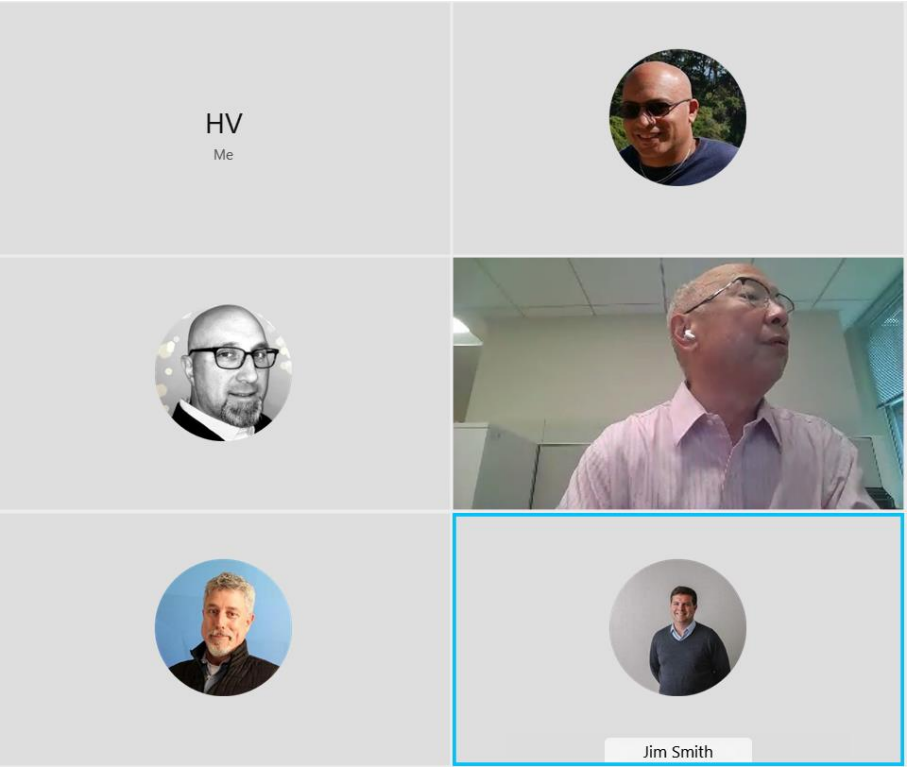


Participants (6)

Search

H HV
Me

Anthony Marusic
Host

Amir Gerges

AL allen lum

Brian Cusack

Jim Smith

Agenda

Covering the following topics

- 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

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

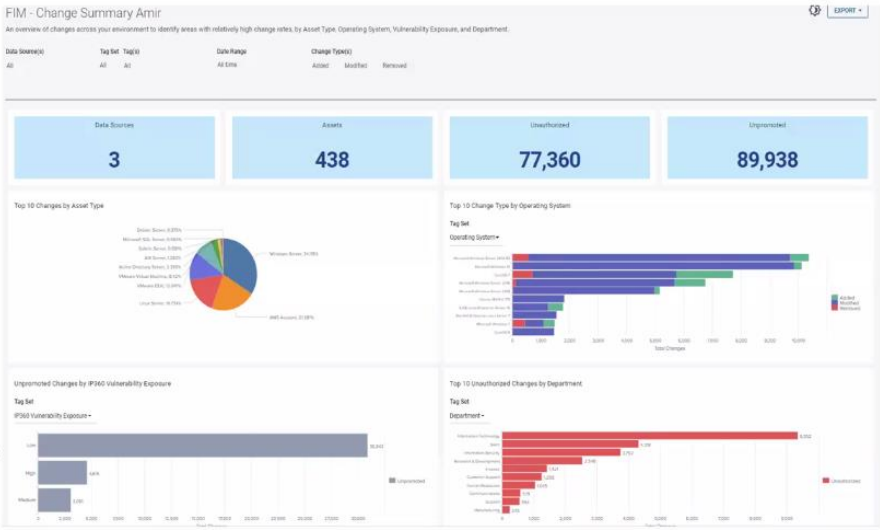
Tripwire Security Configuration Management

Know Your Current System State	• Baselining Systems Tells You What You Currently Have • Files, Registry, Database Configurations, Network Devices, Active Directory
Know your Desired System State	• Security Policies Can Define Your Desired State • Industry Standard Hardening, Compliance, Self-Created
Know How To Transition From Current To Desired State	• Compare Your State To Desired and Correct Differences • Assessment, Deviations, Variance, Remediation, Automation
Know When Your Desired State Changes	• Agent and Agentless Change Detection • Scheduled Scanning & Real Time
Know Why Things Changed	• Deep Change Inspection • Who, What, When, Where, Detailed Content, Change Management Processes
Know If Those Changes Are Good or Bad	• Sources Of Truth • Change Windows, Patch Reconciliation, BAU, CMDB Reconciliation, Threat Intel
Know 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

