QSC 23

Remediation & Beyond: Alternative Mitigation Paths for Reducing Operational Risk

Eran Livne
Sr Director Product Management

Qualys®

Enterprise TruRisk™ Platform

Measure, Communicate, and eliminate cyber risk.

De-risk your business.

Weaponized Vulns

19.5

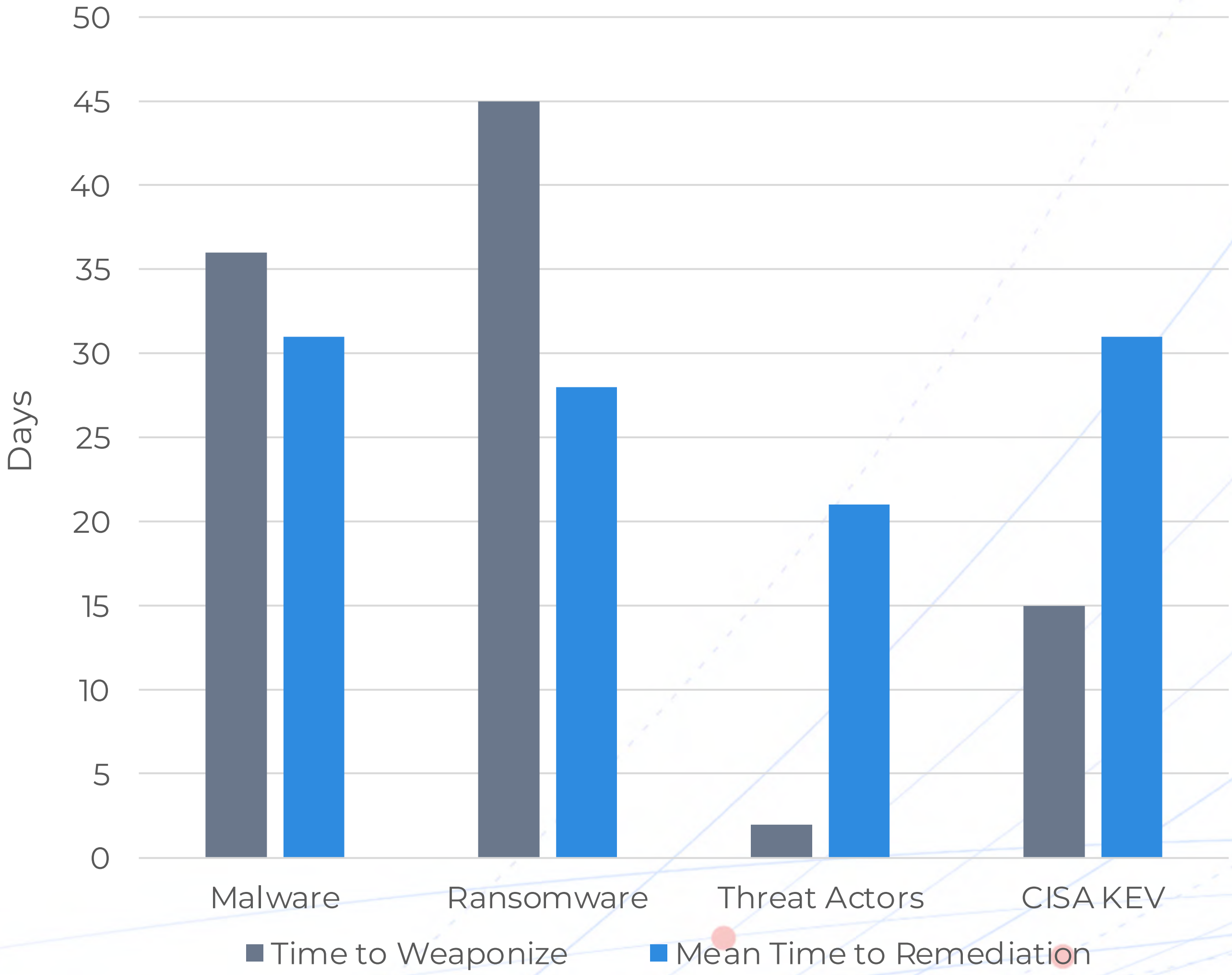
Time to Weaponize (Days)

30.6

Mean Time to Remediate (Days)

57.7%

Remediated Vulnerabilities



Qualys.

Qualys Threat Research Unit

Top Detected Weaponized Vulnerabilities

# of detections	CVE	Product	RTI
1	CVE-2022-2856	Google Chrome	Weaponized, CISA
2	CVE-2022-41049	MS Windows	Weaponized, CISA
3	CVE-2022-4135	Google Chrome	CISA
4	CVE-2022-2294	Google Chrome	Weaponized, CISA, APT
5	CVE-2022-3075	Google Chrome	Weaponized, CISA
6	CVE-2022-30170	MS Windows	Weaponized, APT
7	CVE-2022-24521	MS Windows	Weaponized, CISA, APT, Ransomware, Malware
8	CVE-2022-26904	MS Windows	Weaponized, CISA
9	CVE-2022-37969	MS Windows	Weaponized, CISA
10	CVE-2022-1096	Google Chrome	Weaponized, CISA

TruRisk

TruRisk Eliminate

Qualys.

Patch Management (Remediation)

- ✓ Qualys Patch Management
- ✓ Jeff Huffman, Senior Director, IT Security and Administration - **New Orleans Saints**
- ✓ Panel:
  Haydur Agha, VP, Global InfoSec – **Sony Music**
  Nick Shimmen, Technical Consultant, CISO group
  Associated British Food

Mitigation

- ✓ Announcing Mitigation

How Qualys Patch Management helps Organizations Eliminate Risk?

(without replacing IT patching tools)

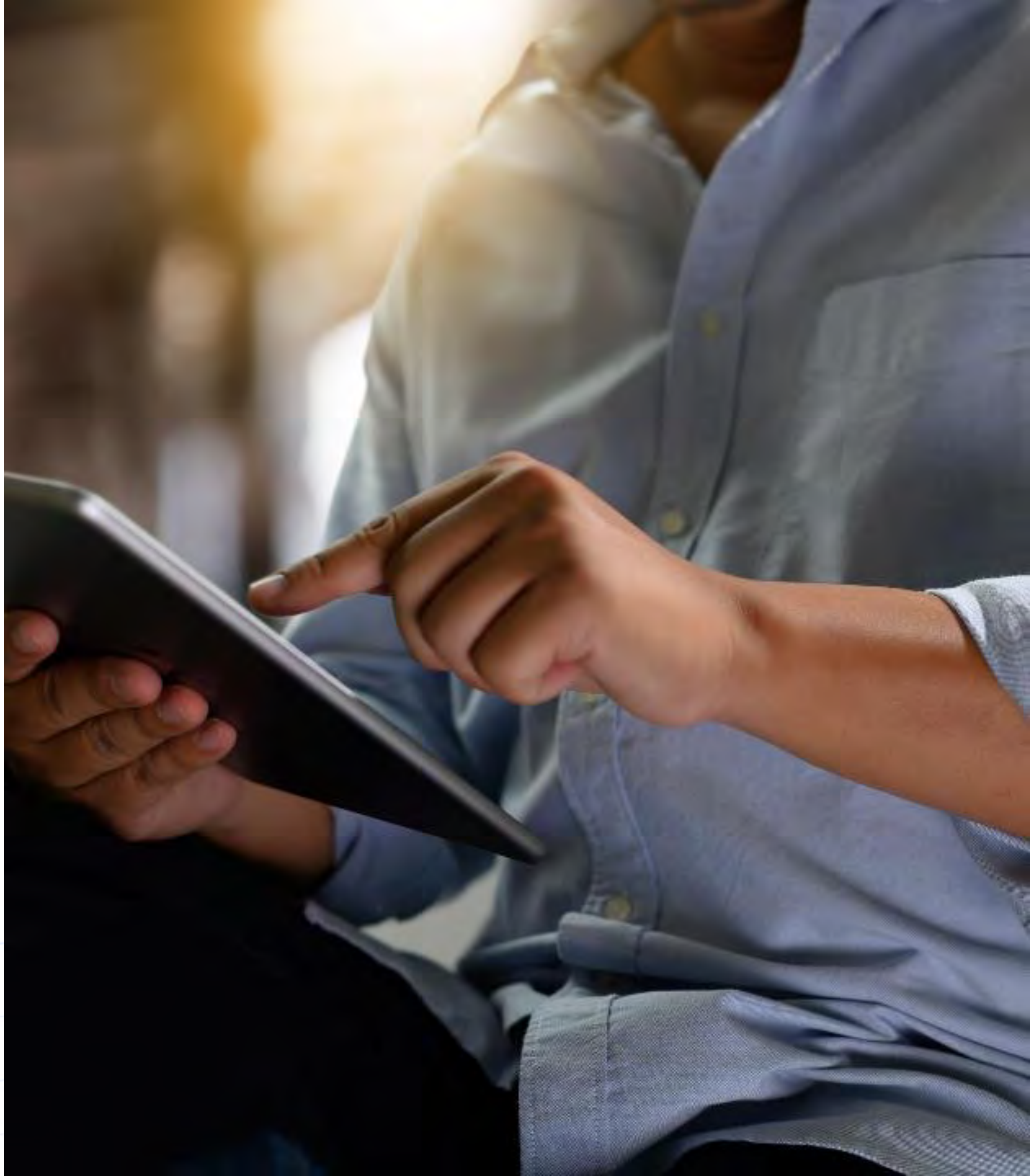
Qualys.

54M

Patches Deployed
Last Year

Smart Automation for your Low Hanging Fruits

Qualys.



