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

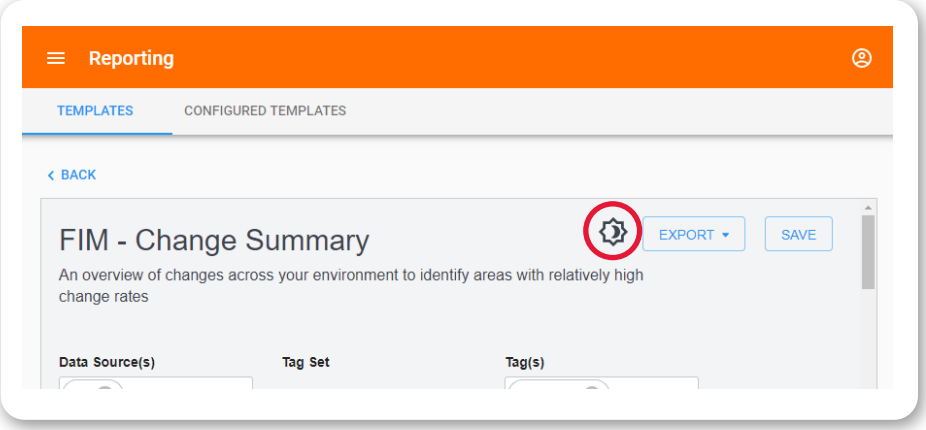
Enables administrators to perform SPL queries against the Tripwire Connect indexes to get targeted search results or to test queries to be added to a custom report template.

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.

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.

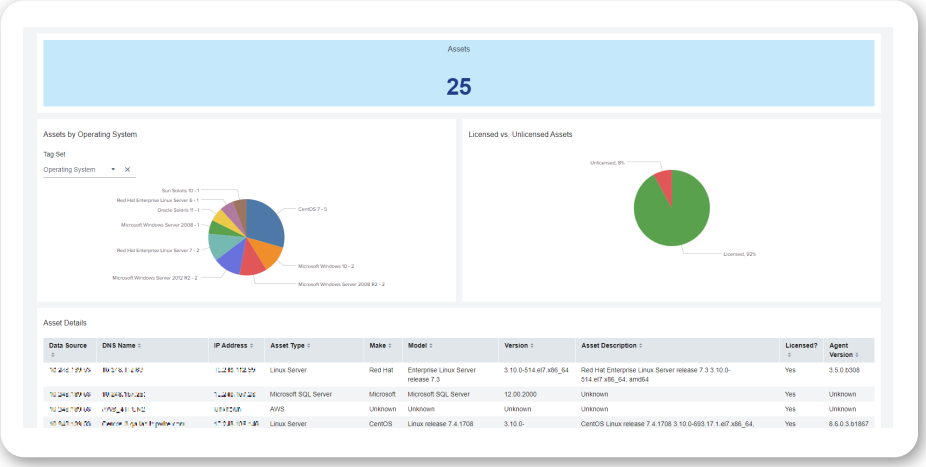


Tripwire Enterprise Asset Inventory

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?

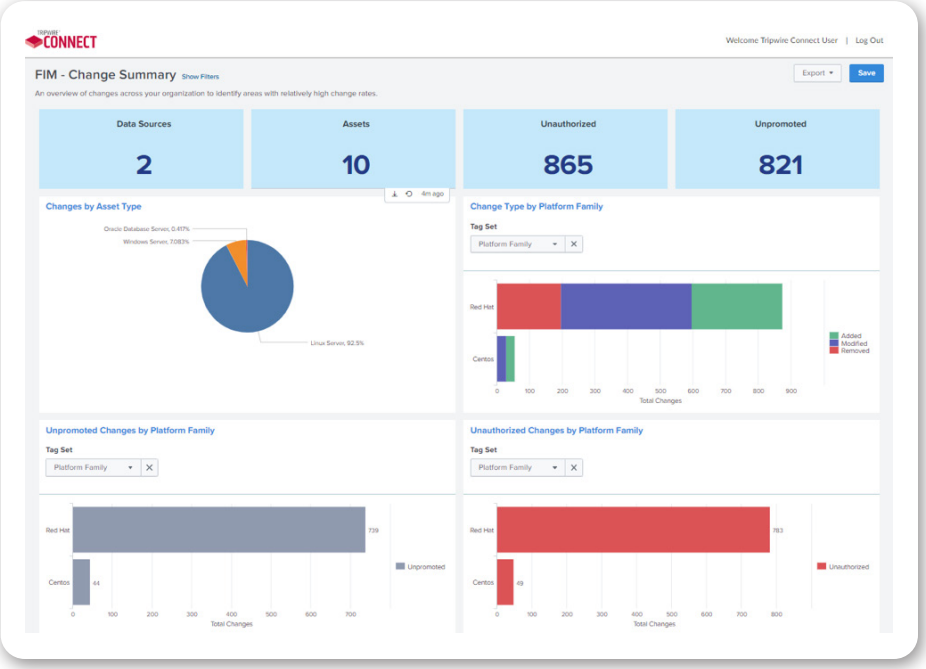
FIM Reports

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?

