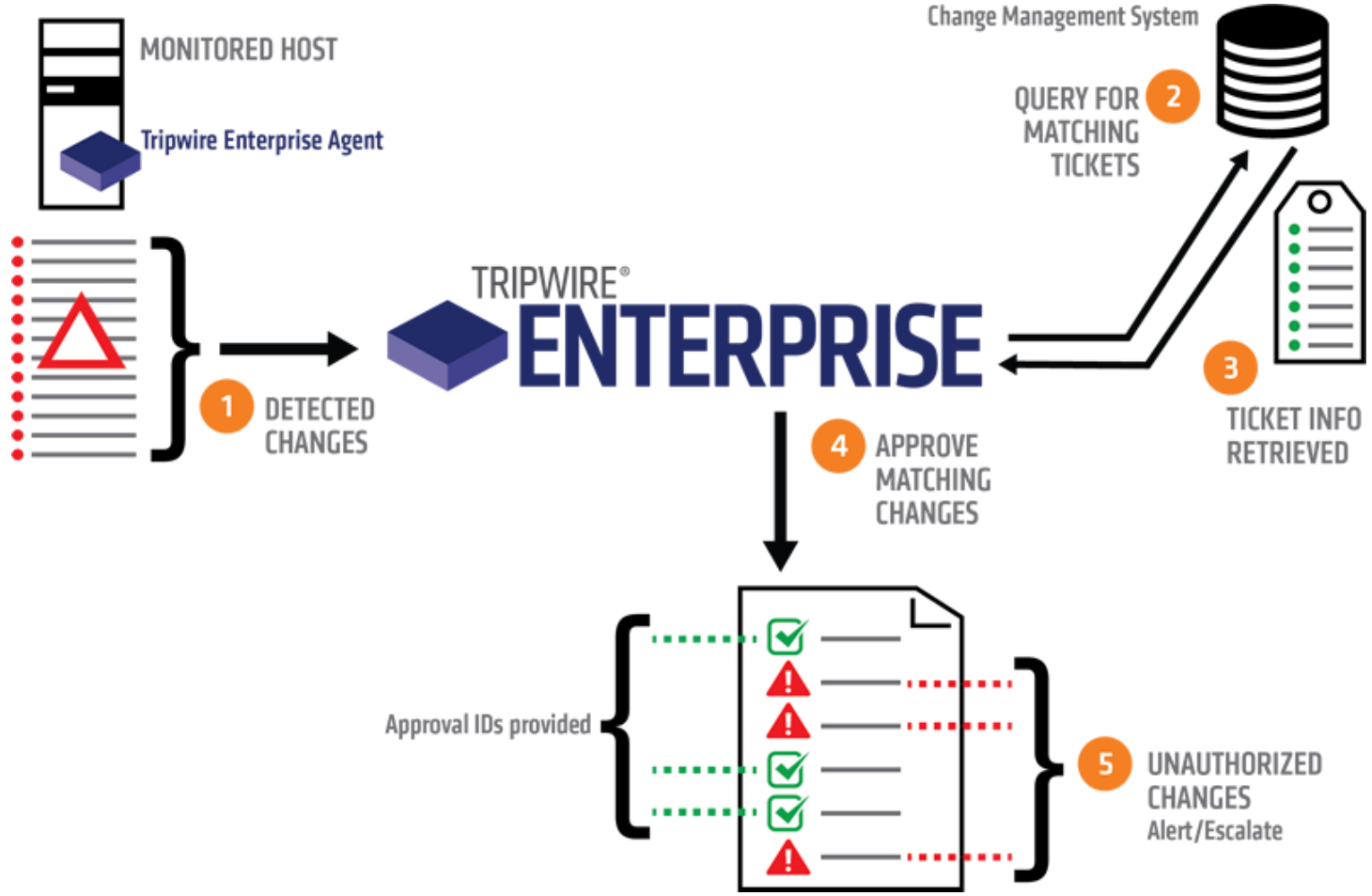
1	**Tripwire Enterprise Integration Framework (TEIF)**– Bi-directional integration with Ticketing provides automation to further differentiate good change from bad change or approved changes from unapproved changes
2	**Dynamic Software Reconciliation (DSR)** - reconciles changes detected by Tripwire against posted MS Windows Updates, Linux RPM changes and user-defined Windows-based software
3	**Tripwire Threat Intelligence Integration** – Tripwire Enterprise provides real-time endpoint and server monitoring and detection, with protection from advanced, evasive, and zero-day exploits through integration with Leading Breach Detection Partners
4	**Tripwire Event Sender -** File integrity and Change data is not available in Log Intelligence solutions/SIEMs. It is difficult to make effective risk-based decisions without complete data, including Who made the change, Exact before and after file configurations, Severity of change

