



Tripwire Connect Report Catalog

December 2020

FOUNDATIONAL CONTROLS FOR
SECURITY, COMPLIANCE & IT OPERATIONS

Introduction

Tripwire® Connect is the highly-customizable analytics, reporting, integration and management platform for Tripwire Enterprise and Tripwire IP360™. Available in both on-prem and SaaS versions, it can deploy and scale according to your organization's needs.

While Tripwire has always provided users an abundance of invaluable security and compliance data, Tripwire Connect extends the value of that data even further by combining information from multiple sources and presenting it in a unified way. Its rich, visual analytics and reports help security teams translate Tripwire solution data into the strategic remediation activities that can most effectively reduce your cyber risk.

This report catalog gives a quick overview of features and file integrity monitoring (FIM), secure configuration management (SCM) and vulnerability management (VM) reports and dashboards. When you're ready for a demo, visit tripwire.com/contact/request-demo and we'll be happy to give you a deeper look into Tripwire Connect.

Key New Features

Ability to Create Custom Report Templates

Create a copy of existing report templates and tailor them to meet your specific reporting needs.

Ad-Hoc Search

Enables administrators to perform SPL queries against the Tripwire Connect indexes to get targeted search results or to test queries to be added to a custom report template.

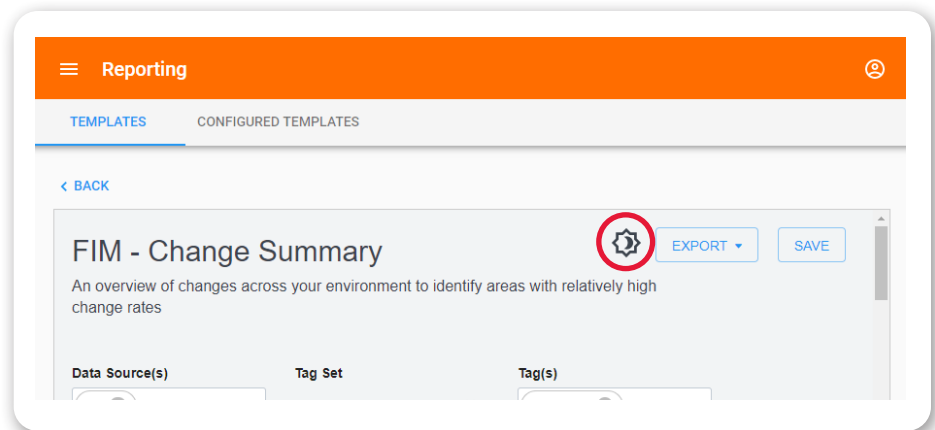
Asset Service for Categorizing Assets

Organize your assets by automatically applying tags based on metadata about the assets and their vulnerability or compliance scan results. These tags can then be organized into Tag Sets and used for filtering report output on all Tripwire Connect reports.

This catalog may include existing, planned, or potential reports and dashboards. Tripwire has no obligation to offer a commercial version of any reports or dashboards shown below. No oral or written information or advice given by Tripwire or Tripwire's authorized representatives shall create a warranty or other obligations on behalf of Tripwire. Any purchase by customers shall not be contingent on the delivery of any future functionality, features, or reports nor dependent on any oral or written comments made by Tripwire or its representatives regarding such future functionality, features, or reports.

Darkmode Option

All reports in Tripwire Connect have the ability to toggle the light/dark mode configuration for each template, and save that configuration for use in scheduling or pinning to the dashboard section of the Tripwire.io UI.

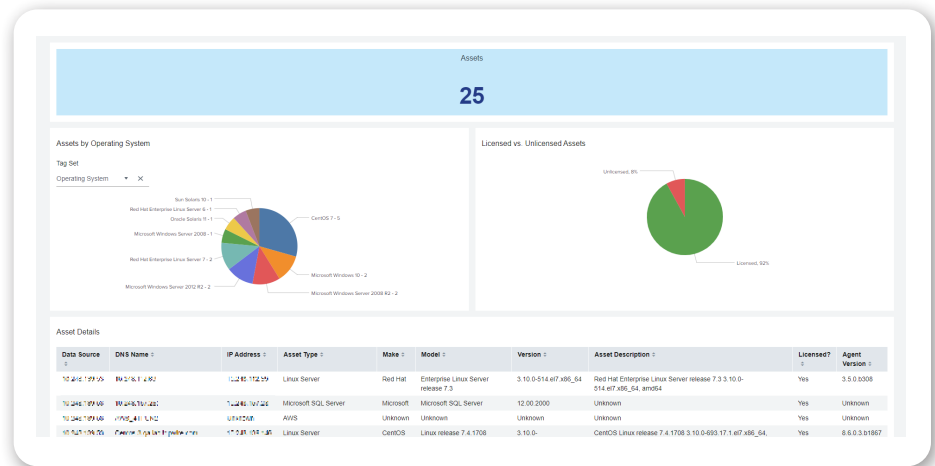


Tripwire Enterprise Asset Inventory

For each system monitored by Tripwire Enterprise, this Report Template provides the make, model, version, and other related information.

Questions answered:

- » How many licensed assets are in my Tripwire Enterprise environment?
- » Which assets are running older versions of the Java or Tripwire Axon agents?
- » How many assets in my environment are on a specific OS version?

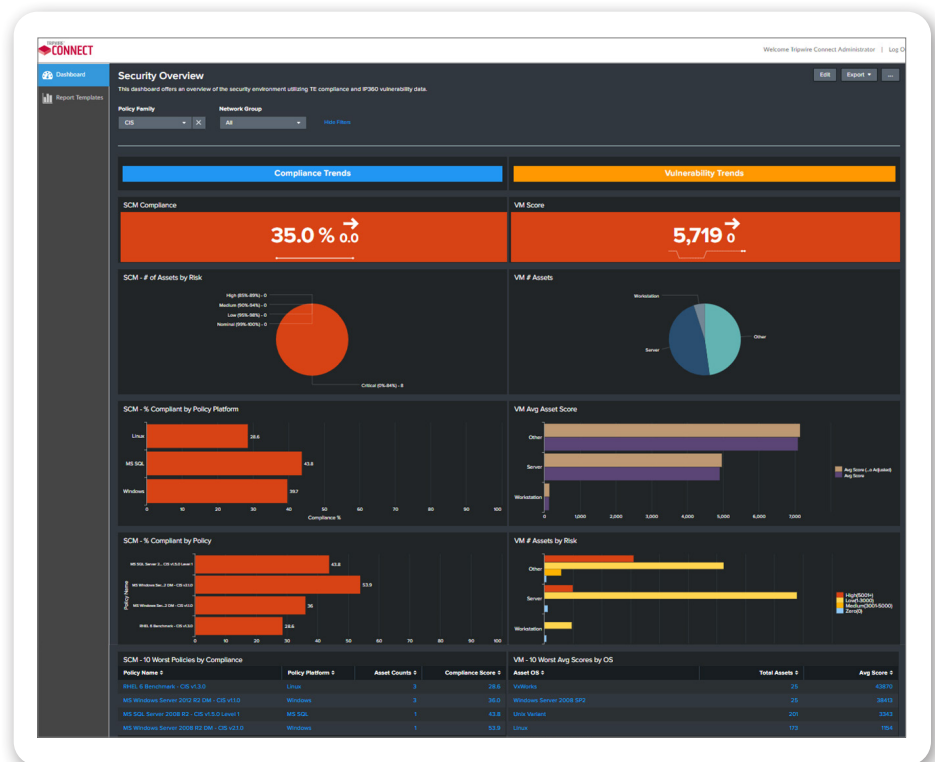


Security Overview Report

Provides an overview of your security environment utilizing Tripwire Enterprise compliance and Tripwire IP360 vulnerability data.

