Tanium Benchmark User Guide

2026H2 Semiannual Release

Version 2.19

November 20, 2026



The information in this document is subject to change without notice. Further, the information provided in this document is provided "as is" and is believed to be accurate, but is presented without any warranty of any kind, express or implied, except as provided in Tanium's customer sales terms and conditions. Unless so otherwise provided, Tanium assumes no liability whatsoever, and in no event shall Tanium or its suppliers be liable for any indirect, special, consequential, or incidental damages, including without limitation, lost profits or loss or damage to data arising out of the use or inability to use this document, even if Tanium Inc. has been advised of the possibility of such damages.

Any IP addresses used in this document are not intended to be actual addresses. Any examples, command display output, network topology diagrams, and other figures included in this document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

Please visit https://help.tanium.com for the most current Tanium product documentation.

This documentation may provide access to or information about content, products (including hardware and software), and servicesprovided by third parties ("Third Party Items"). With respect to such Third Party Items, Tanium Inc. and its affiliates (i) are not responsible for such items, and expressly disclaim all warranties and liability of any kind related to such Third Party Items and (ii) will not be responsible for any loss, costs, or damages incurred due to your access to or use of such Third Party Items unless expressly set forth otherwise in an applicable agreement between you and Tanium.

Further, this documentation does not require or contemplate the use of or combination with Tanium products with any particular Third Party Items and neither Tanium nor its affiliates shall have any responsibility for any infringement of intellectual property rights caused by any such combination. You, and not Tanium, are responsible for determining that any combination of Third Party Items with Tanium products is appropriate and will not cause infringement of any third party intellectual property rights.

Tanium is committed to the highest accessibility standards for our products. To date, Tanium has focused on compliance with U.S.Federal regulations - specifically Section 508 of the Rehabilitation Act of 1998. Tanium has conducted 3rd party accessibility assessments over the course of product development for many years. We certify against the WCAG 2.2 / VPAT 2.5 standards for all major product modules. Tanium performs ongoing reassessments as appropriate, given the scope and type of changes to the UI and product features from release to release. In the most recent testing, the Tanium Console UI achieved supports or partially supports for all applicable WCAG 2.2 criteria. Tanium can make available any VPAT reports on a module-by-module basis as part of a larger solution planning process for any customer or prospect.

As new products and features are continuously delivered, Tanium will conduct testing to identify potential gaps in compliance with accessibility guidelines. Tanium is committed to making commercially reasonable efforts to address any gaps as quickly as is feasible, given the severity of the issue and scope of the changes. Tanium factors these objectives into the ongoing delivery schedule of features and releases with our existing resources.

Tanium welcomes customer input on making solutions accessible based on your Tanium modules and assistive technology requirements. Accessibility requirements are important to the Tanium customer community and we are

©2026 Tanium Inc. All Rights Reserved

committed to prioritizing these compliance efforts as part of our overall product roadmap. Tanium maintains transparency on our progress and milestones and welcomes any further questions or discussion around this work. Contact your sales representative, Tanium Support atsupport@tanium.com, or email accessibility@tanium.com to make further inquiries.

Tanium is a trademark of Tanium, Inc. in the U.S. and other countries. Third-party trademarks mentioned are the property of the irrespective owners.

Kubernetes®, K8s®, and the Kubernetes logo are registered trademarks of The Linux Foundation®.

Android, ChromeOS, and Google are trademarks of Google LLC.

iOS, iPad, iPadOS, iPhone, Mac, and macOS are trademarks of Apple Inc., and registered in the U.S. and other countries and regions.

Patents: https://www.tanium.com/patents

Tanium Open Source Disclosure : https://tanium.github.io/opensource/

© 2026 Tanium Inc. All rights reserved.

Table of contents

Overview 8
- Benchmarks 8
- Risk score 10
- Vulnerabilities 10
- Tanium Risk Assessment 10
- Tanium Autonomous IT Platform in Benchmark 11
- Interoperability with other Tanium products 11

Gaining organizational effectiveness 13

Requirements 18
- Core platform dependencies 18
- Solution dependencies 18
  - Tanium recommended installation 18
  - Import specific solutions 19
  - Required dependencies 19
  - Feature-specific dependencies 19
- Client extensions and endpoint tools 20
- Tanium™ Module Server 20
- Endpoints 20
  - Supported Internet protocols 21
  - Supported operating systems 21
- Host and network security requirements 21
  - Ports 21
    - Ports for Benchmark communication 22
  - Security exclusions 22
    - Benchmark server exclusions 22
    - Benchmark endpoint exclusions 23
- User role requirements 23
  - Optional Benchmark role for Guide observations 26

©2026 Tanium Inc. All Rights Reserved

Solutions and permissions for Tanium Risk Assessment 26

Installing 29
Before you begin 29
Import Benchmark with default settings 30
Default settings for Benchmark 30
Import Benchmark with custom settings 30
Manage solution dependencies 31
Upgrade Benchmark 31
Verify Benchmark version 31

Configuring 32
Restricted targeting 32
Tanium Endpoint Configuration 32
Manage solution configurations with Tanium Endpoint Configuration 32
Configure Benchmark 34
Configure the Benchmark action group 34
(Optional) Set company name 35
(Optional) Set industry 35
(Optional) Configure computer groups 35
(Optional) Configure data collection frequency 36
(Optional) Assign target goals 36
(Optional) Assign endpoint criticality 37
(Optional) Enable data collection for Tanium Risk Assessment 37
Tanium Criticality Endpoint Rules 38
Set up Benchmark users 39
Registered sensors 40
(Optional) Enable Benchmark scheduled actions 40
(Optional) Configure port exclusions for Certificate Manager 41
Configure port exclusions if Certificate Manager is installed 41
Configure port exclusions if Certificate Manager is not installed 41
Add port exclusions 42
Delete port exclusions 42

Evaluating your risk score 44
Risk score calculation 44

©2026 Tanium Inc. All Rights Reserved

Risk score range 44
Risk score formulas 45
Risk score metrics 45
Endpoint criticality value 46
View risk score 46

Reviewing benchmark metrics 48
Benchmark values 48
View benchmarks 48
Investigate benchmark results 50
Summary 50
Results 51
Endpoints 51
Set benchmark target goals 52
About bell curve charts 53
Enterprise Risk metrics 54
Guardian metrics 56
July 2025 SharePoint Server RCE Vulnerabilities 56
June 2025 Windows SMB Signing - Kerberos Reflection 56
Security metrics 56
Operations metrics 59

Reviewing your risk dashboards 62
View the dashboards 62
Inventory 62
CISA Known Exploited Vulnerability Metrics 63
Vulnerability Management 65
Patch Management 66
Software Management and Distribution 67
Asset Health and Security 68
What to do next 69

Reviewing your vulnerability dashboards 71
Vulnerability impact and priority calculation 71
Vulnerability impact formula 71
Vulnerability priority formula 71

©2026 Tanium Inc. All Rights Reserved

Endpoint criticality value 71
View your vulnerability dashboard 72
Vulnerability metrics 72
CVEs sorted by vulnerability priority 73

Generating the Tanium Risk Assessment 76

Troubleshooting 78
Collect logs 78
Perform monthly maintenance 78
Monitor and troubleshoot Benchmark metric health 79
Metric Health for Supported Endpoints 79
Metric Health 79
Improve Metric Health 79
Unable to generate or export Tanium Risk Assessment 80
Remove Benchmark tools from endpoints 81
Uninstall Benchmark 83
Contact Tanium Support 83

Reference: Gateway examples for Benchmark 84
Get endpoint with Tanium Risk Score 2.0 information 84

©2026 Tanium Inc. All Rights Reserved

Benchmark overview

Use Tanium Benchmark to understand the state of your security program, compared to other Tanium™ Cloud customers. You can use the reports to communicate key trends, improvements, and industry benchmarks for executive and board-level reporting. By using Benchmark to continuously monitor Tanium Client managed endpoints, you can improve your compliance and risk posture.

Benchmarks

Use benchmark metrics to compare your environment to other Tanium customers. Benchmark data is collected from Tanium Cloud customers, where contractually allowed. This data is stored in aggregate and anonymized.

For each metric, the data is presented over time as a percentile value and by detailed data. You can compare your data to the benchmark values.

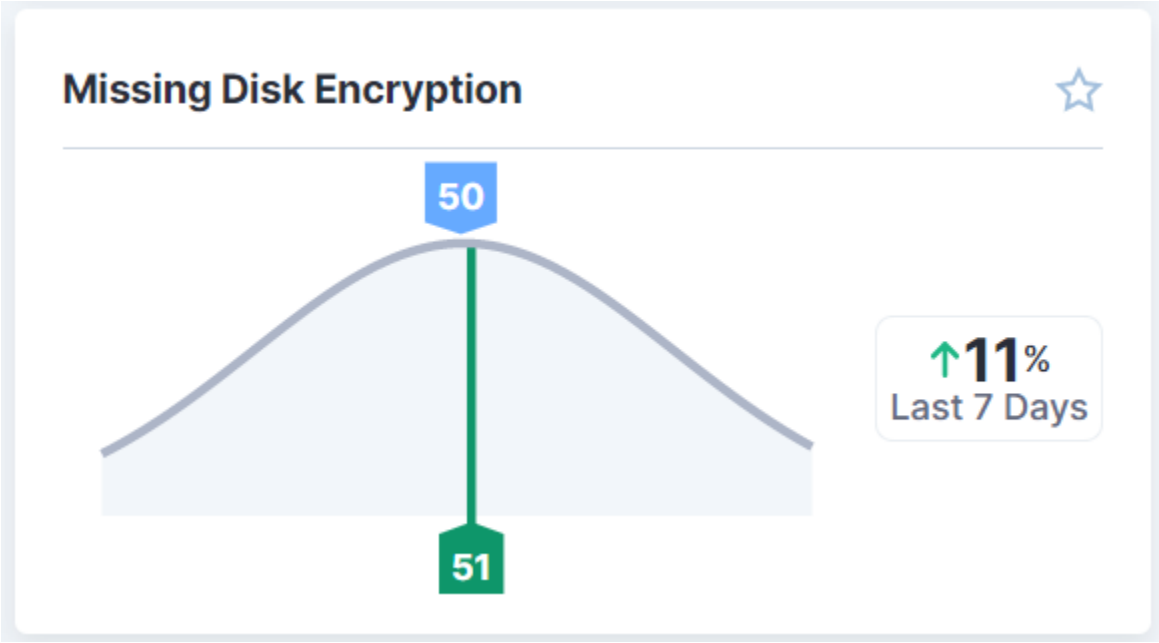
On the Benchmark home page, you can view the metrics as a **Percentile Distribution** or **Percentile Over Time** chart.

Percentile distribution

The **Percentile Distribution** chart for each metric is a bell chart distribution of values across all Tanium customers, and shows the target benchmark percentile you selected, along with your current percentile for the metric. The 50% indicator is the median for this data set. The center of the curve in the chart shows the mean of the data set. In the following example, the target benchmark percentile is 50, and your value is in the 51st percentile.

Figure 1. Missing Disk Encryption Percentile Distribution chart

©2026 Tanium Inc. All Rights Reserved



Percentile over time

The **Percentile Over Time** chart is a time series representation of the data. In the following example, the straight line represents the target benchmark and the data points for this metric in your environment for the selected time period.

Figure 2. Missing Disk Encryption Percentile Over Time chart



For more information about Benchmark metrics, see Reviewing benchmark metrics on page 48.

©2026 Tanium Inc. All Rights Reserved

Risk score

Benchmark calculates Tanium risk score using narrowly defined risk metrics. Risk metrics each measure one specific attribute.

Important: You must have Tanium Comply installed and configured to view the risk score.

The risk score is a numerical score that represents the overall risk of the enterprise based on data from every managed endpoint. The possible range for a risk score is 1-1000. A lower score indicates a lower risk for the enterprise or endpoint. Scores are categorized into low, medium, high, or critical:

- Low: 1-250
- Medium: 251-500
- High: 501-750
- Critical: 751-1000

Benchmark uses Tanium Data Service to include results for offline endpoints. For more information about Tanium Data Service, see Tanium Interact User Guide: Managing Tanium Data Service.

For more information, see Evaluating your risk score on page 44.

Vulnerabilities

Benchmark evaluates the vulnerabilities in your environment and provides both an impact score and priority score for each vulnerability.

Vulnerability impact scores are calculated by multiplying CVSS score and the number of endpoints that contain the vulnerability. Vulnerability priority scores are a calculation of vulnerability impact scores and endpoint criticality values.

For more information, see Reviewing your vulnerability dashboards on page 71.

Tanium Risk Assessment

©2026 Tanium Inc. All Rights Reserved

A Tanium Risk Assessment is a report of operational and security risks in your organization. The assessment is based on metrics and data points identified during the evaluation. The assessment provides dynamic scoring for each endpoint against multiple risks. The assessment is targeted at organizational executives and board members and can be useful for executive reporting to highlight areas of risk and trends over time.

You can generate an executive summary or a more extensive detailed report. You can export the assessment to JSON or HTML, so you can import the data into your own solutions. For more information, see Generating the Tanium Risk Assessment on page 76.

For ongoing visibility into operational and security risks, use the **Risk Dashboards** page. For more information, see Reviewing your risk dashboards on page 62.

Tanium Autonomous IT Platform in Benchmark

Tanium Autonomous IT Platform comprises a set of interrelated features across multiple Tanium solutions. The Autonomous IT Platform provides guided initial configuration for solutions, proactively collects intelligence about conditions in Tanium environments, provides guidance based on those conditions, and enables automated workflows to address issues. For more information, see Tanium Console User Guide: Working with the Tanium Autonomous IT Platform. Tanium Benchmark provides the following Autonomous IT Platform features:

- **Guide notifications**: Benchmark can generate Guide observations related to risk score and benchmark metric changes. Tanium operators who receive these observations can view the risk score or benchmark metrics and remediate the situation. For more information, see Evaluating your risk score on page 44, Reviewing benchmark metrics on page 48, and Tanium Guide User Guide: Viewing and managing notifications.

Interoperability with other Tanium products

Benchmark works with other Tanium products that provide benchmark metrics or additional features. The metrics that display are affected by which products are installed. For more information, see Reviewing benchmark metrics on page 48.

Comply

Tanium™ Comply provides data about endpoint vulnerabilities and compliance to Benchmark for risk

©2026 Tanium Inc. All Rights Reserved

score calculations.

Criticality

Tanium™ Criticality provides data about the relative importance of each endpoint for risk score calculations.

Guide

Tanium™ Guide can generate Benchmark-related notifications for Tanium operators, which provide insight into Tanium, network, and endpoint performance.

For more information, see Tanium Guide User Guide: Overview.

Impact

Tanium™ Impact provides data about administrative access for endpoints, users, and groups to Benchmark for risk score calculations.

©2026 Tanium Inc. All Rights Reserved

Gaining organizational effectiveness with Benchmark

The four key organizational governance steps to maximizing the value that is delivered by Benchmark are as follows:

- Develop a dedicated change management process. For more information, see Change management on page 13.
- Define distinct roles and responsibilities. For more information, see RACI chart on page 14.
- Track operational maturity. For more information, see Operational metrics on page 15.
- Validate cross-functional alignment. For more information, see Organizational alignment on page 15.

Change management

Develop a tailored, dedicated change management process for risk management, taking into account the new capabilities provided by Tanium.

- Update SLAs and align activities to key resources for risk management activities across IT Security, IT Operations, and IT Risk and Compliance based on industry comparisons.
- Identify internal and external dependencies to your risk management process. For example, achieve effective integrations with Tanium Comply and Tanium™ Patch.
- Designate change or maintenance windows for various risk management scenarios. For example, emergency patching versus general maintenance patching.
- Create a Tanium steering group (TSG) for risk management activities, to expedite reviews and approvals of processes that align with SLAs.

©2026 Tanium Inc. All Rights Reserved

RACI chart

A RACI chart identifies the team or resource who is Responsible, Accountable, Consulted, and Informed, and serves as a guideline to describe the key activities across the security, risk/ compliance, and operations teams. Every organization has specific business processes and IT organization demands. The following table represents Tanium's point of view for how organizations should align functional resources against risk management. Use the following table as a baseline example.

