DATA SHEET

Top Tanium Use Cases

☑ Endpoint Detection and Response

☑ Security Hygiene

☑ IT Operations Management

☑ IT Asset Visibility

Tanium Product Modules

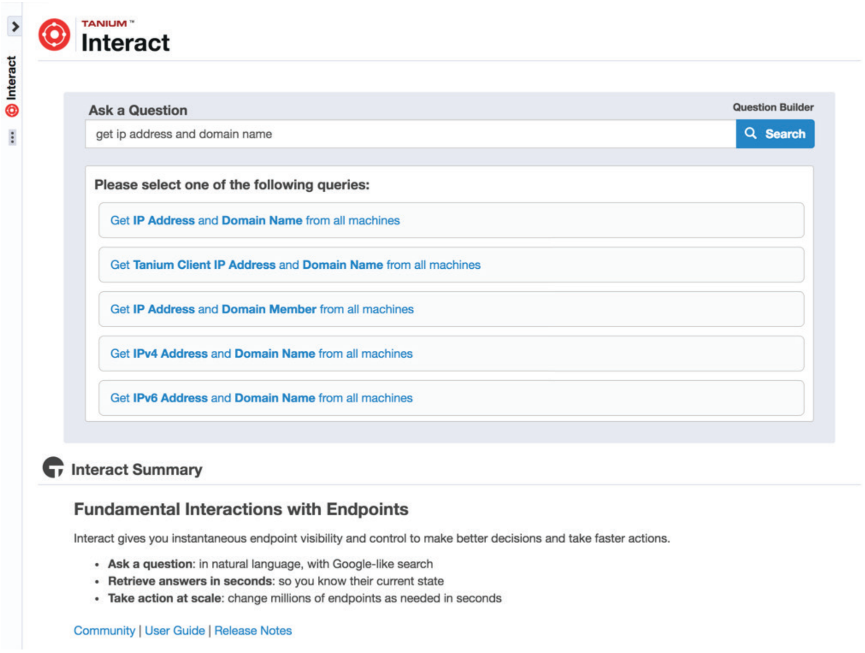
Stop Breaking Your Endpoints

See everything, do anything with Tanium

Relying on a patchwork of point solutions and legacy platforms is a recipe for failure. It's time to re-platform. Take back control with Tanium.

Tanium Core Platform

Regain control by asking questions about endpoints in plain English and getting accurate answers in seconds so corrective action can be taken quickly. Visualize results and feed endpoint data into SIEMs, help desk ticketing systems, CMDBs, and other third-party systems for additional analysis.



Interact

Ask a Question

get ip address and domain name

Please select one of the following queries:

- Get **IP Address** and **Domain Name** from all machines
- Get **Tanium Client IP Address** and **Domain Name** from all machines
- Get **IP Address** and **Domain Member** from all machines
- Get **IPv4 Address** and **Domain Name** from all machines
- Get **IPv6 Address** and **Domain Name** from all machines

Interact Summary

Fundamental Interactions with Endpoints

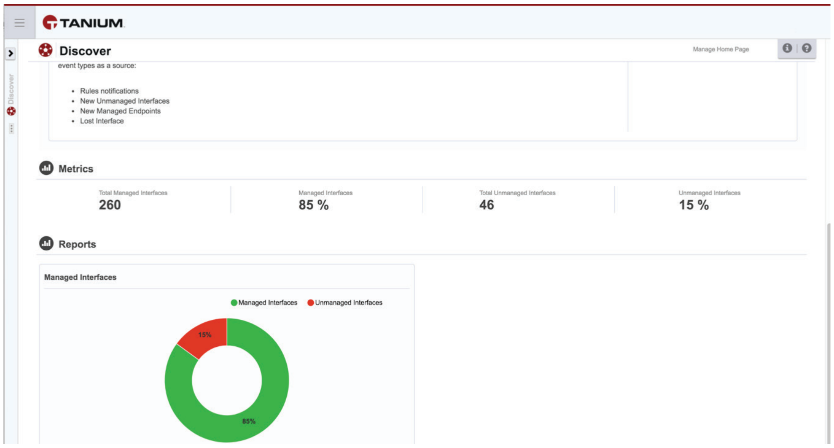
Interact gives you instantaneous endpoint visibility and control to make better decisions and take faster actions.