Questions answered:

- » Am I above or below my security or compliance threshold?
- » Do certain operating systems have more vulnerability associated risk than others in my environment?
- » What policies have the worst compliance rates in my organization?



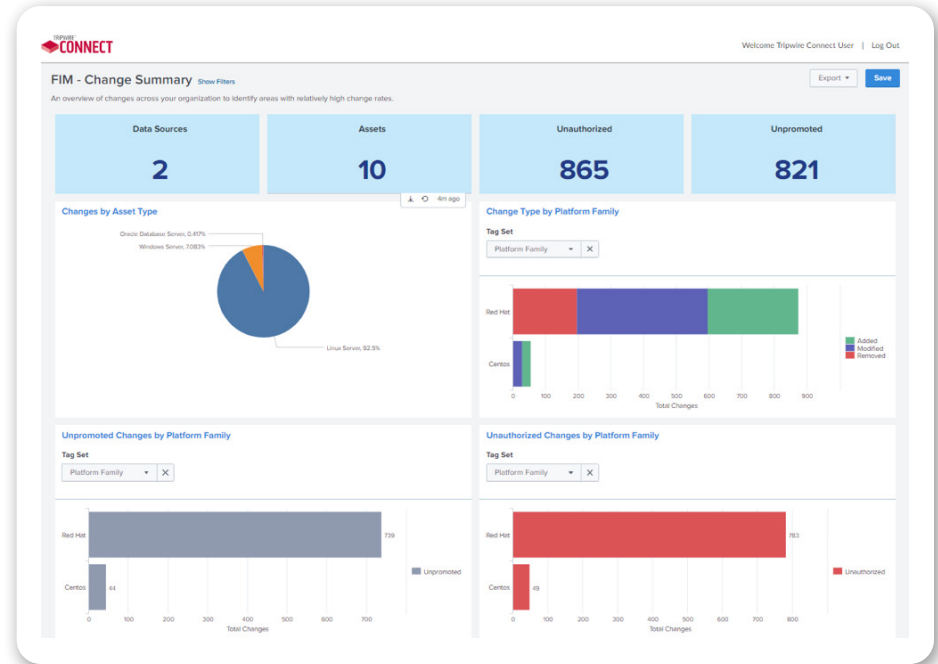
FIM Reports

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?

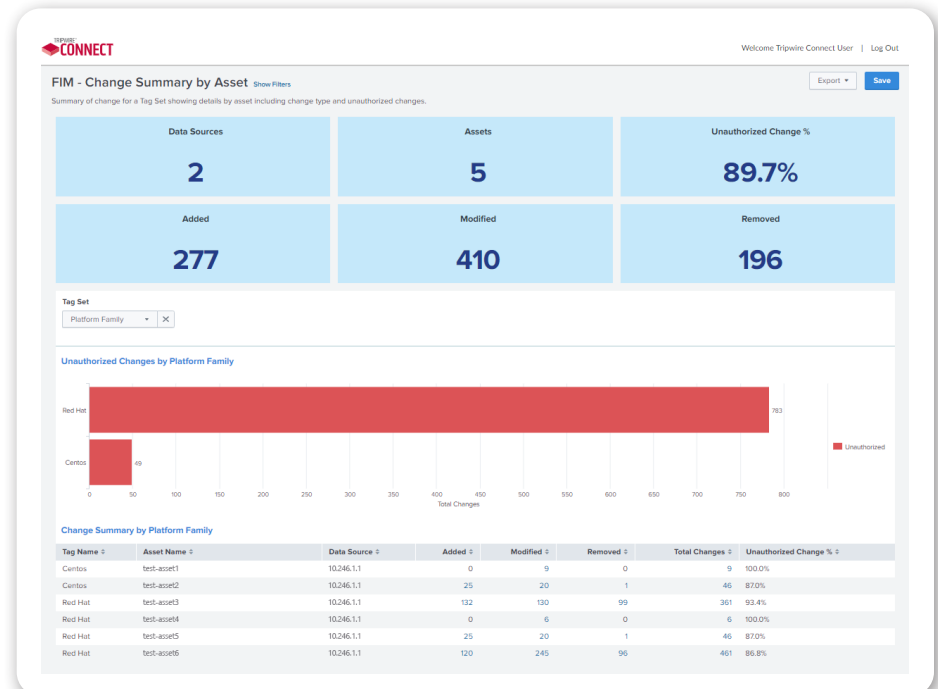


FIM – Change Summary by Asset

View which assets have the highest number of element changes in your environment and/or have the highest unauthorized change percentage.

Questions answered:

- » Which asset groups (by tag) have the most unauthorized change in my environment?
- » Which assets have the highest percentage of unauthorized change in my environment?

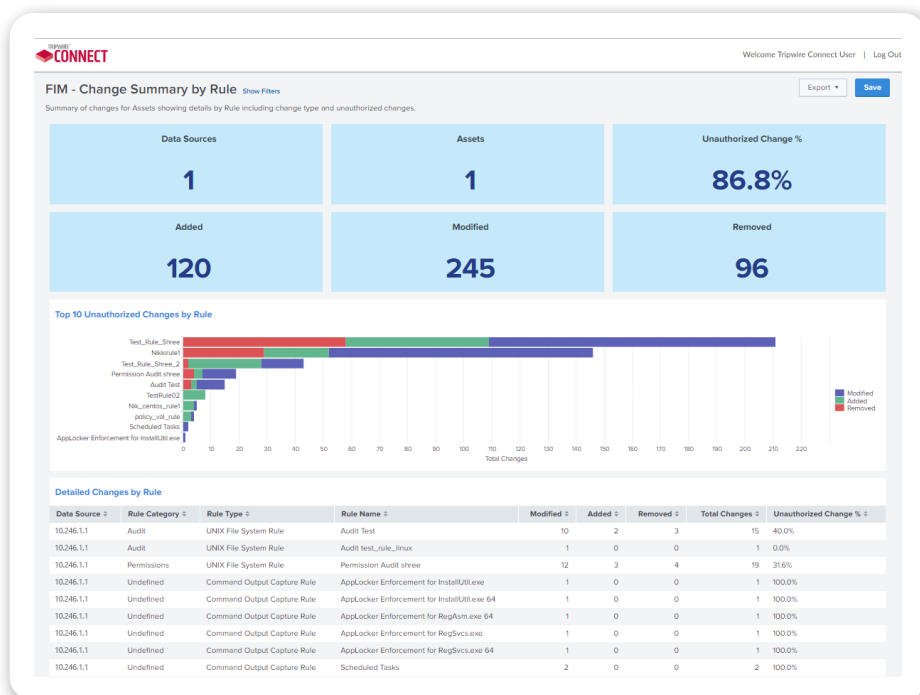


FIM – Change Summary by Rule

View which Tripwire Enterprise rules are generating the most element changes in your environment and/or have the highest unauthorized change percentage.

