Qualys.
ROCon 25
The Risk Operations Conference
AMERICAS

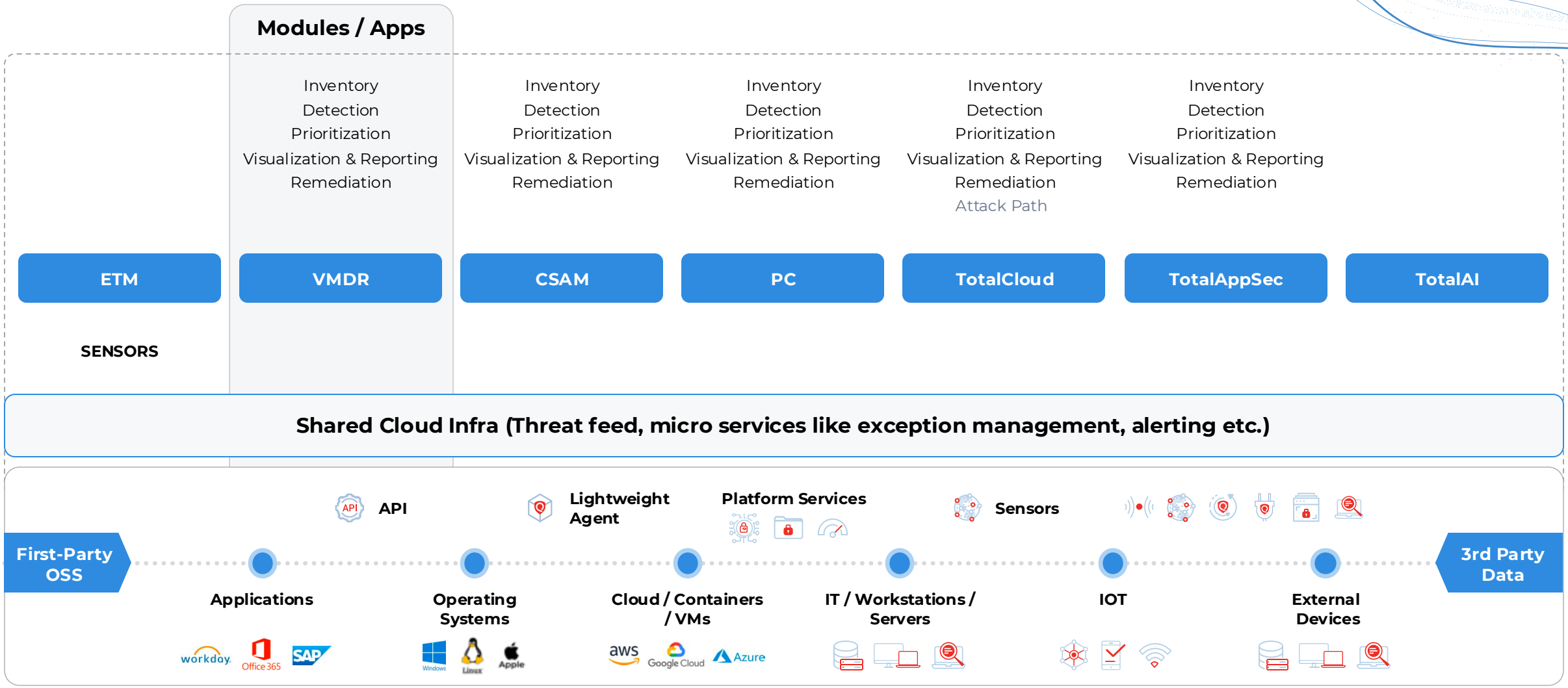
Innovations to Power your Risk Operations Center (ROC)

Shailesh Athalye
Senior Vice President,
Product Management and GTM

Risk Operations Center (ROC)

How ROC gets operational with Qualys Innovations

Previous view of the Platform



Qualys TruRisk Platform

Qualys. ROCon 25
The Risk Operations Conference
AMERICAS

Use-cases

CTEM	ASPM	CNAPP	Cyber Risk Quantification	Compliance & Audit
Cyber Risk Management	**App Security (ASPM)**	**Money-minded CNAPP**	**CRQ**	**ETM Audit**

Enterprise TruRisk Management (ETM)

Native Agentic AI

Threat Intelligence
TruLens

Asset Intelligence
EOL/EOS, EASM

Business Context
GRC/BIA/Cyber Insurance

Exposures

Qualys Sensors

VMDR | TC | TAS | PC | ISPM | ...

3rd Party Sensors

Tenable | CRWD | Wiz | MS Defender | ...

Qualys.
ROCon 25
The Risk Operations Conference
AMERICAS

The World's First
ROC in the Cloud
QUALYS

Enterprise TruRisk Management

Qualys Enterprise TruRisk Management (ETM)

Qualys. ROCon 25 The Risk Operations Conference AMERICAS

First Risk Operations Center (ROC)

885 Critical TruRisk™ Score

Unified Asset Inventory → **Risk Factors Aggregation** → **Threat Intelligence** → **Business Context** → **Risk Prioritization** → **Risk Response Orchestration** → **Compliance & Executive Reporting**

Security and Risk Findings | Risk Identification

(Built in threat intel feeds, enriched with in-house vuln research)

(CMDB, Custom Data Sources)

QUALYS

- Vulnerability
- App Security
- Configuration
- Asset Management
- Compliance
- Attack Surface
- Cloud Security
- AI Security

NON-QUALYS

- Vulnerability Management
- Compliance
- Runtime Security
- Vulnerability Management

THREAT INTELLIGENCE

packet storm, McAfee, FireEye, MISP Threat Sharing, Immunity, GitHub, Canadian Centre for Cyber Security, Reversing Labs, Qualys Vulnerability Research Team, Project Zero, VDE, Kaspersky Industrial CyberSecurity, MITRE ATT&CK, EPSS, Talos, Square Security, GreyNoise Intelligence

BUSINESS CONTEXT

CMDB, GRC, Active Directory

MEASURE | Quantify Cyber Risk in Business Terms

COMMUNICATE | Executive Reporting and Ticketing

ELIMINATE | Patch Mitigate & Track


Unified Asset Inventory | **Risk Factors Aggregation** | Threat Intelligence | Business Context | Risk Prioritization | Risk Response Orchestration | Compliance & Executive Reporting

Unified Asset Discovery & Inventory

Qualys ROCon 25 The Risk Operations Conference AMERICAS

Known Asset Sources

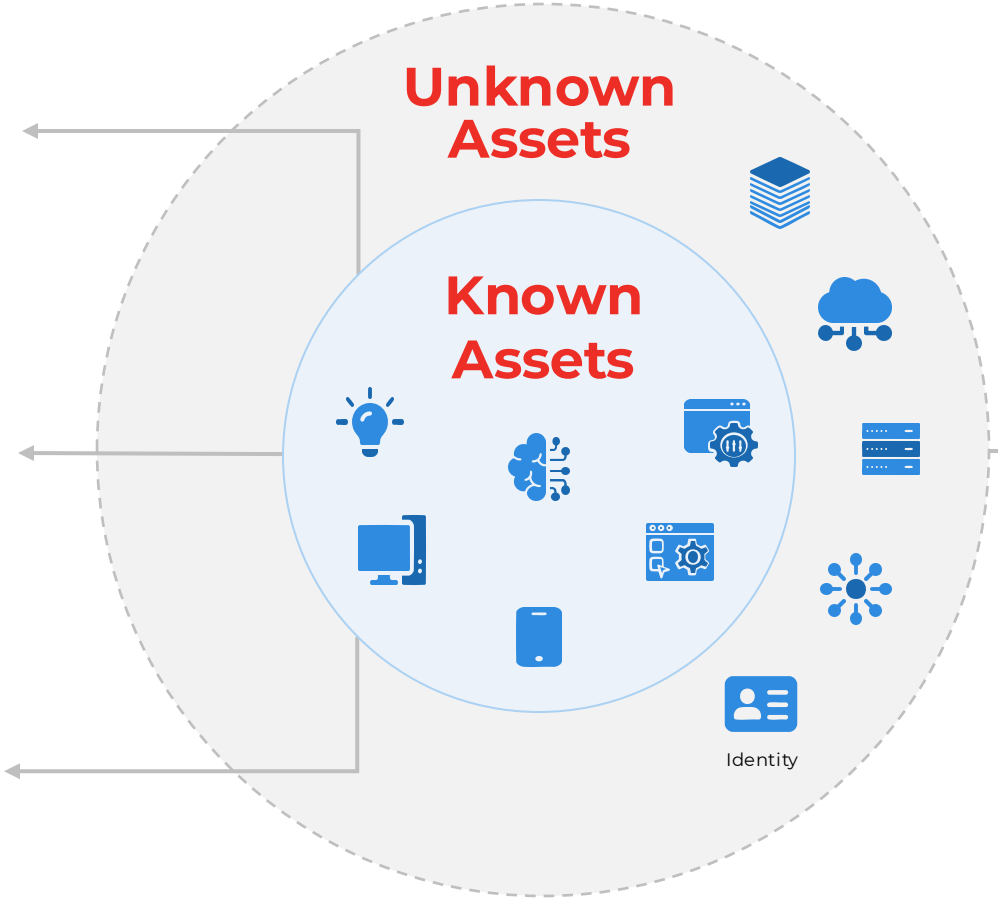
Qualys Native Sensors

Qualys 3rd Party Connectors

WIZ, tenable, CROWDSTRIKE, Microsoft Defender

CMDB Connectors

Active Directory, servicenow, bmc helix, vmware



Unknown External Assets

SHODAN, Scanner, DNS, Whois Identity for everyone

Unified Asset Inventory: Business Context

A Real-World Illustration

Qualys. ROCon 25 The Risk Operations Conference AMERICAS

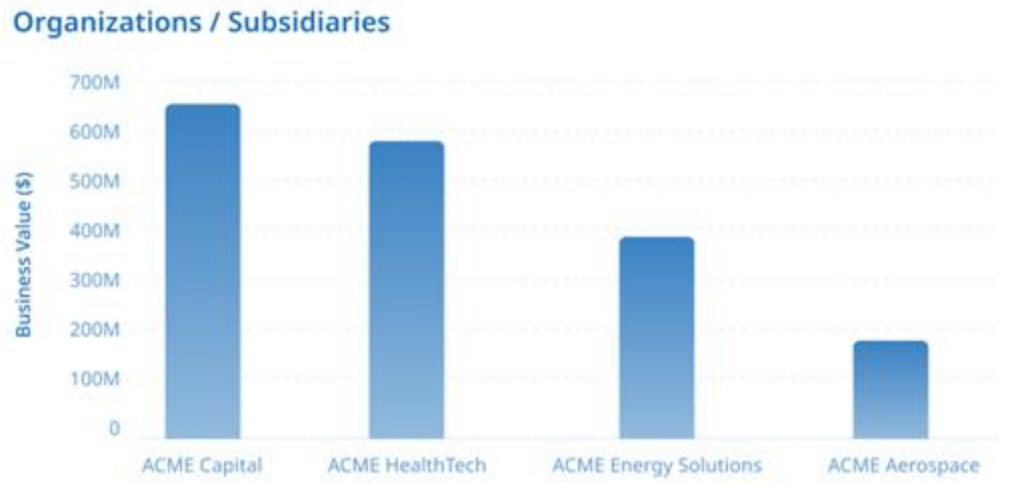
Business Asset Context

Departments
Revenue making Group 1, Department U, Department X

App Tiers w/criticality
Tier 1, Tier 2, Tier 3

Business Value
Dollar value

Users/Ownership
Apps vs Infra



Unified Asset Inventory

Purpose built for cyber risk management

Qualys. ROCon 25 The Risk Operations Conference AMERICAS

Smartly Aggregate & de-duplicate assets

One Inventory to track blind spots for cyber risk

30% more assets included in cyber program

Tech-Debt (EOS/EOL) with risk context

Proactively manage EOL/EOS up to

12 months in advance for risk-based decisions on upgrades

Get hacker's view of your external assets

Mitigate risk from

21% of unknown assets with risky open ports (on average)

With ownership sync, close tickets faster

Close tickets faster with

96% accuracy with bi-directional CMDB sync & ITSM integration

Unified Asset Inventory: Risk Forest

Know exactly which assets drive your TruRisk with a **live asset relationship graph** from business entities → apps → asset types/components, with TruRisk at every node

Risk Forest

01

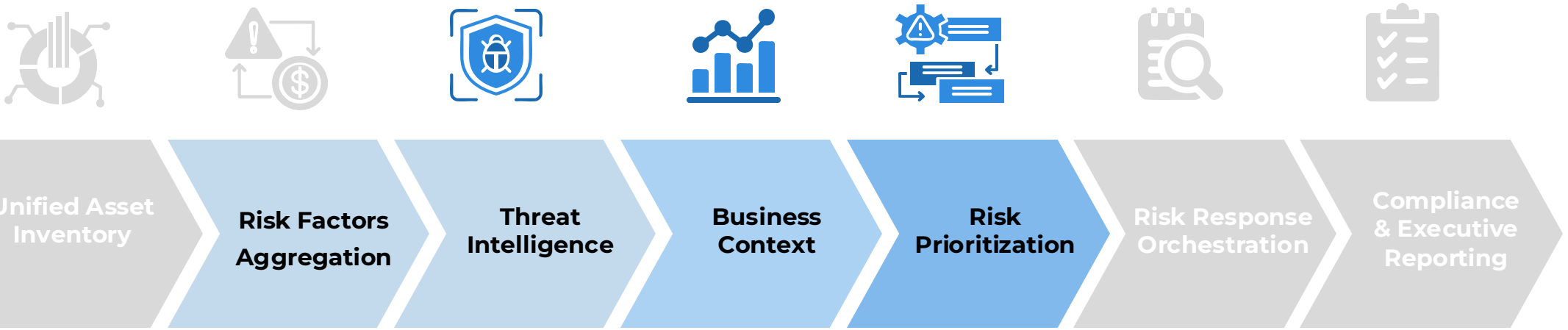
Business-first visualization (not just assets) to find asset components increasing TruRisk