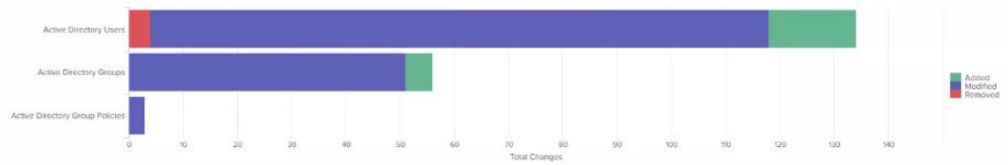
Questions answered:

» 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

Unauthorized Changes by Rule



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

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%

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

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=tripwire,DC=local CN=svc_teadmon,OU=Service Accounts,OU=Tripwire,DC=tripwire,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=tripwire,DC=local

FIM – Change Details
WHO CHANGED it?

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

FIM – Change Details
WHAT CHANGED?

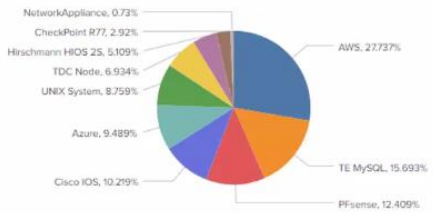
Detailed Changes by Element

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

FIM – Unauthorized Changes %
Percent of Changes to devices by Asset
Network devices tag sets.

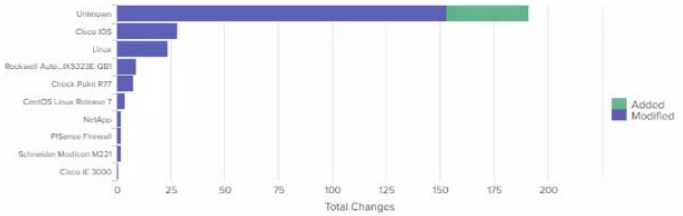
Top 10 Changes by Asset Type



Top 10 Change Type by Network Device

Tag Set

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

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.

Beyond FIM: Policy Compliance Management

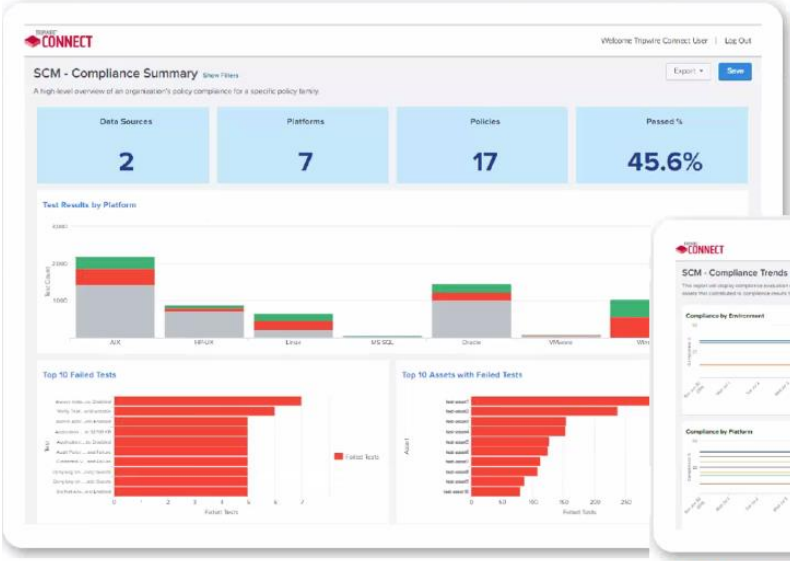
Compliance policy management ensures the integrity of your IT configurations by proactively comparing them against internal policies or external policies for standards, regulations and security best practices.