Questions answered:

- » Which Tripwire Enterprise rules are generating the most unauthorized change in my environment?
- » Which Tripwire Enterprise rules are generating the highest volume of changes in my environment?

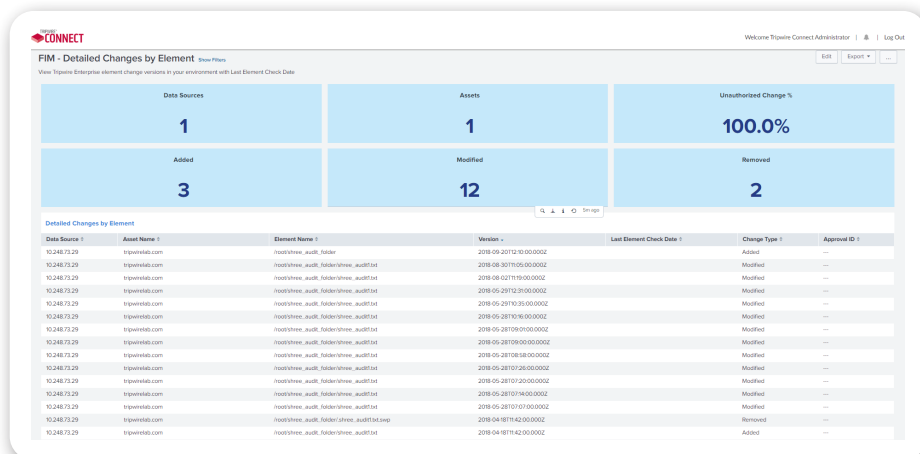


FIM – Detailed Changes by Element

A detailed view of elements that have changed for a specific asset, including change type and last date the element was evaluated for change.

Questions answered:

- » What elements changed on a specific asset in the last 7 days?
- » Who approved a specific element change?

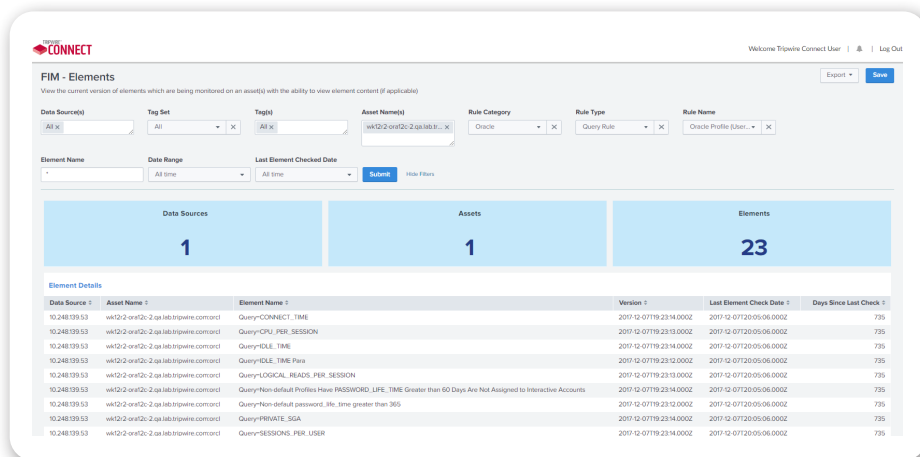


FIM – Elements

View the current version of elements which are being monitored on an asset(s), including the option to view Tripwire Enterprise element content in the report.

Questions answered:

- » Which elements have not been evaluated for change in the last “x” days?
- » Which elements are currently being monitored for a single asset or group of assets?



FIM – Reference Asset Variance

View a list of all elements that differ between a reference asset and one or more comparison assets, including the option to view Tripwire Enterprise element content in the report.

Questions answered:

- » How can I be certain that what I just promoted to production matches the reference asset or container image?
- » Do I have any configuration drift in my group of assets that should always have the same configuration?

FIM - Reference Asset Variance

Identify all elements that differ between a reference asset and one or more compare assets.

EditExport ▾⋮Save

Reference Data Source and Asset

Data Source(s)

All x

Tag SetBusiness Units X

Tag(s)AME x

Asset Name0.0.3.75 X

Compared Data Source and Assets

Data Source(s)

Tag SetBusiness Units X

Tag(s)AME x

Asset Name(s)0.0.10.52 X

Rule CategoryAudit X

Rule TypeCommand Output... X

Rule NameAudit Policy Comm... X

Difference TypeDifferent xMissing xUnexpected x

Compare TypeBaseline to Current ▾

Compare HashSHA-1 ▾

Regular Expression ⓘ

SubmitHide Filters

Different0

Missing2

Unexpected14

Total16

Reference Asset and Rule Details

Reference Data Source :	Reference Asset :	Rule Category :	Rule Type :	Rule Name :
scm-sdgt-0	0.0.3.75	Audit	Command Output Capture Rule	Audit Policy Command file

Elements with Differences

Element	Asset		
Element Name :	Difference Type :	Data Source :	Compare Asset Name :
/etc/locale.alias	Unexpected	scm-sdgt-0	0.0.10.52
/etc/locale.gen	Unexpected	scm-sdgt-0	0.0.10.52
/etc/localtime	Unexpected	scm-sdgt-0	0.0.10.52
/etc/logcheck	Unexpected	scm-sdgt-0	0.0.10.52
/etc/login.defs	Unexpected	scm-sdgt-0	0.0.10.52
/etc/pass-release	Unexpected	scm-sdgt-0	0.0.10.52
/etc/machine-id	Unexpected	scm-sdgt-0	0.0.10.52
/etc/magic.mime	Unexpected	scm-sdgt-0	0.0.10.52