02

Agentic AI to get insights on asset risk, down to root cause of asset components to drive remediation

03

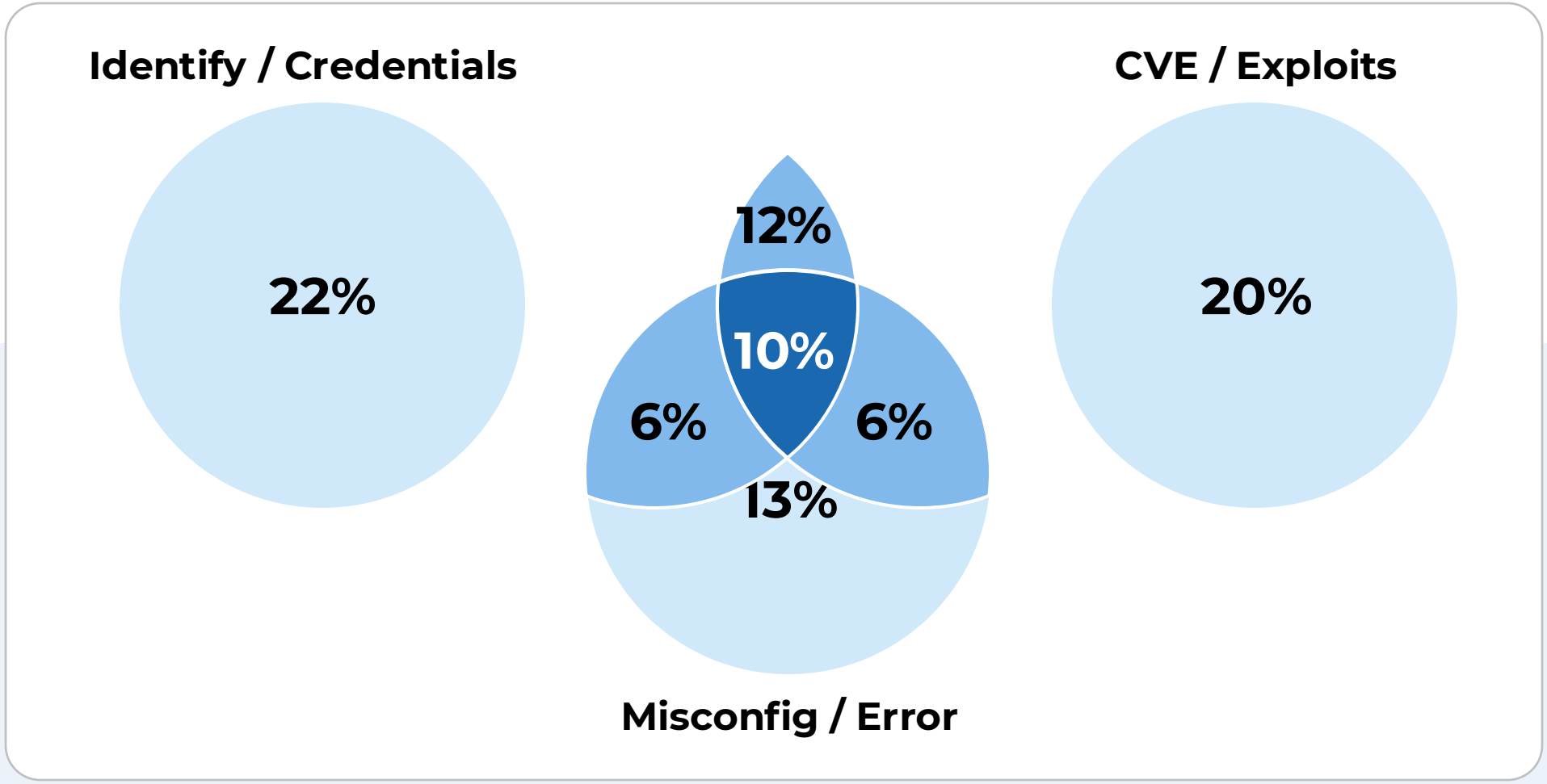
With ownership data, go from risky node to owners, SLAs, and Eliminate plans


Unified Asset Inventory
Risk Factors Aggregation
Threat Intelligence
Business Context
Risk Prioritization
Risk Response Orchestration
Compliance & Executive Reporting

Which exposures should we bring in?

Qualys. ROCon 25 The Risk Operations Conference AMERICAS

34% of the breach vectors are a combination of Identity, CVEs, & Misconfigs.

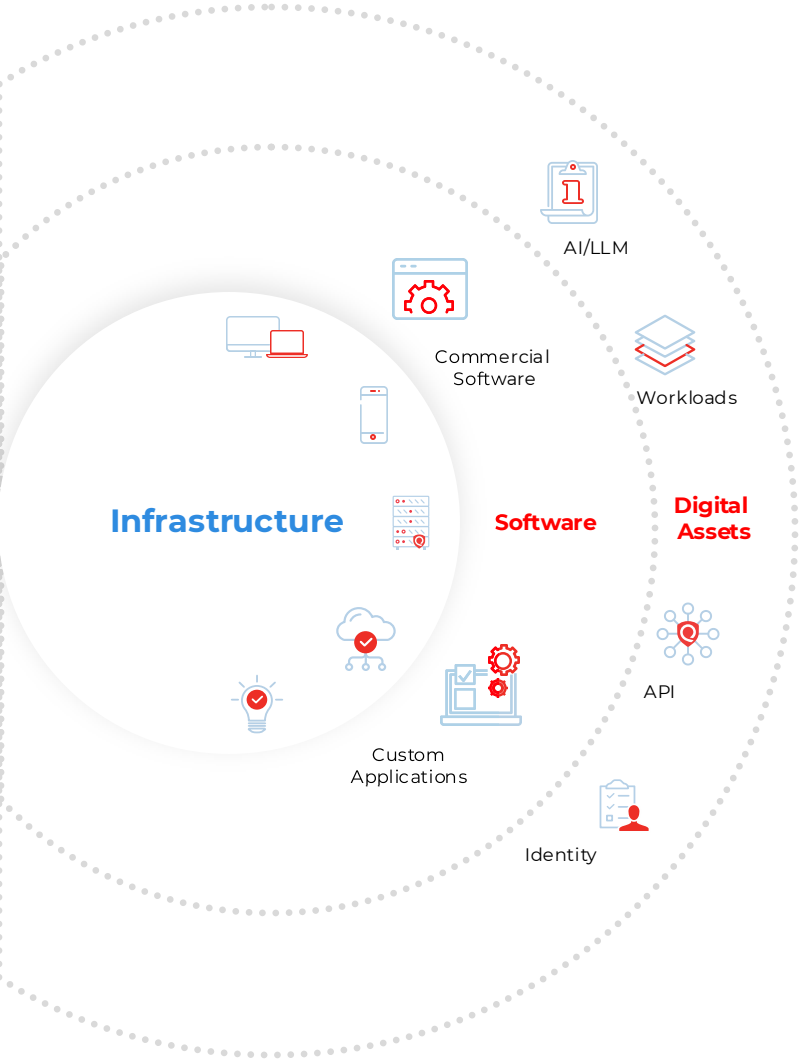


Modeled Overlap of Breach Vectors (DBIR 2025 + M-Trends 2025)

One Security Finding Spans Across Multiple Environments

Multiple SPM tools and Scattered exposures...

Qualys. ROCon 25
The Risk Operations Conference
AMERICAS



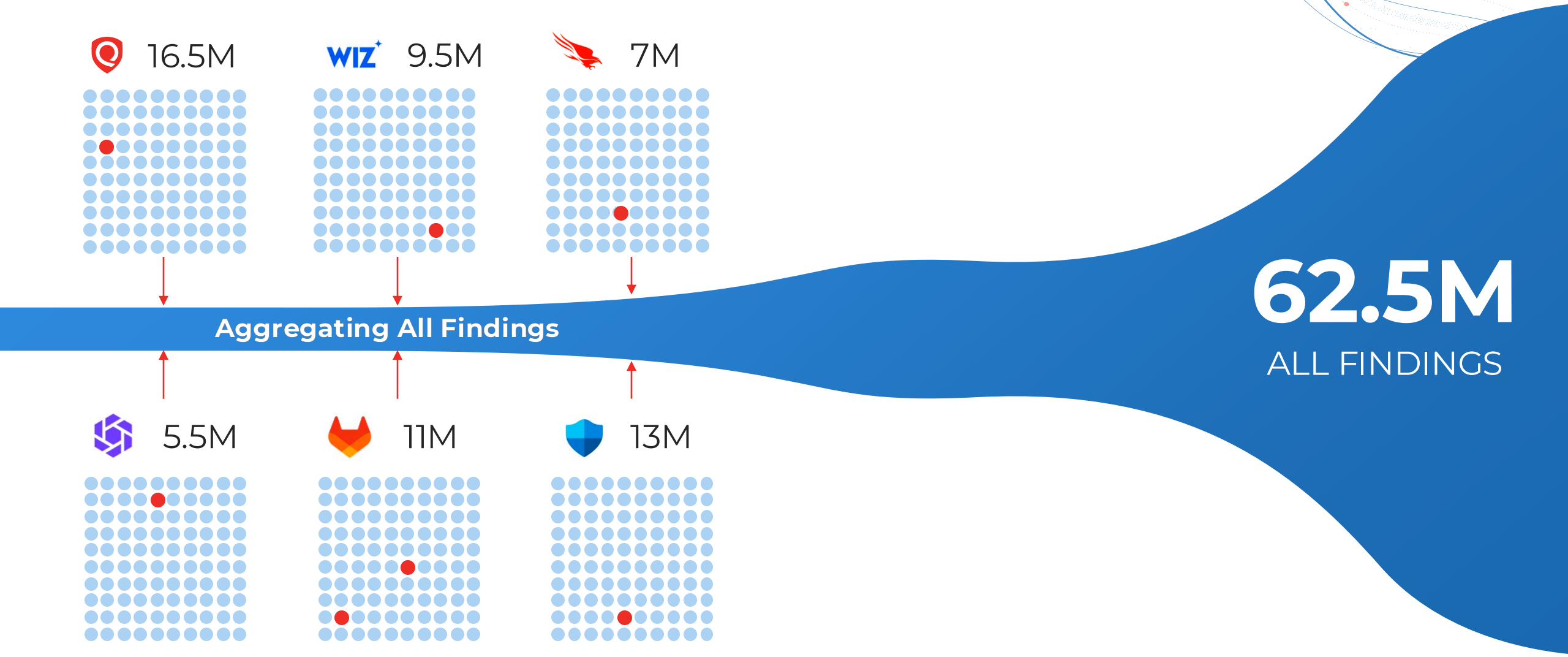
VM	CSPM
ISPM	DSPM
SSPM	AISPM

- Asset Critically
- Location of the Asset
- Infra Vulnerabilities
- Infra, DB misconfigurations
- Certificates
- Open-source software vulns
- EOL Software
- Web Application vulns
- Cloud Misconfigurations
- Unauthorized software, Absence of security tools
- External Attack Surface/Exposures – ports, services

*Enterprises have **70+ security tools on average**

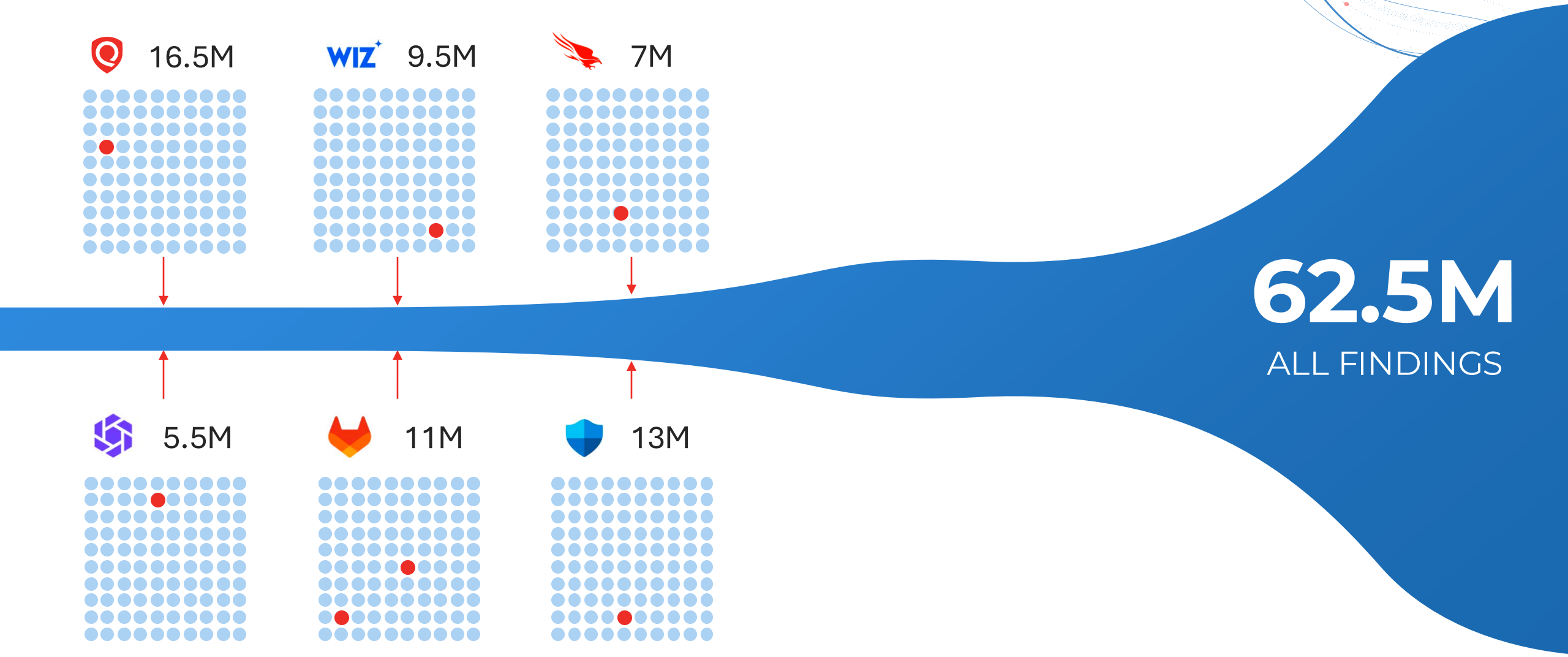
Aggregate millions of exposures effectively

