Qualys.

ROCon 25

The Risk Operations Conference

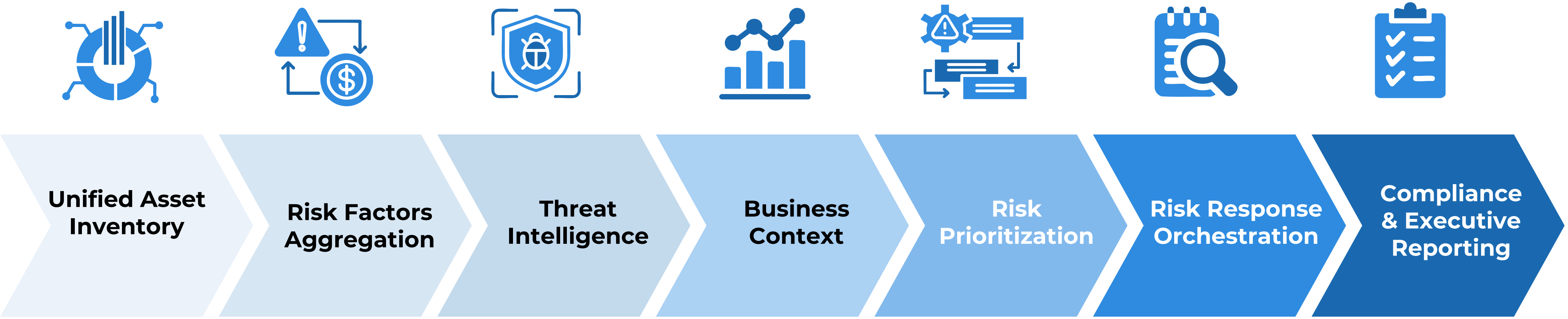
APAC

Innovations to Power your Risk Operations Center (ROC)

Shailesh Athalye

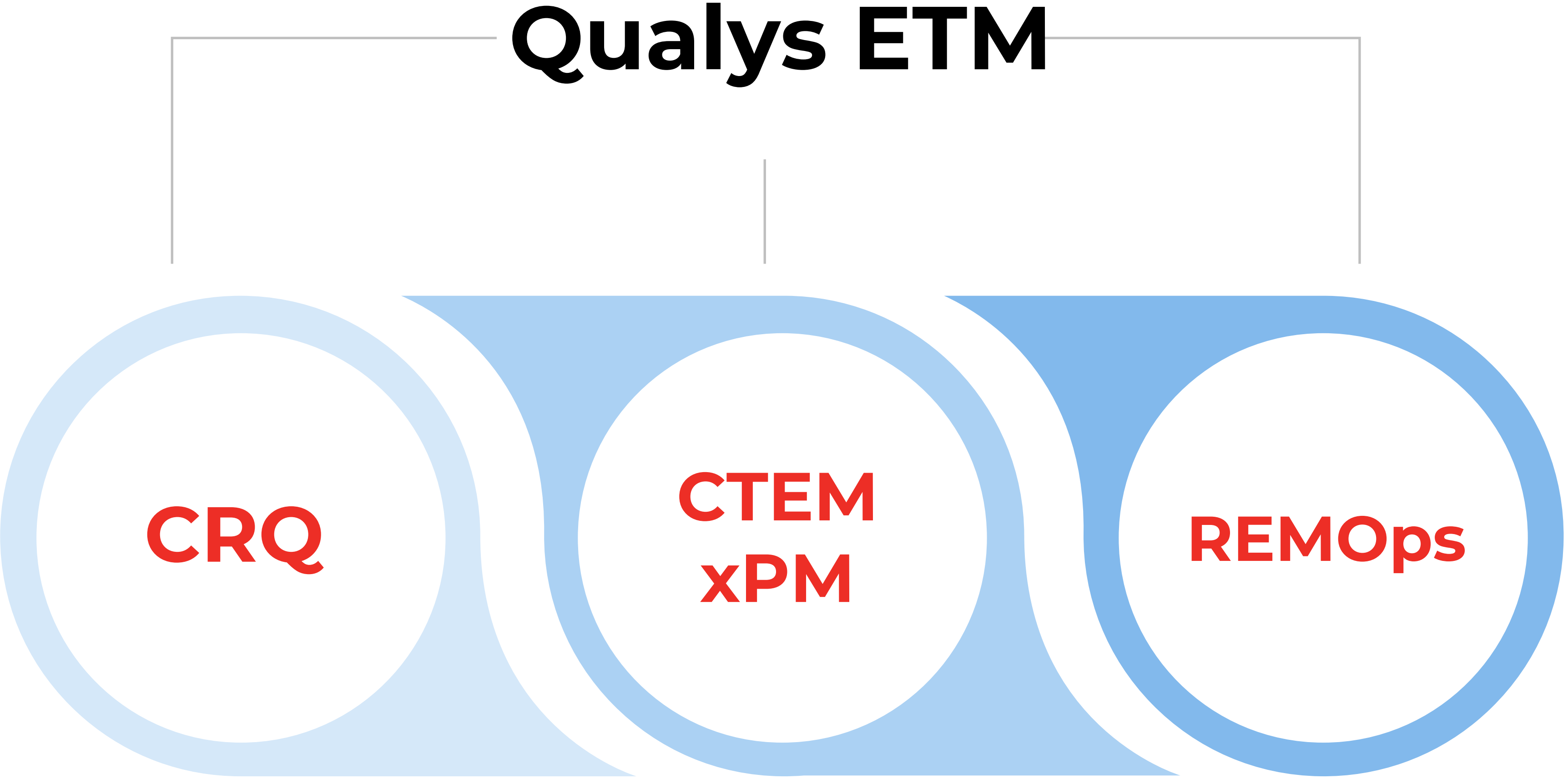
Senior Vice President,
Product, GTM & Solutions

Risk Operations Center (ROC)



How ROC gets operational with Qualys Innovations

Qualys ETM



CRQ

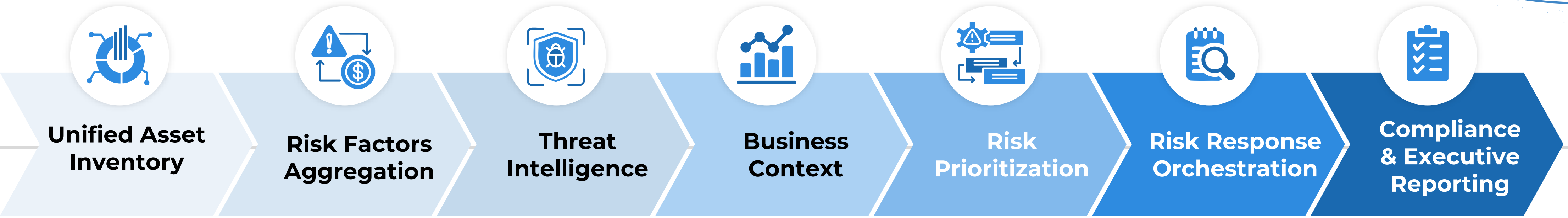
CTEM
xPM

REMOps

Qualys Enterprise TruRisk Management (ETM)

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

QUALYS

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

NON-QUALYS

Vulnerability Management

Compliance aws Google Cloud WIZ

Runtime Security

Vulnerability Management VERACODE Checkmarx snyk Burp Suite

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

THREAT INTELLIGENCE

packet storm McAfee FIREEYE

MISP Threat Sharing IMMUNITY GitHub CANADIAN CENTRE FOR CYBER SECURITY

REVERSING LABS Qualys Vulnerability Research Team PZ PROJECT ZERO VDE

Kaspersky Industrial CyberSecurity MITRE ATT&CK EPSS TALOS

Square Security GREYNOISE INTELLIGENCE

(CMDB, Custom Data Sources)

BUSINESS CONTEXT

CMDB GRC

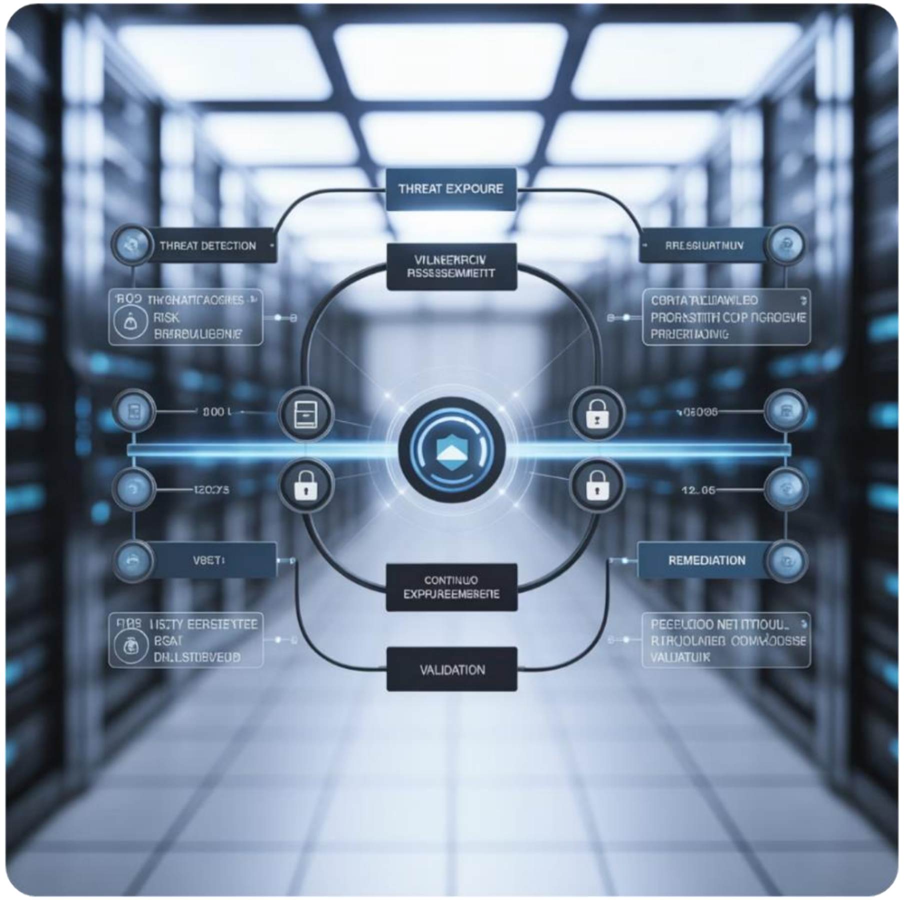
Active Directory

MEASURE | Quantify Cyber Risk in Business Terms

COMMUNICATE | Executive Reporting and Ticketing

ELIMINATE | Patch Mitigate & Track

How ETM Powers CTEM End-to-End...