Chrome: 2647
(2008-2023)

Firefox: 2131
(2003-2023)

Adobe

Adobe: 1530
(2004-2023)

iTunes: 613
(2005-2023)

VLC: 105
(2007-2022)

Smart Automation

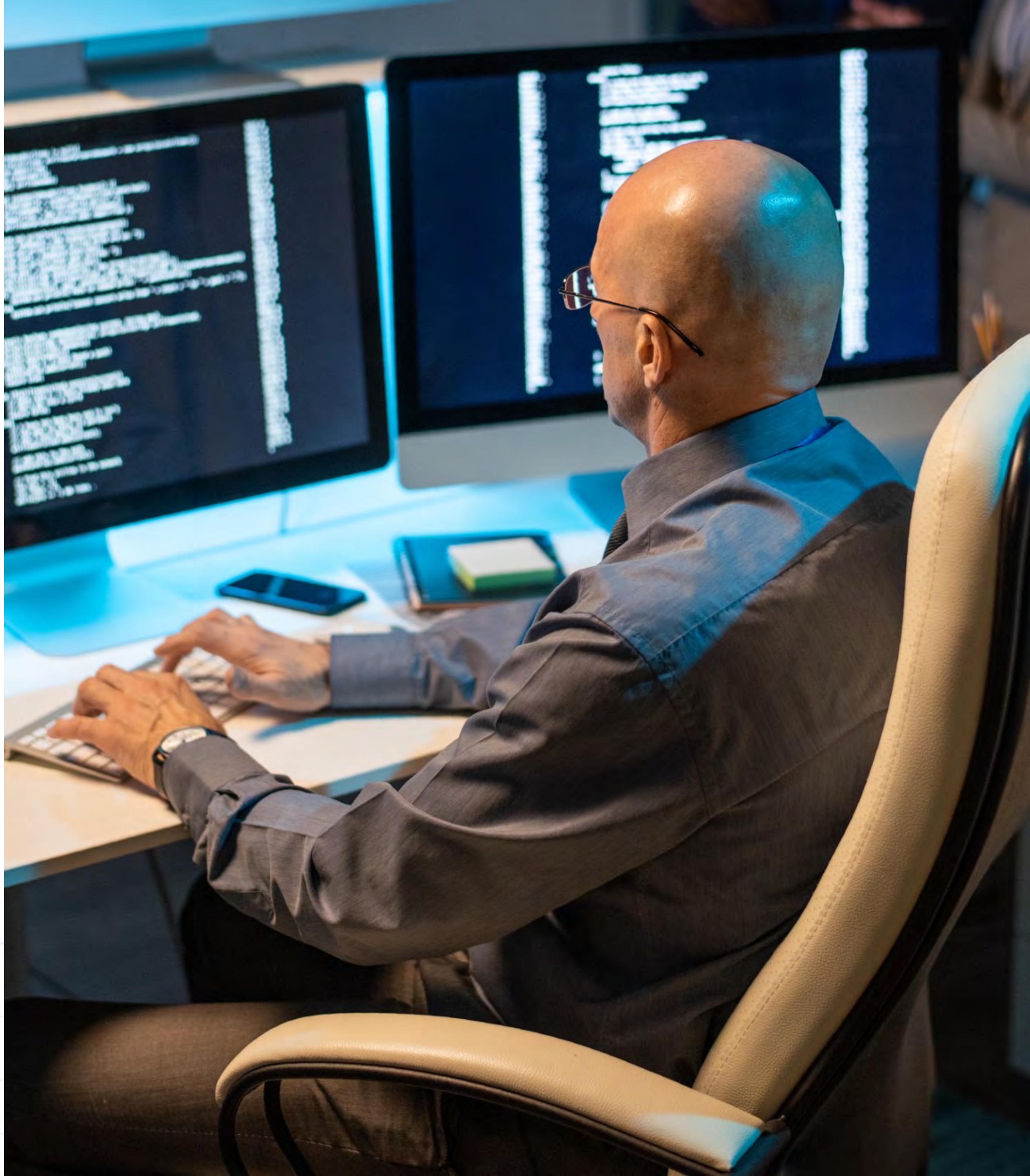
Automate Low Hanging Fruits: Make sure products that introduce low risk of breaking when patched are always up to date

Focus on High-Risk high Reward Products: identify products that introduce the most risk to your environment and focus on those first

Automate based on Risk where Possible: Automatically patch assets if a ransomware related vuln is detected, a CISA related one etc.

Simplify Remediation for the Measured Risk

Smart Automation



Qualys.

Vulnerability **Not** Equals a Patch

CVE-2021-34527 **“PrintNightmare”**

“In addition to installing the updates, in order to secure your system, you must confirm registry settings are set to 0”

Remediation = RegKey Change + Latest Patch

Smart Automation

Let the Product do the research for you: Find the right patches and configuration changes required to remediate vulnerabilities

Test, Approve, Deploy: fully integrated with current IT best practices & tools

Communicate Results: view results in your risk and vulnerabilities dashboards.