Reference Asset and Rule Details				
Reference Data Source :	Reference Asset :	Rule Category :	Rule Type :	Rule Name :
scm-sdgt-0	0.0.375	Audit	Command Output Capture Rule	Audit Policy Command line
Elements with Differences				
Element	Asset			
Compare Asset Name :	Difference Type :	Data Source :	Element Name :	
0.010.52	Missing	scm-sdgt-0	C:\Windows\System32 Query=SELECT * FROM scm.message_landing WHERE id=510;	
0.010.52	Unexpected	scm-sdgt-0	/etc/locale.alias /etc/locale.gen /etc/localtime /etc/logcheck /etc/login.defs /etc/passwd-release /etc/machine-id /etc/magic.mime /etc/mailcap /etc/mimepaths.config /etc/mime.types /etc/mke2fs.conf C:\Program Files\BBj\TigpwinTE\Server\data/config C:\sysprep	


SCM – Compliance Detailed Test Results

Questions answered:

- [illegible]

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

Questions answered:

- 
Welcome Tripwire Connect User | [Log Out](#)

SCM - Compliance Summary [Show Filters](#)

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

Export ▼
Save

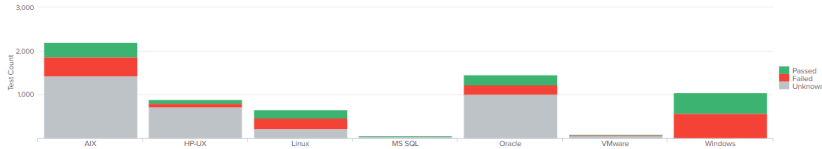
Data Sources
2

Platforms
7

Policies
17

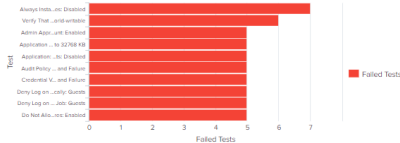
Passed %
45.6%

Test Results by Platform



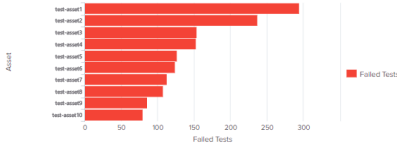
Platform	Passed	Failed	Unknown
AIX	~1500	~400	~200
HP-UX	~800	~100	~50
Linux	~400	~200	~100
MS SQL	~100	~10	~10
Oracle	~1000	~400	~200
VMware	~100	~10	~10
Windows	~500	~400	~300

Top 10 Failed Tests



Test	Failed Tests
Always Install .msi Disallowed	7
Verify That .and.exe is not	6
Active Setup .and.exe is not	5
Application .msi to S2761 KB	5
Application .msi Disallowed	5
Audit Policy .and Forum	5
Content Type .and Forum	5
Deny Log on	5
Deny Log on	5
Do Not Allow	5

Top 10 Assets with Failed Tests



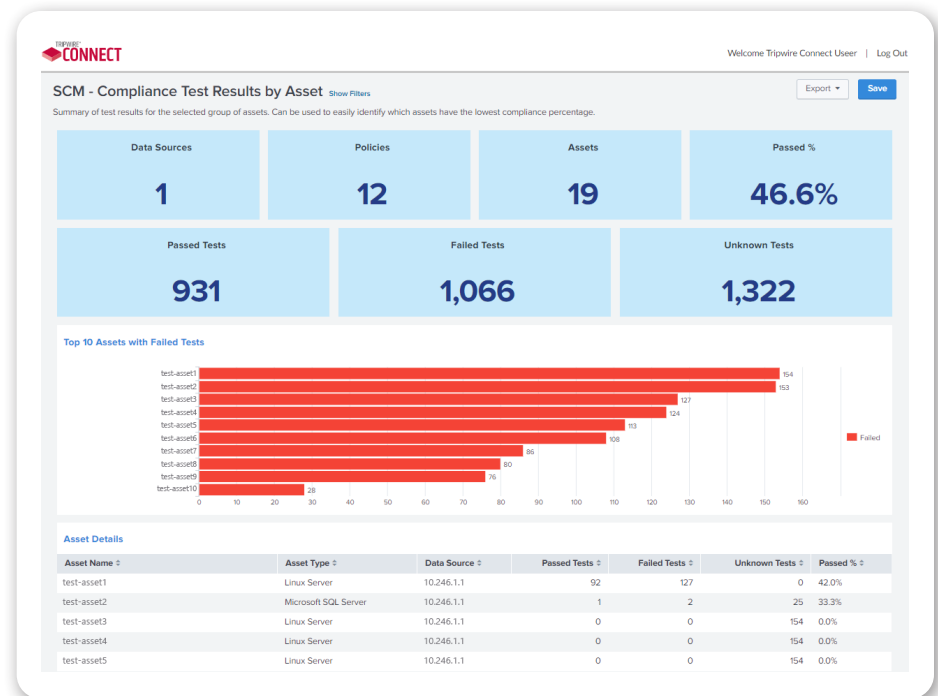
Asset	Failed Tests
test-asset1	~280
test-asset2	~230
test-asset3	~180
test-asset4	~140
test-asset5	~120
test-asset6	~100
test-asset7	~90
test-asset8	~80
test-asset9	~70
test-asset10	~60

SCM – Compliance Test Results by Asset

Summary of test results for the selected group of assets. Can be used to easily identify which assets have the lowest compliance percentage.

Questions answered:

- » Which assets have the most failing tests in my environment or with specific tags?
- » Which assets have the most unknown test results?
- » Which assets have the most test results with waivers applied?

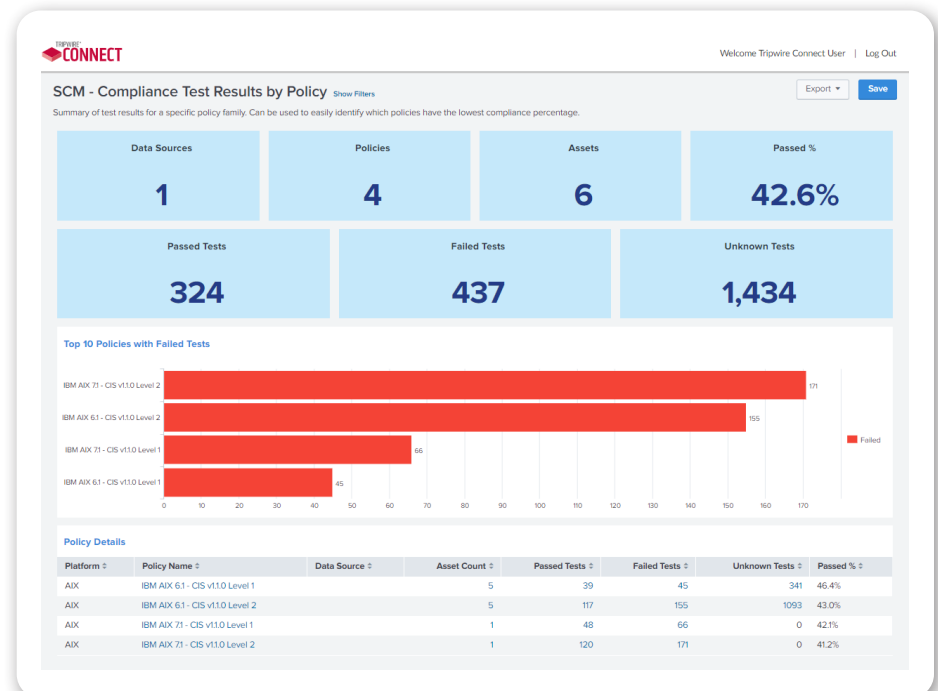


SCM – Compliance Test Results by Policy

Summary of test results for a specific policy family. Can be used to easily identify which policies have the lowest compliance percentage.