01

Scoping & Discovery

Unified visibility across on-premises, cloud, and hybrid assets with automatic classification and inventory management – **CSAM/Unified Asset Inventory**

02

Prioritization

TruRisk scoring combines **TruRisk** - **QDS/QVSS** vulnerability data with threat intelligence and business context for precise risk ranking

03

Validation

TruConfirm delivers safe exploit validation, confirming real exploitability without business disruption

04

Mobilization

TruRisk Eliminate orchestrates automated patch and mitigation workflows across ITSM platforms

05

Measurement

Executive dashboards and **CRQ financials** provide board-level visibility into risk posture and remediation progress

□ **Industry-Leading CTEM Coverage:** Qualys ETM is the only platform that maps to all five Gartner CTEM phases within a single, unified architecture—eliminating the need for point solutions and vendor sprawl.:

01 Vulnerability Management (change from management):

"I can assess vulnerabilities"

What You Get:

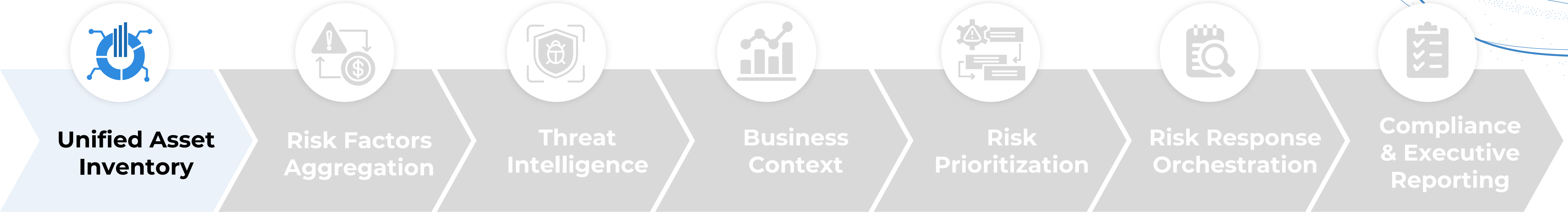
- ✓ Scan for CVEs
- ✓ CVSS based prioritization
- ✓ Compliance based reporting

How do I know the risk of the unknowns?

1%

of unknown Assets have RDP/SSH Ports Open and have Database open

ETM: Moving from VM to Attack Surface



CTEM Scoping

Attack Surface

Discovery

CTEM

Prioritization & Risk Validation

Mobilization

Cyber Risk Quantification (CRQ)

Get Inventory of all your assets – known + unknown

Known Asset Sources

Qualys Native Sensors

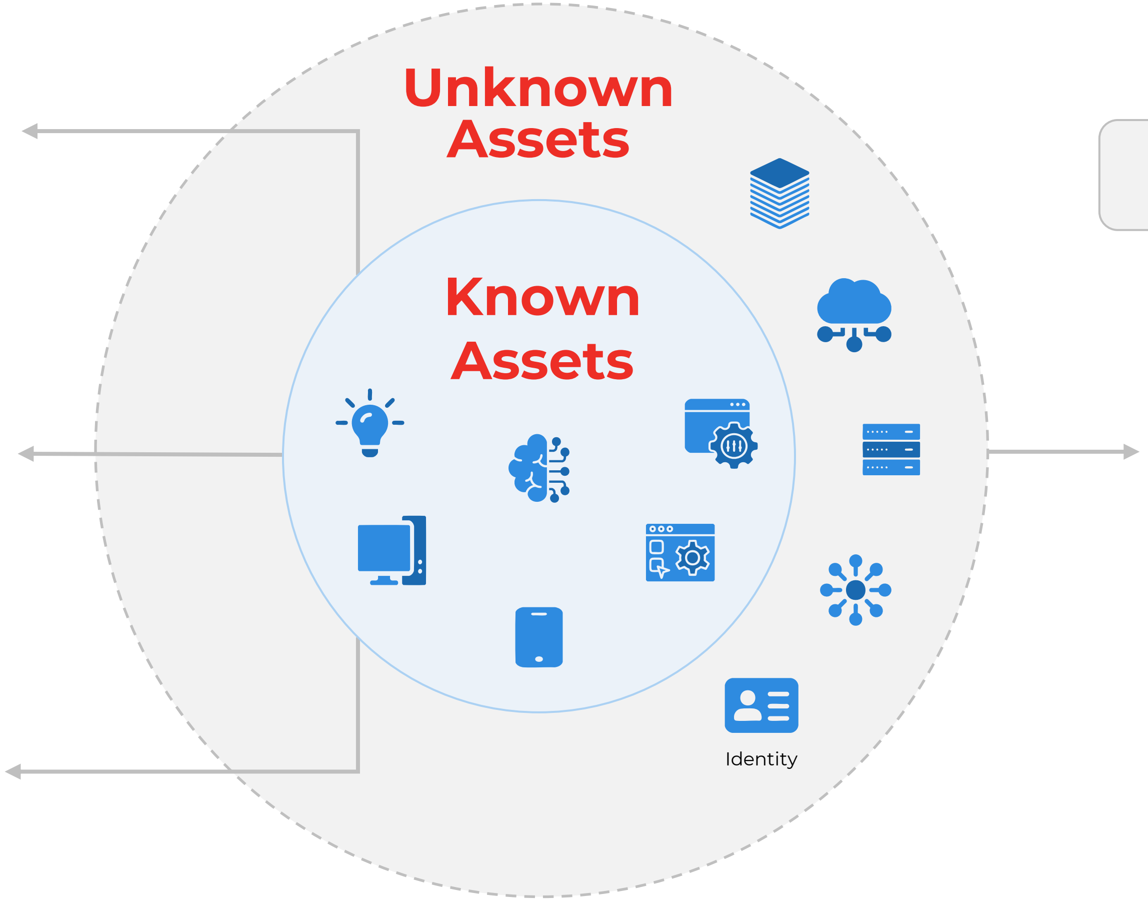
Qualys 3rd Party Connectors

WIZ tenable CROWDSTRIKE Microsoft Defender

CMDB Connectors

Active Directory servicenow

bmc helix vmware

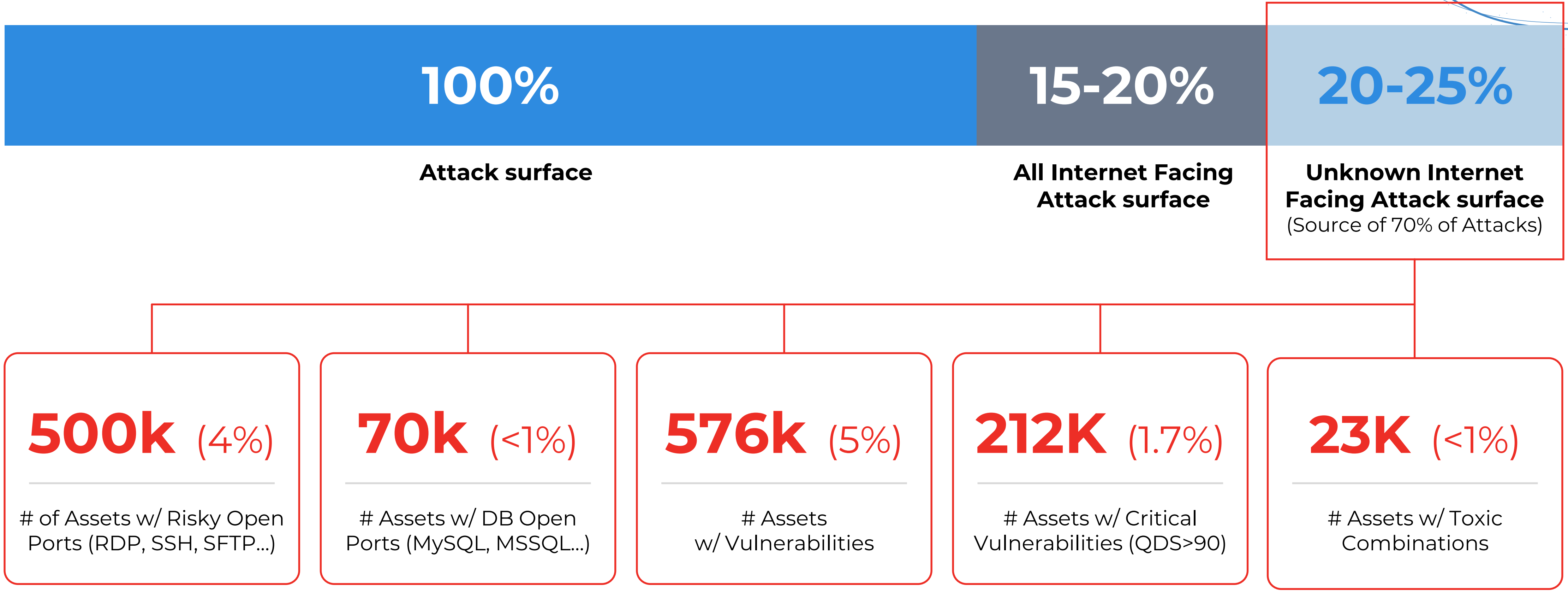


Unknown External Assets

SHODAN Scanner

DNS Whois Identity for everyone

Inventory to Attack Surface to Risk Surface



100%

Attack surface

15-20%

All Internet Facing Attack surface

20-25%

Unknown Internet Facing Attack surface (Source of 70% of Attacks)

