Tanium Risk Assessment Detailed Report

Prepared for: Software Company

Customer Industry: Business Services

Targeted Group: All Computers

Calculated Risk Score:

415

- Risk Score of 0 represents best in class risk avoidance practice
- Risk score of 1,000 is the worst score representing maximum risks in the environment

Author: lucas.lyon@tanium.com
Created On: 8/12/2025

The Tanium Risk Assessment ("TRA") has been created using Tanium Inc. proprietary software products to analyze customer's endpoint environment. Tanium provides the TRA to customer "as-is" and gives no representation, warranty, indemnity, guarantee, or condition of any kind. To the maximum extent permitted by law, Tanium's total aggregate liability and that of its licensors, suppliers, and partners is expressly limited to five hundred dollars ($500) for any and all damages related to the TRA, regardless of the nature of the claim or theory of liability.

As consideration for receiving this report, customer permits Tanium to use the data contained herein on an aggregated and/or anonymized basis for benchmarking and marketing purposes.

Table of Contents

Part 1: Asset Inventory Covered by the Assessment

Tanium provides an end-to-end platform that allows organizations to manage end user, server and cloud endpoints with speed, scale and reliability, and provides complete, accurate and up-to-date endpoint data for operations, security and risk teams.

Within the network locations that Tanium was given access to, we have discovered the following estate:

1359
Total Interfaces

1312
Managed interfaces (Endpoints running the Tanium client)

42
Unmanaged interfaces (Endpoints not running the Tanium client)

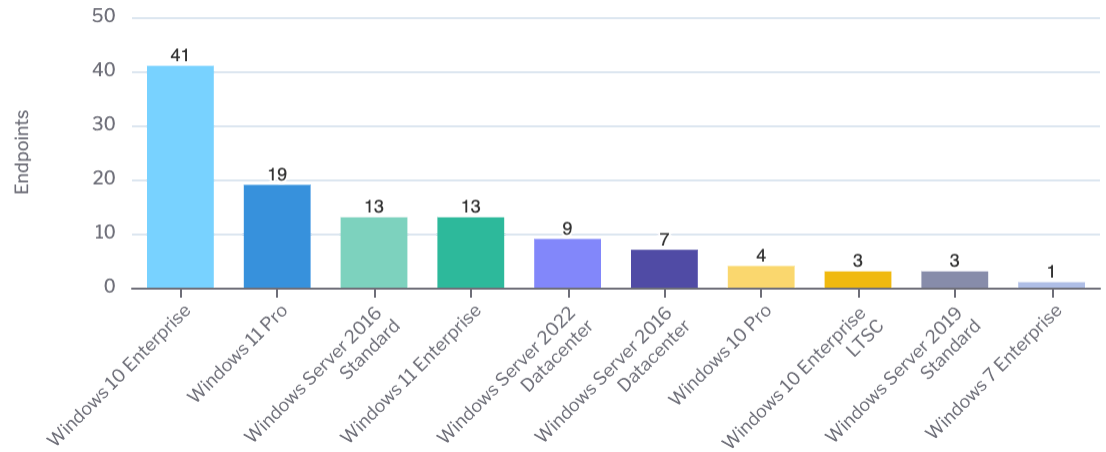
2
Lost interfaces (Interfaces found on endpoints that were previously seen running the Tanium client, but are no longer reporting as Managed)

Interfaces are not 1:1 for endpoints and devices. A detected interface indicates a functional network connection that Tanium was able to observe or interact with.

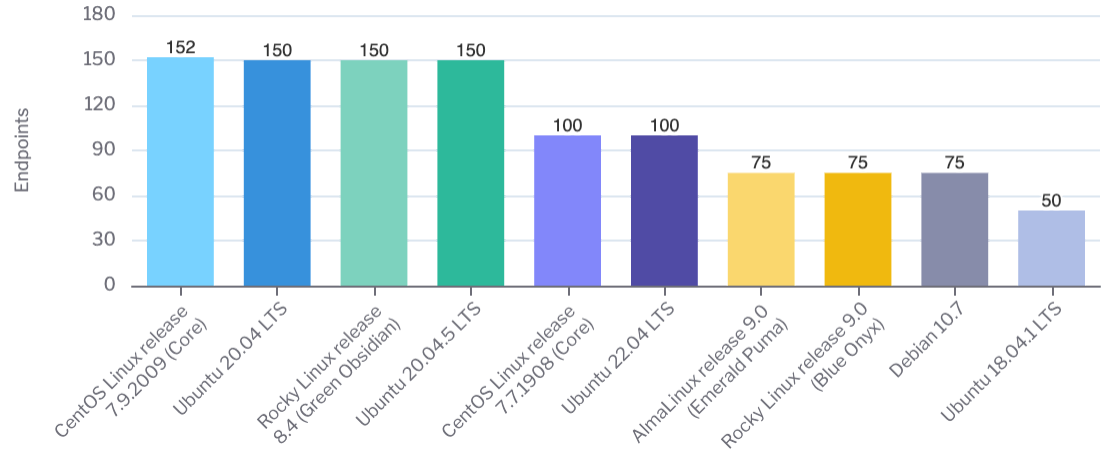
Unmanaged interfaces (typically endpoints not running the Tanium client) represent blind spot risk for the organization, as the visibility and ability to build a service dependency map for those endpoints are limited. Unmanaged interfaces also include devices that cannot run the Tanium Client (such as printers and switches) but these devices remain discoverable via remote asset discovery and vulnerability scanning functionality.

The following is the operating system type distribution across the managed estate:

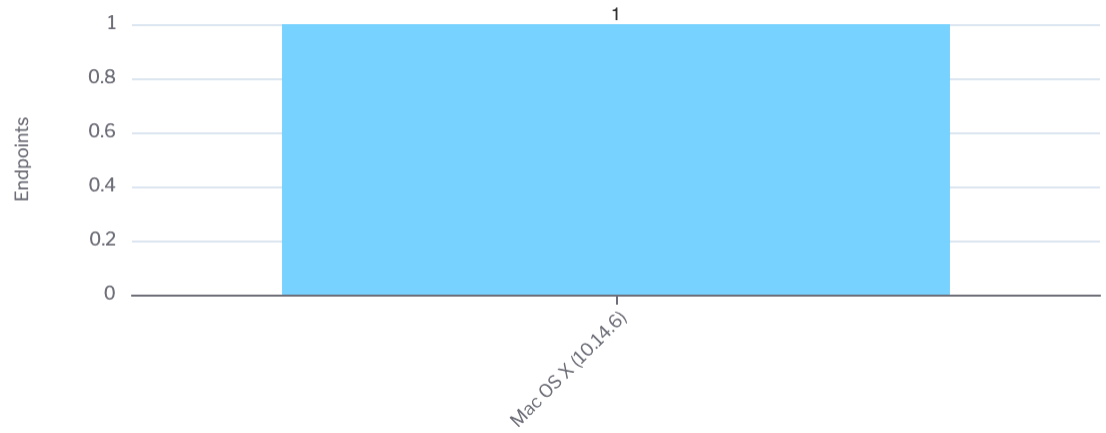
Top 10 Windows Operating System Versions



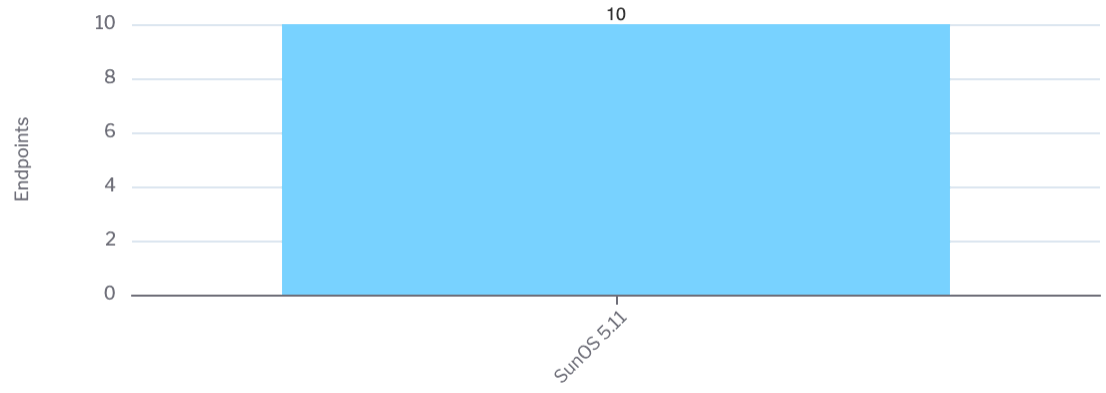
Top 10 Linux Operating System Versions



Top 10 macOS Operating System Versions



Top 10 Solaris Operating System Versions



Within the environment visible to the Tanium platform, Tanium identified **1081** endpoints with EOL version of an operating system as well as **163** endpoints with uptime of more than 30 days (with the highest uptime value found of **878 days**). Note: This data does not take into account extended support agreements that may be in place with specific vendors for specific operating systems. The information provided in this report is a snapshot in time and may no longer represent the state of the environment at present.

Endpoint Criticality

It is important to acknowledge that not all endpoints are created equal, and some endpoints can (and should) have a varying degree of impact on the organization's risk score based on their criticality and importance to the organization and its business processes.

For the endpoints included in the assessment, the following table identifies the top 10 criticality rules by priority and criticality level. You can also review the number of endpoints assigned to each level.

Note: Endpoints are assigned to the **Critical** criticality level if they do not match a criticality rule.

Endpoint Criticality Level	Top 10 Highest Priority Criticality Rules	Endpoints with Criticality Level
Critical	• TRA Critical Endpoints (Priority 1) • Risk Dedicated Machines (Priority 2) • v1-criticality-csv-critical (Priority 5) • Domain Controllers • TRA - Database Servers • TRA - EoL Operating Systems • TRA - Unencrypted Physical Disks	627
High	• v1-criticality-csv-high (Priority 3) • TRA High Endpoints (Priority 4) • Servers	682
Medium	*No active medium criticality rules in the top 10 rules by priority*	0
Low	*No active low criticality rules in the top 10 rules by priority*	0

Endpoints Missing A/V Processes

The following table provides a partial list (10 out of 1199) of endpoints that are not running Software Company's standard AV protection software.

Endpoint Name	Operating System	Lateral Movement Risk
rev-wn-381.demo.tanium.local	Windows 10	Medium
rev-wn-382.demo.tanium.local	Windows 10	Medium
rev-wn-380.demo.tanium.local	Windows 10	Medium
jfk-lxc-10021.demo.tanium.local	Ubuntu 20.04	N/A
den-lxc-2432.demo.tanium.local	Ubuntu 20.04	N/A
ord-lxc-1222.demo.tanium.local	CentOS 7	N/A
sfo-lxc-11504.demo.tanium.local	AlmaLinux 9	N/A
dfw-lxc-2319.demo.tanium.local	Ubuntu 20.04	N/A
jfk-lxc-10115.demo.tanium.local	Ubuntu 22.04	N/A

Endpoint Name	Operating System	Lateral Movement Risk
lax-lxc-2118.demo.tanium.local	Ubuntu 18.04	N/A

Part 2: Risk Metrics Analysis

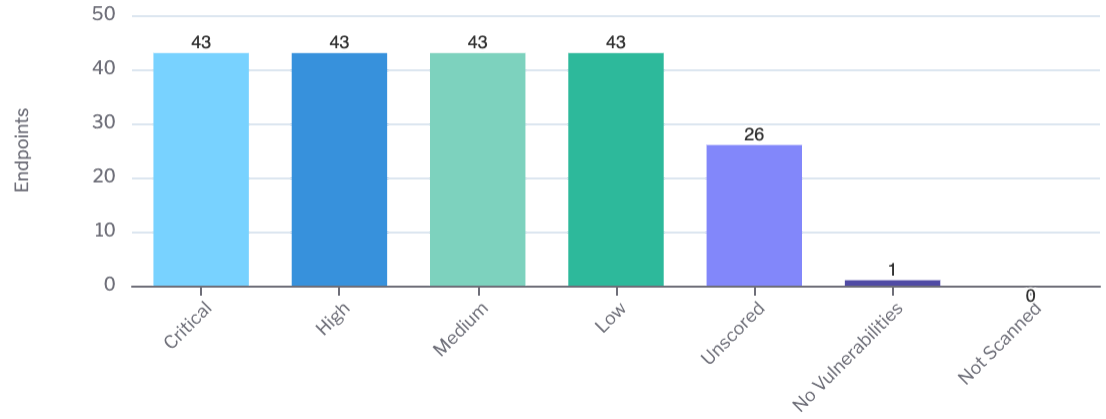
In the following section, we provide Software Company with factual data regarding risk in the environment prioritized by its overall impact on the overall risk posture. Identified issues and gaps can be remediated using the Tanium platform without requiring additional tools or agents.

System Vulnerabilities

Most common attacks exploit endpoints with operating system or application misconfigurations. To measure the security exposure, the high and critical vulnerability metrics consider the presence of endpoints with critical or high vulnerabilities, which puts organizations at greater risk of disruption or breach. High and critical system vulnerability metrics comprise part of the Tanium risk score.

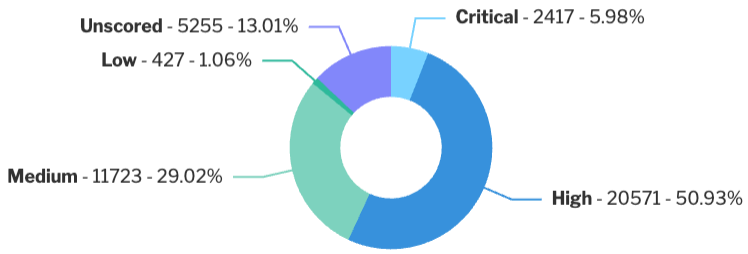
Overall Vulnerability Scan Results

Results of vulnerability scan on endpoints. If an endpoint has multiple vulnerabilities, the endpoint is counted in each applicable severity.



Vulnerabilities by Severity

Number of vulnerabilities by severity across all endpoints



During the assessment, the following system vulnerabilities observations were made:

- A total of 40393 vulnerabilities were found across 43 endpoints (939.37 per endpoint).
  - 2417 total vulnerabilities with critical severity (56.21 per endpoint)
  - 20571 total vulnerabilities with high severity (478.4 per endpoint)
  - 11723 total vulnerabilities with medium severity (272.63 per endpoint)
  - 427 total vulnerabilities with low severity (9.93 per endpoint)
- A total of 9929 unique vulnerability check IDs were found in the environment.