Questions answered:

- » What policies have the most failed tests in my environment or for a group of assets?
- » What policies have the worst compliance percentage in my environment or for a group of assets?
- » What/how many assets are being evaluated for compliance of a specific policy?

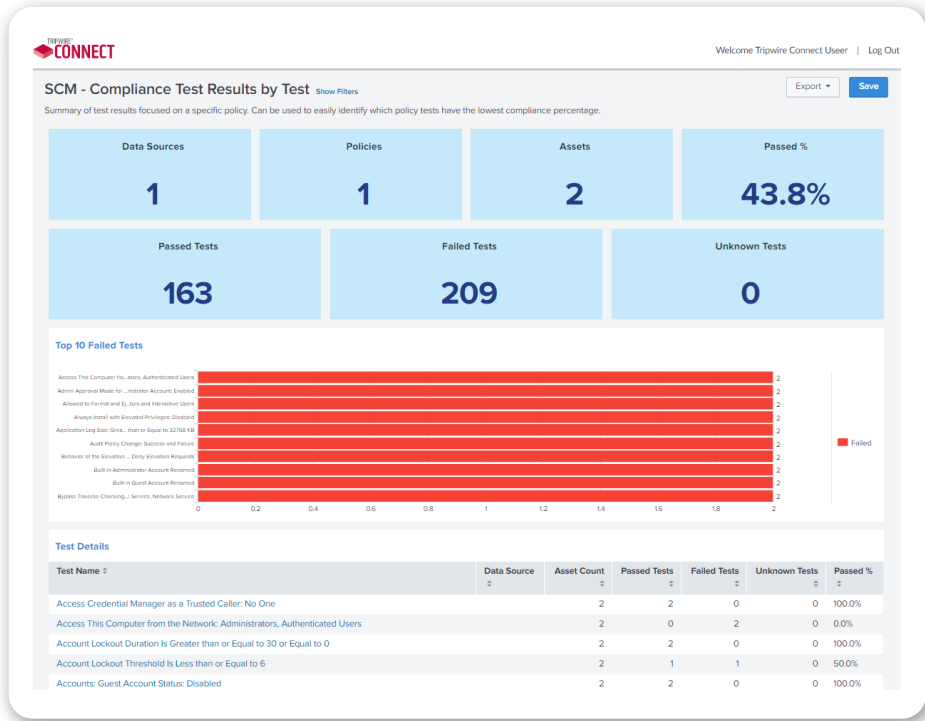


SCM – Compliance Test Results by Test

Summary of test results focused on a specific policy. Can be used to easily identify which policy tests have the lowest compliance percentage.

Questions answered:

- » What are the top 10 policy tests with failed test results in my environment or for a group of assets?
- » Which policy tests have the lowest percentage of failed test results in my environment or for a group of assets?
- » What/how many assets are being evaluated for a specific policy test?

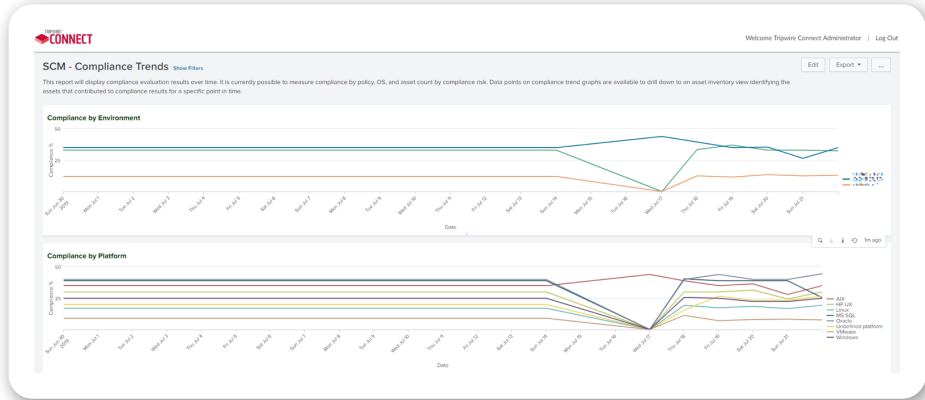


SCM – Compliance Trends

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?



VM Reports

Tripwire IP360 Risk Matrix

The Risk Matrix allows users to quickly and intuitively identify vulnerability risk in their environment. The matrix is interactive so that when you click on a cell, the associated vulnerabilities are displayed on the screen, or drill into the details to see vulnerabilities with the corresponding Risk and Skill.

The Risk Matrix is available in these Tripwire IP360 report templates:

- » VM – Asset Details
- » VM – Vulnerability Inventory
- » VM – Vulnerability Management Summary

Vulnerability Count Risk Matrix

	Exposure	Local Availability	Local Access	Local Privileged	Remote Availability	Remote Access	Remote Privileged
Automated Exploit	0	35	309	168	32	54	87
Easy	0	78	579	147	34	59	45
Moderate	0	8	23	9	4	20	3
Difficult	0	19	58	4	16	44	11
Extremely Difficult	0	376	492	218	60	46	19
No Known Exploit	1230	941	799	827	350	342	163

VM – Asset Details and VM – Vulnerability Details Report Templates

Now includes data elements such as:

- » The IP360 Rule used to detect the presence of a vulnerability or application
- » The associated transcript for each IP360 Rule (evidence data)
- » Solution data such as links to application advisories used to resolve a vulnerability
- » Host information such as SSL certificate, encryption ciphers, open ports, etc.

Vulnerability Information

Vulnerability ID	433488	Date	2020-06-02
Vulnerability Name	MS-2019 May - Remote Desktop Service Remote Code	Skill	Automated Exploit
Vulnerability Score	31387	Risk	Remote Privileged
CVE(s)	CVE-20	CVSSv3	10
Instance	2		

Vulnerability Description

Microsoft Windows is prone to a pre-authentication remote code execution vulnerability within Remote Desktop Service (formerly Terminal Services). An attacker can exploit this vulnerability by connecting to the host using Remote Desktop Protocol (RDP) and then sending specially crafted messages successful exploitation allows arbitrary code execution with full system privileges. Microsoft has correct the issue through updates to host RDP connection are handled.