500k (4%)

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

70k (<1%)

# Assets w/ DB Open Ports (MySQL, MSSQL...)

576k (5%)

# Assets w/ Vulnerabilities

212K (1.7%)

# Assets w/ Critical Vulnerabilities (QDS>90)

23K (<1%)

# Assets w/ Toxic Combinations

02 Attack Surface Management

> *"I know ALL my assets (known + unknown) with business context"*

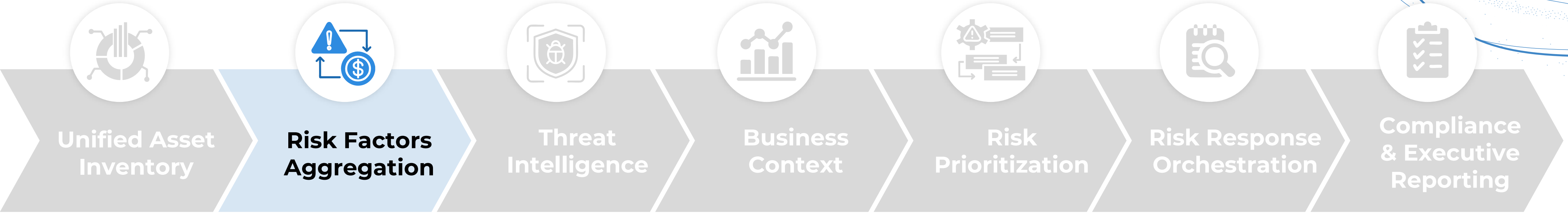
What You Get:

- ✓ Unifies inventory: on-prem + cloud + containers + external
- ✓ External attack surface management
- ✓ Business criticality mapped to assets

4%

Of riskiest exposures which matter!

ETM: Moving to Aggregation



Unified Asset Inventory

Risk Factors Aggregation

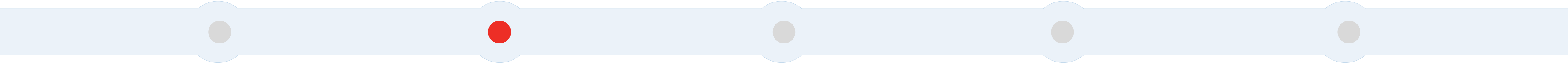
Threat Intelligence

Business Context

Risk Prioritization

Risk Response Orchestration

Compliance & Executive Reporting



CTEM Scoping

CTEM

Discovery

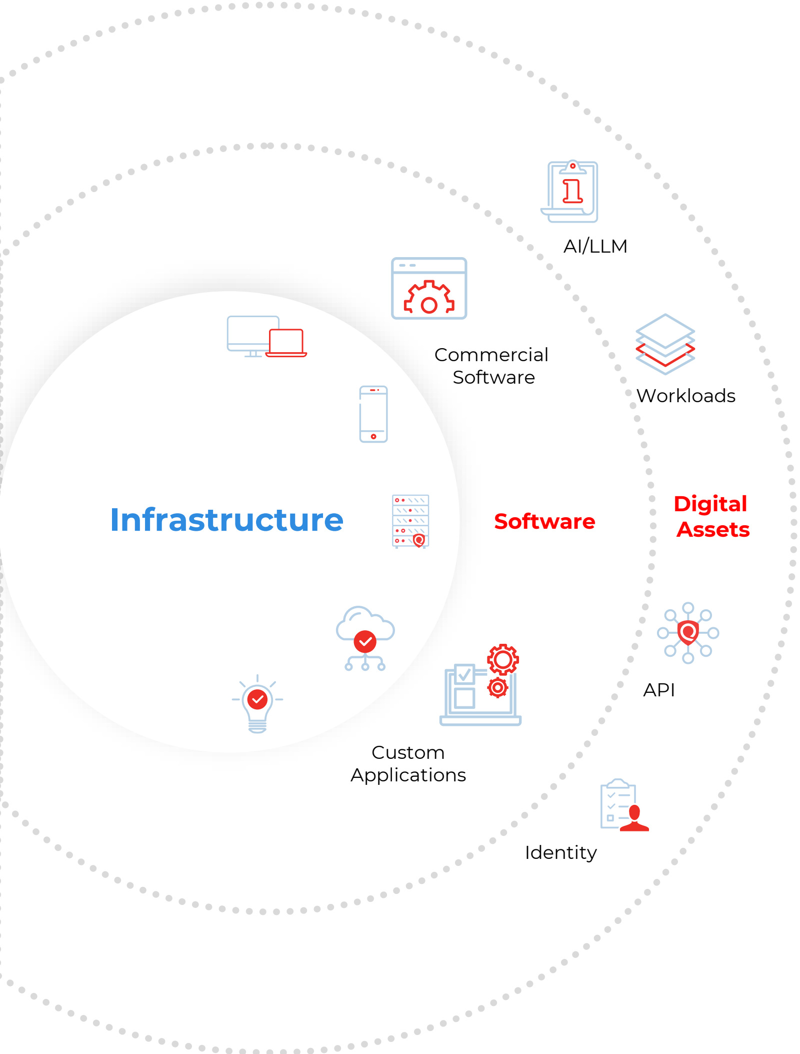
CTEM

Prioritization & Risk Validation

Mobilization

Cyber Risk Quantification (CRQ)

Bring in Siloed Exposures from Security tools



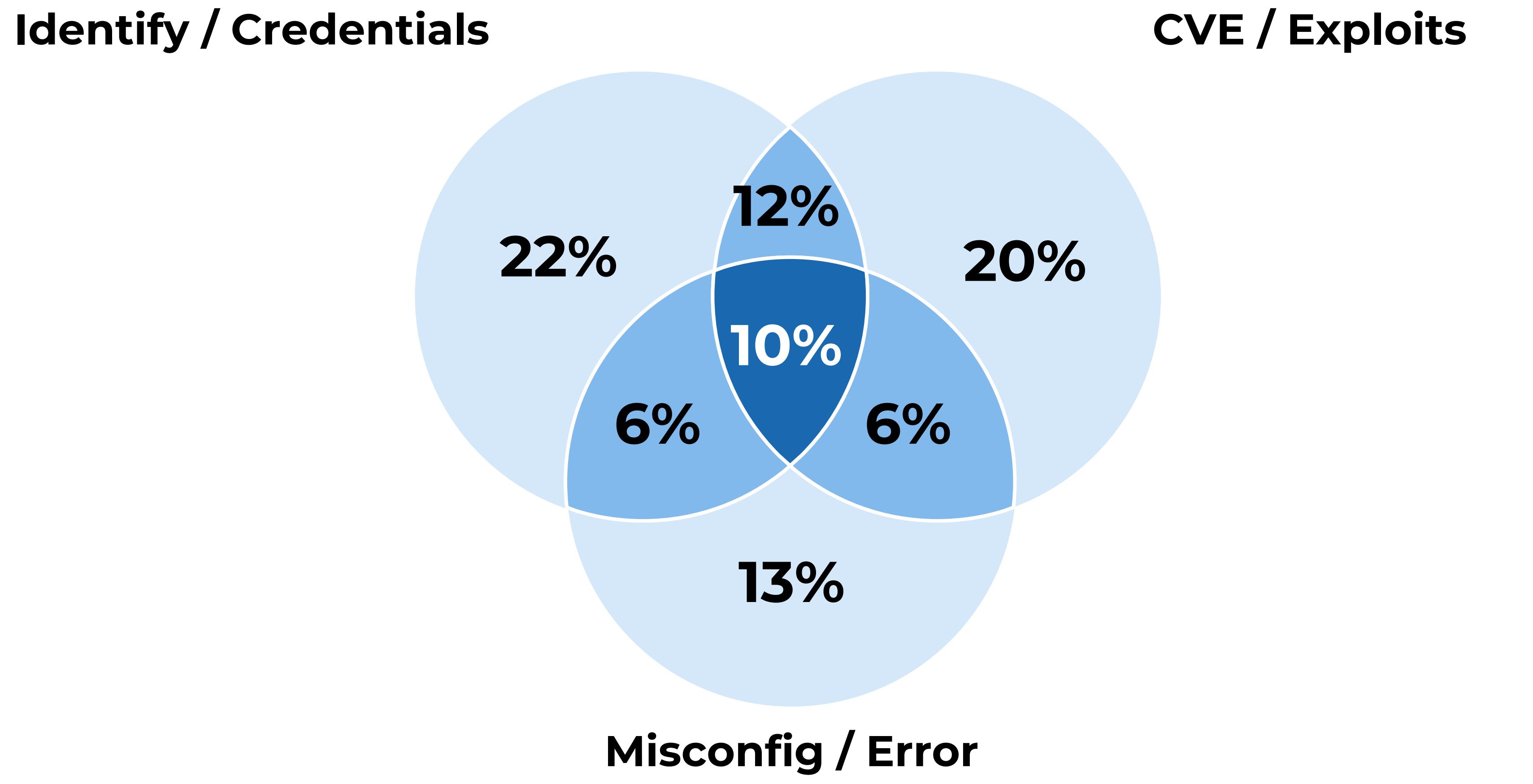
VM	CSPM
ISPM	DSPM
SSPM	AISPM

- 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**

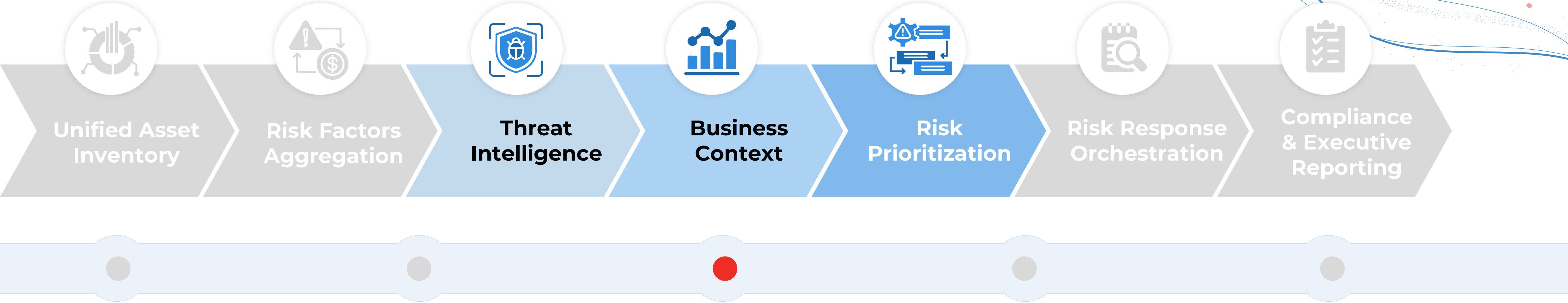
Which exposures are most important?