Tripwire TEIF – Tripwire Enterprise Integration Framework

Automated way for systems to directly integrate and communicate with each other. Integrates with Cherwell, ServiceNow, Jira, Remedy, CA, ServiceDesk and more

Benefits

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

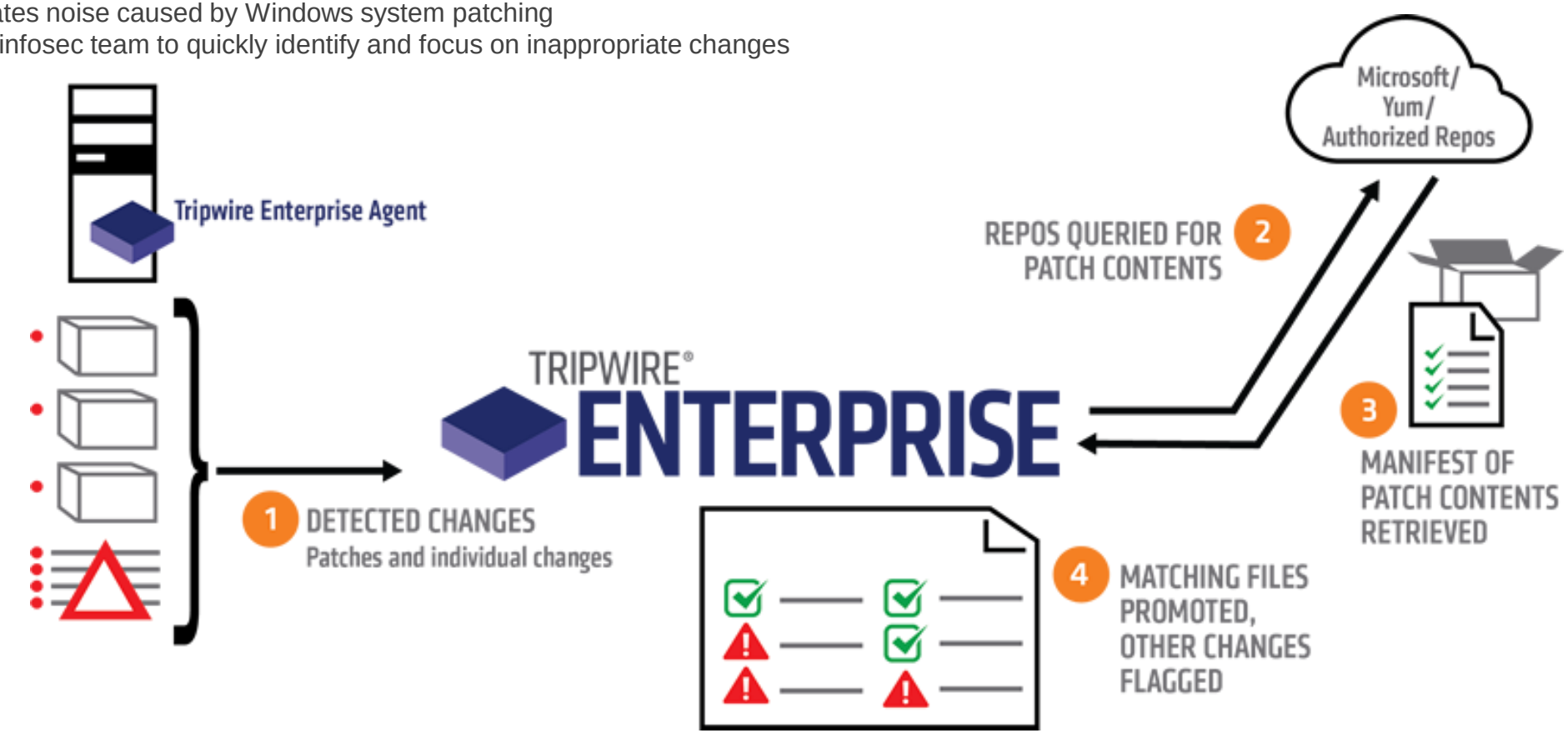


Dynamic Software Reconciliation

Identifies changes made by approved system updates (e.g. Windows Hotfixes), and automatically promotes them within Tripwire

