To Patch or Not to Patch: Achieving Immediate Risk Reduction with Qualys

Agenda

01 **The Goal:** 5 Steps to Improve Risk Reduction

02 **Patch and Mitigation:** Best Practices and Demo

03 **Roadmap**

National Cyber Security Centre

A vulnerability management process shouldn't exist in isolation. It is a cross-cutting effort and involves not just those working in IT operations, but also security and risk teams.

More Open Vulnerabilities
More Patches to Deploy

Higher Chance of an Outage

78M

Patches Deployed
Since Jan 2024

24 Days

Faster remediation
of CISA KEV Vulns

160M

CISA KEV Vulns
Remediation with
Qualys Patch

TruRisk Eliminate

Expanding Remediation Beyond Patching

TruRisk Eliminate

Patch + TruRisk Mitigate + TruRisk Isolate

Eliminate it, don’t just measure it.

TruRisk Mitigate

Fix Vulns That DO NOT Have a Patch

Map QIDs to Remediation Actions

Qualys prepares and tests the relevant configuration change or uninstall command to fix EOL vulnerable software

Customer can test and deploy the remediation actions to the vulnerable assets only using the Qualys agent

Vulnerabilities will be marked as closed in VMDR reports

Address Vulnerabilities That Cannot Be Patched Due to High Risk for an Outage

Map QIDs to Alternative Mitigations

- Qualys Threat Research prepares and validates mitigation options for critical vulns
- Mitigation techniques examples: block ports, stop services, conf changes, Etc.
- Most mitigations can be easily rollbacked compared to rolling-back a patch
- Customer can test and deploy those mitigations instead of deploying the patch
- Mitigated status and risk reduction are reflected in all VMDR reports

Address Zero-day Vulns Until a Patch Is Available

Mitigation to Address a Zero-day

Qualys Threat Research prepares and validates a mitigation option

Customer can test and deploy the mitigation ASAP

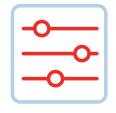
Mitigated status and risk reduction are reflected in all VMDR reports

