Remediating the Nightmares: Preparing to Reduce Risk Comprehensively with TruRisk Eliminate

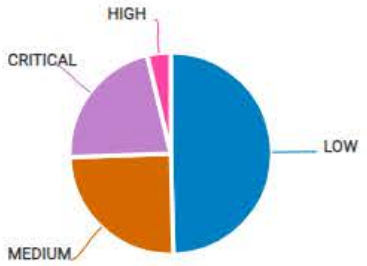
Eran Livne
Sr Director Product Management

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 C...

27.54%

193K Old Microsoft Vulns / 7... Total vulns

How can we be more efficient?

...CK PROGRESS, VULNS REDUCTION OVER TIME

193K

-0.07%

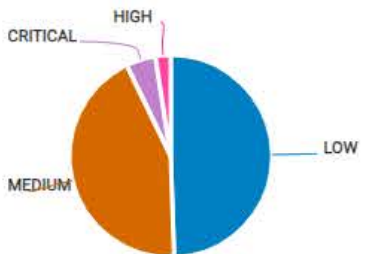
showing last 63 days

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

GUIDANCE

Vulnerability management

This area provides advice, guidance and other resources aimed specifically at those with an interest in vulnerability management.

1. Put in place a policy to update by default

Apply updates as soon as possible, and ideally automatically, in line with our best-practice timescales.

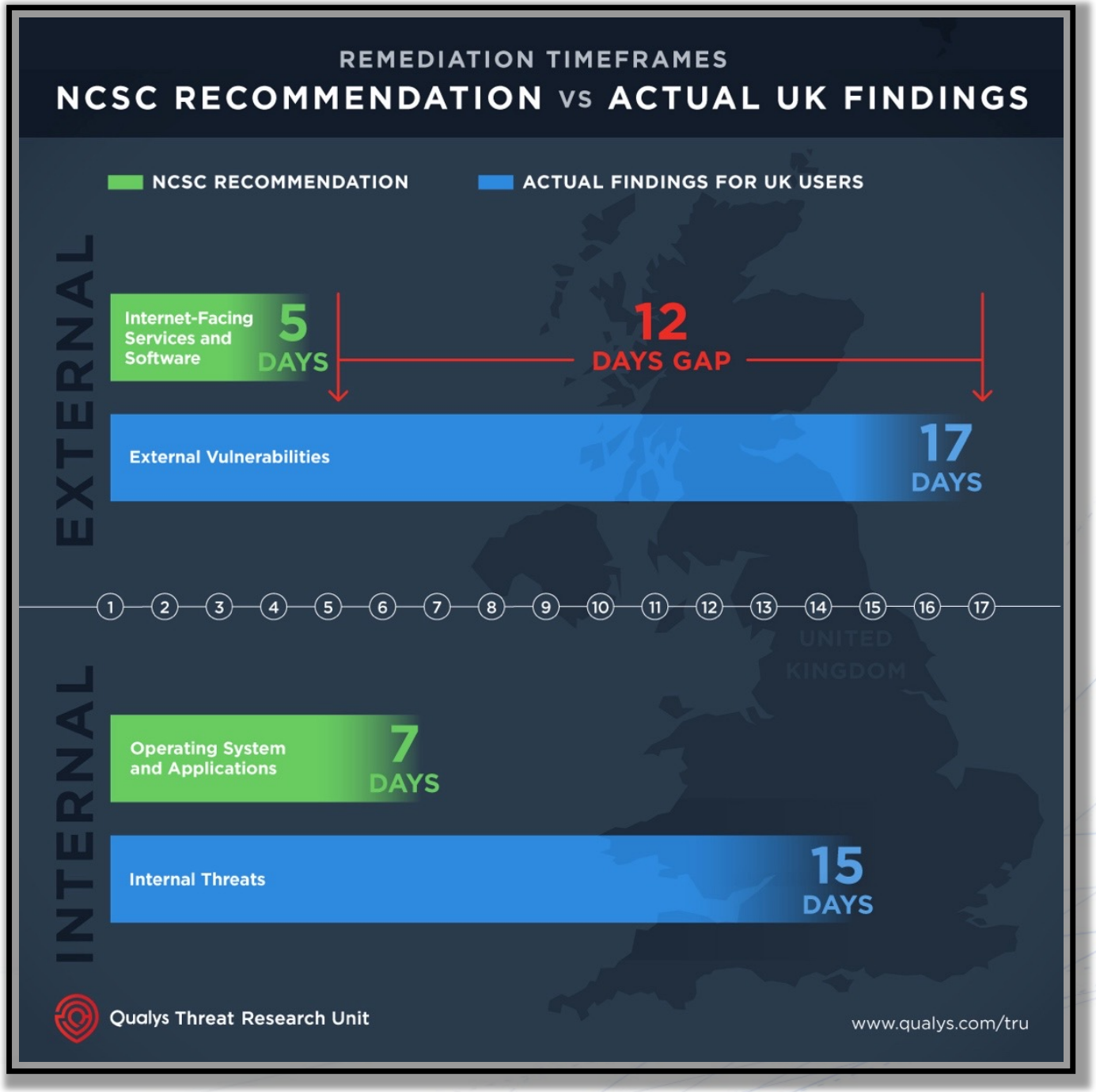
Thinking behind this principle

Installing the latest updates is critical to ensuring the security of your estate. **You should put in place a policy to update by default, where you always apply software updates as soon as possible, and ideally automatically.** This should be at the core of your update

National Cyber Security Centre

Type of estate	Rollout	Update completed within
Internet-facing services and software	Install on test environment or backup first. Test and rollout (a phased rollout can be used if applicable).	5 days
Operating system and applications	These updates should be applied automatically, as soon as an update is published. Phased rollout, for example 10% of the estate updated per day. Pause/rollback if issues encountered.	7 days
Internal/air-gapped service and software	Install on test environment or backup first. Test and rollout.	14 days

Qualys.