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



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

ETM: Risk Prioritization & Validation



CTEM Scoping

Discovery

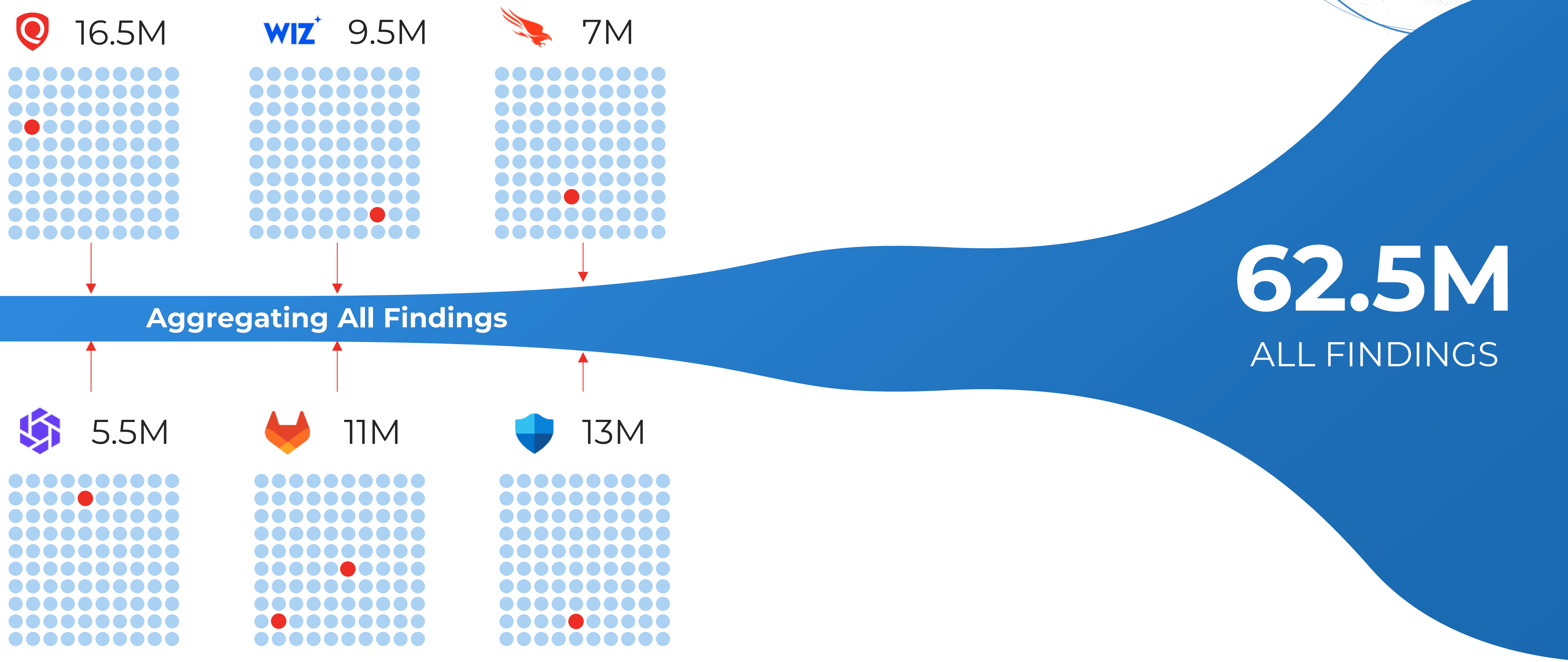
CTEM

Prioritization & Risk Validation

Mobilization

Cyber Risk Quantification (CRQ)

Millions of Fragmented Exposures coming together



16.5M

9.5M

7M

Aggregating All Findings

5.5M

11M

13M

62.5M

ALL FINDINGS

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

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

NATIONAL SECURITY AGENCY UNITED STATES OF AMERICA

CENTRAL SECURITY SERVICE UNITED STATES OF AMERICA

PZ PROJECT ZERO

Square Security

EPSS Exploit Prediction Scoring System

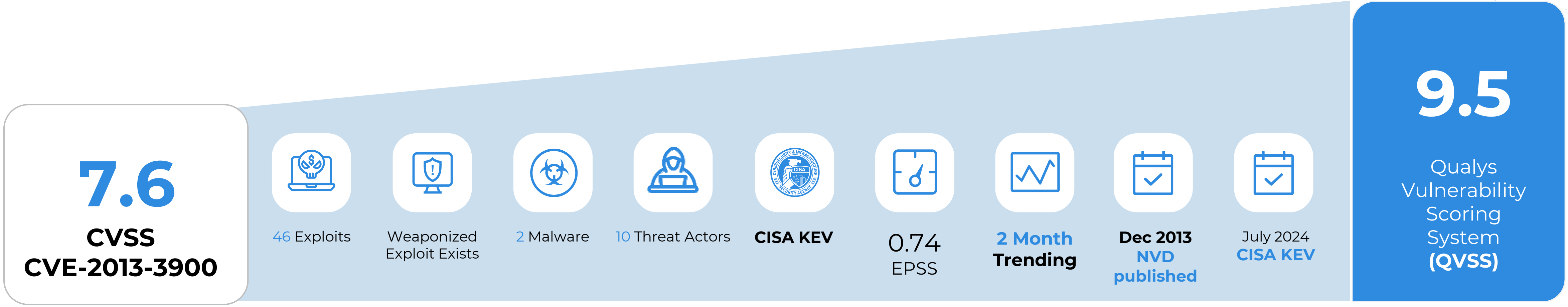
TALOS

Google

IMMUNITY

metasploit

Prioritize the exposure with threat-context



7.6

CVSS

CVE-2013-3900

46 Exploits

Weaponized Exploit Exists

2 Malware

10 Threat Actors

CISA KEV

0.74

EPSS

2 Month Trending

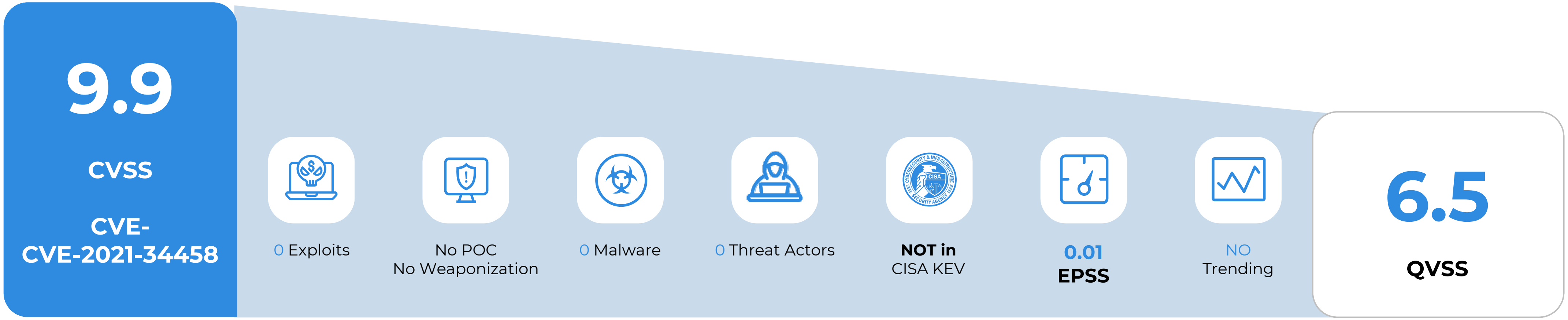
Dec 2013 NVD published

July 2024 CISA KEV

9.5

Qualys Vulnerability Scoring System (QVSS)