- **Ask a question**: in natural language, with Google-like search
- **Retrieve answers in seconds**: so you know their current state
- **Take action at scale**: change millions of endpoints as needed in seconds

Community | User Guide | Release Notes

Tanium Discover

Find unmanaged assets within the enterprise environment and bring them under control in seconds. Take immediate action on rogue assets and get a rich set of information for all located assets.



event types as a source:

- Rules notifications
- New Unmanaged Interfaces
- New Managed Endpoints
- Lost Interface

Metrics

Total Managed Interfaces	Managed Interfaces	Total Unmanaged Interfaces	Unmanaged Interfaces
260	85 %	46	15 %

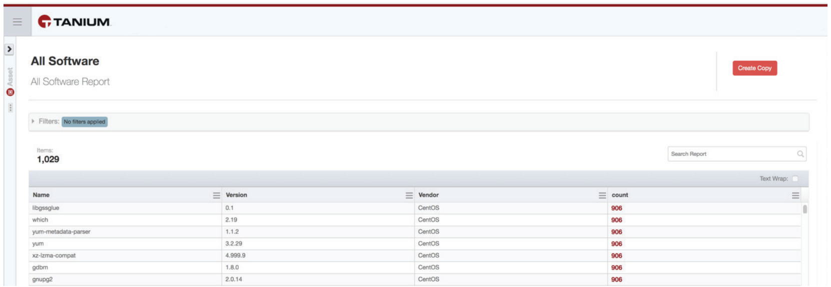
Reports

Managed Interfaces

🟩 Managed Interfaces 🟥 Unmanaged Interfaces

Tanium Asset

Get a thorough and up-to-date picture of hardware and software inventory to make the right decisions deploying assets efficiently, and enrich Configuration Management Databases with accurate information.



All Software

All Software Report

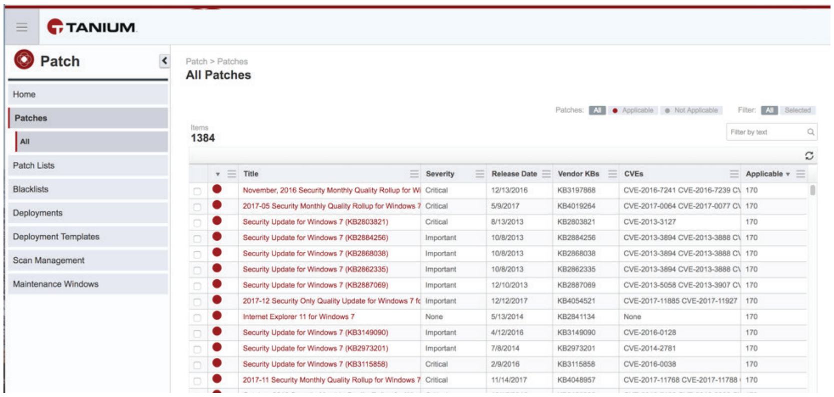
Filters: No filters applied

Items:
1,029

Name	Version	Vendor	count
libgssglue	0.1	CentOS	906
which	2.19	CentOS	906
yum-metadata-parser	1.1.2	CentOS	906
yum	3.2.29	CentOS	906
xz-lzma-compat	4.999.9	CentOS	906
gdbm	1.8.0	CentOS	906
gnupg2	2.0.14	CentOS	906

Tanium Patch

Customize patch workflows with up-to-the-second endpoint visibility and control. Define custom workflows and generate patch reports from every endpoint across the environment.



