Qualys Platform: A 25 Year Journey of Relentless Innovation

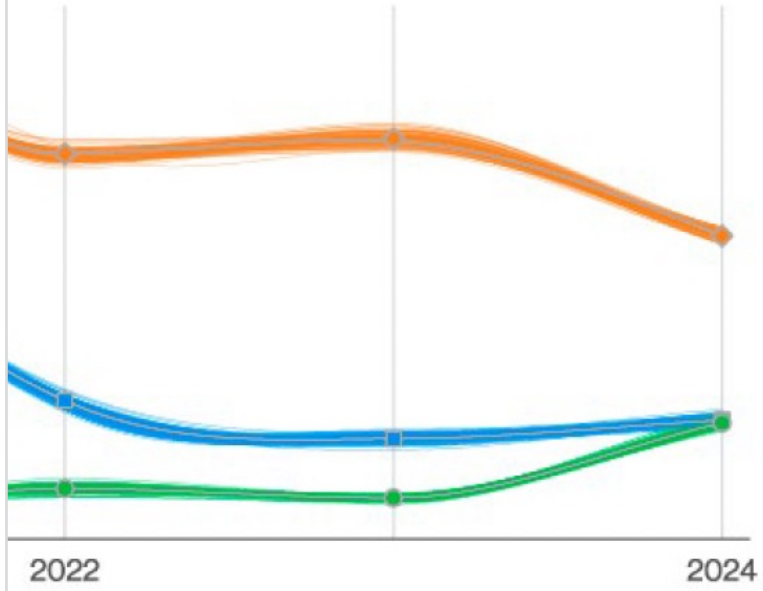
Shailesh Athalye

Qualys Product Management

Operationalize

The Risk Operations Center (ROC)