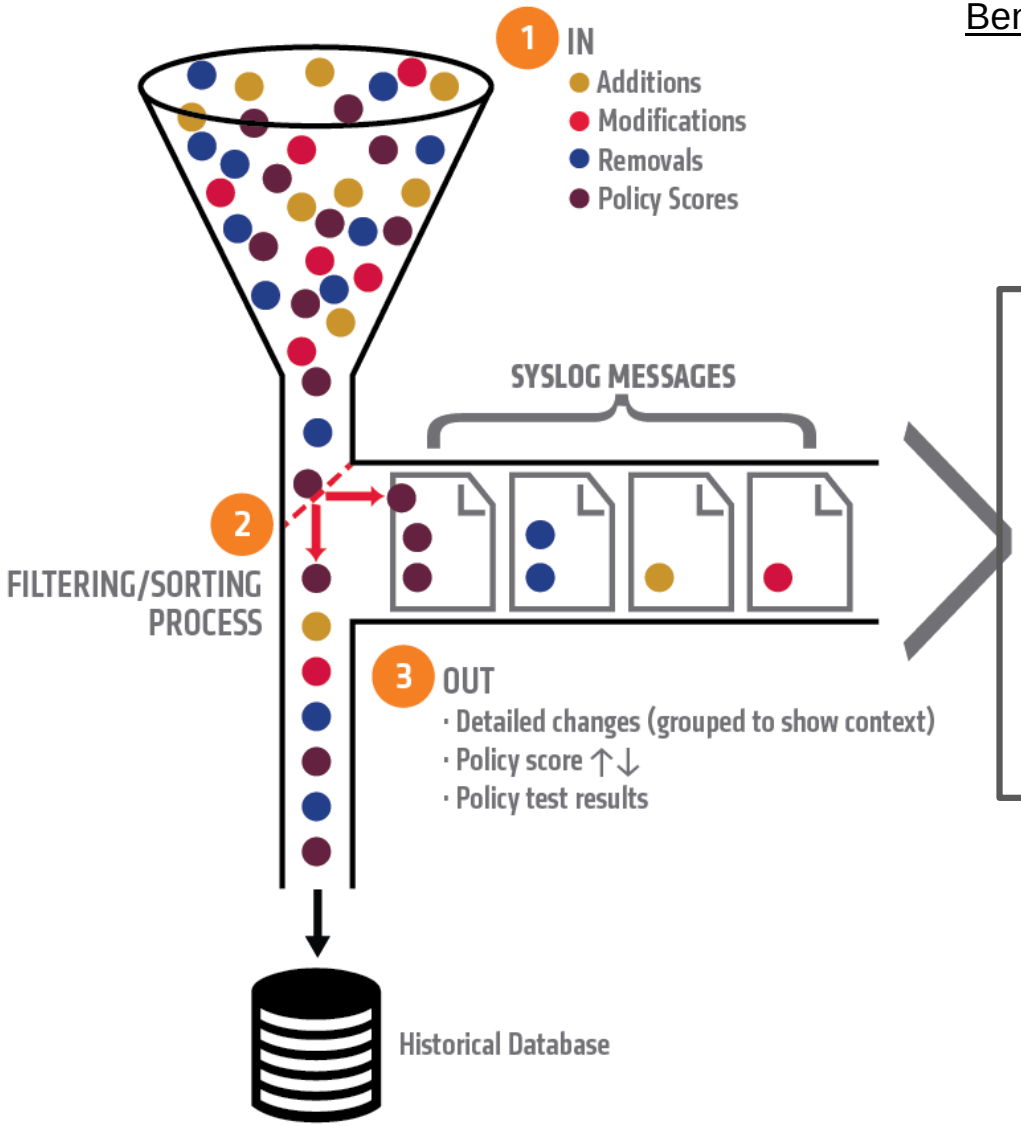
Benefits

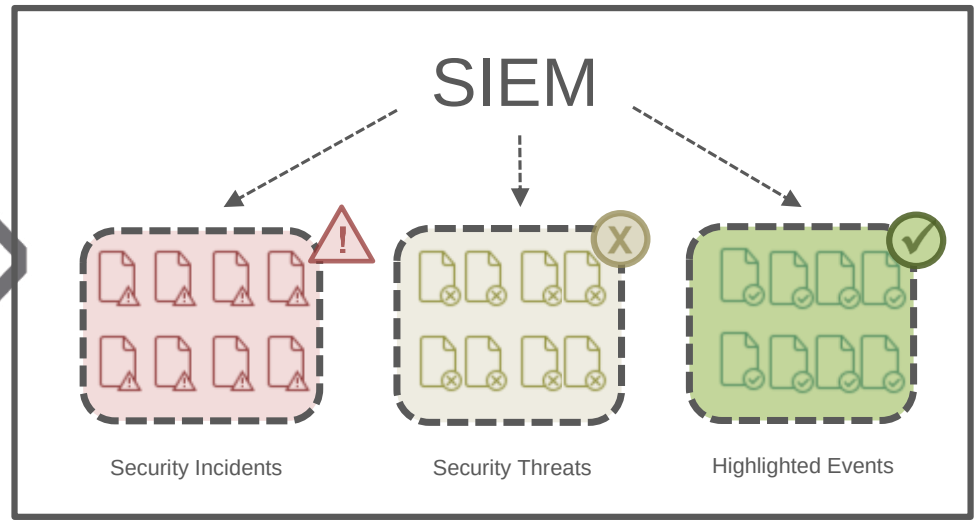
- Eliminates noise caused by Windows system patching
- Allows infosec team to quickly identify and focus on inappropriate changes



Event Sender

Aggregates Tripwire Enterprise change/audit data. Generates events for SIEM collection/correlation.