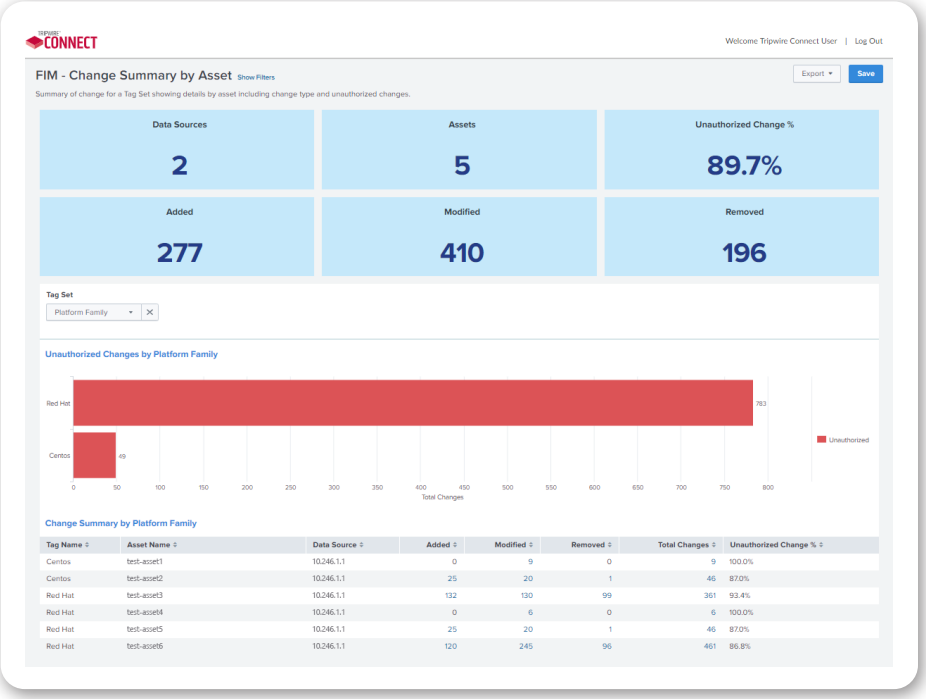


FIM – Change Summary by Asset

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?

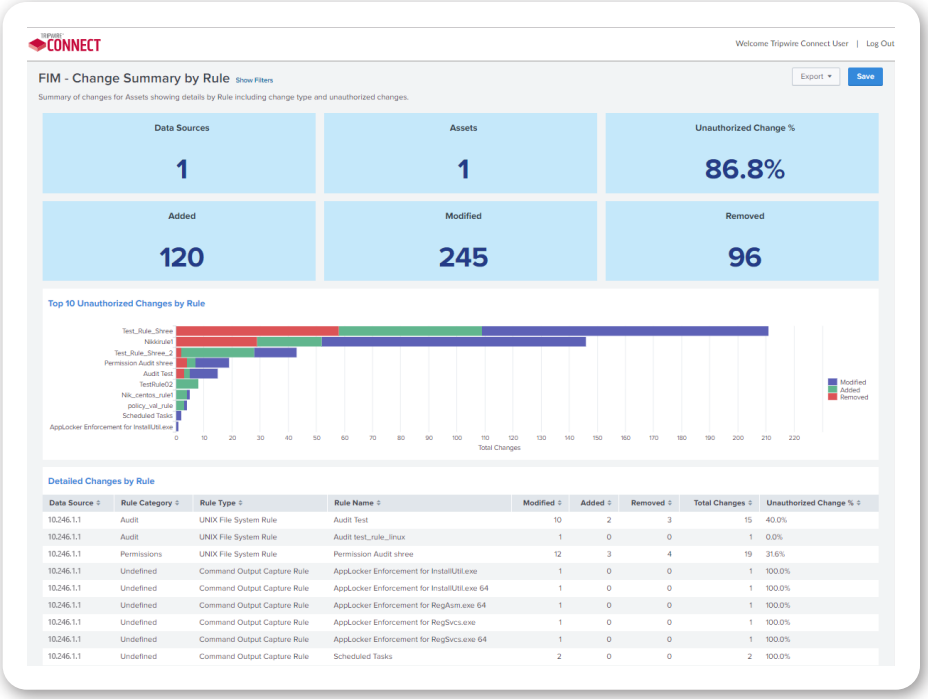


FIM – Change Summary by Rule

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?

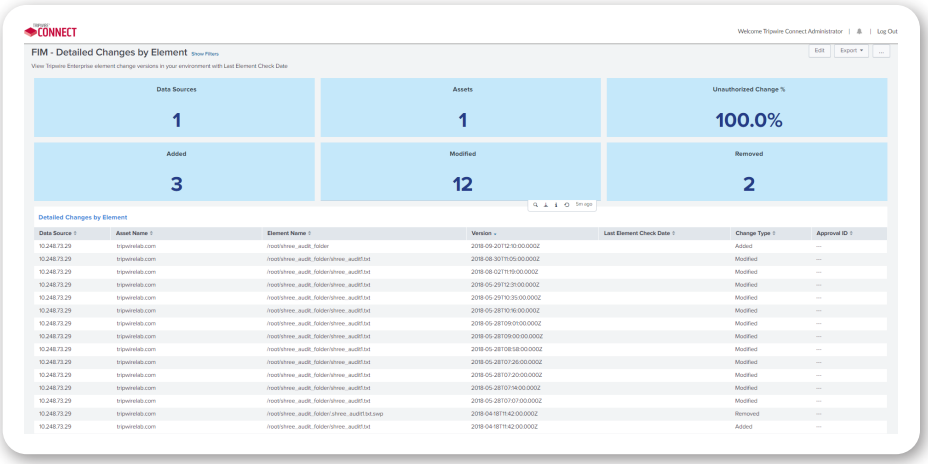


FIM – Detailed Changes by Element

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?

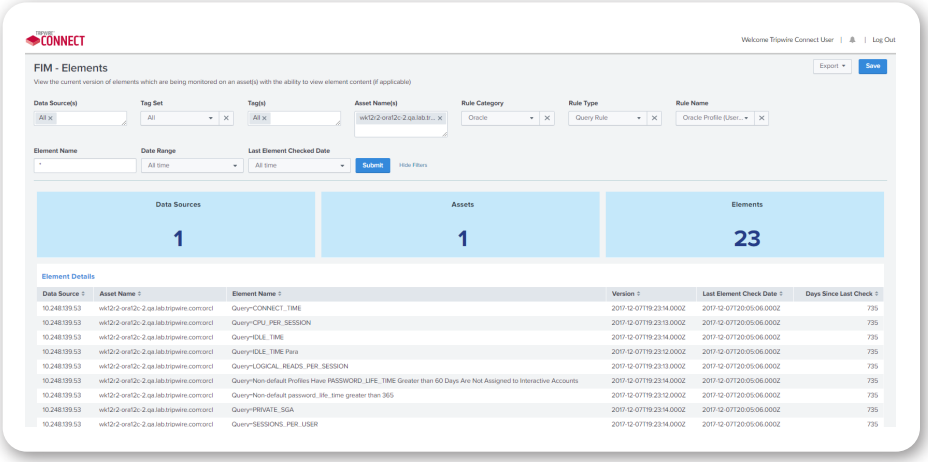


FIM – Elements

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?