REMEDIATION TIMEFRAMES
NCSC RECOMMENDATION vs ACTUAL UK FINDINGS
NCSC RECOMMENDATION
ACTUAL FINDINGS FOR UK USERS
EXTERNAL
Internet-Facing Services and Software
5 DAYS
12 DAYS GAP
External Vulnerabilities
17 DAYS
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17
INTERNAL
Operating System and Applications
7 DAYS
Internal Threats
15 DAYS
UNITED KINGDOM
Qualys Threat Research Unit
www.qualys.com/tru

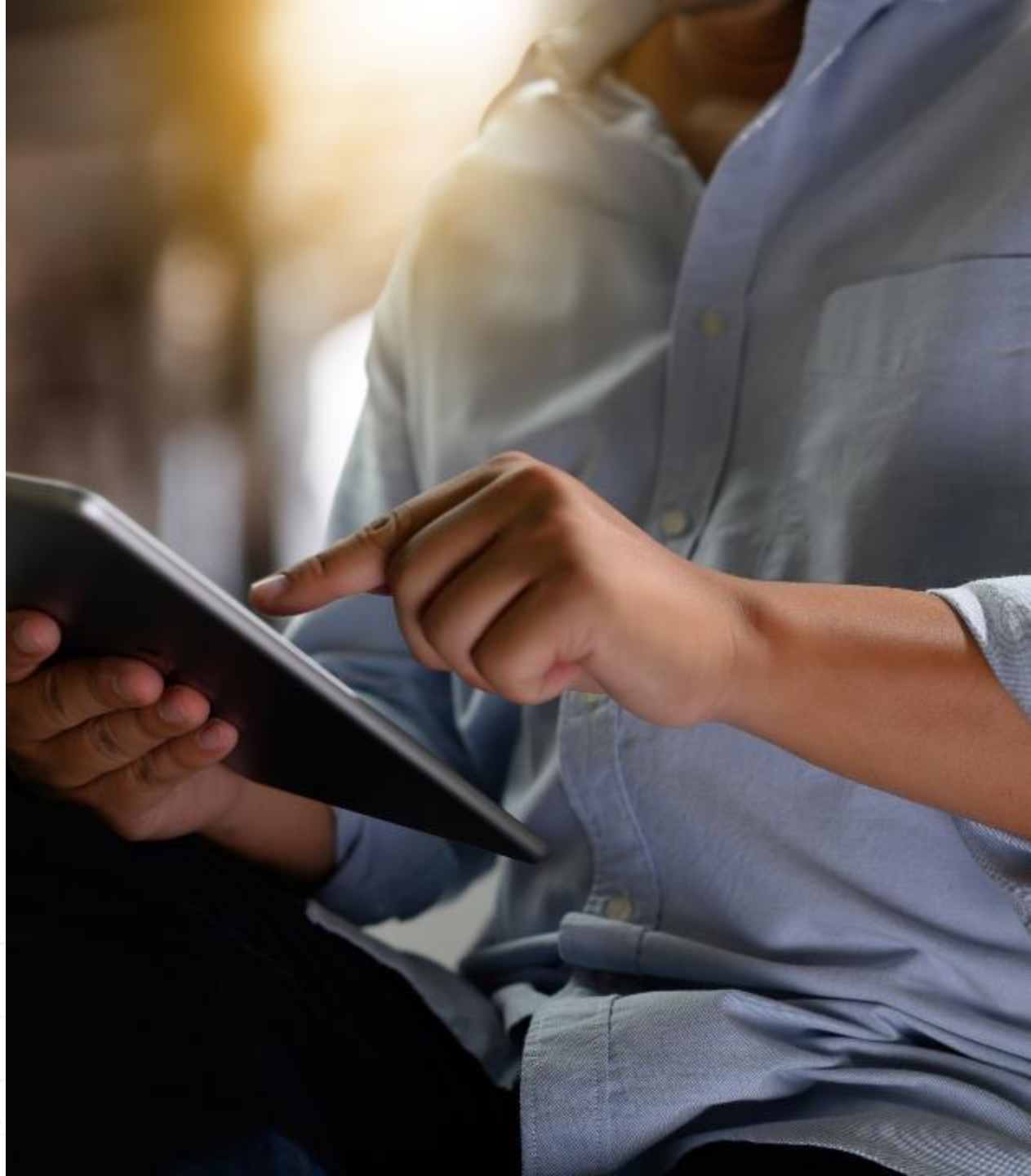
Qualys.

Qualys Patch can Help

Qualys.

Step 1:

Smart Automation for Low Hanging Fruit



Qualys.