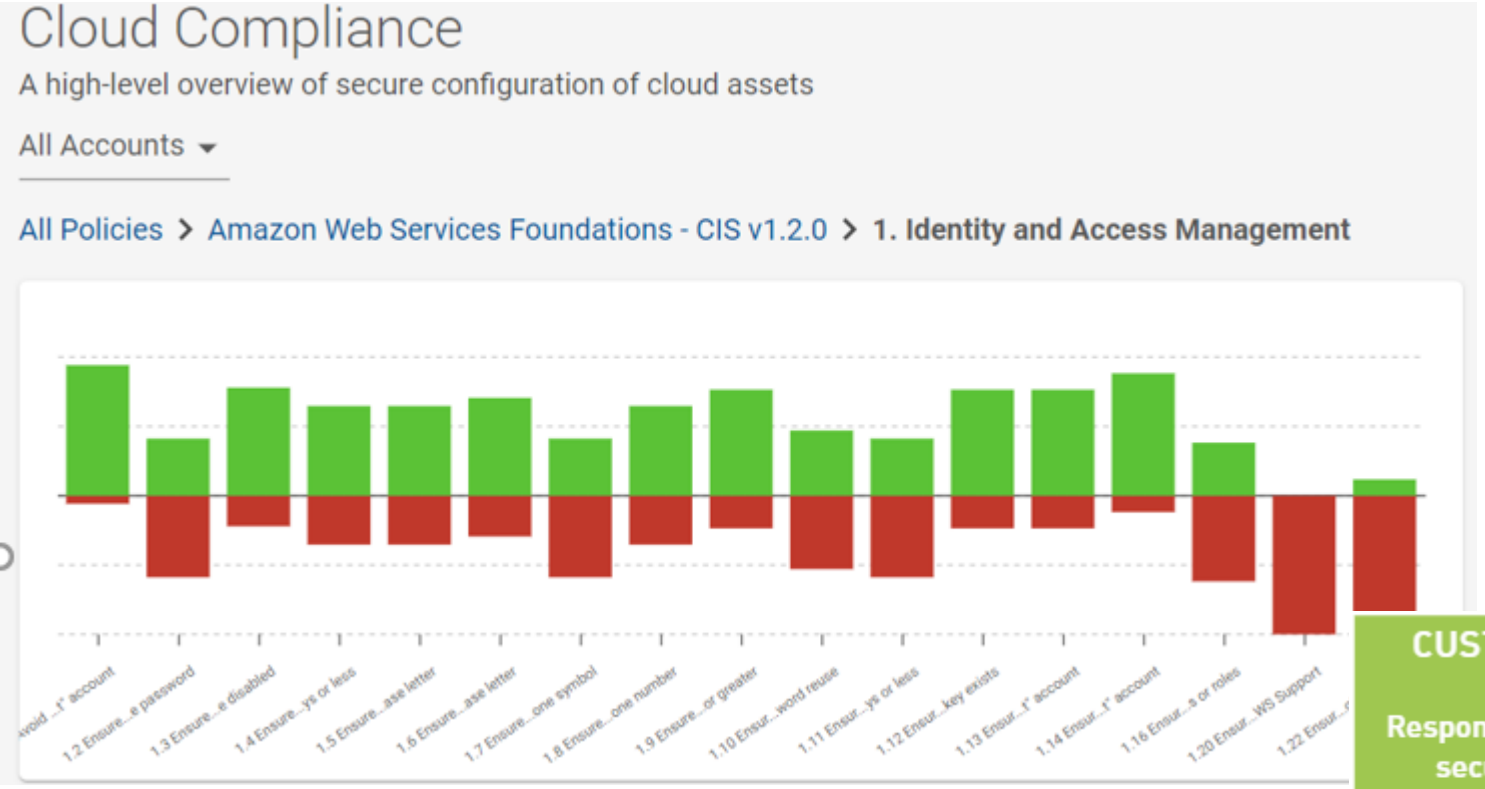




Benefits

- Significantly improves correlation and alerting abilities
- Better identify security risks and operational issues
- Supports ‘single pane of glass’ analysis and workflows

Tripwire Configuration Manager



- Designed to monitor configurations of your cloud accounts and data storage.
- Automatically enforce secure configurations or get step-by-step instructions to make corrections yourself.
- Ensures that your environment is protected by assessing your cloud account configurations against the industry standard Center for Internet Security (CIS) Foundations Benchmarks. AWS, GCP, or Azure.
- Removes the guesswork as to how to best harden your organization's security.
- Shows you a prioritized list of risks across all of your cloud accounts in one consolidated Dashboard.