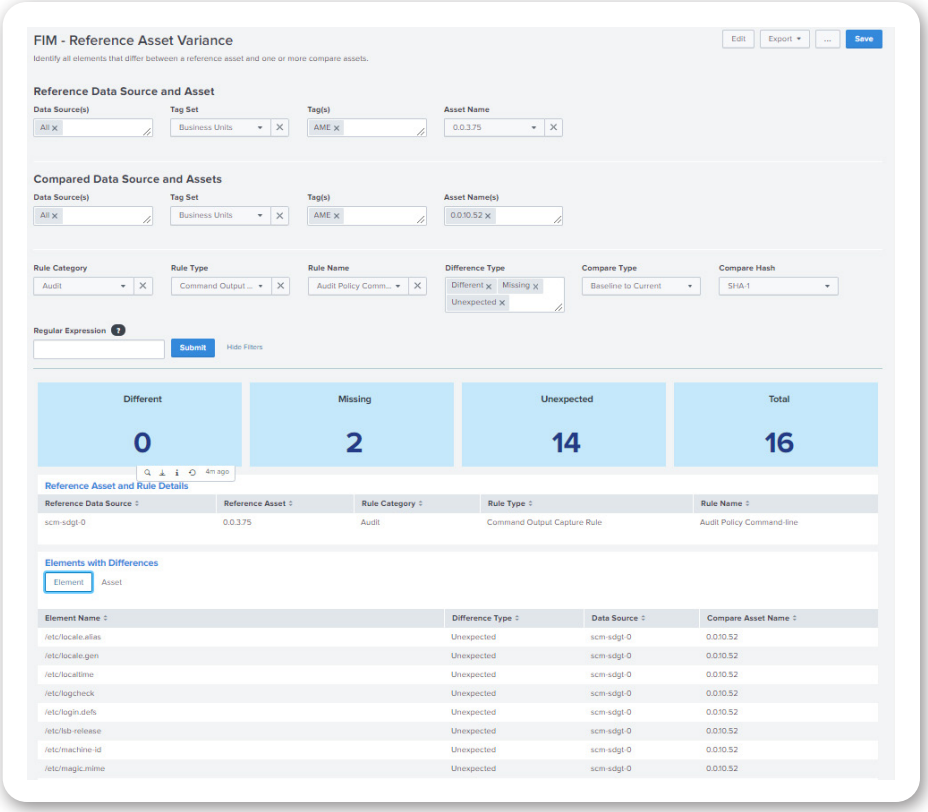


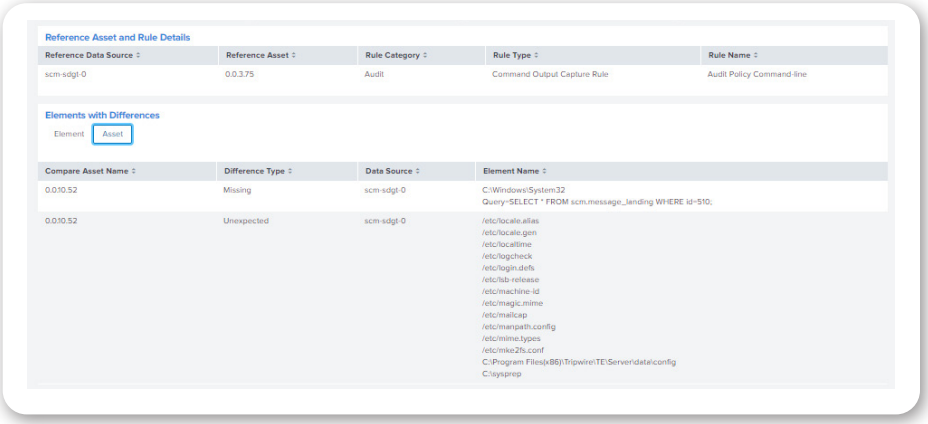
FIM – Reference Asset Variance

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?





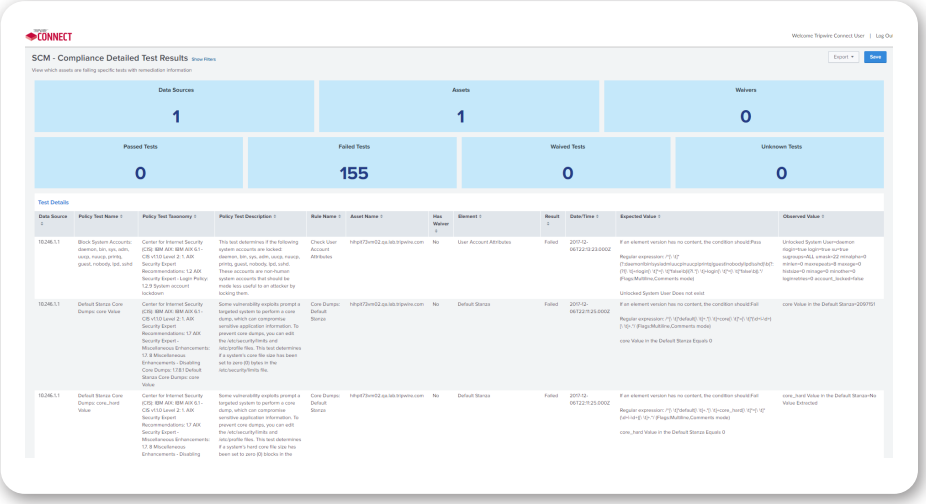
SCM Reports

SCM – Compliance Detailed Test Results

View detailed policy test results for use in an audit or to identify failing policy tests on specific assets, including the option to view Tripwire Enterprise element content in the report.

Questions answered:

» How can I create a report for an auditor to prove an asset is being monitored for PCI compliance?