First Release in : 865

Vulnerability Solution

Disable the service if it is not essential to the server's operation. Telnet is an insecure method of system administration due to its clear-text transmission of data. We suggest you replace this with SSH. If for some reason it is necessary to run Telnet in your environment, configure packet filters on firewalls and border routers to block external access to port 23 on your internal network. Additionally use TCP wrappers to restrict access to this service to a limited set of trusted hosts. TCP wrappers is used to control access to services by IP address or hostname, and provides enhanced logging facility or services it protects. Be advised, services protected in this manner will still be vulnerable to IP spoofing attacks, however the program does provide a much needed additional all over of security.

References

Associated HTML Name and Links

[Microsoft Guidelines For Windows XP and Server 2003](#)
[Exploit DB 46946](#)

Advisory Name and Links

[CVSSv3 Base Score : 9.8](#)
[CVSSv3 Base Vector : CVSS 3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A/M](#)

May 4th, 2020 7:00 AM May 4th, 2020 9:00 AM

Protocol	1191	Port	1191
Associated Application	HTTP		
Rule	SEND String [TRACE / HTTP / 1.0]vdvdvdvd THEN CHECK Contains / HTTP/1.1.200 OKvdvdvdvd BEFORE Contains/ Content-Type: message/httpvdvdvdvdHEN CHECK Contains / HTTP/1.1.200 OKvdvdvdvd BEFORE Contains/ Content-Type: message/httpvdvdvdvdHEN CHECK Contains / HTTP/1.1.200 OKvdvdvdvdvd BEFORE Contains/ Content-Type: message/httpvdvdvdvd		
Transcript			

VM – Application Details

For an application or group of applications, shows detailed information about the assets that have the application(s).

Questions answered:

- » What assets in my environment have a specific application present?
- » What port(s) was a specific application found on?

App ID	App Name	Asset IP	Asset DNS	Asset OS	Protocol	Port	Scan Finish Time	NetBIOS Domain	NetBIOS Name
16157	NTP-Based OS Detection	192.168.1.1	192.168.1.1	Linux	udp	123	08/16/2019	null	null
16157	NTP-Based OS Detection	192.168.1.2	192.168.1.2	Linux	udp	123	08/16/2019	null	null
16157	NTP-Based OS Detection	192.168.1.3	192.168.1.3	Linux	udp	123	08/16/2019	null	null
16157	NTP-Based OS Detection	192.168.1.4	192.168.1.4	Linux	udp	123	08/16/2019	null	null
16157	NTP-Based OS Detection	192.168.1.5	192.168.1.5	Linux	udp	123	08/16/2019	null	null
16157	NTP-Based OS Detection	192.168.1.6	192.168.1.6	Linux	udp	123	08/16/2019	null	null

VM – Application Inventory

List of applications running in the environment with a count of the assets that have the application present.

Questions answered:

- » What applications are present in my environment?
- » For each application, how many assets have that application present?

App ID	App Name	App Description	App Protocol	Port List	Asset Count	Scan Finish Time
10211	VMware ESX Server (via SSH)	SSH DRT Discovered Operating System, SSH DRT, SSH	ip	0	17	01/10/2019
10486	Mac OS X 10.5.x (via SSH)	Mac OS X 10.5.x (via SSH), SSH DRT Discovered Operating System, SSH DRT, SSH	ip	0	11	01/10/2019
1196	DNS LDAP		udp	53	25	01/10/2019
11513	Apple Safari for OS X (via SSH)	Mac OS X Applications (via SSH), SSH DRT Discovered Application, SSH DRT, SSH	ip	0	37	01/10/2019
12784	Oracle Enterprise Linux (via SSH)	Red Hat / Fedora / CentOS / Oracle Linux (via SSH), Linux (via SSH), SSH DRT Discovered Operating System, SSH DRT, SSH	ip	0	47	01/10/2019
1352	Microsoft Windows NetBIOS Session Service	NetBIOS Session Service	tcp	139	50	01/10/2019
13564	Java Runtime Environment 1.6.0_02 (via SSH)	Java Runtime Environment 1.6.0 (via SSH), Java Runtime Environment 1.6.x (via SSH), Java Runtime Environment (via SSH), SSH DRT Discovered Application, SSH DRT, SSH	ip	0	23	01/10/2019
165	DCERMS RPC over TCP		tcp	135	75	01/10/2019
165	DCERMS RPC over TCP		tcp	4954	25	01/10/2019
16530	Java Development Kit 1.5.0_24 for OS X (via SSH)	Java Development Kit 1.5.0 for OS X (via SSH), Java Development Kit 1.5.x for OS X (via SSH), Java Development Kit for OS X (via SSH), Mac OS X Applications (via SSH), SSH DRT Discovered Application, SSH DRT, SSH	ip	0	14	01/10/2019

VM – Asset Details

List of the vulnerabilities present on a specific asset

Questions answered:

- » What vulnerabilities are present on a specific asset?
- » Are there any critical vulnerabilities present on a specific asset?
- » What is/are the CVE(s) associated with a vulnerability?

Vuln ID	Vuln Name	Vuln Score	CVE(s)	S&E	Risk	CVSS(s)	Port	Protocol	Remediation
19962	SSH RC4 Cipher Disabled	0	4.3	5.4	No Known Exploit	Local Access	22	tcp	Q
1406	Portmapper RPC enumeration	0	0.0	0.0	No Known Exploit	Exposure	111	tcp	Q
1406	Portmapper RPC enumeration	0	0.0	0.0	No Known Exploit	Exposure	111	udp	Q
83	Portmapper Available	0	0.0	0.0	No Known Exploit	Exposure	111	tcp	Q

VM – Asset Inventory

This report lists all known Tripwire IP360 assets in the environment with their IP360 Host Score, vulnerability count, highest CVSSv3 on each asset, and last scan date.

Questions answered:

- » Which/how many assets are being scanned for vulnerabilities in my environment?
- » Are there any assets in my environment with an IP360 Host Score above my security department's pre-defined threshold?
- » Are there any assets in my environment with a Critical CVSSv3 vulnerability?