Patch > Patches

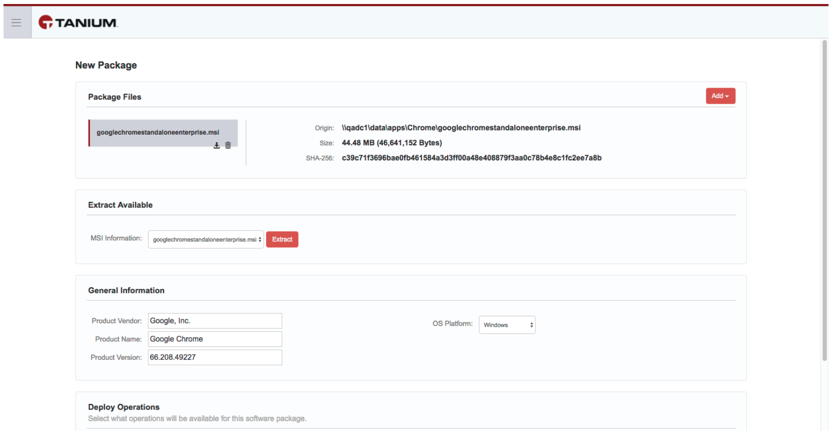
All Patches

Items
1384

		Title	Severity	Release Date	Vendor KBs	CVEs	Applicable
□	●	November, 2016 Security Monthly Quality Rollup for Wi	Critical	12/13/2016	KB3197868	CVE-2016-7241 CVE-2016-7239 CV	170
□	●	2017-05 Security Monthly Quality Rollup for Windows 7	Critical	5/9/2017	KB4019264	CVE-2017-0064 CVE-2017-0077 CV	170
□	●	Security Update for Windows 7 (KB2803821)	Critical	8/13/2013	KB2803821	CVE-2013-3127	170
□	●	Security Update for Windows 7 (KB2884256)	Important	10/8/2013	KB2884256	CVE-2013-3894 CVE-2013-3888 CV	170
□	●	Security Update for Windows 7 (KB2868038)	Important	10/8/2013	KB2868038	CVE-2013-3894 CVE-2013-3888 CV	170
□	●	Security Update for Windows 7 (KB2862335)	Important	10/8/2013	KB2862335	CVE-2013-3894 CVE-2013-3888 CV	170
□	●	Security Update for Windows 7 (KB2887069)	Important	12/10/2013	KB2887069	CVE-2013-5058 CVE-2013-3907 CV	170
□	●	2017-12 Security Only Quality Update for Windows 7 fc	Important	12/12/2017	KB4054521	CVE-2017-11885 CVE-2017-11927	170
□	●	Internet Explorer 11 for Windows 7	None	5/13/2014	KB2841134	None	170
□	●	Security Update for Windows 7 (KB3149090)	Important	4/12/2016	KB3149090	CVE-2016-0128	170
□	●	Security Update for Windows 7 (KB2973201)	Important	7/8/2014	KB2973201	CVE-2014-2781	170
□	●	Security Update for Windows 7 (KB3115858)	Critical	2/9/2016	KB3115858	CVE-2016-0038	170
□	●	2017-11 Security Monthly Quality Rollup for Windows 7	Critical	11/14/2017	KB4048957	CVE-2017-11768 CVE-2017-11788	170

Tanium Deploy

Simplify software deployment, update, repair, and reclamation to reduce risk and cost.



New Package

Package Files

googlechromestandaloneenterprise.msi

Origin: \\qadc1\data\apps\Chrome\googlechromestandaloneenterprise.msi
Size: 44.48 MB (46,641,152 Bytes)
SHA-256: c39c71f3696bae0fb461584a3d3ff00a48e408879f3aa0c78b4e8c1fc2ee7a8b

Extract Available

MSI Information: googlechromestandaloneenterprise.msi

General Information

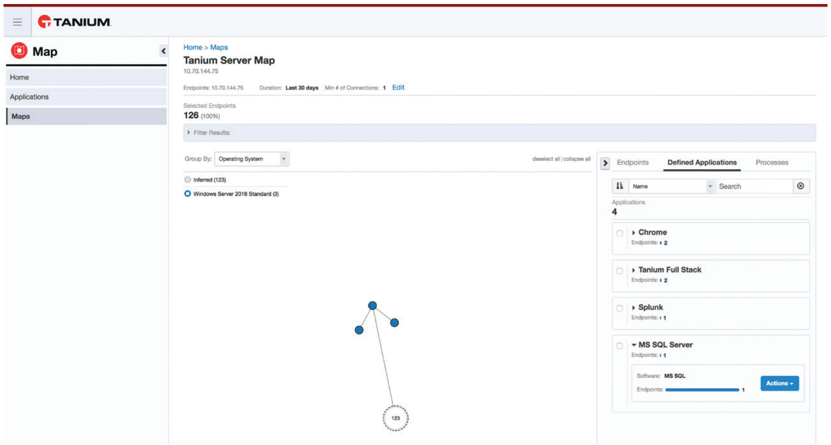
Product Vendor: Google, Inc.
Product Name: Google Chrome
Product Version: 66.208.49227
OS Platform: Windows

Deploy Operations

Select what operations will be available for this software package.

Tanium Map

Quickly and precisely understand your application infrastructure and interrelationships between endpoints. Prevent self-inflicted outages, identify single points of failure, provide redundancy, and segment applications.