Qualys. ROCon 25
The Risk Operations Conference
AMERICAS



Aggregate millions of exposures effectively

Qualys. ROCon 25
The Risk Operations Conference
AMERICAS



Democratizing Threat Intel through Award Winning Threat Research Unit (TRU)

Qualys ROCon 25
The Risk Operations Conference
AMERICAS

Continuously curated and auto-cross-mapped to every security finding for prioritization by 120+ threat engineers

25+ Threat Sources

McAfee
GitHub
MISP Threat Sharing
Canadian Centre for Cyber Security
Cybersecurity & Infrastructure Security Agency
FireEye
packet storm
VDE
Reversing Labs
MITRE ATT&CK
Kaspersky Industrial CyberSecurity
GreyNoise Intelligence
NSA
Project Zero
Square Security
EPSS Exploit Prediction Scoring System
Talos
Google
Immunity
metasploit

Prioritize the exposure with threat-context

Qualys. ROCon 25
The Risk Operations Conference
AMERICAS

7.6
CVSS
CVE-2013-3900


46 Exploits


Weaponized Exploit Exists


2 Malware


10 Threat Actors


CISA KEV


0.74
EPSS


2 Month
Trending


Dec 2013
NVD published


July 2024
CISA KEV

9.5

Qualys Vulnerability Scoring System **(QVSS)**

Deprioritize the exposure, if no threat-context

Qualys. ROCon 25
The Risk Operations Conference
AMERICAS

9.9

CVSS

CVE-
CVE-2021-34458

0 Exploits

No POC
No Weaponization

0 Malware

0 Threat Actors

NOT in
CISA KEV

0.01
EPSS

NO
Trending

6.5

QVSS

Prioritizing risky exposures which Matter, from millions of exposures

Qualys. ROCon 25
The Risk Operations Conference
AMERICAS

Risk Operations Center (ROC)

62.5M
ALL FINDINGS

2.17 M (4%)
Risky Exposures (QDS/QVSS)

304K (<1%)
Prioritized exposures for Business (with ACS context)

96% Reduction

99% Reduction

$3.12 M
Cost of Remediation

THREAT INTELLIGENCE

Dark web trending
Weaponized by threat actors
Malware/Ransomware attacks in the industry

$612K
Cost of Remediation

ASSET CONTEXT

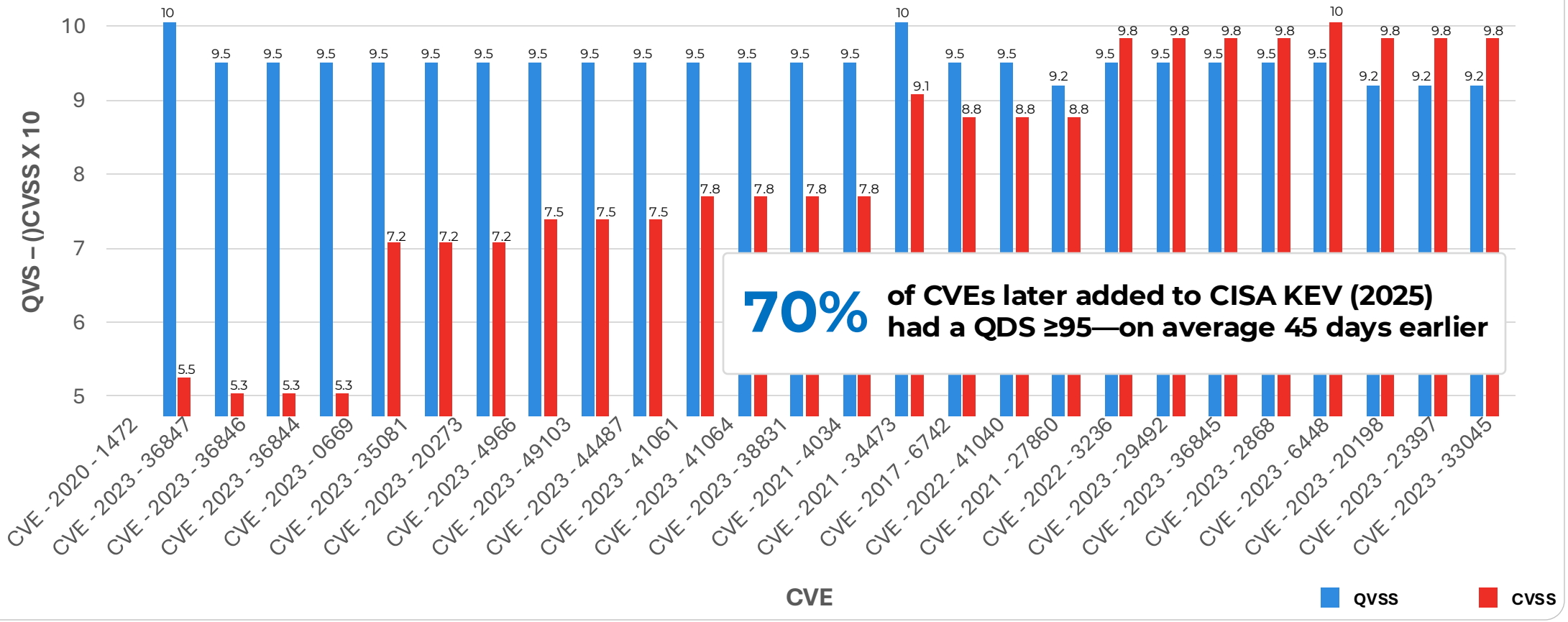
Business Critical Assets (PCI, Internet Facing, DB, Revenue making App

$311K
Cost of Remediation

With TruRisk, You are Prioritizing Vulnerabilities before they are in CISA KEV

Qualys. ROCon 25 The Risk Operations Conference AMERICAS

The graph depicts QVSS (QDS is x10) vs CVSS comparison for sample CVEs from CISA KEVs (2025) for their criticality 45 days before they got added to CISA KEV.

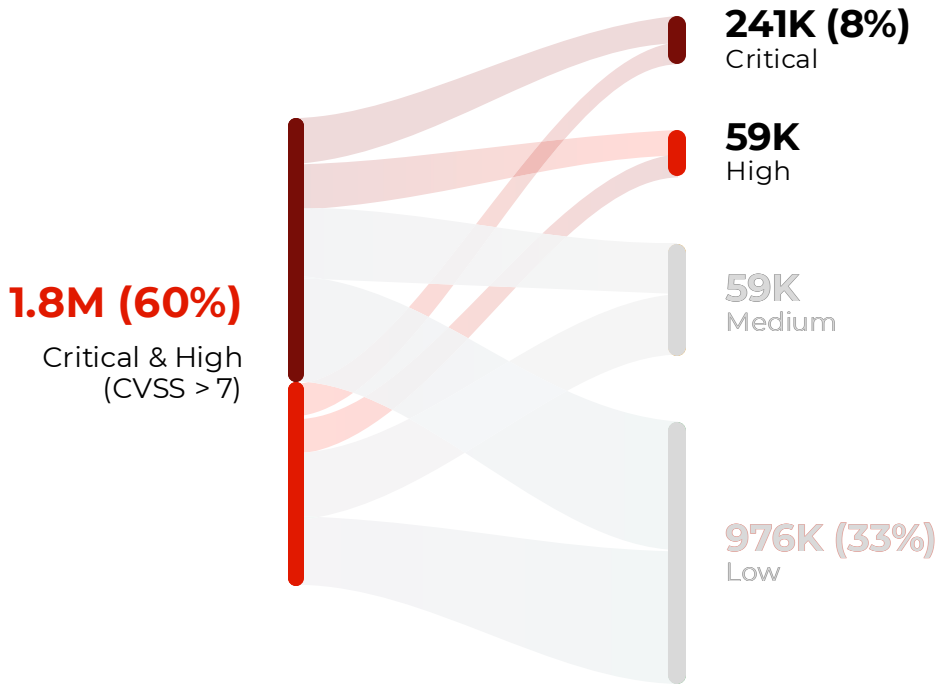


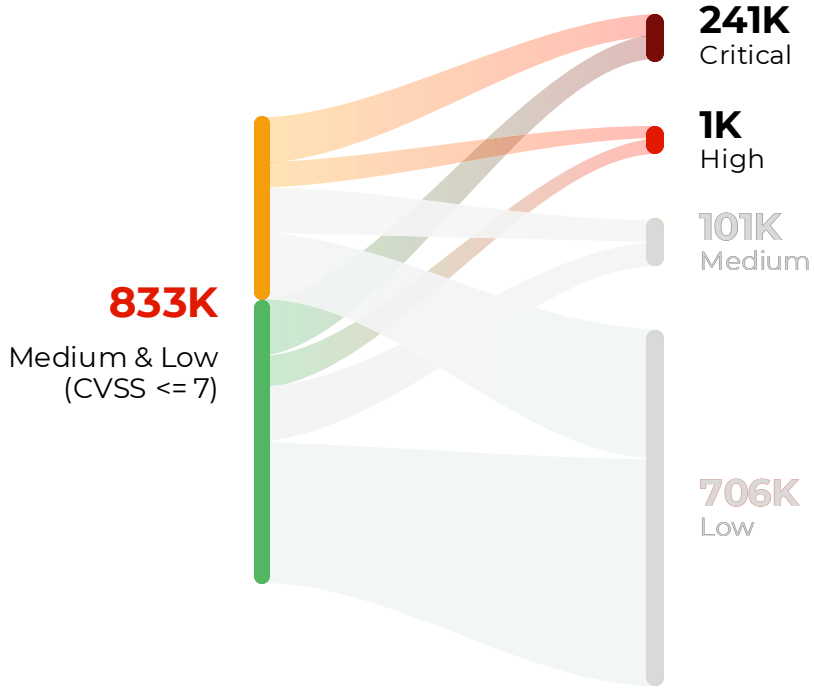
70% of CVEs later added to CISA KEV (2025) had a QDS ≥95—on average 45 days earlier

Risk Prioritization and De-Prioritization

Qualys. ROCon 25
The Risk Operations Conference
AMERICAS

3.02M Total exposures





84.9% of critical & high CVSS reduced to Low & Medium severity.

3.0% of critical & high vulnerabilities are overlooked by CVSS.