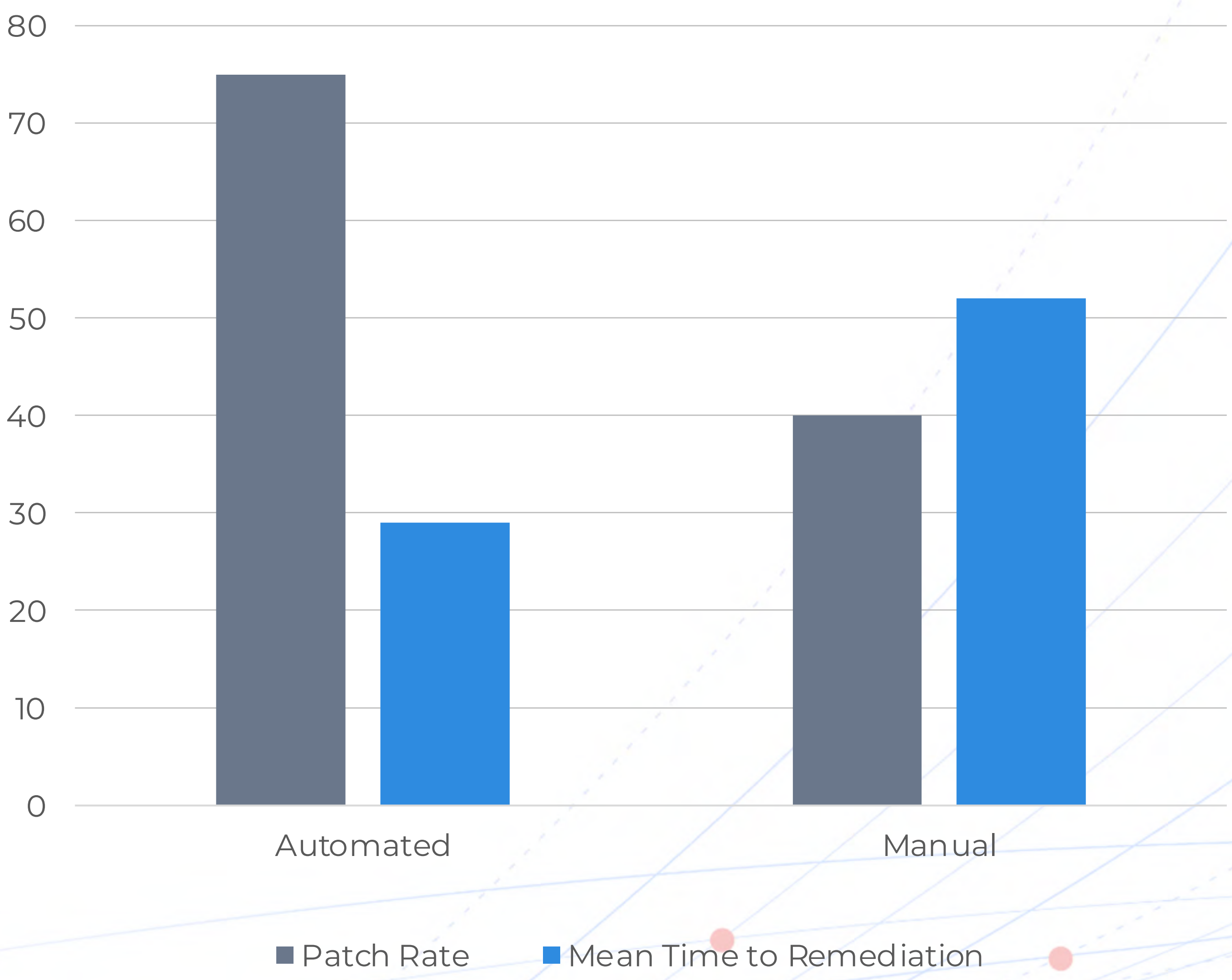
Automation is Key

89.5%

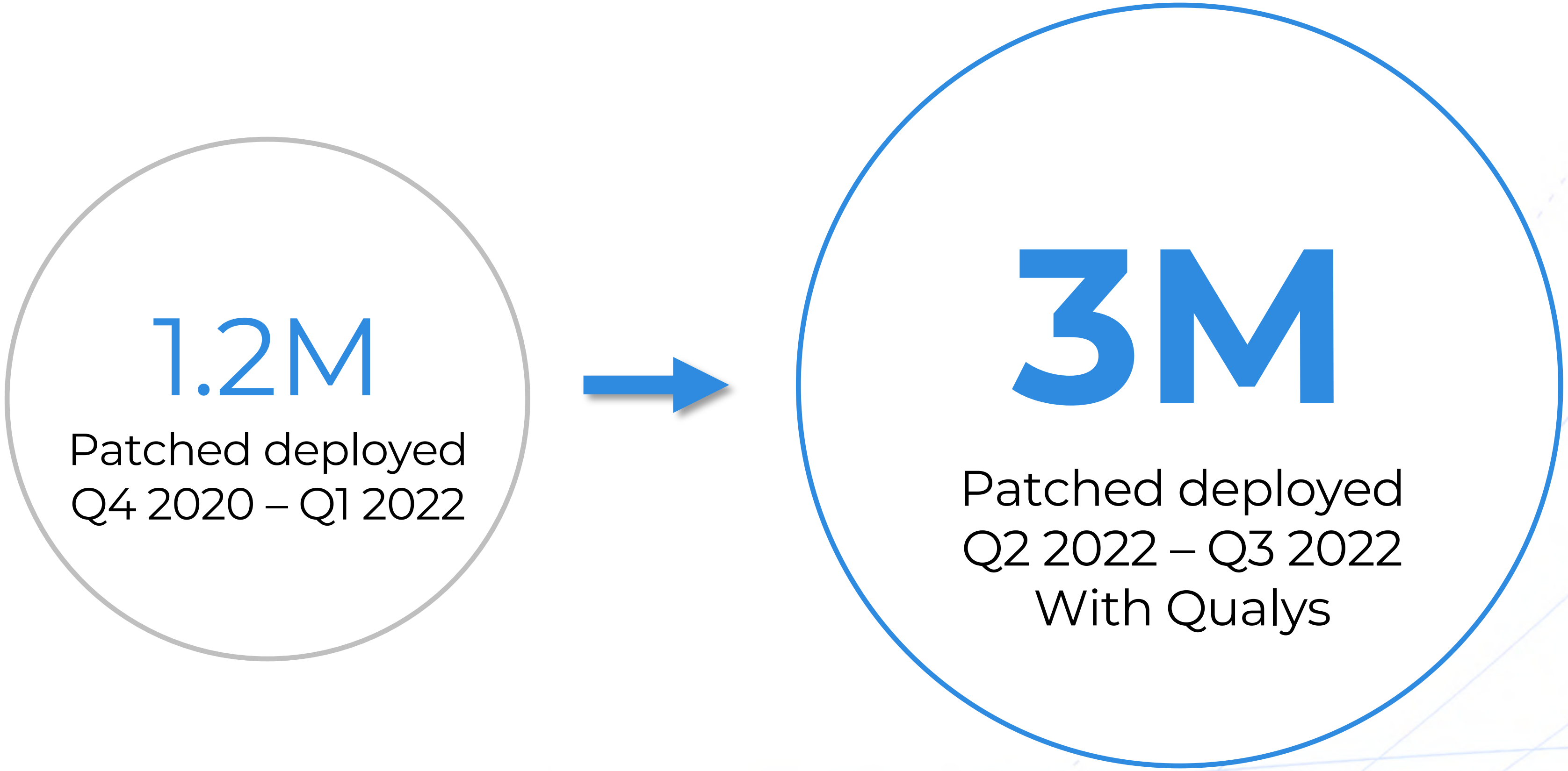
Improvement in Patching Rates

43.1%

Improvement in MTTR Speed



Customer's Real Risk Elimination



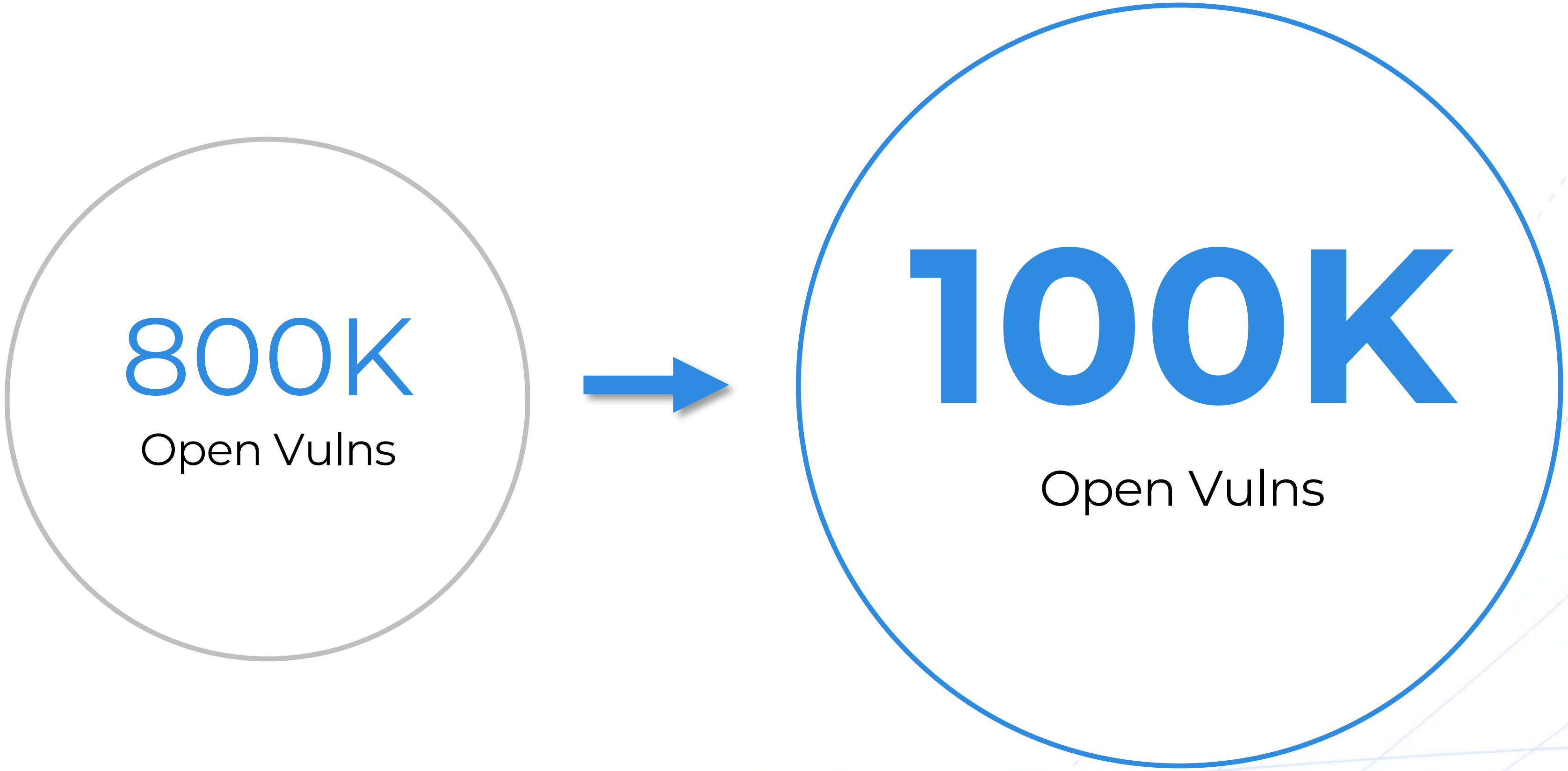
1.2M

Patched deployed
Q4 2020 – Q1 2022

3M

Patched deployed
Q2 2022 – Q3 2022
With Qualys

Customer's Real Risk Elimination: in a Month



800K

Open Vulns

100K

Open Vulns

Risk Elimination Across Multiple Attack Surfaces

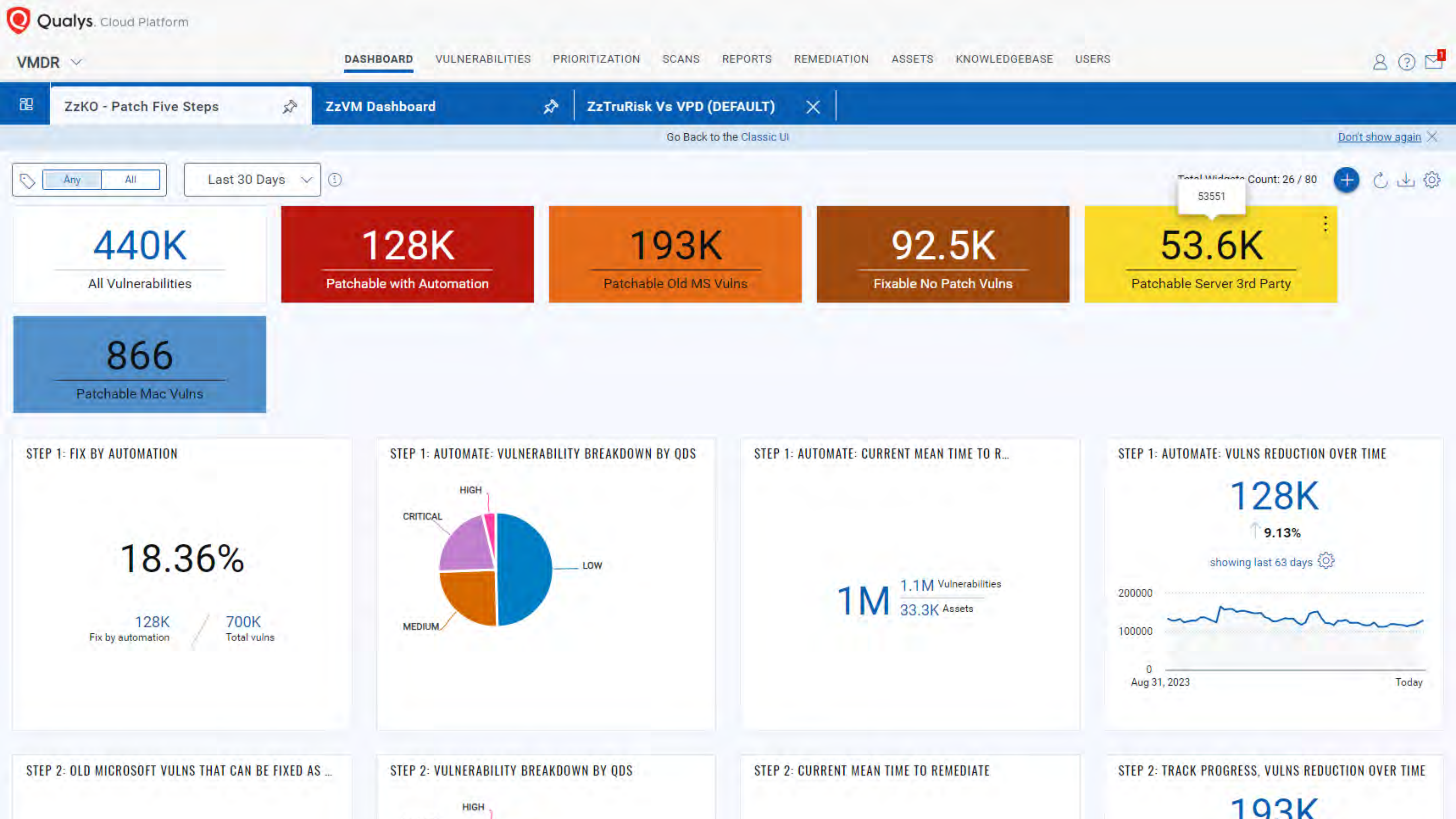
On-Prem Assets

Cloud Assets

Work From Home (WFH)
or Roaming Assets

5 Easy Steps for Eliminating your Risk by Complimenting your SCCM

Qualys.



440K
All Vulnerabilities

128K
Patchable with Automation

193K
Patchable Old MS Vulns

92.5K
Fixable No Patch Vulns

53.6K
Patchable Server 3rd Party

866
Patchable Mac Vulns

STEP 1: FIX BY AUTOMATION

18.36%

128K
Fix by automation

700K
Total vulns

STEP 1: AUTOMATE: VULNERABILITY BREAKDOWN BY QDS

STEP 1: AUTOMATE: CURRENT MEAN TIME TO R...