Home > Maps

Tanium Server Map

10.70.144.75

Endpoints: 10.70.144.75 Duration: Last 30 days Min # of Connections: 1 Edit

Selected Endpoints
126 (100%)

Filter Results:

Group By: Operating System

Inferred (123)
Windows Server 2016 Standard (3)

Applications
4

Chrome
Endpoints: 2

Tanium Full Stack
Endpoints: 2

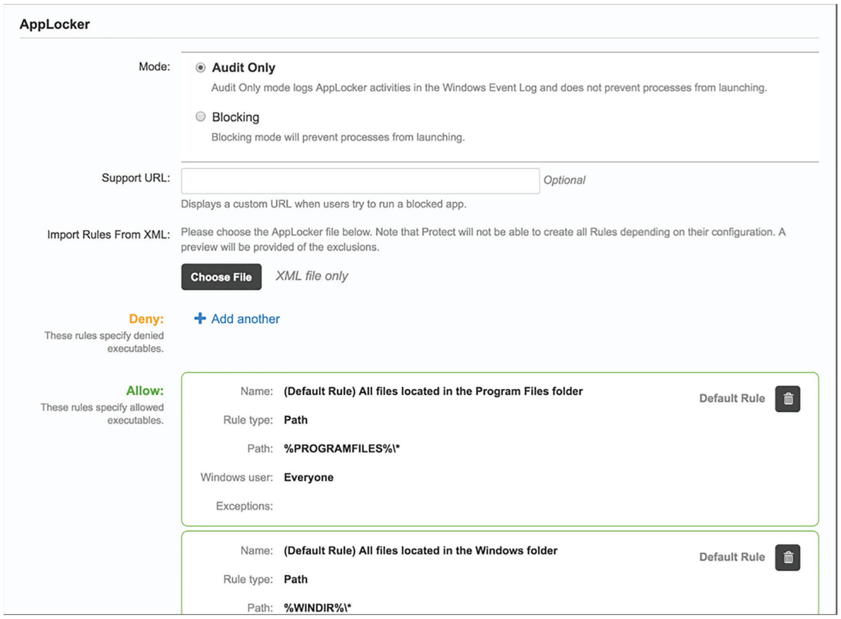
Splunk
Endpoints: 1

MS SQL Server
Endpoints: 1

Software: MS SQL
Endpoints: 1

Tanium Protect

Manage native operating system controls at enterprise scale. Simplify application control, anti-malware, and exploit mitigation to reduce the cost and complexity of endpoint security.



AppLocker

Mode:

● **Audit Only**
Audit Only mode logs AppLocker activities in the Windows Event Log and does not prevent processes from launching.

○ Blocking
Blocking mode will prevent processes from launching.

Support URL: ________ *Optional*
Displays a custom URL when users try to run a blocked app.

Import Rules From XML: Please choose the AppLocker file below. Note that Protect will not be able to create all Rules depending on their configuration. A preview will be provided of the exclusions.

XML file only

Deny: These rules specify denied executables.

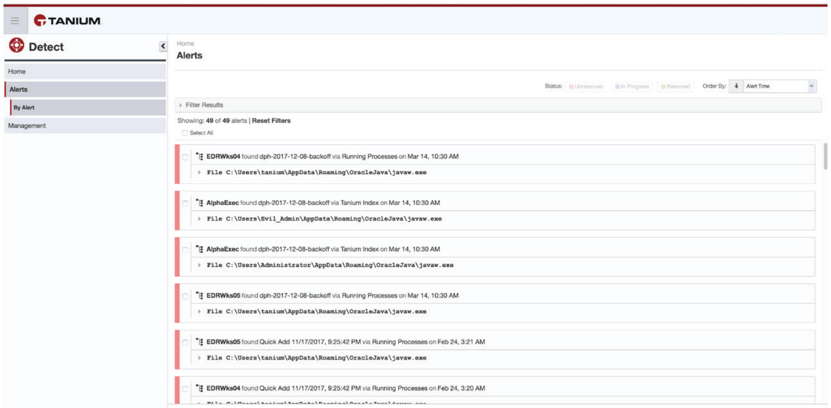
Allow: These rules specify allowed executables.

Name: **(Default Rule) All files located in the Program Files folder** — Default Rule
Rule type: **Path**
Path: **%PROGRAMFILES%***
Windows user: **Everyone**
Exceptions:

Name: **(Default Rule) All files located in the Windows folder** — Default Rule
Rule type: **Path**
Path: **%WINDIR%***

Tanium Threat Response

Hunt, detect, investigate, contain, and remediate threats and vulnerabilities with speed and scalability. Quickly piece together the story of what happened on a single endpoint and remediate endpoints across the enterprise in seconds.



