

TruRisk™ Eliminate Report

Generated for **ACME Corporation**

Powered by



Confidential and Proprietary Information: Qualys makes no warranty that the information contained in this report is complete or error-free. Copyright 2026, Qualys, Inc.

01

Enterprise TruRisk™

Vulnerability Coverage by TruRisk™ Eliminate

02

Zero-Touch Remediation Using AI Powered Patch Reliability

Top Recommendations for Zero-Touch Patch Automation

03

MTTR Performance and Risk Elimination

Your Remediation Speed And Exposure Gaps

04

Deep Dive into Risk Sources

Vulnerabilities from 3rd Party Apps

Microsoft Vulnerabilities Published Over 30 Days Ago

Vulnerabilities with No Patch Available

Vulnerabilities from Linux

05

Industry Trends in Permanent and Temporary Mitigations

Top CVEs Being Mitigated By Peer Organizations Using Qualys Threat Research Mitigations

06

Uninstall EOS Software

Remove Top EOL/EOS Bloatware Products Driving Risk

This report highlights your remediation gaps and MTTR impact, and outlines how Qualys TruRisk Eliminate enables faster risk elimination using AI Powered Patch Reliability

Enterprise TruRisk™

Highlights the TruRisk™ of your organisation with focus on Risky vulnerabilities



Affected Assets
1.3M

853K
Internet Facing Assets



Total Vulnerabilities
9.1M

4.8M
Risky Vulnerabilities



4.8M

Risky vulnerabilities



12%

CISA KEV known Exploitable



08%

Weaponized



40%

Associated Threat Actors



20%

Publicly Exploitable

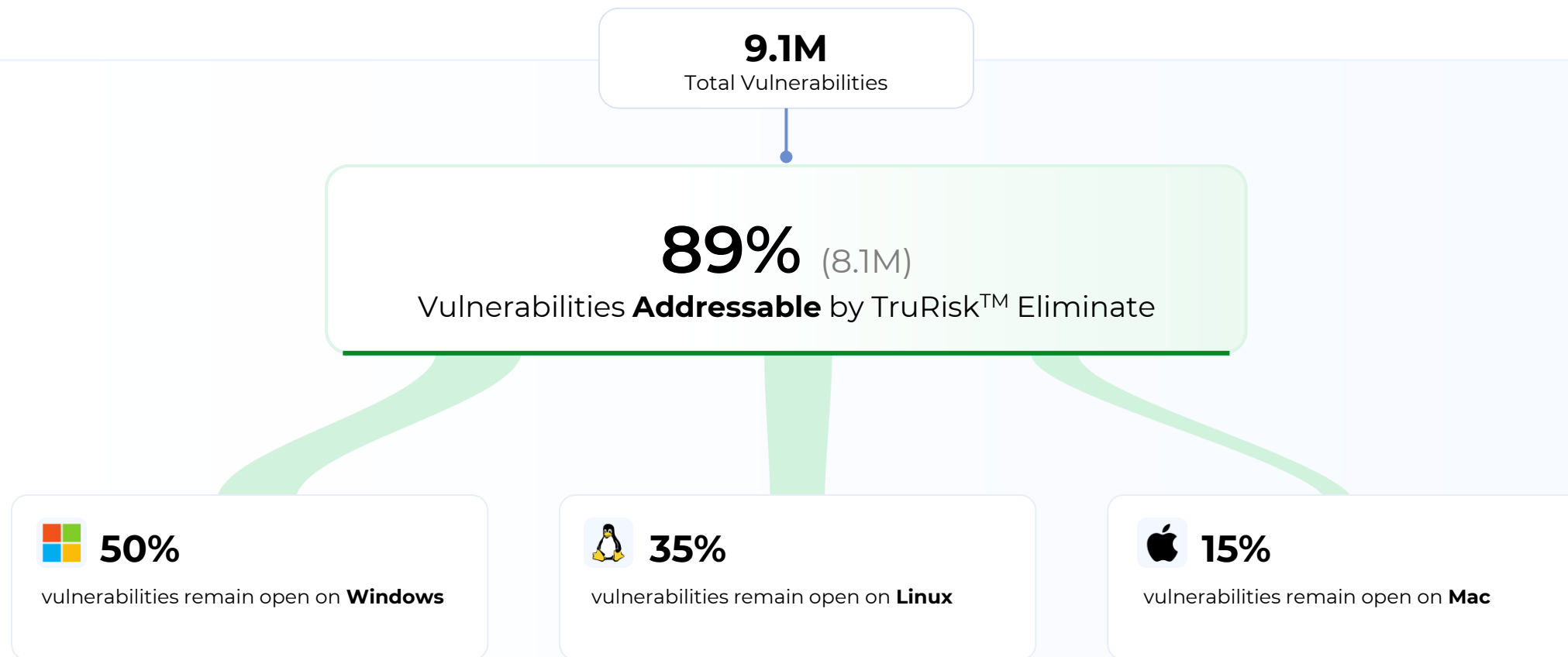


20%

Ransomware

Vulnerability Coverage by TruRisk™ Eliminate

Vulnerabilities that can be patched or mitigated using Qualys TruRisk™ Eliminate, broken down by operating system