Deprioritize the exposure, if no threat-context



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

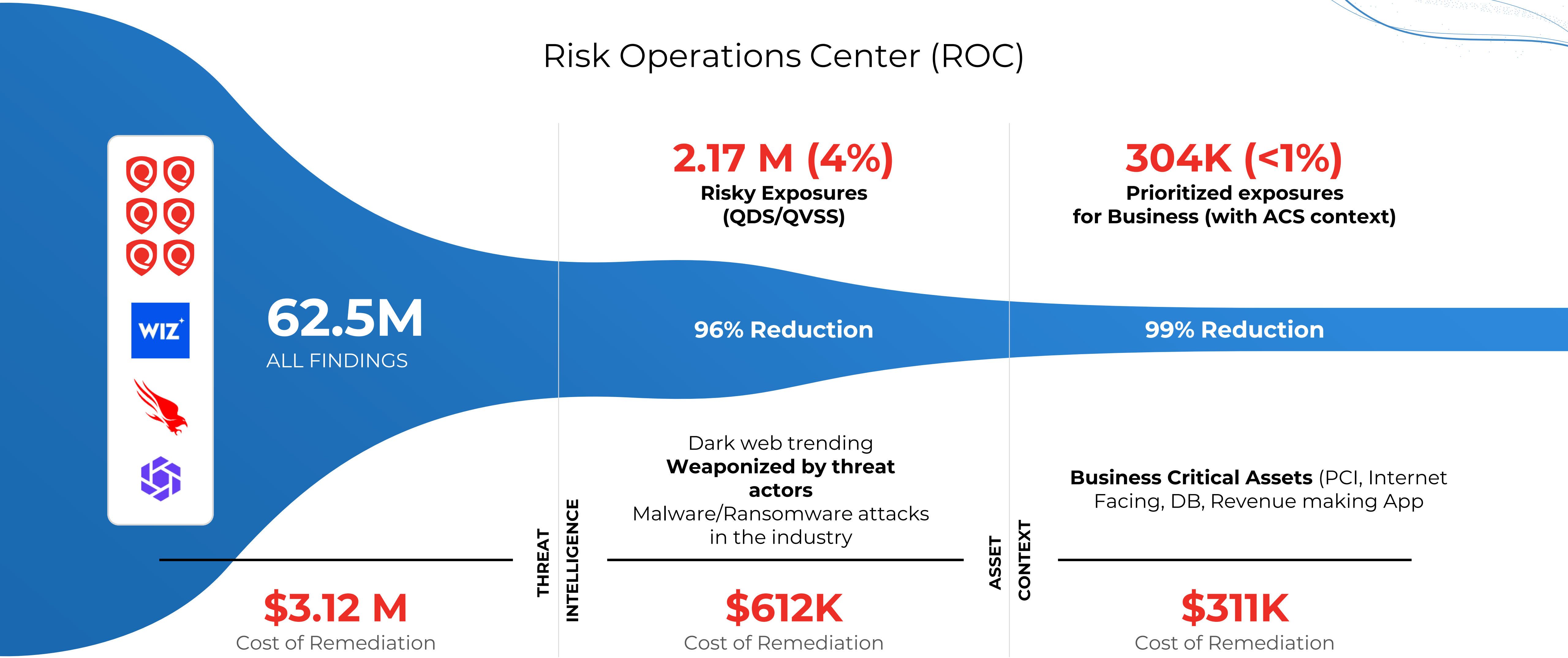
NO
Trending

6.5

QVSS

Prioritizing risky exposures which Matter, from millions of exposures

Risk Operations Center (ROC)



62.5M

ALL FINDINGS

$3.12 M

Cost of Remediation

THREAT INTELLIGENCE

2.17 M (4%)

Risky Exposures (QDS/QVSS)

96% Reduction

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

$612K

Cost of Remediation

ASSET CONTEXT

304K (<1%)

Prioritized exposures for Business (with ACS context)

99% Reduction

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

$311K

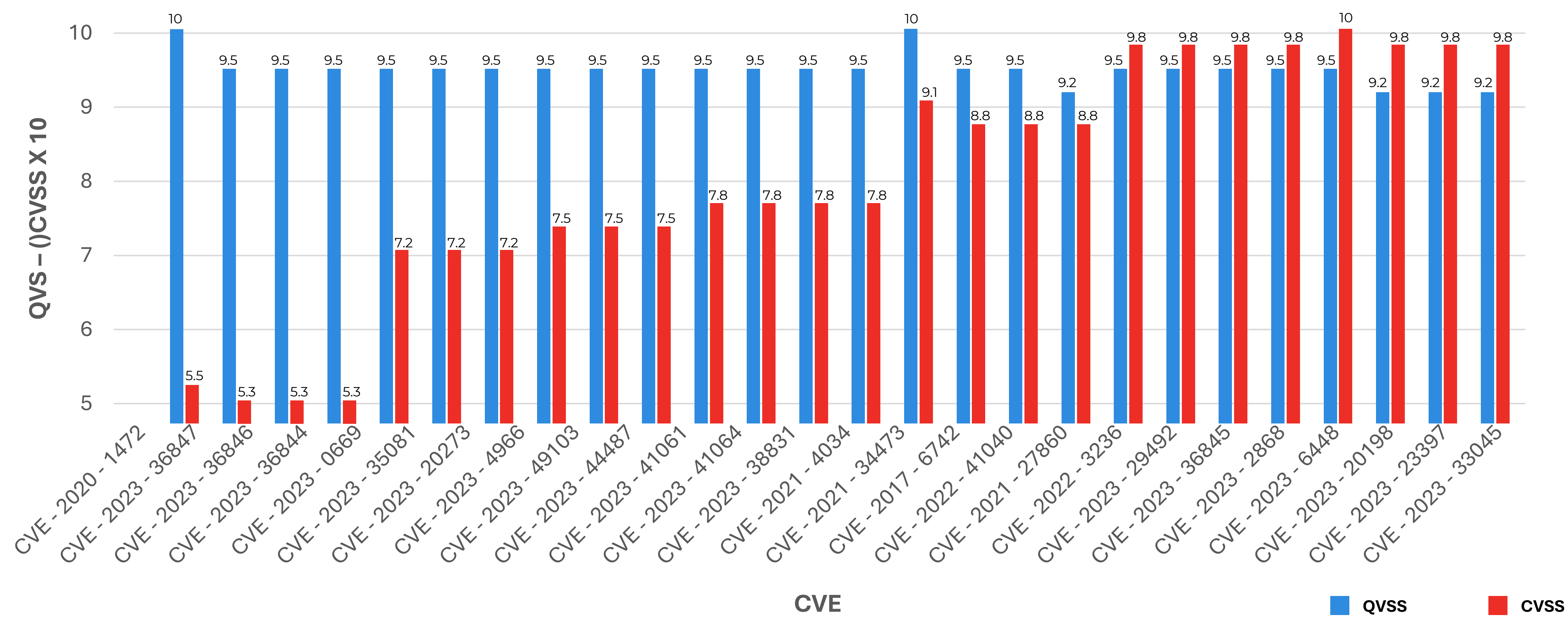
Cost of Remediation

How Proactive is your Risk Prioritization...

TruRisk Prioritizes Exposures **45 days before** CISA adds them to the KEV...

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

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.



03 Risk-Based Prioritization

> *"I know which 4% of exposures cause the most risk"*

What You Get:

- ✓ TruRisk scoring (Qualys detection score + asset business context)
- ✓ 25+ threat intel feeds
- ✓ 95% noise reduction
- ✓ Focus on business-critical few

My Risk is not just Vulnerabilities

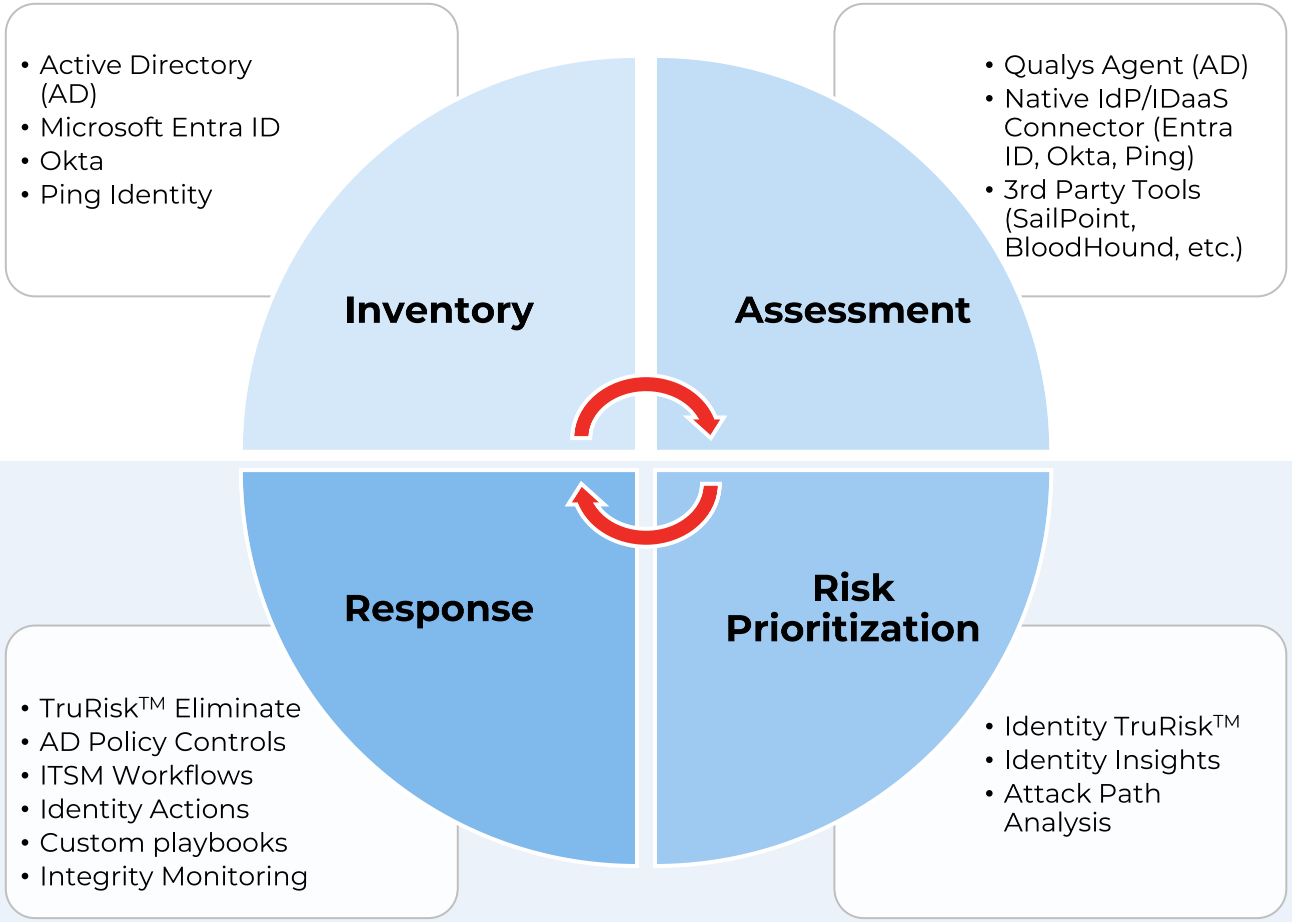
35%

Of Attacks are due to the toxic combination of Identity, CVEs, & Misconfigurations

