QSC22

Unlocking Intelligence-Backed Remediation: Insights from the Qualys Threat Research Unit

Travis Smith – Vice President, Threat Research Unit

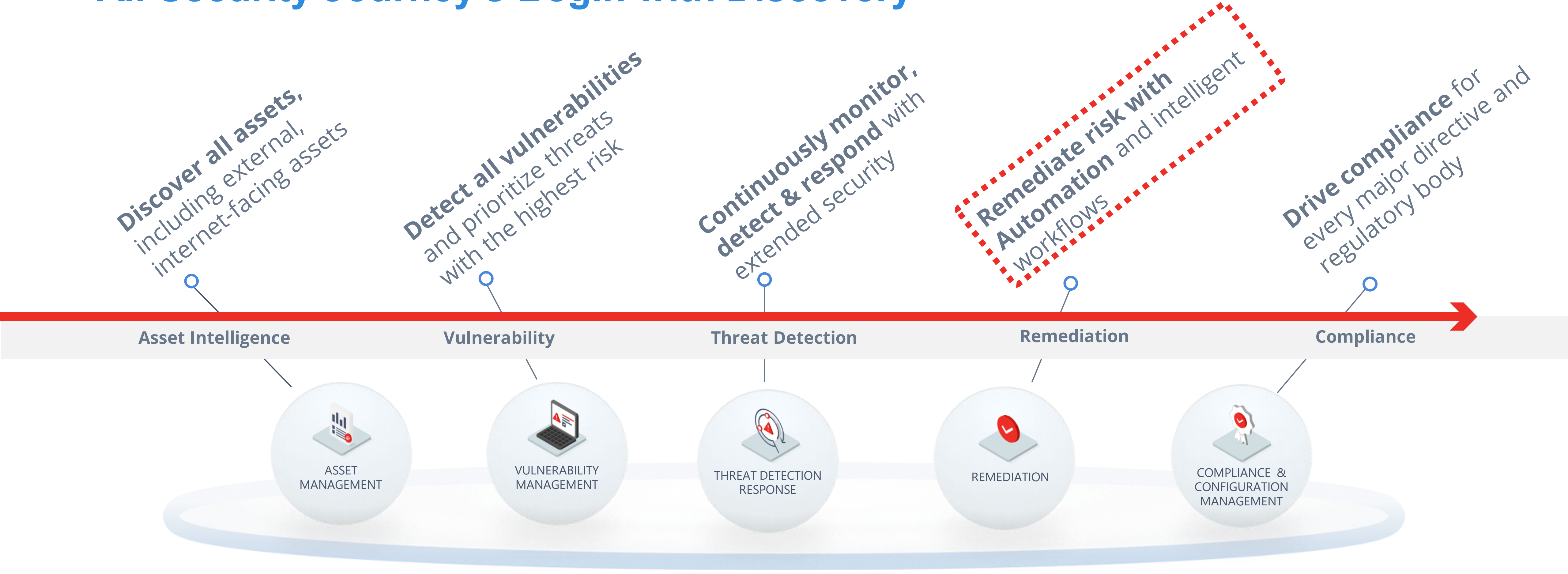
Eran Livne – Sr Director, Endpoint Remediation

Qualys Security Conference

Qualys.

A Risk-based Approach to Cybersecurity

All Security Journey's Begin with Discovery



Discover all assets, including external, internet-facing assets

Detect all vulnerabilities and prioritize threats with the highest risk

Continuously monitor, detect & respond with extended security

Remediate risk with Automation and intelligent workflows

Drive compliance for every major directive and regulatory body

Qualys Threat Research Unit

Prevention Is Key to Reducing Digital Risk

Speed is the Key to Out-maneuvering Adversaries

Automation is the Difference Between Success and Failure

Initial Access Brokers Attack What Organizations Ignore

Misconfigs Still Prevalent in Web Applications

Infrastructure Misconfigs Open the Door to Ransomware

In 2022, **25,000 NEW** vulnerabilities were added!

CISA Updates Its List of Known Exploited Vulnerabilities

The Cyber Security and Infrastructure Security Agency (CISA) in the US has made 17 new additions to its list of vulnerabilities that are known to be exploited by malicious actors.

Software vulnerabilities are exploited by a range of actors to gain initial access to a network, which then enables them to carry out further attacks.

Two notable additions to the list are: the vulnerability in ‘October CMS’ (CVE-2021-32648) that may have been used to **deface Ukrainian government websites** and the new SolarWinds vulnerability (CVE-2021-35247) that actors unsuccessfully **attempted to exploit to propagate Log4j attacks.**

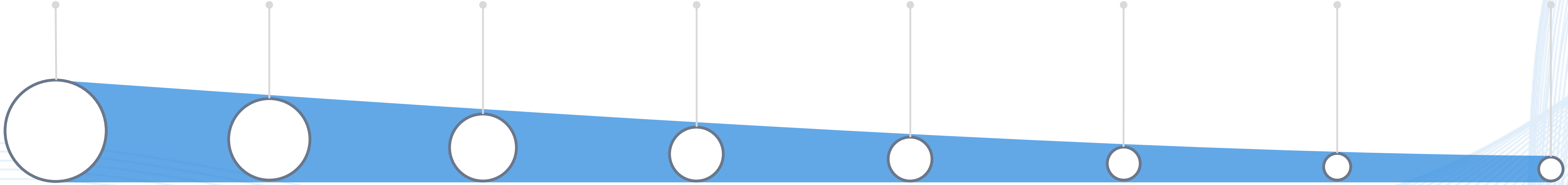
The full list of known exploited vulnerabilities is on the CISA website. This is also a reminder to organizations of the need to install security updates to patch vulnerabilities. See NSCS guidance on **mitigating malware** and **vulnerability management** for more information.

https://www.ncsc.gov.uk/report/weekly-threat-report-28th...

Vulnerability Threat Landscape

2022

100%	25,228	All Known Vulnerabilities
30%	7,786	Vulnerabilities With Exploits Available
0.6%	159	Vulnerabilities With Weaponized Exploit Code
.36%	93	CISA Known Exploited Vulnerabilities
.28%	73	Named Vulnerabilities (PwnKit, Spring4Shell)
.11%	28	Exploited by Threat Actors
.09%	23	Exploited by Malware
.07%	18	Exploited by Ransomware