11% of Non-Addressable Vulnerabilities are either due to products not covered by TruRisk™ Eliminate or assets not getting scanned in recent time

Zero-Touch Remediation Using **AI Powered Patch Reliability** ✨

See how many vulnerabilities can be Eliminated with zero-touch deployment using High Reliability patches



***Low operational risk:** Applications are typically browsers and standalone apps that pose minimal disruption risk and are safe for zero-touch patching

Top Recommendations for Zero-Touch Patch Automation

Automate zero-touch patching to fix new vulnerabilities the moment a vendor releases an update.

Product	Associated Vulnerabilities	
Chrome	2.3K	4.3% Risky
Notepad++	16.4K	100% Risky
Firefox	8.4K	22% Risky
Git	1.4K	99% Risky
Zoom	1.3K	0% Risky



Zero-touch Patch Automation are set-and-forget patch jobs that automatically deploy patches as soon as the vendor releases them. No manual intervention is needed.

Curious how fast you're closing risk?

Let's see how your **MTTR performance compares with peer organizations already using**  **TruRisk™ Eliminate**

MTTR Performance Benchmarking

Measure your remediation speed and exposure gap against organizations using Qualys TruRisk™ Eliminate

Overall MTTR Analysis

3.3x Slower ↘

Than **Qualys Customers**



Your current MTTR

2 M 13 D

Qualys Customers'
Average MTTR

22 D

Exposure Window

51 Days

You're exposed to threats 51 days longer than the average Qualys customer



Impact of TruRisk™ Eliminate on MTTR

Use the power of Qualys TruRisk™ Eliminate to reduce your risk

Based on your overall MTTR Analysis, we have calculated that you can achieve

70%

Faster Remediation

With  TruRisk™ Eliminate

Let's check out the Top **Risky** vulnerabilities on



141K Risky

Windows Servers



4.9M Risky

Windows Desktops



505K Risky

Linux



6.4K Risky

Mac

Deploy Available **Patches** or **Mitigations** for maximum Risk Reduction

Vulnerabilities Addressable by TruRisk™ Eliminate: Windows Servers

Critical vulnerabilities on Windows Servers that can be patched or mitigated by TruRisk™ Eliminate



Windows Servers
18.2K servers affected



Unique QIDs
2.2K



Detections
277.5K

Top 5 Risky vulnerabilities with maximum detections

QID	Title	Elimination Status		QDS	Instances
386589	Microsoft Edge Based on Chromium Prior to 145.0.3800.58...	 02	 01	95	12.2K
105484	Windows Unquoted/Trusted Service Paths Privilege Escalation...	 0	 01	95	11.4K
92351	Microsoft Windows Server Security Update for February 2026	 12	 12	95	7.9K
92358	Microsoft Windows Shell Security Feature Bypass Vulnerability...	 12	 01	95	7.9K
92360	Microsoft Windows Remote Access Connection Manager Denial...	 13	 01	95	7.9K

Vulnerabilities Addressable by TruRisk™ Eliminate: Windows Desktops

Critical vulnerabilities on Windows Desktops that can be patched or mitigated by TruRisk™ Eliminate



Windows Desktops
122.8K desktops affected



Unique QIDs
5K



Detections
11.6M

Top 5 Risky vulnerabilities with maximum detections

QID	Title	Elimination Status		QDS	Instances
110519	Microsoft Office Security Feature Bypass Vulnerability	 09	 01	95	468.7K
110516	Microsoft Office Security Feature Bypass Vulnerability...	 12	 02	95	437.7K
92350	Microsoft Windows Security Update for February 2026	 12	 12	95	302.2K
92358	Microsoft Windows Microsoft Hypertext Mark Up Language...	 12	 01	95	301.9K
92360	Microsoft Windows Remote Access Connection Manager Denial...	 12	 01	95	300.7K

Vulnerabilities Addressable by TruRisk™ Eliminate: Linux

Critical vulnerabilities on Linux that can be patched or mitigated by TruRisk™ Eliminate