Risk prioritization: Identities…

Integrated with ETM

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



Inventory

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

Assessment

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

Risk Prioritization

- Identity TruRisk™
- Identity Insights
- Attack Path Analysis

Response

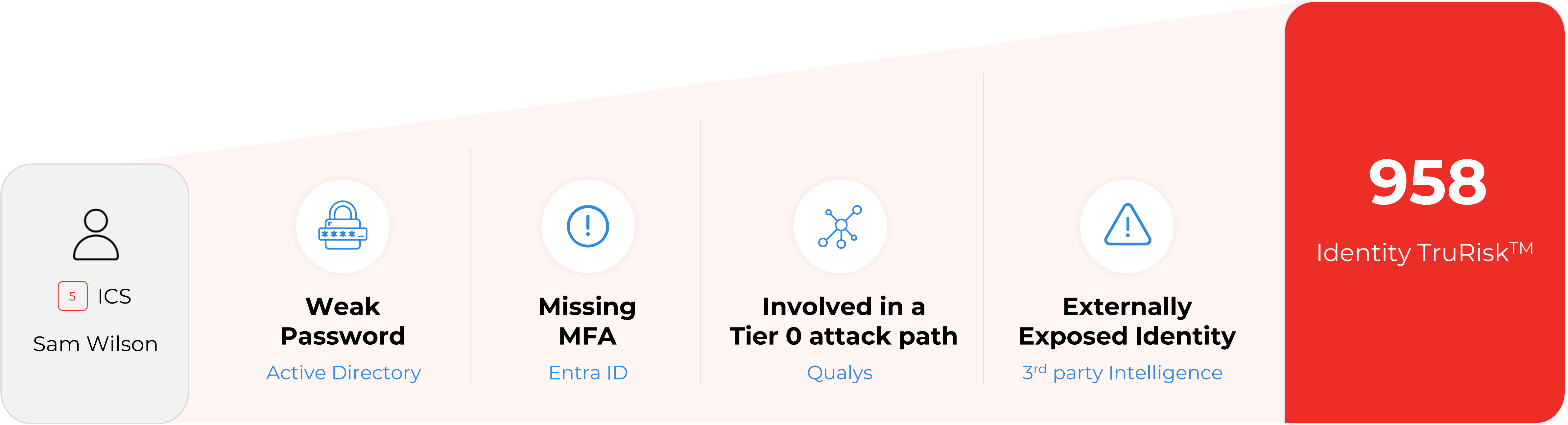
- TruRisk™ Eliminate
- AD Policy Controls
- ITSM Workflows
- Identity Actions
- Custom playbooks
- Integrity Monitoring

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

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

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

Prioritize Identities based on Risk



5 ICS

Sam Wilson

Weak Password
Active Directory

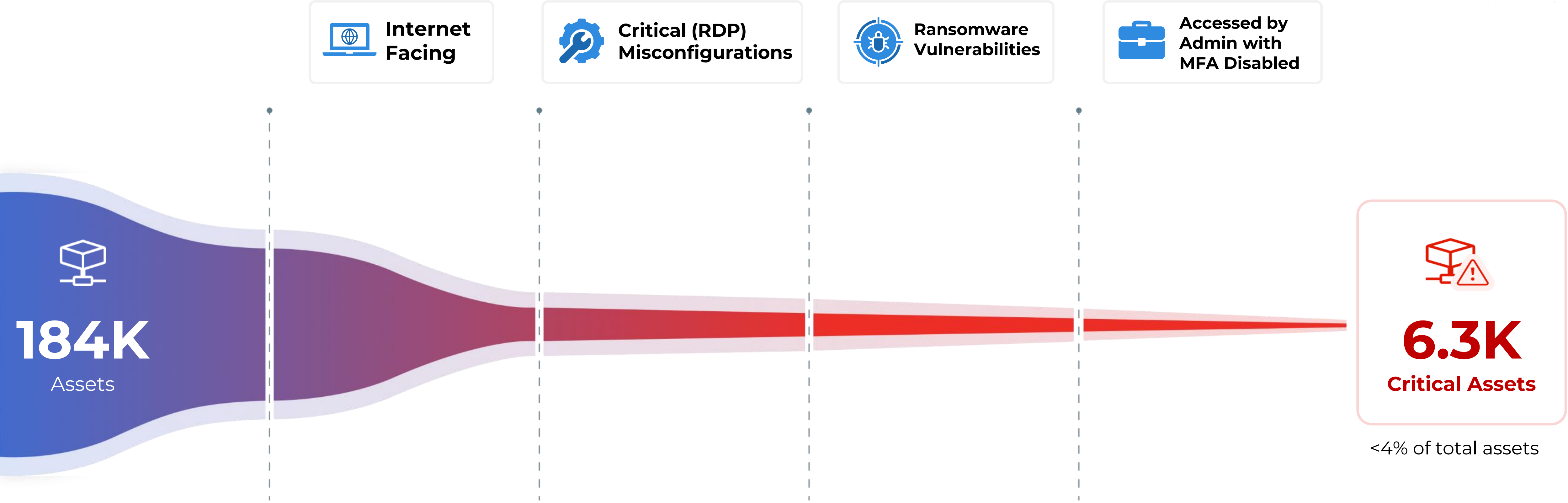
Missing MFA
Entra ID

Involved in a Tier 0 attack path
Qualys

Externally Exposed Identity
3rd party Intelligence

958
Identity TruRisk™

Toxic Risk Combinations from Siloed Findings... Helping Prioritize Assets needing attention


Internet Facing
Critical (RDP) Misconfigurations
Ransomware Vulnerabilities
Accessed by Admin with MFA Disabled
184K
Assets
6.3K
Critical Assets

<4% of total assets

03 Risk-Based Prioritization

“I know which 4% of exposures cause the most risk”

What You Get:

- ✓ TruRisk scoring (Qualys detection score + asset business context)
- ✓ 25+ threat intel feeds
- ✓ 95% noise reduction
- ✓ Focus on business-critical few

How can I know if I have risk from the trending threats in my industry…

Adversary based Risk Prioritization & Remediation

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 APAC

03 Risk-Based Prioritization

“I know which 4% of exposures cause the most risk”

What You Get:

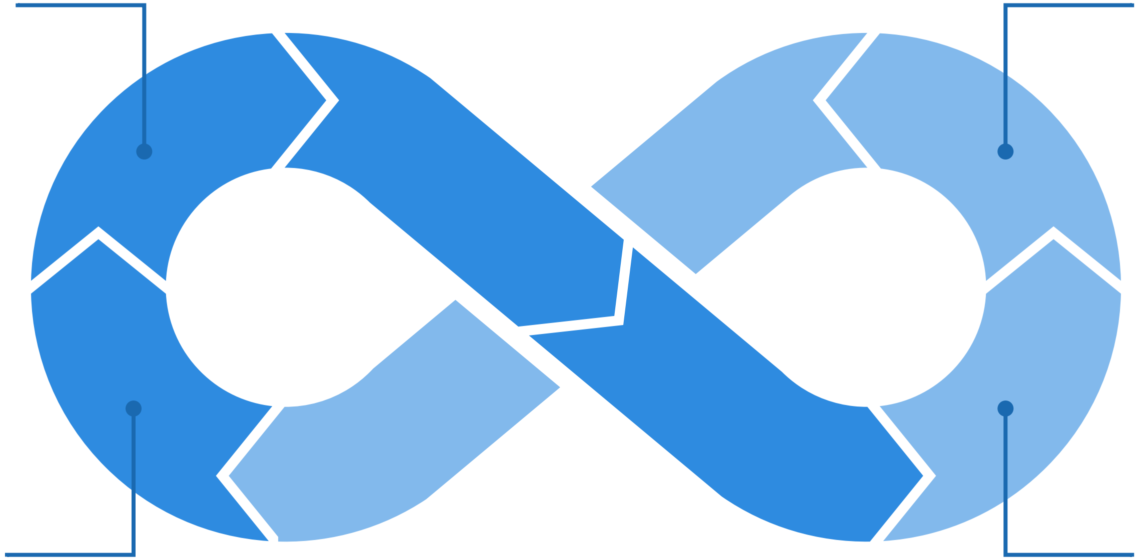
- ✓ TruRisk scoring (Qualys detection score + asset business context)
- ✓ 25+ threat intel feeds
- ✓ 95% noise reduction
- ✓ Focus on business-critical few