- 728 unique vulnerabilities with critical severity
- 4221 unique vulnerabilities with high severity
- 2630 unique vulnerabilities with medium severity
- 124 unique vulnerabilities with low severity

A critical component of successfully remediating risk factors is the ability to prioritize the action needed to take place as part of the remediation plan. The following are the top 10 endpoints with the highest Critical Severity Vulnerabilities risk metric scores. Remediate the vulnerabilities on these endpoints first to reduce the risk that the endpoints present.

Note: Endpoint criticality is discussed in part 1

Endpoint Name	Endpoint Criticality	Critical Severity Vulnerabilities Risk Metric Score	Risk Score	Operating System	Number of Critical Severity Vulnerabilities
rsk-lx-2904.demo.tanium.local	Critical	1000	855	CentOS 7	12
rsk-wn-2903.demo.tanium.local	Critical	1000	826	Windows Server 2019	502
demo-ras-satellite.demo.tanium.local	Critical	1000	816	CentOS 8	15
edr-wn-2518.demo.tanium.local	Critical	1000	718	Windows 11	26
edr-wn-2516.demo.tanium.local	Critical	1000	718	Windows 11	24
edr-wn-2519.demo.tanium.local	Critical	1000	718	Windows 11	16
edr-wn-2517.demo.tanium.local	Critical	1000	718	Windows 11	16
edr-wn-2510.demo.tanium.local	Critical	1000	718	Windows Server 2022	12
rsk-lx-2905.demo.tanium.local	Critical	1000	713	CentOS 8	53
edr-wn-2513.demo.tanium.local	Critical	1000	704	Windows 10	31

A critical component of successfully remediating risk factors is the ability to prioritize the action needed to take place as part of the remediation plan. The following are the top 10 endpoints with the highest High Severity Vulnerabilities risk metric scores. Remediate the vulnerabilities on these endpoints first to reduce the risk that the endpoints present.

Endpoint Name	Endpoint Criticality	High Severity Vulnerabilities Risk Metric Score	Risk Score	Operating System	Number of High Severity Vulnerabilities
rsk-lx-2904.demo.tanium.local	Critical	1000	855	CentOS 7	37
rsk-wn-2903.demo.tanium.local	Critical	1000	826	Windows Server 2019	1913
demo-ras-satellite.demo.tanium.local	Critical	1000	816	CentOS 8	61
edr-wn-2510.demo.tanium.local	Critical	1000	718	Windows Server 2022	338
edr-wn-2516.demo.tanium.local	Critical	1000	718	Windows 11	303
edr-wn-2518.demo.tanium.local	Critical	1000	718	Windows 11	266
edr-wn-2519.demo.tanium.local	Critical	1000	718	Windows 11	130
edr-wn-2517.demo.tanium.local	Critical	1000	718	Windows 11	130
rsk-lx-2905.demo.tanium.local	Critical	1000	713	CentOS 8	300
edr-wn-2513.demo.tanium.local	Critical	1000	704	Windows 10	353

The following 10 vulnerabilities have the highest severity ratings and affect the largest number of endpoints. Remediate these vulnerabilities first to significantly reduce your overall vulnerability risk.

CVE	Endpoint Count	CVSS Score	CVE Year	Vulnerability Impact
CVE-2024-24790 - The various Is methods (IsPrivate, IsLoopback, etc) did not work as expected for IPv4-mapped IPv6 addresses, returning false for addresses which would return true in their traditional IPv4 forms.	41	9.8	2024	402
CVE-2023-39323 - Line directives ("//line") can be used to bypass the restrictions on "//go:cgo_" directives, allowing blocked linker and compiler flags to be passed during compilation. This can result in unexpected execution of arbitrary code when running "go build". The line directive requires the absolute path of the file in which the directive lives, which makes exploiting this issue significantly more complex.	41	8.1	2023	332
CVE-2023-29402 - The go command may generate unexpected code at build time when using cgo. This may result in unexpected behavior when running a go program which uses cgo. This may occur when running an untrusted module which contains directories with newline characters in their names. Modules which are retrieved using the go command, i.e. via "go get", are not affected (modules retrieved using GOPATH-mode, i.e. GO111MODULE=off, may be affected).	33	9.8	2023	323
CVE-2021-38297 - Go before 1.16.9 and 1.17.x before 1.17.2 has a Buffer Overflow via large arguments in a function invocation from a WASM module, when GOARCH=wasm GOOS=js is used.	33	9.8	2021	323
CVE-2023-24540 - Not all valid JavaScript whitespace characters are considered to be whitespace. Templates containing whitespace characters outside of the character set "\t\n\f\r\u0020\u2028\u2029" in JavaScript contexts that also contain actions may not be properly sanitized during execution.	33	9.8	2023	323
CVE-2023-29405 - The go command may execute arbitrary code at build time when using cgo. This may occur when running "go get" on a malicious module, or when running any other command which builds untrusted code. This is can by triggered by linker flags, specified via a "#cgo LDFLAGS" directive. Flags containing embedded spaces are mishandled, allowing disallowed flags to be smuggled through the LDFLAGS sanitization by including them in the argument of another flag. This only affects usage of the gccgo compiler.	33	9.8	2023	323
CVE-2023-29404 - The go command may execute arbitrary code at build time when using cgo. This may occur when running "go get" on a malicious module, or when running any other command which builds untrusted code. This is can by triggered by linker flags, specified via a "#cgo LDFLAGS" directive. The arguments for a number of flags which are non-optional are incorrectly considered optional, allowing disallowed flags to be smuggled through the LDFLAGS sanitization. This affects usage of both the gc and gccgo compilers.	33	9.8	2023	323
CVE-2023-24538 - Templates do not properly consider backticks (`) as Javascript string delimiters, and do not escape them as expected. Backticks are	33	9.8	2023	323

CVE	Endpoint Count	CVSS Score	CVE Year	Vulnerability Impact
used, since ES6, for JS template literals. If a template contains a Go template action within a Javascript template literal, the contents of the action can be used to terminate the literal, injecting arbitrary Javascript code into the Go template. As ES6 template literals are rather complex, and themselves can do string interpolation, the decision was made to simply disallow Go template actions from being used inside of them (e.g. "var a = {{.}}"), since there is no obviously safe way to allow this behavior. This takes the same approach as github.com/google/safehtml. With fix, Template.Parse returns an Error when it encounters templates like this, with an ErrorCode of value 12. This ErrorCode is currently unexported, but will be exported in the release of Go 1.21. Users who rely on the previous behavior can re-enable it using the GODEBUG flag jstmpllitinterp=1, with the caveat that backticks will now be escaped. This should be used with caution.				
CVE-2023-44487 - The HTTP/2 protocol allows a denial of service (server resource consumption) because request cancellation can reset many streams quickly, as exploited in the wild in August through October 2023.	41	7.5	2023	308
CVE-2023-45285 - Using go get to fetch a module with the ".git" suffix may unexpectedly fallback to the insecure "git://" protocol if the module is unavailable via the secure "https://" and "git+ssh://" protocols, even if GOINSECURE is not set for said module. This only affects users who are not using the module proxy and are fetching modules directly (i.e. GOPROXY=off).	41	7.5	2023	308

Lateral Movement Risk

Nearly all cyberattacks today involve lateral movement (using stolen credentials to move from endpoint to endpoint). Lateral movement and overly permissive administrative rights enable the propagation of malware and ransomware and exfiltration of sensitive data. This risk metric considers administrative and access rights based on your Active Directory environment and the identified potential for lateral movement. Administrative access management and risk of lateral movement are used as part of creating the Tanium Risk Score.

A critical component of successfully remediating risk factors is the ability to prioritize the action needed to take place as part of the remediation plan. The following are the top 10 endpoints with the highest Lateral Movement Risk risk metric scores. Reduce administrative access to these endpoints to lower lateral movement risk and insider threat probability.

Note: Endpoint criticality is discussed in part 1. *Impact rating* is influenced by potential inbound impact by users and endpoints and potential outbound impact by users and endpoints. Endpoints, users, and groups with a critical impact rating have the highest potential lateral movement and are likely to be targeted for compromise. *Direct and indirect control* represent the number of endpoints on which this user has administrative rights through a direct entry in the local Administrators object and through an Active Directory group or nested group that has an entry in the local Administrators object. *Inbound* is the sum of the endpoints and users that an attacker can use to move laterally to compromise the user credentials. *Outbound* is the sum of the endpoints and users that an attacker can reach by moving laterally using the compromised credentials. *Sessions* is the number of active sessions the user has open on endpoints.

Endpoint Name	Endpoint Criticality	Lateral Movement Risk Risk Metric Score	Risk Score	Operating System	Impact Rating	Control (dr/idr)	Inbound	Outbound	Sessions
rsk-wn-2903.demo.tanium.local	Critical	500	826	Windows Server 2019	High	791	814	115	1

Endpoint Name	Endpoint Criticality	Lateral Movement Risk Risk Metric Score	Risk Score	Operating System	Impact Rating	Control (dr/idr)	Inbound	Outbound	Sessions
edr-wn-2519.demo.tanium.local	Critical	500	718	Windows 11	High	58	814	115	1
edr-wn-2517.demo.tanium.local	Critical	500	718	Windows 11	High	58	814	115	1
edr-wn-2510.demo.tanium.local	Critical	500	718	Windows Server 2022	High	58	814	115	1
edr-wn-2518.demo.tanium.local	Critical	500	718	Windows 11	High	58	814	115	1
edr-wn-2516.demo.tanium.local	Critical	500	718	Windows 11	High	58	814	115	1
edr-wn-2513.demo.tanium.local	Critical	500	704	Windows 10	High	58	814	115	1
edr-wn-2514.demo.tanium.local	Critical	500	702	Windows 10	High	58	814	115	2
prf-wn-413.demo.tanium.local	Critical	500	499	Windows 10	High	54	814	115	1
inv-wn-2303.demo.tanium.local	Critical	500	499	Windows 11	High	51	814	115	1

The following are the top 10 AD groups that might have members with unintended administrative access as a byproduct of group membership. Review user account membership in these groups and reduce the number of members to decrease the overall risk that these groups and their members represent.

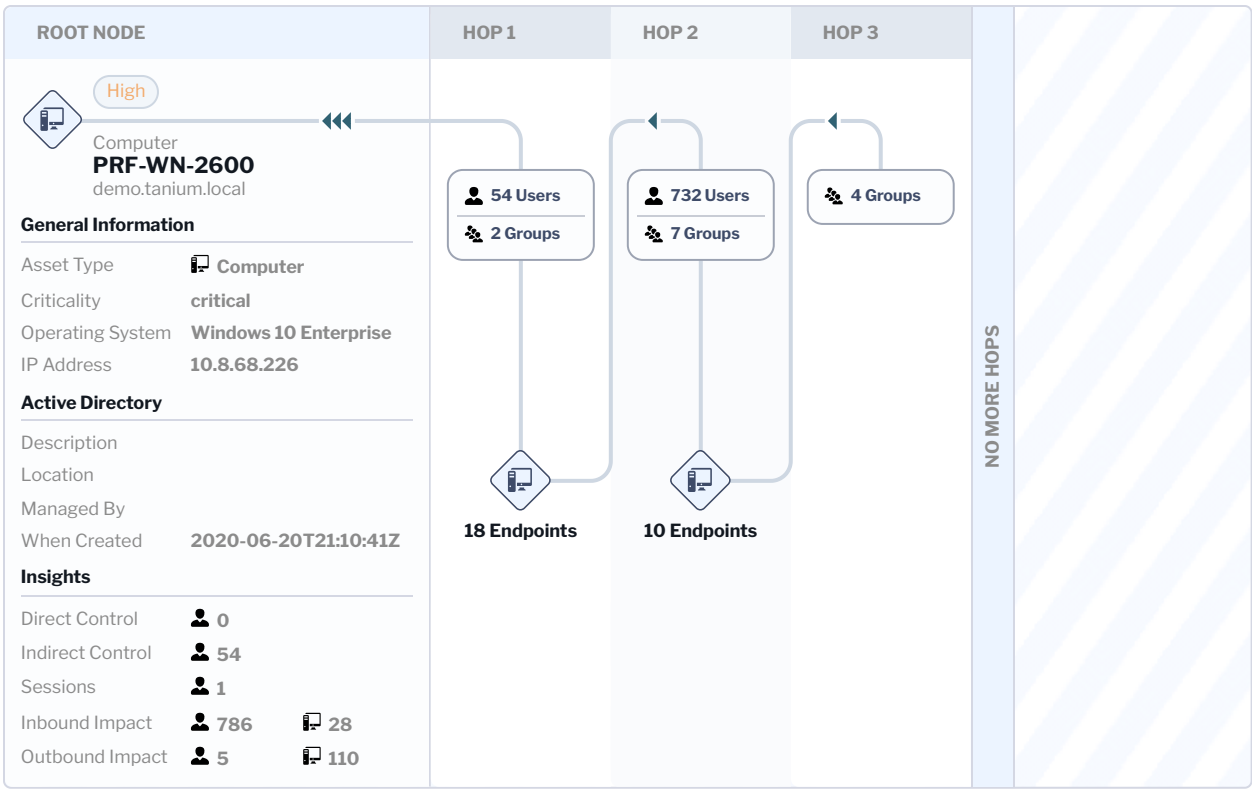
Group Name	Group Criticality	Domain Name	Impact Rating	Direct Members	Indirect Members	Direct Control	Indirect Control
Domain Admins	critical	demo.tanium.local	High	49	0	111	0
Domain Users	low	demo.tanium.local	High	786	0	1	13
Performance Admins	low	demo.tanium.local	High	6	0	7	0
EDR Admins	high	demo.tanium.local	High	9	0	12	0
Threat Response Admins	low	demo.tanium.local	High	5	5	12	0
Impact Admins	low	demo.tanium.local	High	2	784	13	0
Investigate Admins	low	demo.tanium.local	High	3	0	5	0