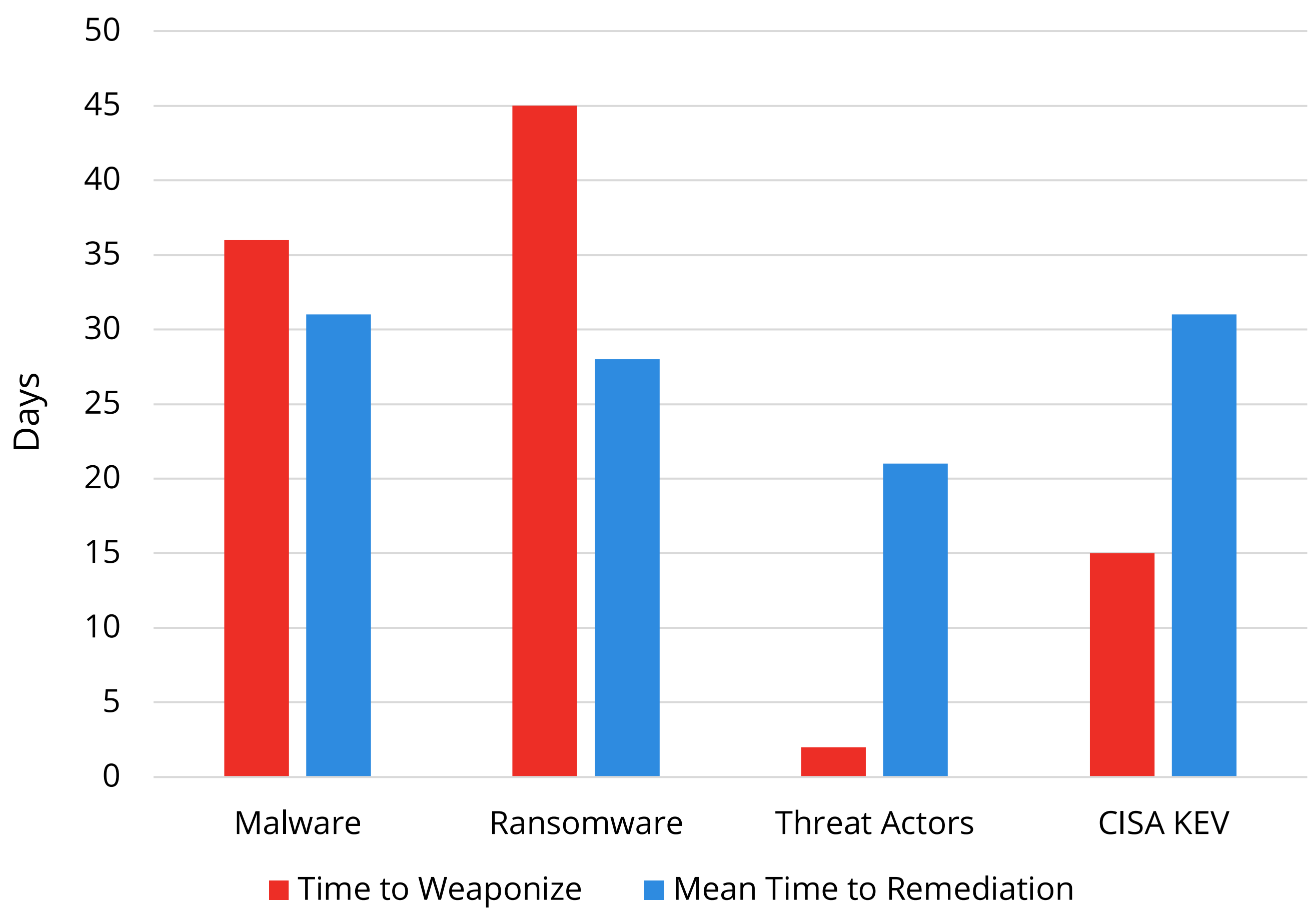


Weaponized Vulns

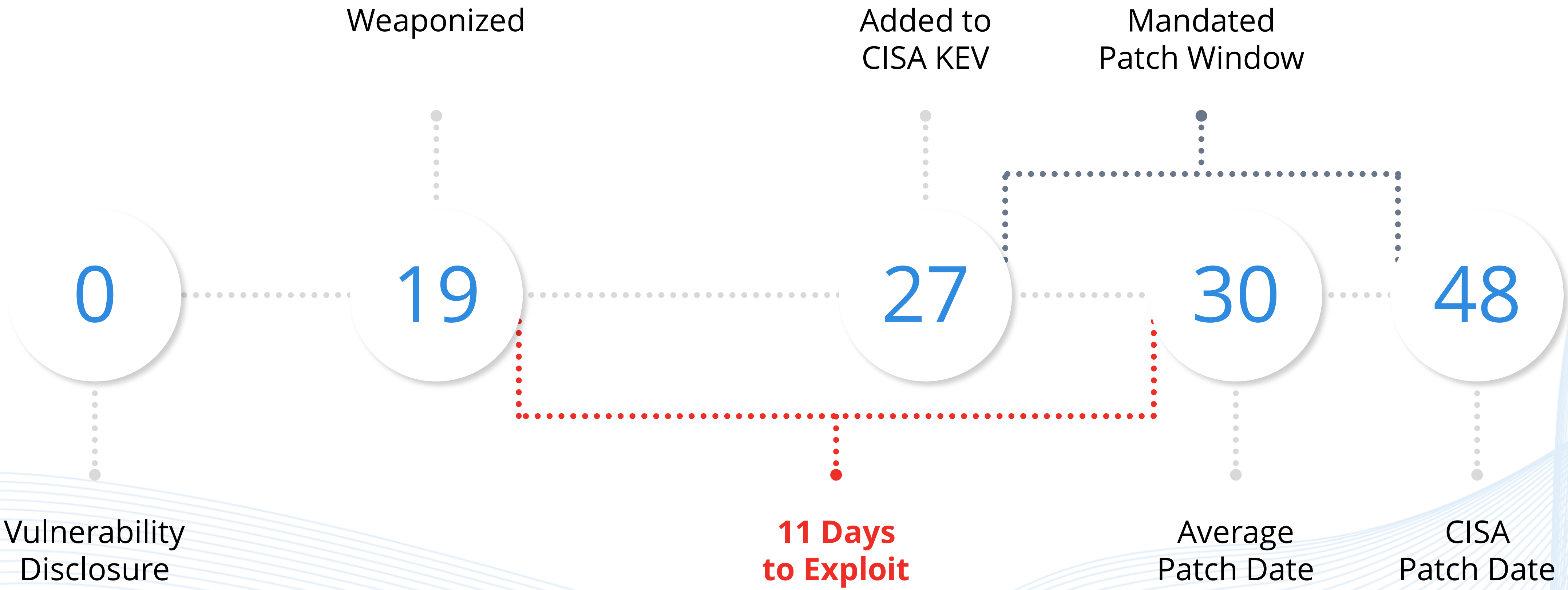
19.5
Time to Weaponize (Days)

30.6
Mean Time to Remediate (Days)

57.7%
Remediated Vulnerabilities



Typical Vulnerability Lifecycle



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

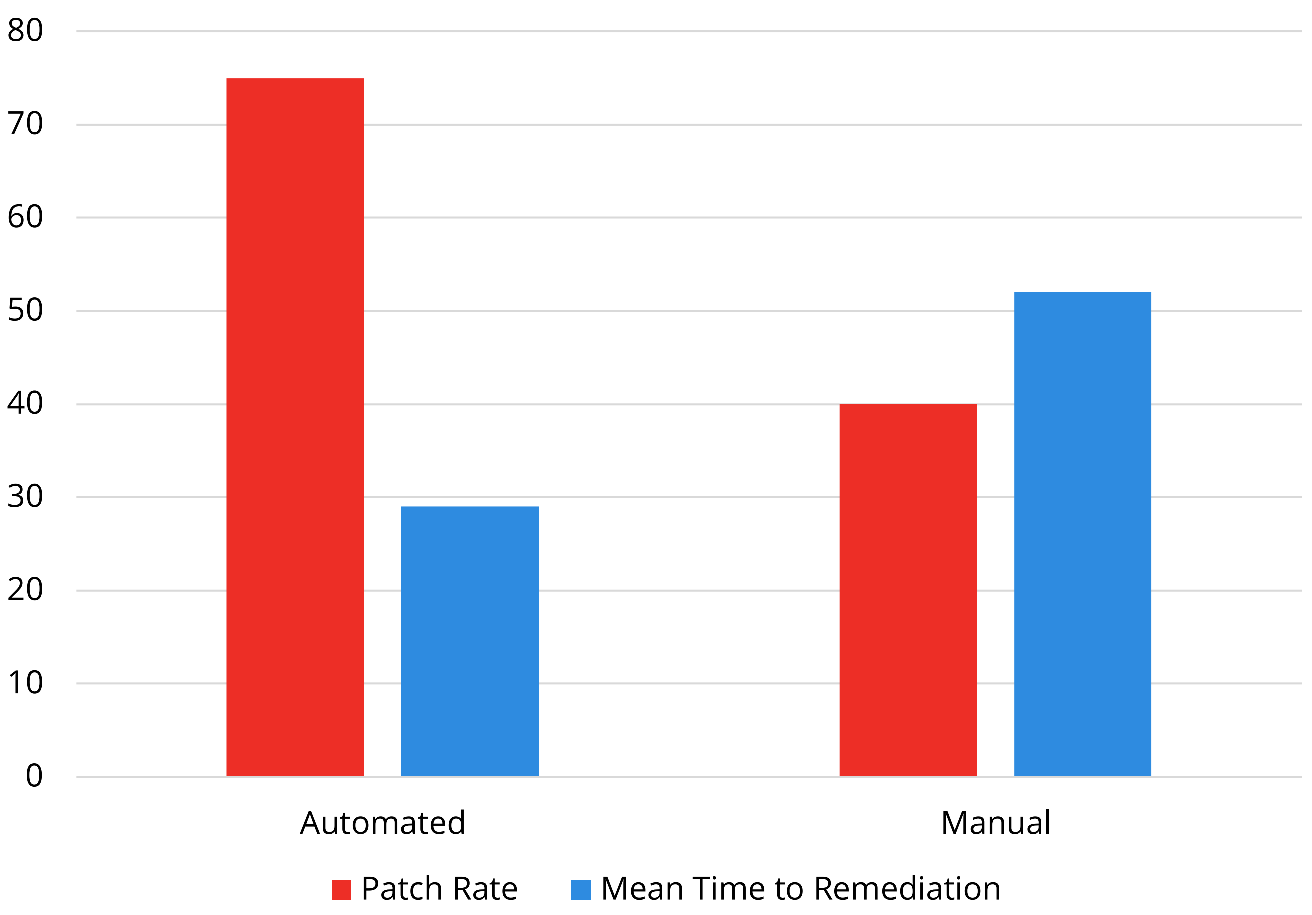
Automation is Key

89.5%

Improvement in Patching Rates

43.1%

Improvement in MTTR Speed



The Tale of Two Vulnerabilities

CVE-2022-1040

Sophos Firewall Remote Code Execution (RCE)

📅	March 25
👁	100
⏱	70 (days)
🛡	34.7%

Manual Patching

CVE-2022-30190

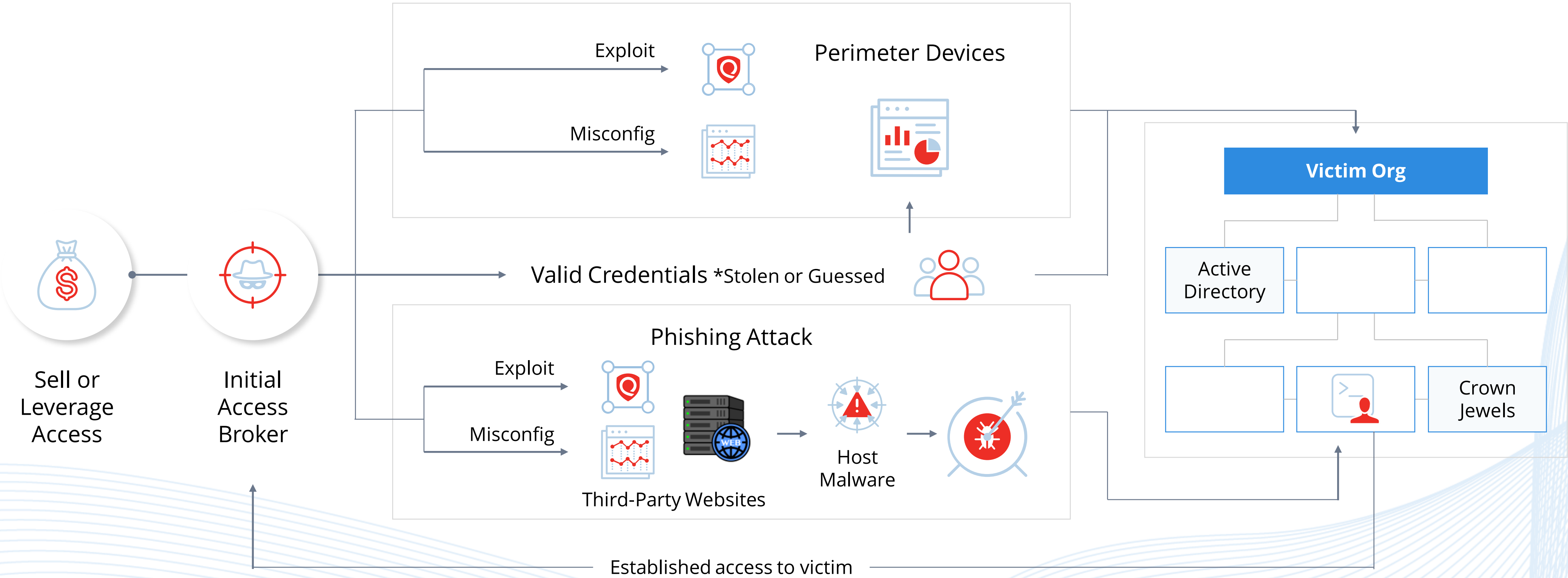
Microsoft Windows Support Diagnostic Tool RCE - Follina