ts are the most
the largest Risk factors
ons Center



st growing vector of attacks
2 years - **Vulnerabilities**

Fastest, Most Comprehensive and Accurate in Vulnerability Detection

103K

CVE-based detections

16K

Detections for Open-source

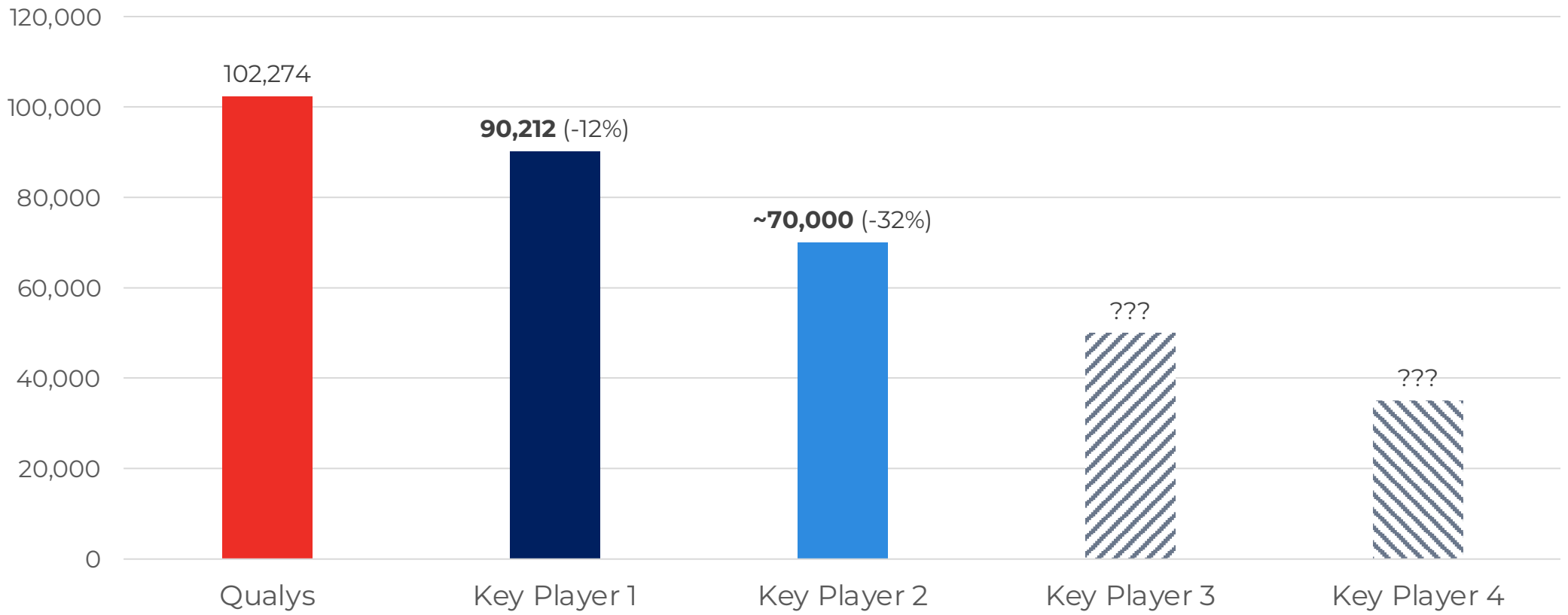
13K

Signatures w/active probing

16 hrs

Response Time - Zero days

Industry Leading Coverage for CVEs



Bringing Multi-Sensor Approach for Detections

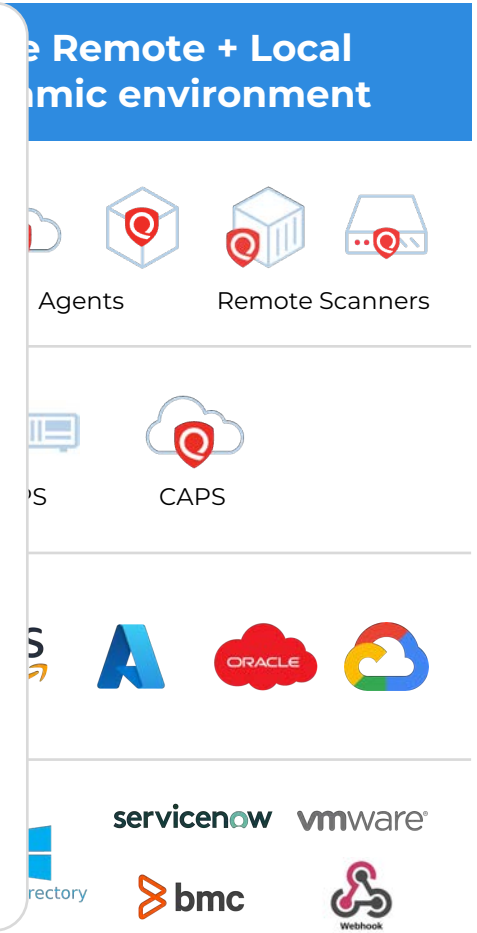
22%

of CVEs applicable for exploited network and perimeter devices

70%

of Risky vulns exploitable remotely

78% detected locally



1172/1187

99%

Coverage for CISA KEVs

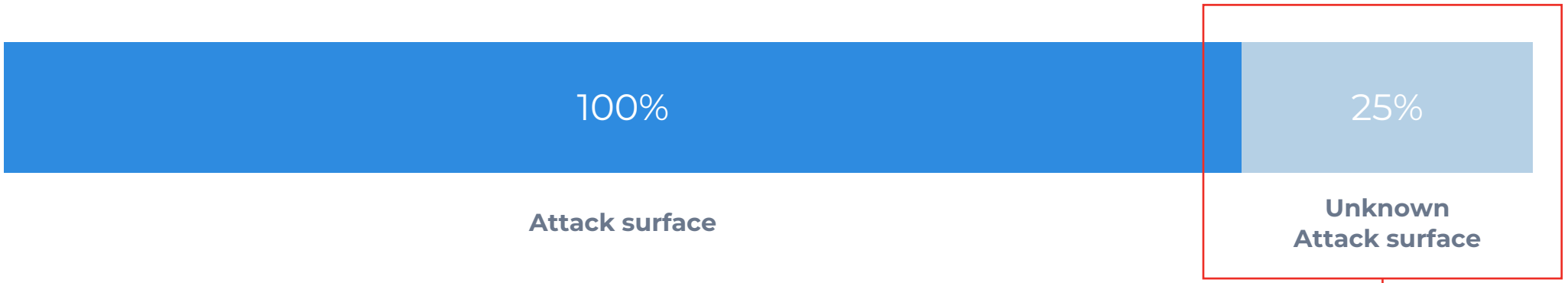
Is Cyber Risk Problem Really a Cyber Risk Problem?

Geoff Belknap (He/Him) • 1st
Microsoft | Former LinkedIn, Slack, Palantir
View my blog
1w •

Today's thought: The hardest problems in Security aren't really "Security" problems.
- Asset Inventory
- Patching Automation
- Config Management
- Device Administration

#security #Cybersecurity #ITSecurity #AssetManagement #Automation #TechManagement #infosec

Known Inventory & Attack Surface != Risk Surface



80%

% of HIGH Confidence EASM Assets to Total EASM Assets

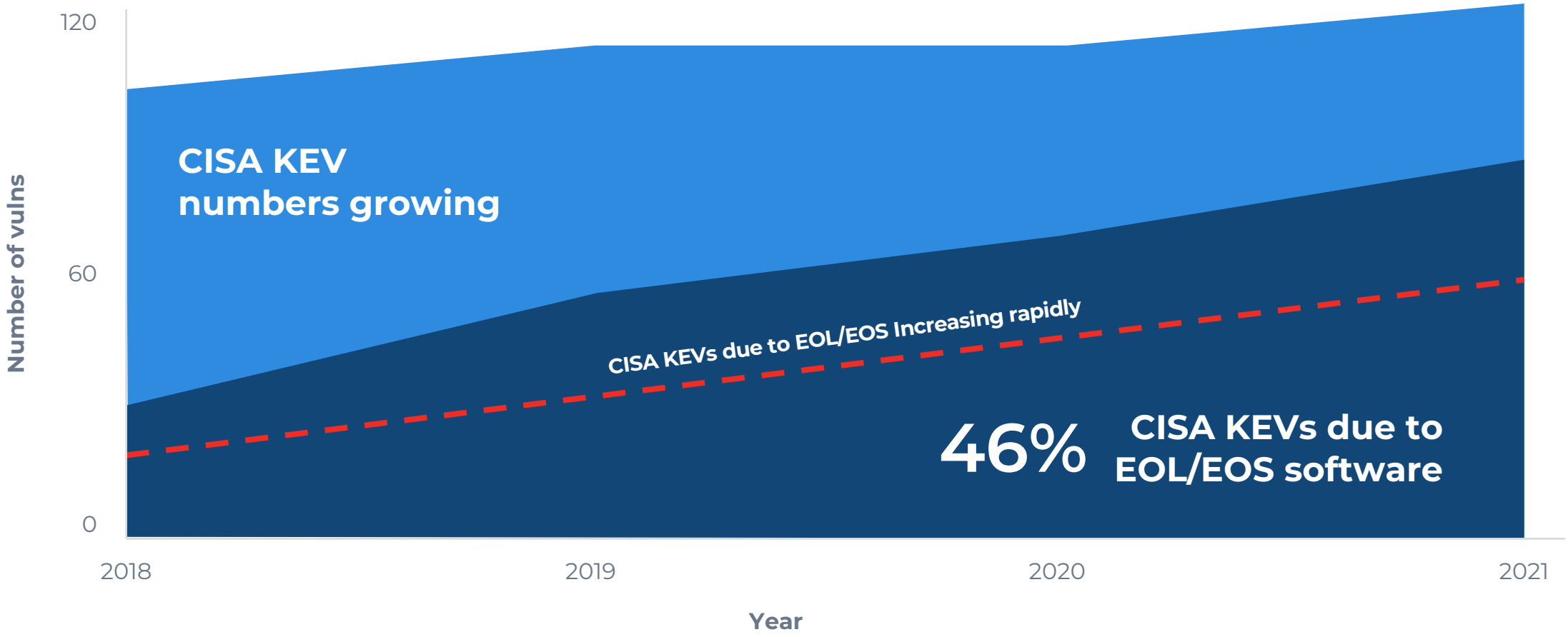
2.2M (15.7%)

# of Assets w/ Risky Open Ports (RDP, SSH, SFTP...)

1.6M (11.4%)

# of Assets w/ DB Open Ports (mssql, mysql...)

EOL/EOS Increasing the Risk of Vulnerabilities...



Increased Risk Due to Unnecessary Software

5M/26M
Servers across Environments

20%
Servers w/highly vulnerable desktop software

22
Vulnerable Desktop Software

4.7K
Unique High/Critical Vulnerabilities (CVE)

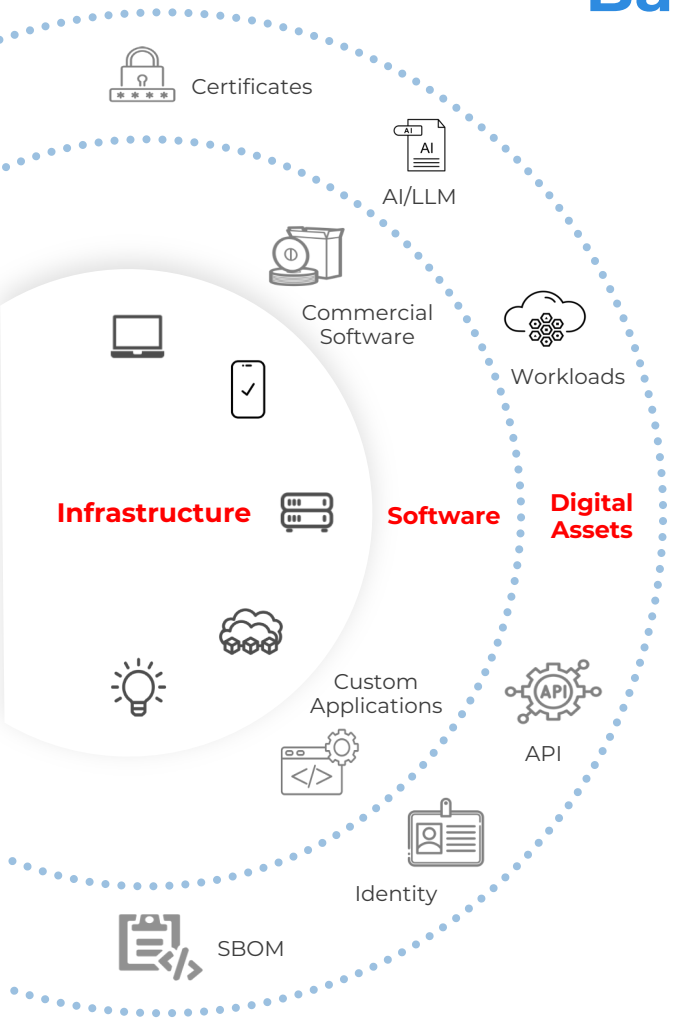
~14
Critical Vulnerabilities per Asset that can be avoided!