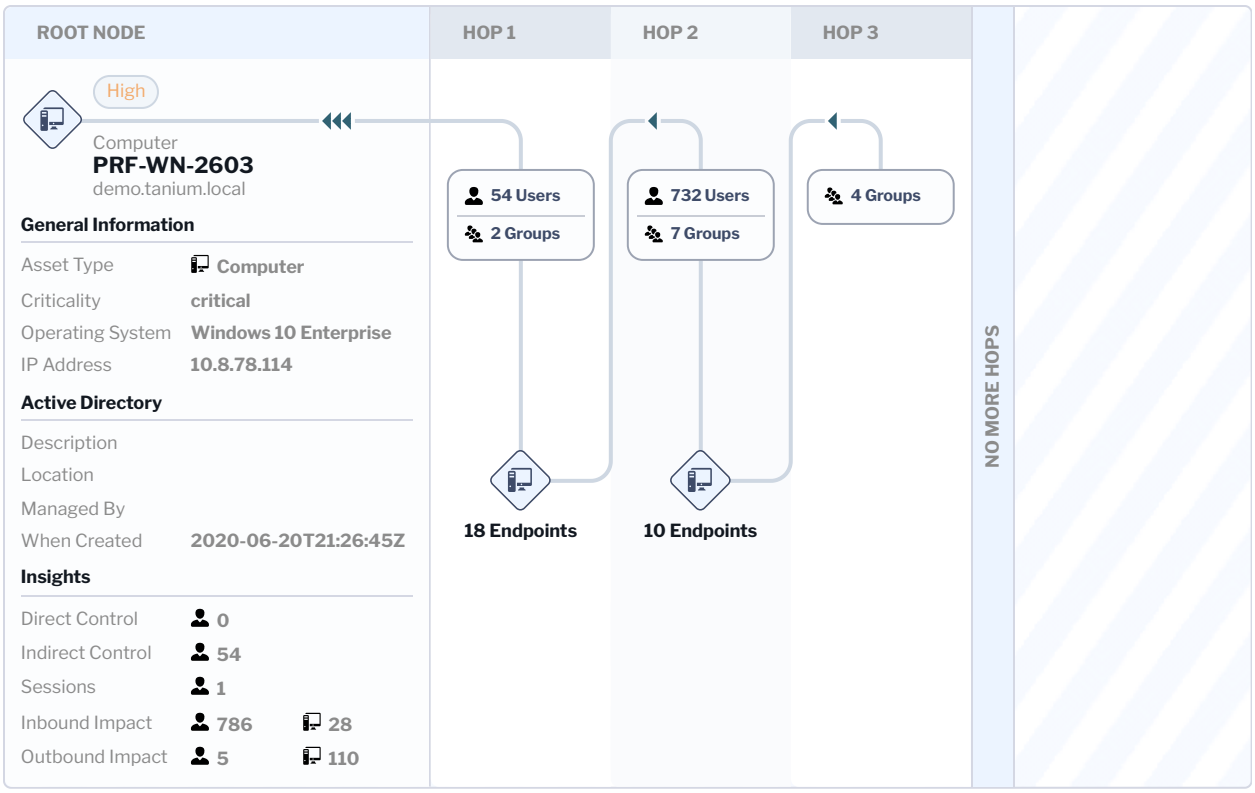
Group Name	Group Criticality	Domain Name	Impact Rating	Direct Members	Indirect Members	Direct Control	Indirect Control
Special Distribution Group	low	demo.tanium.local	High	0	786	0	13
Cert Publishers	low	demo.tanium.local	High	5	0	1	0
Northeast Impact Admins	low	demo.tanium.local	Medium	0	5	10	0

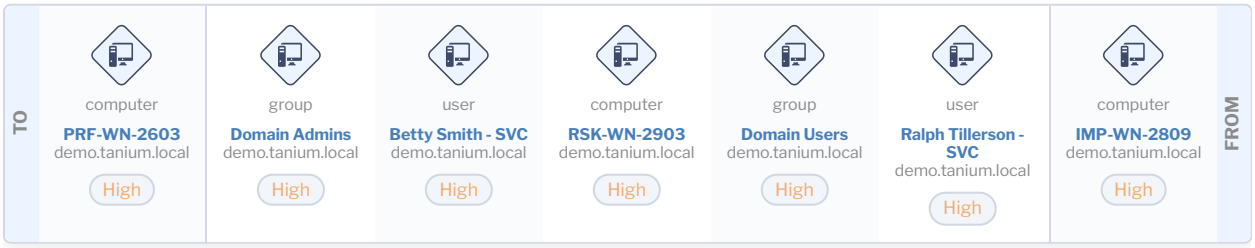
The following are the top 10 AD user accounts that potentially provide attackers with the greatest levels of access to enterprise endpoints. Limit administrative access and implement a least-privilege administrative model to reduce the risk for these accounts.

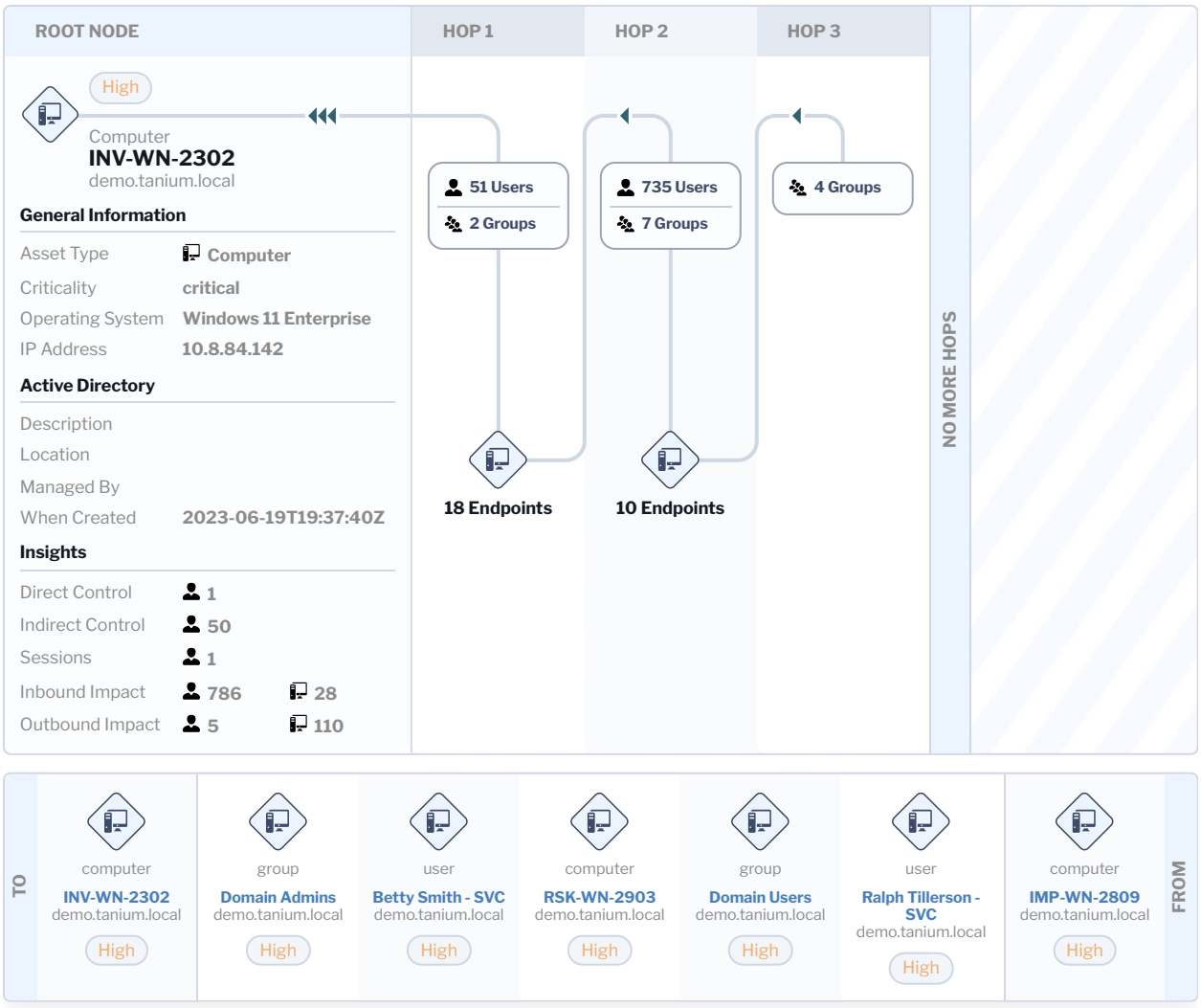
User Name	User Criticality	Domain Name	Impact Rating	Direct Control	Indirect Control
Betty Smith - SVC	critical	demo.tanium.local	High	0	111
James Madison	low	demo.tanium.local	High	2	24
Ralph Tillerson - SVC	low	demo.tanium.local	High	0	14
Ed Masters - SVC	high	demo.tanium.local	High	1	25
Jon Morgan	critical	demo.tanium.local	High	0	111
Wednesday Adams	critical	demo.tanium.local	Medium	32	79
Jimmy Halberd	low	demo.tanium.local	Medium	4	17
Rico Cruz	critical	demo.tanium.local	Medium	0	14
hArmando Espiron	low	demo.tanium.local	Medium	0	25
Mika Yun	low	demo.tanium.local	Medium	0	18

The following example illustrates what Tanium could accomplish given the opportunity to check for classical lateral movement going from a simple endpoint asset to a high value target, VIP targeting with public/reputation threat on known figures, and production disturbance and damage on critical industrial endpoints:


ROOT NODE
HOP 1
HOP 2
HOP 3
High
Computer
PRF-WN-2600
demo.tanium.local
General Information
Asset Type
Computer
Criticality
critical
Operating System
Windows 10 Enterprise
IP Address
10.8.68.226
Active Directory
Description
Location
Managed By
When Created
2020-06-20T21:10:41Z
Insights
Direct Control
0
Indirect Control
54
Sessions
1
Inbound Impact
786
28
Outbound Impact
5
110
54 Users
2 Groups
18 Endpoints
732 Users
7 Groups
10 Endpoints
4 Groups
NO MORE HOPS
TO
computer
PRF-WN-2600
demo.tanium.local
High
group
Domain Admins
demo.tanium.local
High
user
Betty Smith - SVC
demo.tanium.local
High
computer
RSK-WN-2903
demo.tanium.local
High
group
Domain Users
demo.tanium.local
High
user
Ralph Tillerson - SVC
demo.tanium.local
High
computer
IMP-WN-2809
demo.tanium.local
High
FROM


ROOT NODE
HOP 1
HOP 2
HOP 3
High
Computer
PRF-WN-2603
demo.tanium.local
General Information
Asset Type
Computer
Criticality
critical
Operating System
Windows 10 Enterprise
IP Address
10.8.78.114
Active Directory
Description
Location
Managed By
When Created
2020-06-20T21:26:45Z
Insights
Direct Control
0
Indirect Control
54
Sessions
1
Inbound Impact
786
28
Outbound Impact
5
110
54 Users
2 Groups
18 Endpoints
732 Users
7 Groups
10 Endpoints
4 Groups
NO MORE HOPS


TO
computer
PRF-WN-2603
demo.tanium.local
High
group
Domain Admins
demo.tanium.local
High
user
Betty Smith - SVC
demo.tanium.local
High
computer
RSK-WN-2903
demo.tanium.local
High
group
Domain Users
demo.tanium.local
High
user
Ralph Tillerson - SVC
demo.tanium.local
High
computer
IMP-WN-2809
demo.tanium.local
High
FROM

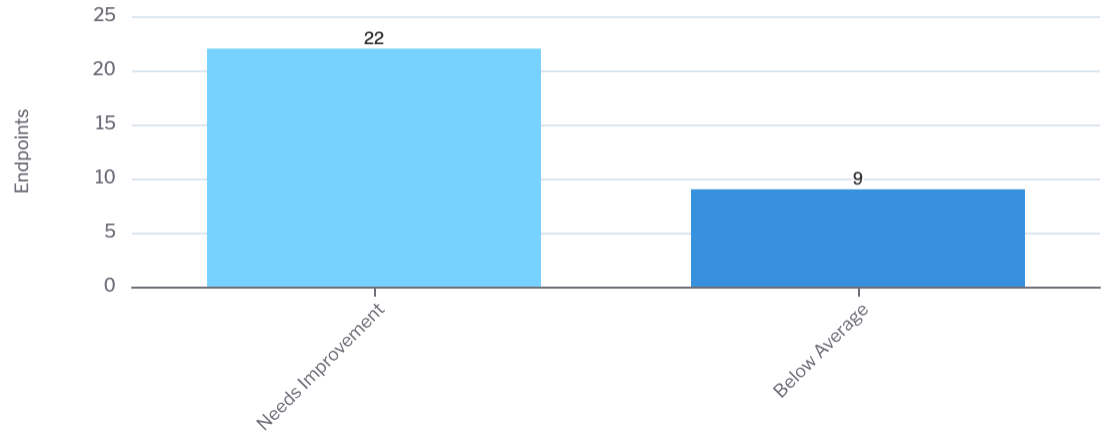


System Compliance

Industry regulatory requirements (such as PCI, HIPAA, and SOX) require organizations to harden endpoint configurations and adhere to corporate mandates based on industry-specific and security best practices benchmarks (for example, CIS, ISO27001, CMMC, or NIST). This risk metric considers gaps in compliance assessment coverage, which could lead to increased exposure to vulnerabilities. System compliance is included as part of the Tanium risk score.

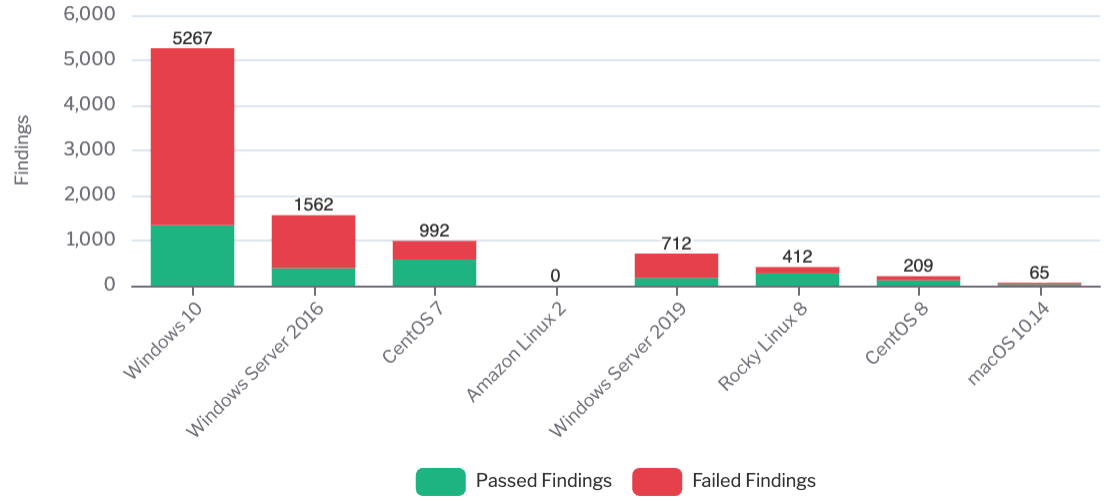
Compliance Exposures

Number of endpoints in each compliance exposure category



Top 10 Operating System Versions with the Most Compliance Findings

Top 10 operating system versions with the most passed and failed compliance findings



During the assessment, the following system compliance observations were made:

- A total of 3496 CIS standard benchmark rules were assessed across 31 endpoints.
- A total of 6322 failed conditions (out of 9219 findings) were identified.