Linux
25.7K assets affected



Unique QIDs
5K



Detections
1M

Top 5 Risky vulnerabilities with maximum detections

QID	Title	Elimination Status		QDS	Instances
6031964	Ubuntu Security Notification for libpng Vulnerability (USN-8039-1)	 02	 0	42	13.9K
6031935	Ubuntu Security Notification for Expat Vulnerabilities (USN-8022-1)	 05	 0	42	13.6K
6031946	Ubuntu Security Notification for Linux kernel Vulnerabilities...	 02	 0	42	12.7K
163397	Red Hat Update for Open Secure Sockets Layer (OpenSSL)...	 01	 0	95	6.1K
162652	Oracle Enterprise Linux Security Update for kernel (ELSA-2025-7898)	 01	 0	42	6.1K

Vulnerabilities Addressable by TruRisk™ Eliminate: Mac

Critical vulnerabilities on Mac that can be patched or mitigated by TruRisk™ Eliminate



Mac
3.6K assets affected



Unique QIDs
593



Detections
23.3K

Top 5 Risky vulnerabilities with maximum detections

QID	Title	Elimination Status		QDS	Instances
42046	OpenSSH Remote Unauthenticated Code Execution Vulnerability...	 03	 0	95	753
383504	Apple macOS Sudo Host Option Elevation of Privilege Vulnerability	 01	 0	42	589
386205	Apple Safari Prior to 26.2 Multiple Vulnerabilities (125892)	 05	 0	95	421
386541	Apple macOS Sequoia 15.7.4 Not Installed (126349)	 03	 0	42	303
386206	Apple macOS Sequoia 15.7.3 Not Installed (125887)	 03	 0	42	270

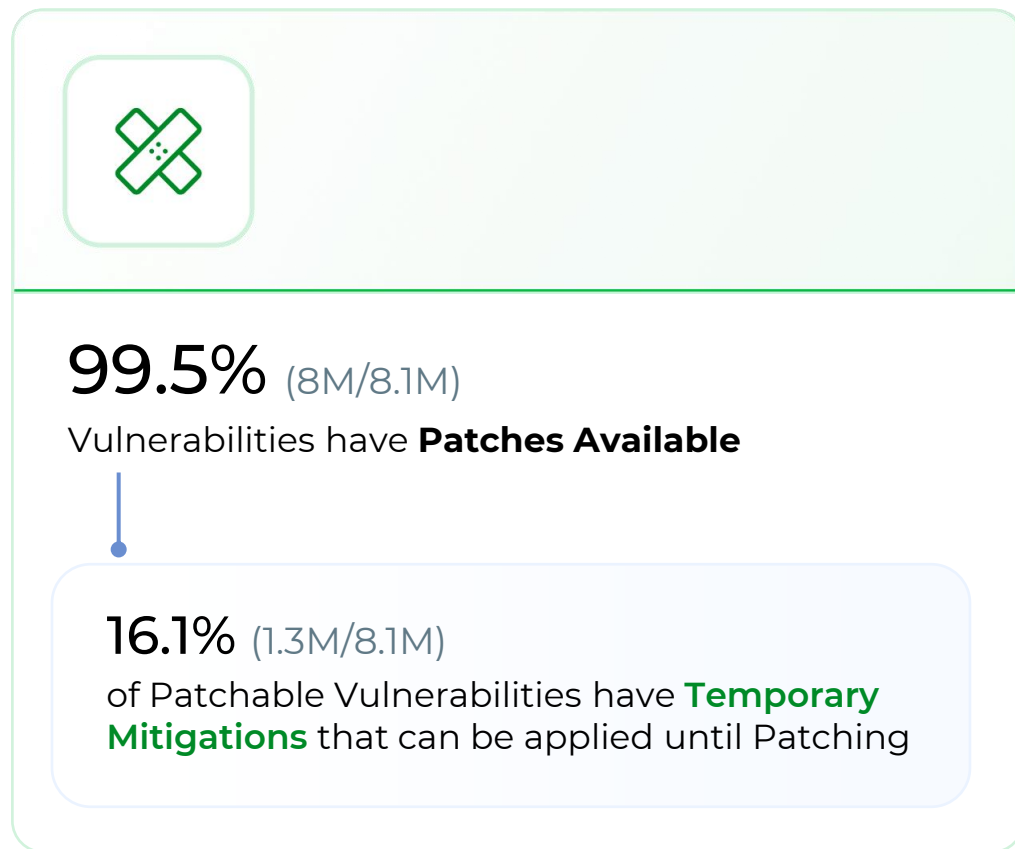
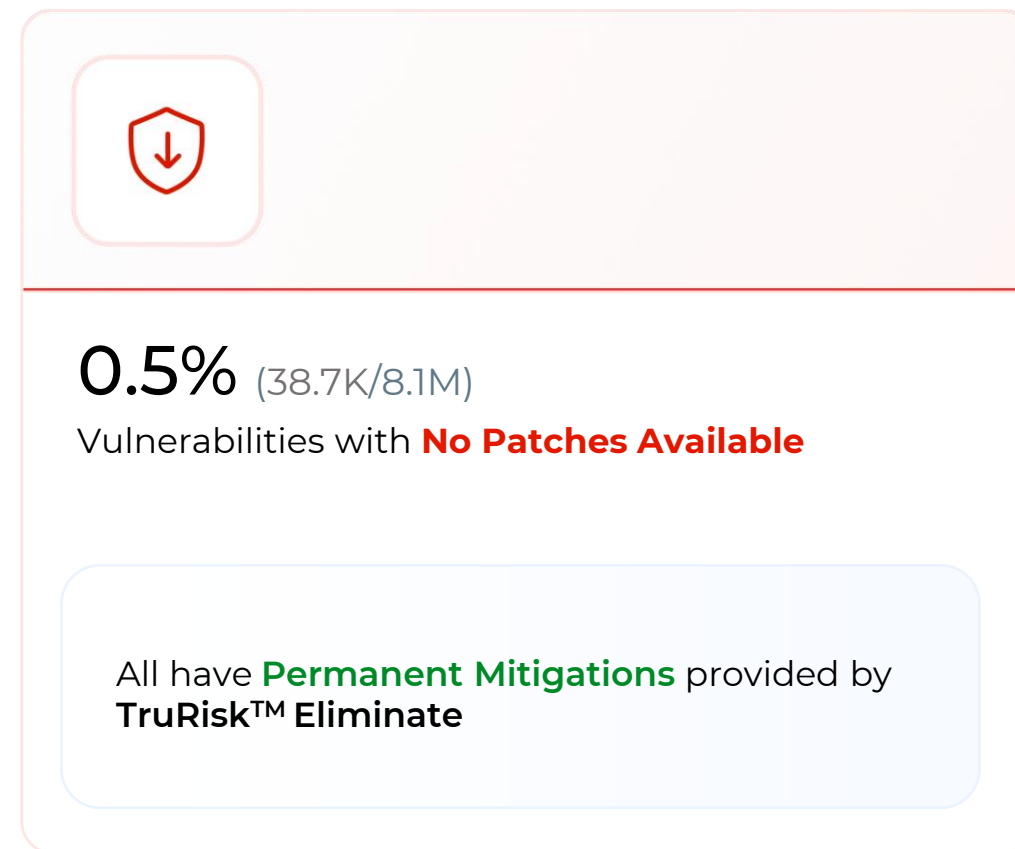