RACI chart for Tanium Benchmark

Task	IT Security	IT Operations	IT Risk/ Compliance	Executive	Rationale
Benchmark coverage of endpoints	C	A/R	C	-	The IT Operations team owns the Tanium platform and is accountable and responsible for the deployment of the Tanium Client, including the Benchmark module. Tanium Client coverage is essential to understand risk in the environment. IT Operations consults with the IT Security and IT Compliance teams on the coverage to identify gaps.
Identify and monitor business critical endpoints	A	R	C	I	The IT Security team monitors business critical endpoints to ensure actions can be taken to reduce risk. The IT Operations team identifies business critical assets and consults with the IT Compliance team to ensure accurate identification of those business critical endpoints. The Executive team is informed to monitor risk.
Monitor the risk score for the enterprise	A/R	R	R	C	The IT Security team monitors the risk score for the enterprise so that action can be taken if the risk score is too high or deviates significantly from the industry benchmark. The IT Operations and IT Compliance teams define asset criticality, ensure Benchmark coverage, and

©2026 Tanium Inc. All Rights Reserved

Task	IT Security	IT Operations	IT Risk/ Compliance	Executive	Rationale
					take necessary actions to reduce the risk score over time. The Executive team is consulted on acceptable risk levels and the actions taken to reduce risk.

Organizational alignment

Successful organizations use Tanium across functional silos as a common platform for high-fidelity endpoint data and unified endpoint management. Tanium provides a common data schema that enables security, operations, and risk/compliance teams to assure that they are acting on a common set of facts that are delivered by a unified platform.

In the absence of cross-functional alignment, functional silos often spend time and effort in litigating data quality instead of making decisions to improve risk management.

Operational metrics

Risk maturity

Benchmark provides components of operational and security-based risk management. A risk management program successfully includes operationalization of the technology and measuring success through key metrics. The four key processes to measure and guide operational maturity of your Tanium Benchmark program are as follows:

Processes to measure Tanium Benchmark maturity

Process	Description
Usage	how and where Tanium Benchmark is used in your organization
Functional Integration	how integrated Tanium Benchmark is, across IT security, IT operations, and IT risk/compliance teams

©2026 Tanium Inc. All Rights Reserved

Process	Description
Reporting	how automated Tanium Benchmark is and who the audience of reporting is

Benchmark operational maturity metrics

In addition to the key processes, the four key benchmark metrics that align to the operational maturity of the Tanium Benchmark program to achieve maximum value and success are as follows:

Benchmark metrics for Tanium Benchmark maturity

Executive Metrics	Benchmark Metrics Health	Tanium Risk Score
Description	Percentage of endpoints on which all metrics were calculated in the last 30 days.	A numerical score that represents the overall risk of the enterprise based on data from every managed endpoint.
Instrumentation	Benchmark provides a dedicated page that uses endpoint health reporting, module health reporting, and Endpoint Configuration Framework (ECF) reporting to identify the health of individual metrics for measured endpoints. For more information, see the **Metric Health for Supported Endpoints** chart and Tanium Endpoint Configuration on page 32 .	For more information about how the risk score is calculated, see Risk score calculation on page 44 .
Why this metric matters	If you are not including all appropriate endpoints in your metrics, you do not have a complete picture of your environment.	As you lower the risk score for your enterprise, you improve your compliance and risk posture.

Use the following table to determine the maturity level for Tanium Benchmark in your organization.

©2026 Tanium Inc. All Rights Reserved

Maturity levels for Tanium Benchmark maturity

		Level 1 (Initializing)	Level 2 (Progressing)	Level 3 (Intermediate)	Level 4 (Mature)	Level 5 (Optimized)
Process	Usage	No dependent modules are configured, and endpoint criticality is left at the default values for all endpoints.	Core content and Comply are configured and feeding into Benchmark .	Core content, Comply and one additional dependent module are configured and feeding into Benchmark .	Core content, Comply, Impact and Tanium™ Reveal are configured and feeding into Benchmark , but not on all applicable endpoints.	Core content, Comply, Impact and Reveal are configured and feeding into Benchmark , and asset criticality is set for all applicable endpoints.
	Functional integration	Benchmark installed, but dependent modules are not installed or configured.	Core content and Comply are configured and feeding into Benchmark .	Core content, Comply and one additional dependent module are configured and feeding into Benchmark .	Core content, Comply, Impact and one additional module are configured and feeding into Benchmark .	Core content, Comply, Impact and all available modules are configured and feeding into Benchmark .
	Reporting	Manual; Reporting for Operators only	Manual; Reporting for Operators only	Automated; Reporting for Operators only	Automated; Reporting tailored to stakeholders ranging from Operator to Executive	Automated; Reporting tailored to stakeholders ranging from Operator to Executive; Drive business decisions using reports
Metrics	Metrics Coverage	0-49%	50-69%	70-94%	95-98%	≥99%
	Tanium Risk Score	751-1000	501-750	501-750	251-500	0-250

©2026 Tanium Inc. All Rights Reserved

Benchmark requirements

Review the requirements before you install and use Benchmark.

Core platform dependencies

Make sure that your environment meets the following requirements:

- Tanium license that includes the Core Plus bundle. For more information about how to get a bundle, see Tanium Solutions & BundlesTanium Solutions & Bundles.
- Tanium™ Core Platform servers
- Tanium Client:

  Any supported version of Tanium Client. For more information, see Client version and host system requirements. If you use a Client version that is not listed, certain product features might not be available, or stability issues can occur that can only be resolved by upgrading to one of the listed Client versions.

Solution dependencies

Other Tanium solutions are required for Benchmark to function (required dependencies) or for specific Benchmark features to work (feature-specific dependencies). The installation method that you select determines if the Tanium Server automatically imports dependencies or if you must manually import them.

Note: Some Benchmark dependencies have their own dependencies, which you can see in the lists of required and feature-specific dependencies below. Where a dependency links to its own user guide, that link opens the guide for the latest version of the solution, not necessarily the minimum version that Benchmark requires.

Tanium recommended installation

©2026 Tanium Inc. All Rights Reserved

If you select **Tanium Recommended Installation** when you import Benchmark, the Tanium Server automatically imports all your licensed solutions at the same time. For more information, see Tanium Console User Guide: Import all modules and services.

Import specific solutions

If you select only Benchmark to import, the Tanium Server automatically imports the latest available versions of any required dependencies that are missing. If some required dependencies are already imported but their versions are earlier than the minimum required for Benchmark, the server automatically updates those dependencies to the latest available versions.

Required dependencies

Benchmark has the following required dependencies. You must install the dependencies in the listed order.

1. Tanium™ Endpoint Configuration
2. Tanium™ Interact
3. Tanium™ Data Service (TDS)
4. Tanium Criticality
5. Tanium™ RDB Service
6. Tanium™ Reporting Service
    - Tanium™ Blob Service
7. Tanium™ Core Content
    - Tanium™ Core Content SSL/TLS Server Audit sensor

Feature-specific dependencies

If you select only Benchmark to import, you must manually import or update its feature-specific dependencies regardless of the Tanium Console or Tanium Core Platform versions. Benchmark has the following feature-specific dependencies:

©2026 Tanium Inc. All Rights Reserved

- Tanium™ Asset is required to show asset details for endpoints.
- Tanium Comply is required to view the System Vulnerability and System Compliance metrics.
- Tanium Impact is required to view the Administrative Access metric.
- Tanium Patch is required to view related patches on endpoints.
- Tanium Reveal is required to view the Password Identification metric.
- Tanium™ Emerging Issues Content is required to view Guardian metrics.
- The detailed report of the Tanium Risk Assessment requires specific solutions for each section. For more information, see Solutions and permissions for Tanium Risk Assessment on page 26.

Client extensions and endpoint tools

Tanium Endpoint Configuration installs Client Extensions and other tools for endpoints. Client extensions perform tasks that are common to certain Tanium solutions. Each Client Extension and tool might have recommended security exclusions to allow them to run without interference. For a list of all Client Extensions and tools, see Reference: Client extensions used for Tanium solutions.

Note: The change management feature of Endpoint Configuration might affect the version of each endpoint tool installed on endpoints.

Tanium™ Module Server

Benchmark is installed and runs as a service on the Module Server host computer. The impact on the Module Server is minimal and depends on usage.

For information about Module Server sizing in a Windows deployment, see Tanium Core Platform User Guide for Windows Deployments: Host system sizing guidelines.

Endpoints

©2026 Tanium Inc. All Rights Reserved

Supported Internet protocols

Benchmark supports IPv4 and IPv6 addresses.

Supported operating systems

For more information, see Tanium Client Management User Guide: Client version and host system requirements.

The following Tanium Client managed endpoint operating systems are supported with Benchmark.

- Windows
- macOS
- Linux

Host and network security requirements

Specific ports and processes are needed to run Benchmark.

Ports

The following ports are required for Benchmark communication.

If you have Tanium Certificate Manager installed, Benchmark uses a limited set of content from Certificate Manager to collect minimal certificate information from endpoints and perform audits. For more information, see Tanium Certificate Manager User Guide: Configuring Certificate Manager.

If you do not have Certificate Manager installed, you must enable the Benchmark scheduled actions to collect this data.

For more information, see (Optional) Enable Benchmark scheduled actions on page 40. Certificate Manager uses port scanning to locate certificates on endpoints. To configure exclusions on the ports that Certificate Manager uses to scan for certificates, see (Optional) Configure port exclusions for Certificate Manager on page 41.

©2026 Tanium Inc. All Rights Reserved

Best Practice: Configure firewall policies to open ports for Tanium traffic with TCP-based rules instead of application identity-based rules. For example, on a Palo Alto Networks firewall, configure the rules with service objects or service groups instead of application objects or application groups.

PORTS FOR BENCHMARK COMMUNICATION

Source	Destination	Port	Protocol	Purpose
Module Server	Module Server (loopback)	17523	TCP	Internal purposes, not externally accessible

Security exclusions

If antivirus (AV) or other security software is in use in the environment to monitor and block unknown host system processes, Tanium requires that a security administrator create exclusions to allow the Tanium processes to run without interference. This software can include security applications that are included with an endpoint operating system, such as fapolicyd on some Linux distributions, or Microsoft Defender on Windows. The configuration of these exclusions varies depending on the security software.

For more information about security exclusions to define across Tanium, see Reference: Endpoint security exclusions. For Windows-based Tanium Core Platform deployments, see Tanium Core Platform Server security exclusions.

Note: If the required exclusions are not configured, or if Tanium suspects interference from AV or security software, Tanium might require you to remove or disable the AV or security software temporarily for the purposes of troubleshooting and restore it once troubleshooting is complete.

BENCHMARK SERVER EXCLUSIONS

©2026 Tanium Inc. All Rights Reserved

Benchmark security exclusions for Tanium Core Platform servers (Windows deployments only)

Target Device	Notes	Exclusion Type	Process
Tanium Module Server		Process	*<Module Server>* \services\benchmark-service\ TaniumBenchmarkService.exe

BENCHMARK ENDPOINT EXCLUSIONS

Benchmark security exclusions for endpoints

Endpoint OS	Notes	Exclusion Type	Process
Windows		Process	*<Tanium Client>* \TaniumCX.exe
		File	*<Tanium Client>* \extensions\TaniumRisk.dll
		Folder	*<Tanium Client>* \Tools\CertificateManager
Linux		Process	*<Tanium Client>* /TaniumCX
		File	*<Tanium Client>* /libTaniumRisk.so
		Folder	*<Tanium Client>* /Tools/CertificateManager
macOS		Process	*<Tanium Client>* /TaniumCX
		File	*<Tanium Client>* /libTaniumRisk.dylib
		Folder	*<Tanium Client>* /Tools/CertificateManager

User role requirements

Predefined roles grant the following permissions, which are required to use Benchmark functionality:

©2026 Tanium Inc. All Rights Reserved

- solution permissions on page 24
- administration and platform content permissions on page 25

To review a summary of the predefined roles, see Set up Benchmark users on page 39.

Permissions for Tanium Guardian are required to enable optional Benchmark functionality. For more information, see Optional Benchmark role for Guide observations on page 26.

Some Benchmark solution permissions provide permissions that are associated with other solutions. Furthermore, all the platform content permissions and some solution permissions apply to content sets that might contain content for other solutions in addition to Benchmark. If you create custom roles for Benchmark users, be sure to assign all the solution permissions and content set permissions that are required for Benchmark functionality. If you are not sure which permissions are required for a custom role, view the permissions of the predefined roles. For more information, see the following sections of the Tanium Console User Guide:

- RBAC overview (provides an overview of roles, permissions, and content sets)
- Provided role permissions
- View effective role permissions
- Configure a custom role

Important: On installation, Benchmark creates a Benchmark user to automatically manage the Benchmark service account. Do not edit or delete the Benchmark user.

Benchmark solution permissions

Permission	Benchmark Administrator [1]	Benchmark Operator [1]	Benchmark User [1]	Benchmark Endpoint Configuration Approver [1]
Benchmark SHOW: View the Benchmark workbench OPERATOR: Provides privileges for the Benchmark Operator role	✓ SHOW	✓ OPERATOR SHOW	✓ SHOW	✗

©2026 Tanium Inc. All Rights Reserved

Permission	Benchmark Administrator [1]	Benchmark Operator [1]	Benchmark User [1]	Benchmark Endpoint Configuration Approver [1]
Benchmark Administrator Provides privileges for the Benchmark Administrator role	✓ ADMINISTER	✗	✗	✗
Benchmark Endpoint Configuration Allows users to approve Endpoint Configuration items for Benchmark	✓ APPROVE	✗	✗	✓ APPROVE
Benchmark Settings Allows reading and updating Benchmark settings	✓ READ WRITE	✓ READ	✗	✗
Benchmark Support Bundle Provides privileges for the Benchmark support bundle	✓ READ	✗	✗	✗

The permissions for these roles provide solution permissions for other solutions. To view the provided permissions, see View effective role permissions .

Benchmark administration and platform content permissions

Permission	Permission Type	Benchmark Administrator	Benchmark Operator	Benchmark User	Benchmark Endpoint Configuration Approver
Action Group	Administration	✓ READ	✓ READ	✓ READ	✗
Computer Group	Administration	✓ READ	✓ READ	✓ READ	✗
Filter Group	Platform Content	✓ READ	✓ READ	✓ READ	✗

©2026 Tanium Inc. All Rights Reserved

Permission	Permission Type	Benchmark Administrator	Benchmark Operator	Benchmark User	Benchmark Endpoint Configuration Approver
Plugin	Platform Content	✓ READ EXECUTE	✓ READ EXECUTE	✓ READ EXECUTE	
Sensor	Platform Content	✓ READ	✓ READ	✓ READ	✓ READ

[1] To view the content sets to which the platform content permissions apply, see View effective role permissions .

Optional Benchmark role for Guide observations

Optional roles for Benchmark

Role	Enables
A custom role that includes the **Benchmark show** and **Token - Use** permissions	Access to Guide observations for Benchmark . Access to Benchmark observations. For more information, see Tanium Console User Guide: Configure a custom role .

Solutions and permissions for Tanium Risk Assessment

To configure and generate the Tanium Risk Assessment (TRA), ensure that you have the necessary role and permissions:

- **Benchmark Administrator** role is required to enable the Tanium Risk Assessment data collection on the **Tanium Risk Assessment** page.
- **Benchmark Administrator** or **Benchmark Operator** role is required to configure and generate the TRA.
- **Sensor read** permission on the **Comply** content set is required to generate the TRA.

To generate the complete Tanium Risk Assessment detailed report, your environment must have certain solutions installed and you must have additional permissions. If you do not have all the

©2026 Tanium Inc. All Rights Reserved

required solutions and permissions for the detailed report, Benchmark does not display those sections in the assessment. For more information, see Generating the Tanium Risk Assessment on page 76.