A critical component of successfully remediating risk factors is the ability to prioritize the action needed to take place as part of the remediation plan. The following are the top 10 endpoints with the highest Compliance Failures risk metric scores. Ensure that these endpoints conform to your organizational security policy to reduce risk and lower the likelihood of successful compromise.

Note: Endpoint criticality is discussed in part 1

Endpoint Name	Endpoint Criticality	Compliance Failures Risk Metric Score	Risk Score	Operating System	Total Failures
rsk-wn-2900.demo.tanium.local	Critical	772	666	Windows 10	475
rsk-wn-2901.demo.tanium.local	Critical	770	566	Windows 10	474

Endpoint Name	Endpoint Criticality	Compliance Failures Risk Metric Score	Risk Score	Operating System	Total Failures
cmp-wn-2102.demo.tanium.local	Critical	760	664	Windows Server 2016	185
rsk-wn-2903.demo.tanium.local	Critical	758	826	Windows Server 2019	270
rsk-wn-2902.demo.tanium.local	Critical	754	662	Windows Server 2019	269
cmp-wn-2106.demo.tanium.local	Critical	744	560	Windows 10	554
cmp-wn-2108.demo.tanium.local	Critical	744	560	Windows 10	554
cmp-wn-2105.demo.tanium.local	Critical	744	560	Windows 10	554
cmp-wn-2107.demo.tanium.local	Critical	744	560	Windows 10	554
cmp-wn-2109.demo.tanium.local	Critical	744	560	Windows 10	554

Insecure Transport Security Protocols

Using insecure and outdated transport layer security protocols (like SSLv3 and TLSv1) to secure communications and network traffic is a security weakness that could leave data and session IDs exposed and vulnerable to exploits. This risk metric considers endpoints currently using insecure transport protocols that could put the confidentiality and integrity of communications at risk. Insecure transport security protocols are used as part of creating the Tanium risk score.

A critical component of successfully remediating risk factors is the ability to prioritize the action needed to take place as part of the remediation plan. The following are the top 10 endpoints with the highest Insecure TLS/SSL risk metric scores. The endpoints use insecure and outdated transport layer security protocols (for example, SSLv3 and TLSv1) to secure communications. Update the transport layer security protocols in use on these endpoints to ensure the confidentiality and integrity of these communications and lower the overall risk for these endpoints.

Note: Endpoint criticality is discussed in part 1

Endpoint Name	Endpoint Criticality	Insecure TLS/SSL Risk Metric Score	Risk Score	Operating System	Detected Protocols	TCP Ports
rsk-lx-2904.demo.tanium.local	Critical	1000	855	CentOS 7	SSL 3.0 TLS 1.0 TLS 1.1	443 443 443
rsk-wn-2903.demo.tanium.local	Critical	1000	826	Windows Server 2019	TLS 1.0 TLS 1.1 TLS 1.1 TLS 1.0 TLS 1.0 TLS 1.1 TLS 1.1 TLS 1.0 TLS 1.1 TLS 1.0 TLS 1.0 TLS 1.1	8446 8446 443 443 8445 8445 8444 8444 8443 8443 3389 3389
demo-ras-satellite.demo.tanium.local	Critical	1000	816	CentOS 8	TLS 1.0 TLS 1.1	631 631
edr-wn-2519.demo.tanium.local	Critical	1000	718	Windows 11	TLS 1.0 TLS 1.1 TLS 1.0 TLS 1.1	3389 3389 5986 5986

Endpoint Name	Endpoint Criticality	Insecure TLS/SSL Risk Metric Score	Risk Score	Operating System	Detected Protocols	TCP Ports
edr-wn-2517.demo.tanium.local	Critical	1000	718	Windows 11	TLS 1.0 TLS 1.1 TLS 1.0 TLS 1.1	5986 5986 3389 3389
edr-wn-2510.demo.tanium.local	Critical	1000	718	Windows Server 2022	TLS 1.0 TLS 1.1 TLS 1.0 TLS 1.1	5986 5986 3389 3389
edr-wn-2518.demo.tanium.local	Critical	1000	718	Windows 11	TLS 1.0 TLS 1.1 TLS 1.0 TLS 1.1	5986 5986 3389 3389
edr-wn-2516.demo.tanium.local	Critical	1000	718	Windows 11	TLS 1.0 TLS 1.1 TLS 1.0 TLS 1.1	3389 3389 5986 5986
edr-wn-2513.demo.tanium.local	Critical	1000	704	Windows 10	TLS 1.0 TLS 1.1 TLS 1.0 TLS 1.1	3389 3389 5986 5986
edr-wn-2514.demo.tanium.local	Critical	1000	702	Windows 10	TLS 1.0 TLS 1.1 TLS 1.0 TLS 1.1	5986 5986 3389 3389

Encryption and Mutual Authentication

SSL certificates provide authentication validation to your domains and are critical for ensuring proper encryption and identity verification. Expired SSL/TLS certificates could lead to severe security risks, service outages, and impact on revenue and could expose you to various attacks and viruses. This risk metric takes into account expired SSL/TLS certificates across the endpoints. Encryption and mutual authentication status are included as part of the Tanium risk score.

A critical component of successfully remediating risk factors is the ability to prioritize the action needed to take place as part of the remediation plan. The following are the top 6 endpoints with the Expired Certificates risk metric scores. Renew the certificates on these endpoints to ensure that certificate revocation information is available and prevent the use of insecure certificates.

Note: Endpoint criticality is discussed in part 1

Endpoint Name	Endpoint Criticality	Expired Certificates Risk Metric Score	Risk Score	Operating System	Protocol	Expired Certificates	TCP Ports
rsk-lx-2904.demo.tanium.local	Critical	1000	855	CentOS 7	SSL 3.0 TLS 1.0 TLS 1.1 TLS 1.2	4	443 443 443 443
rsk-wn-2903.demo.tanium.local	Critical	1000	826	Windows Server 2019	TLS 1.2 TLS 1.1 TLS 1.0 TLS 1.2 TLS 1.1 TLS 1.0 TLS 1.2	9	443 443 443 8444 8444 8444 8443

Endpoint Name	Endpoint Criticality	Expired Certificates Risk Metric Score	Risk Score	Operating System	Protocol	Expired Certificates	TCP Ports
					TLS 1.1 TLS 1.0		8443 8443
rsk-lx-2905.demo.tanium.local	Critical	1000	713	CentOS 8	TLS 1.2	1	443
rsk-lx-2906.demo.tanium.local	Critical	1000	691	Rocky Linux 8	TLS 1.3 TLS 1.2	2	443 443
rsk-wn-2902.demo.tanium.local	Critical	1000	662	Windows Server 2019	TLS 1.2	1	8443
prv-wn-1300.demo.tanium.local	High	835	485	Windows 11	TLS 1.2 TLS 1.2	2	8100 17530

Part 3: Security and Operations Metrics

This section of the report provides the values for the tested metrics across environment endpoints and how each metric in the environment compares to other organizations in the same industry by displaying the environment's values for the metric and the median value across Tanium customers in the same targeted industry as the tested environment.

For each metric identified in the report, the table includes the following information:

- Name: The name of the metric.
- Description: A brief description of the metric.
- Industry Ranking: In your defined industry, the percentage of Tanium customer environments that you are better than or equal to.
- Your Value: The value for each metric identified in the environment for the targeted endpoints.
- Industry Median Value: The median value for the targeted organizational industry.

Customer Industry

For the purposes of this report and the metrics reported in this section, the defined industry for the targeted environment is currently set as **Business Services**. The metrics reported in these sections show the actual values identified in the report environment and how the environment compares to other Tanium customer environments within the same defined industry.

Security Metrics

The following section details the state of several security metrics in the tested environment and how the organization compares to industry peers for each metric. While these metrics are not used as part of generating the Tanium risk score, they provide vital information about the state of the environment, its security hygiene, and whether or not security controls are in place.

Name	Description	Industry Ranking	Your Value	Industry Median Value
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.	84th	6.97 alerts	89.17 alerts
Firewall Disabled	The percentage of endpoints in the environment that have a disabled firewall.	4th	88.68%	13.66%
Impact Rating of Machines with Alerts	The average impact rating of endpoints with threat alerts.	17th	1.81 impact rating	1 impact rating
LSA Protection Disabled (LSASS as PPL)	The percentage of endpoints in the environment that have LSA Protection (LSASS as PPL) disabled.	19th	91.23%	64.16%
Missing Disk Encryption	The percentage of endpoints in the environment that are missing disk encryption.	38th	50.43%	33.29%
Passwords Found	The percentage of endpoints that have confirmed plain-text passwords, which could allow unauthorized access to critical assets and applications. Attackers often locate plain-text passwords and use them to expand access and privileges. Encrypt stored passwords to prevent unauthorized access.	50th	75%	78.79%
Remote UAC Local Account Token Filter Disabled	The percentage of endpoints in the environment that have Remote UAC Local Account Token Filter disabled.	100th	0%	3.18%
Secure Powershell Execution Policy Not	The percentage of endpoints with Secure Powershell Execution Policy not enforced.	71st	8.77%	16.23%

Name	Description	Industry Ranking	Your Value	Industry Median Value
Enforced				
Secure Removable Storage Policy Not Applied	The percentage of endpoints in the environment that do not have a secure removable storage policy applied.	0th	100%	72.68%
User Account Control Disabled	The percentage of endpoints in the environment that have User Account Control disabled.	48th	4.39%	4.3%
Windows Credential Guard Disabled	The percentage of endpoints in the environment that have Windows Credential Guard disabled.	0th	100%	81.28%
Windows Data Execution Prevention (DEP) Disabled	The percentage of endpoints in the environment that do have Windows Data Execution Prevention disabled.	100th	0%	0.27%
Windows Defender Disabled	The percentage of endpoints in the environment that have Windows Defender disabled.	43rd	0.88%	0.62%
Windows Defender Out of Date	The percentage of endpoints in the environment that have Windows Defender out of date.	64th	2.65%	25.88%
Windows Trusted Platform Module (TPM) Not Enabled	The percentage of endpoints in the environment that do not have Windows Trusted Platform Module (TPM) enabled.	100th	0%	0.69%
Windows Workstation Antivirus Disabled	The percentage of windows workstations with antivirus disabled.	8th	3.7%	0.17%
Windows Workstation Antivirus Out of Date	The percentage of windows workstations with out of date antivirus.	100th	0%	0.53%

Operations Metrics

The following section details the state of several operations metrics in the tested environment and how the organization compares to industry peers for each metric. While these metrics are not used as part of generating the Tanium risk score, they provide vital information about the state of the environment, its operational IT hygiene, and whether or not critical systems are healthy.

Name	Description	Industry Ranking	Your Value	Industry Median Value
Domain Membership	The percentage of windows endpoints not joined to a domain.	78th	0.88%	6.69%
High CPU Consumption	The percentage of endpoints with over 95% cpu consumption.	20th	2.55%	0.53%
High Disk Consumption	The percentage of endpoints with less than 5% disk space available.	96th	0.38%	3.34%
High Memory Consumption	The percentage of endpoints with less than 5% system memory available.	83rd	0.15%	0.91%
High Server Uptime	The percentage of servers that have been up more than 30 days.	90th	7.5%	34.46%
High Workstation Uptime	The percentage of workstations that have been up more than 30 days.	1st	92.77%	38.6%
Mean Time to Patch	The average number of days to patch endpoints following the availability of a patch.	35th	29.42 days	19.26 days

Name	Description	Industry Ranking	Your Value	Industry Median Value
Mean Time to Update	The average number of days to deploy software updates to endpoints following the availability of an update.	26th	6.28 days	4.1 days
Patch Compliance	The percentage of endpoints that have been updated with critical or important patches that became available within the last 30 days. Note: A higher value is better.	12th	30.91%	77.07%
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.	99th	8.71%	95.81%

Part 4: Guardian Metrics Risk Exposure Analysis

The following section details the state of specific metrics reported to Tanium customers by the Guardian research and analysis team and how the organization compares to industry peers for each metric. Although these metrics are not used as part of the Tanium risk score, they provide vital information about the state of the environment for security and operations issues. Customers typically focus significant remediation effort on these issues because of their severity and potential impact.

Name	Description	Industry Ranking	Your Value	Industry Median Value
Broken 3rd Party Use of Windows Update Agent	The percentage of endpoints in the environment that have a broken Windows Update Agent.	90th	0.02%	0.12%
SSH Authorized Keys without a Passphrase	The percentage of endpoints in the environment that have SSH authorized keys without a passphrase.	47th	56.43%	54.99%

Part 5: Additional Risk and Cyber Hygiene Metrics

Ransomware incidents are on the rise and pervasive in both public and private sectors. No industry is exempt. Recently, the U.S. federal government urged agency and business leaders to protect themselves by implementing foundational cyber-hygiene best practices, noting that it is their critical responsibility to protect against threats with a strengthening of our nation's resilience against cyberattacks.

With ransomware a threat to core business operations, international security, and the global economy, Tanium wants to help organization achieve the highest degree of certainty when answering the following questions:

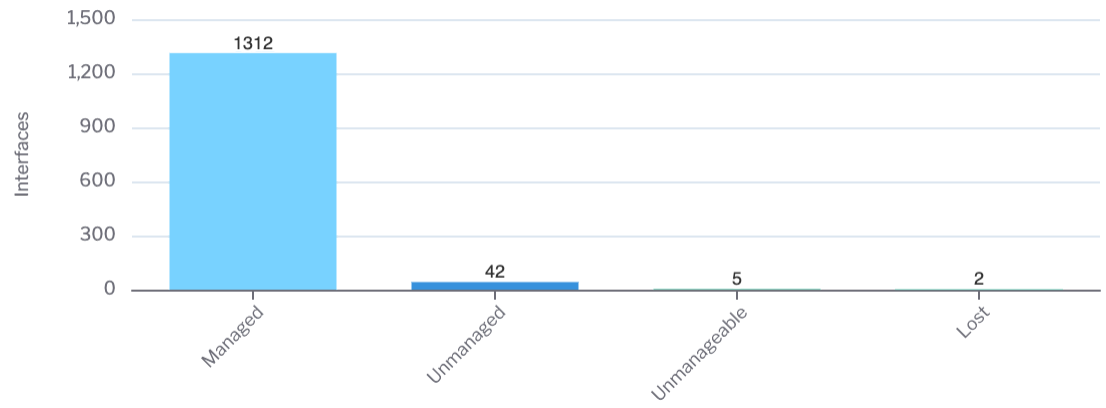
- How many endpoints do I have?
- Is every endpoint properly patched?
- What applications are running in my environment?
- Am I paying for software I am not using?
- What is my risk exposure to vulnerabilities?