Home
Alerts

Status: Unresolved In Progress Resolved Order By: Alert Time

Filter Results

Showing: **49** of **49** alerts | **Reset Filters**

□ Select All

□ **EDRWks04** found dph-2017-12-08-backoff via Running Processes on Mar 14, 10:30 AM
`File C:\Users\tanium\AppData\Roaming\OracleJava\javaw.exe`

□ **AlphaExec** found dph-2017-12-08-backoff via Tanium Index on Mar 14, 10:30 AM
`File C:\Users\Evil_Admin\AppData\Roaming\OracleJava\javaw.exe`

□ **AlphaExec** found dph-2017-12-08-backoff via Tanium Index on Mar 14, 10:30 AM
`File C:\Users\Administrator\AppData\Roaming\OracleJava\javaw.exe`

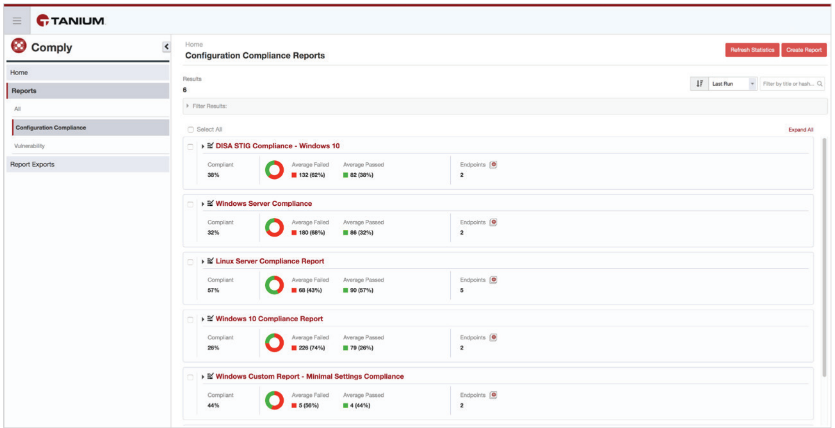
□ **EDRWks05** found dph-2017-12-08-backoff via Running Processes on Mar 14, 10:30 AM
`File C:\Users\tanium\AppData\Roaming\OracleJava\javaw.exe`

□ **EDRWks05** found Quick Add 11/17/2017, 9:25:42 PM via Running Processes on Feb 24, 3:21 AM
`File C:\Users\tanium\AppData\Roaming\OracleJava\javaw.exe`

□ **EDRWks04** found Quick Add 11/17/2017, 9:25:42 PM via Running Processes on Feb 24, 3:20 AM

Tanium Comply

Check endpoints against standard security benchmarks to simplify security hygiene, compliance, and audit preparation.