Required solutions and permissions for complete Tanium Risk Assessment detailed report

Assessment section	Assessment sub-section	Required solution	Additional required permissions
Asset Inventory Covered by the Assessment	Introduction	• Tanium™ Discover • Core Content	**Discover API execute** permission
	Endpoint Criticality	Criticality	
	Endpoints Missing A/V Processes	• Impact • Core Content	
Risk Metrics Analysis	System Vulnerabilities	• Comply • Core Content	
	Lateral Movement Risk	• Impact • Core Content	• **Impact Asset Details read** permission • **Impact Asset Impact read** permission
	System Compliance	• Comply • Core Content	
	Insecure Transport Security Protocols	• Certificate Manager • Core Content	
	Encryption and Mutual Authentication	• Certificate Manager • Core Content	
Security and Operations Metrics	Customer Industry		
	Security Metrics	• Tanium™ Threat	

©2026 Tanium Inc. All Rights Reserved

Assessment section	Assessment sub-section	Required solution	Additional required permissions
		Response • Tanium™ Enforce • Impact • Reveal • Core Content	
	Operations Metrics	• Patch • Tanium™ Deploy • Core Content	
Guardian Metrics Risk Exposure Analysis		Emerging Issues Content	
Additional Risk and Cyber Hygiene Metrics	Endpoint Inventory Management	• Discover • Core Content	**Discover API execute** permission
	Endpoint Health Management	Core Content	
	Vulnerability Management	• Comply • Core Content	
	Patch Management	• Patch • Core Content	**Sensor read** permission on the **Patch Service Objects** content set
	Software Management and Distribution	• Deploy • Tanium™ Asset • Core Content	• **Sensor read** permission on the **Asset** content set • **Sensor read** permission on the **Deploy** content set
	Risk Management	• Comply • Core Content	

©2026 Tanium Inc. All Rights Reserved

Installing Benchmark

About this task

Use the Tanium Console **Solutions** page to install Benchmark and choose either automatic or manual configuration:

- Automatic configuration with default settings : Benchmark is installed along with all other licensed solutions. After installation, the Tanium Server automatically configures the recommended default settings. This option is the best practice for most deployments. For more information, see Import Benchmark with default settings on page 30.
- Manual configuration with custom settings: After installing Benchmark, you must manually configure required settings. Select this option only if Benchmark requires settings that differ from the recommended default settings. For more information, see Import Benchmark with custom settings on page 30.

Before you begin

- Read the release notes.
- Review the Benchmark requirements on page 18.
- If you are upgrading from a previous version, see Upgrade Benchmark on page 31.
- Assign the correct roles to users for Benchmark. Review the User role requirements on page 23.
    - To import the Benchmark solution, you must be assigned the Administrator reserved role.
    - To configure the Benchmark action group, you must be assigned the Administrator reserved role, Content Administrator reserved role, or a role that has the **Action Group write** permission.
- Install or upgrade the required dependencies to the specific version in the specified order. For more information, see Core platform dependencies on page 18.

©2026 Tanium Inc. All Rights Reserved

Import Benchmark with default settings

About this task

You can set the Benchmark action group to target the **No Computers** filter group by enabling restricted targeting before importing Benchmark. This option enables you to control tools deployment through scheduled actions that are created during the import and that target the tools action group. For example, you might want to test tools on a subset of endpoints before deploying the tools to all endpoints. In this case, you can manually deploy the tools to an action group that you configured to target only the subset. To configure an action group, see Targeting actions through action groups. To enable or disable restricted targeting, see Tools deployment and restricted targeting.

To import Benchmark and configure default settings, see Tanium Console User Guide: Import all modules and services. After the import, verify that the correct version is installed: see Verify Benchmark version on page 31.

Default settings for Benchmark

When you import Benchmark with automatic configuration, the following default setting is configured:

Tanium Benchmark default setting

Setting	Default value
Action group	• Restricted targeting disabled (default): `All Computers` computer group • Restricted targeting enabled: `No Computers` computer group

Import Benchmark with custom settings

About this task

To import Benchmark without automatically configuring default settings, be sure to clear the **Apply All Tanium recommended configurations** option while performing the steps in Tanium Console User Guide: Import or update specific solutions. After the import, verify that the correct version is installed: see Verify Benchmark version on page 31.

To configure the Benchmark action group, see Configure the Benchmark action group on page 34.

©2026 Tanium Inc. All Rights Reserved

Manage solution dependencies

Other Tanium solutions are required for Benchmark to function (required dependencies) or for specific Benchmark features to work (feature-specific dependencies).

Upgrade Benchmark

For the steps to upgrade Benchmark, see Tanium Console User Guide: Managing Tanium. After the upgrade, verify that the correct version is installed: see Verify Benchmark version on page 31.

Benchmark uses Tanium Criticality to manage criticality levels for Tanium Client managed endpoints. If you previously uploaded a CSV file to assign endpoint criticality in the **Settings** > **Endpoint Criticality** tab in an older version of Benchmark, the endpoint criticality data has been migrated to Tanium Criticality. For more information, see Tanium Criticality User Guide: Assigning criticality to endpoints.

Verify Benchmark version

After you import or upgrade Benchmark , verify that the correct version is installed.

1. Refresh your browser.
2. From the Main menu, go to **Modules** > **Benchmark** to open the **Overview** page.
3. To show version information, click Info .

©2026 Tanium Inc. All Rights Reserved

Configuring Benchmark

About this task

Configure Tanium Benchmark to ensure your Benchmark metrics are as effective and relevant as possible. Configurations include setting action groups, assigning target goals, and generating a Tanium Risk Assessment.

If you did not install Benchmark with the **Apply All Tanium recommended configurations** option, you must enable and configure certain features.

Restricted targeting

About this task

You can set the Benchmark action group to target the **No Computers** filter group by enabling restricted targeting before importing Benchmark. This option enables you to control tools deployment through scheduled actions that are created during the import and that target the tools action group. For example, you might want to test tools on a subset of endpoints before deploying the tools to all endpoints. In this case, you can manually deploy the tools to an action group that you configured to target only the subset. To configure an action group, see Targeting actions through action groups. To enable or disable restricted targeting, see Tools deployment and restricted targeting.

Tanium Endpoint Configuration

About this task

Manage solution configurations with Tanium Endpoint Configuration

Tanium Endpoint Configuration delivers configuration information and required tools for Tanium Solutions to endpoints. Endpoint Configuration consolidates the configuration actions that traditionally accompany additional Tanium functionality and eliminates the potential for timing errors that occur between when a solution configuration is made and the time that configuration reaches an endpoint. Managing configuration in this way greatly reduces the time to install,

©2026 Tanium Inc. All Rights Reserved

configure, and use Tanium functionality, and improves the flexibility to target specific configurations to groups of endpoints.

Endpoint tools are bundled together in a versioned toolset. Each toolset contains a specific version of each tool. The Endpoint Configuration Toolset Solution provides upgrades to the toolset, and it imports upgraded versions of the entire toolset as needed by upgraded or newly installed solutions.

Important:

When you upgrade Benchmark, the change management feature enables you to perform a staged rollout of the endpoint tools associated with the new version of Benchmark. Benchmark remains compatible with earlier versions of the endpoint tools and so continues to function with endpoints in rings that have not yet received the latest tools. However, any functionality added in the upgrade of Benchmark might not be available on these endpoints until they receive the upgraded tools.

In some cases, multiple solutions install the same endpoint tool, but upgraded endpoint tools remain compatible with all associated solutions. For example, both Tanium™ Threat Response and Tanium™ Reveal install and use index-cx. When you upgrade Threat Response, it might install version x.6.yyyy of index-cx, superseding version x.5.zzzz that Reveal previously installed. The index-cx upgrade from Threat Response does not affect the Index-related functionality of Reveal on the upgraded endpoints. For more information about the change management feature, see Tanium Endpoint Configuration User Guide: Managing endpoint tool upgrade rollouts.

Note: For information about how to install Endpoint Configuration, see Installing Endpoint Configuration.

Optionally, you can use Endpoint Configuration to require approval of configuration changes. When configuration approvals are enabled, Endpoint Configuration does not deploy a configuration change to endpoints until a user with approval permission approves the change. For information about the roles and permissions that are required to approve configuration changes for Benchmark, see User role requirements. For more information about how to enable and use configuration approvals in Endpoint Configuration, see Managing approvals.

©2026 Tanium Inc. All Rights Reserved

Important: For solutions to perform configuration changes or tool deployment through Endpoint Configuration on endpoints with action locks turned on, you must enable the **Manifest Package Ignore Action Lock** and **Deploy Client Configuration and Support Package Ignore Action Lock** settings. To access these settings, from the Endpoint Configuration **Overview** page, click Settings and select **Global**. For more information about action locks, see Managing action locks.

For more information about Endpoint Configuration, see Tanium Endpoint Configuration User Guide.

Configure Benchmark

Configure the Benchmark action group

About this task

Edit the computer groups in the Benchmark action group to specify which managed endpoints are included in Benchmark metrics.

Importing the Benchmark module automatically creates an action group to target specific Tanium Client managed endpoints. If you did not use automatic configuration or you enabled restricted targeting when you imported Benchmark, the action group targets **No Computers**.

If you used automatic configuration and restricted targeting was disabled when you imported Benchmark, configuring the Benchmark action group is optional.

Select the computer groups to include in the Benchmark action group.

Best Practice: Clear the selection for **No Computers** and make sure that all operating systems that are supported by Benchmark are included in the Benchmark action group.

1. From the Main menu, go to **Administration** > **Actions** > **Action Groups**.
2. Click **Tanium Benchmark**.
3. Select the computer groups that you want to include in the action group and click **Save**. If you select multiple computer groups, choose an operator (AND or OR) to combine the groups.

©2026 Tanium Inc. All Rights Reserved

(Optional) Set company name

About this task

You can change the company name that is displayed on charts in the Benchmark user interface.

1. From the Main menu, go to **Modules** > **Benchmark > Overview**. Click Settings and then click **General Settings**.
2. Enter the display name that you want to use and click **Save**.

(Optional) Set industry

About this task

You can change the default industry to compare your environment to customers in a different industry. When you change the industry, the charts on the **Benchmark Overview** page are updated to reflect the new industry.

1. From the Main menu, go to **Modules** > **Benchmark > Overview**. Click Settings and then click **General Settings**.
2. Clear the **Use Tanium Default** option, select the industry that you want to use, and then click **Save**.

Result

The **Industry History** table lists each time the industry was changed, including the industry, who set it, whether it was the default, and the date and time it was changed.

(Optional) Configure computer groups

About this task

By default, Benchmark uses the `All Computers` computer group. If needed, you can change this default computer group. You can also configure the computer groups that are available to select when you analyze benchmarks and risk scores. On all Benchmark pages, you can select a **Computer Groups**.

The computer groups you use for Benchmark must have Tanium Reporting enabled. For more information, see Tanium Reporting User Guide: Select computer groups for data collection.

©2026 Tanium Inc. All Rights Reserved

1. From the Main menu, go to **Modules** > **Benchmark > Overview**. Click Settings and then click **Computer Groups**.
2. If you want to change the default computer group to use as the default for all pages, select that computer group in the **Default** column.
3. If you want to add computer groups, click **Select Computer Groups** and select additional computer groups. Click **Save**.
4. If you want to remove computer groups from the list, click Remove .

(Optional) Configure data collection frequency

About this task

Benchmark collects data from Tanium Client managed endpoints every two hours by default. If needed, you can modify this frequency.

> **Note:** If you make changes to endpoint criticality rules, be aware that Tanium Criticality uses a different update frequency than Benchmark. Criticality updates each hour, whereas Benchmark can update from every 15 minutes or once a day, depending on your configuration. If it is 10:00, for example, and you modify the Benchmark data collection time period to be 15 minutes, Benchmark does not receive updated criticality levels until 11:00, even though Benchmark collects data at 10:15, 10:30, and 10:45.

1. From the Main menu, go to **Modules** > **Benchmark > Overview**. Click Settings and then click **Data Collection**.
2. Specify a time period and select **Minutes** or **Hours**.

Set benchmark target goals

About this task

You can add goal values in addition to the benchmark metric values. These goals are tracked on the detail page charts for each benchmark metric. You must have the Benchmark **Settings write** permission to set goal values.

©2026 Tanium Inc. All Rights Reserved

Note: Guardian Metrics goals are defined by Tanium and cannot be set.

1. From the Main menu, go to **Modules** > **Benchmark > Overview**. Click Settings and then click **Target Goals**.
2. For each metric you want to track, select a goal. The goal can be linked dynamically to the 50th or 75th percentile value, or a specific value. To set goals for all metrics, click **Set Method for All**.
3. Save your changes. Goals can take up to 24 hours to collect data and display on the Results chart for the metric. To start data collection, click **Collect Data**.

(Optional) Assign endpoint criticality

About this task

Endpoint criticality is a level on an individual endpoint that is used to add context about the endpoint in the organization. A higher criticality for a particular endpoint increases its risk score.

Benchmark uses Tanium Criticality to manage criticality levels for endpoints. Benchmark receives the levels from Criticality and factors the criticality into the risk scores for endpoints. For more information, see Tanium Criticality User Guide: Criticality overview.

(Optional) Enable data collection for Tanium Risk Assessment

About this task

Best Practice: For best results, ensure that Tanium Criticality 1.6 or later is installed.

A Tanium Risk Assessment (TRA) is a report of operational and security risks in your organization based on metrics and data points identified during the evaluation. You can generate the assessment as often as needed. For more information, see Tanium Risk Assessment on page 10 and Generating the Tanium Risk Assessment on page 76.

©2026 Tanium Inc. All Rights Reserved

Important: You must have certain roles and permissions to enable data collection and to configure and generate the assessment. For more information, see Solutions and permissions for Tanium Risk Assessment on page 26.

1. From the Main menu, go to **Modules** > **Benchmark** to open the **Overview** page.
2. Click Settings and then click **Risk Assessment**.
3. As a Benchmark Administrator, select **Enable the Tanium Risk Assessment data collection**. This option must be enabled before a Benchmark Administrator or Benchmark Operator can configure and generate the assessment.

   Note: You do not need to enable TRA data collection to use the **Risk Dashboards**.

   Enabling the TRA data collection allows Benchmark to create custom endpoint rules in Tanium Criticality and start automatic Tanium Data Service collection for existing Tanium sensors. The TRA rules dynamically modify endpoint criticality, based on specialized criteria, such as disk encryption status, uptime, insecure wireless configuration, whether or not the endpoint is a database server, and so on. Consider waiting to generate the assessment for at least one hour after you enable data collection, so that the new endpoint criticality rules can be synchronized. For more information, see Tanium Criticality Endpoint Rules on page 38 and Tanium Criticality User Guide: Configuring Criticality.

   If you disable data collection, the corresponding TRA rules are also deleted in Tanium Criticality and Tanium Data Service stops collecting data for Tanium sensors used in TRA rules.

TANIUM CRITICALITY ENDPOINT RULES

Benchmark creates the following endpoint rules in Tanium Criticality:

- TRA - Database Servers
- TRA - EoL Operating Systems
- TRA - High Uptime
- TRA - Insecure Services Running
- TRA - Insecure Wireless Access

©2026 Tanium Inc. All Rights Reserved

- TRA - System Requires Reboot
- TRA - Unencrypted Physical Disks

Set up Benchmark users

You can use the following set of predefined user roles to set up Benchmark users.

For more information, see User role requirements on page 23.

For more information about assigning user roles, see Tanium Core Platform User Guide: Manage role assignments for a user.

> **Note:** Do not assign the **Benchmark Service Account** and **Benchmark Service Account - All Content Sets** roles to users. These roles are for internal purposes only.

Benchmark Administrator

Assign the **Benchmark Administrator** role to users who manage the configuration and deployment of Benchmark functionality to endpoints. This role can perform the following tasks:

- Configure Benchmark service settings
- View and modify Benchmark endpoint criticality configurations
- Enable Tanium Risk Assessment data collection
- Configure and generate a Tanium Risk Assessment

Benchmark Operator

Assign the **Benchmark Operator** role to users who manage the configuration and deployment of Benchmark functionality to endpoints. This role can perform the following tasks:

- Configure Benchmark service settings
- View and modify Benchmark endpoint criticality configurations
- Configure and generate a Tanium Risk Assessment, after data collection is enabled by an administrator

©2026 Tanium Inc. All Rights Reserved

Benchmark User

Assign the **Benchmark User** role to users who need visibility into Benchmark data. This role can view Benchmark.