TruRisk Isolate

Device Isolation

As a Last Resort

Isolate the device from the network



Allow remote patching and control from Qualys and other allowed resources

Agent technology – no EDR technology required

Fully Integrated
with VMDR

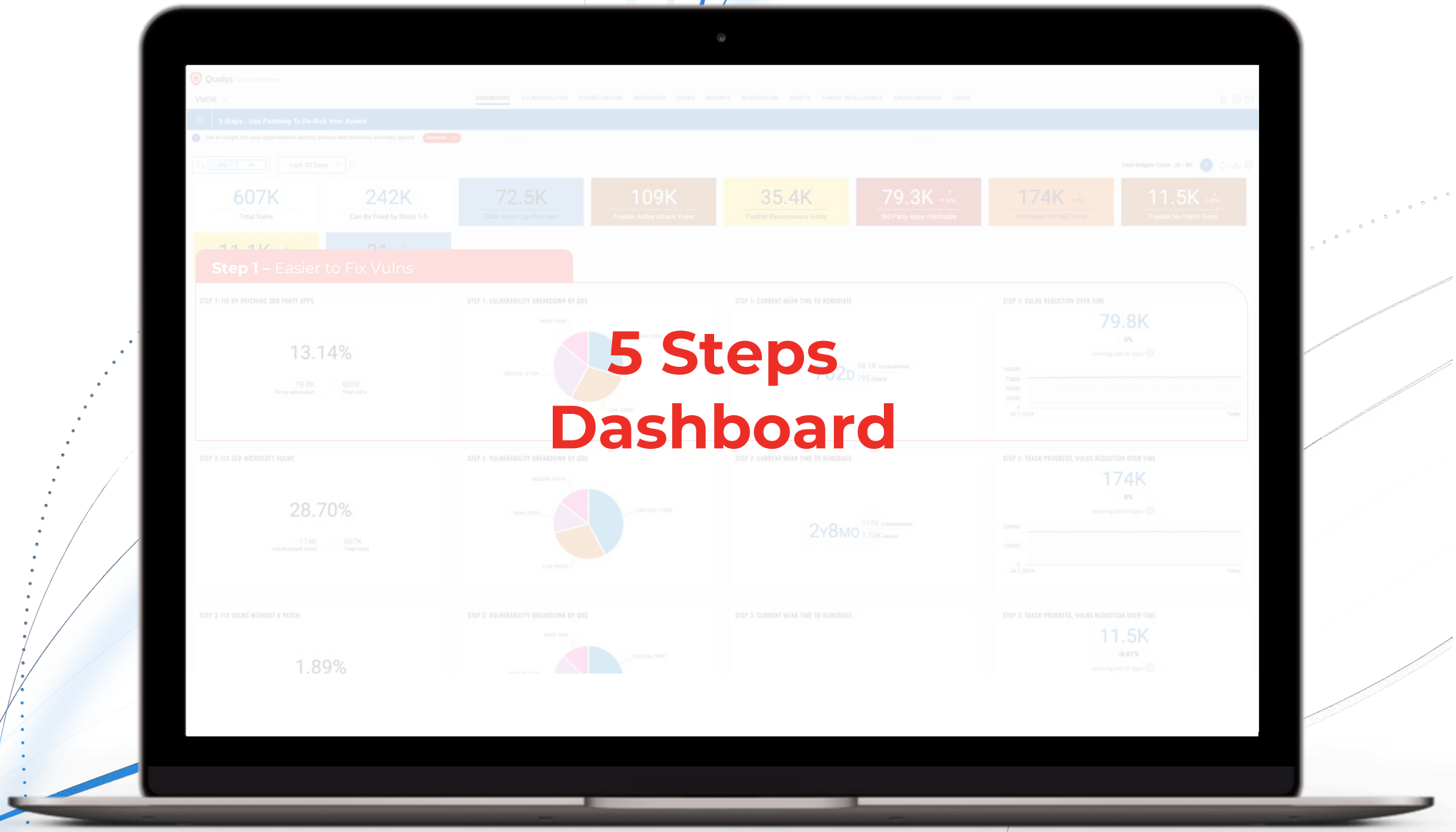
Fully Integrated

Familiar Workflows

Workflows for VMDR, patching, conf changes and mitigation are fully integrated providing same user experience