SCM – Compliance Summary

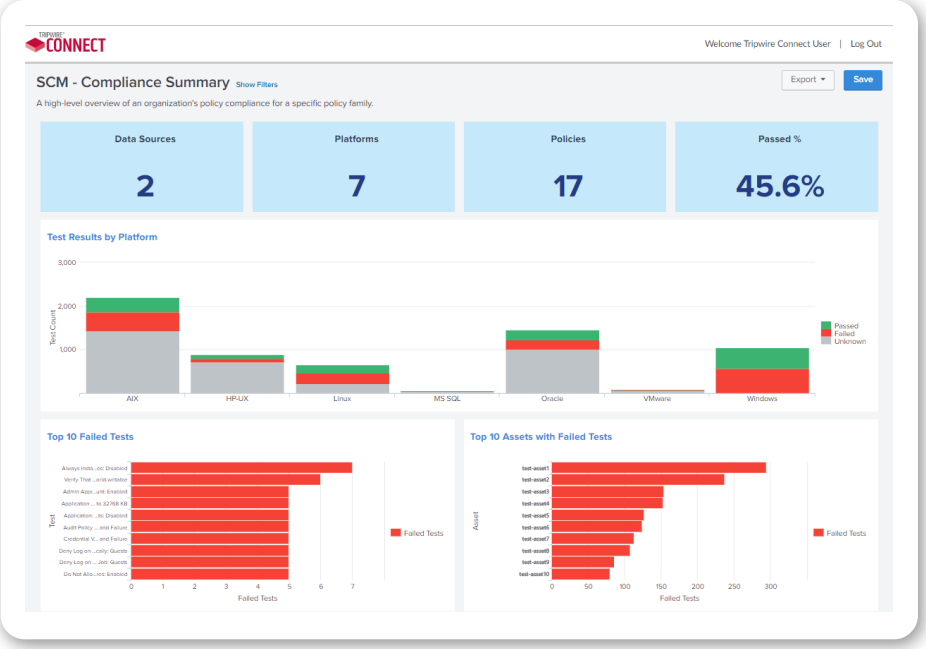
A high-level overview of an organization's policy compliance for a specific policy family

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?

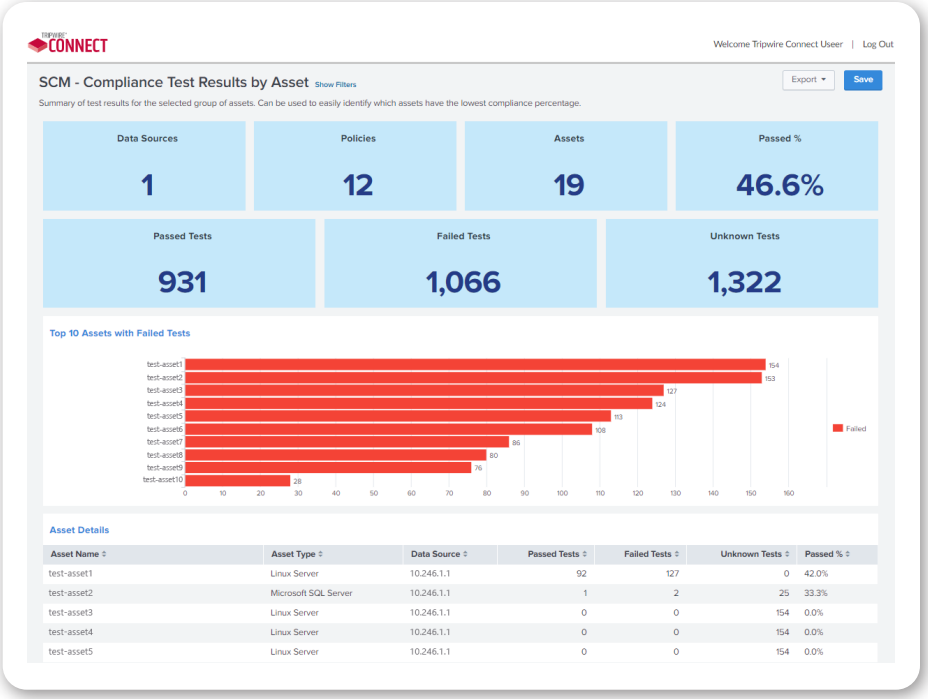


SCM – Compliance Test Results by Asset

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?

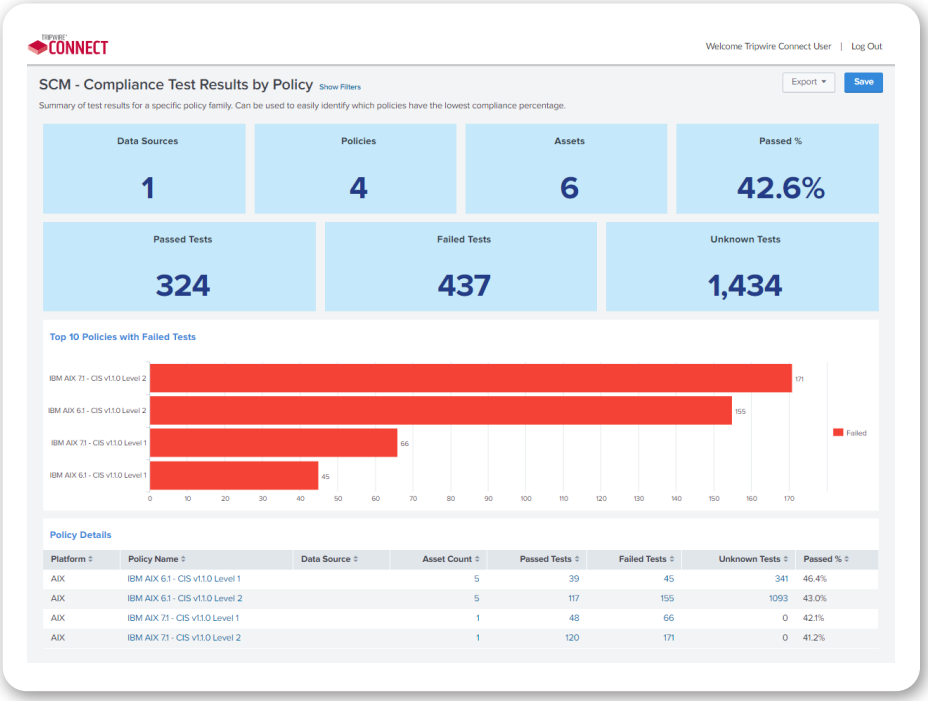


SCM – Compliance Test Results by Policy

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?