Benchmark Endpoint Configuration Approver

Assign the **Benchmark Endpoint Configuration Approver** role to a user who approves or rejects Benchmark configuration items in Tanium Endpoint Configuration. This role approves, rejects, or dismisses changes that target endpoints where Benchmark is installed.

Registered sensors

About this task

Benchmark registers sensors from core content and solutions that are in the environment. Tanium Data Service uses the registered sensors to collect metrics, perform risk scoring, and report health status.

For more information, see Tanium Interact User Guide: Managing Tanium Data Service.

(Optional) Enable Benchmark scheduled actions

About this task

If you have Tanium Certificate Manager installed, Benchmark uses a limited set of content from Certificate Manager to collect minimal certificate information from endpoints and perform audits. For more information, see Tanium Certificate Manager User Guide: Configuring Certificate Manager.

If you do not have Certificate Manager installed, you must enable the Benchmark scheduled actions to collect this data.

You can enable the following scheduled actions to collect data for expired certificates and insecure TLS/SSL metrics:

- Benchmark - Run Certificate Audit [Non-Windows]
- Benchmark - Run Certificate Audit [Windows]

To enable these scheduled actions:

©2026 Tanium Inc. All Rights Reserved

1. From the Main menu, go to **Administration** > **Scheduled Actions**.
2. Select the **Tanium Benchmark** action group or enter Benchmark to filter the list of scheduled actions.
3. Select the **Benchmark - Run Certificate Audit [Non-Windows]** and **Benchmark - Run Certificate Audit [Windows]** scheduled actions and then click **More** > **Enable Actions**.

Result

If Certificate Manager is later installed, these Benchmark scheduled actions are automatically disabled within an hour. Benchmark then defaults to using the **Certificate Manager - Run Certificate Audit [Non-Windows]** and **Certificate Manager - Run Certificate Audit [Windows]** actions instead.

(Optional) Configure port exclusions for Certificate Manager

About this task

Certificate Manager uses port scanning to locate certificates on endpoints. The instructions to configure port exclusions depends on if Certificate Manager is installed in your environment.

CONFIGURE PORT EXCLUSIONS IF CERTIFICATE MANAGER IS INSTALLED

About this task

If Certificate Manager is installed in your environment, you configure port exclusions in a profile. For more information, see Tanium Certificate Manager User Guide: Deploying certificate audits.

CONFIGURE PORT EXCLUSIONS IF CERTIFICATE MANAGER IS NOT INSTALLED

About this task

You can add or delete port exclusions by deploying the following packages:

- **Certificate Audit Add Port Exclusions [Non-Windows]**
- **Certificate Audit Add Port Exclusions [Windows]**
- **Certificate Audit Delete Port Exclusions [Non-Windows]**

©2026 Tanium Inc. All Rights Reserved

- **Certificate Audit Delete Port Exclusions [Windows]**

ADD PORT EXCLUSIONS

About this task
You can add or delete port exclusions by deploying the following packages:

- **Certificate Audit Add Port Exclusions [Non-Windows]**
- **Certificate Audit Add Port Exclusions [Windows]**
- **Certificate Audit Delete Port Exclusions [Non-Windows]**
- **Certificate Audit Delete Port Exclusions [Windows]**

1. From the Main menu, go to **Administration** > **Content** > **Packages** and search for `Certificate Audit`.
2. Select the checkbox for **Certificate Audit Add Port Exclusions [Non-Windows]** or **Certificate Audit Add Port Exclusions [Windows]** and then click **Deploy Action**.
3. In the **Deployment Package** section, enter the **Ports to Exclude**.
4. In the **Targeting Criteria** section, choose an option to target one or more endpoints and then click **Show Preview to Continue**.

   Tip: To add the port exclusion for all endpoints, select **Tanium Certificate Manager** for **Action Group**. For more information, see Configure the Certificate Manager action group.
5. Verify the list of targeted endpoints and click **Deploy Action**.

DELETE PORT EXCLUSIONS

1. From the Main menu, go to **Administration** > **Content** > **Packages** and search for `Certificate Audit`.
2. Select the checkbox for **Certificate Audit Delete Port Exclusions [Non-Windows]** or **Certificate Audit Delete Port Exclusions [Windows]** and then click **Deploy Action**.
3. In the **Deployment Package** section, enter the **Ports to no longer exclude**.

©2026 Tanium Inc. All Rights Reserved

4. In the **Targeting Criteria** section, choose an option to target one or more endpoints and then click **Show Preview to Continue**.

   Tip: To delete the port exclusion for all endpoints, select **Tanium Certificate Manager** for **Action Group**. For more information, see Configure the Certificate Manager action group.

5. Verify the list of targeted endpoints and then click **Deploy Action**.

Result

Note: Although the **Certificate Audit Port Exclusions** sensor displays the updated exclusions, the port exclusions do not take effect until after the next certificate audit runs. You can either deploy a certificate audit package manually (Deploy a certificate audit package), or wait until the next **Certificate Audit [Non-Windows]** and **Certificate Audit [Windows]** scheduled actions run.

©2026 Tanium Inc. All Rights Reserved

Evaluating your risk score

About this task

Assess the overall risk posture of Tanium Client managed endpoints in your environment, prioritize actions, and remediate issues using the Tanium platform.

Important: You must have Tanium Comply installed and configured to view the risk score.

By default, data for the risk score is gathered from managed endpoints and stored every 2 hours throughout the day. The total score for the enterprise is calculated several times per day to update the charts on the Benchmark **Overview**

Note:

Tanium Guide observations and guidance display for users based on user permissions.

- Assign the **Token - Use** administration permission to enable receiving observations and guidance.
- Assign the **Benchmark show** permission to view Risk Score-related observations.

For more information, see Tanium Guide User Guide: Viewing and managing notifications.

Risk score calculation

The Tanium risk score gets calculated for endpoints that are in computer groups that you have configured for Benchmark. For more information, see (Optional) Configure computer groups on page 35. Benchmark uses Tanium Data Service to include results for offline endpoints. For more information, see Tanium Interact User Guide: Managing Tanium Data Service.

Risk score range

©2026 Tanium Inc. All Rights Reserved

The possible range for a risk score is 1-1000. A lower score indicates a lower risk for the enterprise or endpoint. Scores are categorized into low, medium, high, or critical:

- Low: 1-250
- Medium: 251-500
- High: 501-750
- Critical: 751-1000

Risk score formulas

The following formula is used to calculate the risk score per endpoint:

```
Metrics Risk Score Total x Endpoint Criticality Value = Final Risk Score
```

The following formula is used to calculate the risk score for a computer group:

```
Total Endpoint Risk Score Sum of Endpoints / Total # of Endpoints
```

Risk score metrics

These metrics assess the risk for your enterprise in specific categories by using data provided by Tanium solutions. These data points are used as part of the formula to calculate the risk score. The risk score contributing factor is the percentage that the metric contributes to the overall risk score. Each metric can contribute a maximum number of points towards the total risk score.

Risk score metric contributions

Metric	Risk score contributing factor	Risk score contribution point totals
High Severity Vulnerabilities	10%	50/500
Critical Severity Vulnerabilities	25%	125/500
Compliance Failures	20%	100/500
Insecure TLS/SSL	10%	50/500
Expired Certificates	10%	50/500

©2026 Tanium Inc. All Rights Reserved

Metric	Risk score contributing factor	Risk score contribution point totals
Lateral Movement Risk	25%	125/500

ENDPOINT CRITICALITY VALUE

Endpoint criticality is a level on an individual endpoint that is used to add context about the endpoint in the organization. Possible levels are **Critical**, **High**, **Medium**, and **Low**. These levels indicate the importance of the endpoint in your environment.

The score for an endpoint is adjusted based on the criticality level:

- **Low:** No adjustment to the score for the endpoint
- **Medium:** (Default) Multiplies the score for the endpoint by 1.33
- **High:** Multiplies the score for the endpoint by 1.67
- **Critical:** Multiplies the score for the endpoint by 2

For example, if an endpoint has a score of 200, but the endpoint is flagged as critical, the score reported for that endpoint is 400.

Benchmark uses Tanium Criticality to manage criticality levels for endpoints. For more information, see Tanium Criticality User Guide: Criticality overview.

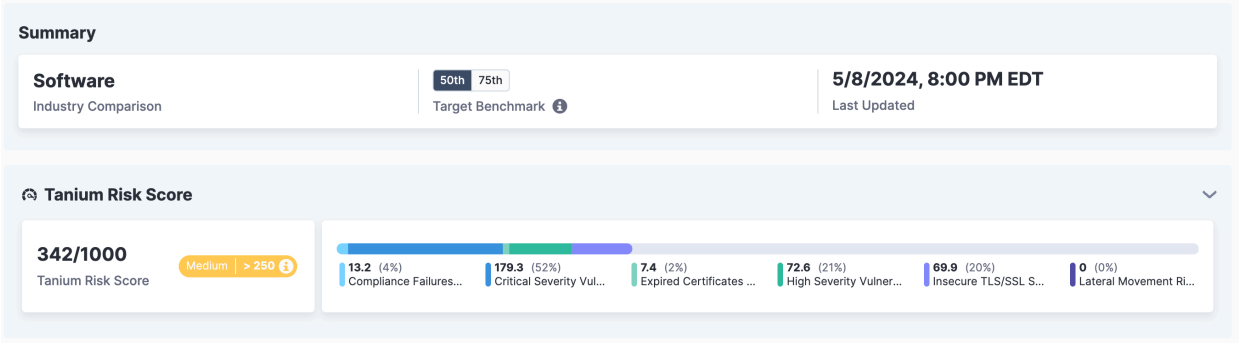
View risk score

About this task

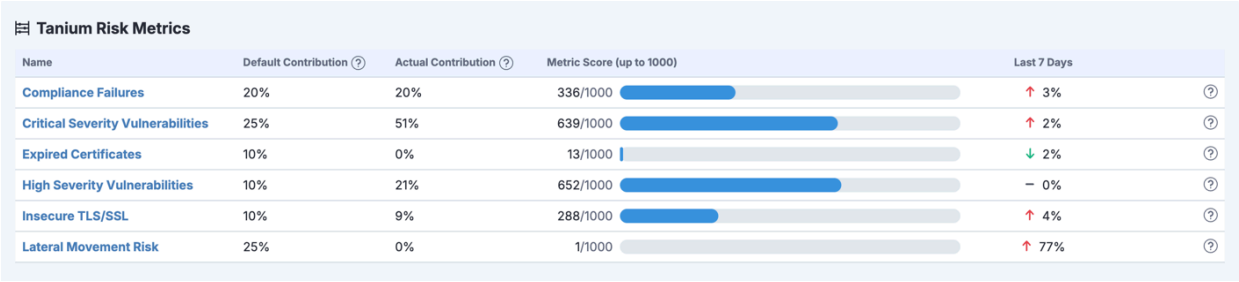
You can review the overall risk score. Drill into more details such as risk scores for each endpoint, and more data about each metric.

1. View the overall risk score. From the Main menu, go to **Modules** > **Benchmark > Risk Score 2.0** and view the **Tanium Risk Score** section. To scope the risk score, select a **Computer Group**.

©2026 Tanium Inc. All Rights Reserved

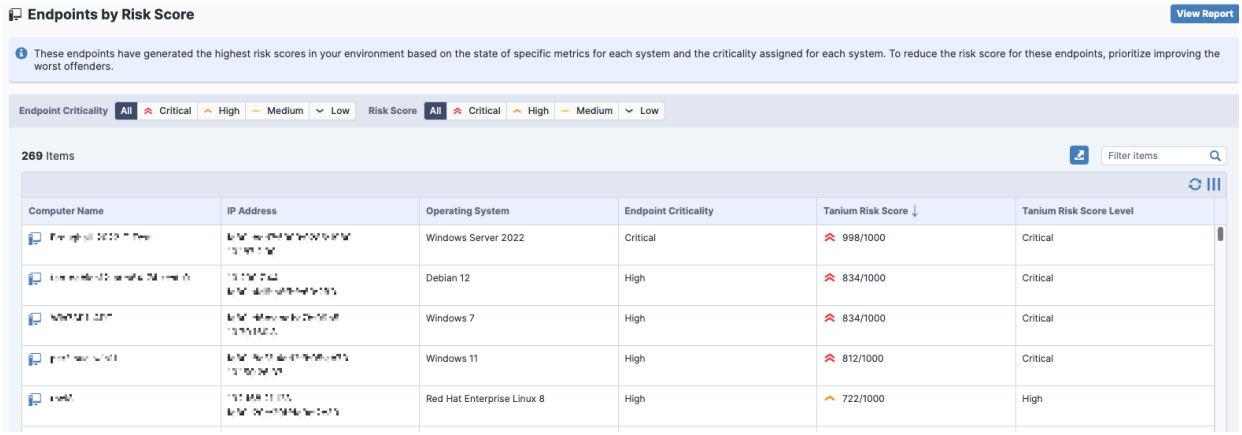


2. View the score for each risk metric that contributes to the overall risk score. Go to the **Tanium Risk Metrics** section.



Click the metric name to view further details about the metric, including detailed information about the riskiest managed endpoints for that metric. For more information, see Investigate benchmark results on page 50.

3. View endpoints by risk score. Go to **Endpoints by Risk Score** and review the endpoints with the highest risk scores.



For more information, click **View Report** or Endpoint Details , then **View Details**.

©2026 Tanium Inc. All Rights Reserved

Reviewing benchmark metrics

About this task

View benchmarks that are grouped into the following categories: enterprise risk, Guardian metrics, security, and operations.

Benchmark values

> **Important:** To see metrics and benchmark values, you must have licenses for the associated modules. For example, to view the **Mean Time to Patch** benchmark, you must have a license for Tanium Patch.

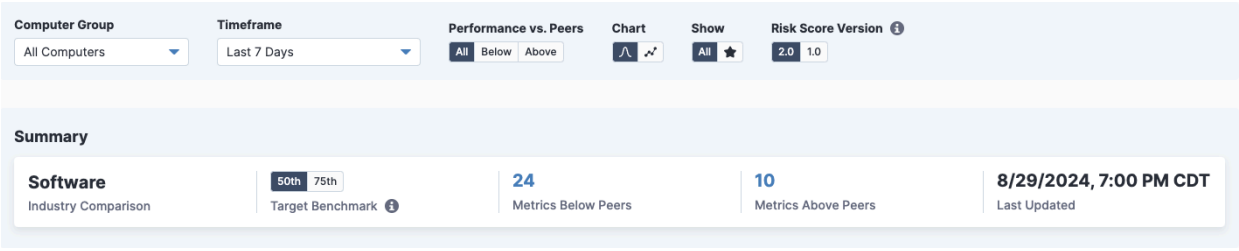
Benchmark values are anonymously collected and aggregated from Tanium Cloud customers. The benchmark data that you see compares the performance of your Tanium metrics with aggregated data that is collected anonymously from other Tanium customers in the same industry. This data is a static representation of the benchmarks at a point in time. The data gets updated when you upgrade Benchmark.

Each metric is presented as both a percentile value and the results, or actual values.

View benchmarks

About this task

- Scope your metrics. From the Main menu, go to **Modules** > **Benchmark > Overview**. Choose a computer group, timeframe, peer performance comparison, chart type, and risk score version.



©2026 Tanium Inc. All Rights Reserved

- Set your target percentile. The percentile indicates a percentage of other Tanium customers that meet or exceed the benchmark value for a metric. You can choose 50th or 75th percentile. From the **Benchmark Overview** page, go to the **Summary** section and select the **Target Benchmark**. The target benchmark is displayed on all of the charts on the Benchmark **Overview** page.

- Choose the type of charts that you want to view on the **Overview** page. Choose either the **Percentile Distribution** or **Percentile Over Time** chart type.

- View an overview of metrics by category. On the **Benchmark Overview** page, you can view an overview of all the metrics that are available compared to the target percentile value that you selected.



- View benchmark details.