TruRisk™ Eliminate has you covered with risk elimination options through Patching and Mitigation **for all 8.1M addressable vulnerabilities**

Let's dive in to see how!

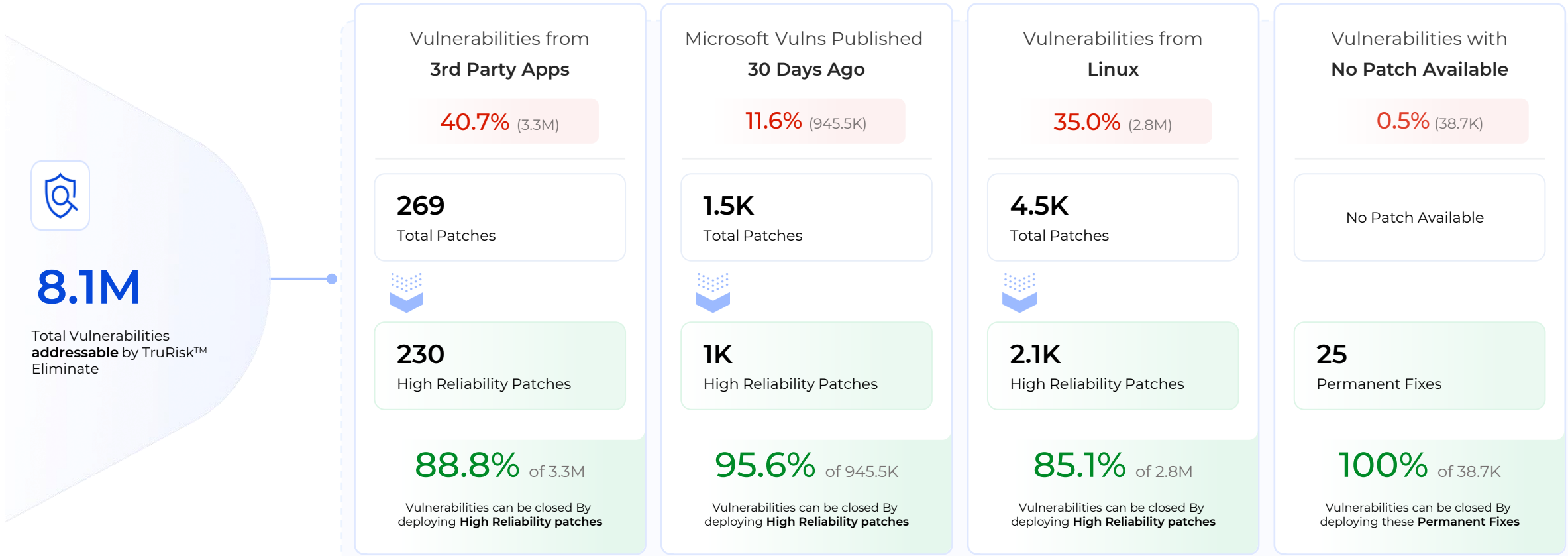
Risk Elimination Options to Accelerate MTTR