Which ones can be actually exploited by an attacker

~2%

Risky exposures are truly exploitable

TruConfirm: Validate Exposures, Confirm Exploitation, Accelerate Remediation



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

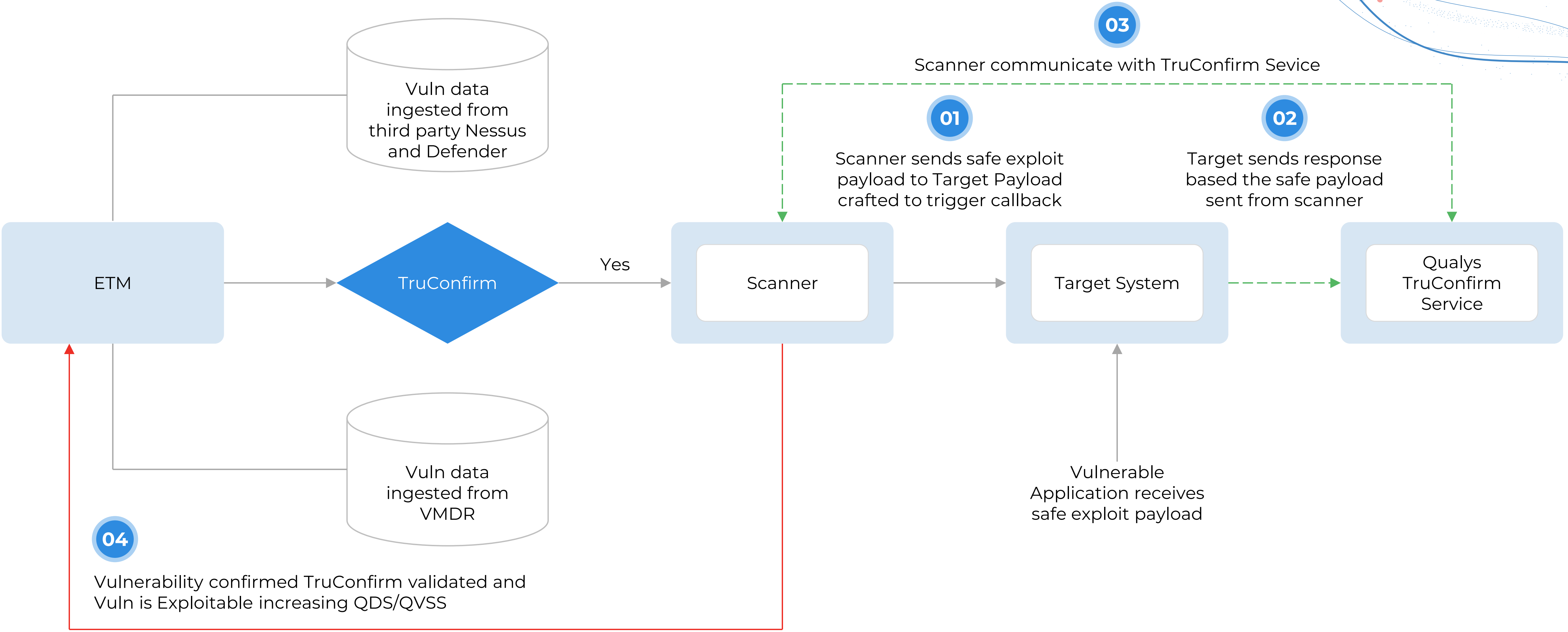
TruRisk Prioritization based on Threats Environmental/business asset context to prioritize risky exposures

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

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

TruConfirm: Safe Exploitation Route

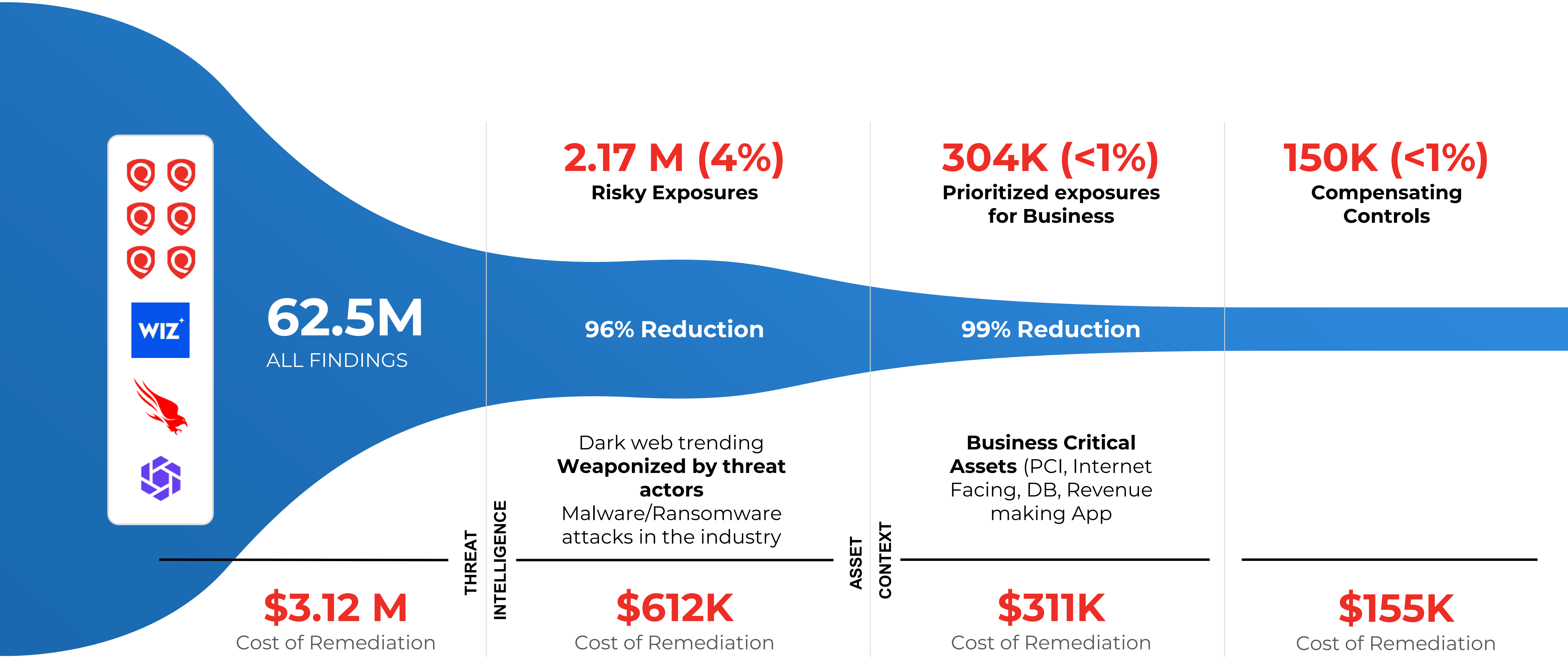
Qualys. ROCon 25 The Risk Operations Conference APAC


03
Scanner communicate with TruConfirm Sevice
Vuln data ingested from third party Nessus and Defender
01
Scanner sends safe exploit payload to Target Payload crafted to trigger callback
02
Target sends response based the safe payload sent from scanner
ETM
TruConfirm
Yes
Scanner
Target System
Qualys TruConfirm Service
Vuln data ingested from VMDR
Vulnerable Application receives safe exploit payload
04
Vulnerability confirmed TruConfirm validated and Vuln is Exploitable increasing QDS/QVSS

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

Prioritizing Risk which Matters, Increases Efficiency

Risk Operations Center (ROC)



62.5M

ALL FINDINGS

$3.12 M

Cost of Remediation

THREAT INTELLIGENCE

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

ASSET CONTEXT

304K (<1%)

Prioritized exposures for Business

99% Reduction

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

$311K

Cost of Remediation

150K (<1%)

Compensating Controls

$155K

Cost of Remediation

04 Validated Risk

“I know which riskiest exposures are confirmed exploitable”

What You Get:

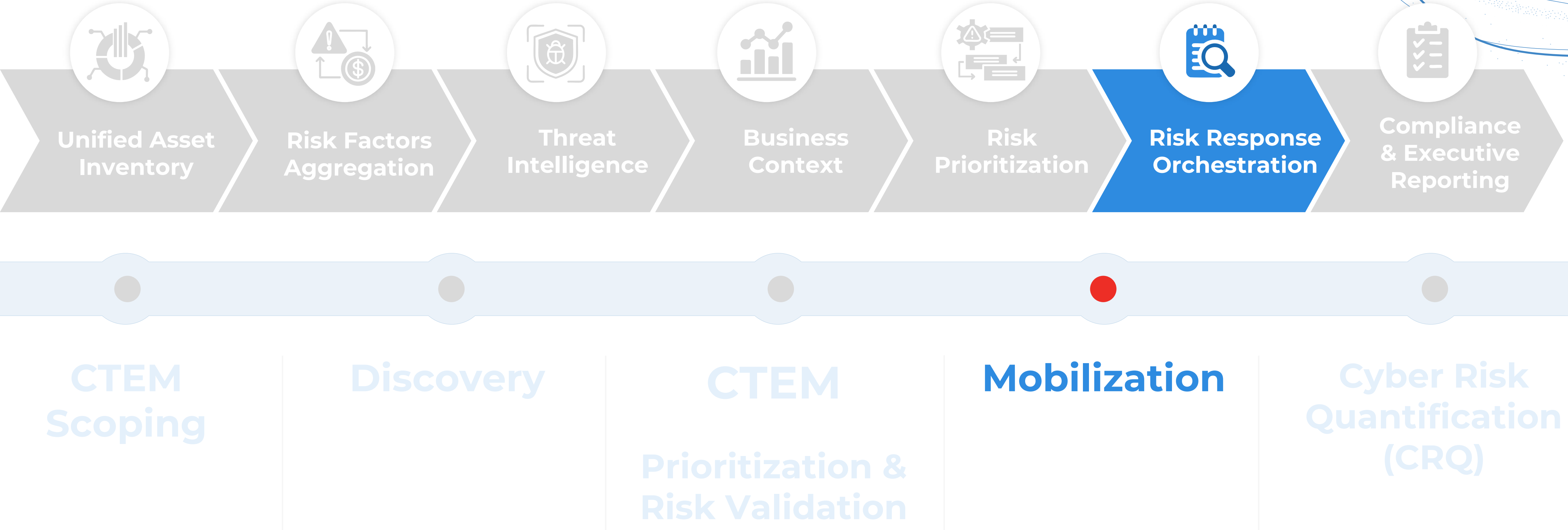
- ✓ TruConfirm validates exploitability
- ✓ Mitigation controls tested
- ✓ Safe exploit tested