All results are reflected in VMDR reports

5 Steps Dashboard



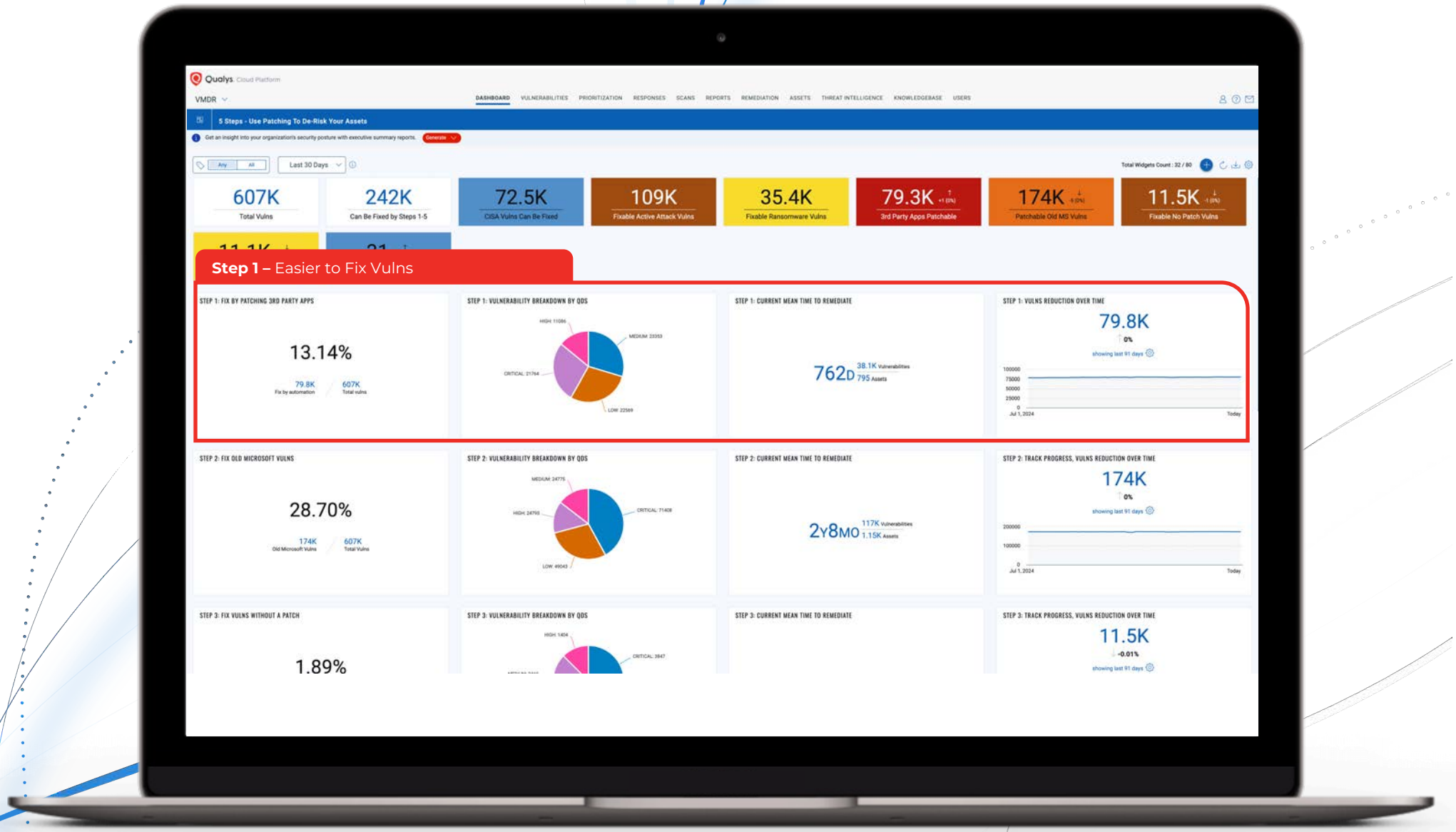
FREE
Five Steps Dashboard