©2026 Tanium Inc. All Rights Reserved



On the **Benchmark Overview** page, click **View Details** next to one of the categories. The percentile and results charts for each metric are displayed. You can hover over parts of the charts for more details. In the **Percentile** charts, you might want to investigate metrics with a **Below Benchmark** indicator. If a goal is set for the metric, a line is available for the in the **Results** chart for the metric, along with an indicator of whether the goal has been met.

For more information, see Set benchmark target goals on page 52.

- View the data that contributed to your metrics. To view a report with data details for the benchmark, click the title of the chart.

Investigate benchmark results

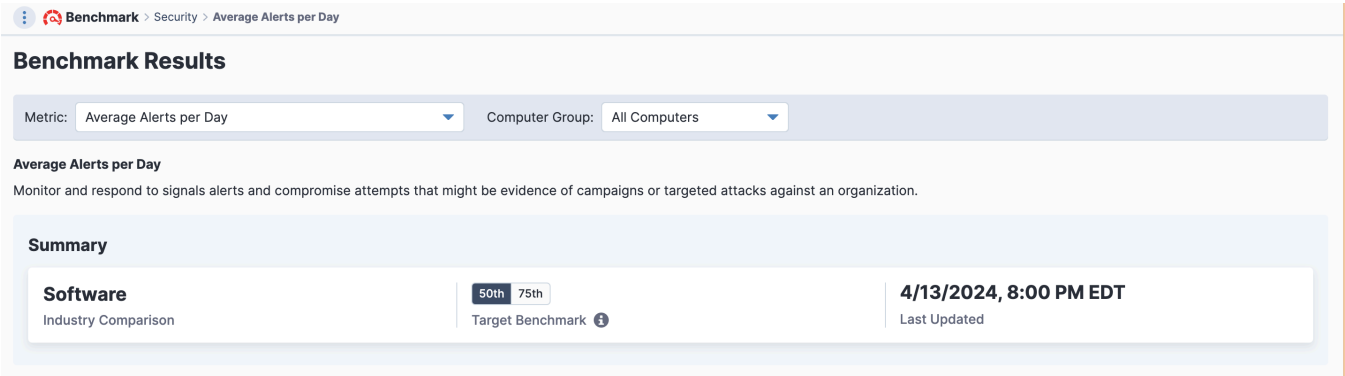
About this task

From the Main menu, go to **Modules** > **Benchmark**. Click the title of a metric chart to view details about the results for that metric. From the **Benchmark Results** page, you can switch between pages for other metrics by selecting a **Metric**. You can also select the **Computer Group** to use for the data. The **Benchmark Results** pages include these sections:

Summary

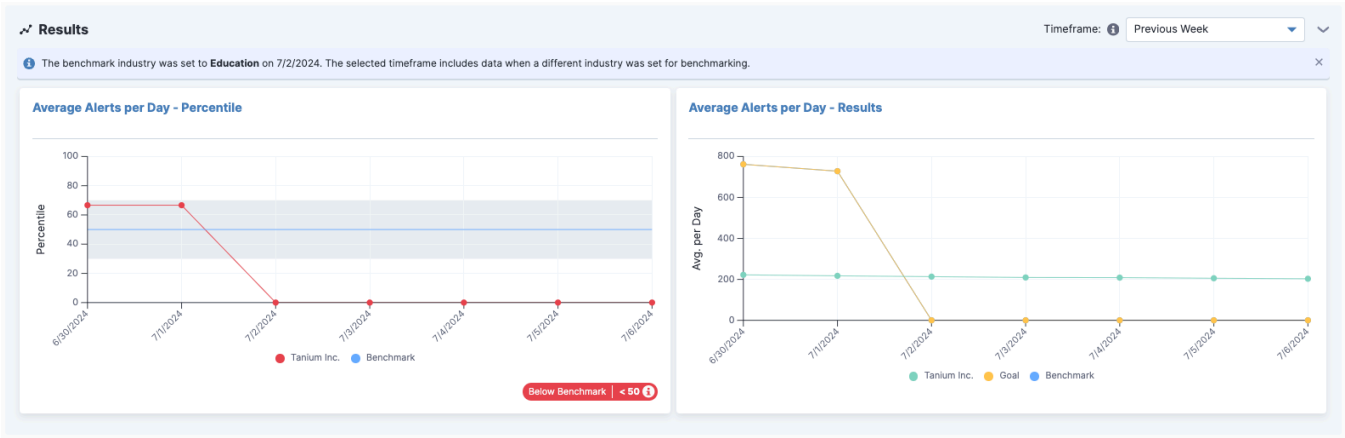
The **Summary** section provides details about the metric, shows the source for the benchmark, the target benchmark, and the date and time that the data was last updated. You can set your target percentile for the metric. The percentile indicates a percentage of other Tanium customers that meet or exceed the benchmark value for a metric. You can choose 50th or 75th percentile.

©2026 Tanium Inc. All Rights Reserved



Results

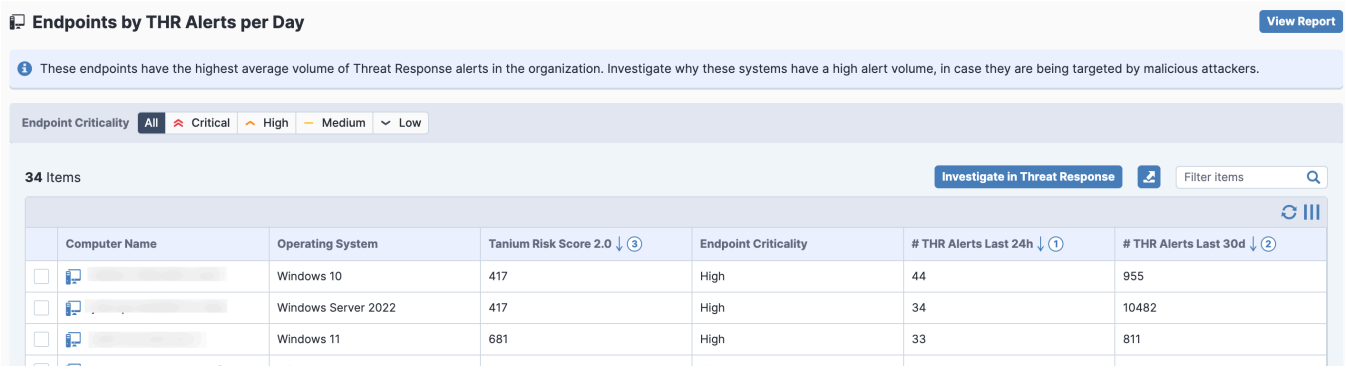
The **Results** section includes charts with the results for the metric, shown both as the percentile and percentage of Tanium Client managed endpoints. Select the **Timeframe** for the charts.



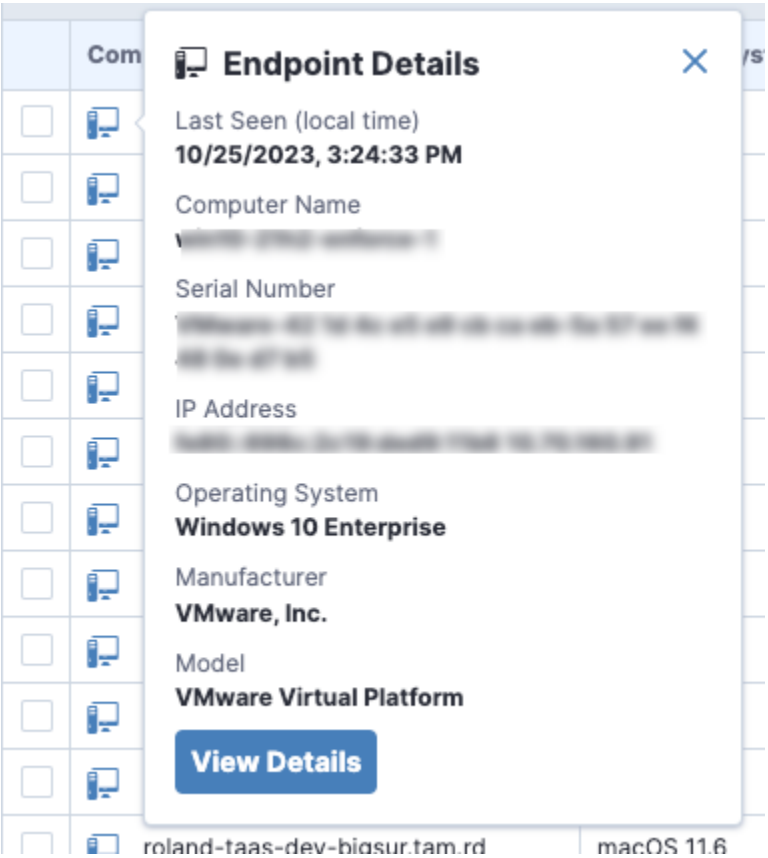
Endpoints

The endpoints table shows the riskiest endpoints for that metric. To open the metric report, click **View Report**. For more information, see Tanium Reporting User Guide: Working with reports. Some metrics include the option to explore, investigate or remediate an issue in other Tanium solutions, including: Comply, Deploy, Enforce, Impact, Patch, and Threat Response. To view details in the Tanium module, select an endpoint and click the button to open the module. For more information, see Security metrics on page 56 and Operations metrics on page 59.

©2026 Tanium Inc. All Rights Reserved



To see details about an endpoint, click Endpoint Details .



Set benchmark target goals

About this task

You can add goal values in addition to the benchmark metric values. These goals are tracked on the detail page charts for each benchmark metric. You must have the Benchmark **Settings write** permission to set goal values.

©2026 Tanium Inc. All Rights Reserved

Note: Guardian Metrics goals are defined by Tanium and cannot be set.

1. From the Main menu, go to **Modules** > **Benchmark > Overview**. Click Settings and then click **Target Goals**.
2. For each metric you want to track, select a goal. The goal can be linked dynamically to the 50th or 75th percentile value, or a specific value. To set goals for all metrics, click **Set Method for All**.
3. Save your changes. Goals can take up to 24 hours to collect data and display on the Results chart for the metric. To start data collection, click **Collect Data**.

About bell curve charts

If you select **Percentile Distribution** for the chart types on the **Benchmark Overview** page, you see a bell curve chart for each metric.

- If you select 50 for your percentile value, 50 is on the chart and represents the median for the dataset.
- The mean value is at the center of the curve, regardless of where the curve sits on the X axis.
- The percentile value for your environment is represented with a vertical line with the percentile value on the X axis.
- The relative position of the median and mean values skews the position of the bell curve on the chart. If the median and mean do not align, the chart is skewed to the right or left.
- The shape of the curve identifies the standard deviation for the dataset.
    - Normal distribution: Most individual values sit in the middle of the range.



    - Deviations: The deviation affects the width of the bell curve, with a thinner curve showing that the values span a smaller range of values.

©2026 Tanium Inc. All Rights Reserved



Enterprise Risk metrics

Tanium Risk Score 2.0

The percentage of risk metric contributions that reflect risk in specific focus areas of endpoint security. A high risk score indicates increased enterprise risk. For more information about this metric, see Evaluating your risk score on page 44.

From solution: Benchmark

Compliance Failures

The average number of compliance failures per endpoint. You can investigate the findings for each endpoint in Comply for more details.

From solution: Comply

Critical Severity Vulnerabilities

The percentage of endpoints in the environment with critical severity vulnerabilities over 7 days old.

From solution: Comply

Expired Certificates

The percentage of endpoints with expired Transport Layer Security (TLS) and Secure Socket Layer (SSL) certificates on endpoints. Expired certificates present security issues because organizations cannot validate certificate revocation status to confirm trust in those certificates. A high metric score indicates increased enterprise risk.

If you have Tanium Certificate Manager installed, Benchmark uses a limited set of content from Certificate Manager to collect minimal certificate information from endpoints and perform

©2026 Tanium Inc. All Rights Reserved

audits. For more information, see Tanium Certificate Manager User Guide: Configuring Certificate Manager.

If you do not have Certificate Manager installed, you must enable the Benchmark scheduled actions to collect this data.

For more information, see (Optional) Enable Benchmark scheduled actions on page 40.

From solution: Core Content

High Severity Vulnerabilities

The percentage of endpoints in the environment with Common Vulnerability Scoring System (CVSS) v3 high and critical vulnerabilities over 7 days old.

From solution: Comply

Insecure TLS/SSL

The percentage of endpoints with insecure and outdated transport layer security protocols (SSLv3, TLSv1). These protocols can expose enterprise endpoints to man-in-the-middle attacks and expose sensitive data to attackers through browser exploitation. A high metric score indicates increased enterprise risk.

If you have Tanium Certificate Manager installed, Benchmark uses a limited set of content from Certificate Manager to collect minimal certificate information from endpoints and perform audits. For more information, see Tanium Certificate Manager User Guide: Configuring Certificate Manager.

If you do not have Certificate Manager installed, you must enable the Benchmark scheduled actions to collect this data.

For more information, see (Optional) Enable Benchmark scheduled actions on page 40.

From solution: Core Content

Lateral Movement Risk

This metric evaluates the least-privilege model on endpoints, determining potential lateral movement if an endpoint is compromised. Limit administrative access to prevent attackers from gaining access to elevated privileges.

©2026 Tanium Inc. All Rights Reserved

From solution: Impact

Guardian metrics

Guardian metrics compare your threat exposure for known vulnerabilities against your peers. You can also view Guardian metrics on the **Guardian Metrics** page from the Benchmark menu.

SSH Authorized Keys without a Passphrase

The percentage of endpoints that have unprotected keys that might be authorized for use. Revoke authorization for each authorized key without a passphrase and issue a new passphrase protected key in its place.

From solution: Core Content, Emerging Issues Content

July 2025 SharePoint Server RCE Vulnerabilities

The percentage of Windows endpoints that have Microsoft SharePoint Server versions included in the July 2025 SharePoint RCE vulnerabilities (CVE-2025-49706, CVE-2025-49704, CVE-2025-53770, and CVE-2025-53771). Install the applicable patches and implement Microsoft recommended best practices to mitigate the identified issues. If possible, rotate SharePoint Server ASP.NET machine keys using SharePoint Central Administration as an additional mitigation.

From solution: Core Content, Emerging Issues Content

June 2025 Windows SMB Signing - Kerberos Reflection

The percentage of Windows endpoints that have SMB signing disabled on the server side of the SMB connection, indicating that the endpoints might be vulnerable to privilege elevation attacks. Update the endpoint configuration to require SMB security signing.

From solution: Core Content, Emerging Issues Content

Security metrics

Security metrics can help you understand how susceptible your environment is to attacks and malware, compared to other Tanium customers.

©2026 Tanium Inc. All Rights Reserved

Average Alerts per Day

The average number of alerts per day provided by Threat Response intel documents. You might have varying numbers and types of intel documents that affect the number of alerts.

To explore this metric in Impact, select an endpoint in the **Endpoints by THR Alerts per Day** section of the **Benchmark Results** page for this metric and click **Explore in Impact** to open the **Impact Details** page for that endpoint. To investigate unresolved alerts related to this metric in Threat Response, click **Investigate in Threat Response**. For more information, see Tanium Threat Response User Guide: Managing alerts.

From solution: Threat Response

Firewall Disabled

The percentage of endpoints in the environment that have a disabled firewall. For more information, see Tanium Enforce User Guide: Monitor and troubleshoot host firewall status on endpoints.

From solution: Enforce

Impact Rating of Machines with Alerts

The average impact rating for endpoints that currently have active Threat Response intelligence alerts.

From solution: Threat Response, Impact

LSA Protection Disabled (LSASS as PPL)

The percentage of endpoints that do not have Local Security Authority (LSA) Protection enabled.

From solution: Incident Response

Missing Disk Encryption (Windows systems)

The percentage of endpoints in the environment that are missing disk encryption. For more information, see Tanium Enforce User Guide: Monitor and troubleshoot disk encryption status on endpoints.

From solution: Enforce

©2026 Tanium Inc. All Rights Reserved

Passwords Found

The percentage of endpoints with confirmed passwords using the Reveal rule: `PCI 2 - System Passwords`. Ensure that passwords are not stored in plain-text to prevent attackers and insider threats from accessing those credentials and gaining unauthorized access to enterprise endpoints.