CONNECT Welcome Tripwire Connect Administrator | Log Out

VM - Asset Inventory [View Files](#) [Edit](#) [Export](#)

List of all known IP360 assets in the environment

Vulnerability by CVSSv3 Score		Avg. Asset Score	Avg. Vulnerability Score	Vulnerabilities	Assets
Critical (9.0-10.0)	161	115,249	470	1,732	12
High (7.0-8.9)	400				
Medium (5.0-6.9)	918				
Low (3.0-4.9)	9				
None (0.0)	264				

Asset Inventory Details

Network Name	Asset IP	Asset DNS	NetBIOS Name	NetBIOS Domain	Operating System	Host Score	Vulnerability Count	CVSSv3	Last Audit ID	Last Scan Date
10.10.10.10	10.10.10.10	10.10.10.10	WINLAB-1	WINLAB-1	Windows Server 2008 for x64-based Systems Service Pack 2	77999	834	6.0	419	07/15/2019
10.10.10.11	10.10.10.11	10.10.10.11	WINLAB-1	WINLAB-1	Windows Server 2012 R2 Update 1	30078	976	5.0	419	07/15/2019
10.10.10.12	10.10.10.12	10.10.10.12	WINLAB-1	WINLAB-1	Windows Server 2012 R2 Update 1	30078	984	4.9	417	07/15/2019
10.10.10.13	10.10.10.13	10.10.10.13	WINLAB-1	WINLAB-1	Windows Server 2012 R2 Update 1	5341	50	1.4	418	07/15/2019
10.10.10.14	10.10.10.14	10.10.10.14	WINLAB-1	WINLAB-1	Windows Server 2012 R2 Update 1	4456	108	4.3	420	07/15/2019
10.10.10.15	10.10.10.15	10.10.10.15	WINLAB-1	WINLAB-1	Windows Server 2012 R2 Update 1	835	295	5.4	419	07/15/2019
10.10.10.16	10.10.10.16	10.10.10.16	WINLAB-1	WINLAB-1	Linux Variant	999	7	1.5	421	07/15/2019
10.10.10.17	10.10.10.17	10.10.10.17	WINLAB-1	WINLAB-1	Linux Variant	999	7	1.5	421	07/15/2019
10.10.10.18	10.10.10.18	10.10.10.18	WINLAB-1	WINLAB-1	Linux Variant	999	10	1.1	421	07/15/2019
10.10.10.19	10.10.10.19	10.10.10.19	WINLAB-1	WINLAB-1	Cisco IOS 12.4	0	1	0.0	414	07/14/2019

VM – Host Information Data

This Report Template identifies SSL certificates that have expired, are about to expire, or are issued by a user-specified certificate authority (CA).

Questions answered:

- » Which SSL certificates exist in my environment?
- » Which SSL certificates have expired or are about to expire?
- » Which SSL certificates are associated with a specific CA?

VM - Host Information Data [Edit](#) [Export](#) [Save](#)

This Report Template identifies SSL certificates that have expired, are about to expire, or are issued by a user-specified certificate authority (CA)

Parameters

Data Source(s): IP Address: OS: Issued By:

Last Scan Date: Certification Expiry Date: Is Expired: [Submit](#) [Hide Filters](#)

Certificate Details

Data Source	IP Address	DNS Name	Port	NetBIOS Name	OS	Last Scan Date	Is Expired	Serial Number	Issued By	Subject
10.10.10.10	10.10.10.10	10.10.10.10	TCP/0	WINLAB-1	Windows Server 2012 R2	2020-06-01	No	WIN1234567	Demo CA	Internet Corporation for Assigned Names and Numbers Secure Multipurpose Internet Extensions Version 3.0
10.10.10.11	10.10.10.11	10.10.10.11	TCP/0	WINLAB-1	Windows Server 2012 R2	2020-06-01	No	WIN1234567	Demo CA	Internet Corporation for Assigned Names and Numbers Secure Multipurpose Internet Extensions Version 3.0
10.10.10.12	10.10.10.12	10.10.10.12	TCP/0	WINLAB-1	Windows Server 2012 R2	2020-06-01	No	WIN1234567	Demo CA	Internet Corporation for Assigned Names and Numbers Secure Multipurpose Internet Extensions Version 3.0
10.10.10.13	10.10.10.13	10.10.10.13	TCP/0	WINLAB-1	Windows Server 2012 R2	2020-06-01	No	WIN1234567	Demo CA	Internet Corporation for Assigned Names and Numbers Secure Multipurpose Internet Extensions Version 3.0

VM – Vulnerability Details

For a vulnerability or group of vulnerabilities, shows detailed information about the assets that have the vulnerability present. Report data can be exported as CSV.

Questions answered:

Which assets have a specific vulnerability?

How do I remediate a specific vulnerability?

Which assets have specific vulnerabilities?

VM - Vulnerability Details [SHOW FILTERS](#) [EDIT](#) [EXPORT](#) [SAVE](#)

For a vulnerability or group of vulnerabilities, show detailed information about the assets that have the vulnerability present

Vulnerability Information

Vulnerability Name	MS-2020-Feb. Microsoft SQL Server Reporting Services Remote Code Execution Vulnerability	Date Published in ASPL	2020-02-11
Vulnerability ID	440154	Skill	Automated Exploit
Vulnerability Score	31	Risk	Local Access
CVE(s)	CVE-2020-0618	CVSSv3	8.8
Asset Count	3	CVSSv2	6.5
Port	1433	Protocol	tcp
Vulnerability Solution	Patch		

Vulnerability Description

Microsoft SQL Server Reporting Services contains a remote code execution vulnerability due to incorrect handling of page requests. An attacker would need to be authenticated before submitting a specially crafted page request to an affected instance in order to exploit this vulnerability. If exploited, the attacker could execute code in the context of the Report Server service account.

Vulnerability Mitigation

Vulnerability Remediation

The vendor has released patches for this vulnerability. Please refer to the advisory links below.

References

Associated HTML Name and Links

Advisory Name and Links

MSRC Guidance: CVE-2020-0618

Exploit Framework - Metasploit: CVE-2020-0618

Affected Assets

Asset IP	Asset DNS	NetBIOS Domain	NetBIOS Name	Operating System	Vulnerability Name	Application Name	Host Score	Last Scan Date	Last Audit ID
10.10.10.1	10.10.10.1	10.10.10.1	10.10.10.1	Windows Server 2012 R2	MS-2020-Feb. Microsoft SQL Server Reporting Services Remote Code Execution Vulnerability	MSSQL/Service TDS	230	Oct 19 2020	102
10.10.10.2	10.10.10.2	10.10.10.2	10.10.10.2	Windows Server 2012 R2	MS-2020-Feb. Microsoft SQL Server Reporting Services Remote Code Execution Vulnerability	MSSQL/Service TDS	230	Oct 19 2020	102
10.10.10.3	10.10.10.3	10.10.10.3	10.10.10.3	Windows Server 2016	MS-2020-Feb. Microsoft SQL Server Reporting Services Remote Code Execution Vulnerability	MSSQL/Service TDS	46	Oct 19 2020	102

VM – Vulnerability Inventory

List of vulnerabilities that exist in the environment with a count of the assets that have the vulnerability present.

Questions answered:

- » What vulnerabilities are present in my environment?
- » Are there any high or critical vulnerabilities in my environment based on the CVSSv3 score?
- » Are there any vulnerabilities in my environment above a certain IP360 Vulnerability Score?
- » When was the last time a specific vulnerability was seen in my environment?
- » How many assets have a specific vulnerability in my environment?