1M

1.1M Vulnerabilities

33.3K Assets

STEP 1: AUTOMATE: VULNS REDUCTION OVER TIME

128K

9.13%

showing last 63 days

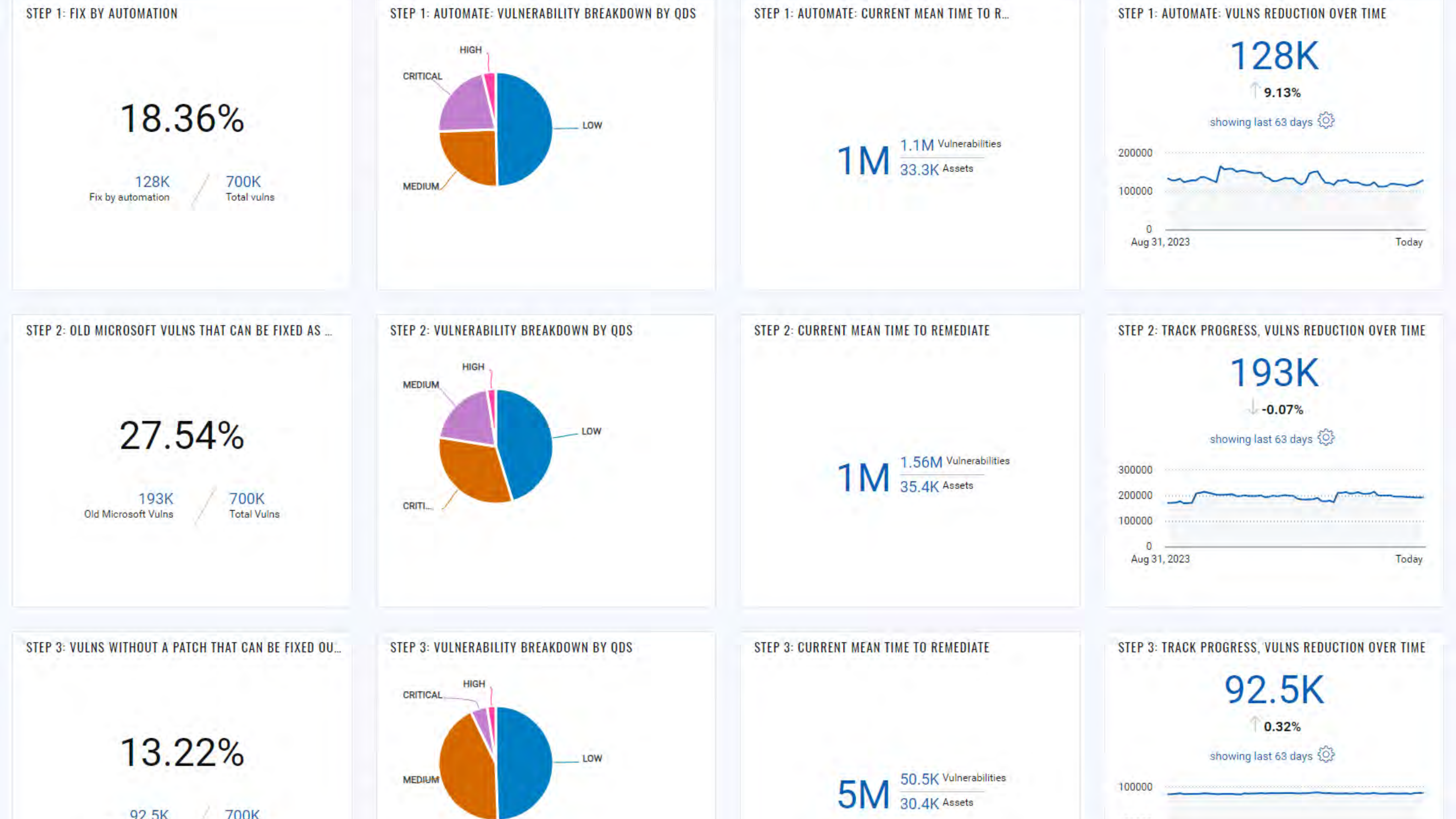
STEP 2: OLD MICROSOFT VULNS THAT CAN BE FIXED AS ...

STEP 2: VULNERABILITY BREAKDOWN BY QDS

STEP 2: CURRENT MEAN TIME TO REMEDIATE

STEP 2: TRACK PROGRESS, VULNS REDUCTION OVER TIME

193K



STEP 1: FIX BY AUTOMATION

18.36%

128K Fix by automation / 700K Total vulns

STEP 1: AUTOMATE: VULNERABILITY BREAKDOWN BY QDS

STEP 1: AUTOMATE: CURRENT MEAN TIME TO R...

1M 1.1M Vulnerabilities 33.3K Assets

STEP 1: AUTOMATE: VULNS REDUCTION OVER TIME

128K

↑ 9.13%

showing last 63 days

STEP 2: OLD MICROSOFT VULNS THAT CAN BE FIXED AS ...

27.54%

193K Old Microsoft Vulns / 700K Total Vulns

STEP 2: VULNERABILITY BREAKDOWN BY QDS

STEP 2: CURRENT MEAN TIME TO REMEDIATE

1M 1.56M Vulnerabilities 35.4K Assets

STEP 2: TRACK PROGRESS, VULNS REDUCTION OVER TIME

193K

↓ -0.07%

showing last 63 days

STEP 3: VULNS WITHOUT A PATCH THAT CAN BE FIXED OU...

13.22%

92.5K / 700K

STEP 3: VULNERABILITY BREAKDOWN BY QDS

STEP 3: CURRENT MEAN TIME TO REMEDIATE

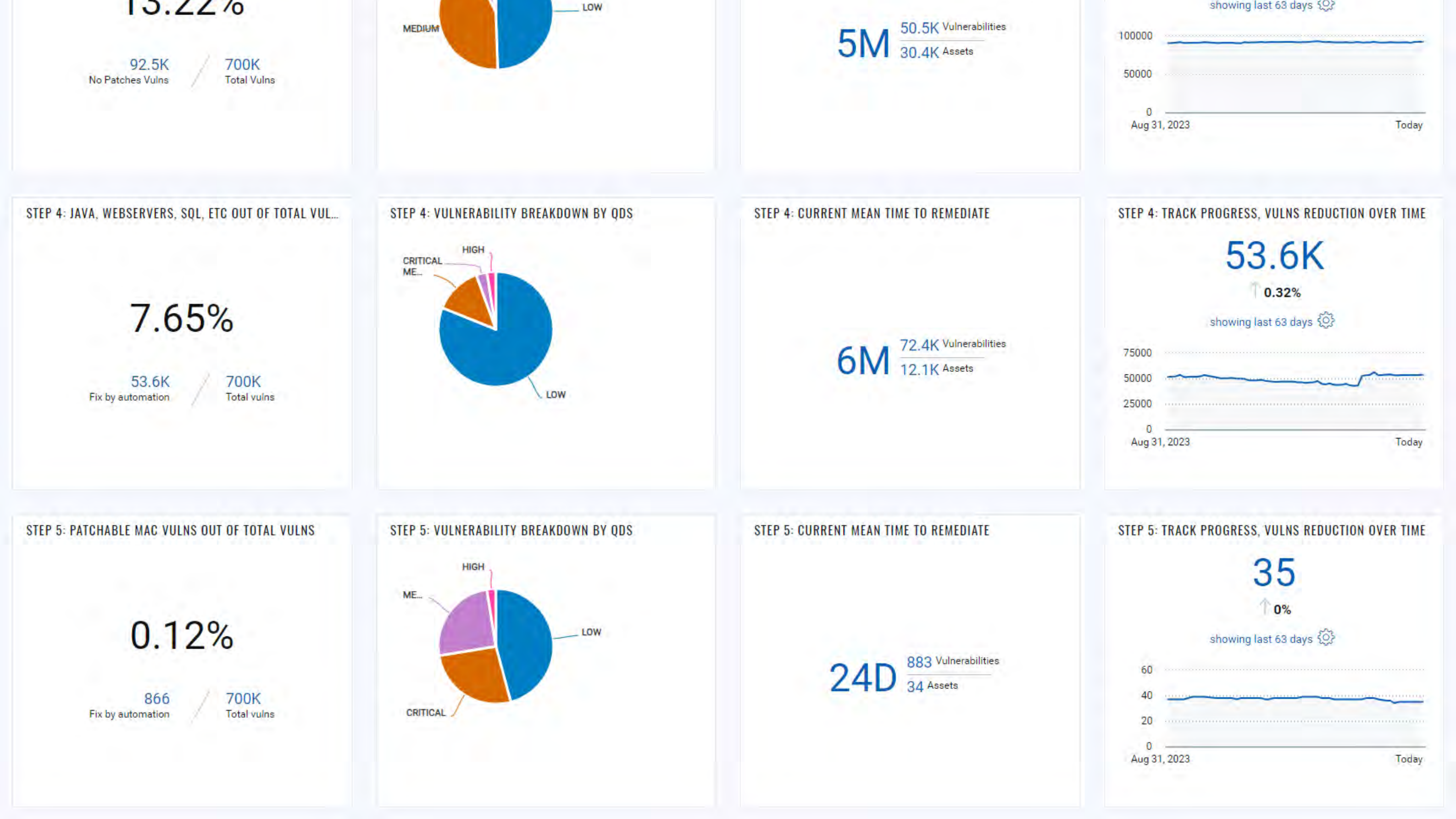
5M 50.5K Vulnerabilities 30.4K Assets

STEP 3: TRACK PROGRESS, VULNS REDUCTION OVER TIME

92.5K

↑ 0.32%

showing last 63 days



13.22%

92.5K No Patches Vulns / 700K Total Vulns

5M 50.5K Vulnerabilities 30.4K Assets

showing last 63 days

STEP 4: JAVA, WEBSERVERS, SQL, ETC OUT OF TOTAL VUL...