From solution: Reveal

Remote UAC Local Account Token Filter Disabled

The percentage of endpoints that do not have the LocalAccountTokenFilterPolicy restriction applied.

From solution: Incident Response

Secure Powershell Execution Policy Not Enforced

The percentage of endpoints that do not have PowerShell execution policies enabled.

From solution: Core Content

Secure Removable Storage Policy Not Applied

The percentage of endpoints that do not have a secure removable storage policy applied.

From solution: Enforce, Core Content

User Account Control Disabled

The percentage of endpoints that do not have user account control enabled.

From solution: Incident Response

Windows Credential Guard Disabled

The percentage of endpoints that do not have Windows Credential Guard enabled.

From solution: Core Content

Windows Data Execution Prevention (DEP) Disabled

The percentage of endpoints that have Windows Data Execution Prevention (DEP) disabled.

©2026 Tanium Inc. All Rights Reserved

From solution: Core Content

Windows Defender Disabled

The percentage of endpoints in the environment that are missing Windows Defender.

From solution: Enforce

Windows Defender Out of Date

The percentage of endpoints in the environment that have out of date Microsoft Defender definition files.

From solution: Enforce

Windows Trusted Platform Module (TPM) Not Enabled

The percentage of endpoints that do not have TPM enabled.

From solution: Benchmark

Windows Workstation Antivirus Disabled

The percentage of endpoints that do not have workstation antivirus enabled.

From solution: Core Content

Windows Workstation Antivirus Out of Date

The percentage of endpoints that have out of date antivirus.

From solution: Core Content

Operations metrics

Operations metrics contain controls that an organization can put in place to prevent attackers from accessing sensitive data or performing malware attacks.

Domain Membership

The percentage of endpoints that are not joined to a domain. (Windows only)

From solution: Core Content

©2026 Tanium Inc. All Rights Reserved

High CPU Consumption

The percentage of endpoints that have over 95% CPU consumption.

From solution: Core Content

High Disk Consumption

The percentage of endpoints that have less than five percent disk space available.

From solution: Core Content

High Memory Consumption

The percentage of endpoints that have less than five percent memory remaining.

From solution: Core Content

High Server Uptime

The percentage of server endpoints that have been up more than thirty days.

From solution: Core Content

High Workstation Uptime

The percentage of workstation endpoints that have been up more than ten days.

From solution: Core Content

Mean Time to Patch

The average number of days to patch endpoints following the availability of a patch.

From solution: Patch

Mean Time to Update

The average number of days to deploy software updates to endpoints following the availability of an update.

From solution: Deploy

©2026 Tanium Inc. All Rights Reserved

Patch Compliance

The percentage of endpoints that have not been updated with available software patches after 30 days since the patch became available. For more information, see Tanium Patch User Guide: Monitor and troubleshoot endpoints missing critical or important patches.

From solution: Patch

Software Update Compliance

The percentage of endpoints that have available software updates that have not been deployed after 30 days since the update became available.

From solution: Deploy

©2026 Tanium Inc. All Rights Reserved

Reviewing your risk dashboards

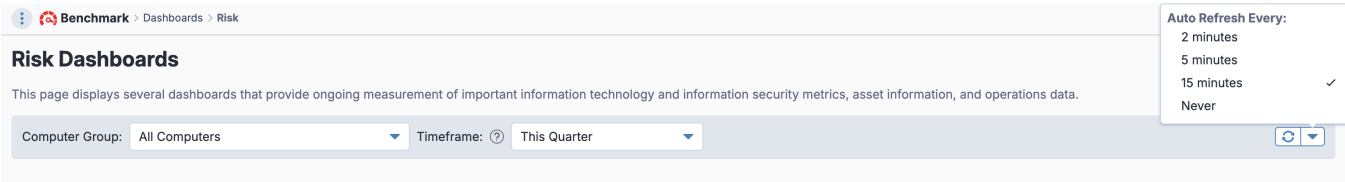
About this task

Review your risk posture in visual dashboards that are a collection of panels, charts and reports based on operational and security risks. Data for these dashboards are based on the solutions that are currently installed and implemented in your environment.

View the dashboards

About this task

From the Main menu, go to **Modules** > **Benchmark Dashboards** > **Risk**. Select the **Computer Group** and **Timeframe** for the dashboards. Click Refresh now to refresh the data in the charts. You can also adjust the auto refresh time frame. Click **Summarize** to generate a summary of your risk dashboards. For more information, see Tanium Reporting User Guide: Summarize dashboards.



Inventory

Use the data in the **Inventory** section to gain insight into the total number, operating systems, and hardware models of endpoints in your environment.

Note: The available charts and reports depend on the solutions currently installed and implemented in your environment. Therefore, the charts and reports for each section might vary between environments.

©2026 Tanium Inc. All Rights Reserved

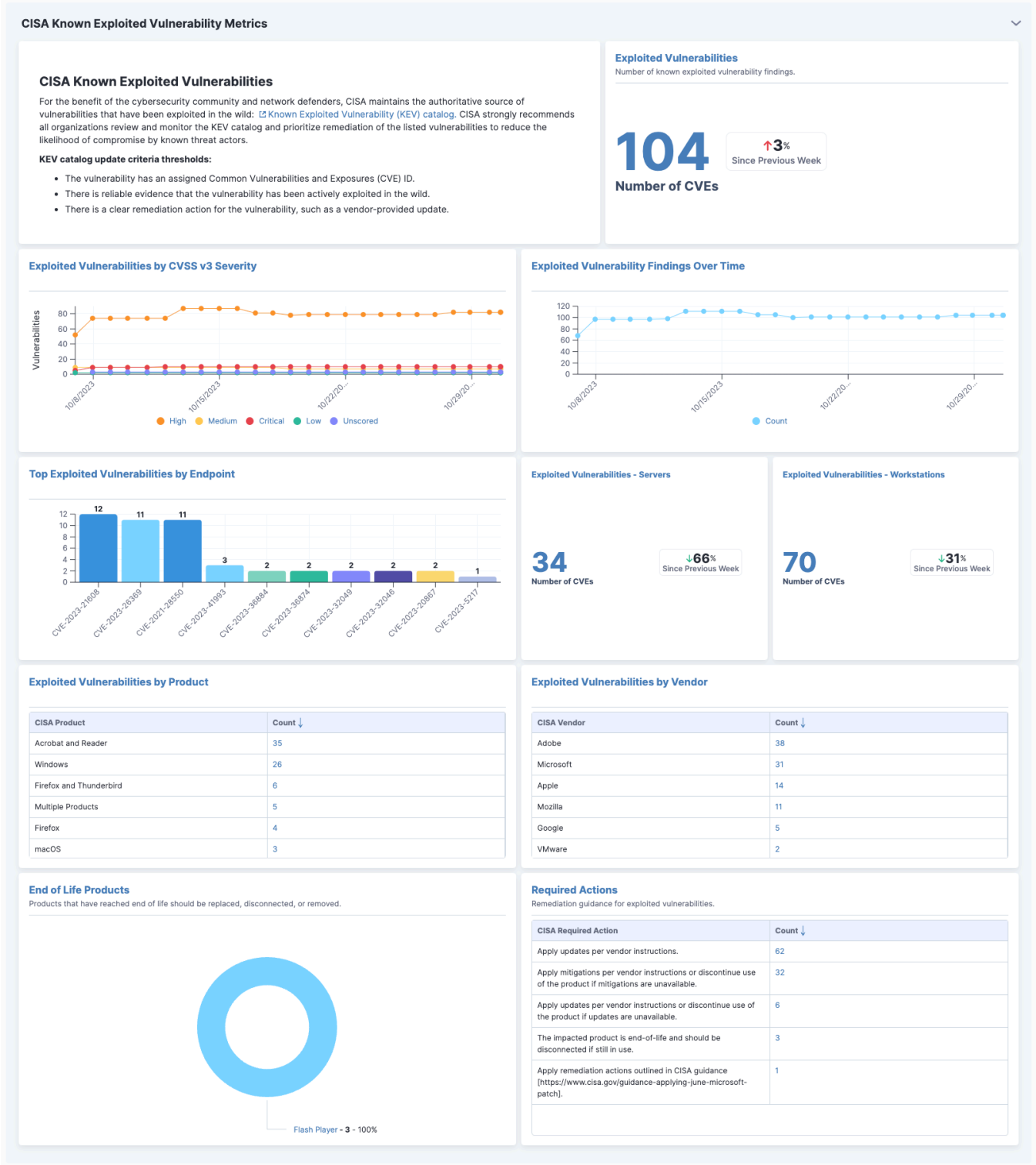


CISA Known Exploited Vulnerability Metrics

Use the data in the **CISA Known Exploited Vulnerability Metrics** section to assess your environment for CISA known exploited vulnerabilities and review remediation guidance.

©2026 Tanium Inc. All Rights Reserved

Note: The available charts and reports depend on the solutions currently installed and implemented in your environment. Therefore, the charts and reports for each section might vary between environments.



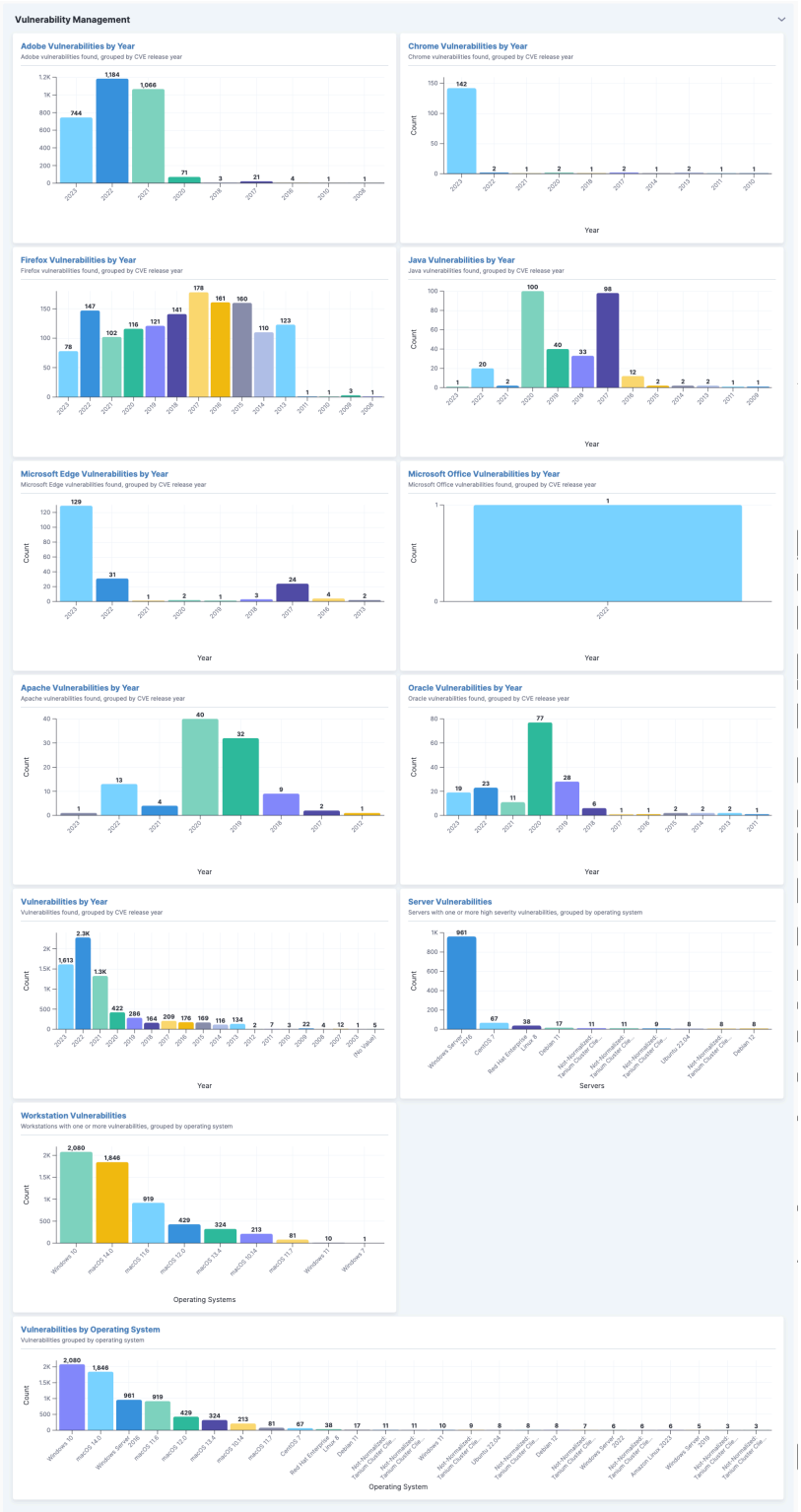
©2026 Tanium Inc. All Rights Reserved

Vulnerability Management

Use the data in the **Vulnerability Management** section to assess the known vulnerabilities in software installed in your environment.

> **Note:** The available charts and reports depend on the solutions currently installed and implemented in your environment. Therefore, the charts and reports for each section might vary between environments.

©2026 Tanium Inc. All Rights Reserved

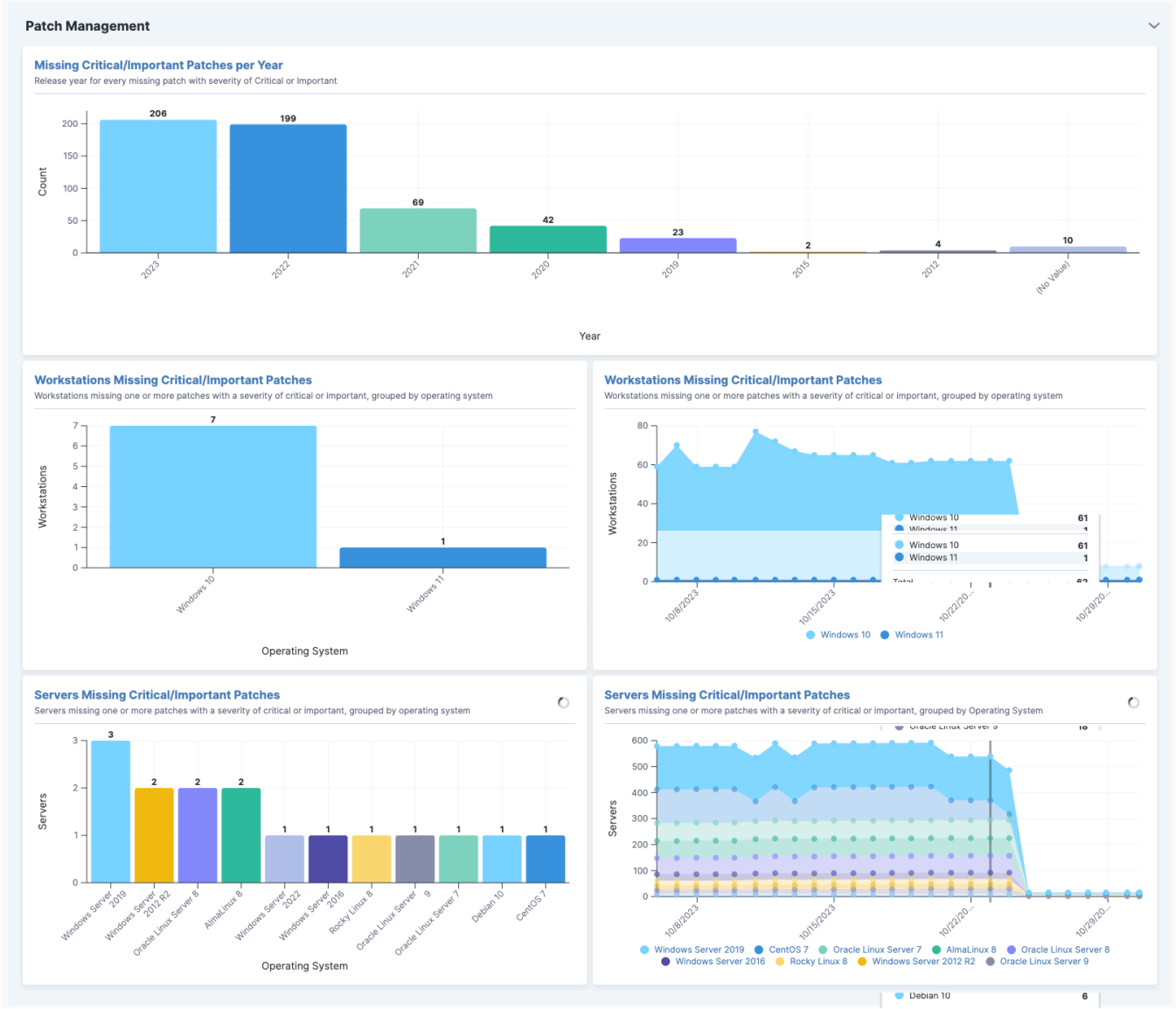


Patch Management

Use the data in the **Patch Management** section to assess the missing patches with a critical or important severity level in your environment.