Chrome: 2647
(2008-2023)

Firefox: 2131
(2003-2023)

Adobe: 1530
(2004-2023)

iTunes: 613
(2005-2023)

VLC: 105
(2007-2022)

Smart Automation

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

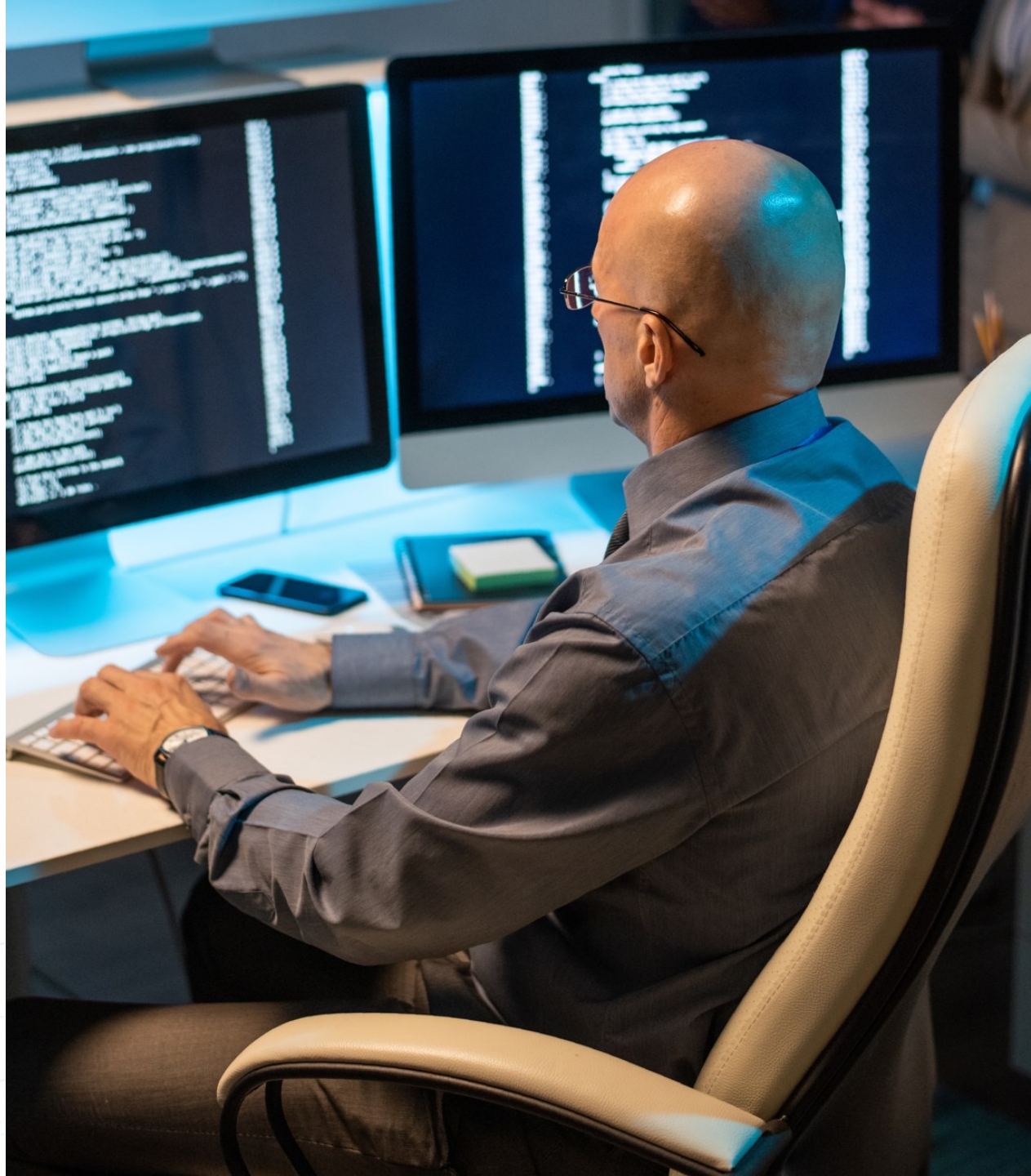
Focus on High-Risk High Reward Products: identify products that introduce the most risk to your environment and focus on those first

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

Qualys.

Step 2:

Complement & Simplify your Current Remediation Workflows



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

Qualys.

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.

Qualys.

Risk Elimination Across Multiple Attack Surfaces

On-Prem Assets

Cloud Assets

Work From Home (WFH)
or Roaming Assets

Qualys.

54M

Patches Deployed Last Year

25%

Faster remediation of internet facing assets with Patch

71%

Ransomware vulns can be fixed with Patch!

Qualys.

Demo

Qualys.

5 Easy Steps for Eliminating Your Risk by Complimenting Your SCCM

Qualys.

Any All | Last 30 Days

Total Widgets Count: 26 / 80

53551

440K
All Vulnerabilities

128K
Patchable with Automation

193K
Patchable Old MS Vulns

92.5K
Fixable No Patch Vulns

53.6K
Patchable Server 3rd Party

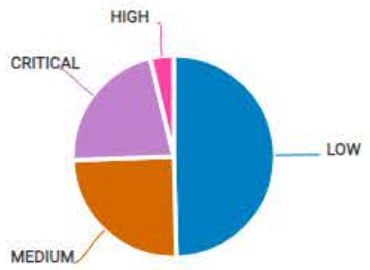
866
Patchable Mac Vulns

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

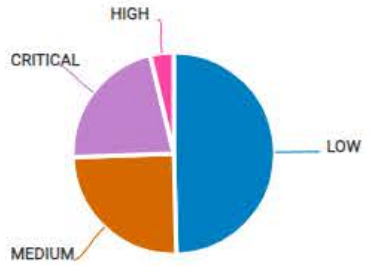
STEP 1: FIX BY AUTOMATION

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

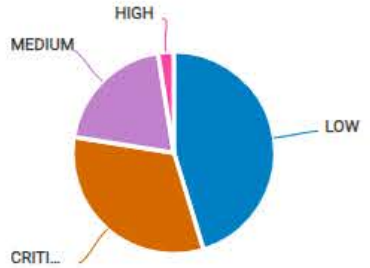
STEP 2: OLD MICROSOFT VULNS THAT CAN BE FIXED AS ...