Parts 1-4 of this assessment report focused on providing an objective quantification to Software Company's overall risk posture. This part will provide some high-level metrics around Software Company's overall Cyber Hygiene posture.

Endpoint Inventory Management

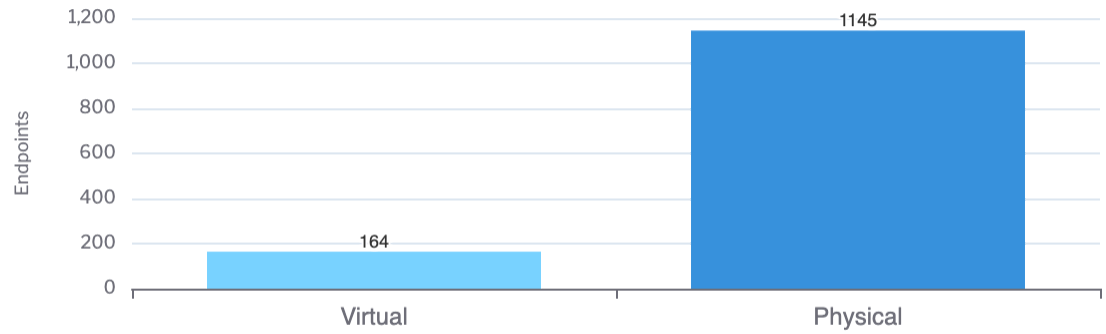
Interfaces Identified by Discover

Number of interfaces identified by Discover at the time of the report export. Lost interfaces are interfaces were previously managed.

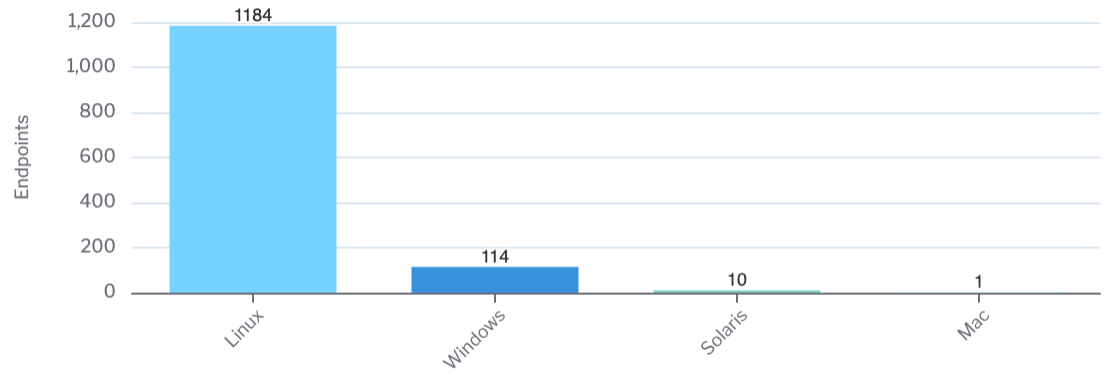


Physical and Virtual Endpoints

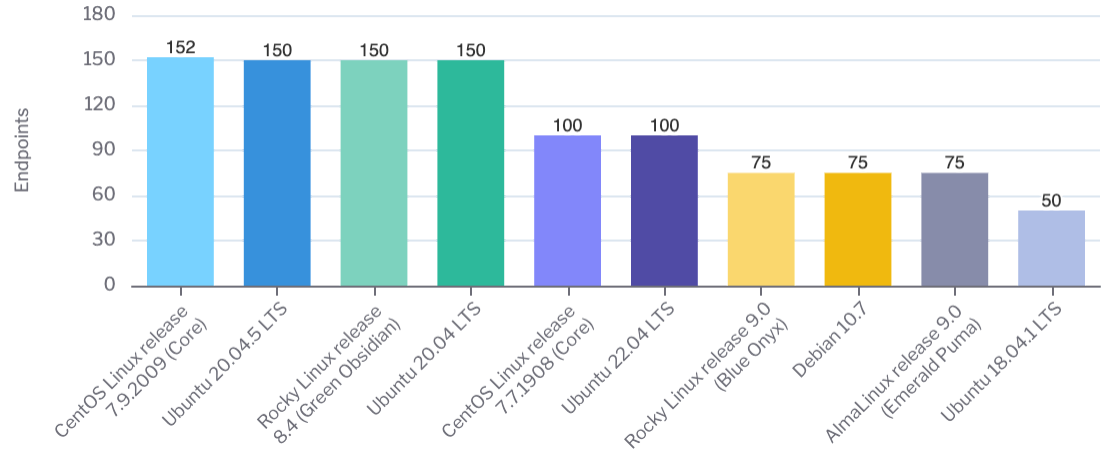
Number of physical and virtual endpoints in your environment



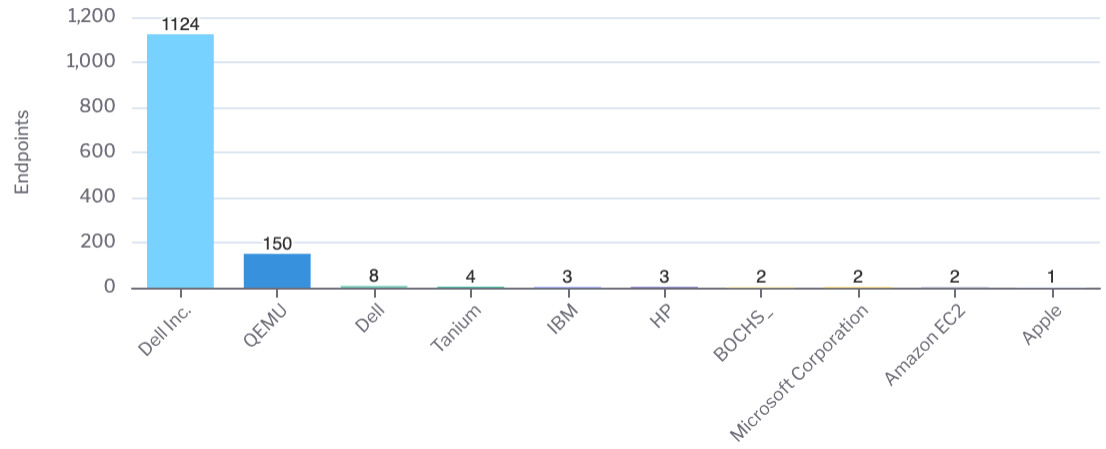
Top 10 Operating System Platforms



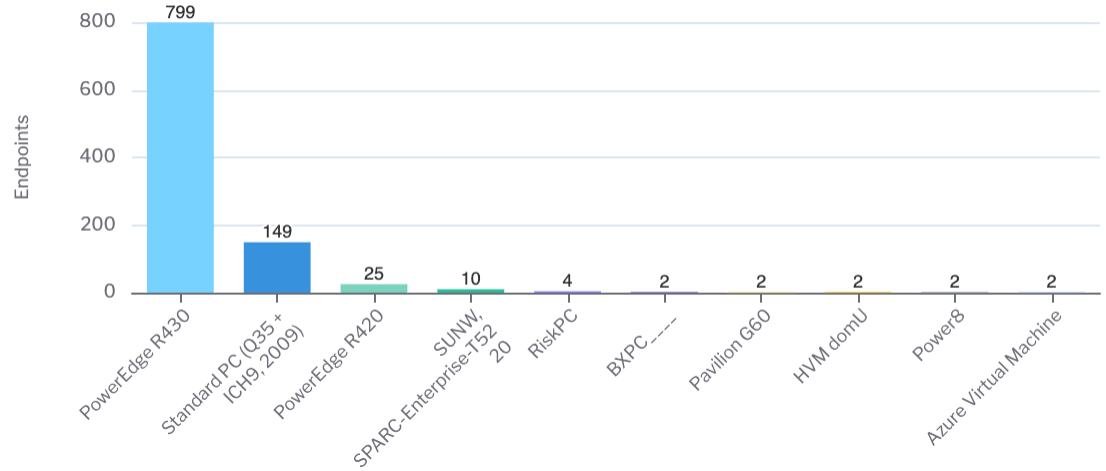
Top 10 Operating System Versions



Top 10 Hardware Manufacturers



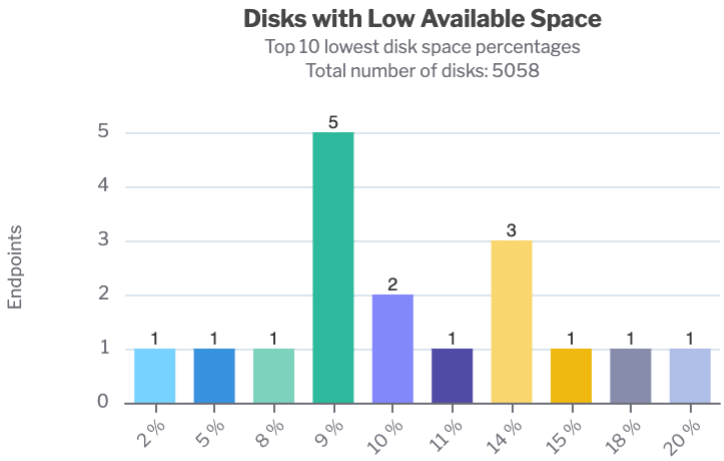
Top 10 Hardware Models



Endpoint Health Management

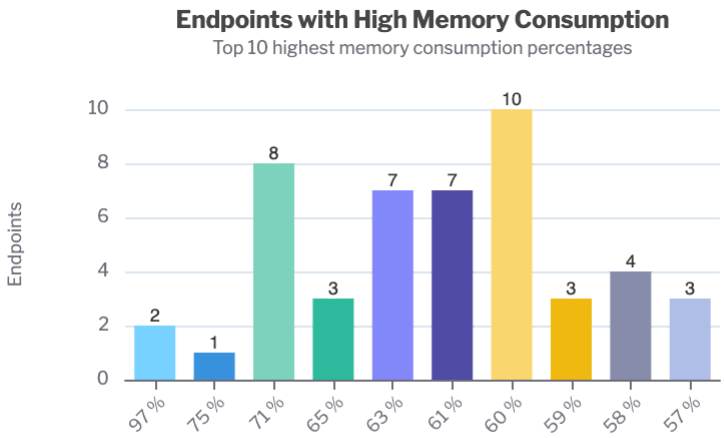
Endpoints with Low Disk Space (<=5%)

2



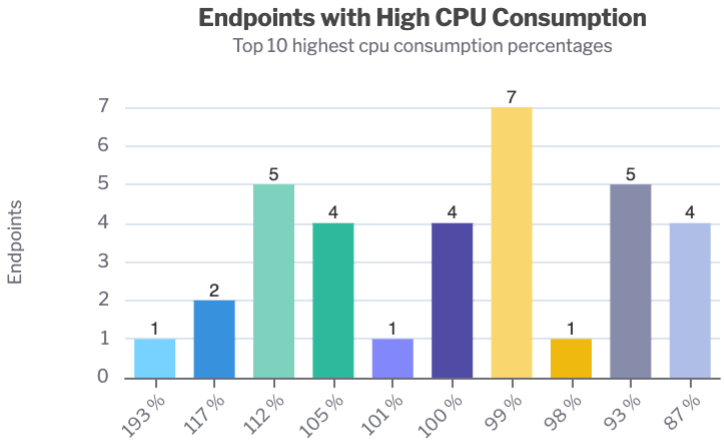
Endpoints with High Memory Consumption (>= 95%)

2



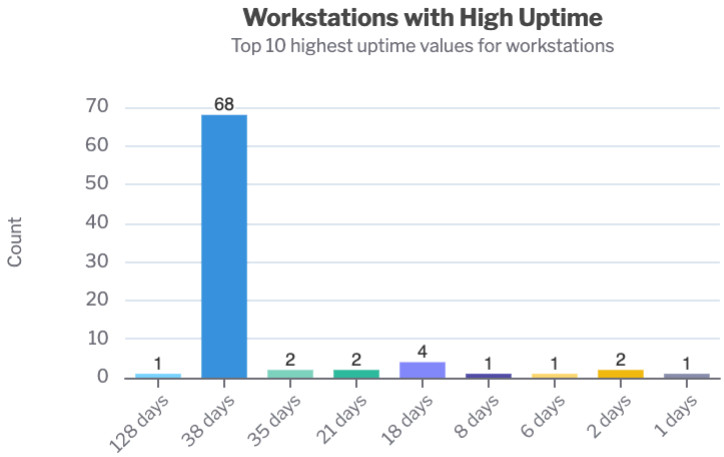
Endpoints with High CPU Consumption (>= 95%)

25



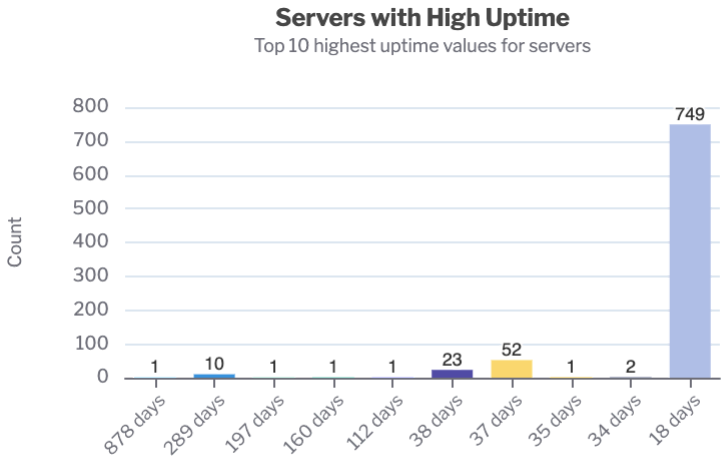
Workstations with High Uptime (>30 days)

71



Servers with High Uptime (>30 days)

92



Laptops with High Uptime (>30 days)

ⓘ *The chart "Laptops with High Uptime" did not contain any data.*

0

Endpoints that Require a Reboot

110

Workstations with >1 Logged In Users

1

Of the managed estate, Tanium has identified 1081 endpoints with EoL version of an operating system. The following table provides a partial report of those endpoints (up to 10 endpoints for each type of operating system).