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

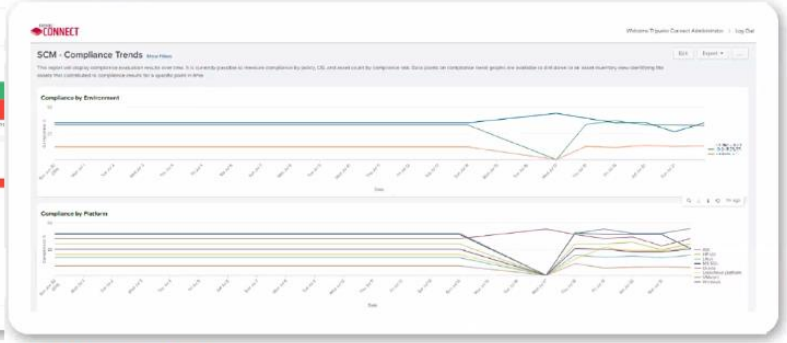


SCM – Compliance Summary

A high-level overview of an organization's policy compliance for a 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

Policy Test Name	Access This Computer from the Network: Administrators, Authenticated Users, Enterprise Domain Controllers	**Policy Test Result**	Failed
Has Waiver	No	**Waiver Name**	[NA]
Policy Test Description	This test determines if the SeNetworkLogonRight right is assigned to Administrators, Authenticated Users, and Enterprise Domain Controller accounts. This right gives users the ability to access resources on the Windows system from anywhere on the system's network.		
Policy Test Remediation	To remediate failure of this policy test, assign the Administrators, Authenticated Users, and Enterprise Domain Controllers groups rights to access this computer from the network. **Modifying user rights assignments**: 1. Select a group policy object to edit within the **Microsoft Management Console**. 2. Select **Computer Configuration > [Policies] > Windows Settings > Security Settings > Local Policies > User Rights Assignment**. 3. Right-click **Access this computer from the network** and select **Properties**. 4. In the **Properties** window, select **Define these policy settings** and in the **Members of this group** panel, select each user and then click **Remove**. 5. Click the **Add User or Group...** button to open the **Add User or Group** window, and then click **Browse...** 6. In the **Enter the object names to select (examples):** box, enter **Administrators**, click **Check Names** to verify the name, and then click **OK** twice to add the **Administrators** group. 7. Repeat steps 5, 6 to add the **Authenticated Users** and **ENTERPRISE DOMAIN CONTROLLERS** groups. 8. Click **OK** to close the **Properties** window. 9. Run the **gpupdate** command to apply the change. **Note**: • To perform this procedure you must be a domain administrator. • If the systems doesn't have **Browse...** button at step 5, please skip this step. For further details, please refer to: http://technet.microsoft.com/en-us/library/dd349804.aspx#BKMK_1		

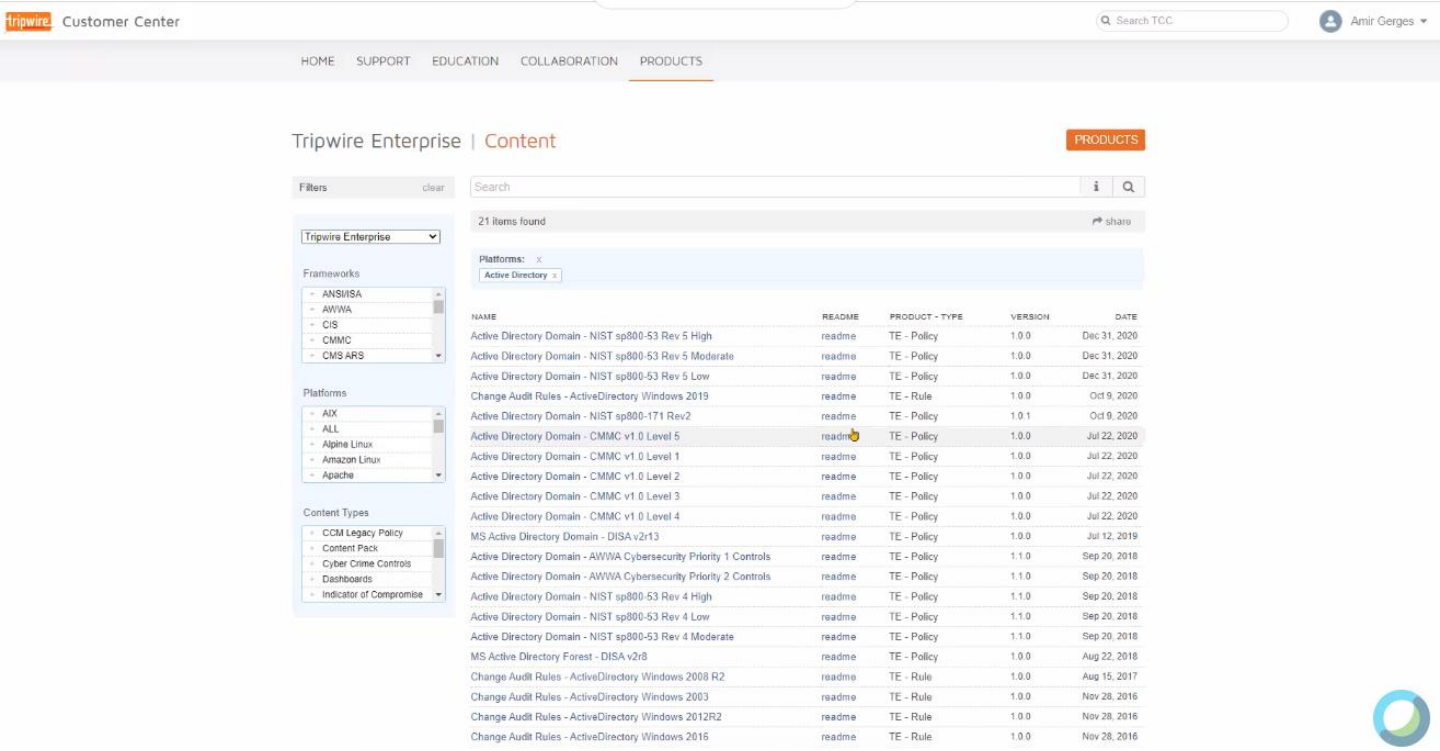
Element Name	Computer	**Last Element Check Date**	[NA]	**Element Result**
Expected Value				Failed
Action if missing:Fail NetworkLogonRight Matches "^\s*BUILTIN\\Administrators\s*,\s*NT\s+AUTHORITY\\Authenticated\s+Users\s*,\s*NT\s+AUTHORITY\\ENTERPRISE\s+DOMAIN\s+CONTROLLERS\s*$"				
Observed Value				
NetworkLogonRight=BUILTIN\Administrators, BUILTIN\Pre-Windows 2000 Compatible Access, Everyone, NT AUTHORITY\Authenticated Users, NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS				