Home

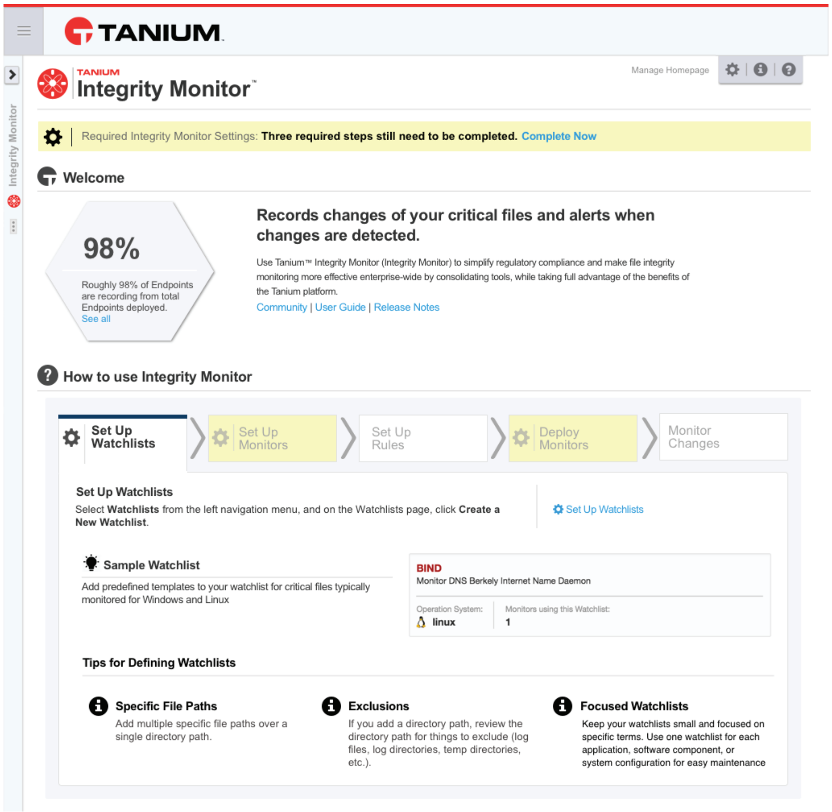
Configuration Compliance Reports

Results
6

Report	Compliant	Average Failed	Average Passed	Endpoints
DISA STIG Compliance - Windows 10	38%	132 (62%)	82 (38%)	2
Windows Server Compliance	32%	180 (68%)	86 (32%)	2
Linux Server Compliance Report	57%	68 (43%)	90 (57%)	5
Windows 10 Compliance Report	26%	226 (74%)	79 (26%)	2
Windows Custom Report - Minimal Settings Compliance	44%	5 (56%)	4 (44%)	2

Tanium Integrity Monitor

Improve regulatory compliance by linking file integrity monitoring with active alert investigation, configuration compliance, and vulnerability scanning.



Required Integrity Monitor Settings: **Three required steps still need to be completed.** Complete Now

Welcome

98%

Roughly 98% of Endpoints are recording from total Endpoints deployed.
See all

Records changes of your critical files and alerts when changes are detected.

Use Tanium™ Integrity Monitor (Integrity Monitor) to simplify regulatory compliance and make file integrity monitoring more effective enterprise-wide by consolidating tools, while taking full advantage of the benefits of the Tanium platform.

Community | User Guide | Release Notes

How to use Integrity Monitor

Set Up Watchlists

Select **Watchlists** from the left navigation menu, and on the Watchlists page, click **Create a New Watchlist**.

Set Up Watchlists

Sample Watchlist

Add predefined templates to your watchlist for critical files typically monitored for Windows and Linux

BIND
Monitor DNS Berkely Internet Name Daemon

Operation System: linux
Monitors using this Watchlist: 1

Tips for Defining Watchlists

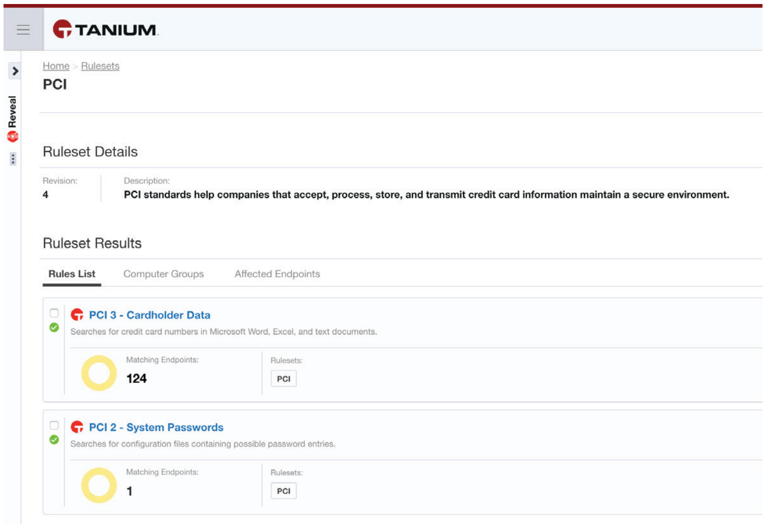
Specific File Paths
Add multiple specific file paths over a single directory path.

Exclusions
If you add a directory path, review the directory path for things to exclude (log files, log directories, temp directories, etc.).

Focused Watchlists
Keep your watchlists small and focused on specific terms. Use one watchlist for each application, software component, or system configuration for easy maintenance

Tanium Reveal

Reduce risks of data exposure, mitigate the impact of breaches, & meet regulatory compliance.



PCI

Ruleset Details

Revision: 4

Description: PCI standards help companies that accept, process, store, and transmit credit card information maintain a secure environment.

Ruleset Results

☐ ✓ PCI 3 - Cardholder Data

Searches for credit card numbers in Microsoft Word, Excel, and text documents.

Matching Endpoints: 124

Rulesets: PCI

☐ ✓ PCI 2 - System Passwords

Searches for configuration files containing possible password entries.

Matching Endpoints: 1

Rulesets: PCI

TANIUM

Tanium gives the world's largest enterprises and government organizations the unique power to secure, control and manage millions of endpoints across the enterprise within seconds. With the unprecedented speed, scale and simplicity of Tanium, security and IT operations teams now have complete and accurate information on the state of endpoints at all times to more effectively protect against modern day threats and realize new levels of cost efficiency in IT operations.

tanium.com

@Tanium

info@tanium.com