CyberSecurity Asset Management

Product	Install Count	Risky Vulns	Total Vulns	Total EOS	% of Unpatchable Vulns (EOS)
Internet Explorer	1,894,087	1,636	3,098,726,332	81,514	4%
Chrome	1,368,291	3,518	4,813,647,738	679,551	50%
Firefox	606,945	2,667	1,618,722,315	354,512	58%
Acrobat Reader DC	487,712	1,715	836,426,080	256,386	53%
Office	439,730	829	364,536,170	130,198	30%
Acrobat Reader	196,300	1,037	203,563,100	80,702	41%
Flash Player	68,573	1,084	74,333,132	67,586	99%
WinRAR	61,592	23	1,416,616	12,713	21%
Zoom	57,181	69	3,945,489	24,523	43%
VLC media player	49,374	114	5,628,636	55	0%
Thunderbird	17,799	1,139	20,273,061	5,613	32%
Foxit Reader	14,195	376	5,337,320	1,619	11%
Foxit PDF Reader	6,299	231	1,455,069	-	0%
QuickTime	3,523	246	866,658	2,884	82%
Safari	504	1,455	733,320	503	100%
iTunes	256	920	235,520	141	55%
Photoshop	138	80	11,040	132	96%
Illustrator	48	120	5,760	46	96%
RealPlayer	26	170	4,420	4	15%
Fusion	1	129	129	-	0%
Grand Total	5,272,574	17,558	11,049,867,905	1,698,682	32%

CyberSecurity Asset Management

Base for your Risk Operations Center (ROC)



Cloud Connectors

aws · Azure · ORACLE · Google Cloud

Key IT Infra Connectors

Active Directory · servicenow · vmware · bmc · Webhook

Active Sensors

Agents · Remote Scanners

Passive Sensors

NPS · CAPS

Cyber Inventory with business and risk context

Internal and External Attack Surface

Integrated w/Risk Management Program

Enhancements to TruRisk™ 2.0

- Vulnerabilities (CVSS / EPSS)
- Malware
- Exploit Type
  Real Threat Indicator
- Certificates
- Unauthorized Software
- CISA KEV
- Exploited by malware threat actors
- Asset Critically
- Unauthorized Ports
- EoL & EoS SW, OS, HW
- Trending – Chatter, Dark Web
- Exploit Code maturity
- Location of the Asset
- Required SW Missing
- Custom Rule-based Risk factor

TruRisk™ Score

Total Assets
110K

Total Findings
1.5M

Top Risk Factors

CISA/NCSC Vulnerabilities
143.2K

Internet Exposed Assets
20.4K

Misconfigurations
92.4K

Incidents
19

TruRisk... By Correlating Security Data

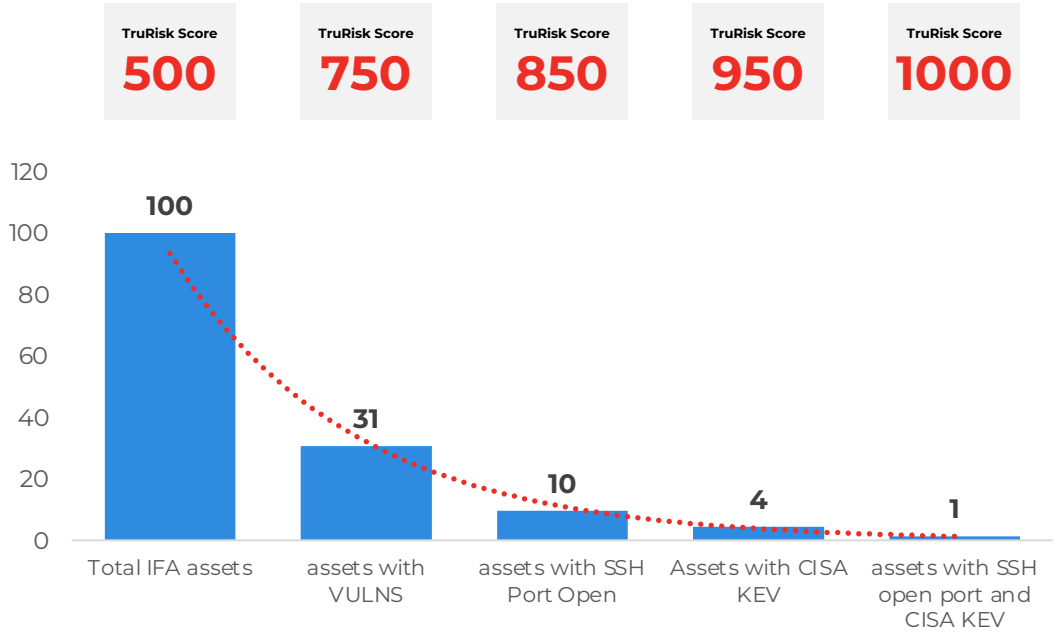
Contributing Factors

- External facing
- Ransomware vulnerabilities
- RDP misconfiguration
- Business-critical asset
- Not running Anti-virus software

Prioritizing the Cyber Risk Needing Attention!