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

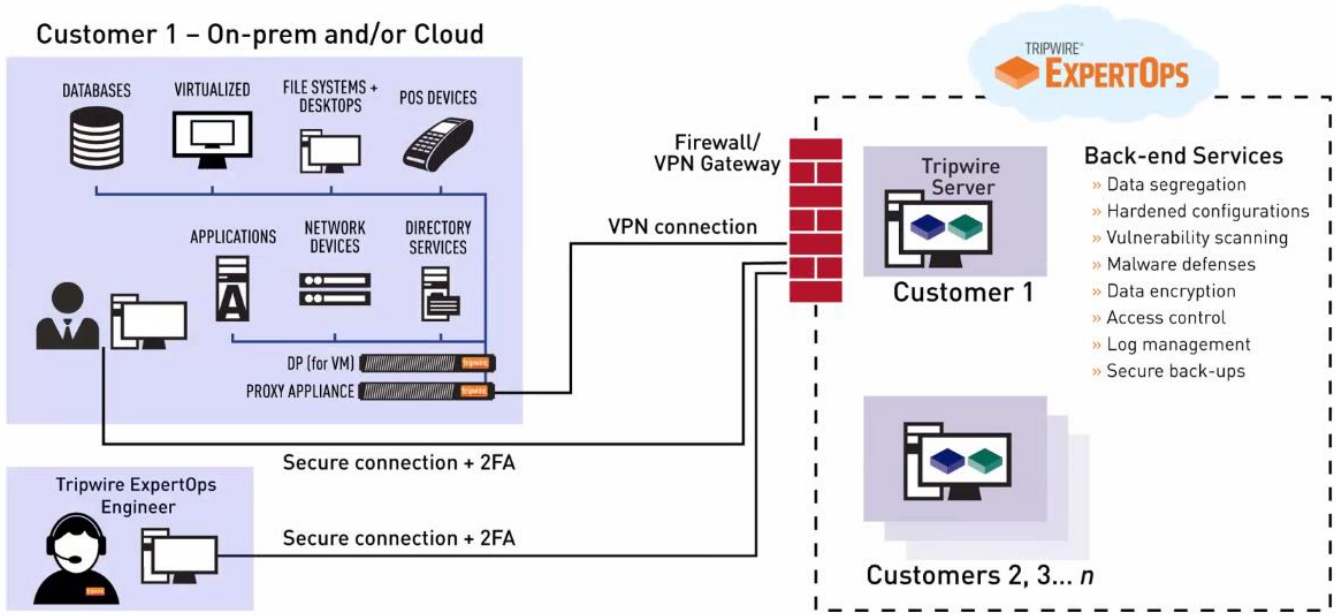
1. **Tripwire Enterprise Integration Framework (TEIF)**– Bi-directional integration with Ticketing provides automation to further differentiate good change from bad change or approved changes from unapproved changes

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

ExpertOps Architecture



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