VM - Vulnerability Inventory [Show Filters](#) [Export](#) [Save](#)

List of vulnerabilities that exist in the environment with a count of the assets that have the vulnerability present

Vulnerability by CVSSv3 Score

CVSSv3 Score	Vulnerabilities	Avg. Asset Score	Avg. Vulnerability Score	Vulnerabilities	Assets
Critical (9.0-10.0)	0	200	11	18	5
High (7.0-8.9)	0				
Medium (4.0-6.9)	2				
Low (0.1-3.9)	0				
None (0.0)	16				

Vulnerability Inventory

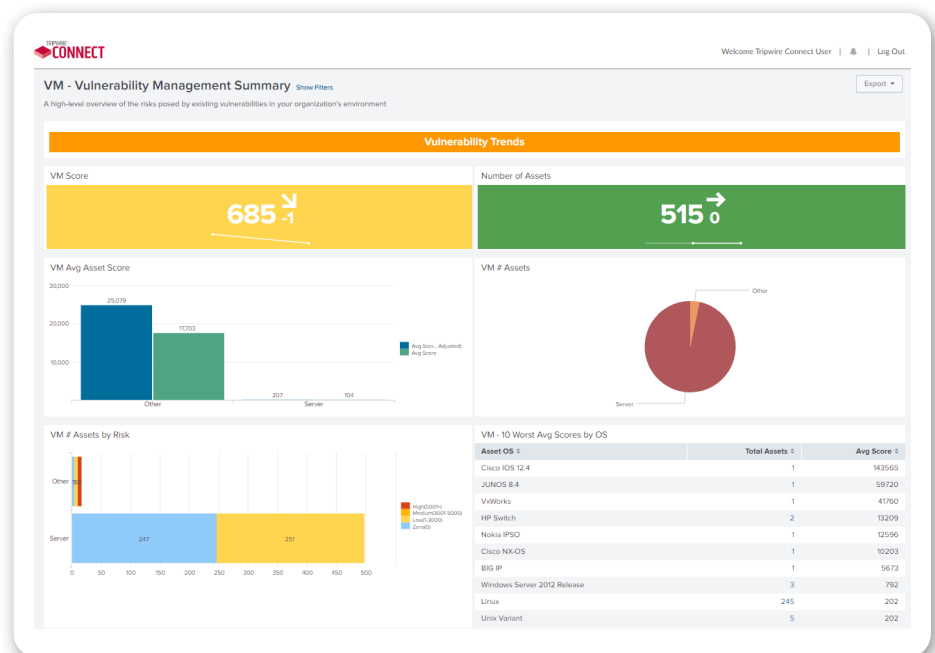
Vulnerability ID	Vulnerability Name	Asset Count	Vulnerability Score	CVSSv3	Remediation	Last Scan Date	Network Name
78685	SSH Insecure HMAC Algorithms Enabled	2	197	5.4	Q	08/16/2019	RHEL-group2
78685	SSH Insecure HMAC Algorithms Enabled	3	197	5.4	Q	08/16/2019	RHEL-group2
78683	SSH RC4 Cipher Enabled	2	3	5.4	Q	08/16/2019	RHEL-group2
78683	SSH RC4 Cipher Enabled	3	3	5.4	Q	08/16/2019	RHEL-group2
99136	TLS Fallback Signaling Not Supported	1	0	0.0	Q	08/16/2019	RHEL-group2
83	Portmapper Available	2	0	0.0	Q	08/16/2019	RHEL-group2
83	Portmapper Available	3	0	0.0	Q	08/16/2019	RHEL-group2
78682	SSH CBC Mode Ciphers Enabled	2	0	0.0	Q	08/16/2019	RHEL-group2
78682	SSH CBC Mode Ciphers Enabled	3	0	0.0	Q	08/16/2019	RHEL-group2
30535	NO SSH AUTHENTICATION ATTEMPTED (no credentials configured)	2	0	0.0	Q	08/16/2019	RHEL-group2
30535	NO SSH AUTHENTICATION ATTEMPTED (no credentials configured)	3	0	0.0	Q	08/16/2019	RHEL-group2

VM – Vulnerability Management Summary

A high-level overview of the risks posed by existing vulnerabilities in your organization's environment.

Questions answered:

- » Am I above or below my security threshold?
- » Do certain operating systems have more vulnerability associated risk than others in my environment?



VM – Vulnerability Remediation

For a specific vulnerability or list of vulnerabilities, this report displays the associated remediation and mitigation information.

Questions answered:

- » How do I remediate a specific vulnerability?
- » Is there anything I can do to mitigate my exposure to a specific vulnerability?
- » What is/are the CVE(s) associated with a vulnerability?

VM - Vulnerability Remediation

For a specific vulnerability or list of vulnerabilities, display the associated remediation and mitigation information.

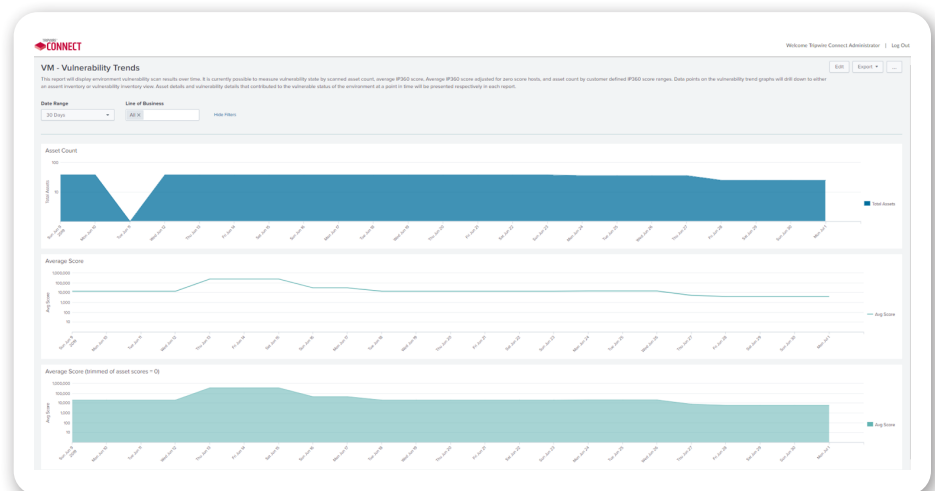
Vulnerability ID	Vulnerability Name	Vulnerability Description	CVE(s)	CVSSv3	Skill	Risk	Strategy	Solution	Mitigation	Remediation
78683	SSH RC4 Cipher Enabled	The arcfour cipher is considered to be flawed.	CVE-2013-2566	5.4	No Known Exploit	Local Access	Data-Driven Attack	Workaround	null	Disable the arcfour cipher.

VM – Vulnerability Trends

Displays trend information of vulnerability scans across the environment or by groups of assets using the IP360 Network Group.

Questions answered:

- » Have the number of assets being scanned for vulnerabilities gone up or down over time?
- » Has the average IP360 Host Score improved or gotten worse over time?





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](#)