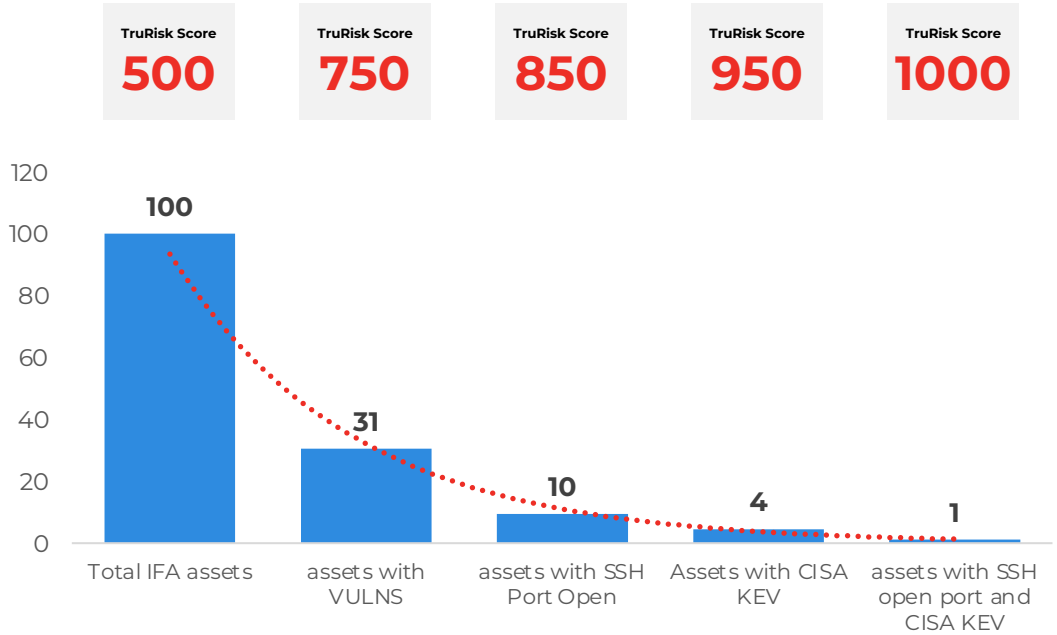
SSH Toxic Combination

100%	31%	10%	4%	1%
Total IFA assets	assets with VULNS	assets with SSH Port Open	Assets with CISA KEV	assets with SSH open port and CISA KEV



RDP Toxic Combination

100%	31%	7%	4%	2%
Total IFA assets	assets with VULNS	Assets with RDP Port Open	Assets with CISA KEV	assets with RDP open port and CISA KEV



How Many Tools = CNAPP?

VMs | CWPP | Containers | CSPM | CMPs | Serverless | IaC | CIEM | CNAPP

100s of CIEMs...

Which ones critical, internet facing?

100 of 1000s of vulns...

- Agent vs Scanner vs APIs (False positives, negatives)
- Which ones mapped to threats, business critical apps

100s of misconfigurations

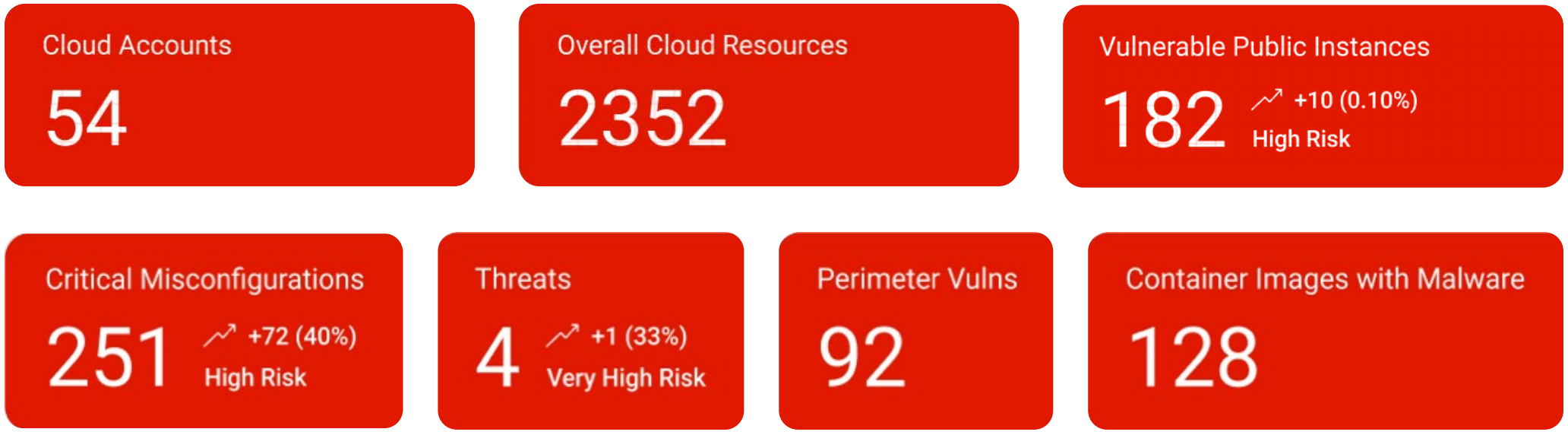
- Which ones impacted by underlying workload risks
- Which ones are risky?

100s of Attack Paths

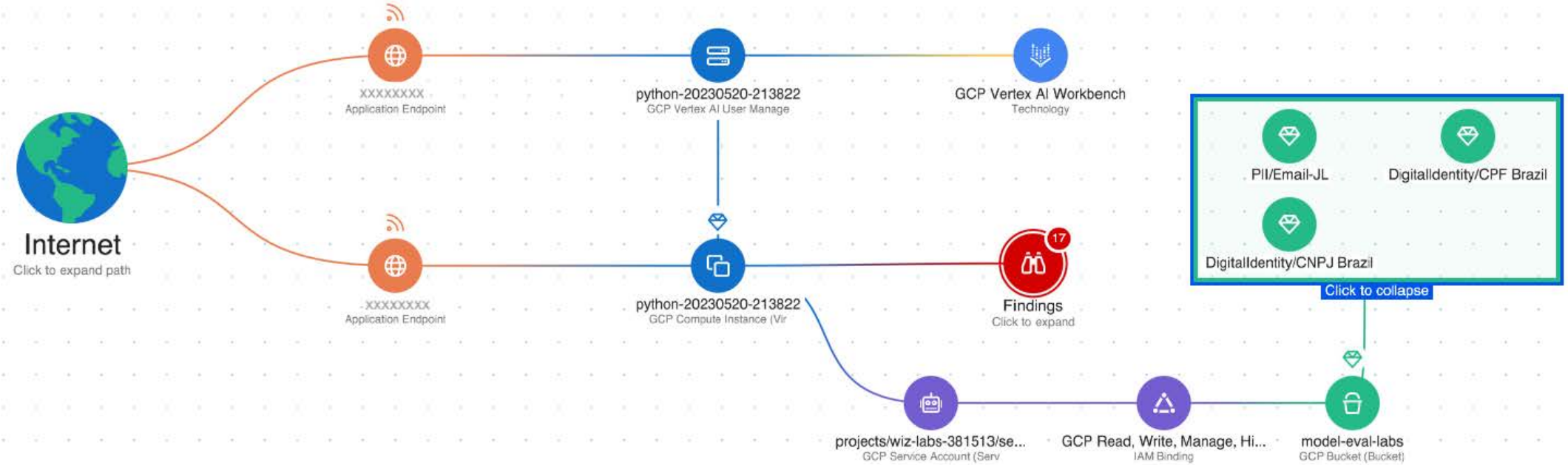
- Based on inaccurate detections?
- Are those Relationship graphs or attack can actually reach?
- What if attacker starts from the middle or from non-cloud asset?