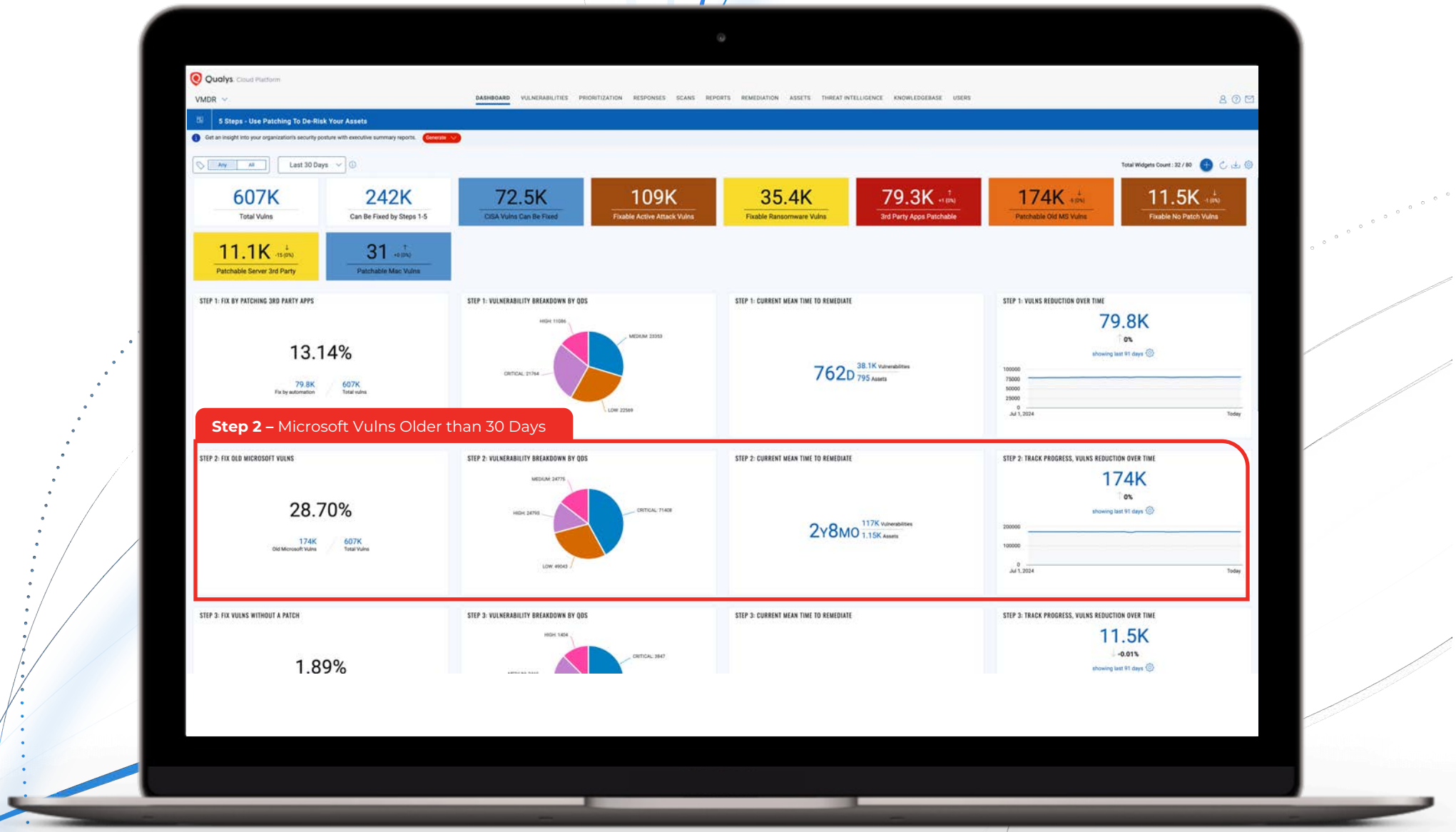
Free to Download Dashboard

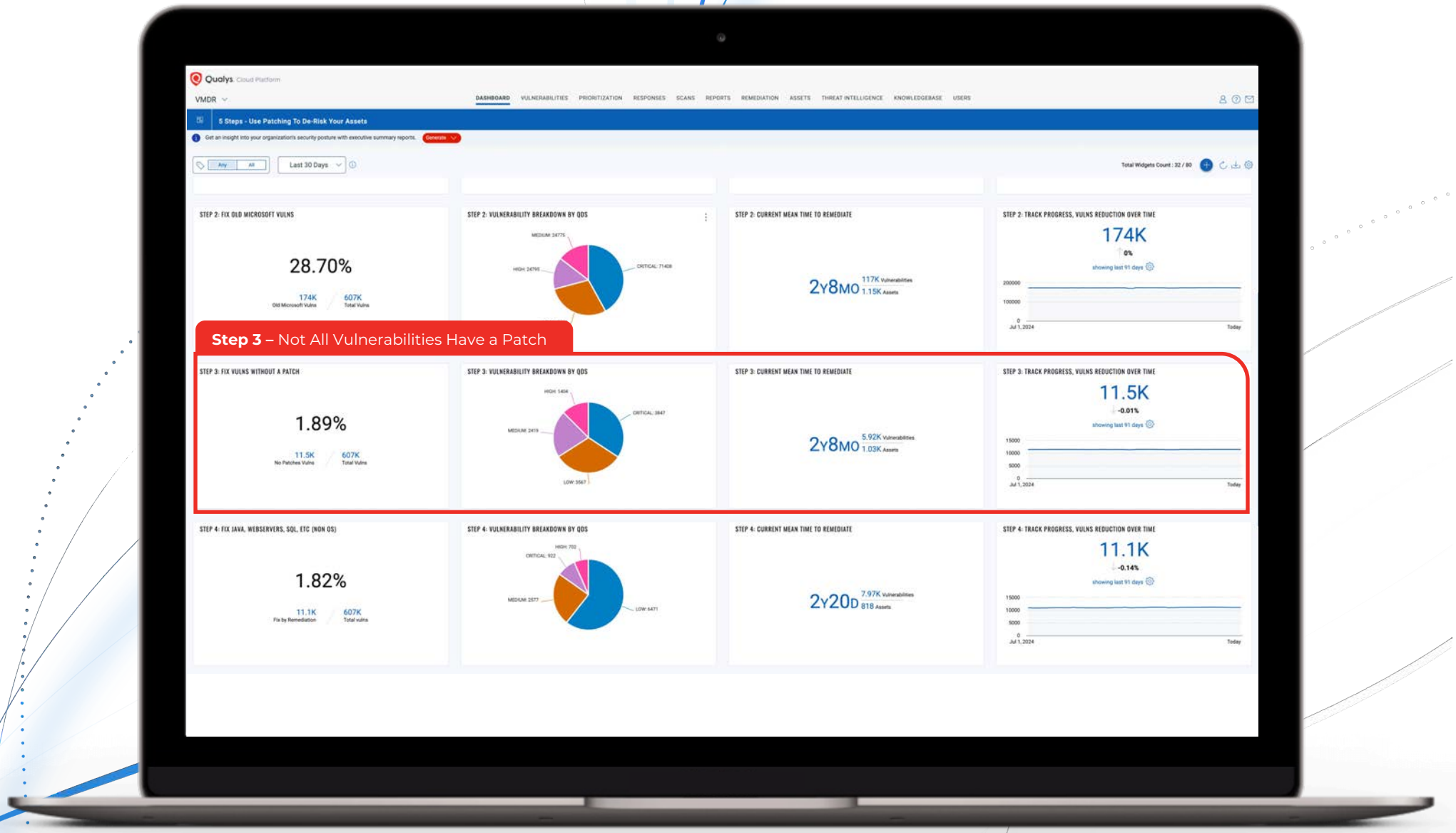