📅	June 1
👁	100
⏱	28.4 (days)
🛡	91.21%

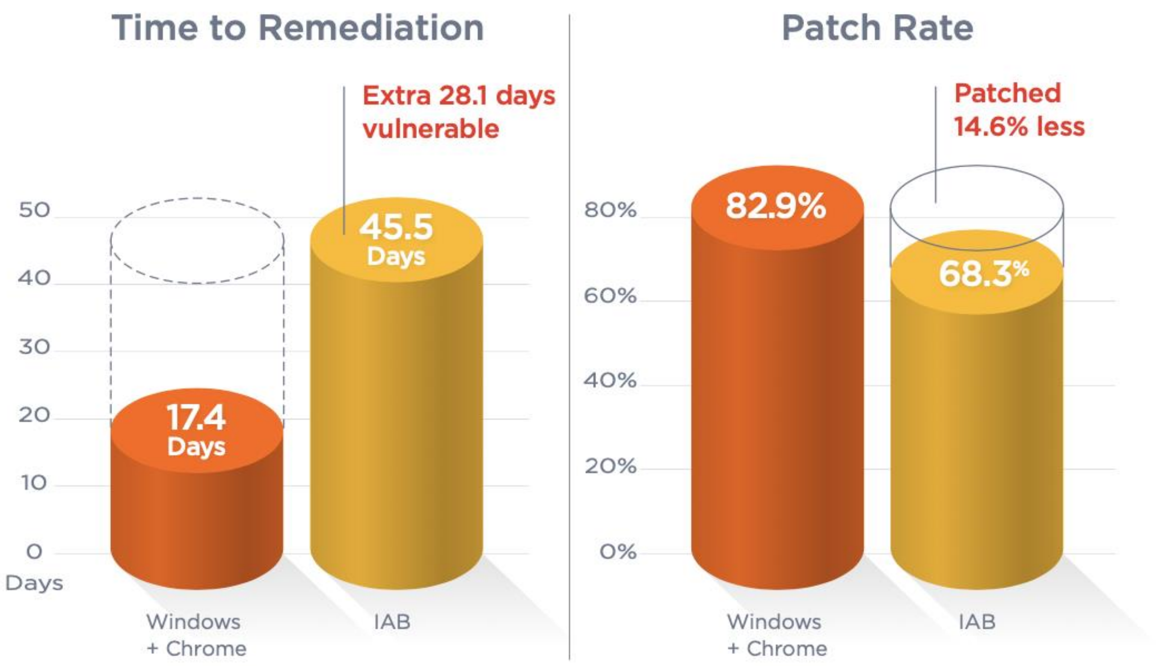
Automatable Patching

Threat Actors are Diversifying from Common Vulnerabilities

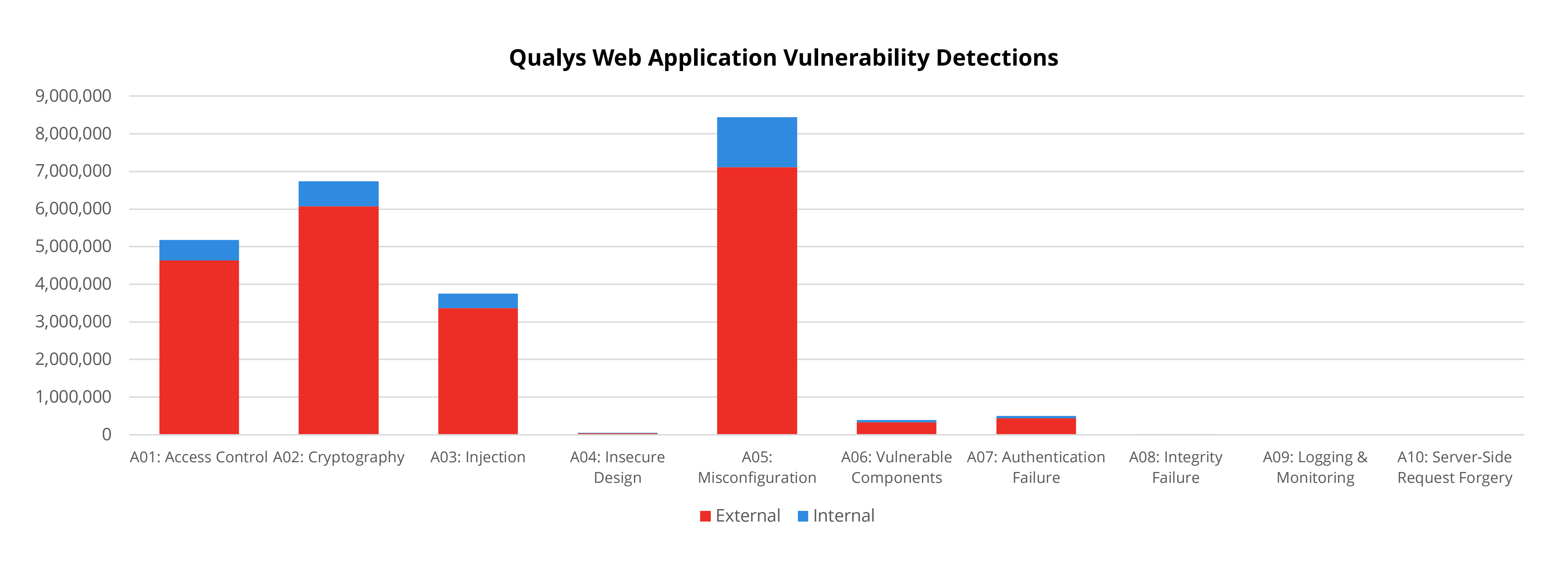
About Initial Access Brokers



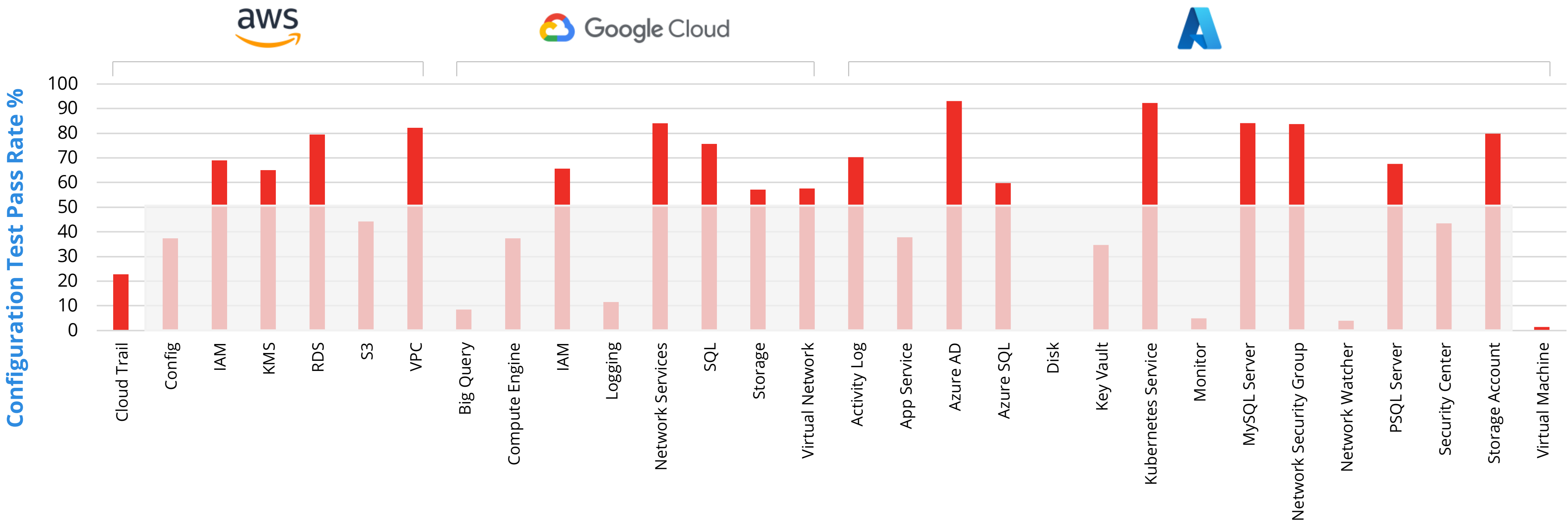
2022 Vulnerabilities Exploited by IABs



Web Application Security Scans

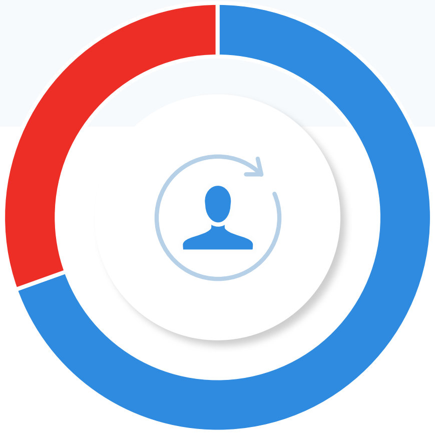


Failing Controls in Cloud Infrastructure

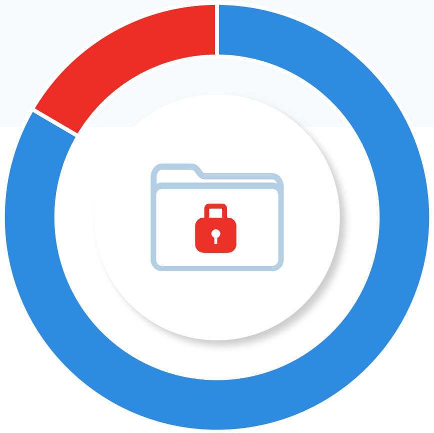


QSC23 | Get More Security

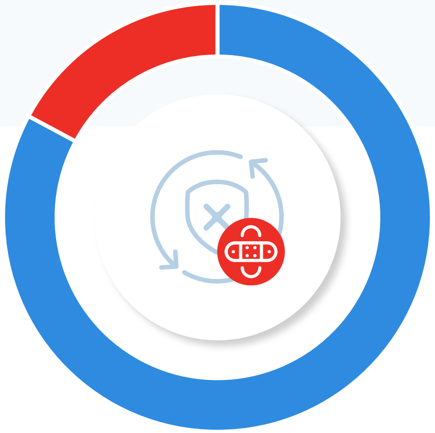
Endpoint Misconfigurations



Password Hygiene

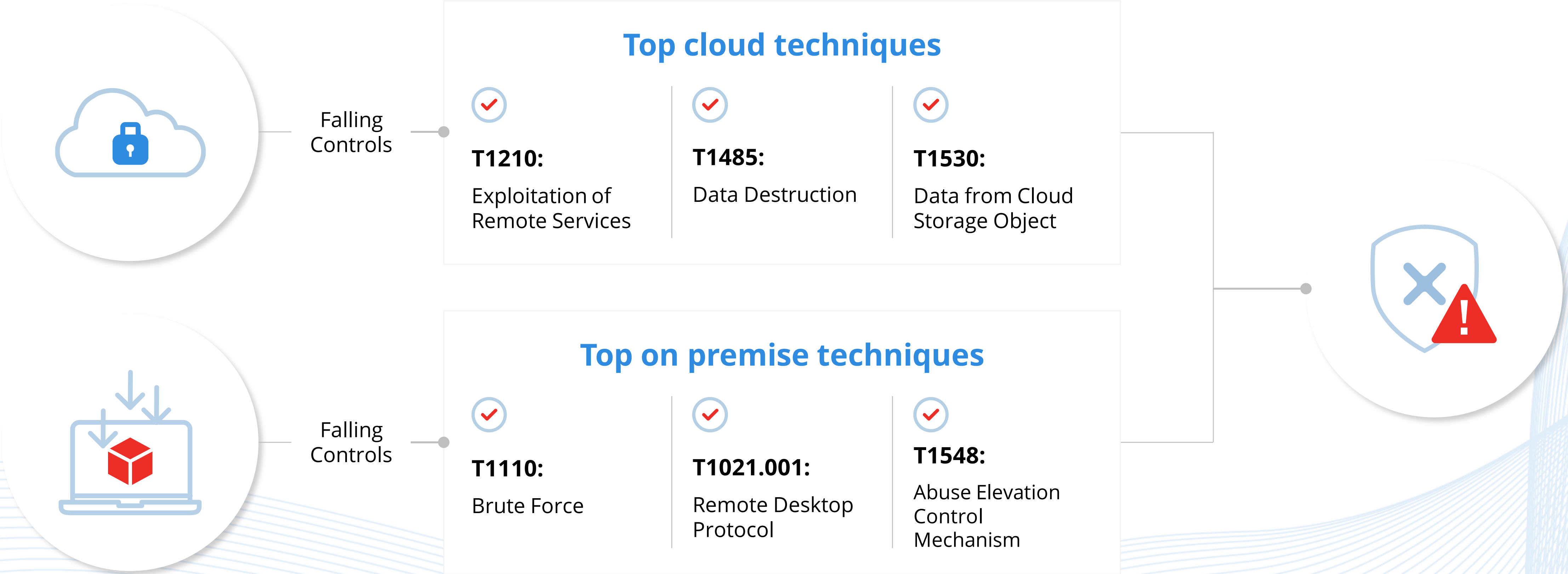


User Permissions



Update Settings

Misconfigurations Leading to Ransomware



Falling Controls

Top cloud techniques

✓ **T1210:** Exploitation of Remote Services

✓ **T1485:** Data Destruction

✓ **T1530:** Data from Cloud Storage Object

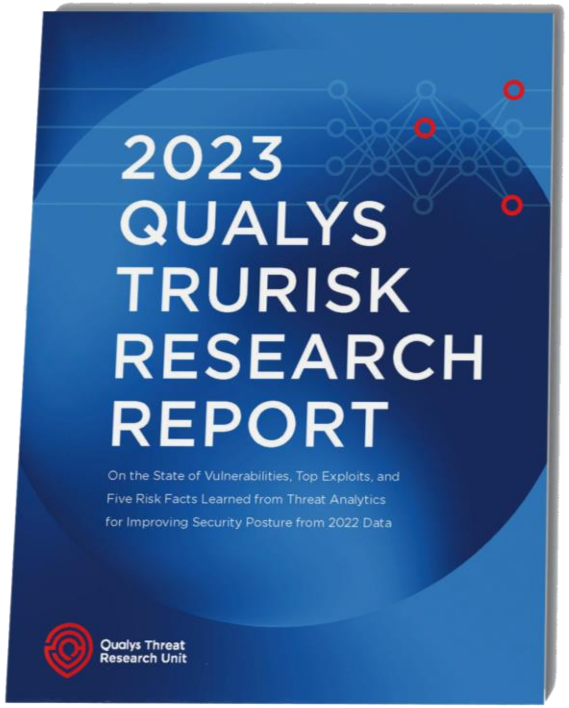
Falling Controls

Top on premise techniques

✓ **T1110:** Brute Force

✓ **T1021.001:** Remote Desktop Protocol

✓ **T1548:** Abuse Elevation Control Mechanism



2023 QUALYS TRURISK RESEARCH REPORT

On the State of Vulnerabilities, Top Exploits, and Five Risk Facts Learned from Threat Analytics for Improving Security Posture from 2022 Data

Qualys Threat Research Unit

RISK FACT 1

1 SPEED IS THE KEY TO OUT-MANEUVERING ADVERSARIES

The doubling of disclosed vulnerabilities over the last five years, the speed at which vulnerabilities are weaponized, and the cyber talent shortage have left teams struggling to wade through a mountain of vulnerabilities with no way to fix them all. Security teams need a systematic approach to cut through the noise and prioritize fixing the most critical vulnerabilities that will reduce risk and enable them to keep up with threat actors.

On average, weaponized vulnerabilities are patched within 30.6 days while only being patched an average of 57.7% of the time. These same vulnerabilities are weaponized by attackers in 19.5 days on average. This means that attackers have 11.1 days of exploitation opportunities before organizations begin patching.

A defender's mean time to remediation (MTTR) shows a slight change in how organizations respond to urgent threats. Vulnerabilities known to be leveraged by named threat actors were remediated eight days faster than those without association to known threat actors. But while defenders are quick to address these, attackers are also quick to weaponize. Threat actors were faster to leverage vulnerabilities that are known to be exploited or were catalogued on CISA's Known Exploited Vulnerability list when compared to those leveraged by malware and ransomware.