©2026 Tanium Inc. All Rights Reserved

Note: The available charts and reports depend on the solutions currently installed and implemented in your environment. Therefore, the charts and reports for each section might vary between environments.

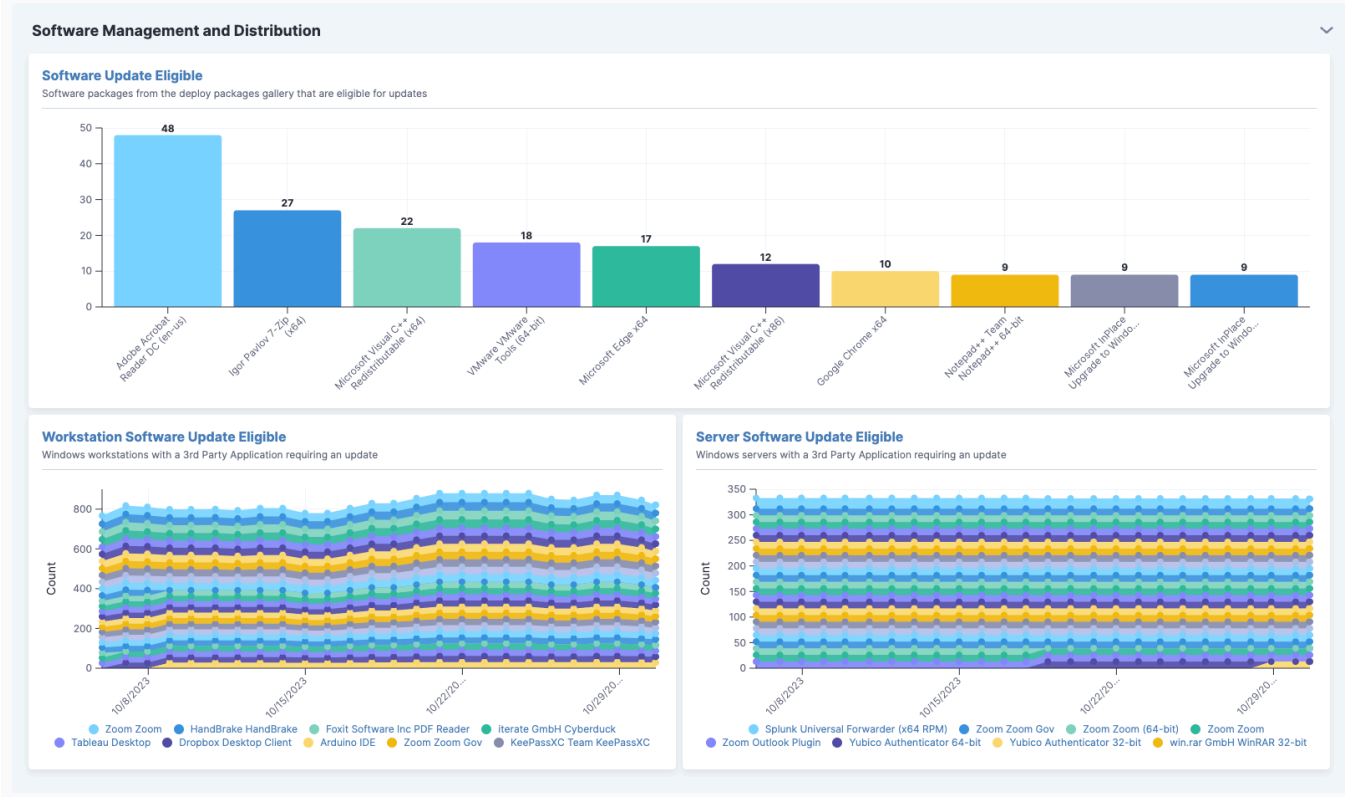


Software Management and Distribution

Use the data in the **Software Management and Distribution** section to assess the software and endpoint operating systems in your environment with available updates.

©2026 Tanium Inc. All Rights Reserved

Note: The available charts and reports depend on the solutions currently installed and implemented in your environment. Therefore, the charts and reports for each section might vary between environments.

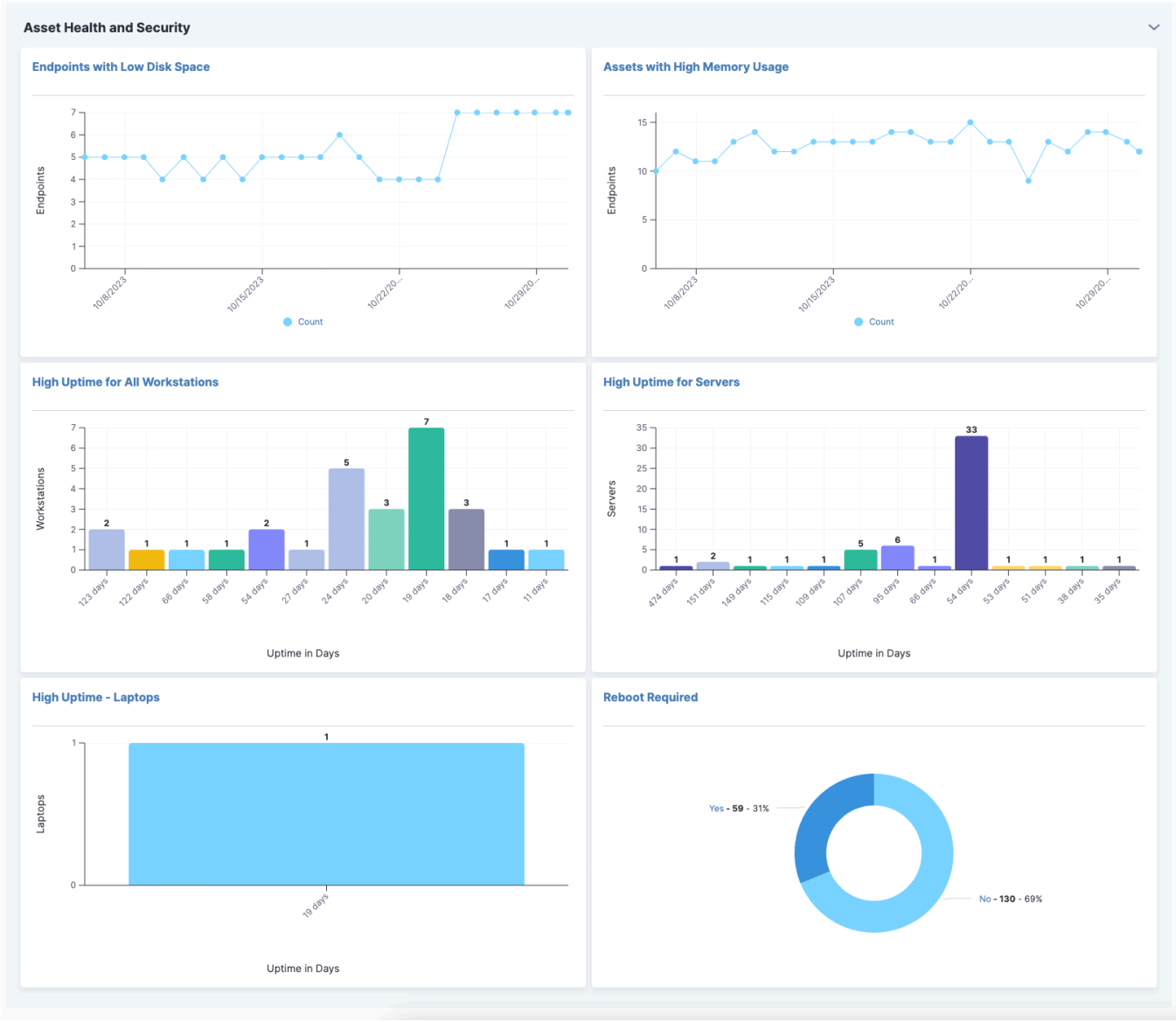


Asset Health and Security

Use the data in the **Asset Health and Security** section to assess the health of endpoints in your environment.

Note: The available charts and reports depend on the solutions currently installed and implemented in your environment. Therefore, the charts and reports for each section might vary between environments.

©2026 Tanium Inc. All Rights Reserved



What to do next

Use the data in this assessment to drive actions in your environment to improve your risk posture:

- Install patches and updates to software and operating systems with known exploited vulnerabilities.
- Update software to ensure that all available security fixes are applied on endpoints.
- Remediate issues with endpoint health:
    - Clean up disk drives or add additional storage for endpoints with low disk space.

©2026 Tanium Inc. All Rights Reserved

- Investigate the cause of high memory usage on endpoints and consider adding additional resources.
- Reboot endpoints with high uptime or those that require a reboot.

©2026 Tanium Inc. All Rights Reserved

Reviewing your vulnerability dashboards

About this task

Review the impact of vulnerabilities in your environment with visual dashboards that are a collection of charts and reports. Vulnerabilities are evaluated based on impact and priority in your environment.

Vulnerability impact and priority calculation

Benchmark evaluates the vulnerabilities in your environment and provides both an impact score and priority score for each vulnerability. Vulnerability impact scores are calculated by multiplying CVSS v3 score and the number of endpoints that contain the vulnerability. Vulnerability priority scores are a calculation of vulnerability impact scores and endpoint criticality values.

Vulnerability impact formula

The following formula is used to calculate the vulnerability impact for a CVE:

```
Common Vulnerability Scoring System (CVSS) v3 score x Total # of Endpoints = Vulnerability Impact
```

Vulnerability priority formula

The following formula is used to calculate the vulnerability priority for a CVE:

```
Vulnerability Impact x Average Endpoint Criticality Value = Vulnerability Priority
```

Endpoint criticality value

Endpoint criticality is a level on an individual endpoint that is used to add context about the endpoint in the organization. Possible levels are **Critical**, **High**, **Medium**, and **Low**. These levels indicate the importance of the endpoint in your environment.

The score for an endpoint is adjusted based on the criticality level:

©2026 Tanium Inc. All Rights Reserved

- **Low:** No adjustment to the score for the endpoint
- **Medium:** (Default) Multiplies the score for the endpoint by 1.33
- **High:** Multiplies the score for the endpoint by 1.67
- **Critical:** Multiplies the score for the endpoint by 2

For example, if an endpoint has a score of 200, but the endpoint is flagged as critical, the score reported for that endpoint is 400.

Benchmark uses Tanium Criticality to manage criticality levels for endpoints. For more information, see Tanium Criticality User Guide: Criticality overview.

View your vulnerability dashboard

About this task

From the Main menu, go to **Modules** > **Benchmark** > **Dashboards** > **Vulnerability**. You can select the **Computer Group** to use for the data. Click Refresh now to refresh the data in the charts. You can also adjust the auto refresh time frame. Click **Summarize** to generate a summary of your vulnerability dashboards. For more information, see Tanium Reporting User Guide: Summarize dashboards.

Vulnerability metrics

Use the data in the Vulnerability Metrics section to gain insight into the highest vulnerability impact and vulnerability priority scores by CVE. You can select a CVE to view CVE details in Tanium Reporting. For more information, see Tanium Reporting User Guide: Summarize dashboards.

Figure 3. Vulnerability metrics by CVE

©2026 Tanium Inc. All Rights Reserved



CVEs sorted by vulnerability priority

Use the data in the **CVEs sorted by vulnerability priority** table to gain insight into high-impact CVEs on your endpoints. Click Refresh to refresh the data.

Important: To explore in Tanium Comply and remediate in Tanium Patch, you must have licenses for the associated modules.

Figure 4. CVEs with the highest severity ratings

CVEs Sorted by Vulnerability Priority

These vulnerabilities are sorted by vulnerability priority, determined by high severity ratings and the number affected of mission-critical endpoints in the environment. Remediate these vulnerabilities to significantly reduce your overall vulnerability risk across endpoints deemed important to your organization.

11,862 Items

View Report | Filter items

Comply - Vulnerabili... Check ID	Comply - Vulnerabili... CVSS v3 Severity	Comply - Vulnerabili... CVSS v3 Base Score	Endpoint Co... (3)	Vulnerability ... (2)	Vulnerability ... (1)	Low Severity Endp...	Medium Severity E...	High Severity Endp...	Critical Severity En...
CVE-2025-55319	Critical	9.8	10	98	183	0	0	4	6
CVE-2025-11002	Critical	9.8	9	88	167	0	0	3	6
CVE-2025-41244	High	7.8	11	86	159	0	0	5	6
CVE-2025-13021	Critical	9.8	8	78	147	0	0	3	5
CVE-2025-13026	Critical	9.8	8	78	147	0	0	3	5
CVE-2025-13023	Critical	9.8	8	78	147	0	0	3	5
CVE-2025-13022	Critical	9.8	8	78	147	0	0	3	5
CVE-2025-12380	Critical	9.8	8	78	147	0	0	3	5
CVE-2025-13024	Critical	9.8	8	78	147	0	0	3	5
CVE-2025-24039	High	7.3	10	73	136	0	0	4	6
CVE-2025-24042	High	7.3	10	73	136	0	0	4	6
CVE-2025-26631	High	7.3	10	73	136	0	0	4	6
CVE-2025-21264	High	7.1	10	71	133	0	0	4	6

©2026 Tanium Inc. All Rights Reserved

- Sort the table. By default, the table is sorted by vulnerability priority, vulnerability impact, and endpoint count, in that order of priority. You can select a column heading to sort the table by descending values for that category. Select the column heading again to sort by ascending values.

- Filter table items. Search for table items in the **Filter items** field. Filters apply to all table columns.

- Customize table columns. Click Customize Columns to select which columns are included in the table and select the left icon to reorder columns. Hover between column titles and drag the double-sided arrow to adjust column width. You can also hover over Information to learn more about columns.

- Investigate vulnerability findings. Select one or more table rows, and click **Explore in Comply** to view vulnerability findings. For more information, see Tanium Comply User Guide: Investigating Findings.