7.65%

53.6K Fix by automation / 700K Total vulns

STEP 4: VULNERABILITY BREAKDOWN BY QDS

STEP 4: CURRENT MEAN TIME TO REMEDIATE

6M 72.4K Vulnerabilities 12.1K Assets

STEP 4: TRACK PROGRESS, VULNS REDUCTION OVER TIME

53.6K

↑ 0.32%

showing last 63 days

STEP 5: PATCHABLE MAC VULNS OUT OF TOTAL VULNS

0.12%

866 Fix by automation / 700K Total vulns

STEP 5: VULNERABILITY BREAKDOWN BY QDS

STEP 5: CURRENT MEAN TIME TO REMEDIATE

24D 883 Vulnerabilities 34 Assets

STEP 5: TRACK PROGRESS, VULNS REDUCTION OVER TIME

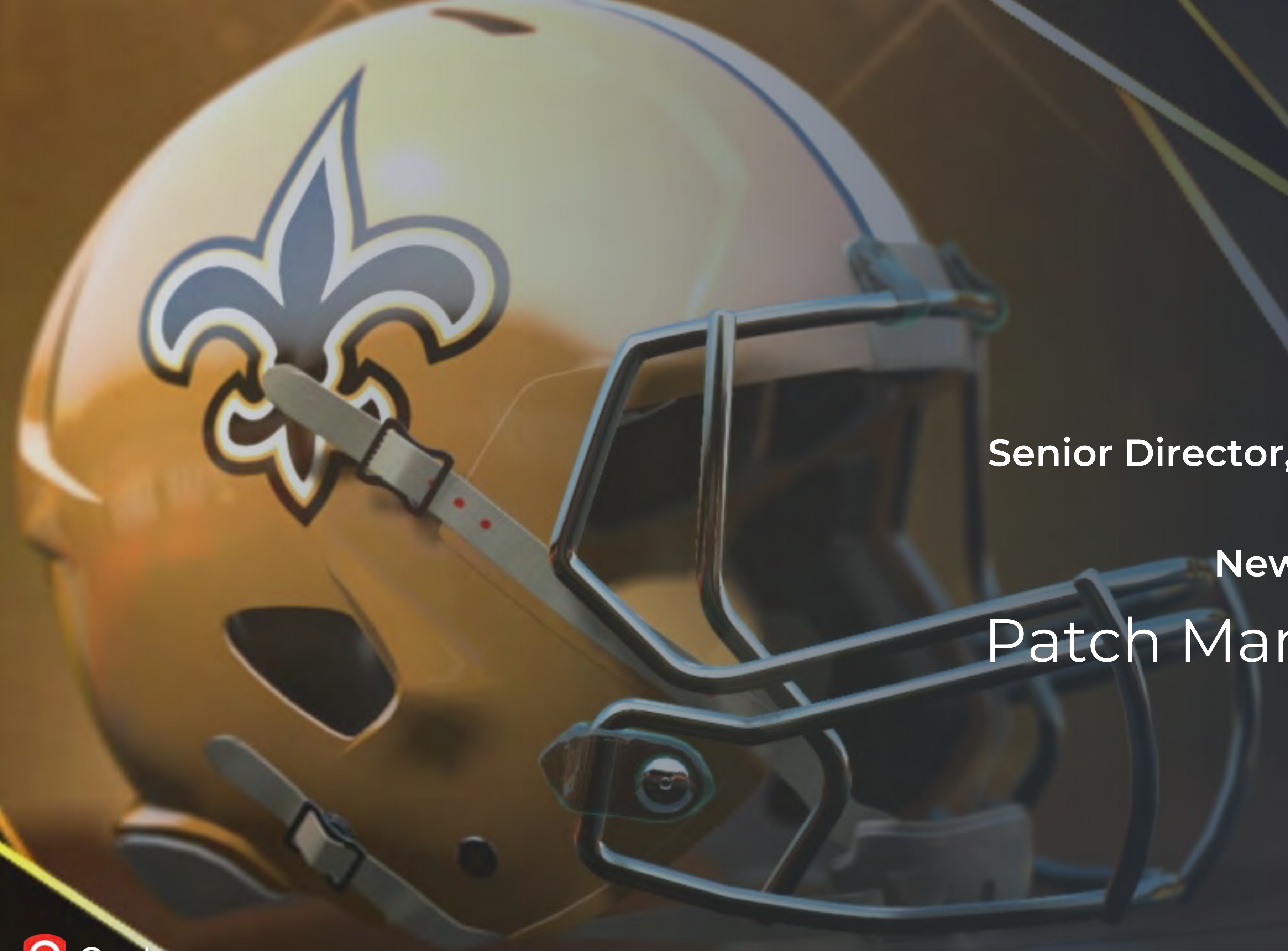
35

↑ 0%

showing last 63 days

Demo

Qualys.



Jeff Huffman

Senior Director, IT Security and Administration

New Orleans Saints

Patch Management

Real Value with Real ROI

SONY MUSIC

Haydur Agha,
VP, Cybersecurity

Associated British Foods plc

Nick Shimmen
Technical Consultant, CISO Group

Introducing TruRisk Eliminate with Mitigation

Qualys.

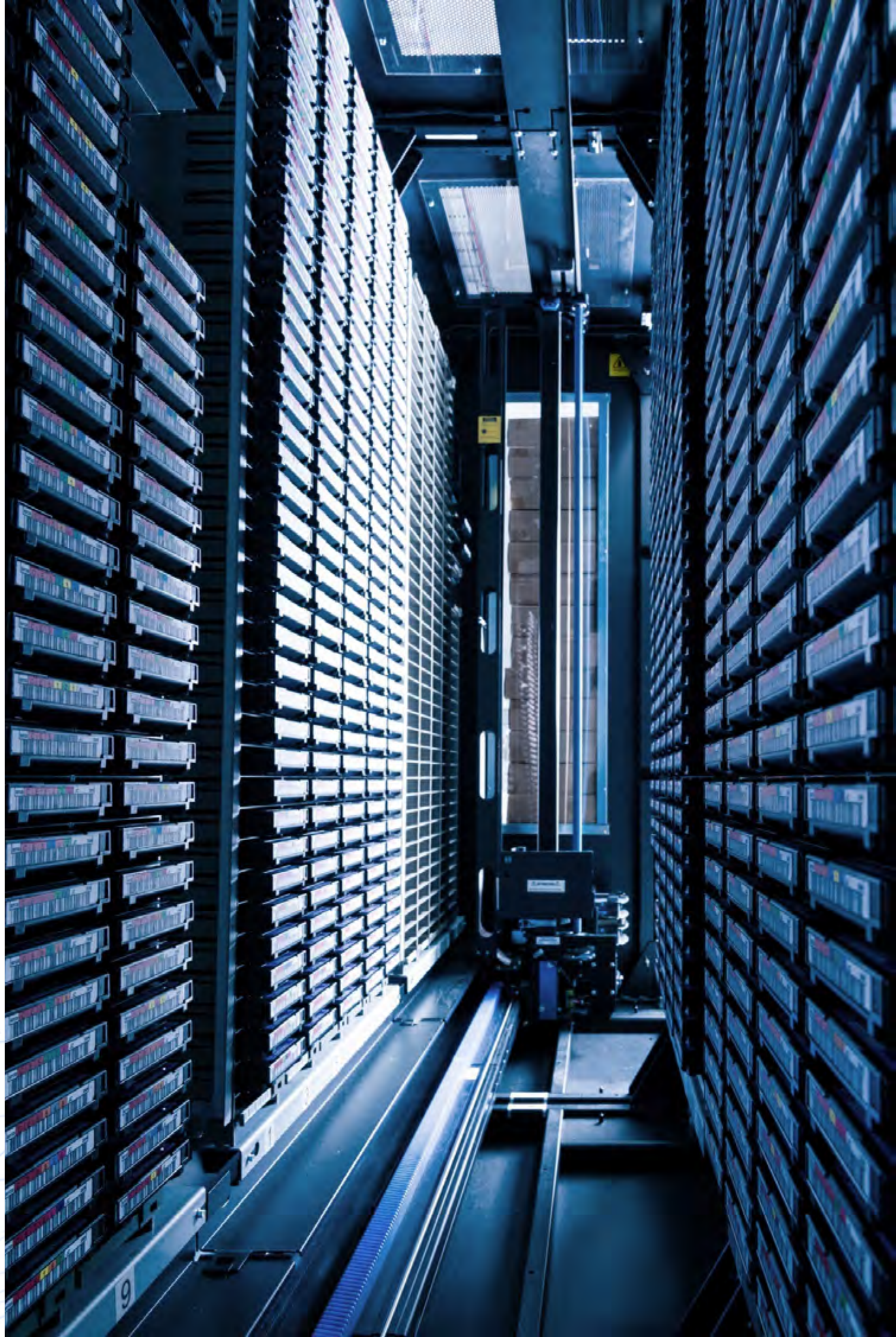
Critical Vuln Detected but, Patch Cannot be Deployed

Business Continuity: The **operational risk** of deploying the patch is too high

Cannot Wait for the Next Maintenance Window: a critical vuln has been released but the next maintenance window is in 2 month!

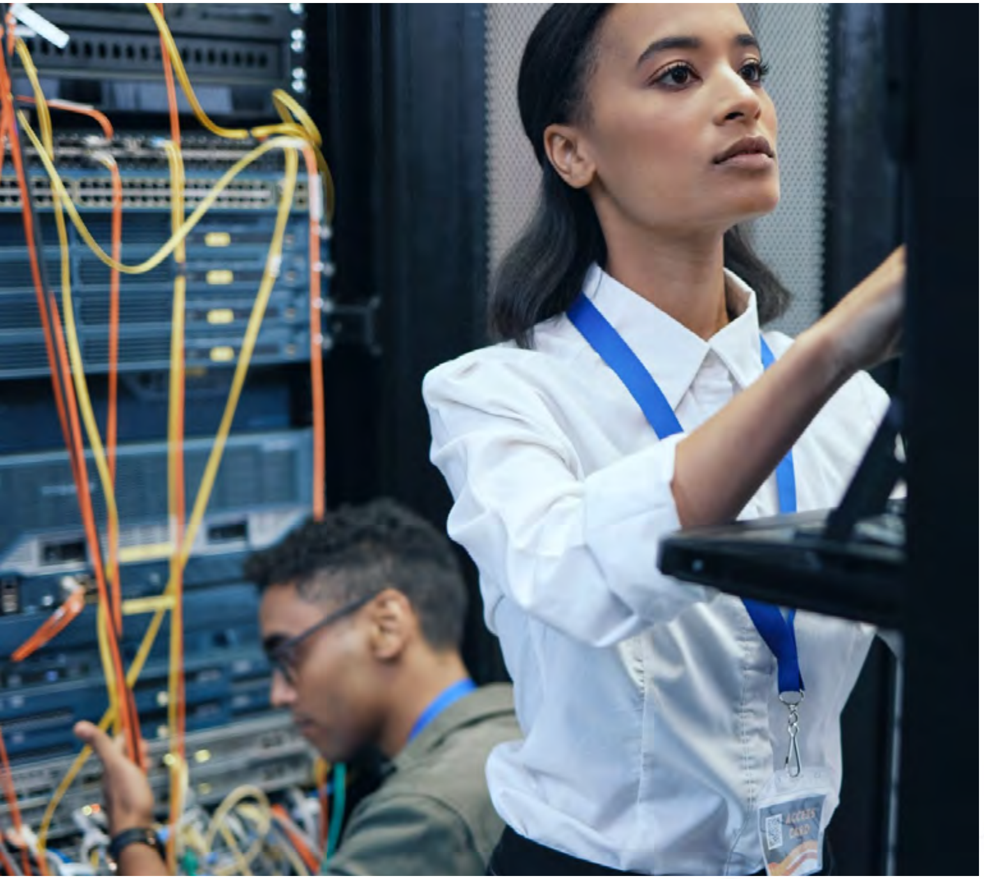
JDK 1.5 Only! Cannot update Java

Qualys.



Eliminate risk by applying the **right remediation** or **mitigation** action in the **context** of your business application.

REMEDIATION: Any action required to fix the risk completely as defined by the vendor.