Figure 5: Time to Weaponize vs. MTTR for Vulnerabilities in 2022

RISK FACT 1: SPEED IS THE KEY TO OUT-MANEUVERING ADVERSARIES | 2023 QUALYS TRURISK RESEARCH REPORT 12

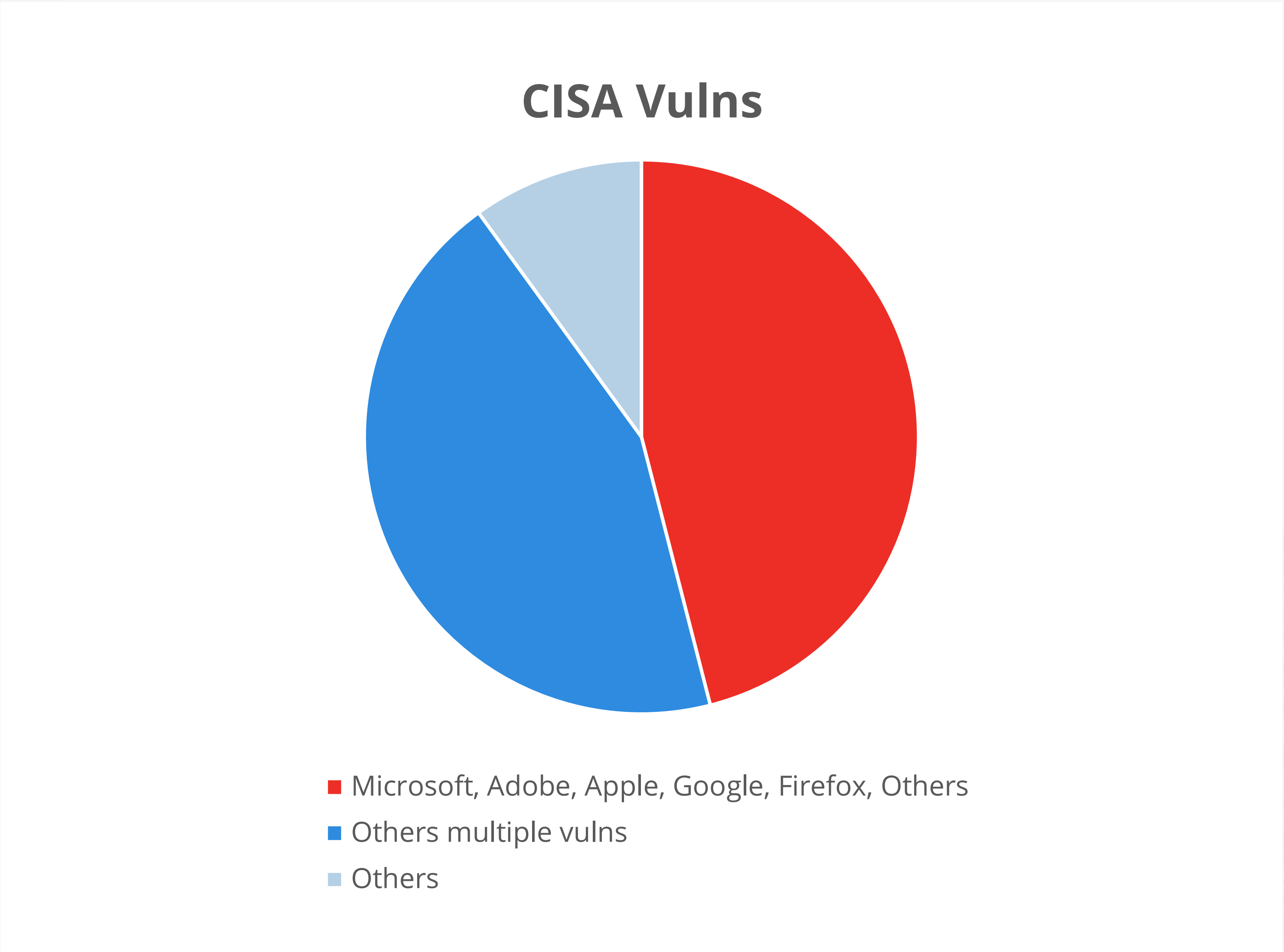
FIV
RIS
LEA
FR
AN
IN 2

Qualys.

https://www.qualys.com/forms/tru-report/

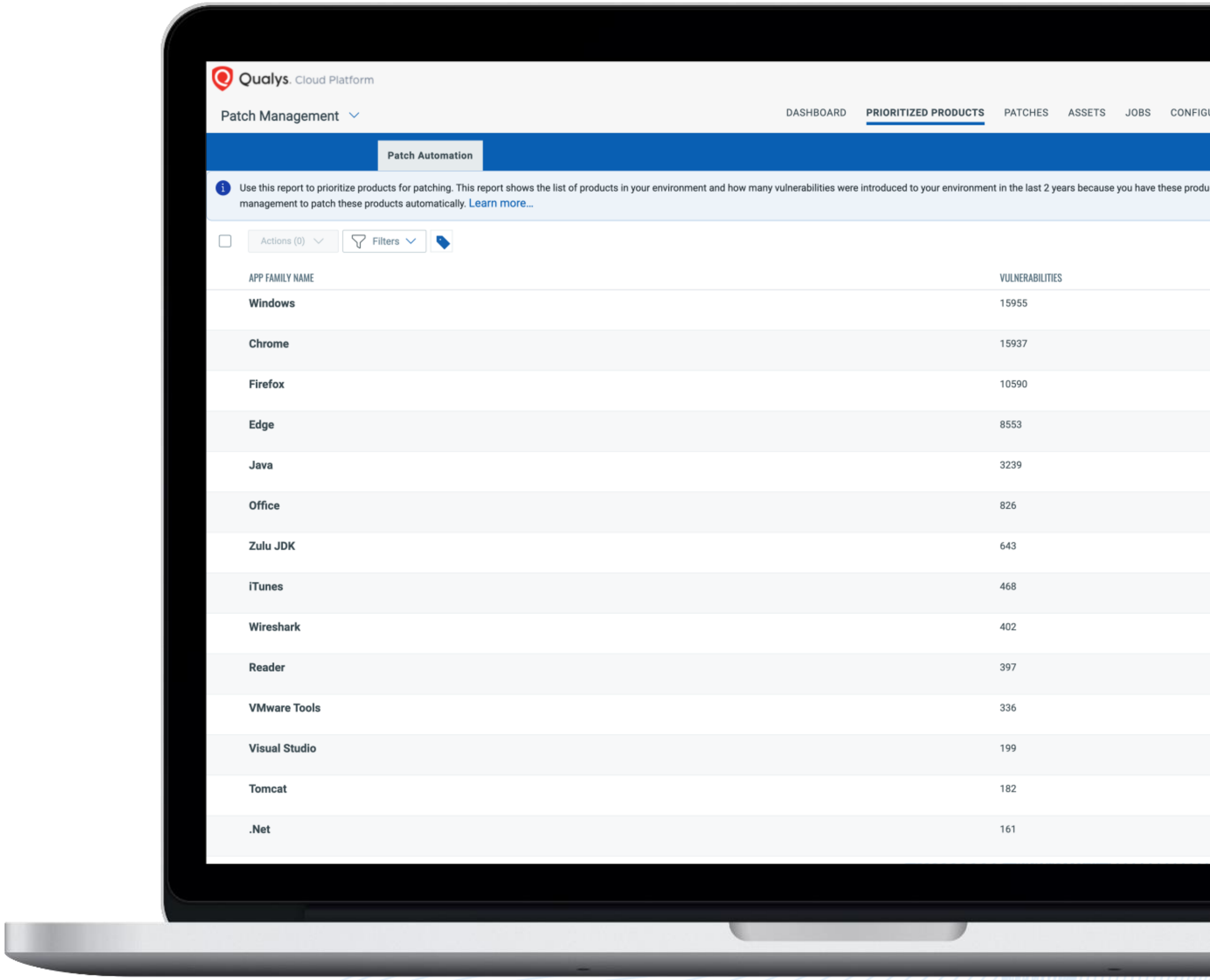
Automation is Key for Successful Risk Reduction

Start with the Low Hanging Fruits



Smart Automation

- ✓ Risk Based Automation
- ✓ Automate where it make sense from operational perspective
- ✓ Test and automate where needed

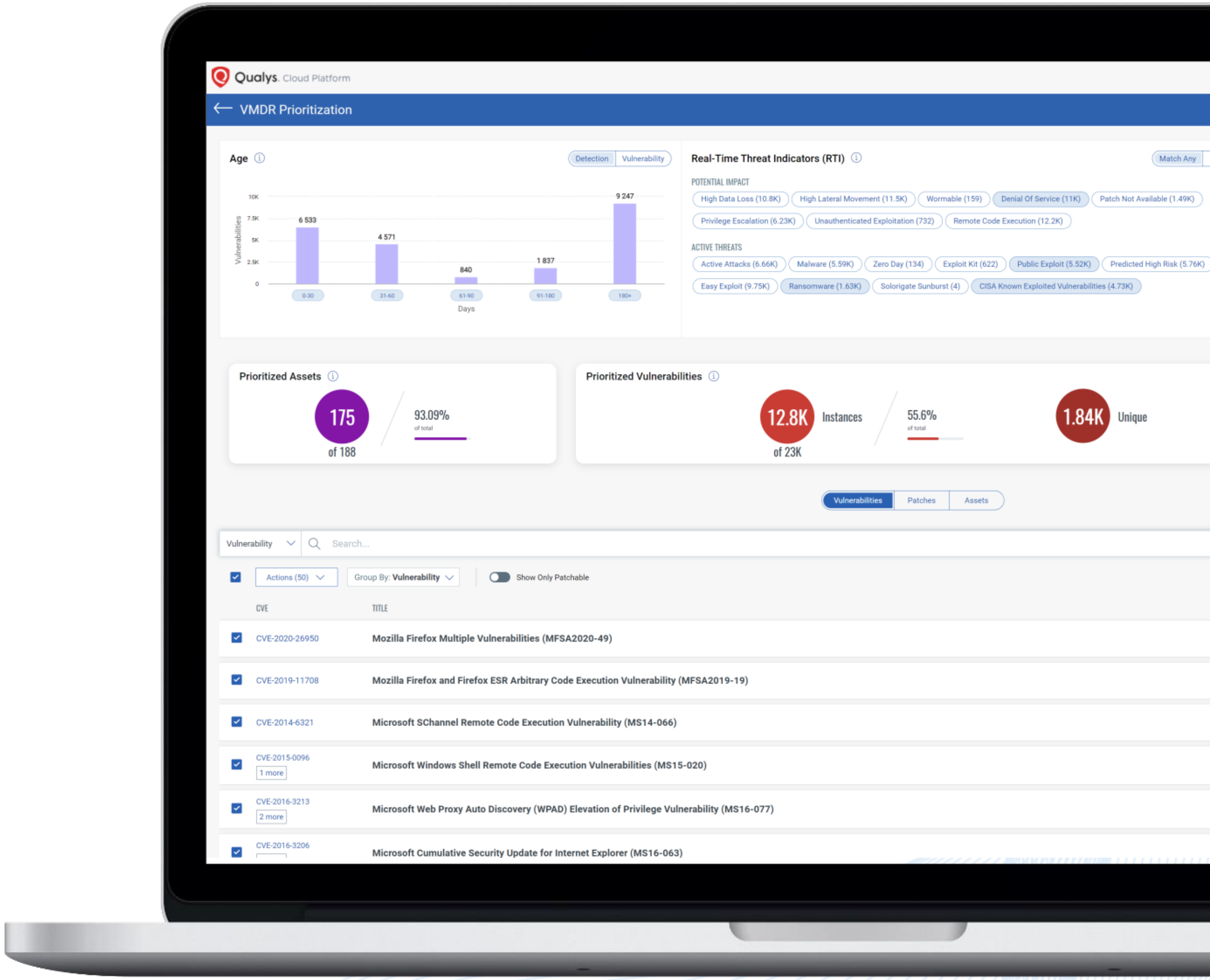


Use this report to prioritize products for patching. This report shows the list of products in your environment and how many vulnerabilities were introduced to your environment in the last 2 years because you have these produ
management to patch these products automatically. Learn more...