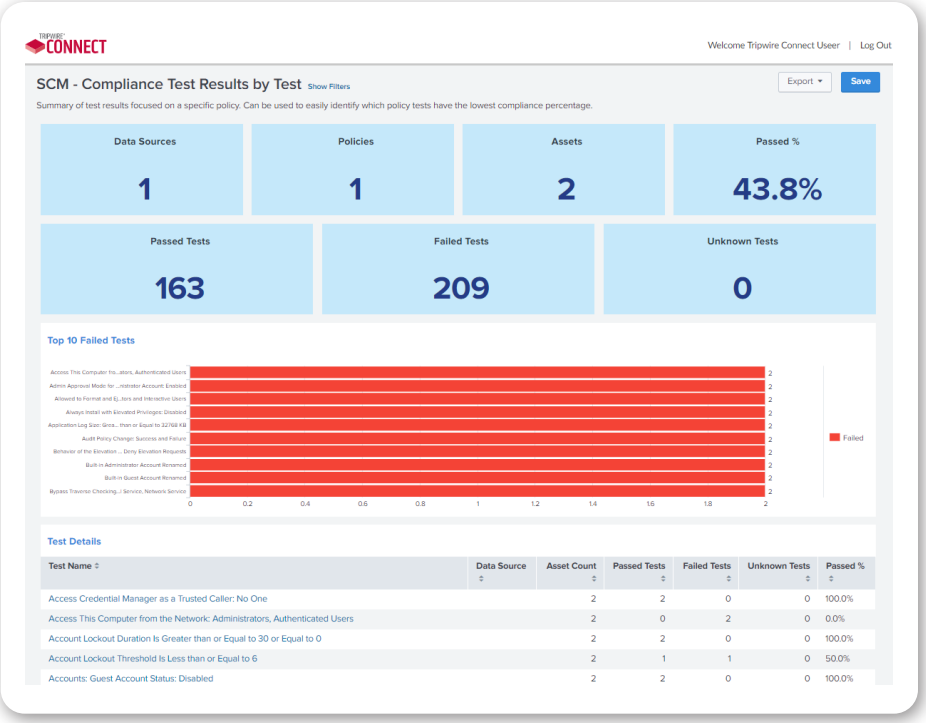


SCM – Compliance Test Results by Test

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?

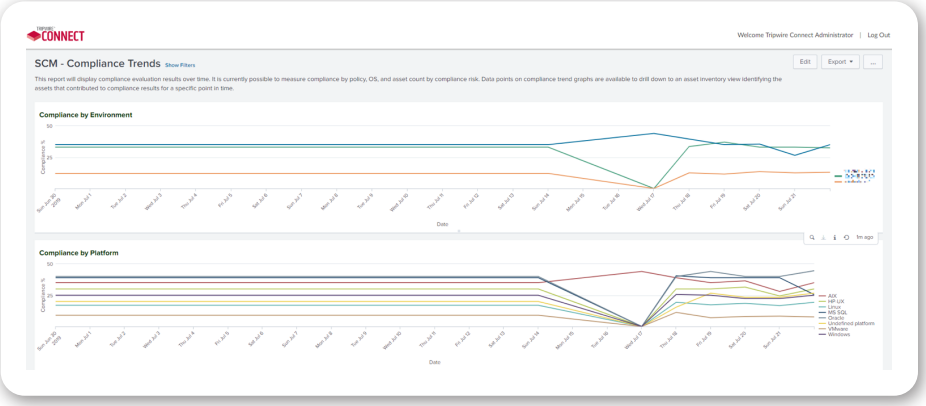


SCM – Compliance Trends

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?



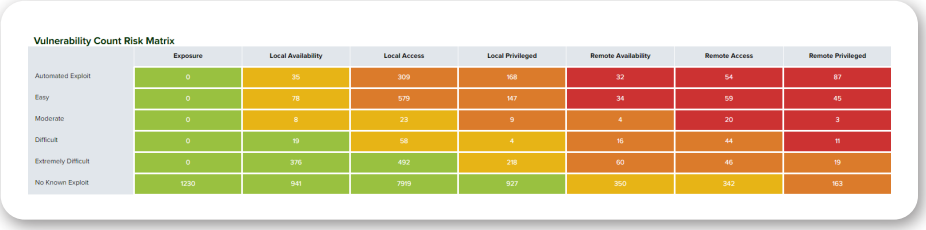
VM Reports

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 be 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