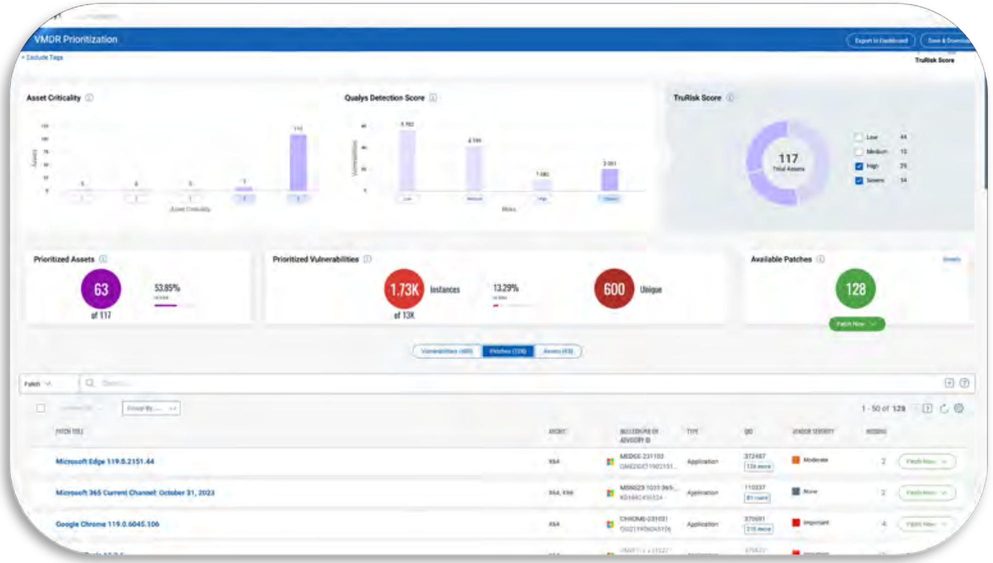
Patches

Deploy patches to the right devices, anywhere

Configuration Changes

Some vulns require conf changes for remediation – provide the visibility and apply

REMEDIATION: Any action required to fix the risk completely as defined by the vendor.



PATCH TITLE	ARCH	BULLETIN/KB OR ADVISORY ID	TYPE	QID	VENDOR SEVERITY	MISSING	
Microsoft Edge 119.0.2151.44	X64	MEDGE-231103	Application	372487 124 more	Moderate	2	Patch Now
Microsoft 365 Current Channel: October 31, 2023	X64, X86	MS0023-1031 365-	Application	110337 81 more	None	2	Patch Now
Google Chrome 119.0.6045.106	X64	CHROME-231031	Application	376691 215 more	Important	4	Patch Now

RIGHT Patches

Deploy the right patches to the right devices, anywhere

RIGHT Configuration Changes

Some vulns require conf changes for remediation – provide the visibility and apply

MITIGATION: Qualys researched alternatives to remediation

RIGHT Mitigation Actions

- Block port
- Isolate
- Restrict access
- Stop services
- Update network devices, firewalls, IPS etc
- Update cloud network polices
- Etc

RIGHT Virtual Patch

In-memory protect a vulnerable asset

Qualys.

80

Weaponized Vulns in 2023

90%

Mitigated By Virtual Patch

5%

Mitigated by Process Stop

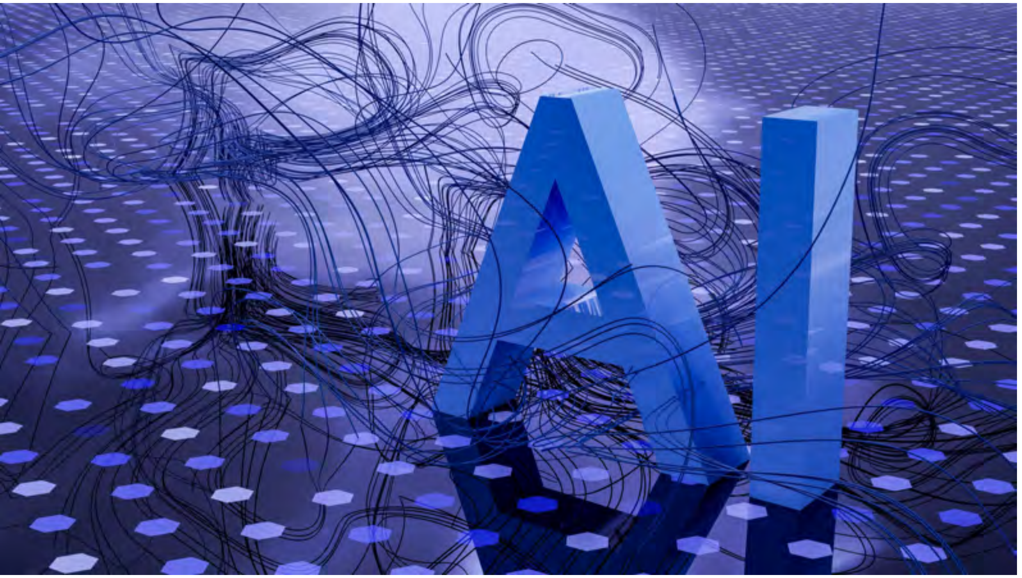
42%

Mitgated by Port Block

14%

Mitigated By File Access Control

TruRisk Eliminate: Powered by AI



Reliability Analysis

Suggest best actions based on contextual historical patch and mitigation reliability

Learn from Others

Learn the operational impact of deploying patches & mitigations to similar customer's environments and suggest the best action

Automation

Automate where operational risk is minimal

Qualys.

Demo

Qualys.

TruRisk Eliminate

RIGHT Remediation or Mitigations: Based on Qualys research team

Test, Approve, Deploy: the remediation or mitigation actions that fits your needs

Fully Integrate: into Qualys TruRisk Platform

Smart Automation: ensure software is always up-to-date or mitigate new weaponized vulns automatically before patch is deployed

Works with your current IT tools: work with your SCCM, rollback mitigation when patch deployed etc.

Qualys.

TruRisk

TruRisk Eliminate

Mitigation Management

- ✓ Available Q2 2024!
- ✓ Accepting Design Partners Starting TODAY!

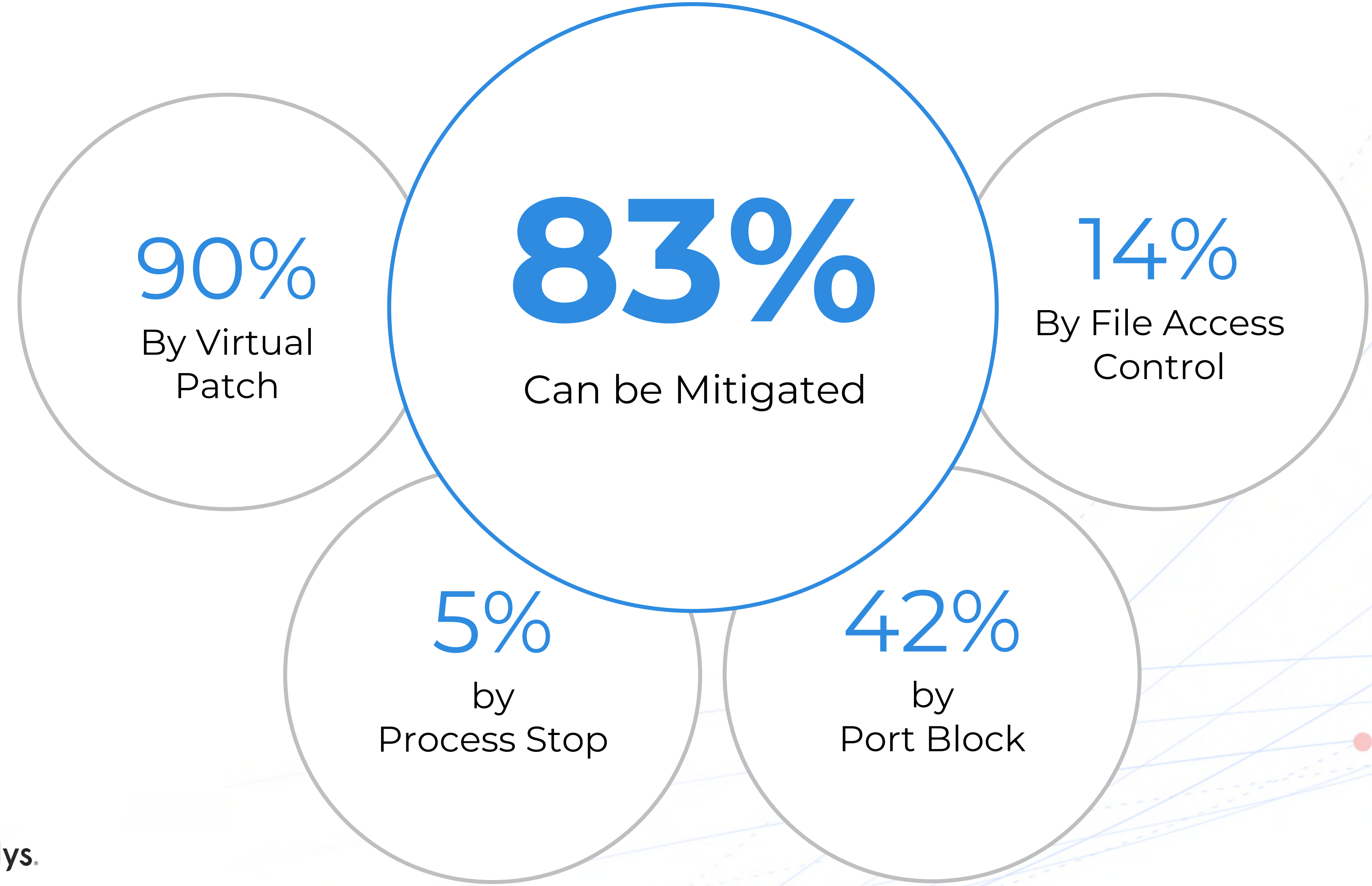
Patch Management (Remediation)

- ✓ Already Available!

Qualys.

QSC23

96 Weaponized vulns in 2023



83%

Can be Mitigated

90%

By Virtual Patch

14%

By File Access Control

5%

by Process Stop

42%

by Port Block

REMEDIATION: Any action required to fix the risk completely as defined by the vendor.

Patches

Deploy patches to the right devices, anywhere

Configuration Changes

Some vulns require conf changes for remediation – provide the visibility and apply

Qualys.