Qualys. ROCon 25
The Risk Operations Conference
AMERICAS

Risk Exposures

Combines Asset Environmental Factors Considers Only

- Active Service/Process
- Attack Path
- Public Exploit
- Public Asset Exposure

WIZ

Medium	CVE-2023-44487
High	CVE-2020-1147
Critical	CVE-2021-41303
Low	CVE-2023-42282
High	CVE-2025-0411
Medium	CVE-2020-11023

CROWDSTRIKE

Medium	CVE-2023-44487
Low	CVE-2023-42282
High	CVE-2020-1147
High	CVE-2025-0411
Medium	CVE-2020-11023
Critical	CVE-2021-41303

QualysTruRisk™

Qualys Threat DB of 25+ Threat Intel Sources | Qualys Research | Vulnerability Environmental

McAfee, FireEye, packet storm, GitHub, CISA, MISP Threat Sharing, Canadian Centre for Cyber Security, VDE, ReversingLabs, metasploit, GreyNoise, MITRE ATT&CK, Kaspersky Industrial CyberSecurity, Talos, Google, EPSS

- Dark web chatter
- Trending patterns
- POC vs Weaponization
- Easy vs complex exploitation (remote vs local)
- Threat actors associated
- Exploited by Malware, Ransomware?
- Celebrity

Risk Exposures Accurately Prioritized

100 | 95 | 90 | 80 | 70 | 60 | 50 | 40 | 30 | 20 | 10

CVE-2023-4487

- POC of Exploit Exists
- Unattributed Threat Actors
- Trending In Mar & Apr 2025
- CISA Known Exploited Vulnerabilities
- CVSS – **7.5** & EPSS – **0.94437**

CVE-2020-1147

- POC Exists and Weaponized
- CISA Known Exploited Vulnerabilities
- Trending in Mar & Apr 2025
- CVSS – **7.8** & EPSS – **0.92695**

CVE-2020-11203

- POC of Exploit Exists
- Threat Actors – **Emissary Panda, Comment Panda**
- CISA Known Exploited Vulnerabilities
- Trending in Mar & Apr 2025
- CVSS – **6.1** & EPSS – **0.11526**

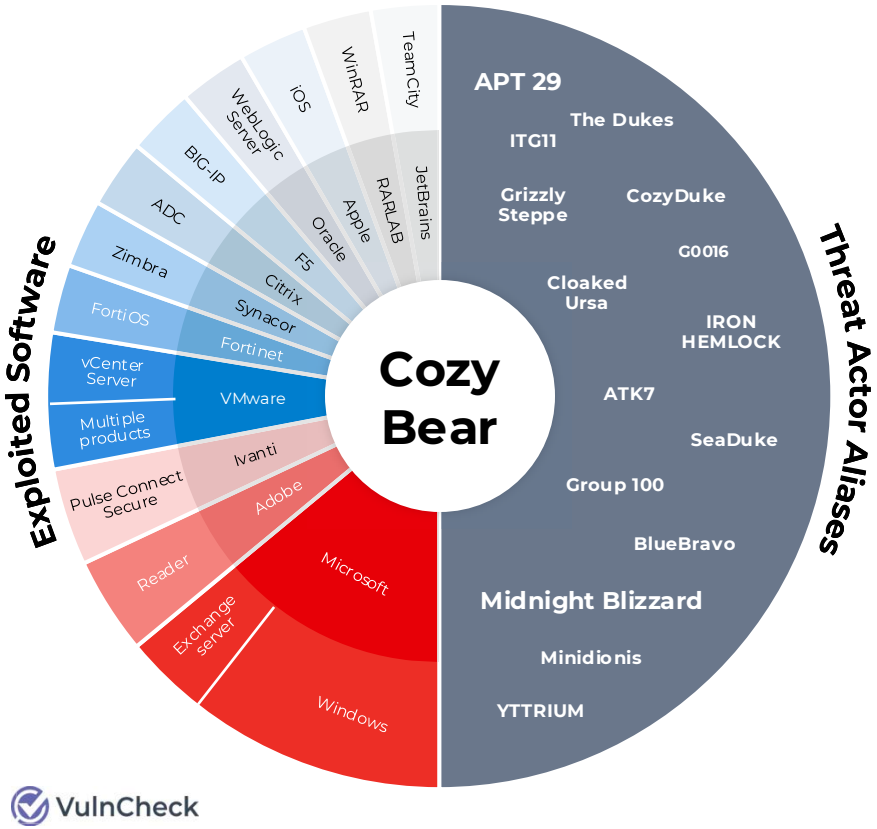
CVE-2021-41303

- Last Trending in Mar 2025
- CVSS – **9.8** & EPSS – **0.65449**
- CVE Is Not Exploited and No
- Other Significant Contributing Factors Observed

Risk of trending threats in the industry

Qualys. ROCon 25
The Risk Operations Conference
AMERICAS

Threat Actor Profile – Cozy Bear (Espionage)



VulnCheck

MITRE ATT&CK® TECHNIQUES					
T1001	T1053-005	T1090-003	T1203	T1547-009	T1566-002
T1027	T1059-006	T1090-004	T1204-002	T1547-001	T1583-006
T1027-002	T1059-001	T1095	T1218-011	T1548-002	T1587-003
T1043	T1070-004	T1102-002	T1546-003	T1550-003	
T1047	T1078-002	T1190	T1546-008	T1566-001	

Known Exploited CVEs			
CVE-2010-0232	CVE-2019-9670	CVE-2020-14882	CVE-2021-36934
CVE-2010-4398	CVE-2019-11510	CVE-2021-21972	CVE-2022-30170
CVE-2013-0640	CVE-2019-19781	CVE-2021-26855	CVE-2023-38831
CVE-2013-0641	CVE-2020-4006	CVE-2021-1879	CVE-2023-42793
CVE-2018-13379	CVE-2020-5902	CVE-2021-22893	

Suspected Victim Countries

United States, Belgium, Ukraine, Kazakhstan, South Korea
Mexico, Portugal, Romania, China, Japan
Brazil, Georgia, Turkey, India, New Zealand

Target Industries

Government
Private Sector

- What are the trending threats for my industry’
- What are my exposures
- What's my risk – high value assets, exposures
- Plan to reduce risk

Adversary based Risk Prioritization & Remediation

Qualys. ROCon 25
The Risk Operations Conference
AMERICAS

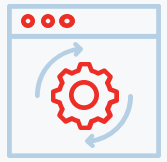
TruLens

01

Industry threat knowledge

ClOP

Scattered Spider



02

Exposures

Vulns

Identities

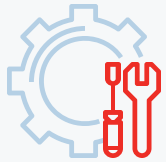
Misconfigs

03

Prioritized Risk

High value assets

Internet facing assets



04

Remediation

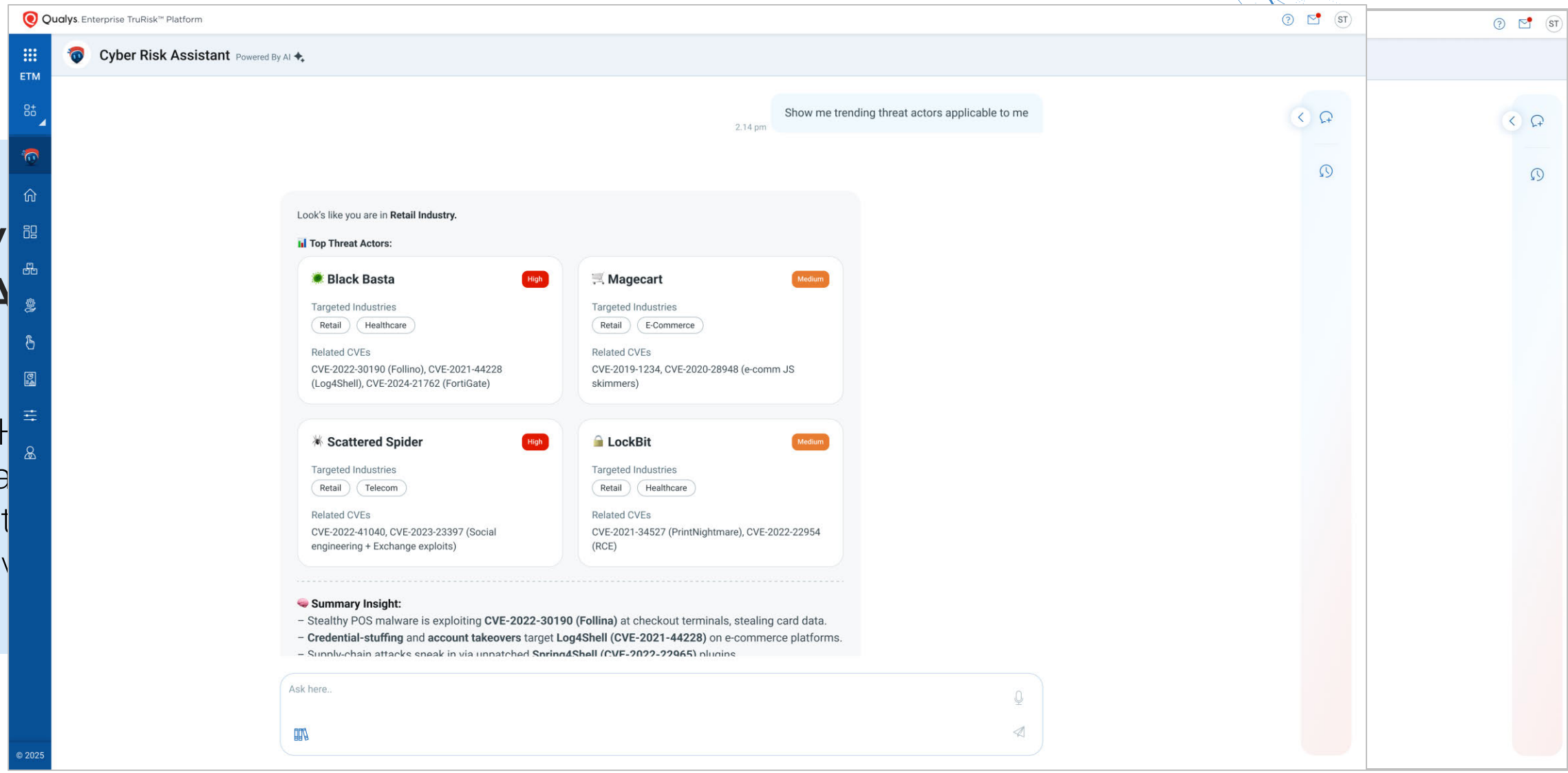
Patch

Mitigation

Qualys ROCon 25
The Risk Operations Conference
AMERICAS

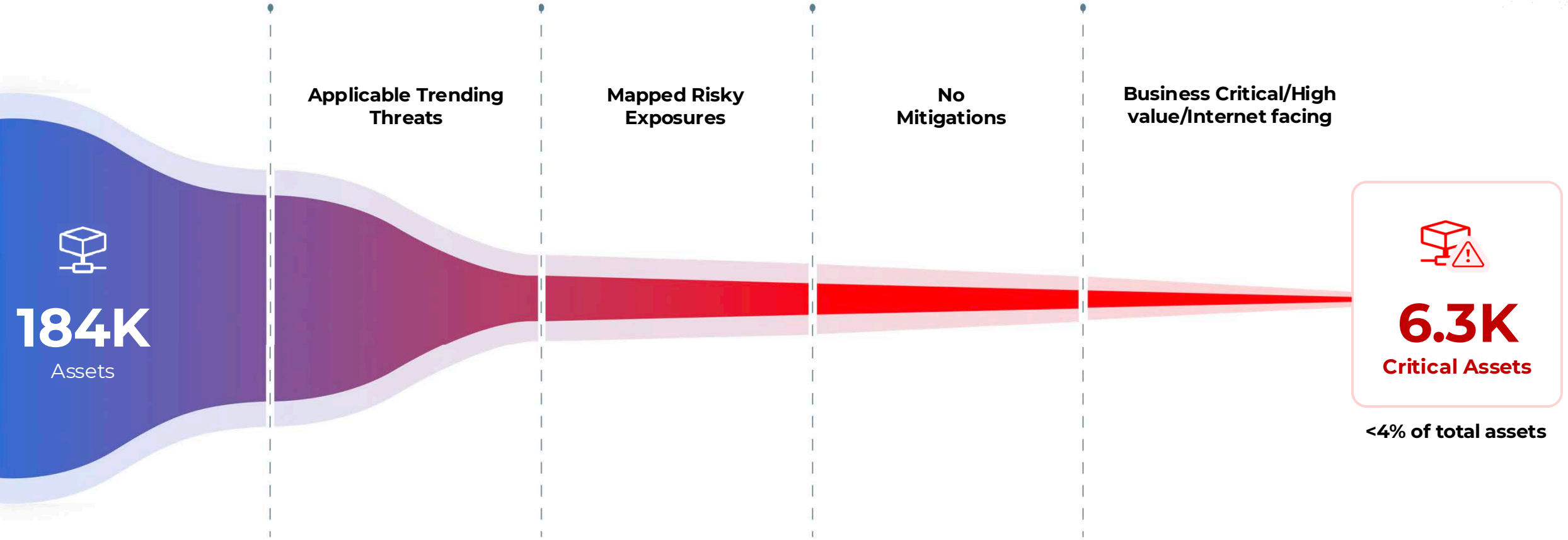
Cy
A

H
na
evaluat
posture v



TruLens: Prioritizing Assets with Toxic Combinations

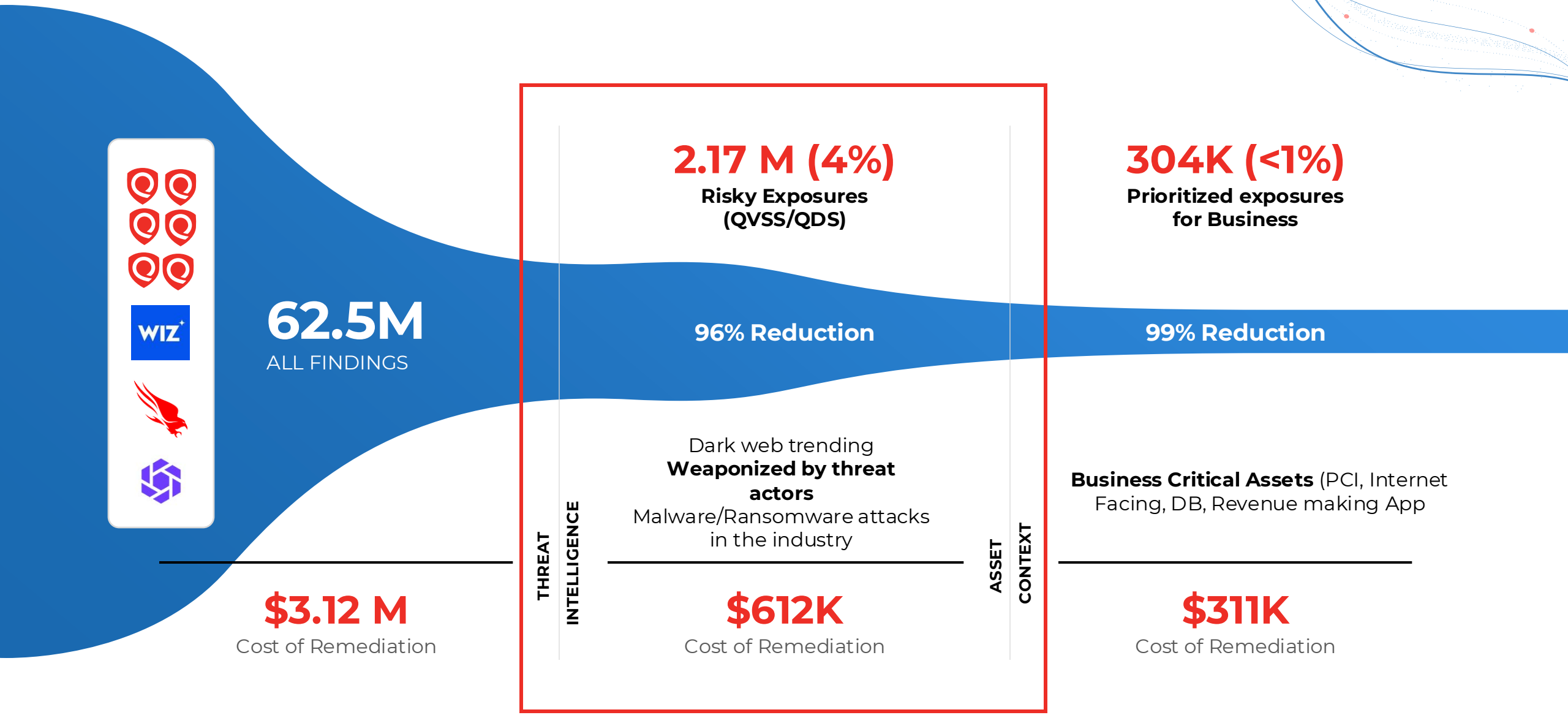
Qualys. ROCon 25
The Risk Operations Conference
AMERICAS