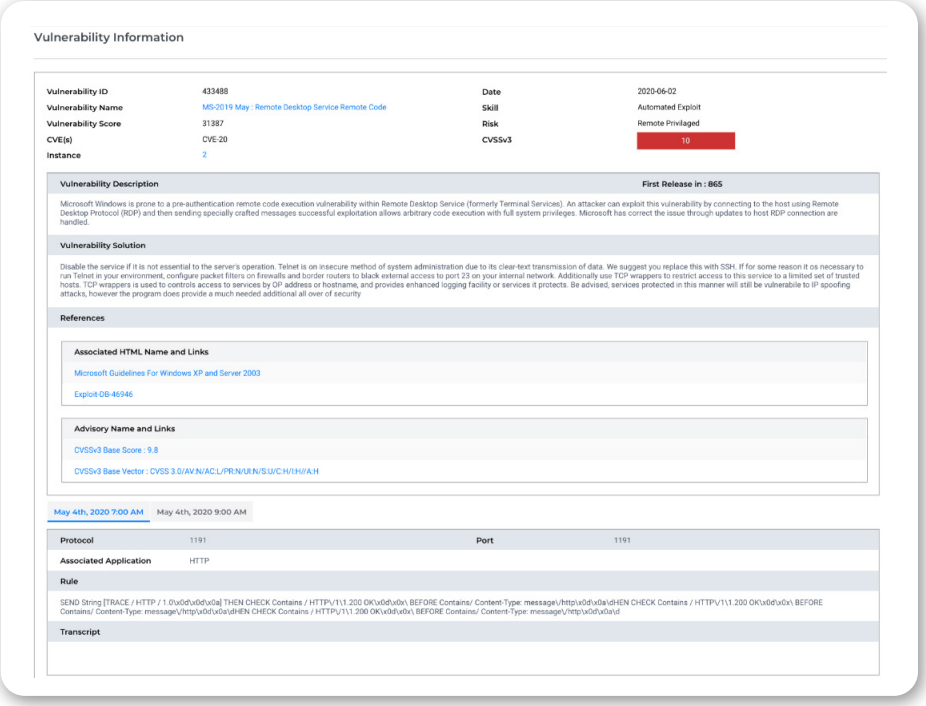
Vulnerability Count Risk Matrix

	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	7919	927	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 — **First Release in : 865**

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.

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 os necessary to run Telnet in your environment, configure packet filters on firewalls and border routers to black 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 controls access to services by OP 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:H/A:H

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\x0d\x0d\x0a] THEN CHECK Contains / HTTP\/1\.1 200 OK\x0d\x0a\ BEFORE Contains/ Content-Type: message\/http\x0d\x0a\dHEN CHECK Contains / HTTP\/1\.1 200 OK\x0d\x0a\ BEFORE Contains/ Content-Type: message\/http\x0d\x0a\dHEN CHECK Contains / HTTP\/1\.1 200 OK\x0d\x0a\ BEFORE Contains/ Content-Type: message\/http\x0d\x0a\d

Transcript

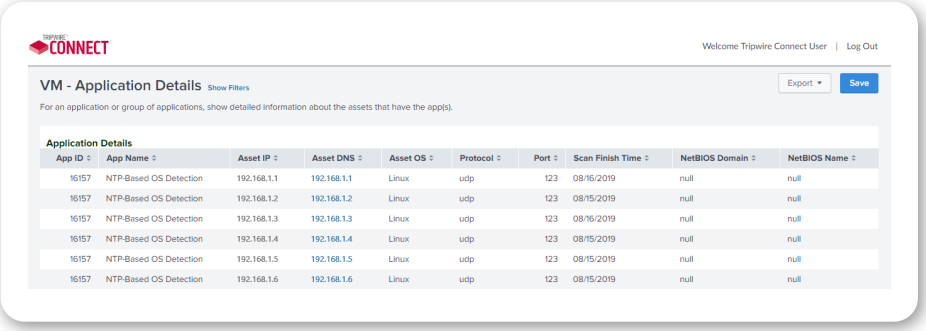
VM – Application Details

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?



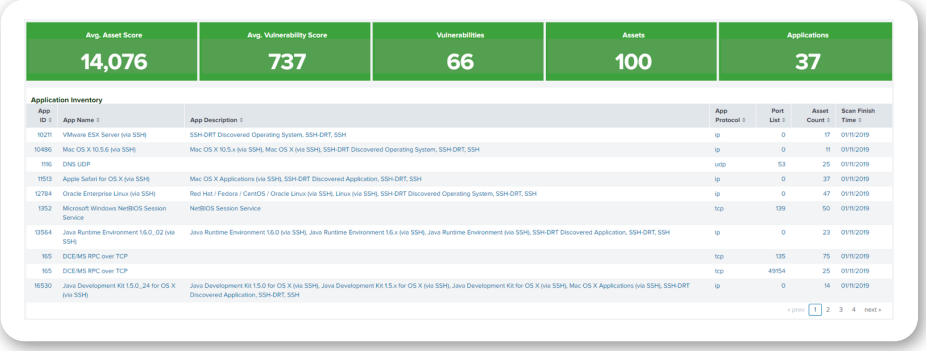
VM – Application Inventory

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?



VM – Asset Details

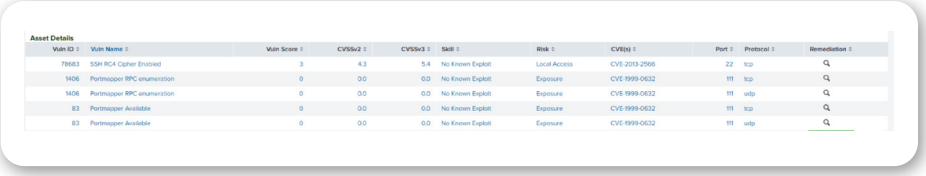
List of the vulnerabilities present on a specific asset

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?

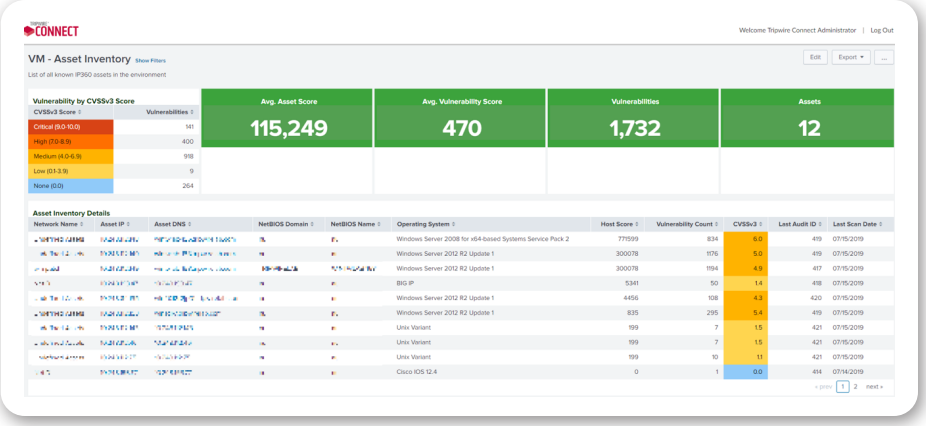


VM – Asset Inventory

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?