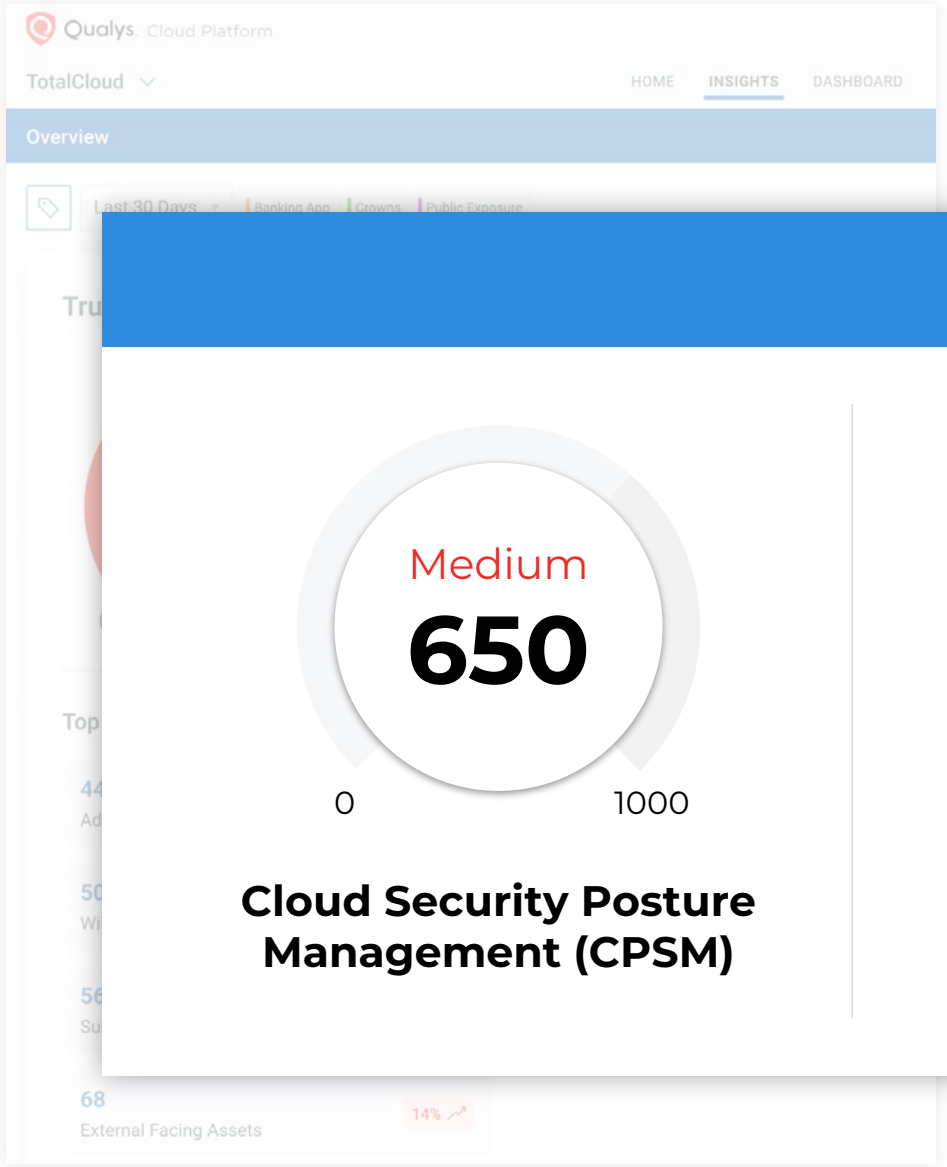
What is My Cloud Risk?

What is My Cloud Risk?



Attacks Paths Show Relationship Data...Not Risk!





Extending the Power of VMDR TruRisk for Cloud

TruRisk™ Score

Cloud Security Posture Management (CPSM)

External Facing Assets
CISA-known Exploitable Vulnerability

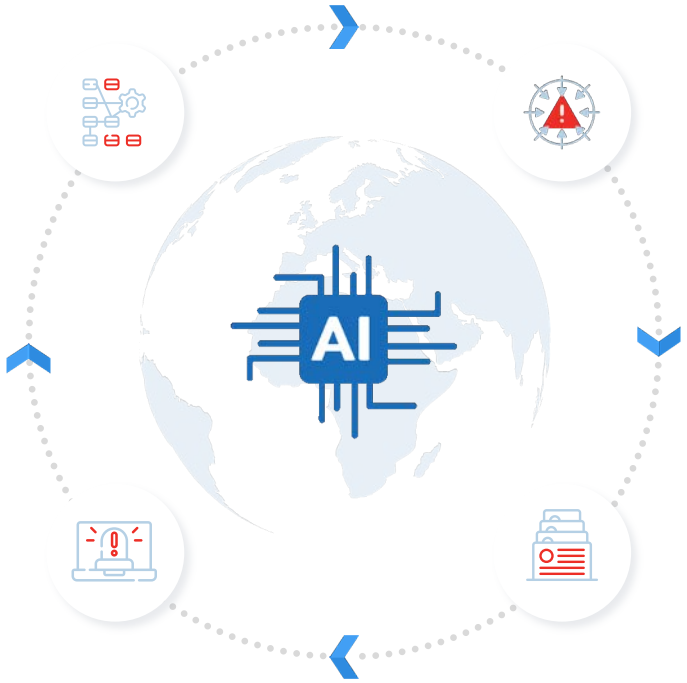
Suspicious Connection
Cloud Detection and Response (CDR)

Introducing Qualys TotalAI

Single platform for a unified view of LLM risk, AI-Workloads, and AI-vulnerabilities

Know where AI is running

- Discover all your AI-Workloads
- Get inventory of AI packages, AI-software and AI-hardware (GPUs)



Know the risk of AI Infra vulns

- 1000+ AI-specific vuln detections correlated with threats for TruRisk
- Patch vuln risks to harden Infra from model and data theft

Know the risk of Model and Data Thefts

- Scan LLM and Application endpoints
- Prompt your LLMs for OWASP TOP 10 to ensure they are not leaking data, showing bias, or can be jailbreak.

Be Audit-ready for using AI

- Prevent fines due to compliance violations (e.g., GDPR, PCI)
- LLM security report for management

Leverages existing Qualys Agent and Scanner

Transformative Evolution of Qualys Console

Transformative Evolution of Qualys Console

Measure, Communicate and Eliminate Risk Faster

Data

Insights to measure

Data

Context to communicate

Figuring out what to do next to

Intuitive for your next action to eliminate

Problem in VM is Remediation

~4

Avg number of Open CISA KEVs on Internet facing asset

1 in 4

Vulns used in top ransomware attacks of last 3 years

NCSC Guidelines on Remediation		Avg Exploitation Days
14 Days Internal	**5 Days** External	**5 Days** External