Standard VMDR Dashboard

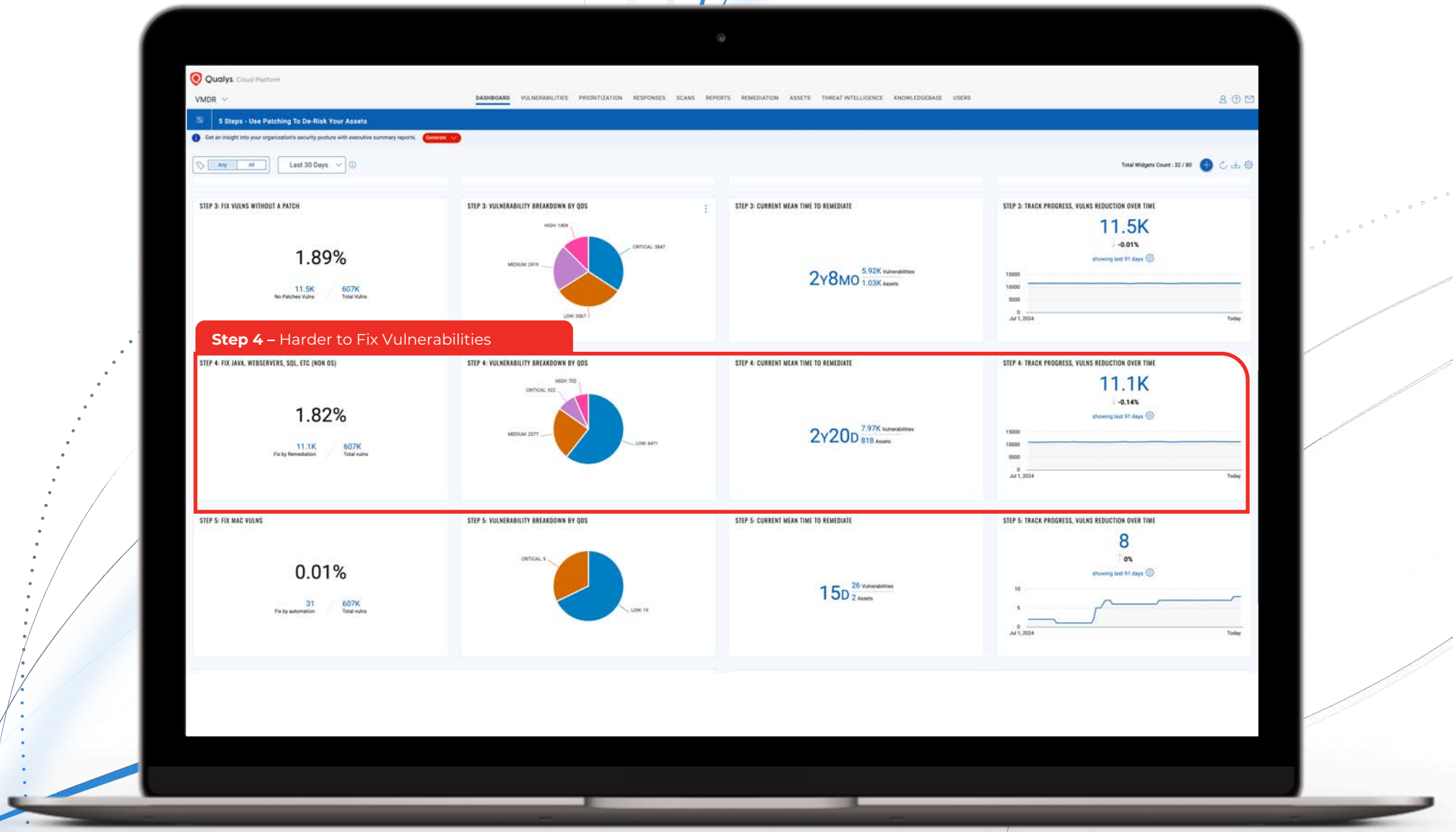
Only requires VM data
(no patch or eliminate license is required)