TruRisk

TruRisk Eliminate

Mitigation Management

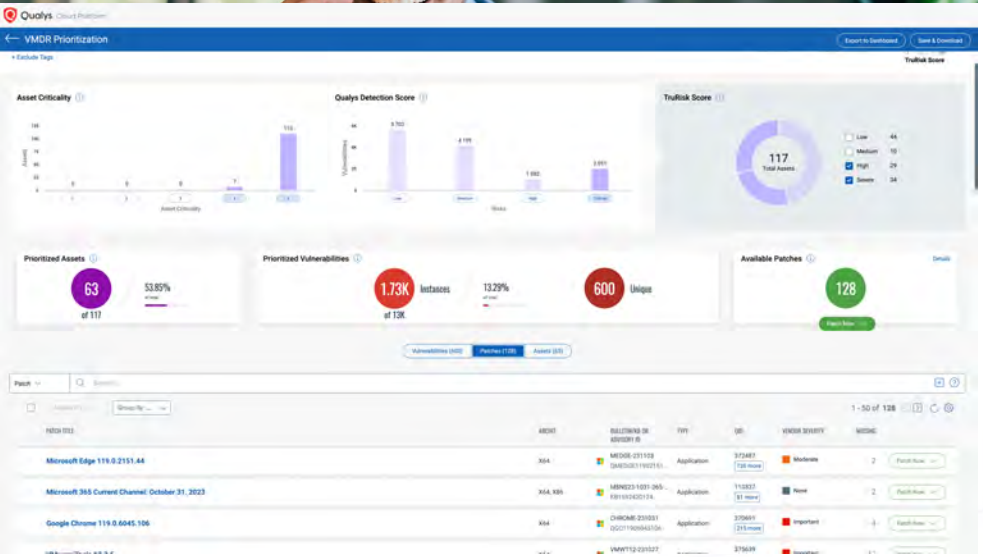
- ✓ Virtual patching
- ✓ Contextual Mitigation Actions
- ✓ Block ports
- ✓ Kill processes
- ✓ Etc

Patch Management (Remediation)

- ✓ Deploy patches & conf changes
- ✓ Already Available!

Qualys.

REMEDIATION: Any action required to fix the risk completely as defined by the vendor.



PATCH TITLE	ARCH	BULLETIN/KB OR ADVISORY ID	TYPE	QID	VENDOR SEVERITY	MISSING	
Microsoft Edge 119.0.2151.44	X64	MEDGE-231103 QMEDGE11902151...	Application	372487 128 more	Moderate	2	Patch Now
Microsoft 365 Current Channel: October 31, 2023	X64, X86	MSNS23-1031-365... KB1692420124...	Application	113837 81 more	None	2	Patch Now
Google Chrome 119.0.6045.106	X64	CHROME-231031 QGC1190604510...	Application	370691 215 more	Important	4	Patch Now
[illegible]	[illegible]	VMWT12-231027	[illegible]	375639	[illegible]	[illegible]	

RIGHT Patches

Deploy the right patches to the right devices, anywhere

RIGHT Configuration Changes

Some vulns require conf changes for remediation – provide the visibility and apply

Qualys.

Real World Risk Elimination

Customers

Within few days of POC: 40% risk reduction in CISA vulns and 32% in 80+ QDS

Patched installed without Qualys Q4 2020 – Q1 2022 = **1.2M**

Patches installed with Qualys Patch Q2 2022 – Q3 2022 **= 3M**

From 800K to 100K in a month

Reduced avg number of vulns per Windows 10 device by 90%

Qualys.

Vulnerability **Not** Equals a Patch

CVE-2021-34527 **"PrintNightmare"**

"In addition to installing the updates, in order to secure your system, you must confirm registry settings are set to 0"

Remediation = RegKey Change + Latest Patch

250K

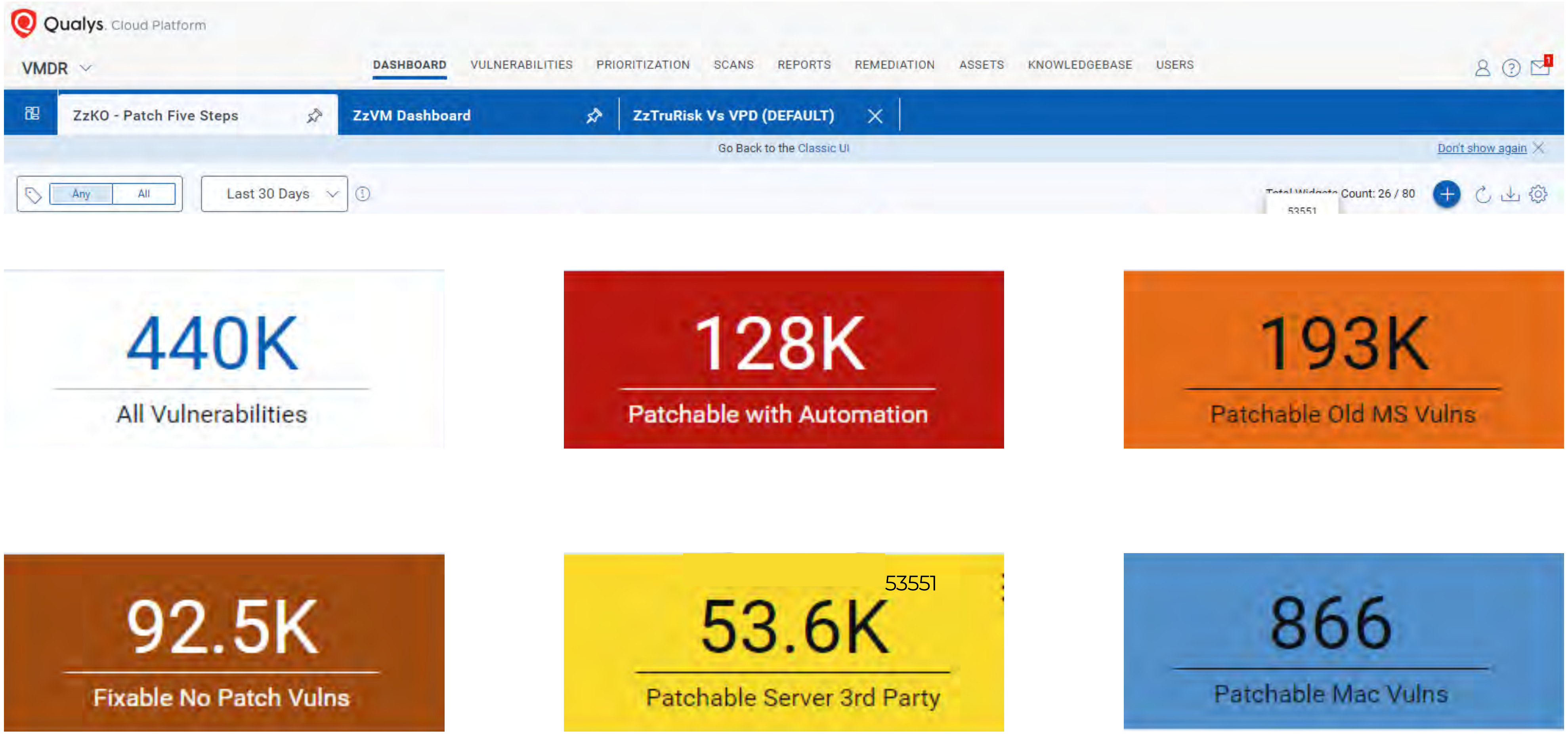
Active Jobs

54M

Patches Deployed
Last Year

11K

Smart Automation,
Zero Touch Jobs



440K
All Vulnerabilities

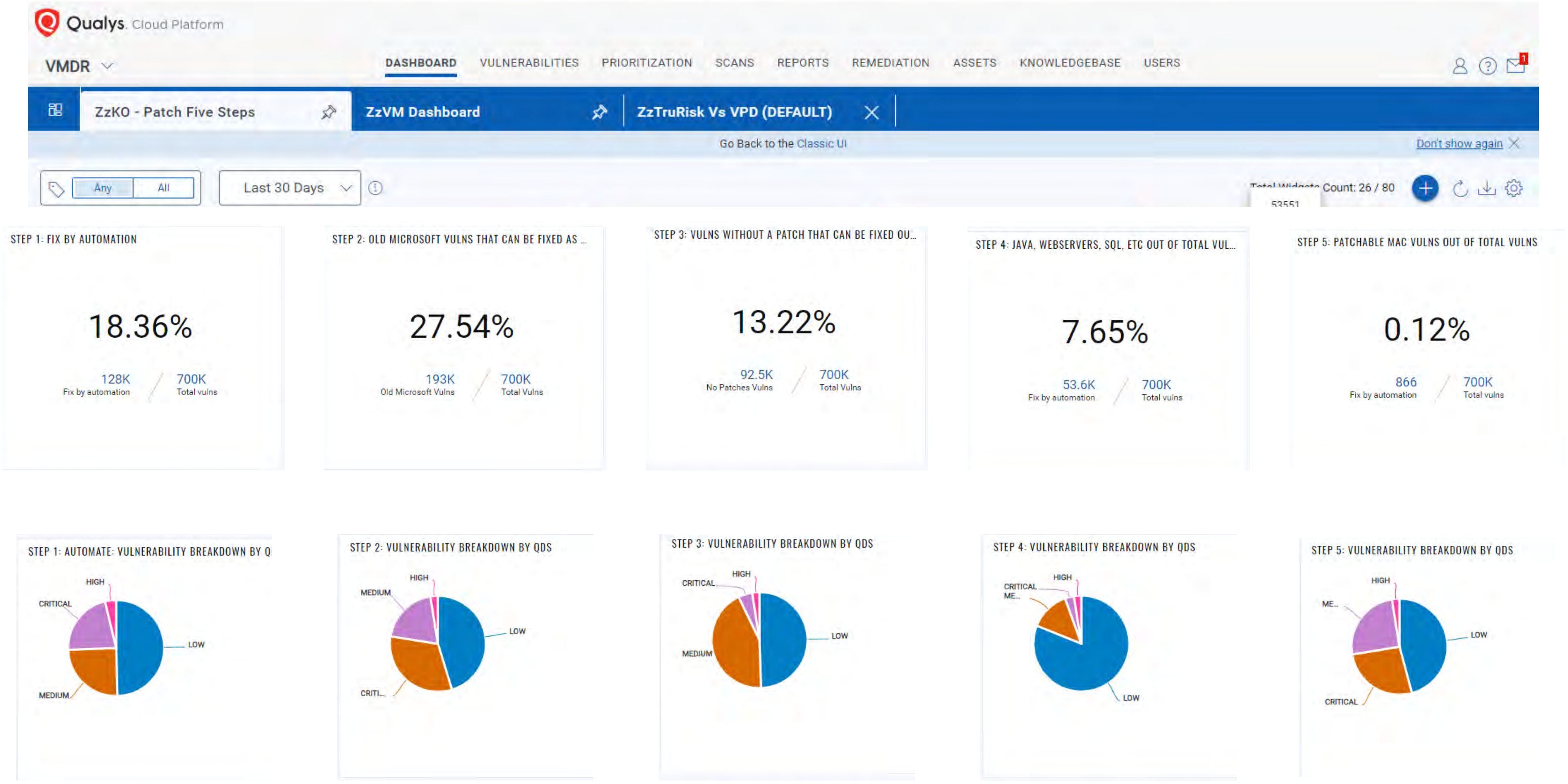
128K
Patchable with Automation

193K
Patchable Old MS Vulns

92.5K
Fixable No Patch Vulns

53551
53.6K
Patchable Server 3rd Party

866
Patchable Mac Vulns



STEP 1: FIX BY AUTOMATION

18.36%

128K Fix by automation / 700K Total vulns

STEP 2: OLD MICROSOFT VULNS THAT CAN BE FIXED AS ...