<4% of total assets

Prioritizing risky exposures which Matter, from millions of exposures

Qualys. ROCon 25
The Risk Operations Conference
AMERICAS



Qualys. ROCon 25
The Risk Operations Conference
AMERICAS

Prioritize riskiest vulnerabilities for your environment

You have the working Mitigations you did not know about

You have failed mitigations/know about

Mitigated

25%

Out of 2.17M (4%)

Exposures (Risky vulnerabilities on critical assets – Internet, PCI, business apps)

10%

confirmed exploitation

What if I tell you

Out of 2.17M (4%)

Exposures (Risky vulnerabilities on critical assets – Internet, PCI, business apps)

Qualys. ROCon 25 The Risk Operations Conference AMERICAS

You have the working Mitigations you did not know about	Mitigations failed
33 % Mitigated	10% confirmed exploitation

Validate Exploitability of risky vulnerabilities in your environment

Qualys. ROCon 25 The Risk Operations Conference AMERICAS

1/3rd

Mitigations/Security controls Fail

1/3rd times the theoretical Mitigations/ Security controls failed to prevent exploitation in production

~50%

CISA KEV List

Known Exploited Vulnerabilities could be prevented with validation

01 Gap between risk prioritization based on industry threat intel and actual exploitability in your environment from hacker's eyes

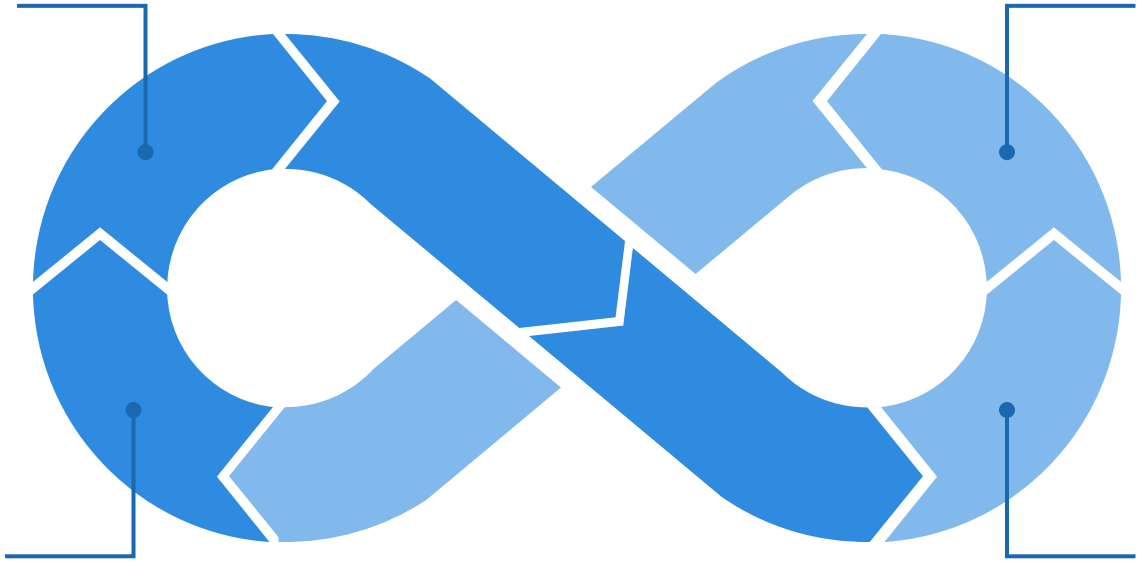
02 BAS teams simulate in non-production environment, relying on data from underlying vulnerability detection and asset attributions

TruConfirm: Validate Exposures, Confirm Exploitation, Accelerate Remediation

Qualys. ROCon 25 The Risk Operations Conference AMERICAS

Exposure Assessment, Detection or collection through VMDR or Vuln exposure data from Tenable, Rapid7, MS Defender

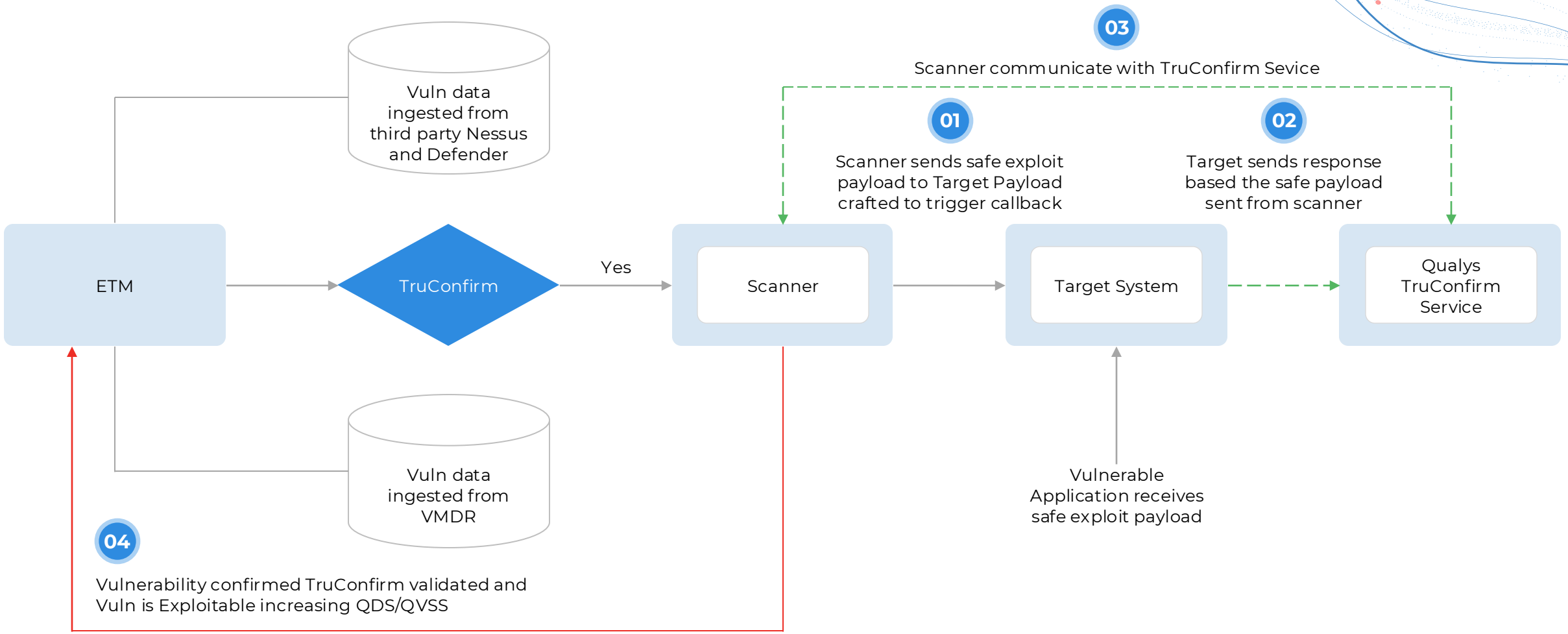
TruRisk Prioritization based on Threats Environmental/business asset context to prioritize risky exposures



TruConfirm provides remediation guidance to patch or mitigate exploitation and reduce TruRisk

TruConfirm scan validates and confirms exploitation using attacker's techniques while validating of mitigation/security controls along the route

TruConfirm: Safe Exploitation Route



This capability extends core TruRisk scoring with real-world exploitation confirmation, helping you prevent exploitation of 88%+ the ransomware vulnerabilities by confirming/validating they celebrity risky vulnerabilities like BlueKeep and Log4Shell are actually exploitable in your specific environment despite of theoretical mitigation controls

Risk prioritization: Misconfigurations…

Assessing CIS/hardening benchmarks to prioritizing risk

CIS Controls for consideration

Bearing in mind the breadth of activity found within this pattern and how actors leverage a wide collection of techniques and tactics, there are a lot of safeguards that organizations should consider implementing. To the right is a small subset of the things an organization could do. They should serve as a starting point for building out your own risk assessments to help determine what controls are appropriate to your organization's risk profile.

Protecting devices

Secure Configuration of Enterprise Assets and Software [4]
- Establish and Maintain a Secure Configuration Process [4.1]
- Establish and Maintain a Secure Configuration Process for Network Infrastructure [4.2]
- Implement and Manage a Firewall on Servers [4.4]
- Implement and Manage a Firewall on End-User Devices [4.5]

Email and Web Browser Protections [9]
- Use DNS Filtering Services [9.2]

Malware Defenses [10]
- Deploy and Maintain Anti-Malware Software [10.1]
- Configure Automatic Anti-Malware Signature Updates [10.2]

Continuous Vulnerability Management [7]
- Establish and Maintain a Vulnerability Management Process [7.1]
- Establish and Maintain a Remediation Process [7.2]

Data Recovery [11]
- Establish and Maintain a Data Recovery Process [11.1]
- Perform Automated Backups [11.2]
- Protect Recovery Data [11.3]
- Establish and Maintain an Isolated Instance of Recovery Data [11.4]

Protecting accounts

Account Management [5]
- Establish and Maintain an Inventory of Accounts [5.1]
- Disable Dormant Accounts [5.3]

Access Control Management [6]
- Establish an Access Granting/ Revoking Process [6.1, 6.2]
- Require MFA for Externally-Exposed Applications [6.3]
- Require MFA for Remote Network Access [6.4]

Security awareness programs

Security Awareness and Skills Training [14]

still one of the breaches

DBIR report **2025**

Qualys. ROCon 25
The Risk Operations Conference
AMERICAS

40%

Avg. Misconfigurations from CIS benchmarks

70%

Misconfigurations mapped to Ransomware Risks

Control ID	Statement	Criticality	Ransomware Risk	Remote Risk	Risk Explanation
CIS Benchmark for IBM DB2 11.x Benchmark			IBM DB2 11		Database
2181	Current list of Groups and User Accounts granted the 'Access this computer from the network' right	URGENT	✅	✅	Allows lateral movement and unauthorized remote access.
CIS Benchmark for Microsoft Windows 10 Benchmark			Microsoft Windows 10		Operating System
2196	Current list of Groups and User Accounts granted the 'Deny Access to this computer from the network' right	CRITICAL	✅	✅	Unauthorized users may access the system remotely.
CIS Benchmark for Mozilla Firefox 102 ESR Benchmark			Mozilla Firefox		Browser
2200	Current list of Groups and User Accounts granted the 'Deny logon through terminal (Remote Desktop) service' right	CRITICAL	✅	✅	Attackers can exploit RDP to gain remote access and deploy ransomware.
CIS Benchmark for Microsoft Internet Explorer 10 Benchmark			Microsoft Internet Explorer 10		Browser
9830	Status of the 'Prevent users from sharing files within their profile' setting	CRITICAL	✅	❌	Ransomware can spread through user-shared folders.
CIS Benchmark for Microsoft Office Enterprise Benchmark			Microsoft Office Enterprise		Middleware
9304	Status of the "Do not preserve zone information in file attachments" setting for Windows users	CRITICAL	✅	❌	Downloaded files lack zone info, allowing ransomware to run without warnings.
CIS Benchmark for Google Chrome Benchmark			Google Chrome		Browser
1318	Status of the 'Enforce password history' setting	URGENT	✅ (Indirectly)	✅	Users may reuse weak or old passwords, aiding brute-force or credential stuffing attacks.
CIS Benchmark for Microsoft Windows 11 Stand-alone Benchmark			Microsoft Windows 11		Operating System
3924	Status of 'Block all Office applications from creating child processes' ASR rule (D4F940AB-401B-4EFC-AADC-AD5F3C50688A)	CRITICAL	✅	❌	Ransomware can use malicious Office macros to spawn additional malware.
CIS Benchmark for Check Point Firewall Benchmark			Check Point Firewall		Network