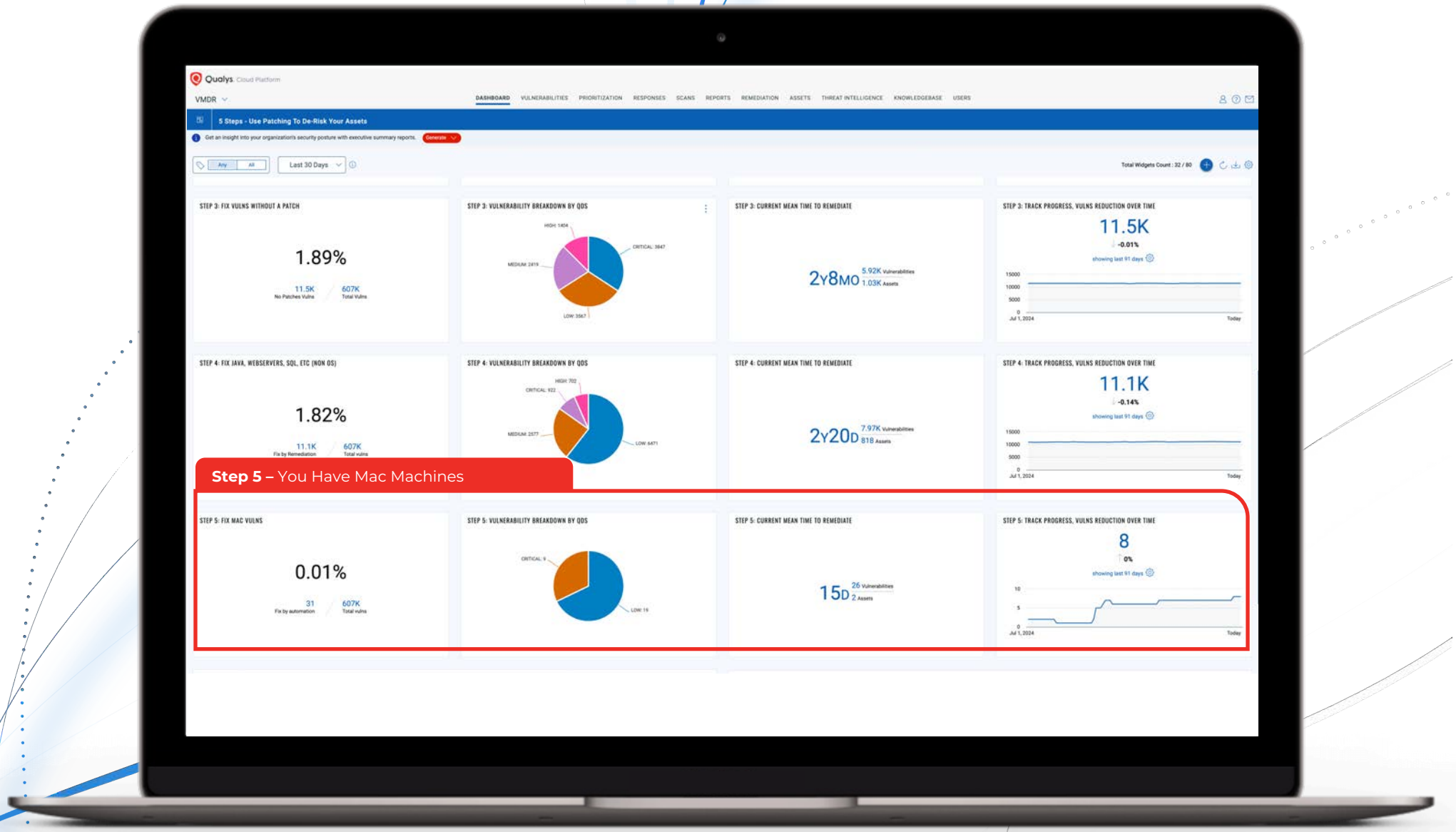
Help address vulnerabilities efferently


Qualys Cloud Platform
VMDR
DASHBOARD
VULNERABILITIES
PRIORITIZATION
RESPONSES
SCANS
REPORTS
REMEDIATION
ASSETS
THREAT INTELLIGENCE
KNOWLEDGEBASE
USERS
5 Steps - Use Patching To De-Risk Your Assets
Get an insight into your organization's security posture with executive summary reports.
Generate
Last 30 Days
607K
Total Vulns
242K
Can Be Fixed by Steps 1-5
72.5K
CISA Vulns Can Be Fixed
109K
Fixable Active Attack Vulns
35.4K
Fixable Ransomware Vulns
79.3K
3rd Party Apps Patchable
174K
Patchable Old MS Vulns
11.5K
Fixable No Patch Vulns
Step 1 – Easier to Fix Vulns
STEP 1: FIX BY PATCHING 3RD PARTY APPS
13.14%
79.8K
Fix by automation
607K
Total vulns
STEP 1: VULNERABILITY BREAKDOWN BY QDS
STEP 1: CURRENT MEAN TIME TO REMEDIATE
762D
38.1K Vulnerabilities
795 Assets
STEP 1: VULNS REDUCTION OVER TIME
79.8K
0%
showing last 91 days
STEP 2: FIX OLD MICROSOFT VULNS
28.70%
174K
Old Microsoft Vulns
607K
Total Vulns
STEP 2: VULNERABILITY BREAKDOWN BY QDS
STEP 2: CURRENT MEAN TIME TO REMEDIATE
2Y8MO
117K Vulnerabilities
1.15K Assets
STEP 2: TRACK PROGRESS, VULNS REDUCTION OVER TIME
174K
0%
showing last 91 days
STEP 3: FIX VULNS WITHOUT A PATCH
1.89%
STEP 3: VULNERABILITY BREAKDOWN BY QDS
STEP 3: CURRENT MEAN TIME TO REMEDIATE
STEP 3: TRACK PROGRESS, VULNS REDUCTION OVER TIME
11.5K
-0.01%
showing last 91 days