Endpoint Name	Operating System	Logged In User	Lateral Movement Risk
inv-wn-2303.demo.tanium.local	Windows 11	Uninitialized - waiting for login	High
prf-wn-2613.demo.tanium.local	Windows 10	.\Tanium	High
inv-wn-2302.demo.tanium.local	Windows 11	Uninitialized - waiting for login	High
sys-x-wn2426.demo.tanium.local	Windows 11	DEMO\wednesday.adams	Medium
sys-x-wn2425.demo.tanium.local	Windows 11	DEMO\wednesday.adams	Medium
enf-wn-2703.demo.tanium.local	Windows 10	.\Admin	Medium
sys-x-wn2424.demo.tanium.local	Windows 11	DEMO\wednesday.adams	Medium
sys-x-wn2422.demo.tanium.local	Windows 11	DEMO\wednesday.adams	Medium
sccm-w10-5.demo.tanium.local	Windows 10	.\root	Medium
sys-x-wn2421.demo.tanium.local	Windows 11	DEMO\wednesday.adams	Medium

Endpoint Name	Operating System	Logged In User	Lateral Movement Risk
jfk-lxc-10021.demo.tanium.local	Ubuntu 20.04	root	N/A
den-lxc-2432.demo.tanium.local	Ubuntu 20.04	root	N/A
ord-lxc-1222.demo.tanium.local	CentOS 7	root	N/A
sfo-lxc-11504.demo.tanium.local	AlmaLinux 9	root	N/A
dfw-lxc-2319.demo.tanium.local	Ubuntu 20.04	root	N/A
lax-lxc-2118.demo.tanium.local	Ubuntu 18.04	wtmp	N/A
jfk-lxc-10713.demo.tanium.local	Debian 11	root	N/A
atl-lxc-2019.demo.tanium.local	Ubuntu 20.04	root	N/A
jfk-lxc-10025.demo.tanium.local	Ubuntu 20.04	root	N/A
sfo-lxc-11419.demo.tanium.local	Rocky Linux 9	root	N/A
pbj-mc-0002	macOS 10.14	taniumadmin	N/A

In addition, Tanium has identified 163 endpoints with uptime of more than 30 days (with the highest uptime value found of 878 days). The following table provides a partial report of those endpoints.

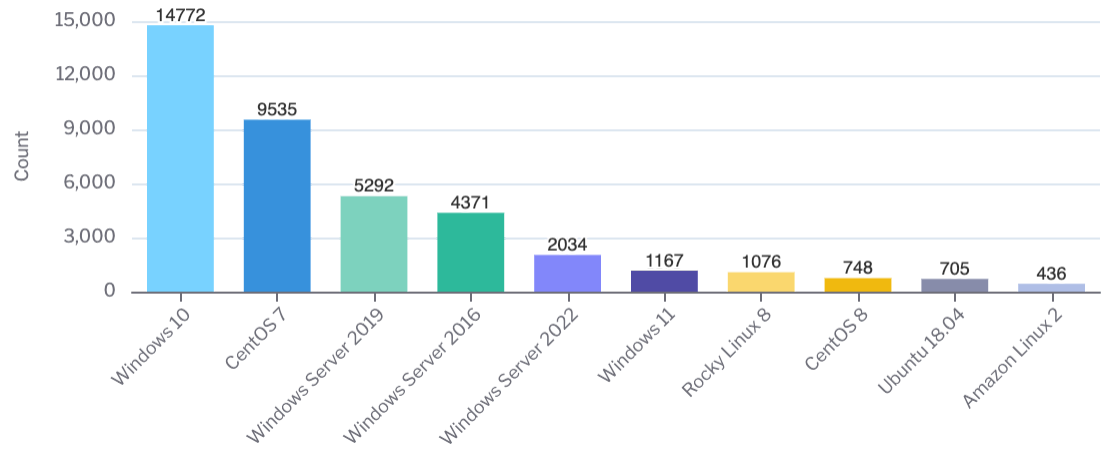
Endpoint Name	Operating System	Uptime	Lateral Movement Risk
az-lx-cl1.mayzlgflhznunhe0hfxg4dqs5b.xx.internal.cloudapp.net	CentOS 7	878 days	N/A
szd5	Solaris 11	289 days	N/A
szd9	Solaris 11	289 days	N/A
szd10	Solaris 11	289 days	N/A
szd8	Solaris 11	289 days	N/A
szd1	Solaris 11	289 days	N/A
szd2	Solaris 11	289 days	N/A
szd3	Solaris 11	289 days	N/A
szd7	Solaris 11	289 days	N/A
szd6	Solaris 11	289 days	N/A

Tanium has also identified 0 endpoints with hostname collisions, a situation that could lead to DNS hostname resolution failures and an inability to successfully register endpoints with an AD domain. The following table provides information about the impacted hostnames:

Host Name	Number of Endpoints with That Hostname
Table contains no results.	

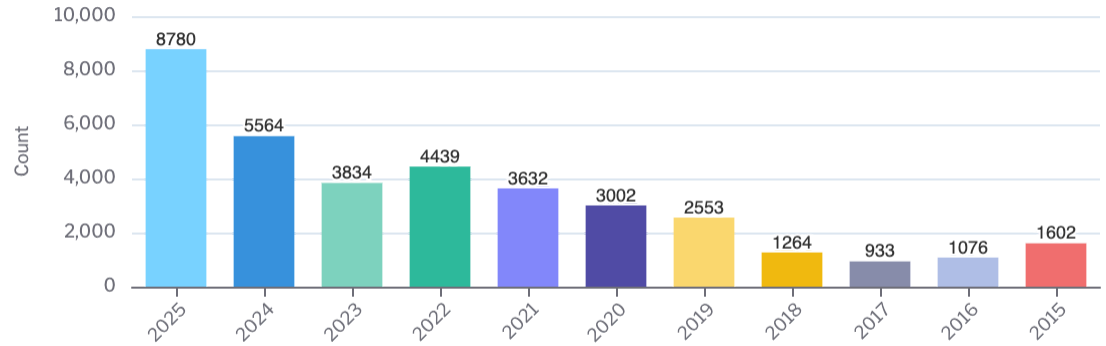
Vulnerability Management

Top 10 Operating System Versions with the Most Vulnerability Counts

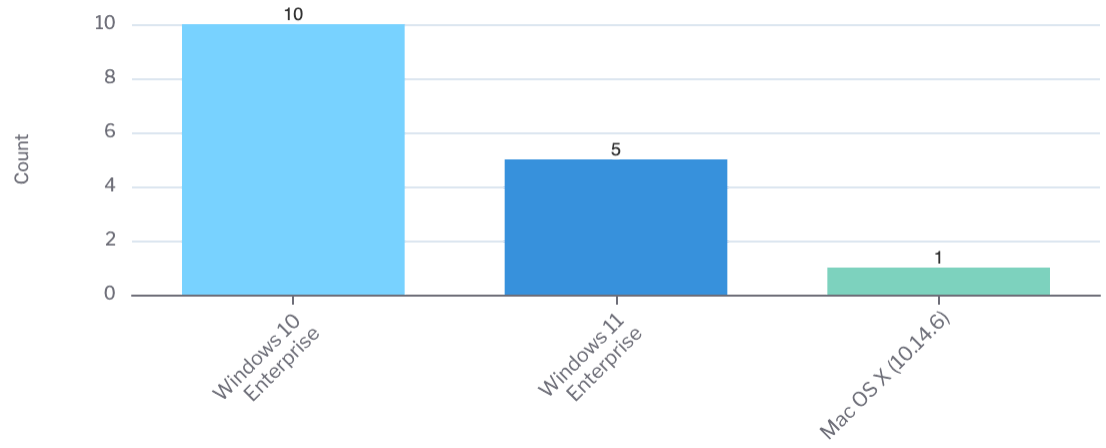


Vulnerability Counts over 10 Years

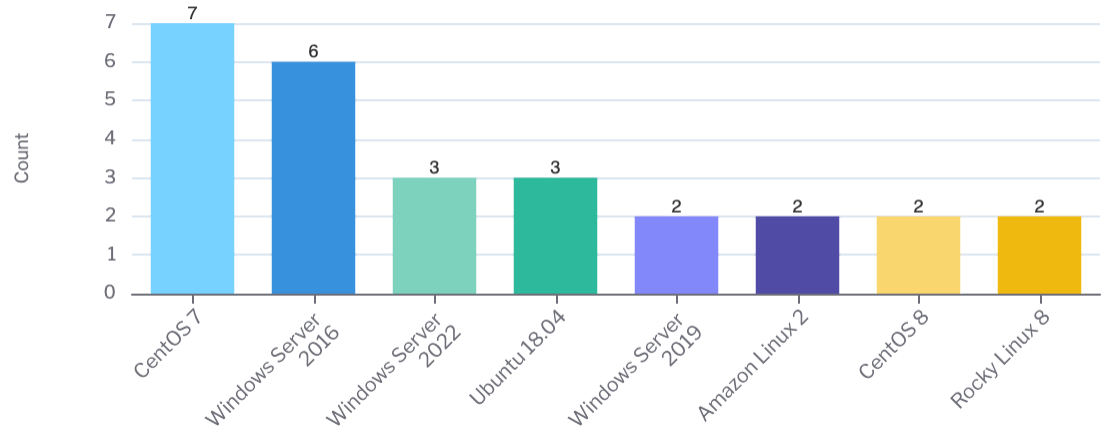
Over the last 10 years, the vulnerability counts for each year based on CVE release year



Top 10 Workstation Operating System Versions with the Most Vulnerability Counts

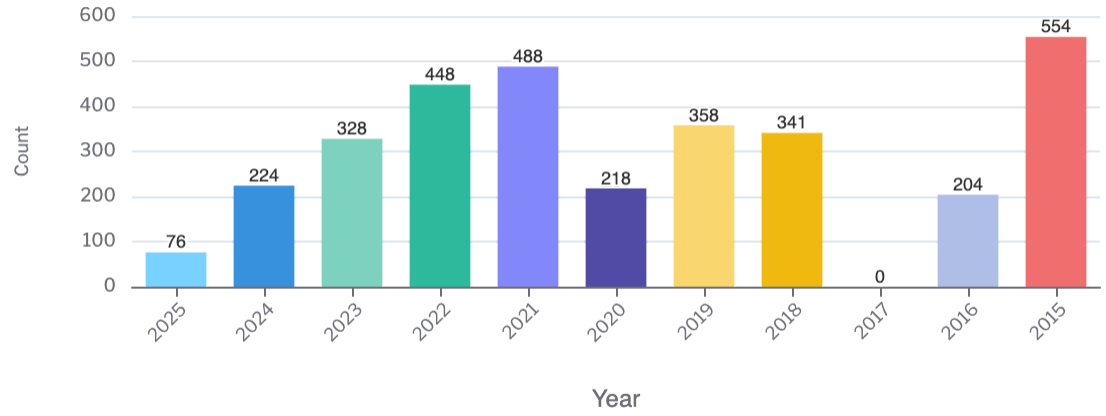


Top 10 Server Operating System Versions with the Most Vulnerability Counts



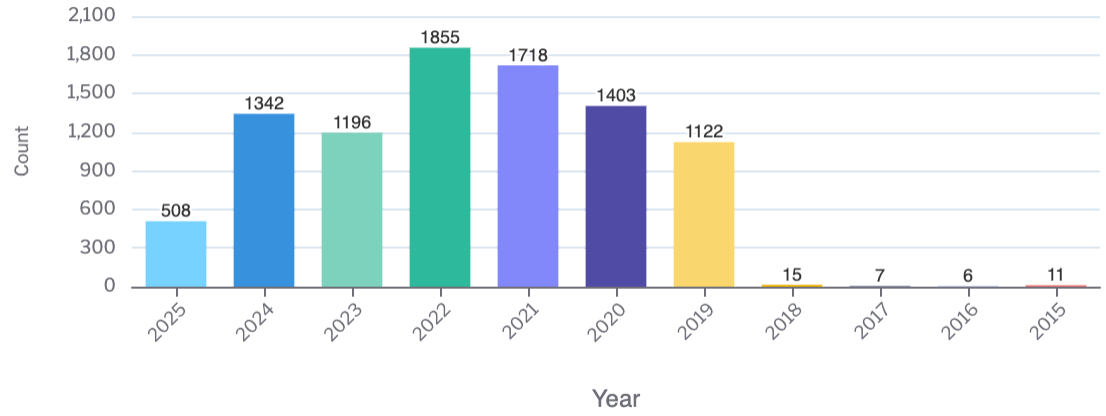
Adobe Vulnerability Counts over 10 Years

Over the last 10 years, the Adobe vulnerability counts for each year based on CVE release year



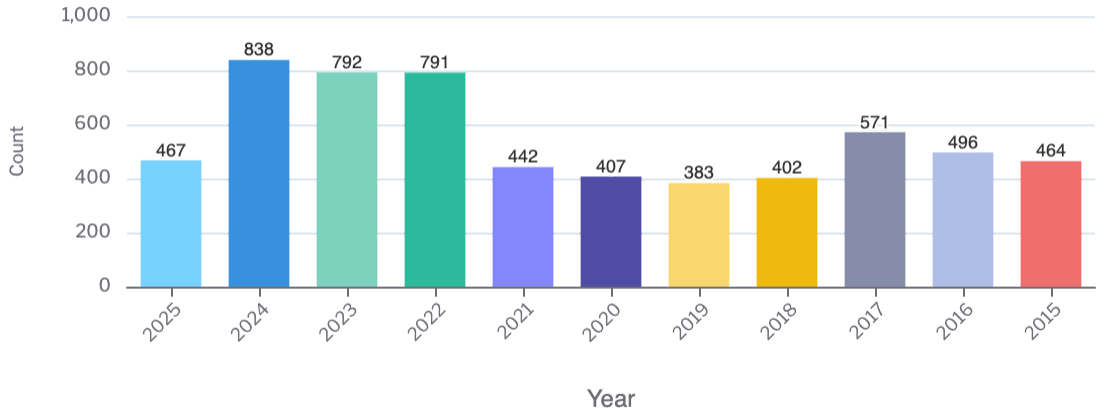
Chrome Vulnerability Counts over 10 Years

Over the last 10 years, the Chrome vulnerability counts for each year based on CVE release year