Explore the "Remediation Buffet" offered by Qualys TruRisk™ Eliminate for Rapid Risk Reduction



Let's Zoom In on Your Top Vulnerability Risk Sources

Prioritize remediation with High Reliability patches and Permanent Fixes



*Total addressable vulnerabilities include macOS; the four risk sources shown above represent the highest priority areas and may not sum to the total.

Vulnerabilities from 3rd Party Apps



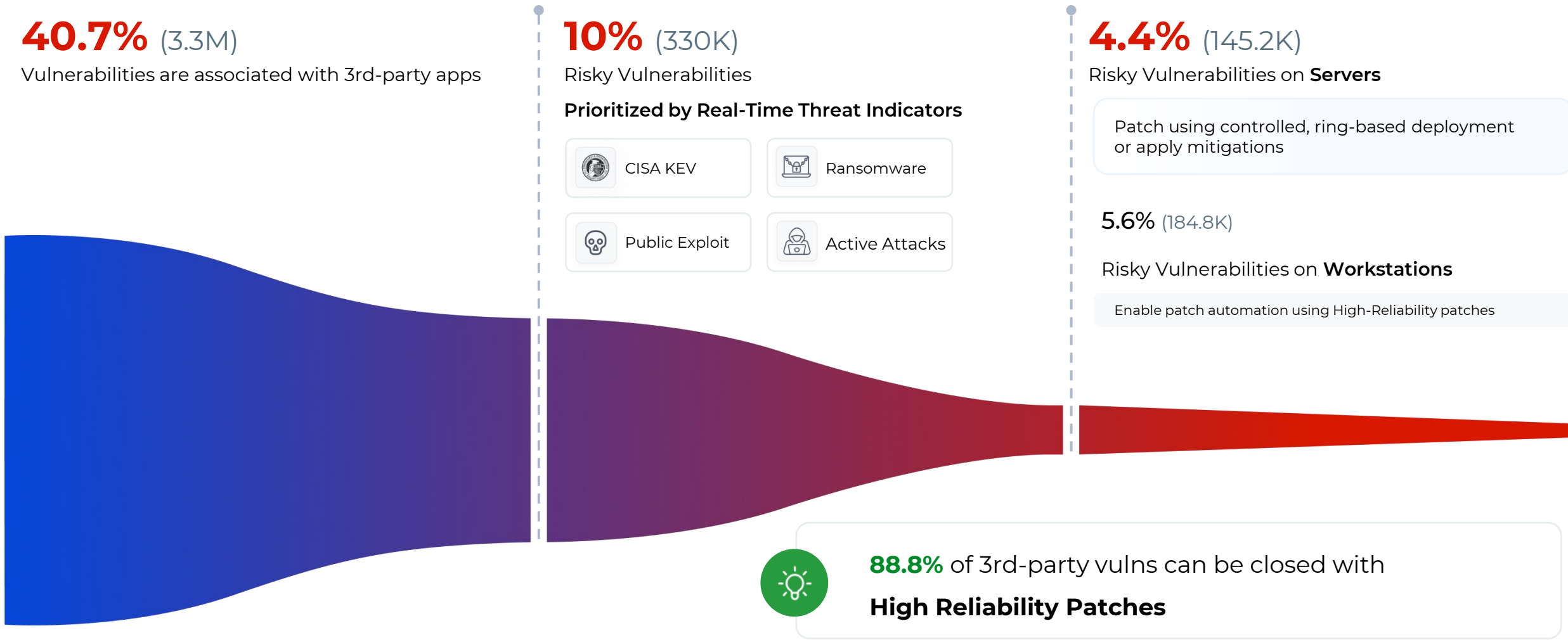
Top 5 Threat Actors
associated with 3rd-Party App
Vulnerabilities on Internet-Facing
Assets

Threat Actors		Vulnerability Count
#1	Unattributed	1.1M
#2	China Attribution	42.3K
#3	Lotus Blossom	28.7K
#4	Taiwan Blossom	16.6K
#5	Intellexa	1.2K