27.54%

193K Old Microsoft Vulns / 700K Total Vulns

STEP 3: VULNS WITHOUT A PATCH THAT CAN BE FIXED OU...

13.22%

92.5K No Patches Vulns / 700K Total Vulns

STEP 4: JAVA, WEBSERVERS, SQL, ETC OUT OF TOTAL VUL...

7.65%

53.6K Fix by automation / 700K Total vulns

STEP 5: PATCHABLE MAC VULNS OUT OF TOTAL VULNS

0.12%

866 Fix by automation / 700K Total vulns

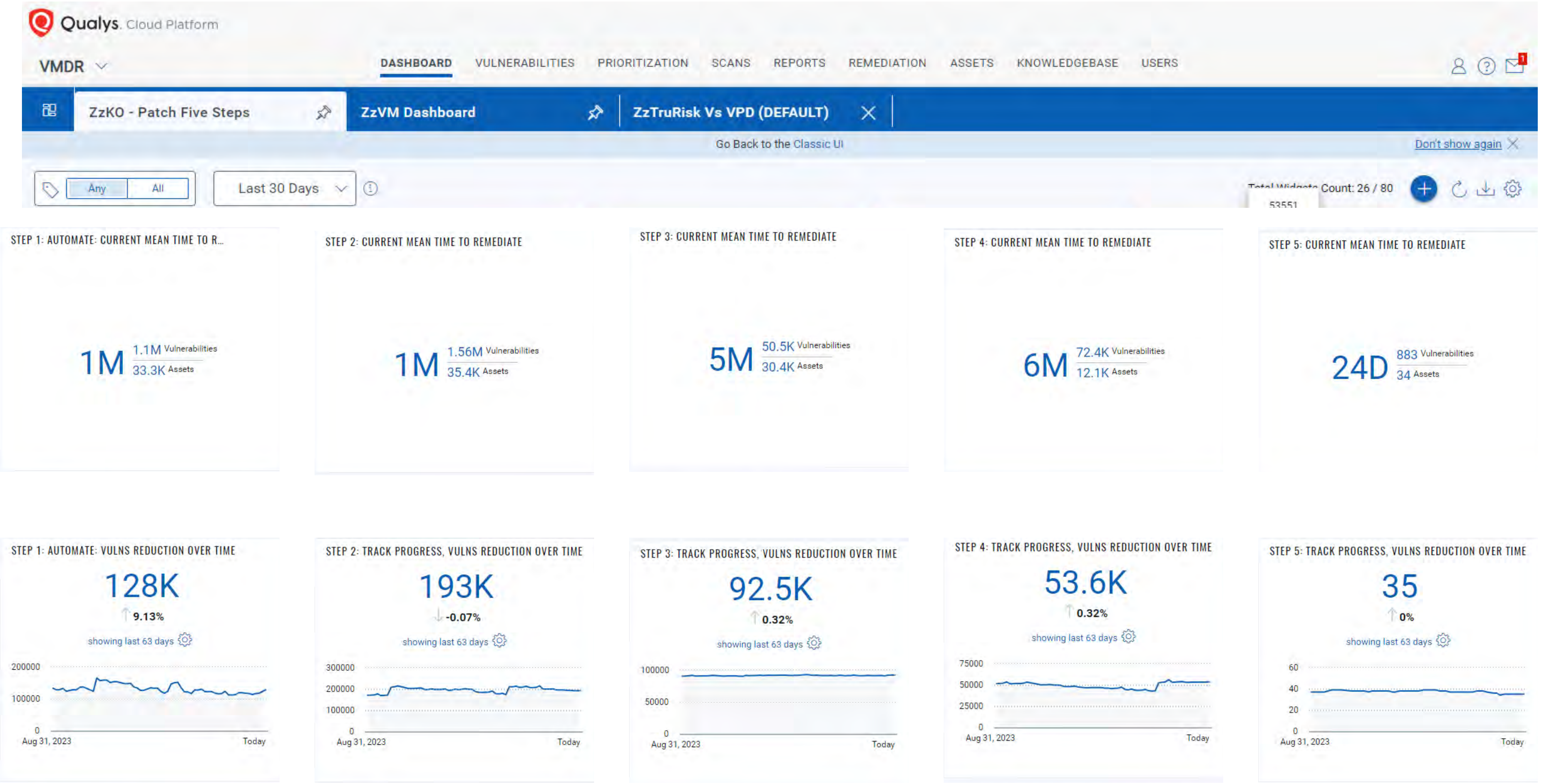
STEP 1: AUTOMATE: VULNERABILITY BREAKDOWN BY Q

STEP 2: VULNERABILITY BREAKDOWN BY QDS

STEP 3: VULNERABILITY BREAKDOWN BY QDS

STEP 4: VULNERABILITY BREAKDOWN BY QDS

STEP 5: VULNERABILITY BREAKDOWN BY QDS



Go Back to the Classic UI

Don't show again

STEP 1: AUTOMATE: CURRENT MEAN TIME TO R...

1M 1.1M Vulnerabilities 33.3K Assets

STEP 2: CURRENT MEAN TIME TO REMEDIATE

1M 1.56M Vulnerabilities 35.4K Assets

STEP 3: CURRENT MEAN TIME TO REMEDIATE

5M 50.5K Vulnerabilities 30.4K Assets

STEP 4: CURRENT MEAN TIME TO REMEDIATE

6M 72.4K Vulnerabilities 12.1K Assets

STEP 5: CURRENT MEAN TIME TO REMEDIATE

24D 883 Vulnerabilities 34 Assets

STEP 1: AUTOMATE: VULNS REDUCTION OVER TIME

128K

↑ 9.13%

showing last 63 days

STEP 2: TRACK PROGRESS, VULNS REDUCTION OVER TIME

193K

↓ -0.07%

showing last 63 days

STEP 3: TRACK PROGRESS, VULNS REDUCTION OVER TIME

92.5K

↑ 0.32%

showing last 63 days

STEP 4: TRACK PROGRESS, VULNS REDUCTION OVER TIME

53.6K

↑ 0.32%

showing last 63 days

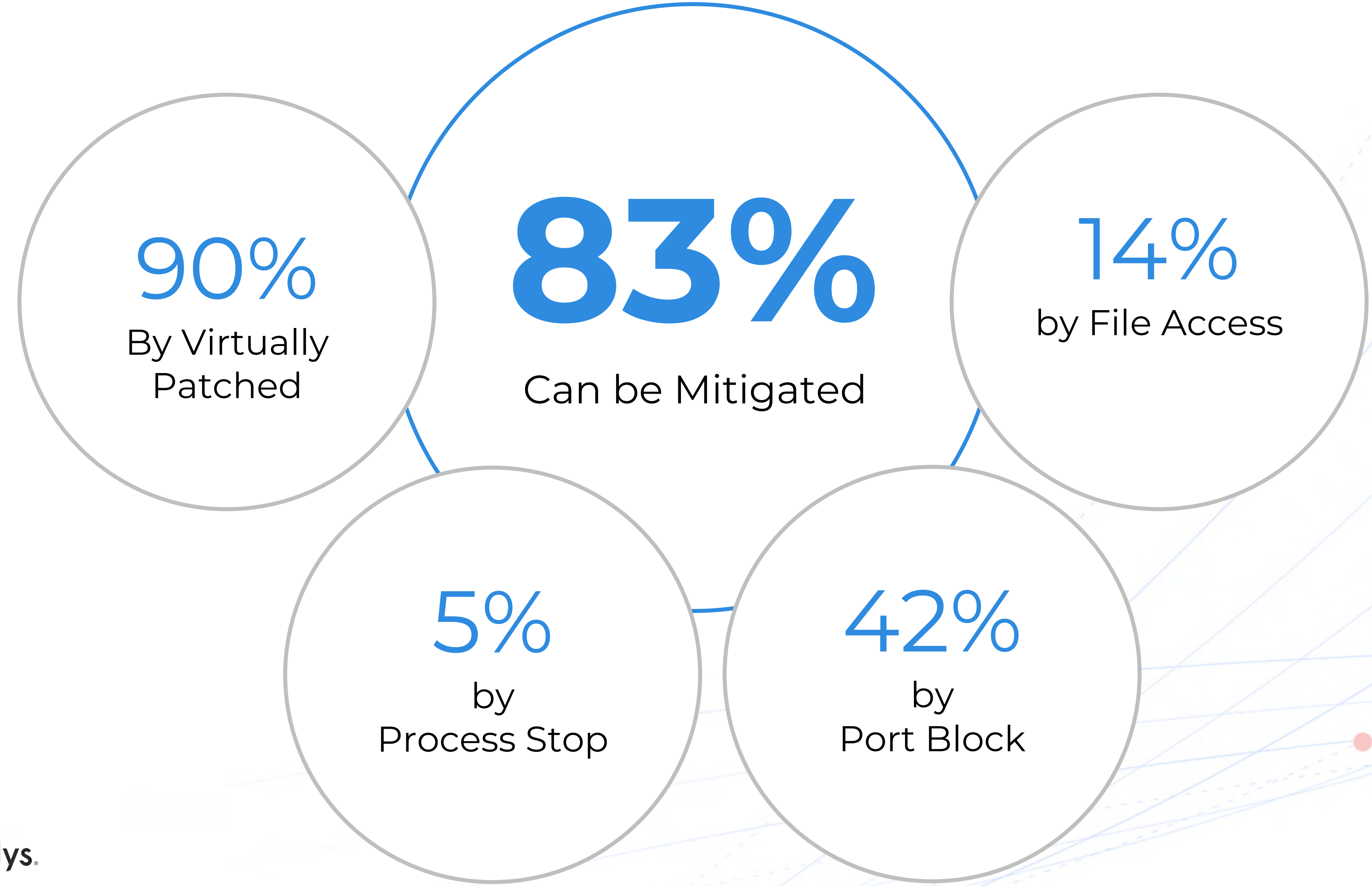
STEP 5: TRACK PROGRESS, VULNS REDUCTION OVER TIME

35

↑ 0%

showing last 63 days

96 Weaponized vulns in 2023



83%

Can be Mitigated

90%

By Virtually Patched

14%

by File Access

5%

by Process Stop

42%

by Port Block

96 Weaponized vulns in 2023

83%

Coverage

90%

Virtual Patch

5%

Process Stop

100%

Qualys Guarantees

42%

Block Ports

14%

File Mitigation

96 Weaponized vulns in 2023

83% Coverage	**90%** Virtual Patch	**5%** Process Stop
100% Qualys Guarantees	**42%** Block Ports	**14%** File Mitigation

Qualys.