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

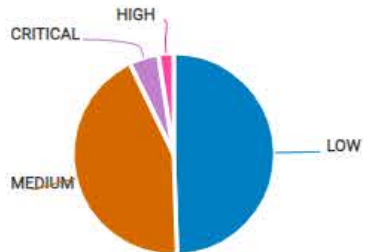
STEP 3: VULNS WITHOUT A PATCH THAT CAN BE FIXED OU...

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

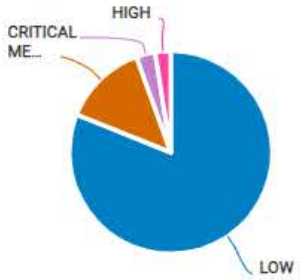
STEP 4: JAVA, WEBSERVERS, SQL, ETC OUT OF TOTAL VUL...

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

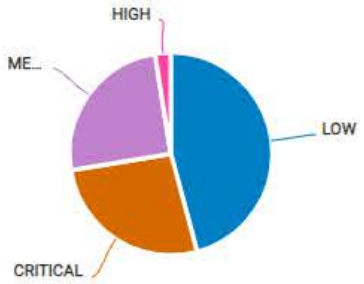
STEP 5: PATCHABLE MAC VULNS OUT OF TOTAL VULNS

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

TruRisk Eliminate with Mitigation

Qualys.

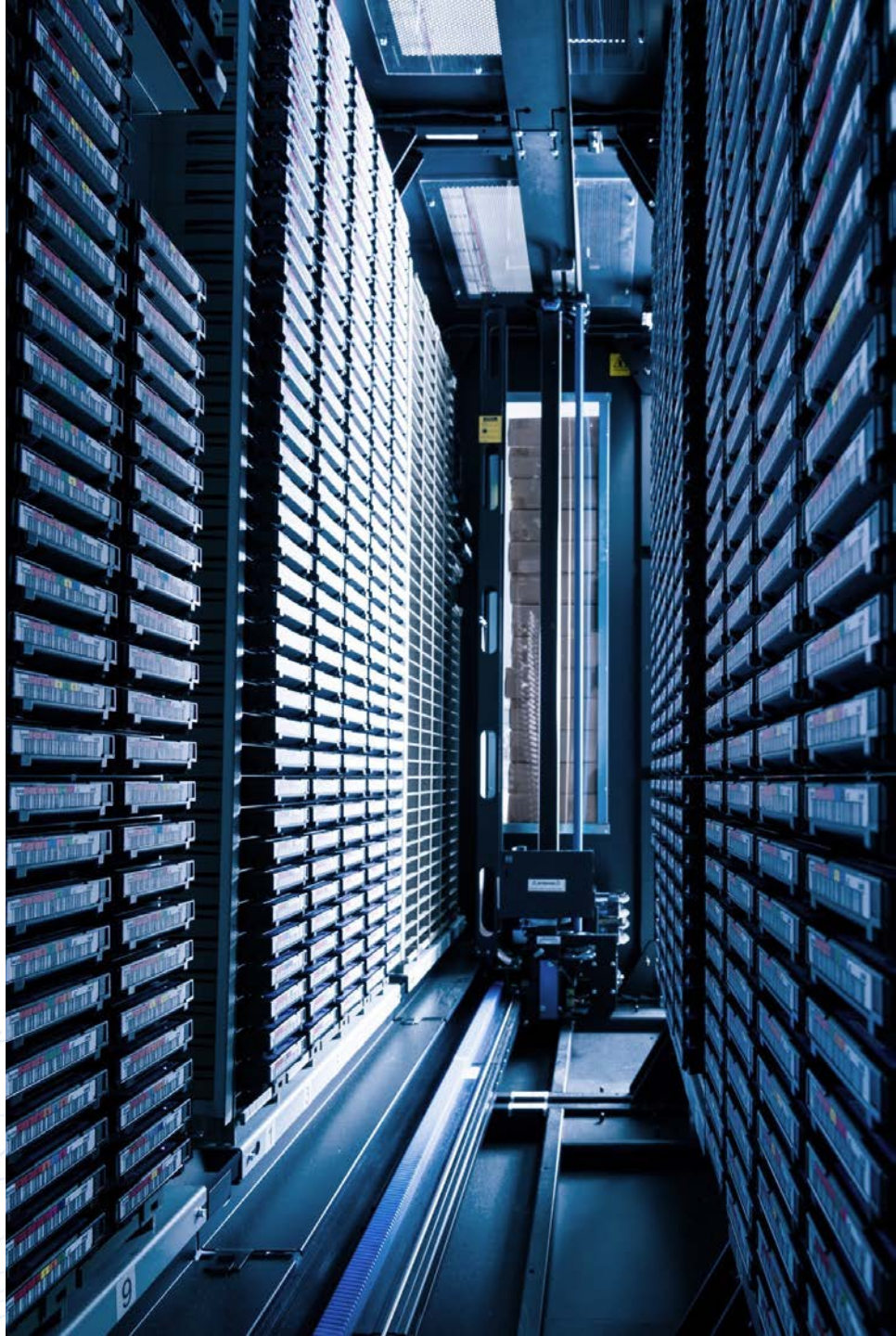
Critical Vuln Detected but, Patch Cannot be Deployed

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!