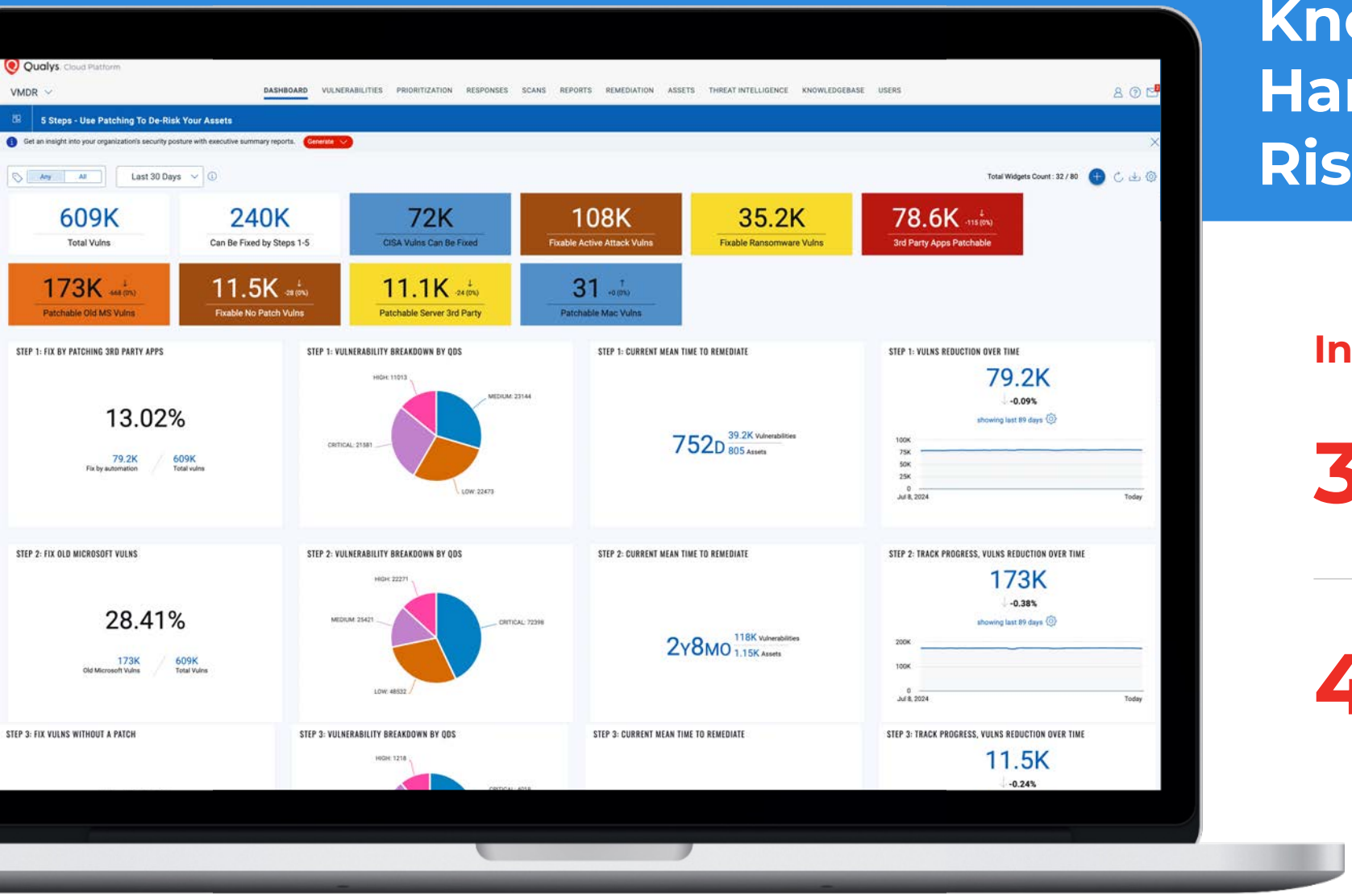
Avg MTTR for External assets

64 Days Healthcare/Pharma	**93 Days** Banking/Financial	**100+ Days** Hospitality

~47 Days

Avg MTTR for External assets

Know Your Low-Hanging Risk Reduction Fruits?



Internet-Facing Assets

33% Residual Old MSFT Patch Tuesday Patches not deployed

40% Vulns due to 3rd party software not patched

Impact of Qualys Patch Management

40%
Faster MTTR than traditional patch

60%
Reduction in vulns on internet-facing assets within

78M
Patches Deployed in last 12 months

5% customers in 0-5 days MTTR

9% customers in 6-10 days

32% customers in 11 to 17 days

Prevented 8 out of Top 10
Ransomware Attacks, including:

- Conti
- Lockbit
- Cl0p
- Petya
- REvil

Impact of Qualys Patch Management

01 Maps right Patches to Risky Vulns & Assets

02 Provides Plan to reduce Risk

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

04 RBAC, ITSM Integrated

40%
Faster MTTR than traditional patch

60%
Reduction in vulns on internet-facing assets within

70M
Patches Deployed in last 12 months

5% customers in 0-5 days MTTR

9% customers in 6-10 days

32% customers in 11 to 17 days

Prevented 8 out of Top 10 Ransomware Attacks, including:

- Conti
- Lockbit
- Cl0p
- Petya
- REvil

Risk Reduction Challenge

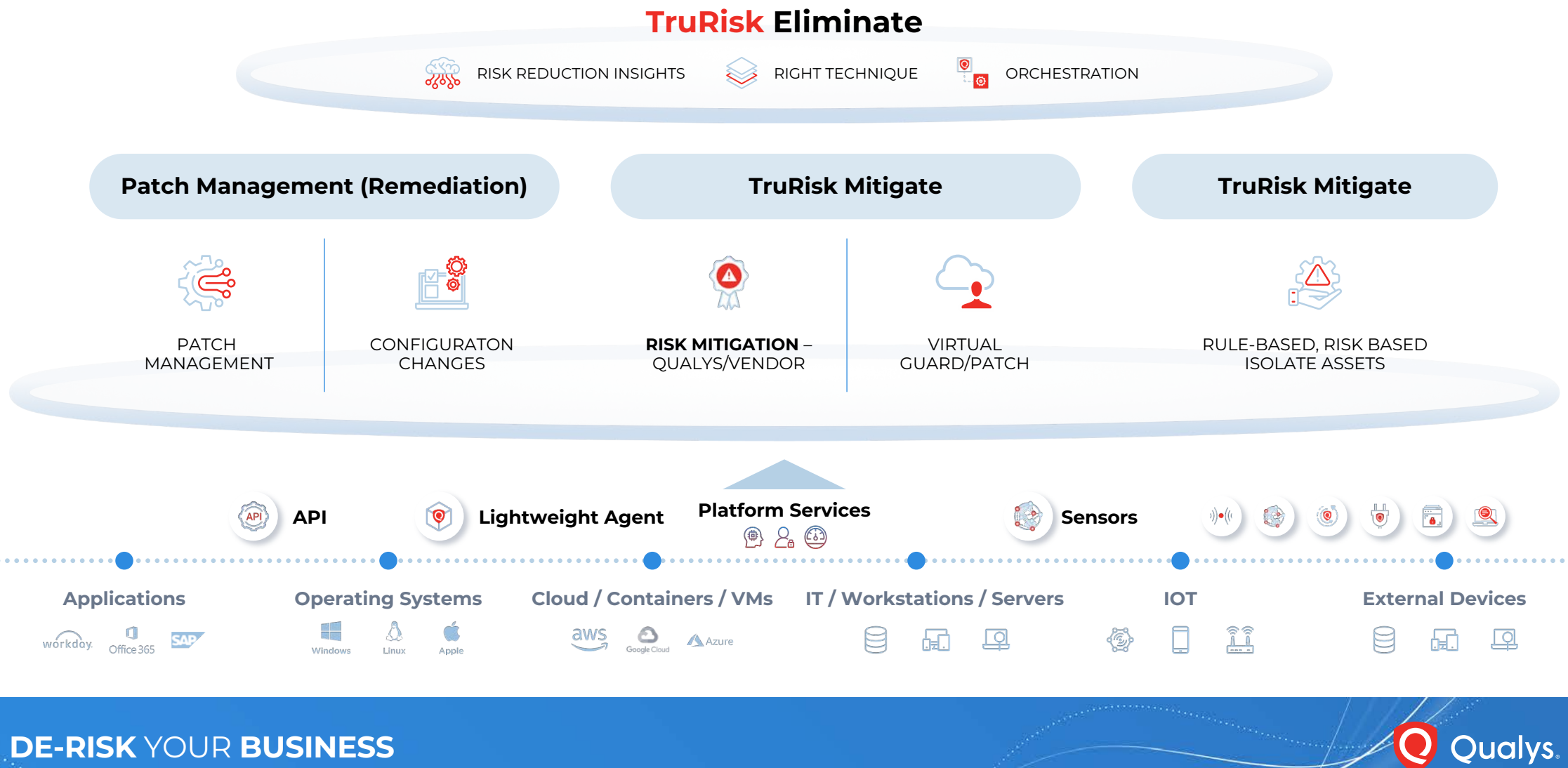
Patch OR Not Patch

Patch	Not Patch
Which Patches to reduce most risk/most vuln	Asset too critical for downtime
Which ones to Automate vs On-demand	No Patch, Zero-day, Patch needs testing

- Reduce Risk
- Reduce MTTR
- Continue Business Operations

TruRisk Eliminate

Reduce Risk... with Patch or Without

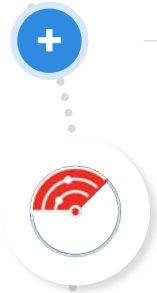


Eliminate Your Risk... Don't Just Measure It!

TruRisk
Eliminate
Address All Types Of Vulnerabilities with or without a Patch

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

Audit-Ready, Continuously Compliant

From Mandates to Requirements to Assessment to Reporting to Remediation

Regulations

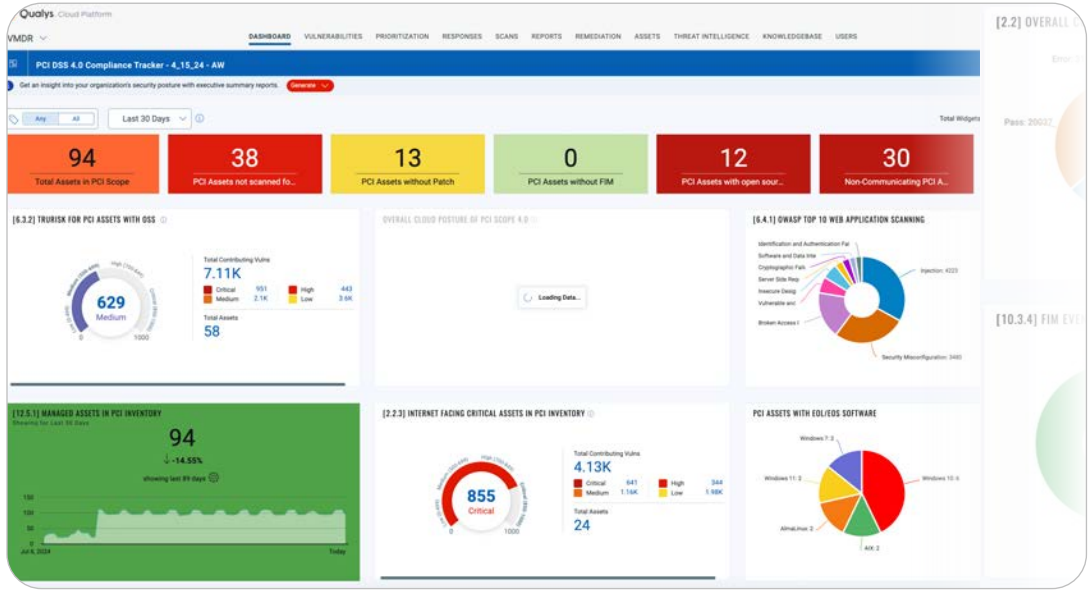
ISO · GDPR · HIPAA · NIST · FedRAMP · PCI DSS v4.0

...and many more!

01
- Authenticated Vuln scans
- Auto-discover Compliance scope for assessment
- File Integrity & access monitoring

02
- Assess, Prioritize and Remediate Misconfigurations
- Risk based assessment

03
- Cloud & container environment
- Noise-canceling FIM for compliance & risks of changes
- Bespoke s/w and risk



API · **Lightweight Agent** · **Platform Services** · **Sensors**

Applications	Operating Systems	Cloud / Containers / VMs	IT / Workstations / Servers	IOT	External Devices
workday. · Office 365 · SAP	Windows · Linux · Apple	aws · Google Cloud · Azure			