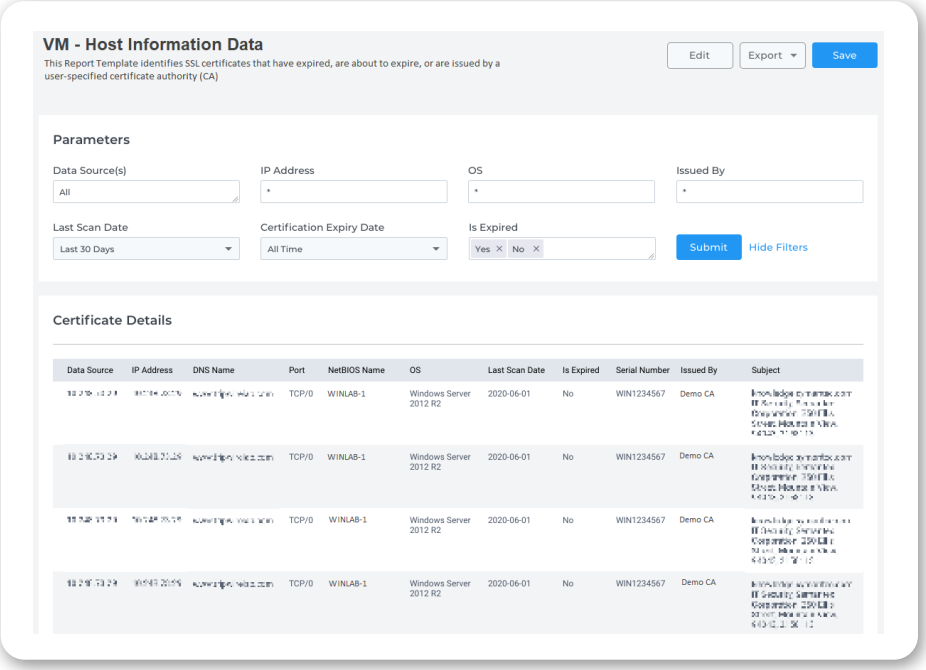


VM – Host Information Data

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 – Vulnerability Details

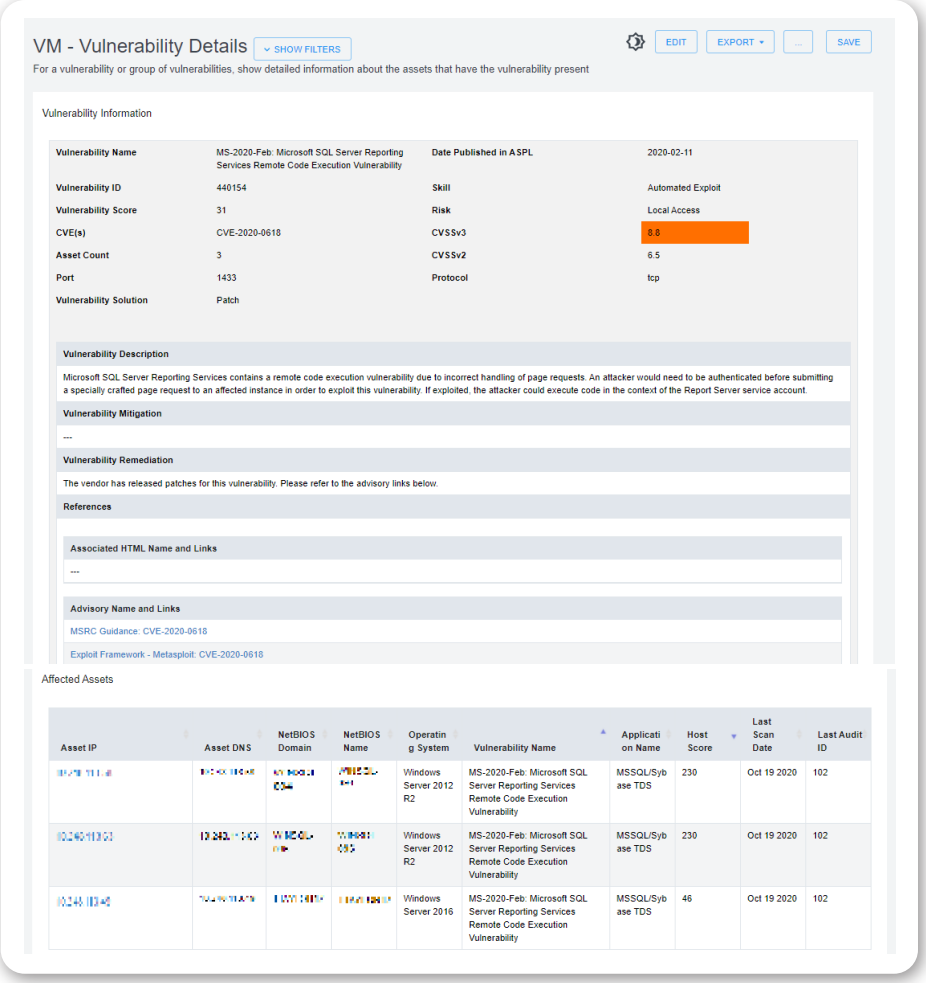
For a vulnerability or group of vulnerabilities, shows detailed information about the assets that have the vulnerability present. Report data can be exported as CSV.

Questions answered:

Which assets have a specific vulnerability?

How do I remediate a specific vulnerability?

Which assets have specific vulnerabilities?