***Unattributed:** Threat actor identity unknown. These vulnerabilities are associated with unclassified or untracked adversaries with no confirmed attribution in threat intelligence databases

Vulnerabilities from 3rd Party Apps (8.1M)

Prioritized view of open vulnerabilities originating from 3rd-party applications



Vulnerabilities from 3rd Party Apps: MTTR Overview

Compare your remediation time against customer averages and Patch Compliance SLAs

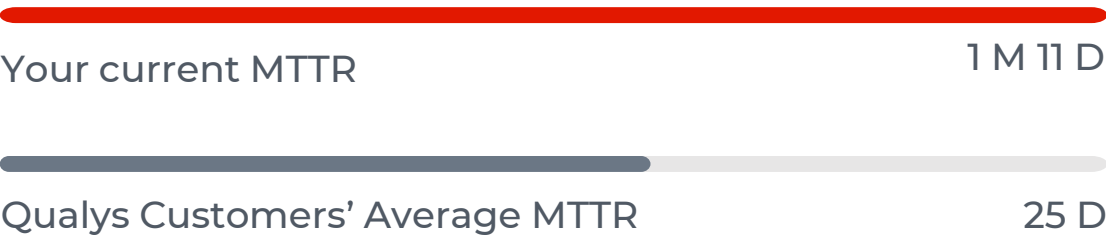
Peer Benchmarking

Your MTTR for overall vulnerabilities from 3rd party apps

1 Month 11 Days



Analysis: 1.6x slower than peers



Critical Patch Compliance SLAs

Your MTTR for critical vulnerabilities is **18 Days** as compared to regulatory requirements

PCI DSS 30 Days	NCSC UK (Internet-facing) 5 Days	NCSC UK (Internal) 14 Days	CIS Patch Management 7 Days
CISA 15 Days	IRS (USA) 30 Days	NIST 30 Days	

Microsoft Vulnerabilities published over 30 days ago



Top 5 Threat Actors
associated with Microsoft
Vulnerabilities on Internet-Facing
Assets

Threat Actors		Vulnerability Count
#1	Unattributed	25K
#2	China Attribution	15K
#3	Dalbit	11.9K
#4	Graceful Spider	7.5K
#5	Wizard Spider	5K

***Unattributed:** Threat actor identity unknown. These vulnerabilities are associated with unclassified or untracked adversaries with no confirmed attribution in threat intelligence databases

Microsoft Vulnerabilities Published Over 30 Days Ago (8.1M)

Prioritized view of open vulnerabilities originating from Microsoft vulnerabilities

11.6% (945.5K)

Microsoft vulnerabilities published over 30 days ago remain unpatched

18% (170.2K)

Risky Vulnerabilities

Prioritized by Real-Time Threat Indicators



CISA KEV



Ransomware



Public Exploit



Active Attacks

2.7% (25.5K)

Risky Vulnerabilities on **Servers**

Patch using controlled, ring-based deployment or apply mitigations

15.3% (144.7K)

Risky Vulnerabilities on **Workstations**

Enable patch automation using High-Reliability patches



95.6% of Microsoft vulns can be closed with
High Reliability Patches

Microsoft Vulnerabilities Published Over 30 Days Ago: MTTR Overview

Compare your remediation time against customer averages and Patch Compliance SLAs

Peer Benchmarking

Your MTTR for Microsoft Vulnerabilities Published Over 30 Days Ago

2 Months 29 Days



Current MTTR: **Below Average (4.2x Slower)**

Your current MTTR

2 M 29 D

Qualys Customers' Average MTTR

21 D

Critical Patch Compliance SLAs

Your MTTR for critical vulnerabilities is **60 Days** as compared to regulatory requirements



PCI DSS
30 Days



NCSC UK (Internet-facing)
5 Days



NCSC UK (Internal)
14 Days



CIS Patch Management
7 Days



CISA
15 Days



IRS (USA)
30 Days



NIST
30 Days



Vulnerabilities with No Patch Available



Threat Actors		Vulnerability Count
#1	Unattributed	3.1K
#2	PROMETHIUM	1.8K
#3	Aurora Panda	1.4K
#4	Dagger Panda	900
#5	Energetic Bear	620

***Unattributed:** Threat actor identity unknown. These vulnerabilities are associated with unclassified or untracked adversaries with no confirmed attribution in threat intelligence databases

Vulnerabilities with **No Patch Available** (8.1M)

Primary reason for increased MTTR and delayed patch SLAs

0.5% (38.7K)

Vulnerabilities that have no patch available contribute to the tail of risk that attackers are most likely to exploit.