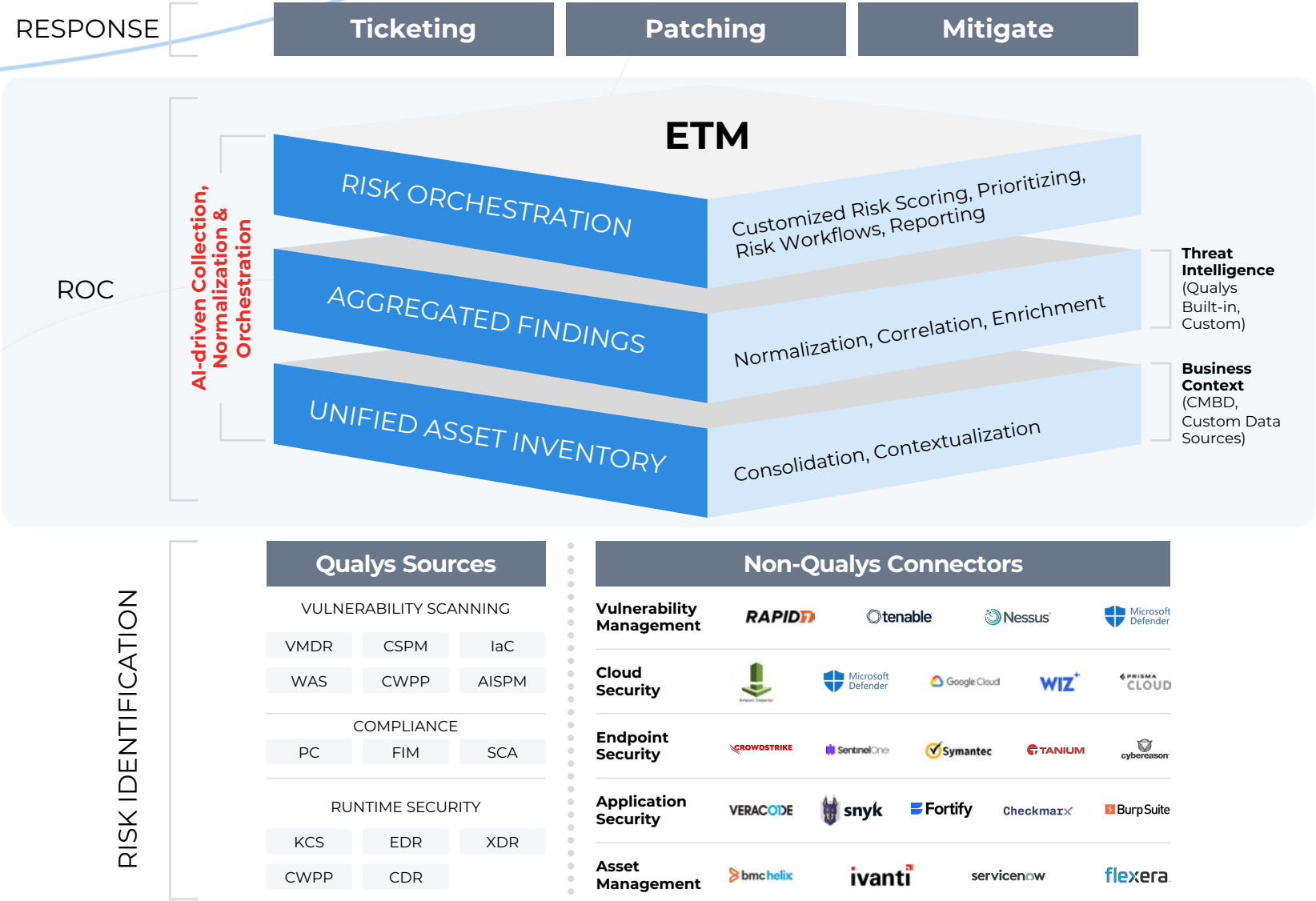
DE-RISK YOUR BUSINESS

Qualys.

ROC-Ready from Day 1

With Asset Inventory to TruRisk Prioritization to Risk Reduction...

Created through 25 years of Innovation



Endpoint Security

Proactive and Reactive Detection & Response

25%

Avg % of External **UNKNOWN** Asset to Total Asset

02

Reactive Endpoint Security

Detect, contain, respond

Attack surface reduction

Close loop intelligent risk remediation to stop repeating attacks

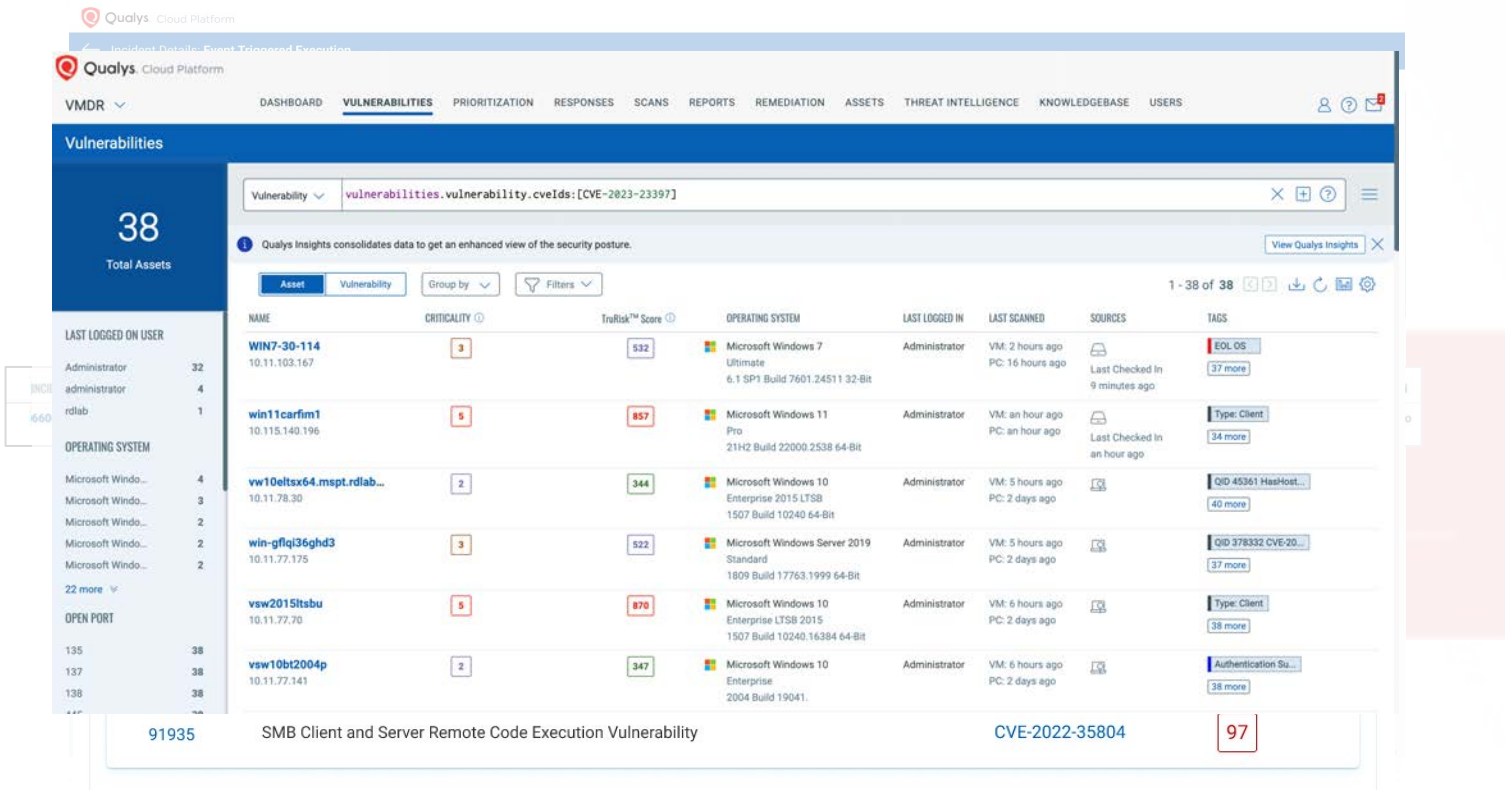
70%

Reported that attack started from unknown, external asset

Proactive Endpoint Security

Shift-left to reduce exposure, risk and business impact

Add business context to prioritize and stop attacks



QSC23

Do you Have What it Takes to Earn the Title of Agent TruRisk?

Risk Busters Contest

Live Capture The Flag (CTF)
Wednesday, October 9,
5:30 PM to **6:30** PM
Silver Pearl Ballroom

Winners Prize Ceremony
Thursday October 10, **12:35** PM
Silver Pearl Ballroom
(Must Be Present to Win)

ADD TO YOUR CALENDAR