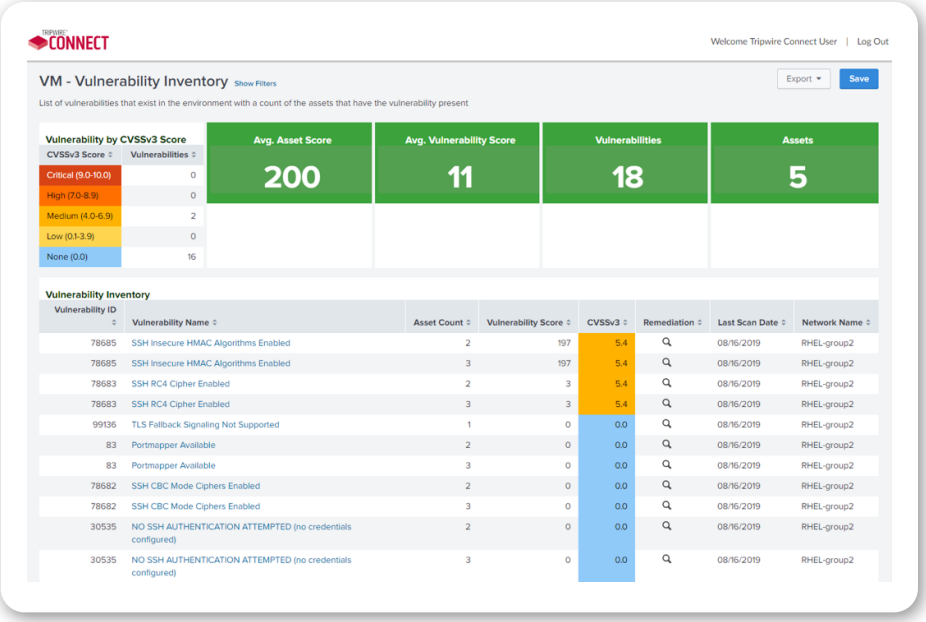


VM – Vulnerability Inventory

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?

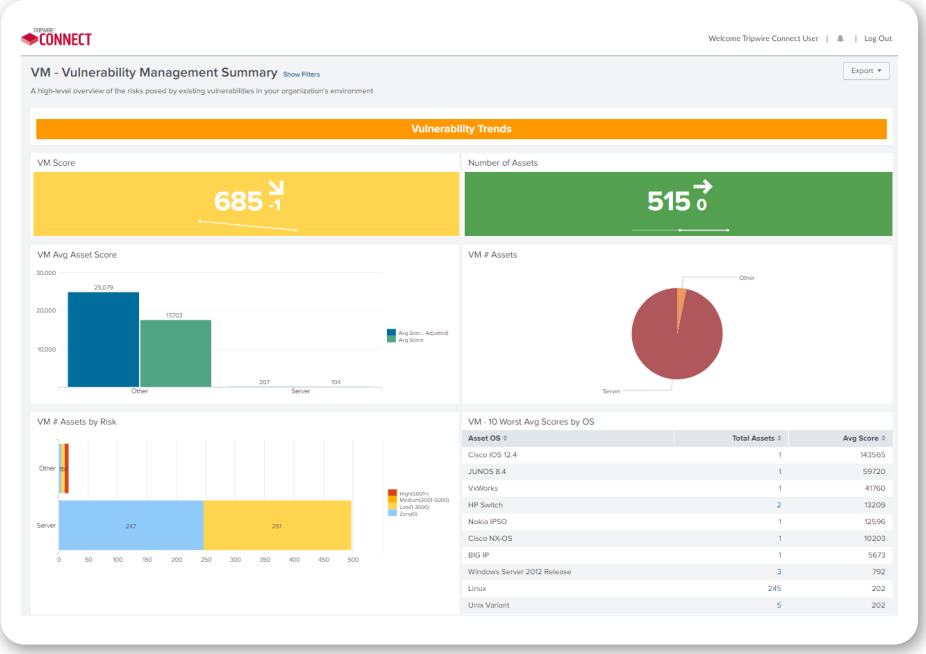


VM – Vulnerability Management Summary

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?

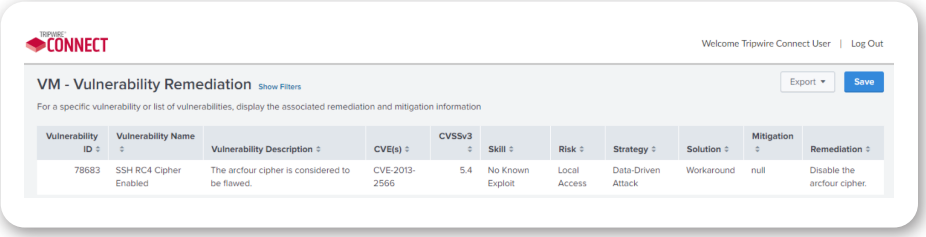


VM – Vulnerability Remediation

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?

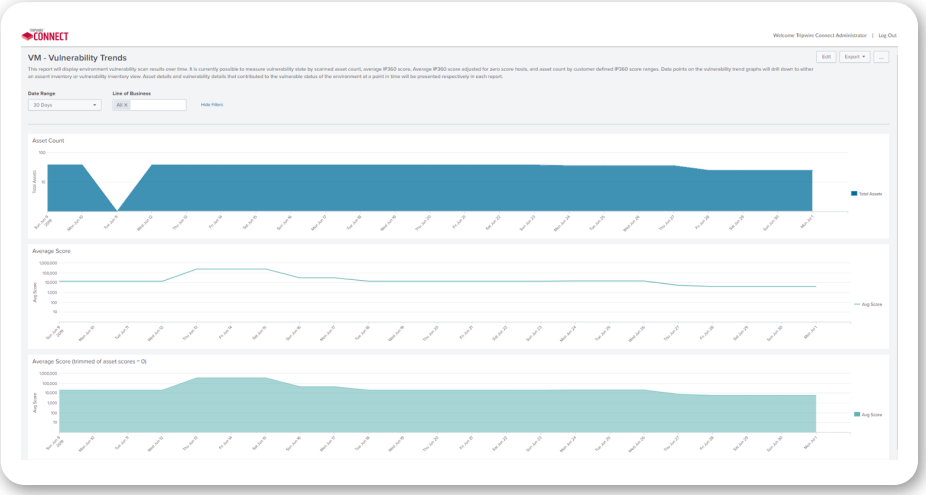


VM – Vulnerability Trends

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

TCRC43a 2012