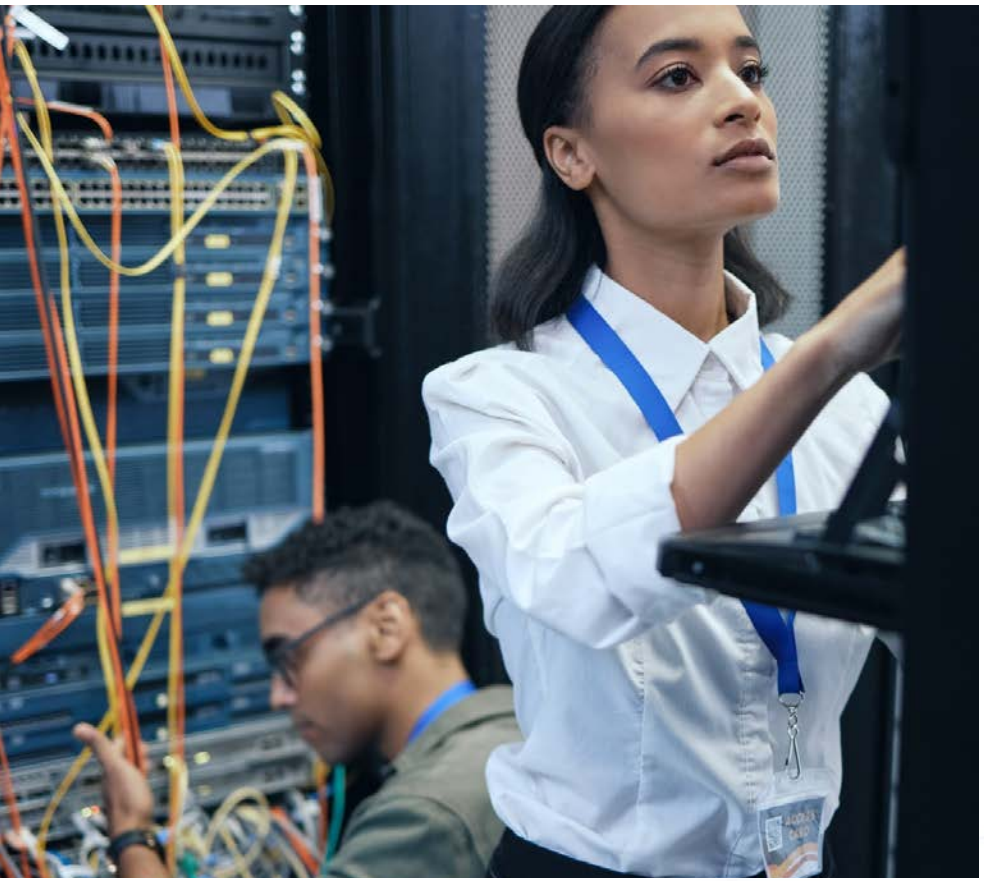
JDK 1.5 Only! Cannot update Java

Qualys.




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

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



Patches

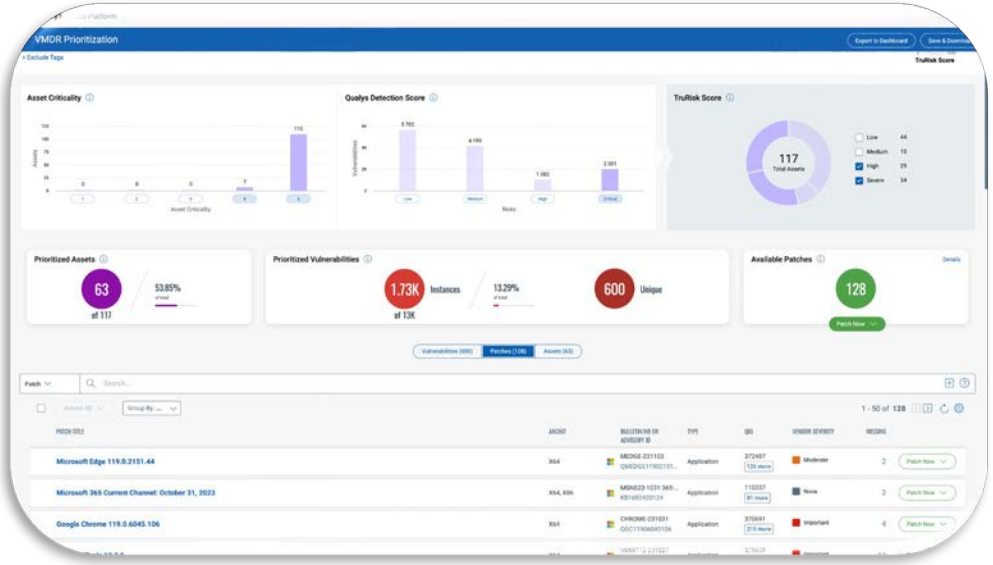
Deploy patches to the right devices, anywhere

Configuration Changes

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

Qualys.

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



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.