<table>
<tr><td rowspan="4">CUSTOMER

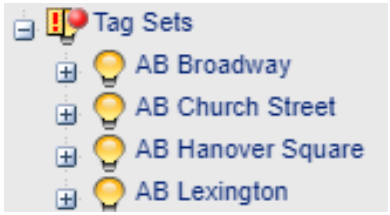
Responsibility for security in the cloud</td><td colspan="4">Customer Data</td></tr>
<tr><td colspan="4">Platform, Applications, Identity & Access Management</td></tr>
<tr><td colspan="4">Operating System, Network & Firewall Configuration</td></tr>
<tr><td>Client-side data encryption & Data integrity authentication</td><td>Server-side Encryption (file system and/or data)</td><td colspan="2">Networking traffic protection (encryption, integrity, identity)</td></tr>
<tr><td rowspan="4">AWS

Responsibility for security of the cloud</td><td colspan="4">Software</td></tr>
<tr><td>Compute</td><td>Storage</td><td>Database</td><td>Networking</td></tr>
<tr><td colspan="4">Hardware/AWS Global Infrastructure</td></tr>
<tr><td>Regions</td><td>Availability Zones</td><td colspan="2">Edge Locations</td></tr>
</table>

Tripwire Axon Agent Benefits

Axon Agent
Automatically places nodes into Smart Node Groups based on OS.

Tag Sets
Assign tags to a group of assets such as Location, Department, Business Unit, Function, Risk, Application, IT Policy, Staging, Production, etc.