Prioritize Misconfigurations based on Risk

Qualys. ROCon 25
The Risk Operations Conference
AMERICAS

Misconfiguration

RDP Access Restriction CIS control

+10 **Dark Web**

+10 **Elevated Privileges**

+10 **Threat Actor**

+10 **CIS Top 5 controls**

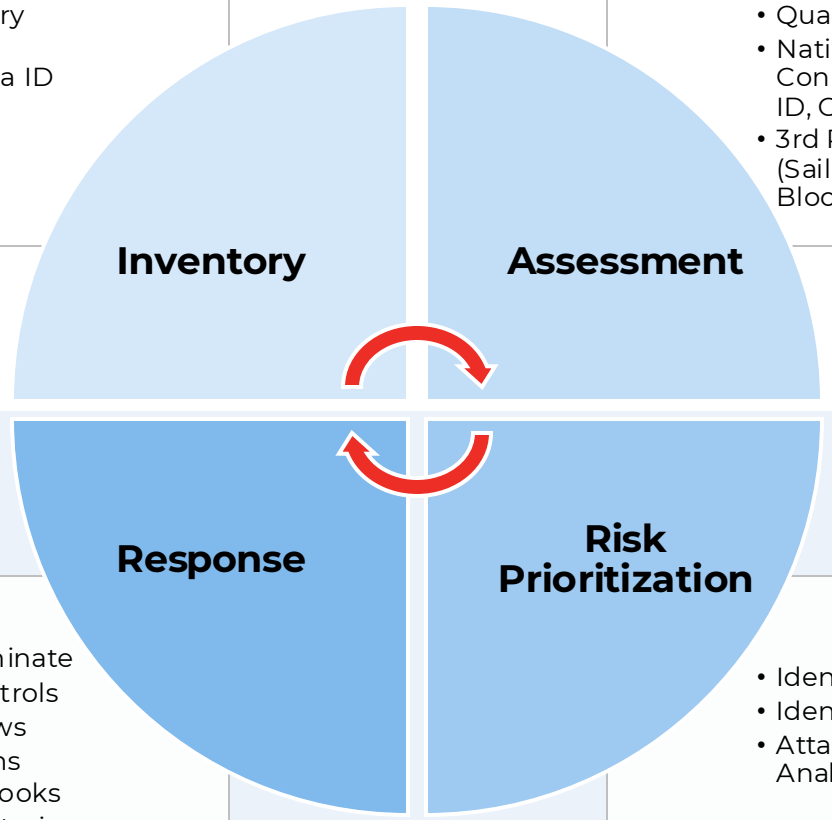
95
Critical

Risk prioritization: Identities…

Integrated with ETM

Comprehensive discovery and inventory of all **human & machine identities**.

- Active Directory (AD)
- Microsoft Entra ID
- Okta
- Ping Identity



- Qualys Agent (AD)
- Native IdP/IDaaS Connector (Entra ID, Okta, Ping)
- 3rd Party Tools (SailPoint, BloodHound, etc.)

Consolidated **identity risk telemetry** from Qualys and third-party solutions.

Orchestrate risk response with **policies, scripts, actions, ITSM workflows, integrity monitoring**.

- TruRisk™ Eliminate
- AD Policy Controls
- ITSM Workflows
- Identity Actions
- Custom playbooks
- Integrity Monitoring

- Identity TruRisk™
- Identity Insights
- Attack Path Analysis

Correlate **Identity TruRisk™** with asset context to prioritize critical "**toxic combinations**" that pose the highest risk

Prioritize Identities based on Risk

Qualys. ROCon 25
The Risk Operations Conference
AMERICAS

5 ICS

Sam Wilson

Weak Password

Active Directory

Missing MFA

Entra ID

Involved in a Tier 0 attack path

Qualys

Externally Exposed Identity

3rd party Intelligence

958

Identity TruRisk™

Prioritizing risky exposures beyond vulnerabilities

Qualys. ROCon 25 The Risk Operations Conference AMERICAS

62.5M
ALL FINDINGS

$3.12 M
Cost of Remediation

THREAT INTELLIGENCE

Risk Operations Center (ROC)

2.17 M (4%)
Risky Exposures

96% Reduction

Dark web trending
Weaponized by threat actors
Malware/Ransomware attacks in the industry

$612K
Cost of Remediation

- Ransomware **vulns (3%)**
- Risky **Misconfigurations (4%)**
- **EASM** asset exposures w/risks **(1.7%)**
- **Identities** at risk **(3%)**

Selection Prioritization Approach

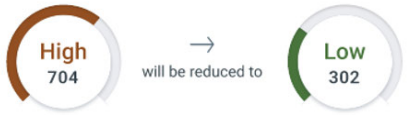
Decide the approach to filter the findings for prioritization. Explore these Qualys-defined templates.

Qualys. ROCon 25 The Risk Operations Conference AMERICAS

Highest Risk Reduction

Critical Vulnerabilities (Ransomware, CISA KEVs) on all assets

Potential TruRisk Reduction



Low Risk Reduction

Patch Critical Vulnerabilities on non-critical assets

Potential TruRisk Reduction

Balanced Risk Reduction

Patch Critical Vulnerabilities on non-critical assets & Mitigate on critical assets

Potential TruRisk Reduction

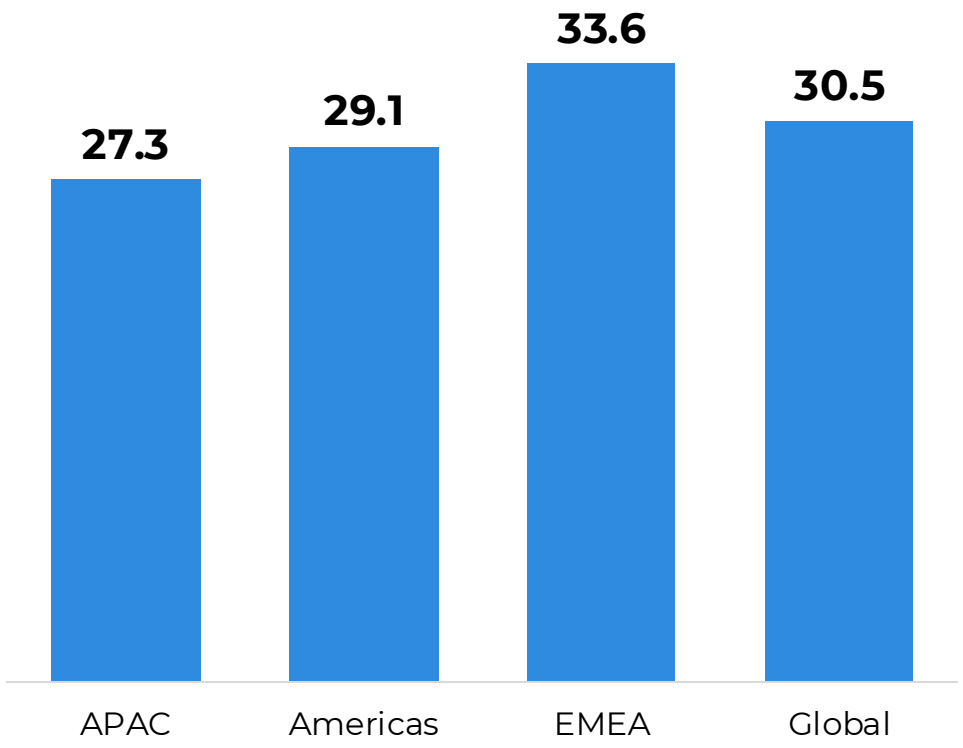
Let Me Decide

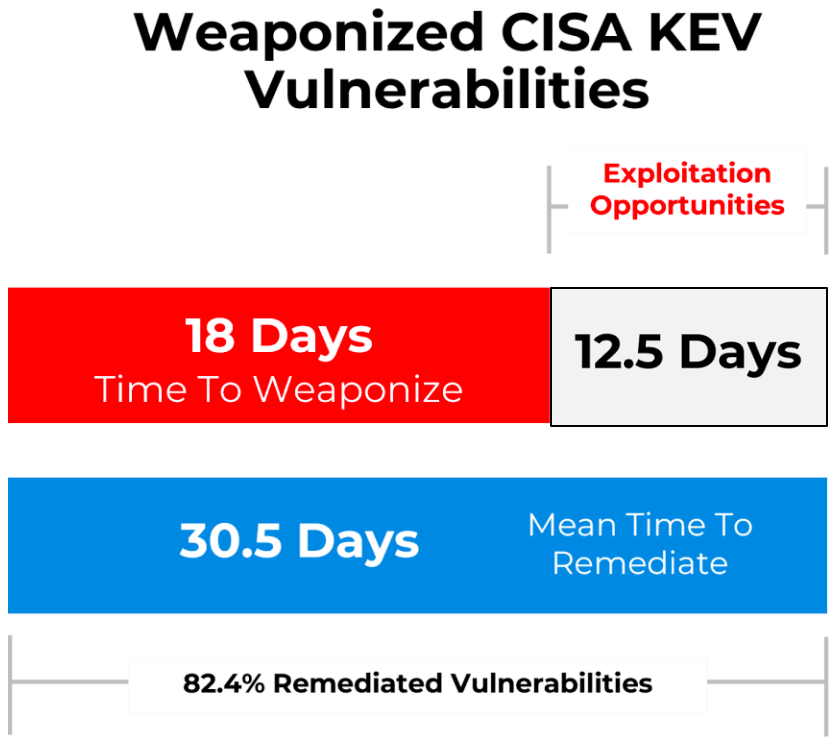
Build a custom template based on your business requirements.

Cancel | Previous | Prioritize Now


Unified Asset Inventory
Risk Factors Aggregation
Threat Intelligence
Business Context
Risk Prioritization
Risk Response Orchestration
Compliance & Executive Reporting

Problem in Risk Reduction is 2-Fold





Impact of Qualys Patch Management

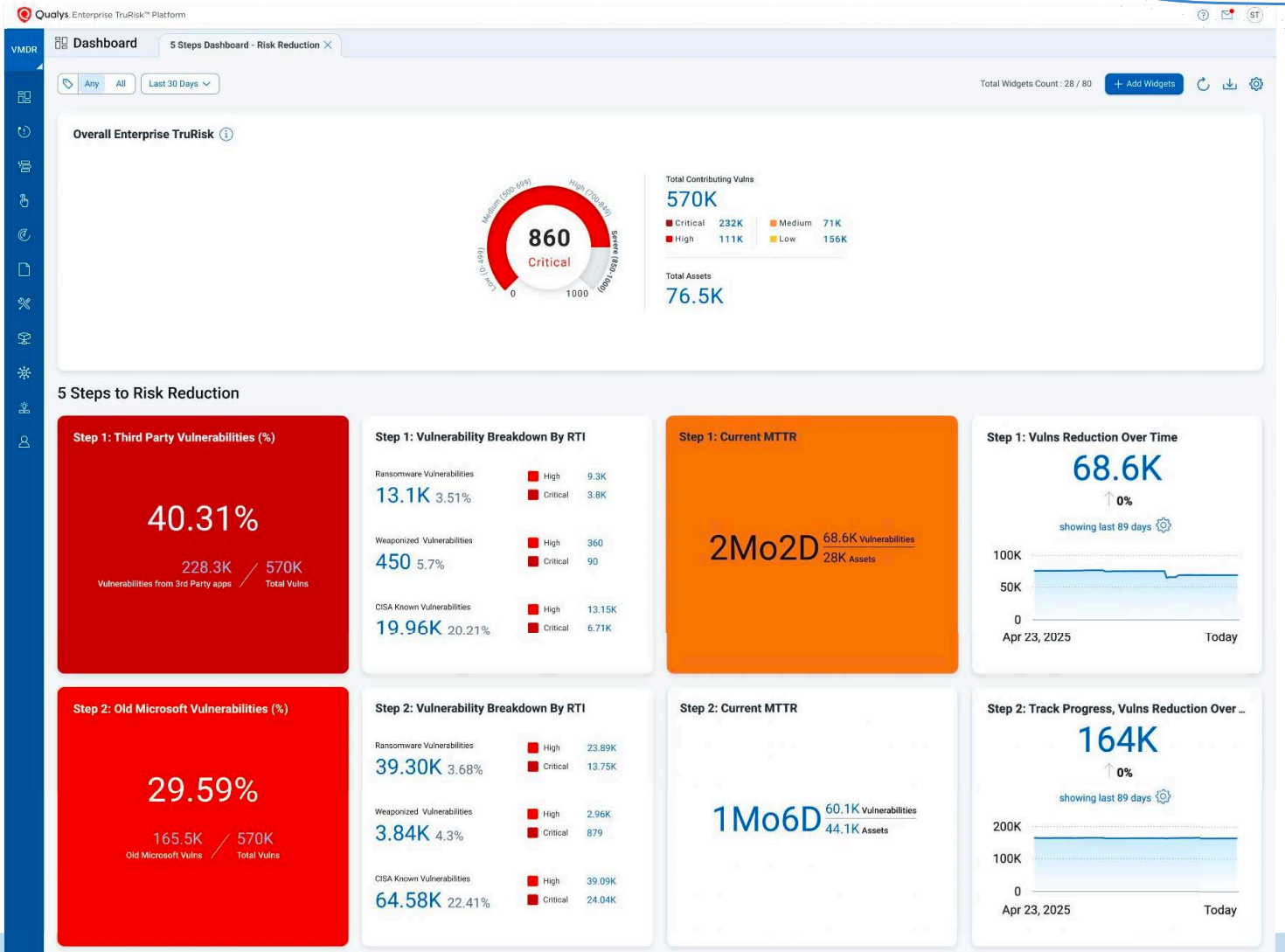
Qualys. ROCon 25
The Risk Operations Conference
AMERICAS