MITIGATION: Qualys researched alternatives to remediation

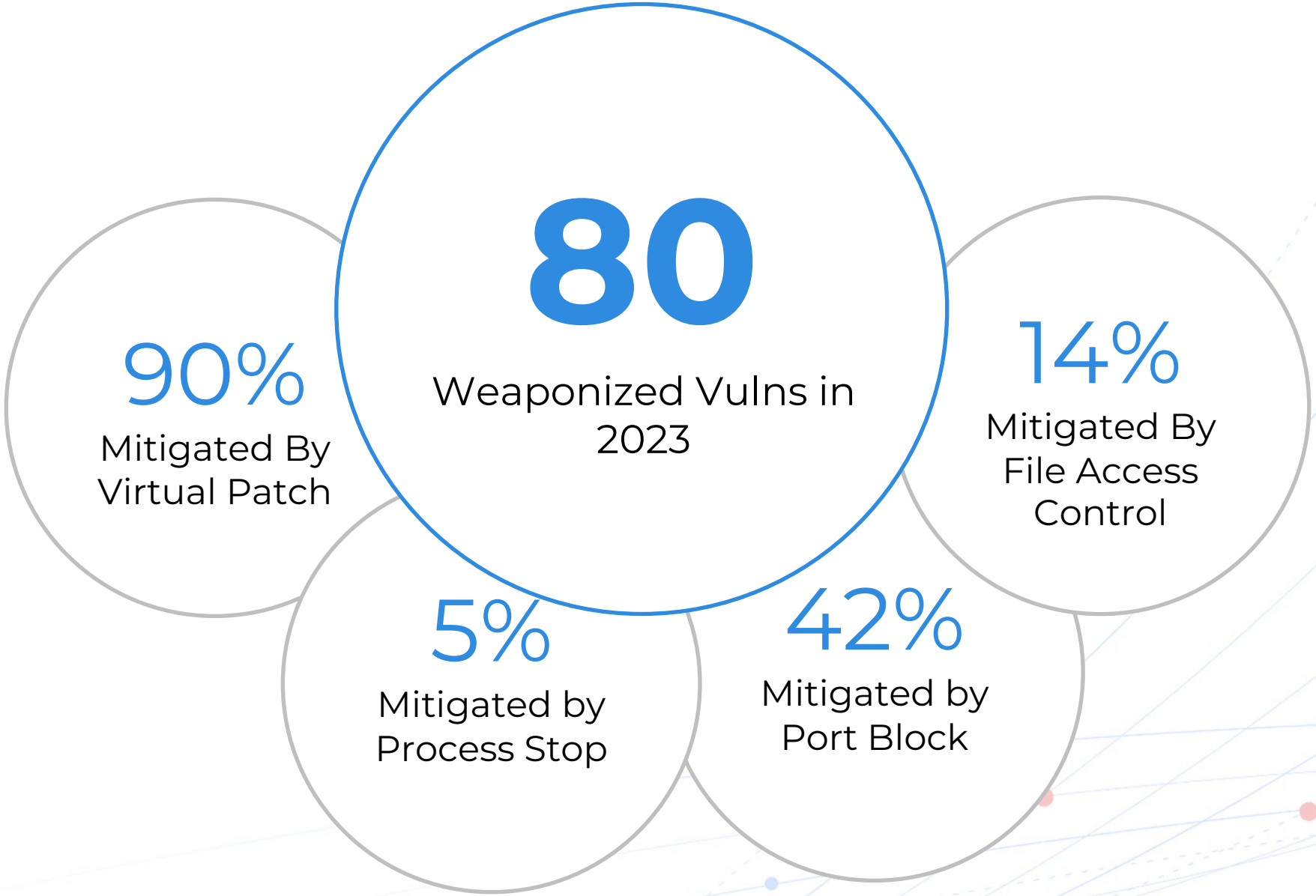
RIGHT Mitigation Actions

- 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.



Qualys.

Qualys Threat Research Unit

Conclusion

Qualys.

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."

Qualys.

Qualys.

Try Now

Master Vulnerability Remediation in 5 Steps.

Gain unmatched insight into a tailored security risk profile using your data and environment through a custom dashboard.

Accelerate vulnerability remediation by 43% with practical recommendations and a strategic roadmap to bolster your security.

Achieve a 90% patch rate improvement through smart automation and Qualys Patch Management.

Download Now

www.qualys.com

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.