Qualys Cloud Platform
VMDR
DASHBOARD
VULNERABILITIES
PRIORITIZATION
RESPONSES
SCANS
REPORTS
REMEDIATION
ASSETS
THREAT INTELLIGENCE
KNOWLEDGEBASE
USERS
5 Steps - Use Patching To De-Risk Your Assets
Get an insight into your organization's security posture with executive summary reports.
Generate
Last 30 Days
607K
Total Vulns
242K
Can Be Fixed by Steps 1-5
72.5K
CISA Vulns Can Be Fixed
109K
Fixable Active Attack Vulns
35.4K
Fixable Ransomware Vulns
79.3K
3rd Party Apps Patchable
174K
Patchable Old MS Vulns
11.5K
Fixable No Patch Vulns
11.1K
Patchable Server 3rd Party
31
Patchable Mac Vulns
STEP 1: FIX BY PATCHING 3RD PARTY APPS
13.14%
79.8K
Fix by automation
607K
Total vulns
STEP 1: VULNERABILITY BREAKDOWN BY QDS
STEP 1: CURRENT MEAN TIME TO REMEDIATE
762D
38.1K Vulnerabilities
795 Assets
STEP 1: VULNS REDUCTION OVER TIME
79.8K
0%
showing last 91 days
Step 2 – Microsoft Vulns Older than 30 Days
STEP 2: FIX OLD MICROSOFT VULNS
28.70%
174K
Old Microsoft Vulns
607K
Total Vulns
STEP 2: VULNERABILITY BREAKDOWN BY QDS
STEP 2: CURRENT MEAN TIME TO REMEDIATE
2Y8MO
117K Vulnerabilities
1.15K Assets
STEP 2: TRACK PROGRESS, VULNS REDUCTION OVER TIME
174K
0%
showing last 91 days
STEP 3: FIX VULNS WITHOUT A PATCH
1.89%
STEP 3: VULNERABILITY BREAKDOWN BY QDS
STEP 3: CURRENT MEAN TIME TO REMEDIATE
STEP 3: TRACK PROGRESS, VULNS REDUCTION OVER TIME
11.5K
-0.01%
showing last 91 days


Qualys Cloud Platform
VMDR
DASHBOARD VULNERABILITIES PRIORITIZATION RESPONSES SCANS REPORTS REMEDIATION ASSETS THREAT INTELLIGENCE KNOWLEDGEBASE USERS
5 Steps - Use Patching To De-Risk Your Assets
Get an insight into your organization's security posture with executive summary reports.
Generate
Any All
Last 30 Days
Total Widgets Count : 32 / 80
STEP 2: FIX OLD MICROSOFT VULNS
28.70%
174K Old Microsoft Vulns
607K Total Vulns
STEP 2: VULNERABILITY BREAKDOWN BY QDS
MEDIUM: 24775
HIGH: 24795
CRITICAL: 71408
STEP 2: CURRENT MEAN TIME TO REMEDIATE
2Y8MO
117K Vulnerabilities
1.15K Assets
STEP 2: TRACK PROGRESS, VULNS REDUCTION OVER TIME
174K
0%
showing last 91 days
200000
100000
0
Jul 1, 2024
Today
Step 3 – Not All Vulnerabilities Have a Patch
STEP 3: FIX VULNS WITHOUT A PATCH
1.89%
11.5K No Patches Vulns
607K Total Vulns
STEP 3: VULNERABILITY BREAKDOWN BY QDS
HIGH: 1404
CRITICAL: 3847
MEDIUM: 2419
LOW: 3567
STEP 3: CURRENT MEAN TIME TO REMEDIATE
2Y8MO
5.92K Vulnerabilities
1.03K Assets
STEP 3: TRACK PROGRESS, VULNS REDUCTION OVER TIME
11.5K
-0.01%
showing last 91 days
15000
10000
5000
0
Jul 1, 2024
Today
STEP 4: FIX JAVA, WEBSERVERS, SQL, ETC (NON OS)
1.82%
11.1K Fix by Remediation
607K Total vulns
STEP 4: VULNERABILITY BREAKDOWN BY QDS
HIGH: 702
CRITICAL: 922
MEDIUM: 2577
LOW: 6471
STEP 4: CURRENT MEAN TIME TO REMEDIATE
2Y20D
7.97K Vulnerabilities
818 Assets
STEP 4: TRACK PROGRESS, VULNS REDUCTION OVER TIME
11.1K
-0.14%
showing last 91 days
15000
10000
5000
0
Jul 1, 2024
Today