9.4% (3.6K)

Risky Vulnerabilities

Prioritized by Real-Time Threat Indicators



CISA KEV



Ransomware



Public Exploit



Active Attacks

5.2% (2.0K)

Risky Vulnerabilities on **Servers**

Prioritize controlled deployment of permanent fixes to reduce MTTR

4.2% (1.6K)

Risky Vulnerabilities on **Workstations**

Deploy permanent fixes immediately at scale to accelerate risk reduction



25 Qualys curated **Permanent Fixes** are available to fix all of these open vulnerabilities

Vulnerabilities with No Patch Available: MTTR Overview

Primary reason for increased MTTR and delayed patch SLAs

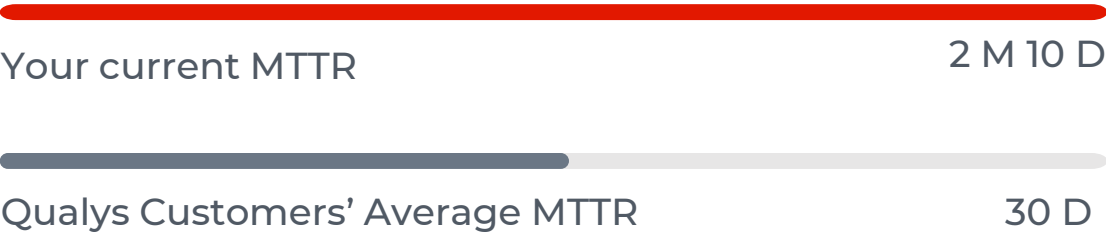
Peer Benchmarking

Your MTTR for Vulnerabilities with No Patch Available

2 Month 10 Days



Current MTTR: Below Average (2.4x slower)



Critical Patch Compliance SLAs

Your MTTR for critical vulnerabilities is 40 Days as compared to regulatory requirements

<div> PCI DSS 30 Days </div>	<div> NCSC UK (Internet-facing) 5 Days </div>	<div> NCSC UK (Internal) 14 Days </div>	<div> CIS Patch Management 7 Days </div>
<div> CISA 15 Days </div>	<div> IRS (USA) 30 Days </div>	<div> NIST 30 Days </div>	

Vulnerabilities from Linux



Top 5 Threat Actors
associated with Linux
Vulnerabilities

Threat Actors		Vulnerability Count
#1	Unattributed	904K
#2	Ghostwriter	190K
#3	Anonymous Sudan	45K
#4	UNC6353	27K
#5	Comment Panda	24K

***Unattributed:** Threat actor identity unknown. These vulnerabilities are associated with unclassified or untracked adversaries with no confirmed attribution in threat intelligence databases

Vulnerabilities from **Linux** (8.1M)

Prioritized view of open vulnerabilities originating from Linux

35.0% (2.8M)

Vulnerabilities are associated with Linux

35.4% (991.2K)

Risky Vulnerabilities

Prioritized by Real-Time Threat Indicators



CISA KEV



Ransomware



Public Exploit



Active Attacks

34.7% (971.6K)

Risky Vulnerabilities on **Servers**

Patch using controlled, ring-based deployment or apply mitigations

0.7% (19.6K)

Risky Vulnerabilities on **Workstations**

Enable patch automation using High-Reliability patches



85.1% of Linux vulnerabilities can be closed with
High Reliability Patches

Vulnerabilities from Linux: MTTR Overview

Compare your remediation time against customer averages and Patch Compliance SLAs

Peer Benchmarking

Your MTTR for overall vulnerabilities from Linux

1 Months 13 Days



Analysis: 1.4x slower than peers



Critical Patch Compliance SLAs

Your MTTR for critical vulnerabilities is 42 Days as compared to regulatory requirements

 PCI DSS 30 Days	 NCSC UK (Internet-facing) 5 Days	 NCSC UK (Internal) 14 Days	 CIS Patch Management 7 Days
 CISA 15 Days	 IRS (USA) 30 Days	 NIST 30 Days	

Want to see the top CVEs where peer organizations are applying **permanent** and **temporary** mitigations created by Qualys Threat Research team

This view also shows how many assets in your environment are currently affected by these open CVEs.

Let's take a look!