Modular pluggable architecture

- Supports Tripwire portfolio and easy to update

Efficient and Fast collection and access architecture

- For deep and broad data capture and response

Resilient design

- Self-healing agent and offline or connected data collection and transmission

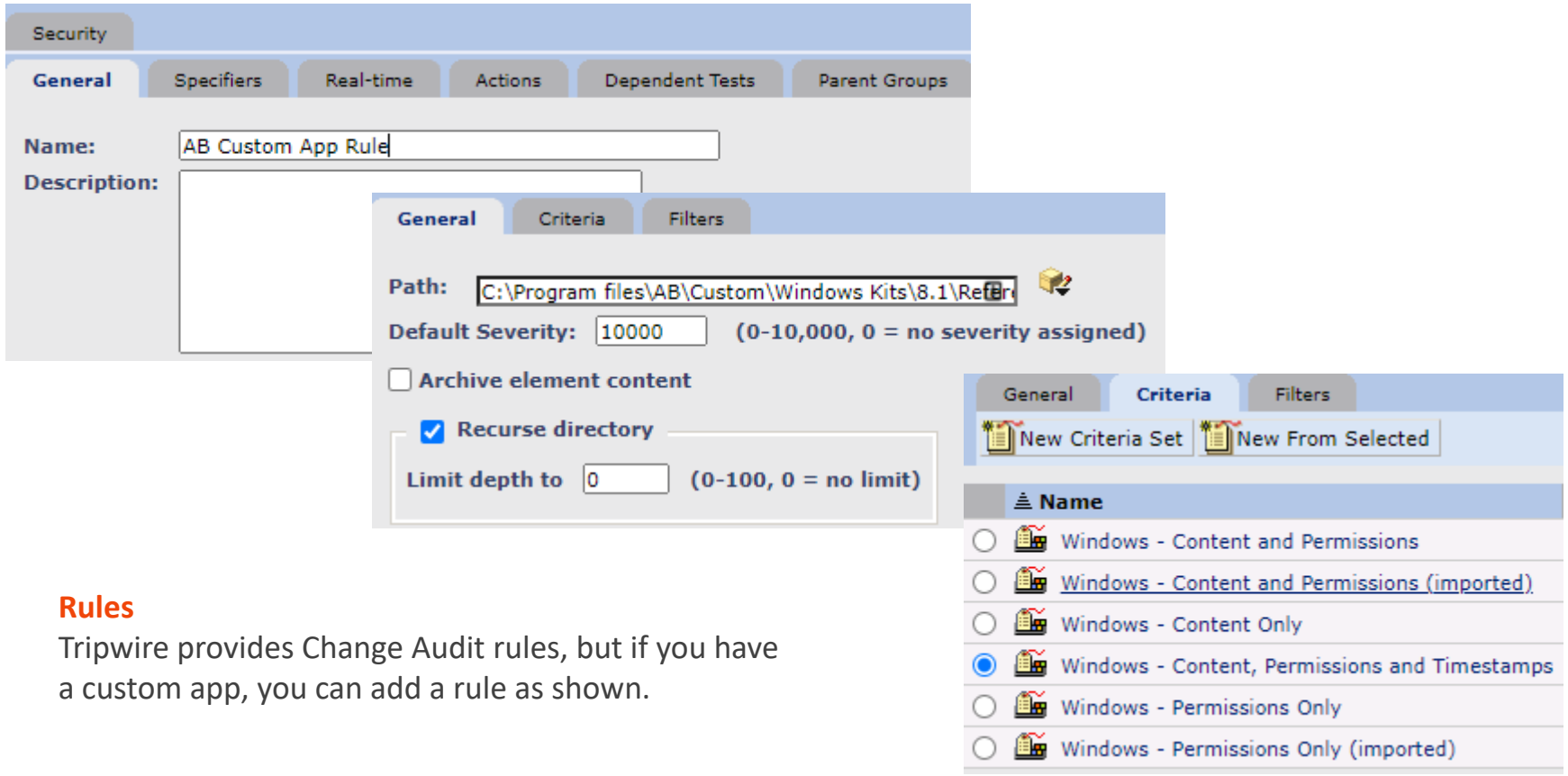
Extensible and Scalable

- For emerging platforms, services and applications

Lean and Agile

- Consumes fewer endpoint & network resources while delivering vital functionality

Creating Custom Rules



Rules

Tripwire provides Change Audit rules, but if you have a custom app, you can add a rule as shown.

Tripwire Content

Example of Windows Change Audit rules ready for use on Customer Center.

NAME
MITRE Detection Rules - MS Windows
Critical Change Audit Rules - MS Windows 2019
Critical Change Audit Rules - MS Windows 2016
Critical Change Audit Rules - MS Windows
Change Audit Rules - MS Windows 2008 R2
Change Audit Rules - MS Windows 2019
Change Audit Rules - MS Windows 2016
Change Audit Rules - MS Windows 10
Change Audit Rules - MS Windows 2012 R2
Change Audit Rules - MS Windows 8.1
Change Audit Rules - MS Windows 8