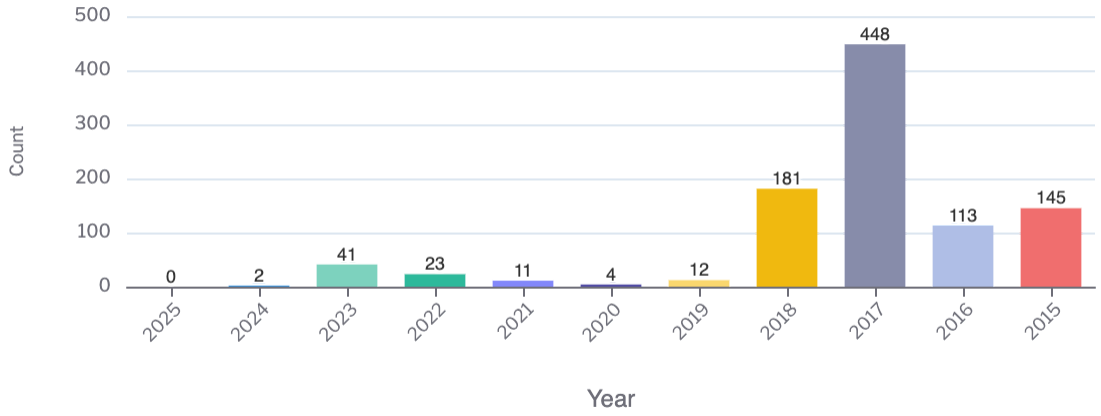
Firefox Vulnerability Counts over 10 Years

Over the last 10 years, the Firefox vulnerability counts for each year based on CVE release year



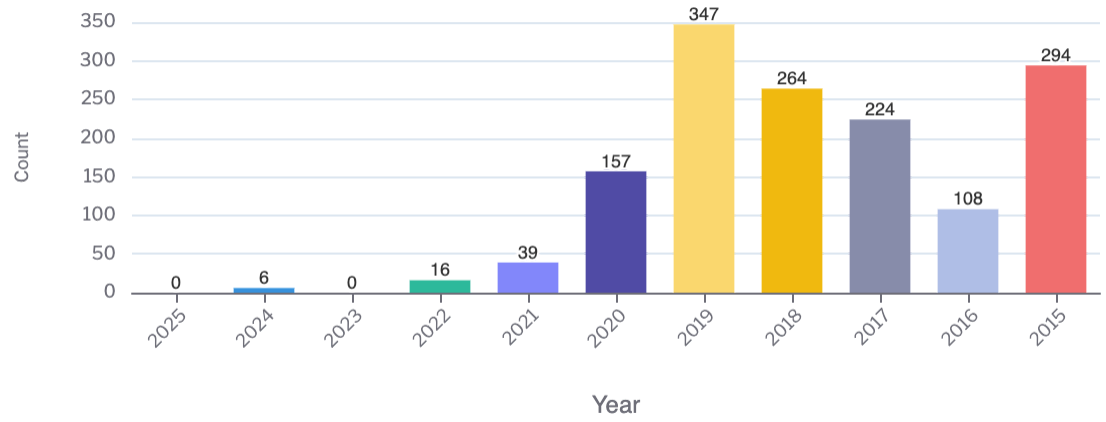
Java Vulnerability Counts over 10 Years

Over the last 10 years, the Java vulnerability counts for each year based on CVE release year



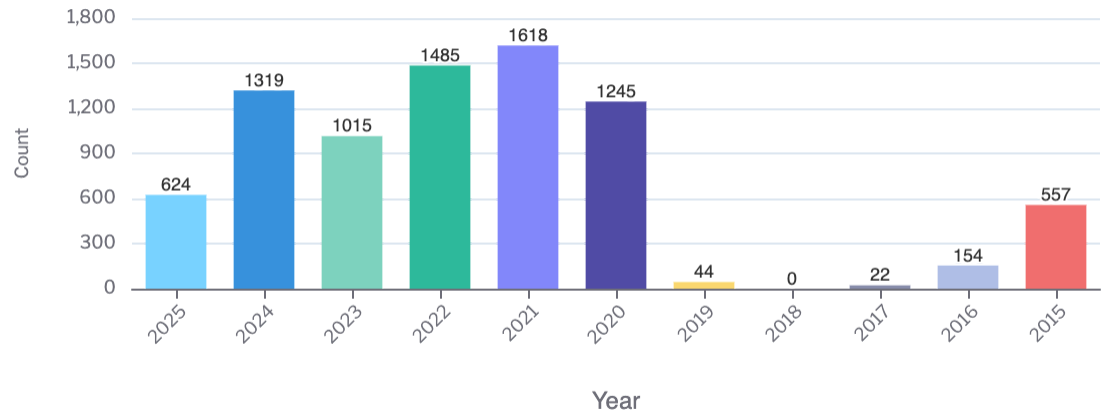
Safari Vulnerability Counts over 10 Years

Over the last 10 years, the Safari vulnerability counts for each year based on CVE release year



Microsoft Edge Vulnerability Counts over 10 Years

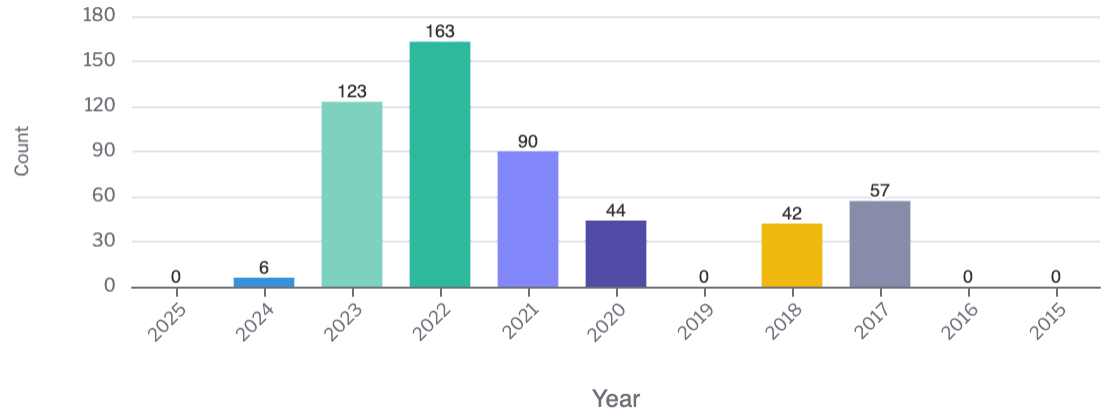
Over the last 10 years, the Microsoft Edge vulnerability counts for each year based on CVE release year



ⓘ *The chart "Microsoft Office Vulnerability Counts over 10 Years" did not contain any data.*

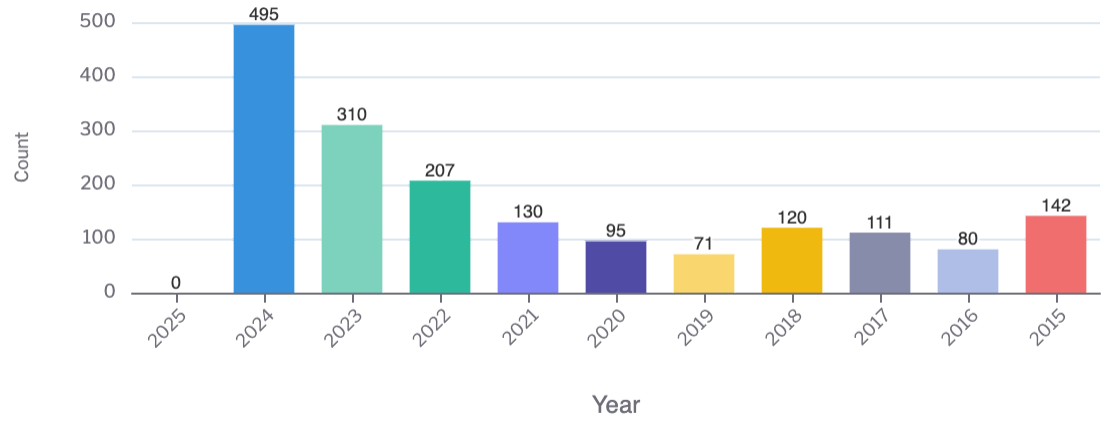
Apache Vulnerability Counts over 10 Years

Over the last 10 years, the Apache vulnerability counts for each year based on CVE release year

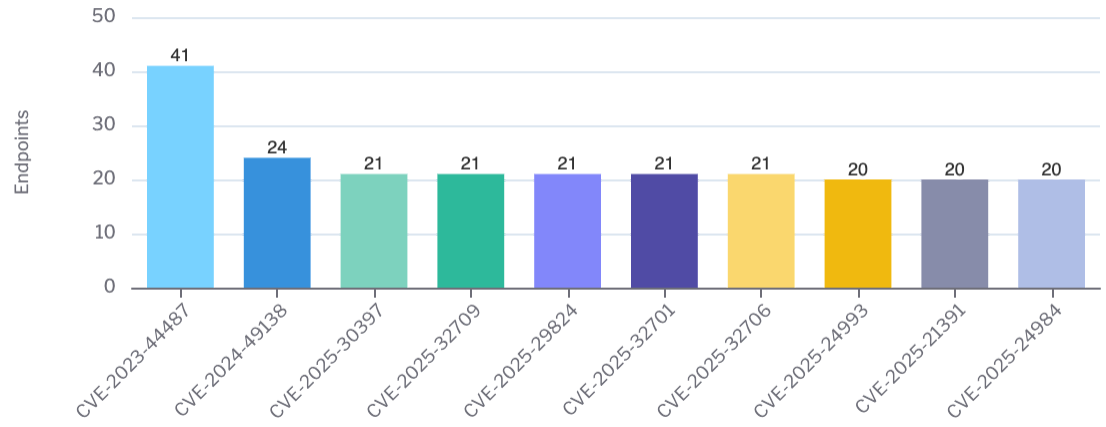


Oracle Vulnerability Counts over 10 Years

Over the last 10 years, the Oracle vulnerability counts for each year based on CVE release year



Top 10 CISA KEV Vulnerabilities by Endpoint



CISA KEV Vulnerabilities on Workstations

313

Number of Vulnerabilities

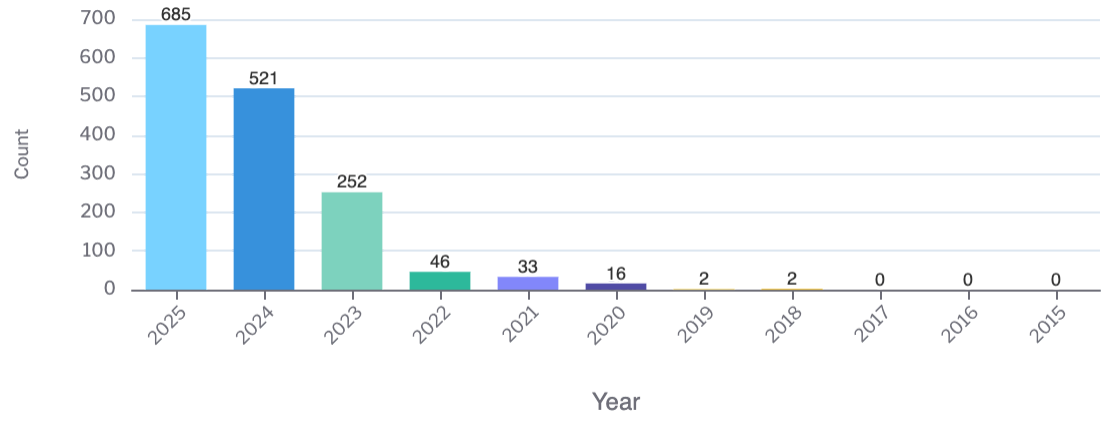
CISA KEV Vulnerabilities on Servers

556

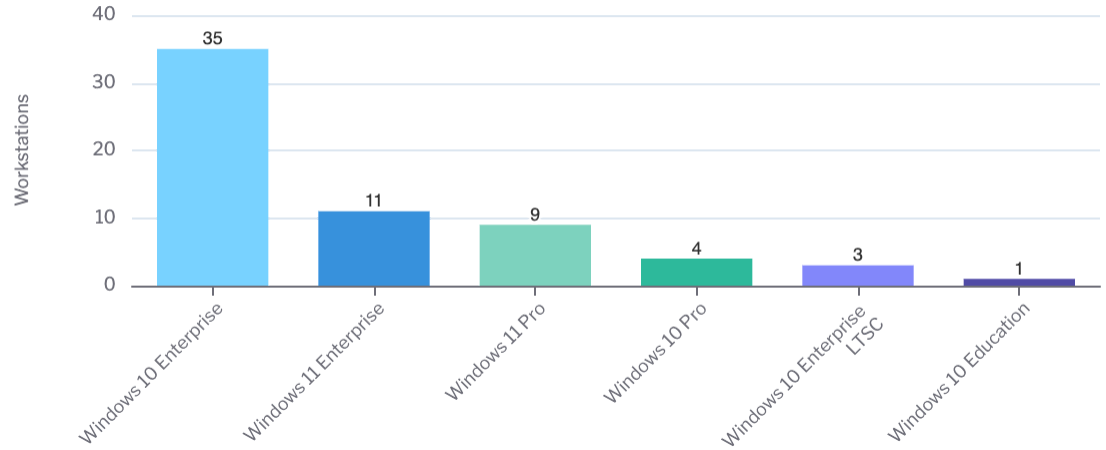
Number of Vulnerabilities

Patch Management

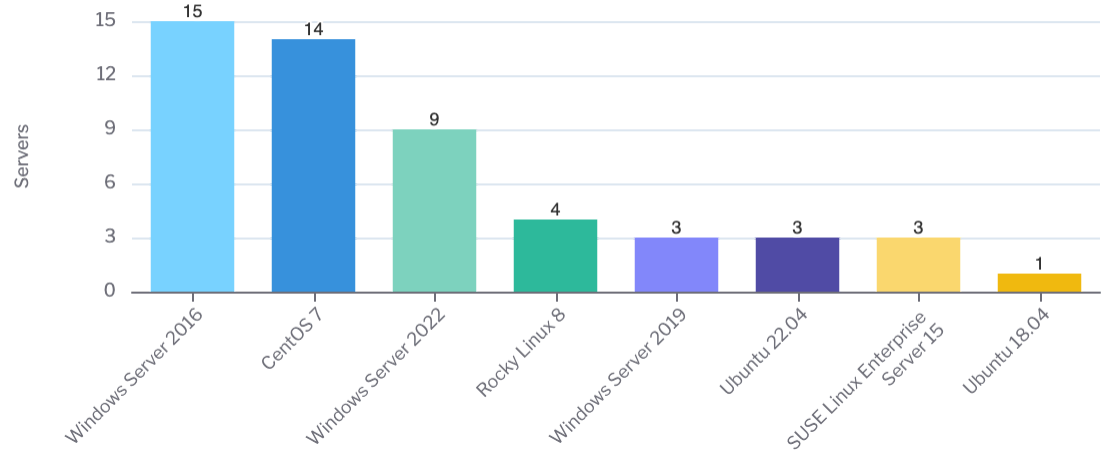
Missing Critical or Important Patches in Last 10 Years



Workstation Operating System Versions Missing Critical or Important Patches



Server Operating System Versions Missing Critical or Important Patches



Software Management and Distribution

During the assessment, Tanium was used to examine usage of installed applications across organizational endpoints. The following table shows the list of the top 25 installed applications by number of endpoints where the application is not in use. These unused applications could represent an opportunity to either reclaim licenses or reduce the overall attack surface through software removal.