Qualys Cloud Platform
VMDR
DASHBOARD VULNERABILITIES PRIORITIZATION RESPONSES SCANS REPORTS REMEDIATION ASSETS THREAT INTELLIGENCE KNOWLEDGEBASE USERS
5 Steps - Use Patching To De-Risk Your Assets
Get an insight into your organization's security posture with executive summary reports.
Generate
Any All
Last 30 Days
Total Widgets Count : 32 / 80
STEP 3: FIX VULNS WITHOUT A PATCH
1.89%
11.5K
No Patches Vulns
607K
Total Vulns
STEP 3: VULNERABILITY BREAKDOWN BY QDS
HIGH: 1404
CRITICAL: 3847
MEDIUM: 2419
LOW: 3567
STEP 3: CURRENT MEAN TIME TO REMEDIATE
2Y8MO
5.92K Vulnerabilities
1.03K Assets
STEP 3: TRACK PROGRESS, VULNS REDUCTION OVER TIME
11.5K
-0.01%
showing last 91 days
15000
10000
5000
0
Jul 1, 2024
Today
Step 4 – Harder to Fix Vulnerabilities
STEP 4: FIX JAVA, WEBSERVERS, SQL, ETC (NON OS)
1.82%
11.1K
Fix by Remediation
607K
Total vulns
STEP 4: VULNERABILITY BREAKDOWN BY QDS
HIGH: 702
CRITICAL: 922
MEDIUM: 2577
LOW: 6471
STEP 4: CURRENT MEAN TIME TO REMEDIATE
2Y20D
7.97K Vulnerabilities
818 Assets
STEP 4: TRACK PROGRESS, VULNS REDUCTION OVER TIME
11.1K
-0.14%
showing last 91 days
15000
10000
5000
0
Jul 1, 2024
Today
STEP 5: FIX MAC VULNS
0.01%
31
Fix by automation
607K
Total vulns
STEP 5: VULNERABILITY BREAKDOWN BY QDS
CRITICAL: 9
LOW: 19
STEP 5: CURRENT MEAN TIME TO REMEDIATE
15D
26 Vulnerabilities
2 Assets
STEP 5: TRACK PROGRESS, VULNS REDUCTION OVER TIME
8
0%
showing last 91 days
10
5
0
Jul 1, 2024
Today



Step 5 – You Have Mac Machines

5 Steps Dashboard DEMO

with TruRisk Eliminate

Qualys

Roadmap

Qualys

Roadmap: 2025

Mitigate + Isolate
Continue investment

SCCM/Intunes Integration
IT can use SCCM to deploy jobs

Virtual Patch
In memory containers protection

Integrations
ServiceNow and others

Roadmap: Q4 2024, Q1 2025

Patch + Configuration Mapping
Map QIDs to patch + conf changes require to fix a vuln

New Reporting
Patch and asset-based reports to track successes and failures

Re-run Jobs
Edit and re-run jobs, specifically on-demand

Linked Jobs Progress Based on Success
Automatically start a linked job based on the success of the test job

Roadmap:
Q4 2024, Q1 2025

Pause/Cancel Job Pre-Actions
Use pre-action script to pause or cancel a patch job (before patching starts)

On-Demand Job Start Agent API
Start a job by notifying the agent over API – use for new images

On-Demand Job Start End User
Allow end user to choose when to start a patch job

Rollback For Linux Jobs
Rollback patch Linux jobs

Roadmap: Q4 2024, Q1 2025 (Others)

Other Important Improvements

- Support for Ubuntu 18, 20 and 22 ESM and RHEL 8.2, 8.4, 9.0 and 9.2
- Ability to patch ARM architecture-based Linux systems
- Log and audit all Patch Management admin actions
- Add support for Windows Server 2012 which is in ESU

Conclusion

Qualys®

Eliminate It, Don’t Just Measure It.

TruRisk **Eliminate**

Address All Types of Vulnerabilities

TruRisk Patch

- Test and deploy patches to fix vulns
- Fully automate patch deployment based on risk
- Windows, Mac, Linux OS and 3rd party app support

TruRisk Mitigate

- Remediate vulns that don’t have a patch
- Mitigate vulns that cannot be patched due to operational risk
- Address Zero Day vulns before the patch is available

TruRisk Isolate

- Isolate device to ensure vulns cannot be exploited
- Allow exceptions to ensure device can be patched and managed

Q&A

Qualys®