Change Audit Rules - MS Windows 2008
Change Audit Rules - MS Windows 2012
Change Audit Rules - MS Windows 7

Tripwire Technology Alliance Partners and API

TAP partners for Tripwire platforms

Integration:

Tripwire provides integrations with many partners using Tripwire Professional services, Rest API, or existing Apps with partners.

REST API

nodes Show/Hide | List Operations | Expand Operations

GET	/nodes	Search nodes (since 1.3)
POST	/nodes	Create a node (since 1.11)
POST	/nodes/agentUpgradeRequests	Upgrade agents on nodes (since 1.16)
GET	/nodes/agentUpgradeRequests/{requestId}	Get the status of an agent upgrade request (since 1.16)
POST	/nodes/createTag	Create a tag (since 1.20)
GET	/nodes/customPropertyTypes	Search custom property types (since 1.5)
POST	/nodes/customPropertyTypes	Create a node custom property definition (since 1.5)
DELETE	/nodes/customPropertyTypes/{rkCustomPropertyTypeId}	Delete a custom property type (since 1.6)
GET	/nodes/customPropertyTypes/{rkCustomPropertyTypeId}	Get a custom property type (since 1.5)
PUT	/nodes/customPropertyTypes/{rkCustomPropertyTypeId}	Update an existing node custom property type (since 1.6)

Q&A and Next Steps