Product Name	Vendor Name	Number of Installations	Used	Unused
Microsoft® Windows® Operating System	Microsoft	1207	1075	132
Microsoft OneDrive	Microsoft	141	24	117
Npcap OEM	Nmap Project	116	1	115
Microsoft Visual C++ X86 Additional Runtime	Microsoft	113	0	113

Product Name	Vendor Name	Number of Installations	Used	Unused
QEMU guest agent	RedHat	113	1	112
Red Hat QXL controller	Red Hat	112	0	112
Spice Agent 0.10.0-5	Red Hat	112	0	112
Virtio-win-driver-installer	Red Hat	112	0	112
Virtio-win-guest-tools	Red Hat	112	0	112
Internet Explorer	Microsoft	113	2	111
Microsoft Visual C++ 2015-2022 Redistributable	Microsoft	116	7	109
Microsoft Visual C++ X86 Minimum Runtime	Microsoft	113	9	104
Microsoft Visual C++ Redistributable	Microsoft	97	0	97
Adobe Acrobat Reader	Adobe	95	1	94
Microsoft Edge	Microsoft	93	1	92
Microsoft Visual C++ Additional Runtime	Microsoft	92	0	92
Microsoft Visual C++ Minimum Runtime	Microsoft	92	0	92
Microsoft Update Health Tools	Microsoft	77	0	77
Microsoft Malware Protection	Microsoft	88	18	70
Office 16 Click-to-Run Licensing Component	Microsoft	46	0	46
Chrome Browser	Google	50	5	45
Office 16 Click-to-Run Extensibility Component	Microsoft	46	2	44
Teams Machine-Wide Installer	Microsoft	41	0	41
Office 16 Click-to-Run Localization Component	Microsoft	41	1	40
DefaultPackMSI	Microsoft	41	5	36

As part of the assessment, Tanium examined the volume of installed software and applications and their versioning. The following section provides information about unique versions of applications that exist across endpoints targeted for the report. Having multiple versions of the same software installed on multiple endpoints in the same environment can increase the attack surface of an environment significantly, as malicious code that requires specific vulnerable versions of the software to execute has a higher likelihood of successful execution.

In addition, software, like web browsers, being installed at older versions makes them much more vulnerable to "drive-by" download attacks and users unknowingly executing malicious web code.

Top 10 Applications by Number of Unique Versions (Version Sprawl)

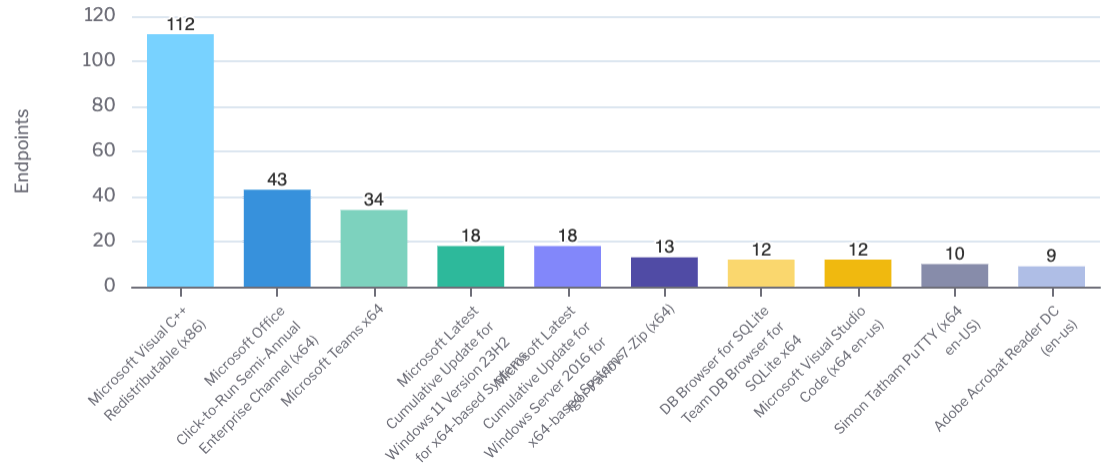
Application	Number of Unique Versions	Number of Endpoints Affected
Microsoft OneDrive	35	65
Windows® Search	24	81

Application	Number of Unique Versions	Number of Endpoints Affected
Adobe Acrobat Reader	18	35
Microsoft® .NET Framework	19	110
Microsoft Malware Protection	14	78
Internet Explorer	11	112
Google Chrome Browser	17	52
Microsoft Edge Update	10	90
Windows Installer - Unicode	10	109
Microsoft Office	9	49

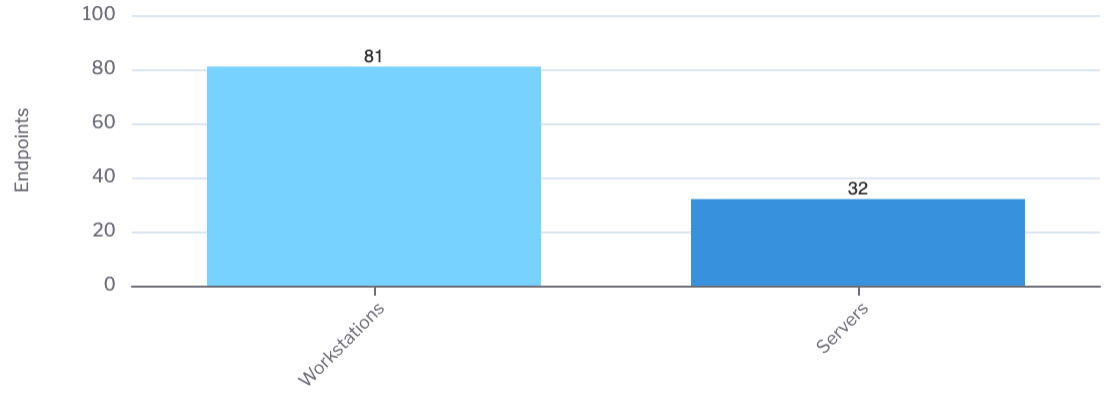
During the assessment, Tanium analyzed the state of common software updates on endpoints in the environment. While organizations often focus significant energy on ensuring that server and workstation operating systems are kept patched and up to date, it is important that similar effort be applied to make sure that commonly used applications and software on the endpoints are also kept up to date and patched.

Updating secondary software and applications is often more complex and more difficult than patching core operating systems. But doing so is equally important to ensure that malicious code, such as ransomware, is unable to gain a foothold in the environment. This section provides details about software update eligibility for servers and workstations targeted for this report.

Top 10 Packages from Deploy Package Gallery That Require Updates

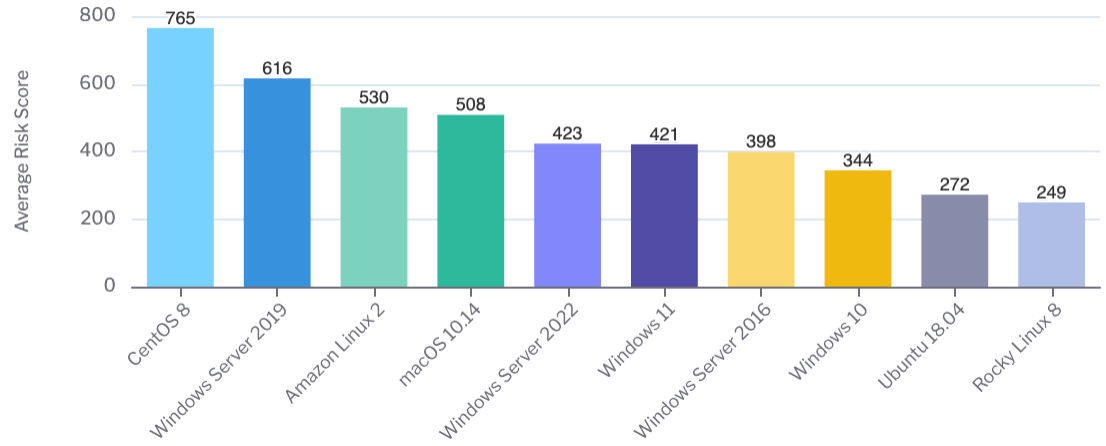


Endpoints with Deploy Package Gallery Packages That Require Updates



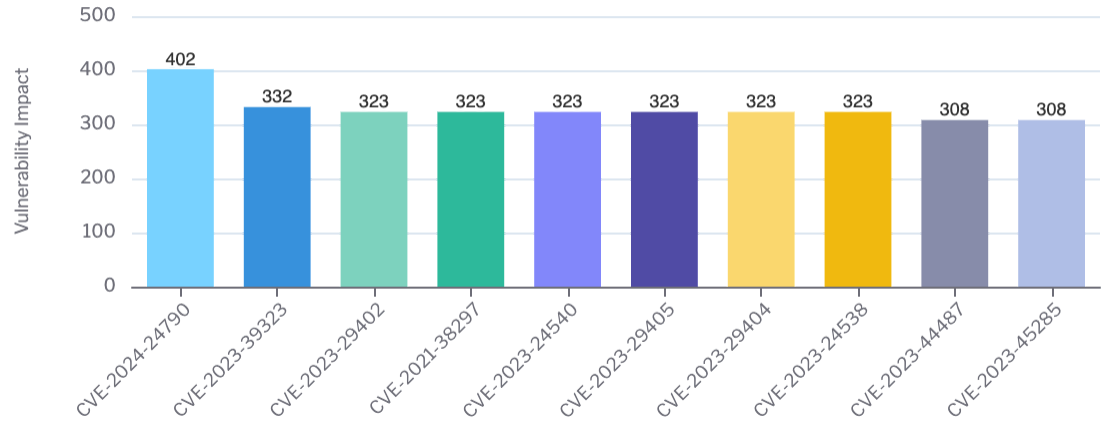
Risk Management

Top 10 Operating System Versions with Highest Average Risk Scores

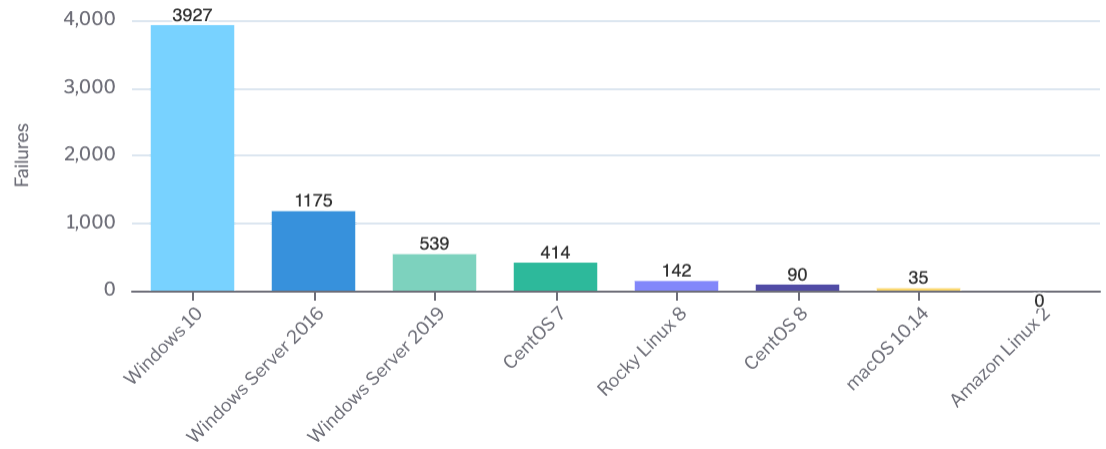


Top 10 Vulnerabilities with Highest Impact

Top 10 CVEs based on vulnerability impact, which is CVSS score multiplied by endpoint count

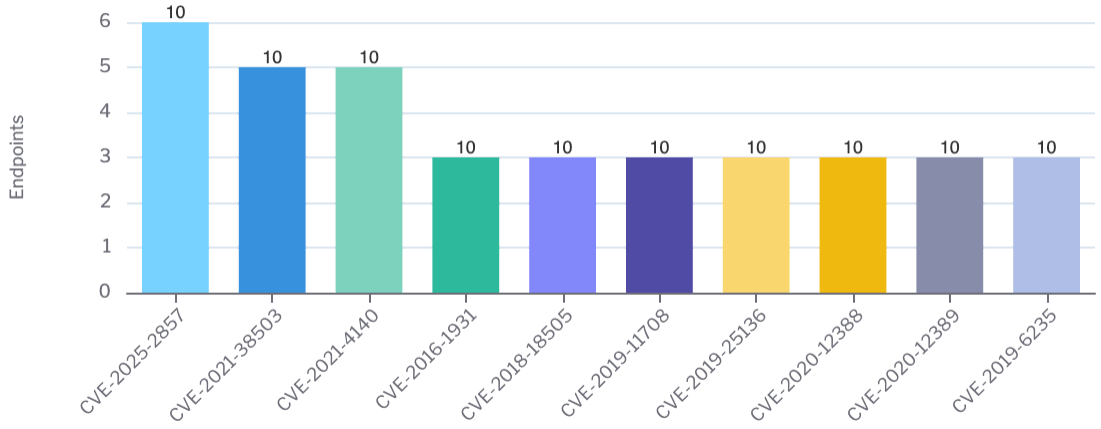


Top 10 Operating System Versions with Most Compliance Failures



Top 10 Vulnerabilities with Highest CVSS Score

Top 10 CVEs based on the CVSS score, which displays above the colored bars



Part 6: About Tanium

Tanium Autonomous Endpoint Management (AEM) offers the most comprehensive solution for intelligently managing endpoints across industries, providing capabilities for asset discovery and inventory, vulnerability management, endpoint management, incident response, risk and compliance, and digital employee experience. The platform supports 34 million endpoints worldwide, including 40% of the Fortune 100, delivering increasingly efficient operations and an improved security posture at scale, with confidence, and in real-time. For more information on The Power of Certainty™, visit www.tanium.com and follow us on LinkedIn and X.