Vulnerabilities with **No Patch Available:** Industry Trends in Applying **Permanent Mitigations**

Top CVEs being fixed by peer organizations using Qualys permanent mitigations

<div> <div>CVE-2013-3900</div> <div>Critical</div> <div>Microsoft WinVerifyTrust function Remote Code Execution</div> <div> <div>Permanent mitigations available for</div> <div>120K Assets affected by this vulnerability</div> </div> </div>	<div> <div>CVE-2014-8439</div> <div>Critical</div> <div>Adobe Flash Player Dereferenced Pointer Vulnerability</div> <div> <div>Permanent mitigations available for</div> <div>3.1K Assets affected by this vulnerability</div> </div> </div>	<div> <div>CVE-2016-2183</div> <div>Medium</div> <div>Birthday attacks against Transport Layer Security (TLS) ciphers with 64bit block size</div> <div> <div>Permanent mitigations available for</div> <div>131K Assets affected by this vulnerability</div> </div> </div>
<div> <div>CVE-2024-39818</div> <div>Low</div> <div>Zoom Workplace Apps and SDKs - Protection Mechanism Failure</div> <div> <div>Permanent mitigations available for</div> <div>12.8K Assets affected by this vulnerability</div> </div> </div>	<div> <div>CVE-2025-0167</div> <div>Low</div> <div>Microsoft Curl Exposure of Sensitive Information Vulnerability</div> <div> <div>Permanent mitigations available for</div> <div>6.2K Assets affected by this vulnerability</div> </div> </div>	

Vulnerabilities that Can Be Mitigated Until Patching: Industry Trends in Applying Mitigations

Top CVEs being fixed by peer organizations using Qualys temporary mitigation

CVE-2025-21307

Medium

Windows Reliable Multicast Transport Driver (RMCAST) Remote Code Execution Vulnerability

Temporary mitigations available for

5.9K Assets affected by this vulnerability

CVE-2025-6554

Critical

Google Chromium V8 Type Confusion Vulnerability

Temporary mitigations available for

14.3K Assets affected by this vulnerability

CVE-2025-49681

High

Windows Routing and Remote Access Service (RRAS) Information Disclosure Vulnerability

Temporary mitigations available for

457 Assets affected by this vulnerability

CVE-2025-47160

Critical

Windows Shortcut Files Security Feature Bypass Vulnerability

Temporary mitigations available for

8.1K Assets affected by this vulnerability

CVE-2018-3639

Critical

Microsoft Windows Security Update Registry Key Configuration Missing

Temporary mitigations available for

23K Assets affected by this vulnerability

Uninstalling or upgrading EOL/EOS software is one of the most effective ways to reduce risk



No Vendor Patches

EOL/EOS software no longer receives vendor patches, resulting in persistent risk



High Risk Assets

Many of your assets have Risky EOL/EOS software_with a QDS > 70



TruRisk™ Eliminate provides Software Uninstallation capability to remove **EOS software**.

Remove Top 10 EOL/EOS Bloatware Products Diving Risk

Ranked by unique CVEs attributable to the product on Servers

Software Product	Affected Servers	Associated Unique CVEs	
Firefox	252	2.5K	18 Malware_CVEs
Chrome	5K	2K	06 Malware_CVEs
Safari	1	1K	01 Malware_CVEs
Flash Player	57	1K	60 Malware_CVEs
Internet Explorer	33K	790	30 Malware_CVEs
Acrobat Reader	199	609	31 Malware_CVEs
Acrobat	11	471	14 Malware_CVEs
Wireshark	377	451	01 Malware_CVEs
Foxit Reader	493	285	01 Malware_CVEs
Adobe AIR	6	133	06 Malware_CVEs



TruRisk™ Eliminate provides Software Uninstallation capability to eliminate risk from EOS software

Activate TruRisk™ Eliminate

Use the power of Qualys TruRisk™ Eliminate to reduce your risk

As implied in MTTR analysis, if you want

70%

Faster Remediation

Try out  TruRisk™ Eliminate



TruRisk™ Eliminate

Sign up to enable TruRisk™ Eliminate trial

Appendix: Definitions

Key terms and thresholds used in this report

Critical Assets

Assets with a criticality score ≥ 4

Risky Vulnerabilities

Vulnerabilities associated with **Threat Indicators**

Critical Vulnerabilities

Vulnerabilities with QDS > 90

Permanent Fix

A permanent mitigation developed by the Qualys Threat Research team for vulnerabilities where no patch is available, including vulnerabilities originating from **EOL/EOS software** for which vendors no longer provide patches.

Temporary Mitigations

When vulnerabilities have patches but are not deployed due to operational risks, temporary mitigations can be applied until patching is completed to keep the vulnerability unexploitable.

Powered By



The leading provider of information security and compliance cloud solutions. More than 10,000 subscription customers worldwide in more than 130 countries trust Qualys to underpin digital transformation for greater agility, better business outcomes, and substantial cost savings. The Enterprise TruRisk Platform and its integrated apps help businesses simplify security operations and lower the cost of compliance by delivering critical security intelligence on demand and automating the full spectrum of auditing, compliance and protection for IT systems and web applications.

Copyright © 2026, Qualys and/or its affiliates. All rights reserved. This document is provided for information purposes only, and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document, and no contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior written permission. Qualys is registered trademarks of Qualys and/or its affiliates. Other names may be trademarks of their respective owners.