APP FAMILY NAME	VULNERABILITIES
Windows	15955
Chrome	15937
Firefox	10590
Edge	8553
Java	3239
Office	826
Zulu JDK	643
iTunes	468
Wireshark	402
Reader	397
VMware Tools	336
Visual Studio	199
Tomcat	182
.Net	161

TruRisk Based Automation

- ✓ Remediate riskiest vulns
- ✓ Block ransomware before it starts
- ✓ Focus on active attacked vulns
- ✓ Etc.

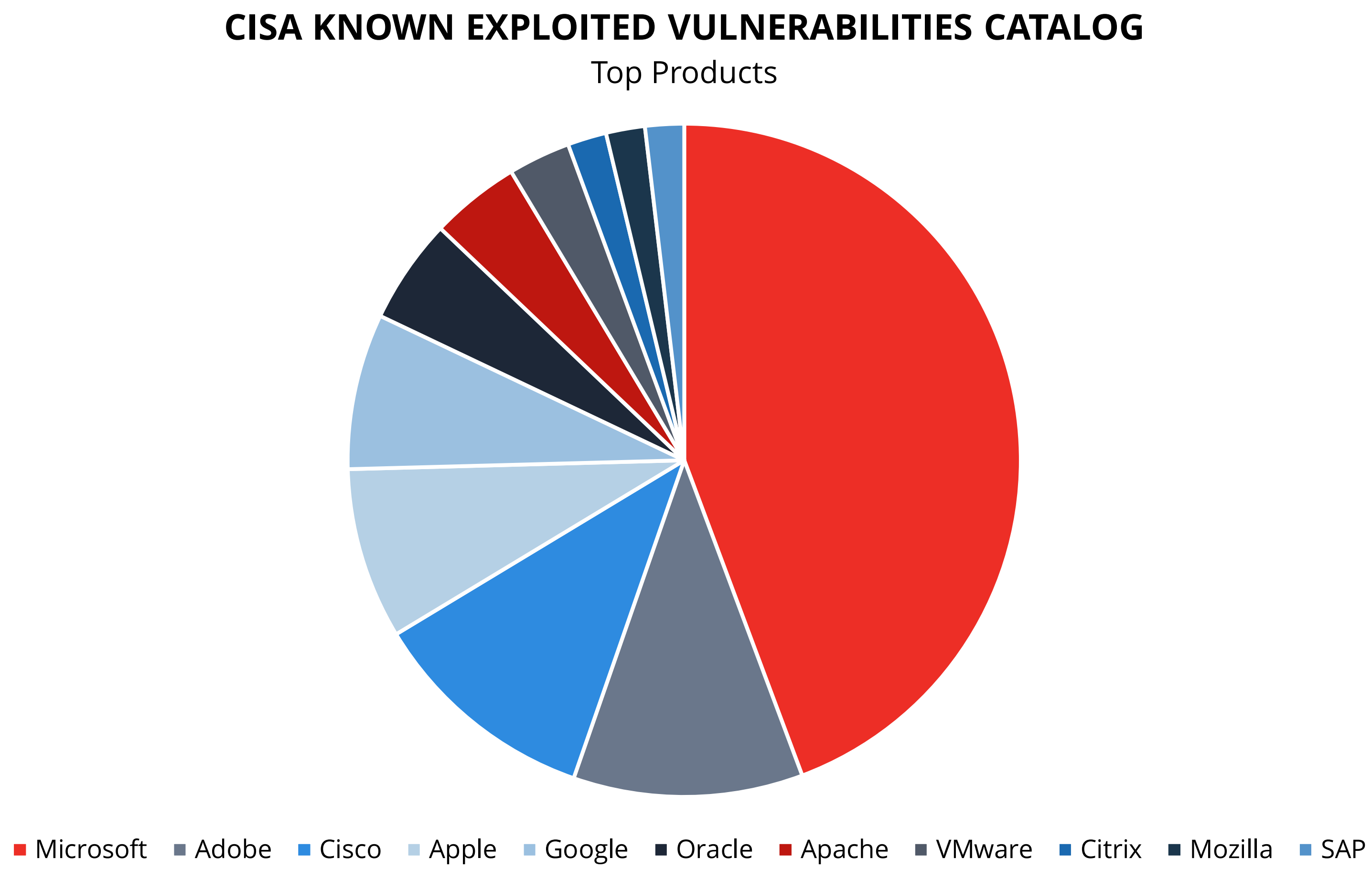


☑	CVE	TITLE
☑	CVE-2020-26950	Mozilla Firefox Multiple Vulnerabilities (MFSA2020-49)
☑	CVE-2019-11708	Mozilla Firefox and Firefox ESR Arbitrary Code Execution Vulnerability (MFSA2019-19)
☑	CVE-2014-6321	Microsoft SChannel Remote Code Execution Vulnerability (MS14-066)
☑	CVE-2015-0096 1 more	Microsoft Windows Shell Remote Code Execution Vulnerabilities (MS15-020)
☑	CVE-2016-3213 2 more	Microsoft Web Proxy Auto Discovery (WPAD) Elevation of Privilege Vulnerability (MS16-077)
☑	CVE-2016-3206	Microsoft Cumulative Security Update for Internet Explorer (MS16-063)

Risk is Everywhere

Out-of-the-box support for patching Windows OS, Linux, macOS and 3rd party applications