01 Maps right Remediations to Risky Vulns & Assets to reduce mean time to communicate

02 Patches Win, Mac, Linux and 200+ 3rd party apps, no need of VPN

03 **Now** provides a Risk elimination plan to reduce risk

04 Drives patching thr' MS SCCM/Intune RBAC, ITSM Integrated



Impact of Qualys TruRisk Eliminate

Qualys. ROCon 25
The Risk Operations Conference
AMERICAS

140M

Patches + Mitigations Deployed in last 12 months

Smart Chaining
No VPN
Rollback
RBAC
Patch via SCCM
Intune
ServiceNow

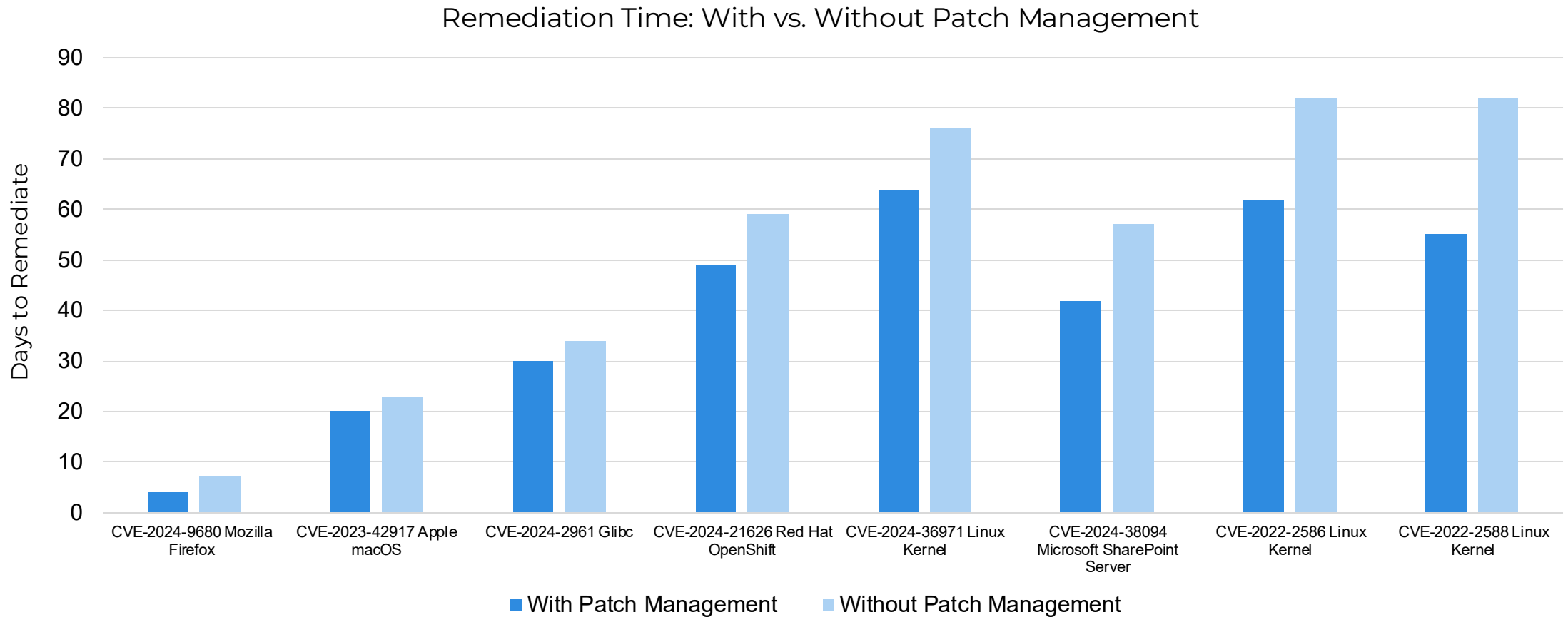
40%
Faster MTTR than traditional patch

5% Windows
Customers in 0-5 days MTTR

9%
Customers in 6-10 days

32%
Customers in 11 to 17 days

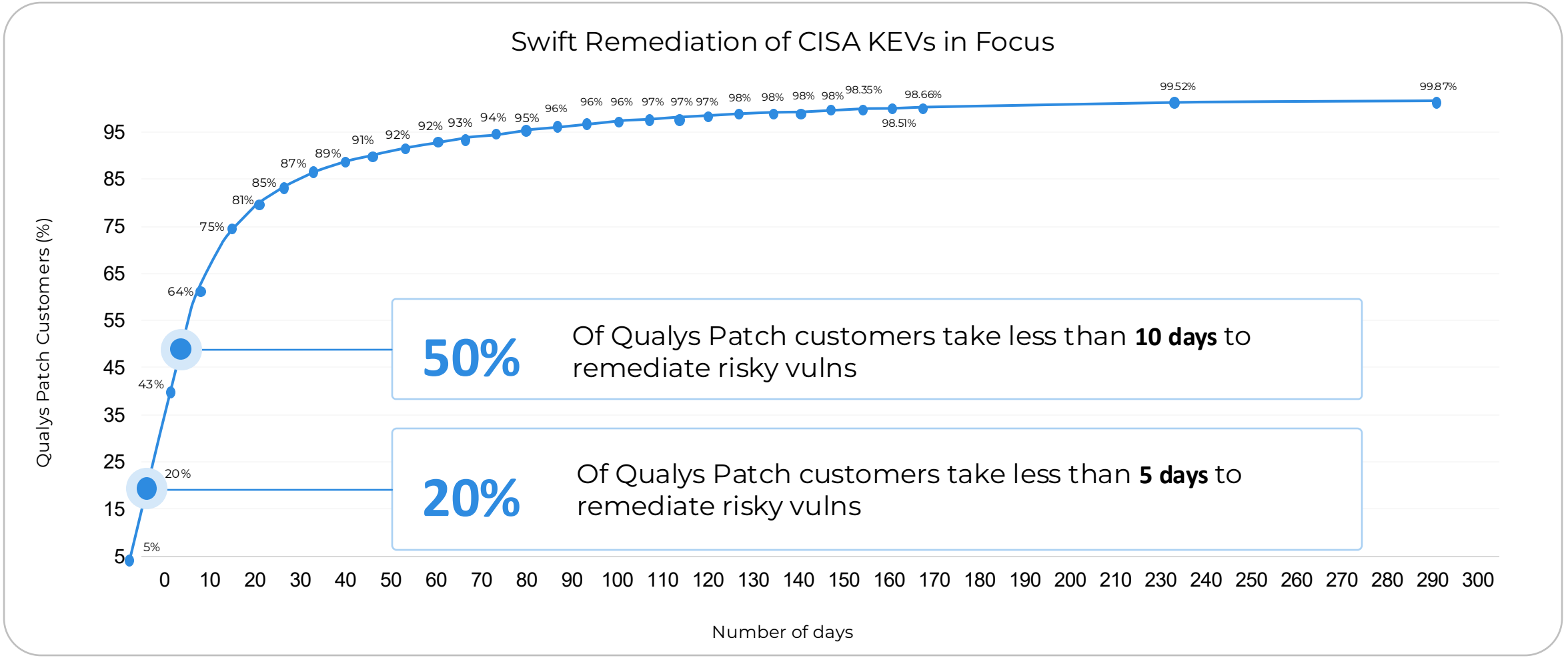
Patching Risky Vulns Faster than any other patch tool



Formal patch management accelerates high-risk vulnerability remediation, cutting exposure windows.

With TruRisk Eliminate, You are Remediating Risky Vulnerabilities, before they are in CISA KEV

Qualys. ROCon 25 The Risk Operations Conference AMERICAS



Make your ITOps the Heroes

Let them know that they would prevent **8 out of 10 Attacks** Before Attackers could Exploit them...

Qualys. ROCon 25
The Risk Operations Conference
AMERICAS

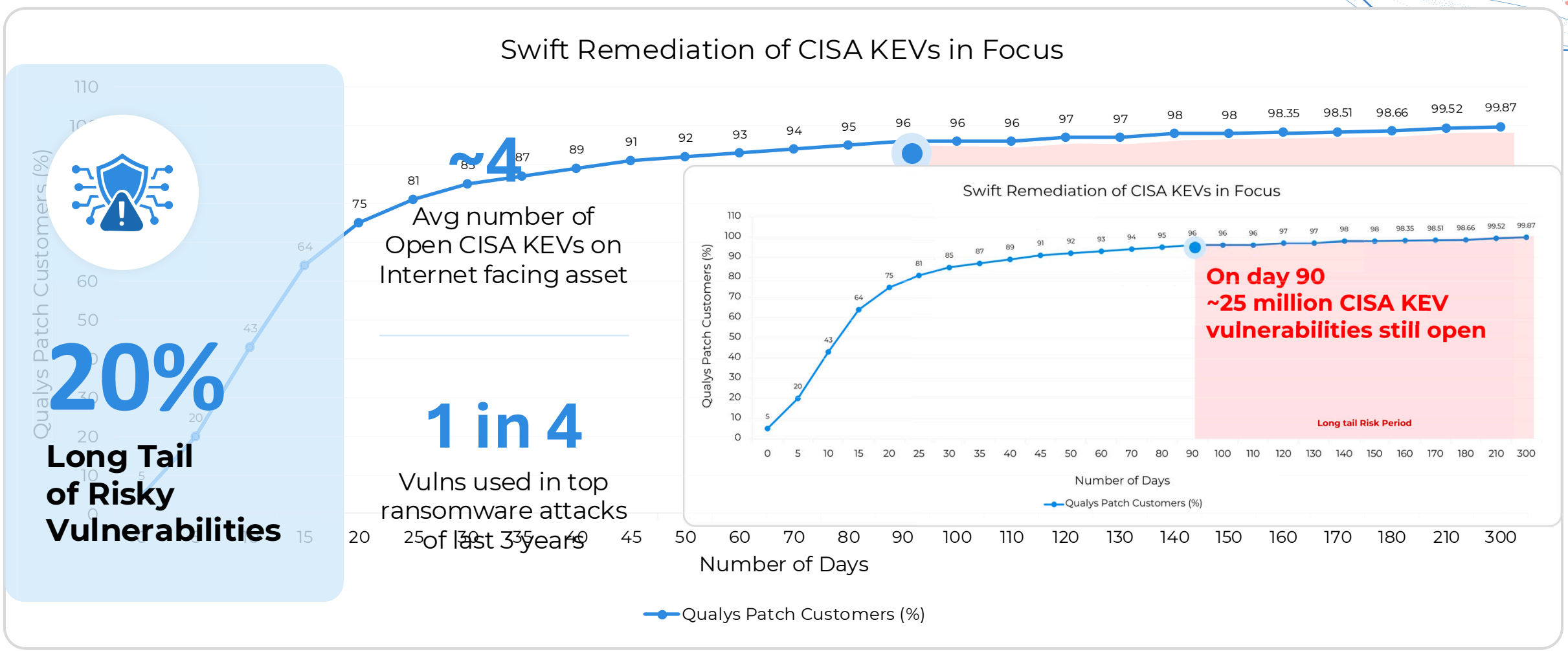
Cloud
Ransomware

Candiru	Luckycat	Operation Dragon Castling	Ajax Security Team	Sandworm Team
Wizard Spider	APT28	APT38	Dragonfly	Fin7
FoxKitten	Lazarus Group	menuPass	Threat Group 3390	Tonto Team

Top attacks of 2023 and 2024

Long Tail of Vulnerabilities are what Attackers are After...

Qualys. ROCon 25
The Risk Operations Conference
AMERICAS



In 2024, while most CISA KEV vulnerabilities are rapidly patched, the last 1-2% can remain open well past six months, exposing organizations to unnecessary risk

The patch can break my critical assets

Remediate Smart, Break Less with AI-powered Patch Reliability Score

Qualys. ROCon 25
The Risk Operations Conference
AMERICAS

Automate the safe majority

- Classify each patch (High, Medium or Low)
- Risky vulns with **high-reliability** recommended for automated patching.
- Cutting **MTTR by 50–75%**

Fewer outages, smarter testing

- Focus human effort on **Medium** with smart patch ring jobs.
- Result: **change-failure rate ≤5–10%** and fewer SEV incidents tied to patching.

Risk-aware when patching is risky

- When reliability is **low**, recommends mitigate / isolate until safe to patch.
- Keeping MTTR for risky vulns in single digits while protecting crown-jewel assets.

Accelerate MTTR with Patch Reliability Score

Qualys. ROCon 25
The Risk Operations Conference
AMERICAS

Avg Risky Vulnerabilities per customer		Higher MTTR	Threat Actors
01 Existing on **Non-Critical** Assets	10.2K	1M 10D	ExCobalt
02 Existing on **Critical** Assets	30K	1M 25D	Silent Chollima
03 Not Patched due to **Business Impact**	16.3K	6M 7D	Cobalt Spider
04 Exist on Critical Assets with **No Patch Available**	6K	7M 9D	Russia Attribution
			Stone Panda

Enterprise TruRisk

This report presents your TruRisk posture from open vulnerabilities that can be patched or mitigated with Qualys TruRisk Eliminate.