SC
24

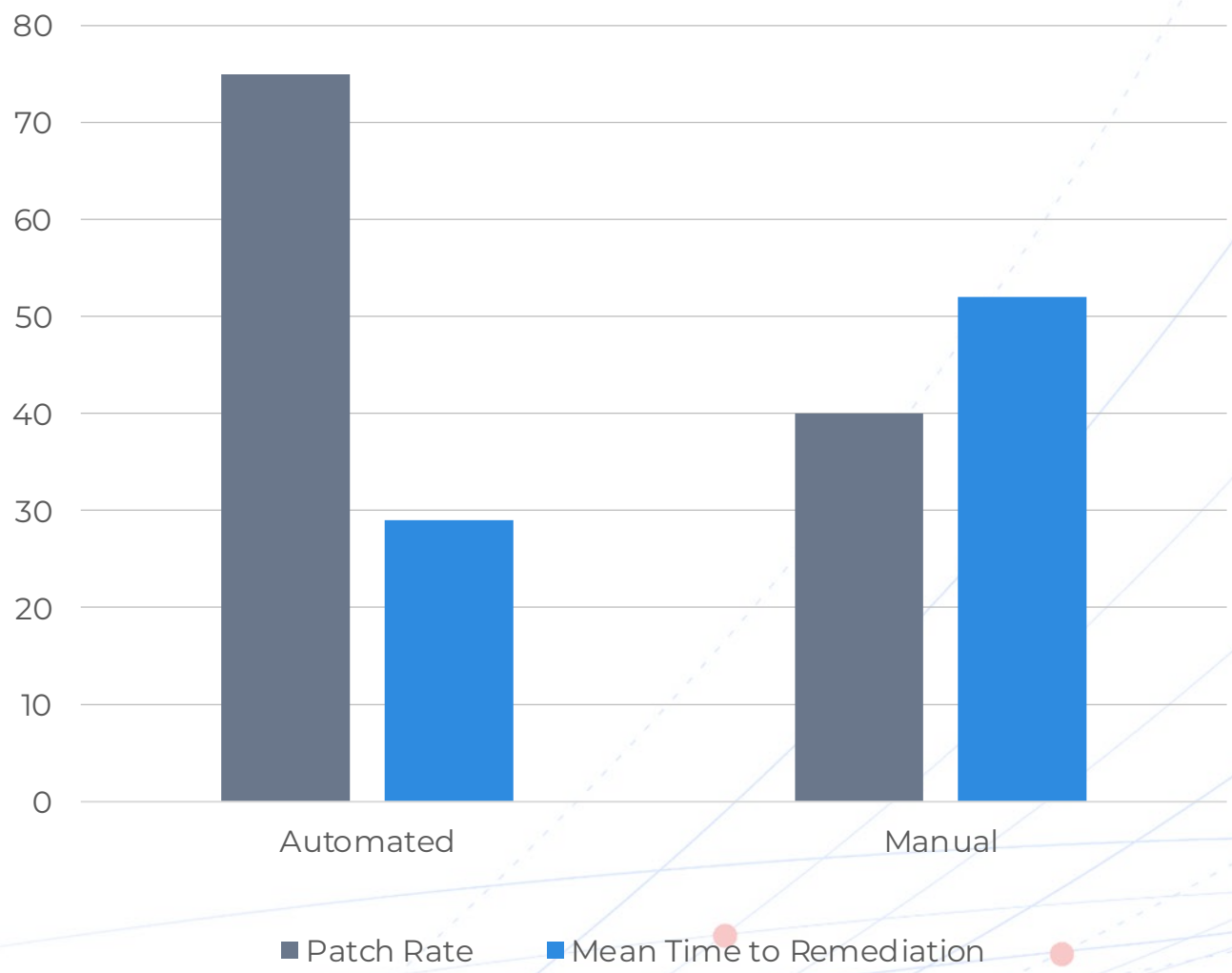
Automation is Key

89.5%

Improvement in Patching Rates

43.1%

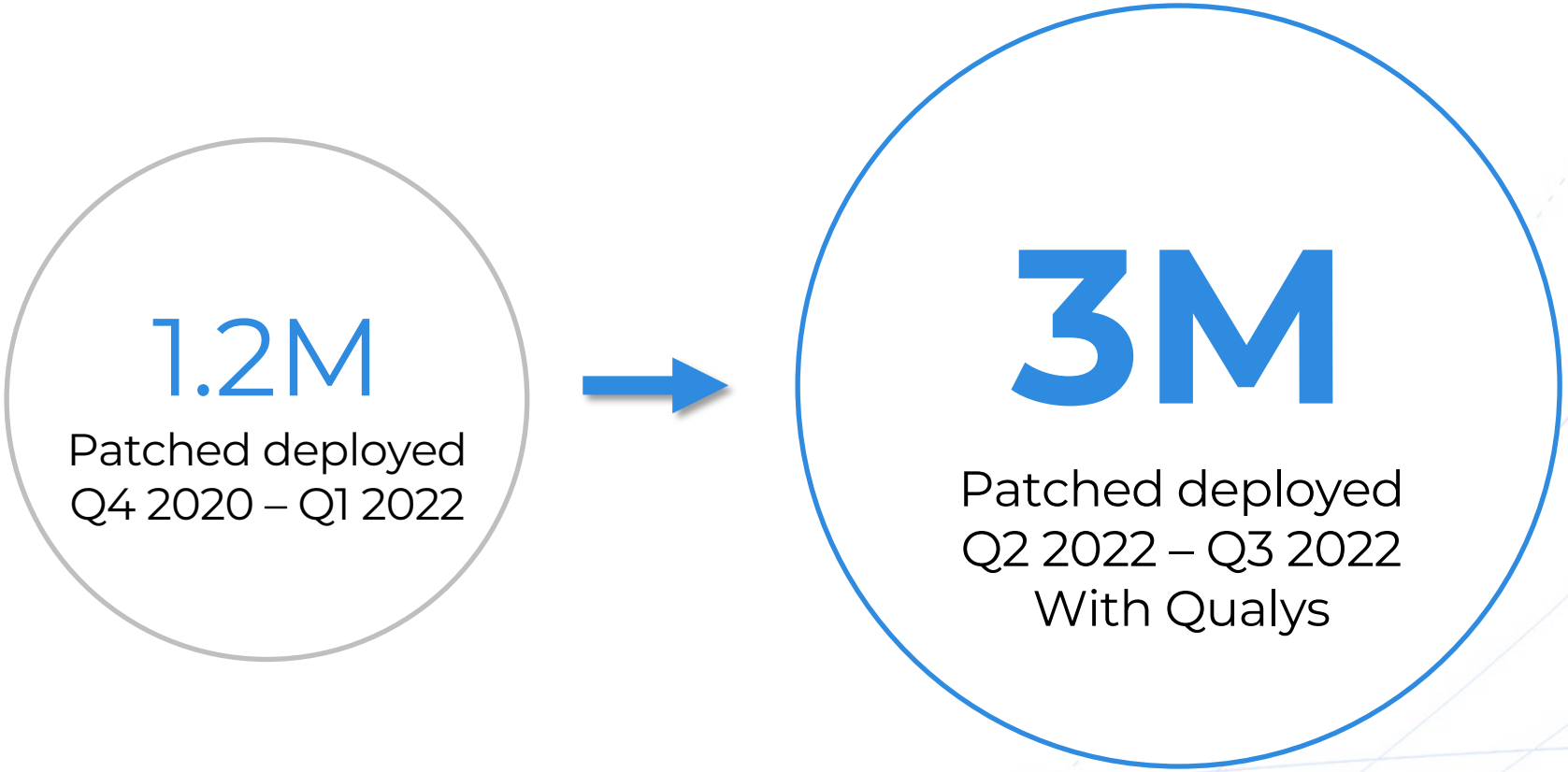
Improvement in MTTR Speed