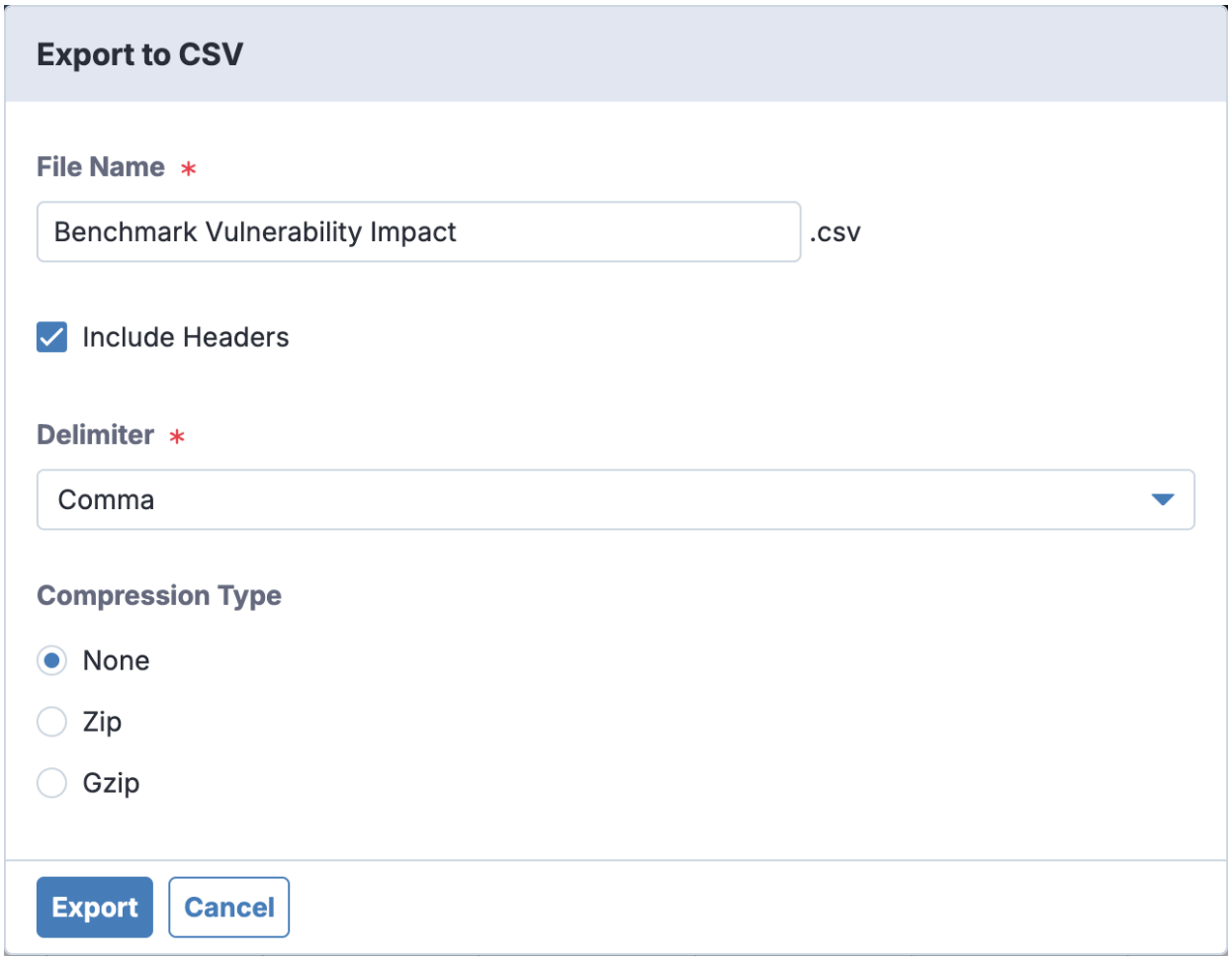
- Remediate vulnerability findings. Select one or more table rows. If there are applicable patches in the Patch module, you can click **Remediate in Patch** to view and take actions for missing patches. For more information, see Tanium Patch User Guide: Managing patches.

- View detailed data in Tanium Reporting. To open the **Benchmark Vulnerability Impact** report, click **View Report**. For more information, see Tanium Reporting User Guide: Working with reports.

- Export table data. Click the Export button to view the **Export to CSV** window. Specify the file name, headers option, delimiter format, and compression type, then click **Export**.

  Figure 5. Export to CSV window settings

©2026 Tanium Inc. All Rights Reserved



©2026 Tanium Inc. All Rights Reserved

Generating the Tanium Risk Assessment

About this task

The Tanium Risk Assessment (TRA) is a report of operational and security risks in your organization based on metrics and data points identified during the evaluation. You can generate the assessment as often as needed. For more information, see Tanium Risk Assessment on page 10.

Before you begin

- Ensure that you have the necessary roles and permissions to enable data collection and to configure and generate the assessment. For more information, see Solutions and permissions for Tanium Risk Assessment on page 26.
- Ensure that data collection is enabled. For more information, see (Optional) Enable data collection for Tanium Risk Assessment on page 37.

> **Best Practice:** For best results, ensure that Tanium Criticality 1.6 or later is installed.

Configure and generate Tanium Risk Assessment

You can generate an executive summary or a more extensive detailed report. You can export the assessment to JSON or HTML, so you can import the data into your own solutions.

1. From the Main menu, go to **Modules** > **Benchmark** > **Risk Assessment**.
2. Select a Benchmark computer group to use in the assessment.
   You can select a different computer group each time that you generate the assessment.

©2026 Tanium Inc. All Rights Reserved

> **Note:** The computer group and your management rights for the endpoints in the computer group might affect the number of endpoints included in the assessment.

3. If you have Impact installed and configured, select up to three Windows endpoints in the computer group to demonstrate lateral impact risk in the detailed report.
   By default, three endpoints with the highest impact rating have been selected. To select other endpoints, remove an endpoint and enter a computer name to search for another endpoint. Refresh the page to return to the default selections.

4. Generate the assessment.
   a. Select if you want the assessment to include sections with no applicable endpoints or no identified risks.
      A section has no applicable endpoints when the endpoints do not apply to the risk identified in the section, for example, Linux endpoints in a section for a Windows risk. A section has no identified risks when the endpoints were evaluated and do not contain the risk identified in the section. If you select this option, tables, charts, and other items appear with a message that the endpoints do not include the risk. You might include these items in the assessment to be aware of all evaluated risks.

   b. Generate either a detailed report or executive summary in HTML or JSON. You might select HTML to easily review the assessment on its own or select JSON to input the data into your own solution.
      The assessment is downloaded to your default downloads folder. Benchmark does not store previously generated TRAs.

5. If you generate the detailed report and a section is missing content because of missing permissions or solutions or other errors, a table appears with the impacted section title and a status describing the issues. The sections with missing content do not appear in the report. Review the table and resolve issues as necessary. For more information, see Unable to generate or export Tanium Risk Assessment on page 80.

©2026 Tanium Inc. All Rights Reserved

Troubleshooting Benchmark

About this task

To collect and send information to Tanium for troubleshooting, collect logs and other relevant information.

Collect logs

About this task

The information is saved as ZIP files that you can download with your browser. The ZIP files are also known as a support bundle.

To download logs:

1. From the Main menu, go to **Modules** > **Benchmark > Overview**. Click Help ?.
2. From the **Troubleshooting** tab, select the solutions for which to gather troubleshooting packages and click **Create Packages**. By default, all solutions are selected.
3. When the packages are ready, click **Download Packages**. ZIP files of all the selected packages download to the local download directory.

   Tip: Some browsers might block multiple downloads by default. Make sure to configure your browser to permit multiple downloads from Tanium Console.
4. Contact Tanium Support to determine the best option to send the ZIP files. For information, see Contact Tanium Support on page 83.

Benchmark monthly maintenance

1. From the Main menu, go to **Modules** > **Benchmark** > **Metric Health**.
2. Review whether you are getting data for each Tanium™ Benchmark metric. For more information, see Tanium Benchmark User Guide: Monitor and troubleshoot Benchmark

©2026 Tanium Inc. All Rights Reserved

metric health.

Monitor and troubleshoot Benchmark metric health

From the Main menu, go to **Modules** > **Benchmark** > **Metric Health**. Use the **Metric Health** page to monitor and improve the data for each Benchmark metric.

Metric Health for Supported Endpoints

The **Metric Health for Supported Endpoints** chart shows how many supported Tanium Client managed endpoints are not sending data for a particular metric. Unsupported endpoints, for example, that use an operating system that is not supported by the metric, are not included in this count. Ideally, the values in this chart are as close to zero as possible. You can click a bar in the chart to view details about the status of that metric.

Note: Some metrics do not return data that can be displayed in this chart. For example, the metric might be calculated across all endpoints, not calculated per endpoint. Some Threat Response data is sent only when an endpoint has data, but if an endpoint does not have data (for example, no alerts), no status is reported.

Metric Health

The **Metric Health** section includes detailed information about endpoints, whether they are supported for the metric and whether they are returning data.

Improve Metric Health

About this task

Improve your Benchmark data by regularly reviewing the metric health and making improvements to enable endpoints to return data.

1. From the Main menu, go to**Modules** > **Benchmark** > **Metric Health**.
2. Review detailed data for a metric. You can either click a bar in the **Metric Health for Supported Endpoints**, or select a metric in the **Filters** section.

©2026 Tanium Inc. All Rights Reserved

3. Identify and resolve problems. In the **Metric Health** section, you can filter the results, or sort by columns in the table to group like results together.
    - **Sending Data**: If the value for this column is **No**, the endpoint is not returning results for this metric. Review the other columns for this endpoint to determine the potential issue. If the value is **Yes**, the endpoint is returning data and no further analysis is required.
    - **Solution Supported**: If the value for this column is **No**, the endpoint cannot return results for this metric. For example, the endpoint could be Linux operating and the metric is only supported for Windows. No further analysis is required for this endpoint.
    - **In Action Group**: If the value for this column is **No**, the endpoint is not in the Benchmark action group. For more information, see Configure the Benchmark action group on page 34.
    - **Health Status**: If the status is anything other than **Optimal**, the solution on the endpoint that is providing the metric data has a problem. Note the value for the **Tanium Solution** column, and then investigate the health status of endpoint in the related solution. For example, if a Patch metric has a health problem, you can investigate further by going to the Patch solution and looking at the **Patch Coverage** section of the home page.
4. Review individual endpoint details. In the **Metric Health** section, click Endpoint Details , then **View Details**.

Unable to generate or export Tanium Risk Assessment

On the **Risk Assessment** page, when you generate or export the Tanium Risk Assessment , you might see an error message at the top of the page or in the **Generate TRA Report** section. Use the information in the following table to resolve the errors.

Tanium Risk Assessment errors

Error message or condition	Corrective action
No endpoints selected	Select up to three Windows endpoints in the computer group to demonstrate lateral impact risk. For more information, see Generating the Tanium Risk Assessment on page 76 .

©2026 Tanium Inc. All Rights Reserved

Error message or condition	Corrective action
User does not have required permissions to this data	Update your permissions. For more information, see Solutions and permissions for Tanium Risk Assessment on page 26 .
• <Solution> is not available • <Sensor> sensor not found • Metrics unavailable	Update the solutions or sensors in your environment as needed. For more information, see Solutions and permissions for Tanium Risk Assessment on page 26 .
Unable to generate the assessment for <name> computer group because no endpoints in the computer group currently have a Tanium risk score	Resolve issues with endpoints that cannot return data. For more information, see Monitor and troubleshoot Benchmark metric health on page 79 .
Assessment does not generate	Try again to generate and export the assessment. If the error persists, Contact Tanium Support on page 83 .

Remove Benchmark tools from endpoints

About this task

You can deploy an action to remove Benchmark tools from an endpoint or computer group. Separate actions are available for Windows and non-Windows endpoints.

1. From the **Tanium Home** page, target the endpoints from which you want to remove the tools. For example, ask a question that targets a specific operating system: `Get Endpoint Configuration - Tools Status from all machines with Is Windows equals true`
2. In the results, select the row for **Risk**, drill down as necessary, and select the targets from which you want to remove Benchmark tools. For more information, see Tanium Interact User Guide: Drill Down.
3. Click **Deploy Action**.
4. For the **Deployment Package**, select **Endpoint Configuration - Uninstall Tool [Windows]** or **Endpoint Configuration - Uninstall Tool [Non-Windows]**, depending on the endpoints you are targeting.
5. For **Tool Name**, select **Risk**.

©2026 Tanium Inc. All Rights Reserved

6. (Optional) By default, after the tools are removed they cannot be reinstalled. To allow tools to be automatically reinstalled, clear the selection for **Block reinstallation**. Re-installation occurs almost immediately.

   Note:
   If reinstallation is blocked, you must unblock it manually:

   - To allow Benchmark to reinstall tools, deploy the **Endpoint Configuration - Unblock Tool [Windows]** or **Endpoint Configuration - Unblock Tool [Non-Windows]** package (depending on the targeted endpoints).
   - If you reinstall tools manually, select **Unblock Tool** when you deploy the **Endpoint Configuration - Reinstall Tool [Windows]** or **Endpoint Configuration - Reinstall Tool [Non-Windows]** package.

7. (Optional) To remove all Risk databases and logs from the endpoints, clear the selection for **Soft uninstall**.

   CAUTION: When you perform a hard uninstallation of some tools, the uninstallation also removes data that is associated with the tool from the endpoint. This data might include important historical or environmental data. If data that you want to keep is associated with the tool, make sure you perform only a soft uninstallation of the tool.

8. To also remove any tools that were dependencies of the Risk tools that are not dependencies for tools from other solutions, select **Remove unreferenced dependencies**.

9. (Optional) In the **Deployment Schedule** section, configure a schedule for the action.

   Best Practice: If some target endpoints might be offline when you initially deploy the action, select **Recurring Deployment** and set a reissue interval.

10. Click **Show preview to continue**.

11. A results grid appears at the bottom of the page showing you the targeted endpoints for your action. If you are satisfied with the results, click **Deploy Action**.

Result

©2026 Tanium Inc. All Rights Reserved

Note: If you have enabled Endpoint Configuration approval, tool removal must be approved in Endpoint Configuration before tools are removed from endpoints.

Uninstall Benchmark

1. From the Main menu, go to **Administration** > **Configuration** > **Solutions**.
2. Select Benchmark, and click **Uninstall**.
3. Review the content that will be removed and click **Uninstall**.
4. Depending on your configuration, enter your password or click **Yes** to start the uninstall process.
5. Return to the **Solutions** page and verify that the **Import** button is available for Benchmark.

Contact Tanium Support

To contact Tanium Support for help, sign in to the Tanium Customer Community.

For more information about submitting a support case, see Case Submission Form.

©2026 Tanium Inc. All Rights Reserved

Reference: Gateway examples for Benchmark

Tanium Gateway provides a GraphQL API integration point for Tanium solutions, including Benchmark. Benchmark queries retrieve endpoints and related risk overview or metric information.

Certain risk metric queries require additional Tanium solutions. For more information, see Solution dependencies on page 18.

For additional Gateway example syntax, see Tanium Gateway User Guide: Reference: Filter syntax and Tanium Gateway User Guide: Reference: Gateway examples.

Get endpoint with Risk Score 2.0 information

(query.endpoints.edges.node.sensorReadings (sensors.filters))

About this task

The following query retrieves the first endpoint with associated Benchmark overview information.

```
query exampleGetEndpoints($first: Int) {
  endpoints(first: $first) {
    edges {
      node {
        name
        sensorReadings(sensors: [{ name: "Tanium Risk Score" }]) {
          columns {
            sensor {
              name
            }
            name
            values
          }
        }
      }
    }
  }
}
```

Include a variable for the number of endpoints to return in the **Variables** panel or in your variables dictionary:

```
{
  "first": 1
```

©2026 Tanium Inc. All Rights Reserved

```
}
```

Example response:


```
{
  "data": {
    "endpoints": {
      "edges": [
        {
          "node": {
            "name": "example-endpoint",
            "sensorReadings": {
              "columns": [
                {
                  "sensor": {
                    "name": "Tanium Risk Score"
                  },
                  "name": "Risk Score",
                  "values": [
                    "438"
                  ]
                },
                {
                  "sensor": {
                    "name": "Tanium Risk Score"
                  },
                  "name": "Critical Severity Vulnerabilities Score",
                  "values": [
                    "665"
                  ]
                },
                {
                  "sensor": {
                    "name": "Tanium Risk Score"
                  },
                  "name": "High Severity Vulnerabilities Score",
                  "values": [
                    "665"
                  ]
                },
                {
                  "sensor": {
                    "name": "Tanium Risk Score"
                  },
                  "name": "Compliance Failures Score",
                  "values": [
                    "486"
                  ]
                },
                {
                  "sensor": {
                    "name": "Tanium Risk Score"
                  },
                  "name": "Lateral Movement Risk Score",
                  "values": [
                    ""
                  ]
                },
                {
                  "sensor": {
                    "name": "Tanium Risk Score"
                  },
```


©2026 Tanium Inc. All Rights Reserved

```
                  "name": "Insecure TLS/SSL Score",
                  "values": [
                    "0"
                  ]
                },
                {
                  "sensor": {
                    "name": "Tanium Risk Score"
                  },
                  "name": "Expired Certificates Score",
                  "values": [
                    "0"
                  ]
                }
              ]
            }
          }
        }
      ]
    }
  }
}
```


©2026 Tanium Inc. All Rights Reserved