Total Assets
15.1K

2.4K
Internet Facing Assets

Total Vulnerabilities
450K

* Only vulnerabilities with detection source 'Cloud Agent' are considered

MTTR Analysis

2x Slower

Than Peers

Your current MTTR 20 D

Industry Average MTTR 10 D

Risk Elimination Options to Accelerate MTTR

82% (369K/450K)

Patchable Vulnerabilities

42%(369K/450K)
Have Mitigations Available

18% (81K/450K)

Vulnerabilities with No Patch Available

Have Permanent Fixes Provided by **TruRisk Eliminate**

TruRisk Eliminate ensures the reduction of Cyber Risk and MTTR through focused Risk Elimination Strategies

Know Your Risk Source

Identify the areas contributing most to your cyber risk and prioritize remediation

01

Vulnerabilities from **3rd Party Apps**

40%
(180K/450K)

02

Microsoft Vulnerabilities Published Over **30 Days Ago**

42%
(189K/450K)

03

Vulnerabilities with **No Patch Available**

18%
(81K/450K)

Vulnerabilities with **No Patch Available**

Primary reason for increased MTTR and delayed patch SLAs

18% (81K/ 450K)

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

9.2% (41.2K)

Risky Vulnerabilities

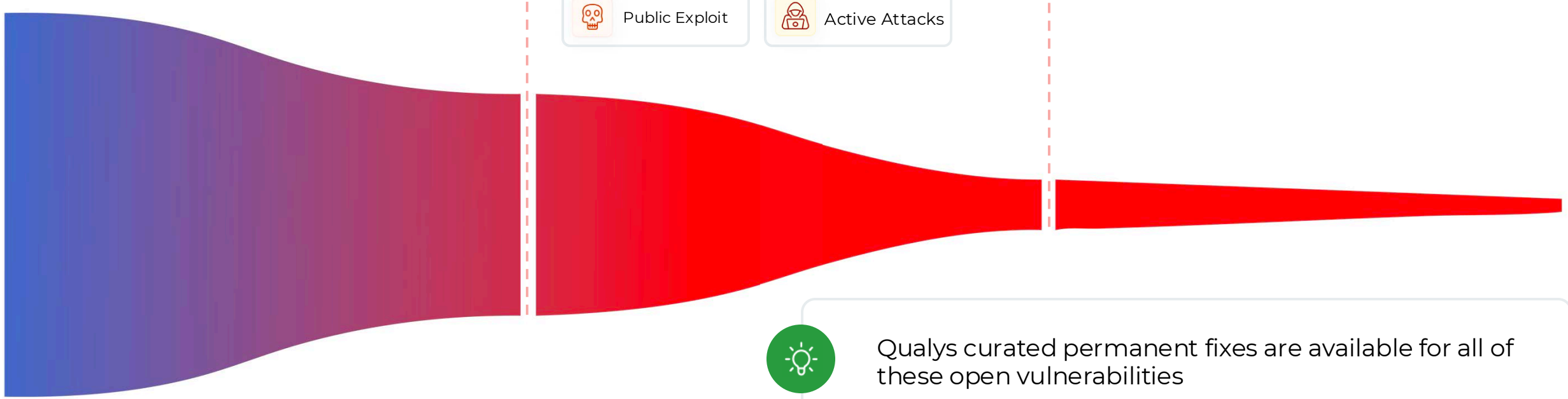
Prioritized by Real-Time Threat Indicators

- CISA KEV
- Ransomware
- Public Exploit
- Active Attacks

6% (27.3K)

Risky Vulnerabilities on Critical Assets

Fix these first for maximum Risk Reduction



Qualys curated permanent fixes are available for all of these open vulnerabilities

Vulnerabilities with No Patch Available: **MTTR Overview**

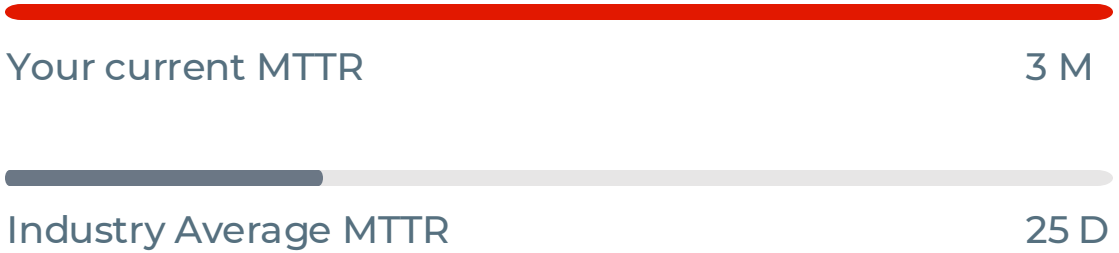
Primary reason for increased MTTR and delayed patch SLAs

Peer Benchmarking

Your MTTR Performance

3 Months

Current MTTR: Below Average (28% slower)



Critical Patch Compliance SLAs

- 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: **Industry Trends in Applying Permanent Fixes**

Top CVEs being fixed by peer organizations using Qualys permanent fixes

CVE-2013-3900

Critical

Microsoft WinVerifyTrust function Remote Code Execution

11K

Affected Assets In Your Environment

CVE-2014-8439

Critical

Adobe Flash Player Dereferenced Pointer Vulnerability

17

Affected Assets In Your Environment

CVE-2016-2183

Medium

Birthday attacks against Transport Layer Security (TLS) ciphers with 64bit block size

22.8K

Affected Assets In Your Environment

CVE-2024-39818

Low

Zoom Workplace Apps and SDKs - Protection Mechanism Failure

472

Affected Assets In Your Environment

CVE-2025-0167

Low

Microsoft Curl Exposure of Sensitive Information Vulnerability

19.5K

Affected Assets In Your Environment

RISK BUSTERS

CAPTURE THE FLAG EVENT

ENTER TO WIN PRIZES

1st Place: **16" MacBook Pro**
2nd Place: **13" iPad Air**
3rd Place: **Apple Watch Series 11**

Wednesday
October 15, 2025
5:15 – 6:30PM

*Do you have what it takes to earn the title of **Agent TruRisk?***

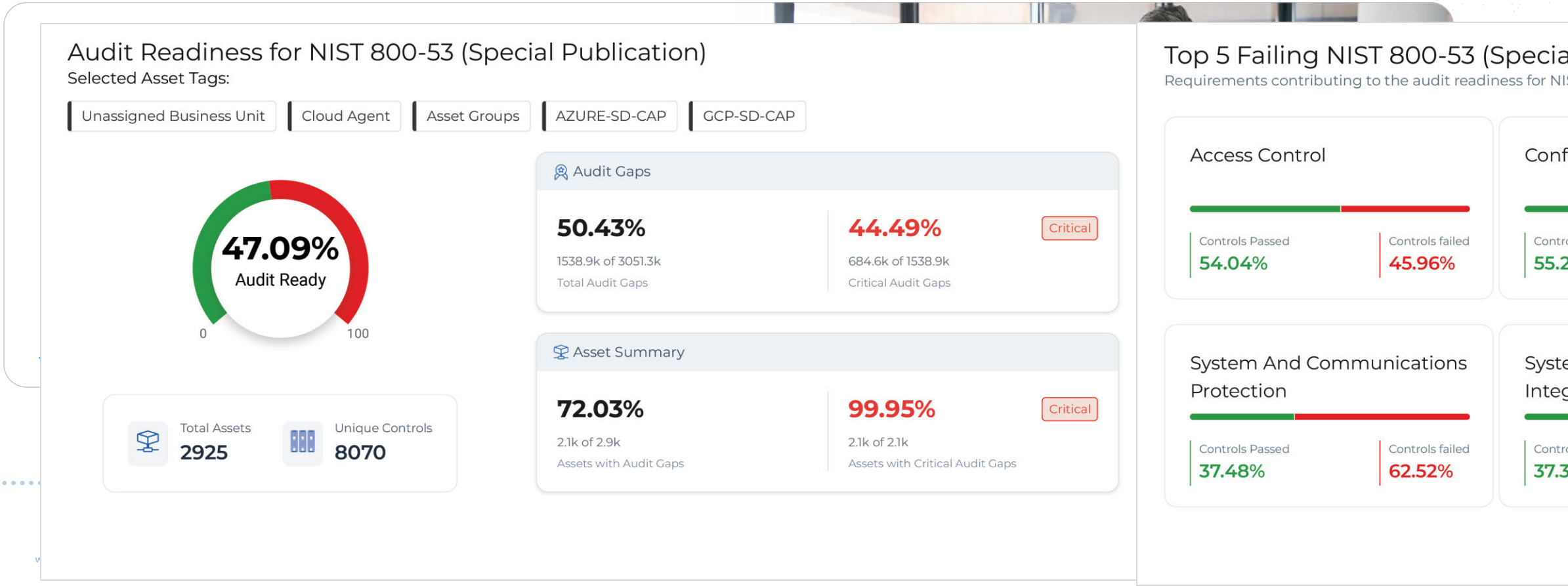
Qualys. ROCon 25


Unified Asset Inventory
Risk Factors Aggregation
Threat Intelligence
Business Context
Risk Prioritization
Risk Response Orchestration
Compliance & Executive Reporting

Compliance Assessment and Reporting

Audit-Ready, Continuously Compliant to 100+ mandates from assessment to fixing

Qualys. ROCon 25
The Risk Operations Conference
AMERICAS



Risk enrichment on top of your exposure data

Qualys. ROCon 25 The Risk Operations Conference AMERICAS

Unified Asset Inventory	Risk Factors Aggregation	Threat Intelligence	Business Context	Risk Prioritization	Risk Response Orchestration	Compliance & Executive Reporting
Business-first visualization of assets and their risk **Tech-debt (EOL/EOS)** based on risk of the exposures	**Aggregation & Risk-based prioritization** – know which exposures matter the most to reduce risk	**TruLens** Threat actor mapping to exposures to for Adversary-based risk prioritization and remediation	**Cyber Risk Rationalizer** To see how much effective the controls are getting to reduce impact and likelihood of loss to business	**TruConfirm** To get exposures validated/confirmed for exploitation	**Eliminate/Remediate** **Get exact remediations (patch/mitigations)** mapped to exposures to reduce risk	**Audit-ready report** Mapped to 100+ mandates to get compliance friendly report

If I have VMDR, What does ETM give me

Unified Asset Management

Comprehensive visibility across **external and internal attack surfaces** with risk context. Automatically link your technical assets to their business entities with criticality and associated risks.

TruRisk: Quantifying Cyber Risk for Business

Aggregating all siloed exposures at scale, across your security tooling to measure and visualize risk in **business value.** See how your exposures get re-prioritized. **Track SLAs. Customize Risk** based on **environmental and mitigation factors**

Adversary-Based Risk Prioritization

Stay ahead of emerging and **trending threats in your industry** with visibility into your risk prioritization and reduction plans for the threats

Specialized Cyber Risk Views – ETM Identity

Get unified view of risk from emerging attack surfaces – Identity security posture management, Post-Quantum readiness etc., instead of looking into it in a siloed manner

Native Agentic AI: Ready to use Cyber Risk Agents and Cyber Risk AI Assistant

TruConfirm: Validate exposures, Confirm Exploitation

confirm exploitation of exposures while validating security mitigations, to accelerate remediation of exposures, validated for exploitation

Speaking the language of the executives...

Qualys. ROCon 25 The Risk Operations Conference AMERICAS

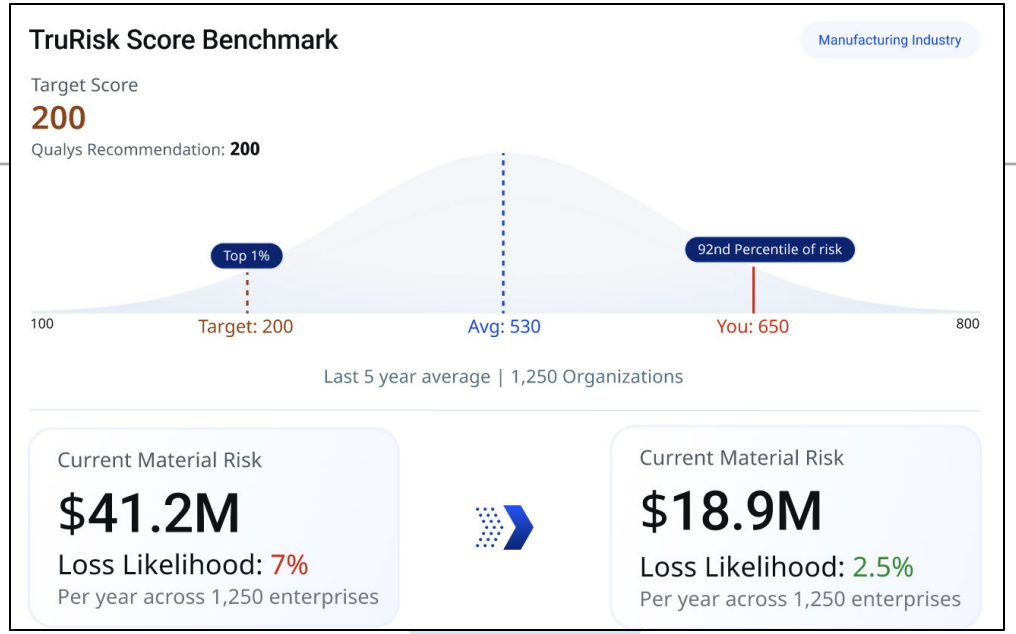
Financial Impact

Executives wanting to know financial impact for budget decisions

Cyber risk and security teams managing exposures and risk

TruRisk

Industry risk



TruRisk Cohort

Qualys.
ROCon 25
The Risk Operations Conference
AMERICAS

Thank You