Qualys.

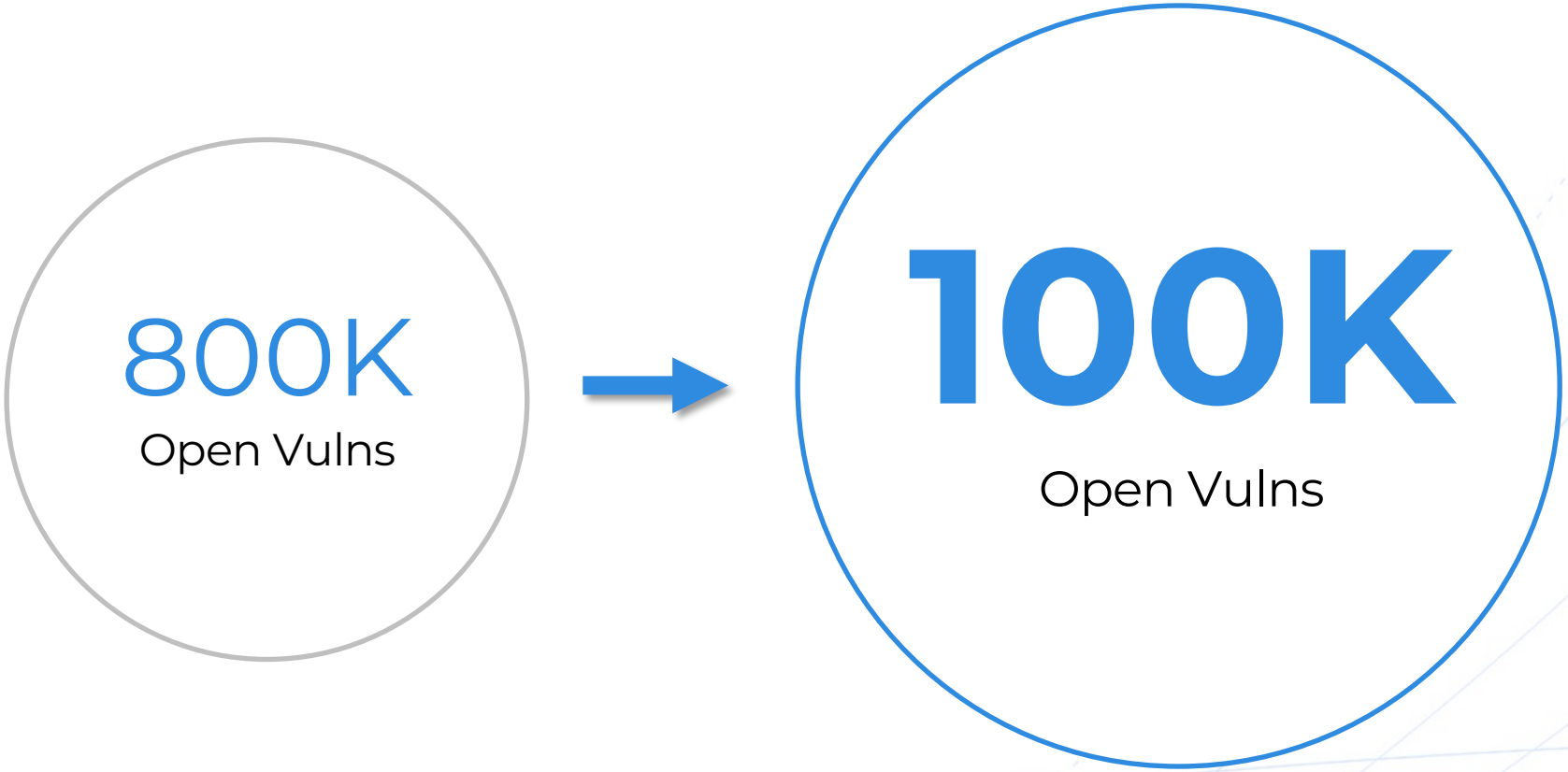
Qualys Threat Research Unit

Customer's Real Risk Elimination



Qualys.

Customer's Real Risk Elimination: in a Month



Qualys.