- ✓ Patch any device anywhere AND automatically where it makes sense



QSC23 | Get More Security

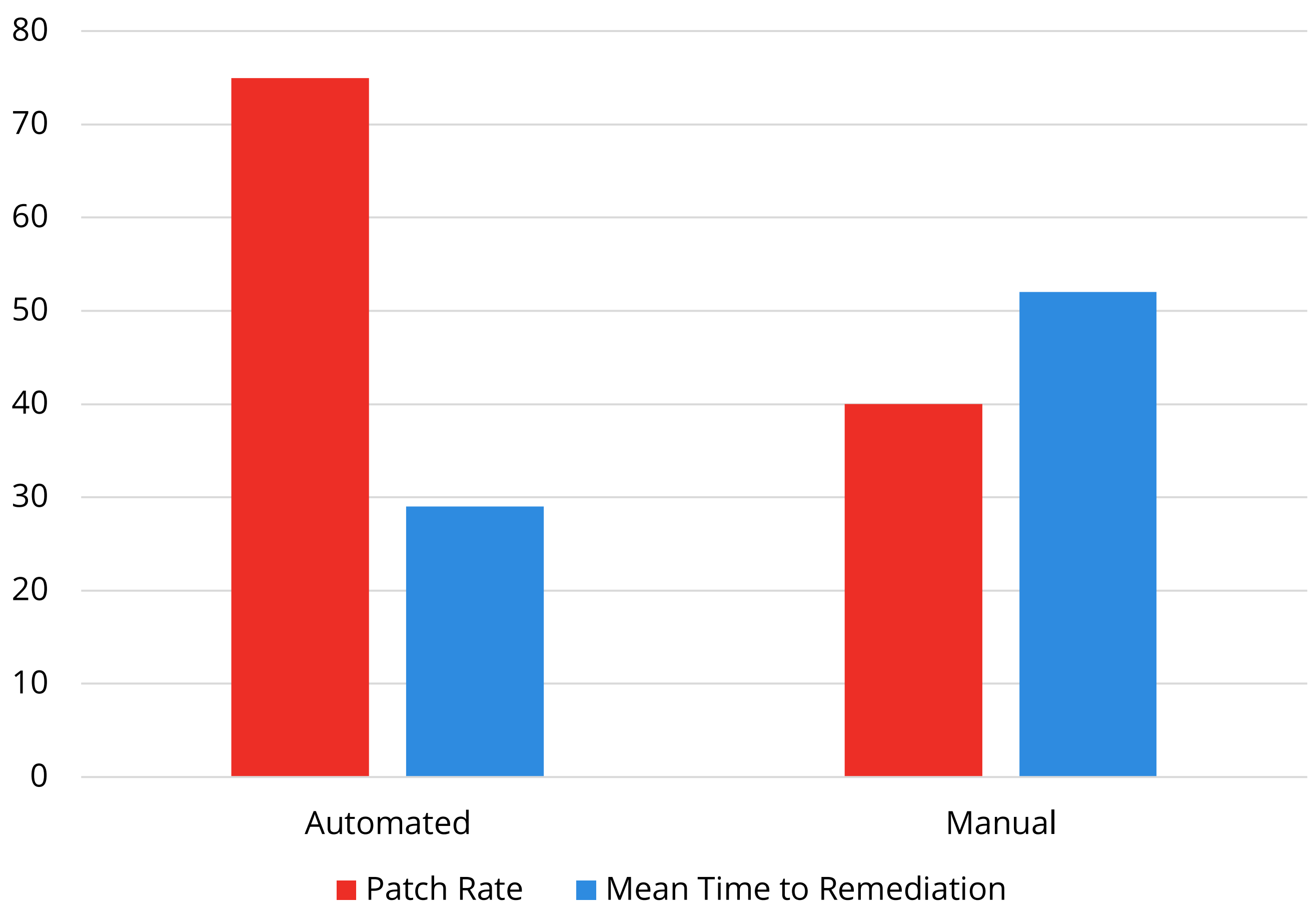
Automation is Key

89.5%

Improvement in Patching Rates

43.1%

Improvement in MTTR Speed

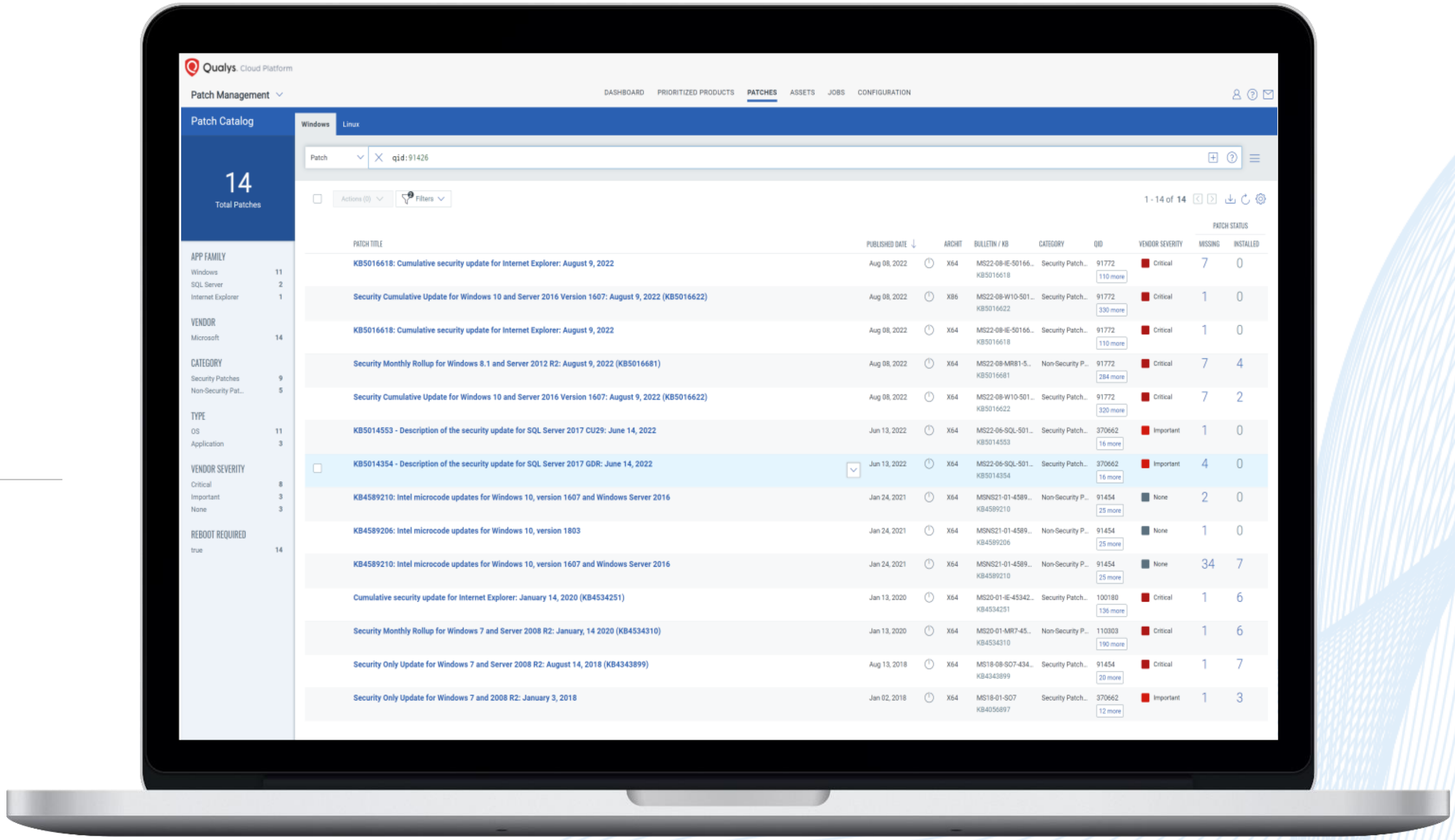


QSC23 | Get More Security

Vulnerability ≠ Patch

Save your IT time – automatically map vulnerabilities to the right patches and configuration changes required for remediation!

- ✓ Prioritize what to patch based on real risk reduction



qid:91426

14
Total Patches

APP FAMILY

Windows	11
SQL Server	2
Internet Explorer	1

VENDOR

Microsoft	14

CATEGORY

Security Patches	9
Non-Security Pat...	5

TYPE

OS	11
Application	3

VENDOR SEVERITY

Critical	8
Important	3
None	3

REBOOT REQUIRED

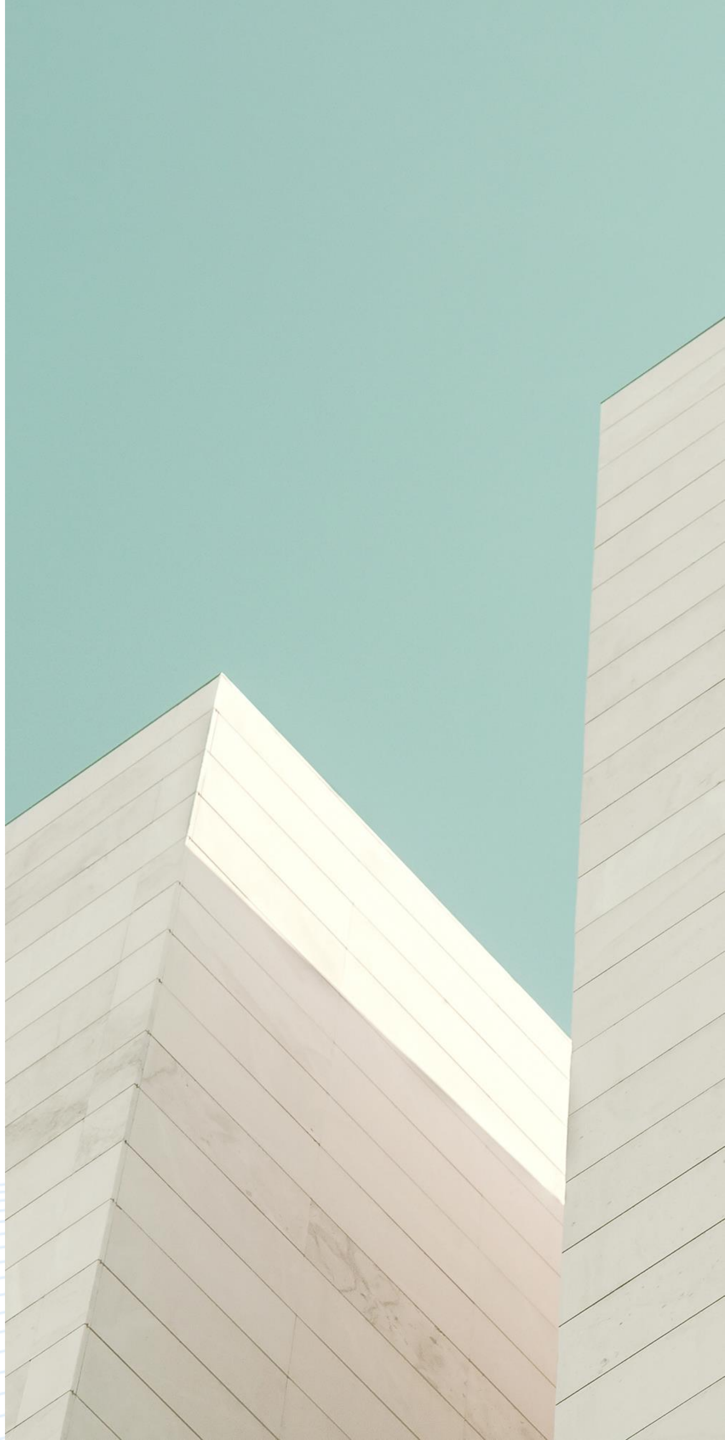
true	14

PATCH TITLE	PUBLISHED DATE ↓	ARCHIT	BULLETIN / KB	CATEGORY	QID	VENDOR SEVERITY	PATCH STATUS MISSING	PATCH STATUS INSTALLED
KB5016618: Cumulative security update for Internet Explorer: August 9, 2022	Aug 08, 2022	X64	MS22-08-IE-50166... KB5016618	Security Patch...	91772 110 more	🟥 Critical	7	0
Security Cumulative Update for Windows 10 and Server 2016 Version 1607: August 9, 2022 (KB5016622)	Aug 08, 2022	X86	MS22-08-W10-501... KB5016622	Security Patch...	91772 330 more	🟥 Critical	1	0
KB5016618: Cumulative security update for Internet Explorer: August 9, 2022	Aug 08, 2022	X64	MS22-08-IE-50166... KB5016618	Security Patch...	91772 110 more	🟥 Critical	1	0
Security Monthly Rollup for Windows 8.1 and Server 2012 R2: August 9, 2022 (KB5016681)	Aug 08, 2022	X64	MS22-08-MR81-5... KB5016681	Non-Security P...	91772 284 more	🟥 Critical	7	4
Security Cumulative Update for Windows 10 and Server 2016 Version 1607: August 9, 2022 (KB5016622)	Aug 08, 2022	X64	MS22-08-W10-501... KB5016622	Security Patch...	91772 320 more	🟥 Critical	7	2
KB5014553 - Description of the security update for SQL Server 2017 CU29: June 14, 2022	Jun 13, 2022	X64	MS22-06-SQL-501... KB5014553	Security Patch...	370662 16 more	🟥 Important	1	0
KB5014354 - Description of the security update for SQL Server 2017 GDR: June 14, 2022	Jun 13, 2022	X64	MS22-06-SQL-501... KB5014354	Security Patch...	370662 16 more	🟥 Important	4	0
KB4589210: Intel microcode updates for Windows 10, version 1607 and Windows Server 2016	Jan 24, 2021	X64	MSNS21-01-4589... KB4589210	Non-Security P...	91454 25 more	■ None	2	0
KB4589206: Intel microcode updates for Windows 10, version 1803	Jan 24, 2021	X64	MSNS21-01-4589... KB4589206	Non-Security P...	91454 25 more	■ None	1	0
KB4589210: Intel microcode updates for Windows 10, version 1607 and Windows Server 2016	Jan 24, 2021	X64	MSNS21-01-4589... KB4589210	Non-Security P...	91454 25 more	■ None	34	7
Cumulative security update for Internet Explorer: January 14, 2020 (KB4534251)	Jan 13, 2020	X64	MS20-01-IE-45342... KB4534251	Security Patch...	100180 136 more	🟥 Critical	1	6
Security Monthly Rollup for Windows 7 and Server 2008 R2: January, 14 2020 (KB4534310)	Jan 13, 2020	X64	MS20-01-MR7-45... KB4534310	Non-Security P...	110303 190 more	🟥 Critical	1	6
Security Only Update for Windows 7 and Server 2008 R2: August 14, 2018 (KB4343899)	Aug 13, 2018	X64	MS18-08-SO7-434... KB4343899	Security Patch...	91454 20 more	🟥 Critical	1	7
Security Only Update for Windows 7 and 2008 R2: January 3, 2018	Jan 02, 2018	X64	MS18-01-SO7 KB4056897	Security Patch...	370662 12 more	🟥 Important	1	3

IT & Security Teams Harmony

- ✓ Unified view across VM & IT
- ✓ Single source of truth increase collaboration and efficiencies in what to remediate
- ✓ Support all IT patch deployment workflows
- ✓ RBAC for “separation” where needed
- ✓ Complements your SCCM/WSUS where needed

Bridge the Gap between Security & IT Teams



Roadmap

What’s Been Delivered. What’s Around the Corner

Q4, Q1 2022/2023

Remediation on Any Device

- NEW: MacOS (OS and 3rd party), Alma, Ubuntu, Debian, Oracle Linux, SUSE.
- Business reports and improved operational reports
- Linux & Mac patch automation
- Automated Phased patch deployment

ServiceNow Integration

- Create change tickets based on open vulns and remediate directly from ServiceNow

Coming in 2023

Risk-Based Product Patching

- Focus on patching products that reduce most risk

Cyber Remediation Insights

- Actionable recommendations on how to best fix vulnerabilities

Remediation Library

- Qualys generated content to fix vulns without a patch

Reporting

- Further improve business and operational reporting

2023 and Beyond

Virtual Patching

- Temporarily protect assets that cannot be patched

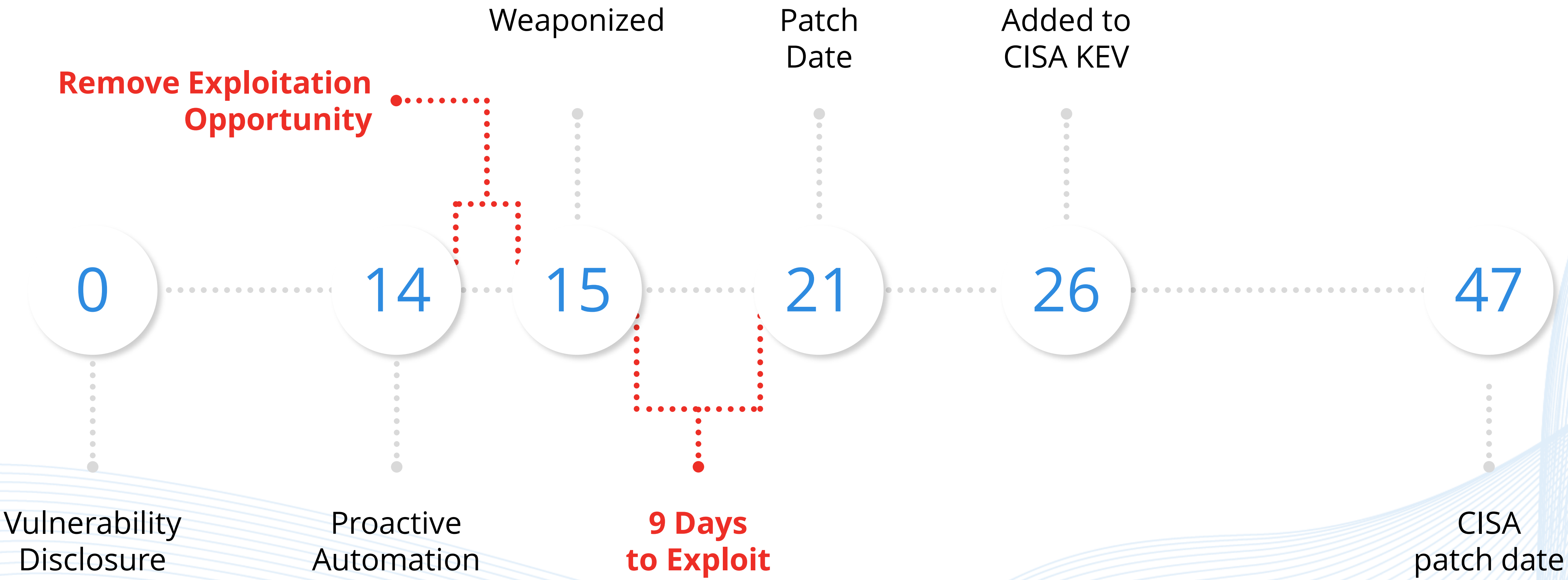
Pre/Post Actions Library

- Manage pre/post actions in libraries
- Import actions from Qualys “canned” library

Real World Risk Reduction - 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%

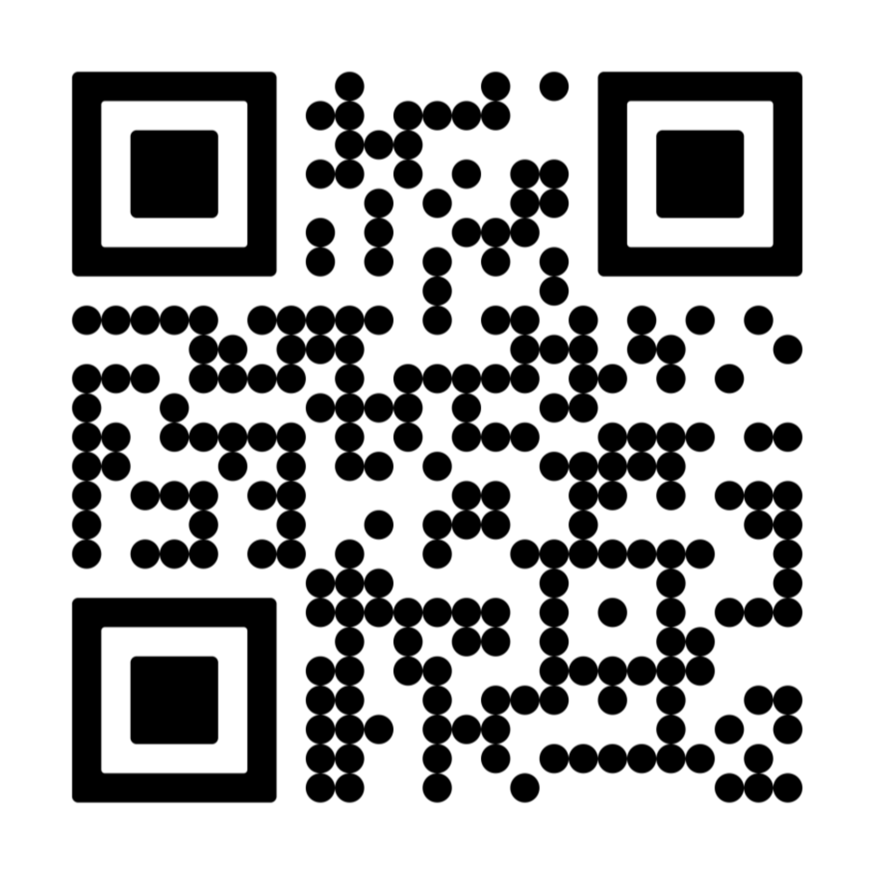
Ideal Vulnerability Lifecycle



Download:

2023 Qualys **TruRisk Research Report**

SCAN ME



https://www.qualys.com/forms/tru-report/

Qualys®

Customer Proof Point Slide

Qualys Security Conference