How should I reduce my risk with or without a patch

< 18

Should be your MTTR for your risky vulnerabilities

Cyber Risk Management Journey

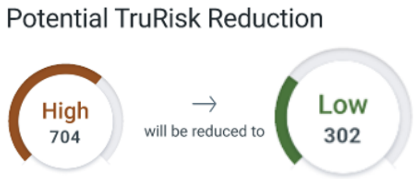


Selection Prioritization Approach

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

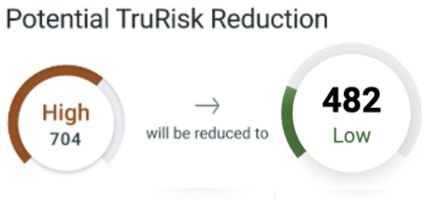
Highest Risk Reduction

Critical Vulnerabilities (Ransomware, CISA KEVs) on all assets


Potential TruRisk Reduction

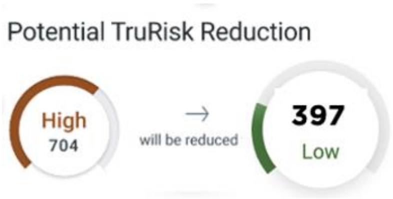
Low Risk Reduction

Patch Critical Vulnerabilities on non-critical assets


Potential TruRisk Reduction

Balanced Risk Reduction

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

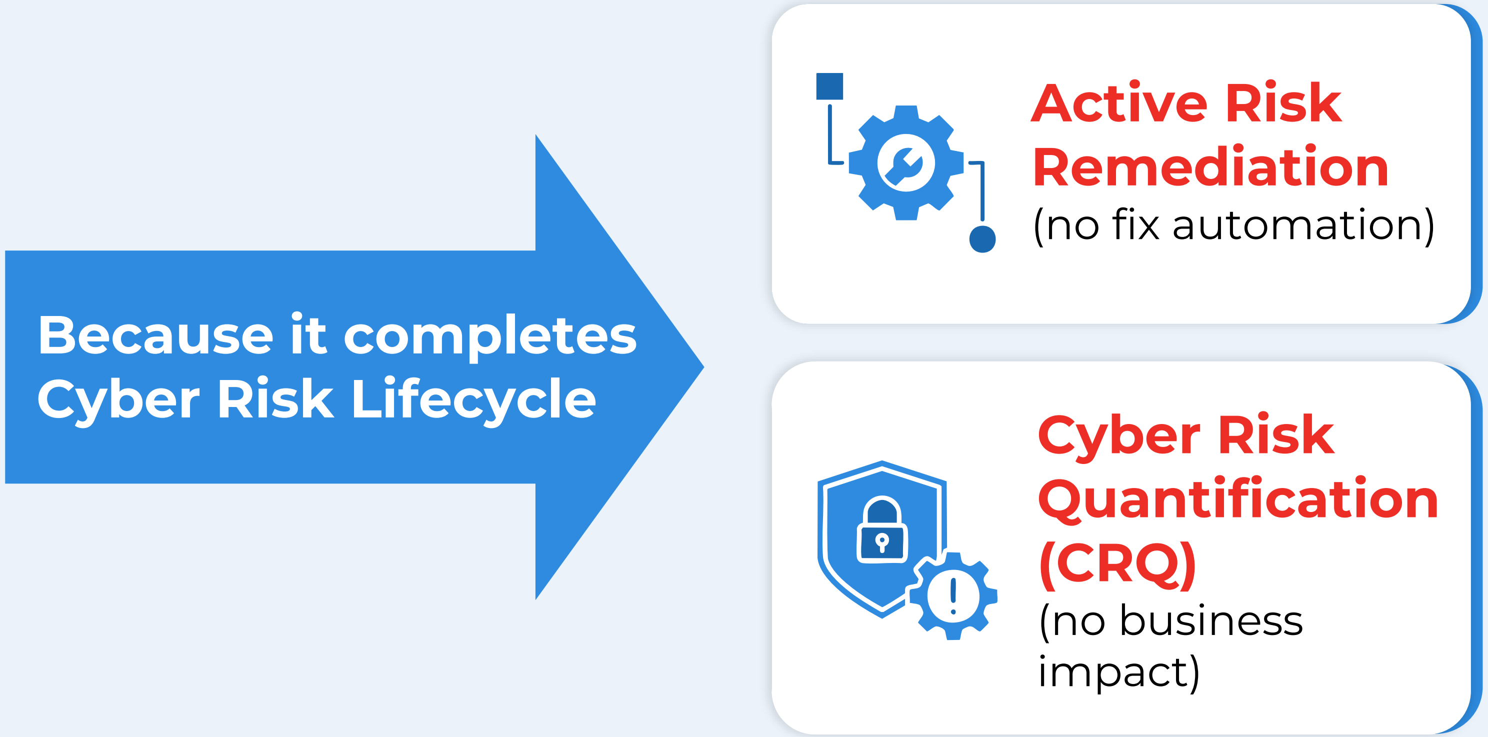

Potential TruRisk Reduction

Let me Decide

Build a custom template based on your business requirements.

CTEM Stops here...

ETM is more than CTEM

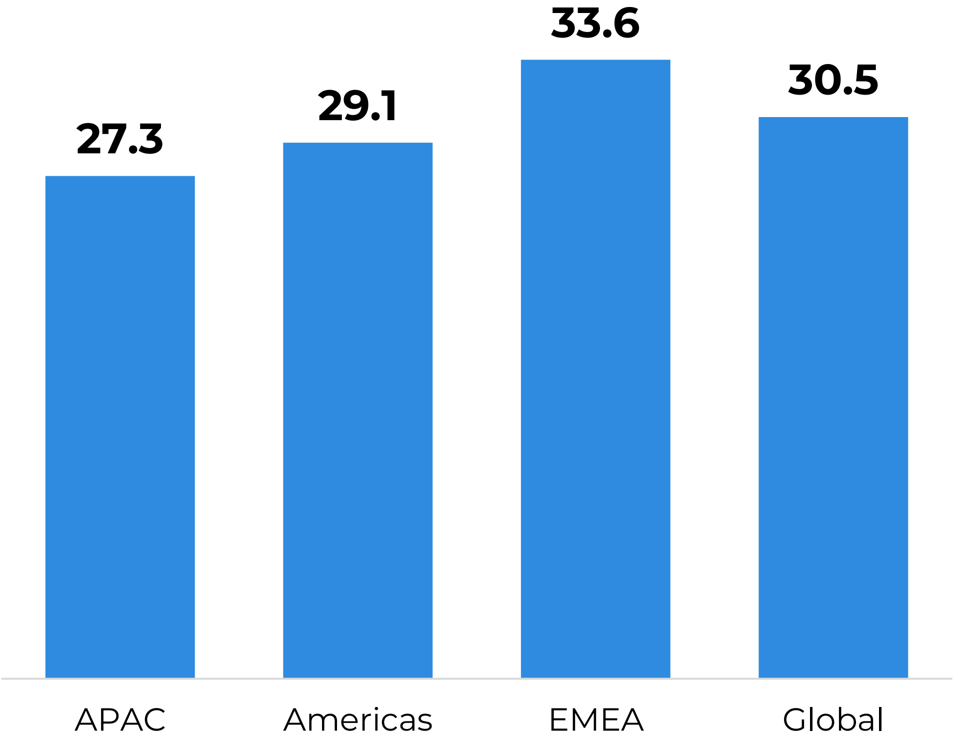


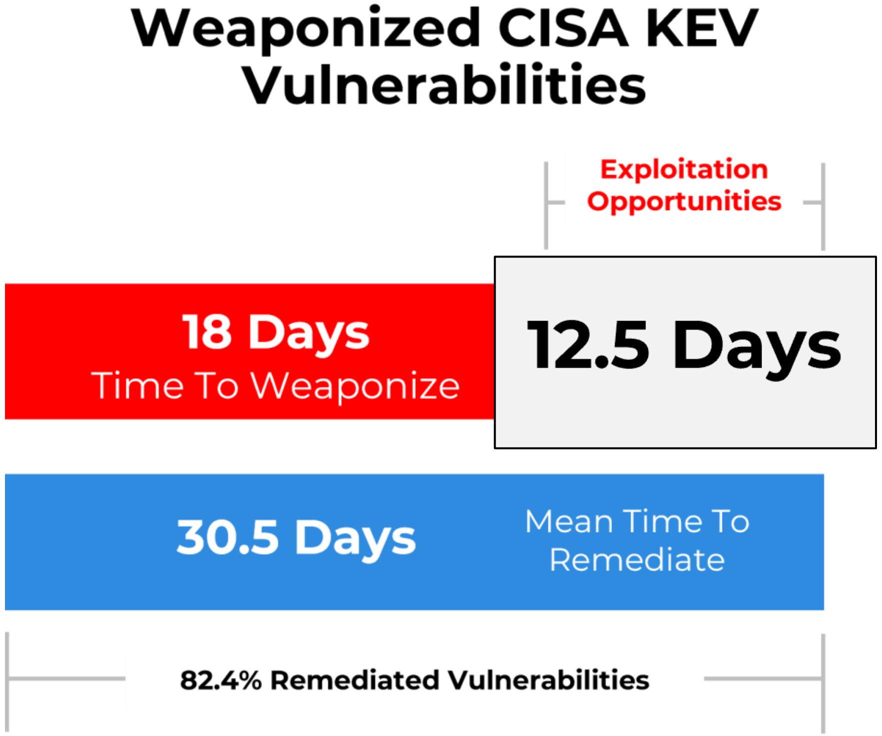
Because it completes Cyber Risk Lifecycle

Active Risk Remediation
(no fix automation)

Cyber Risk Quantification (CRQ)
(no business impact)

Problem in Risk Reduction is 2-Fold




Weaponized CISA KEV Vulnerabilities
Exploitation Opportunities
18 Days
Time To Weaponize
12.5 Days
30.5 Days
Mean Time To Remediate
82.4% Remediated Vulnerabilities

Problem in Risk Reduction is 2-Fold

MTTR for Risky vulnerabilities need to be < 18 Days

Impact of Qualys Patch Management

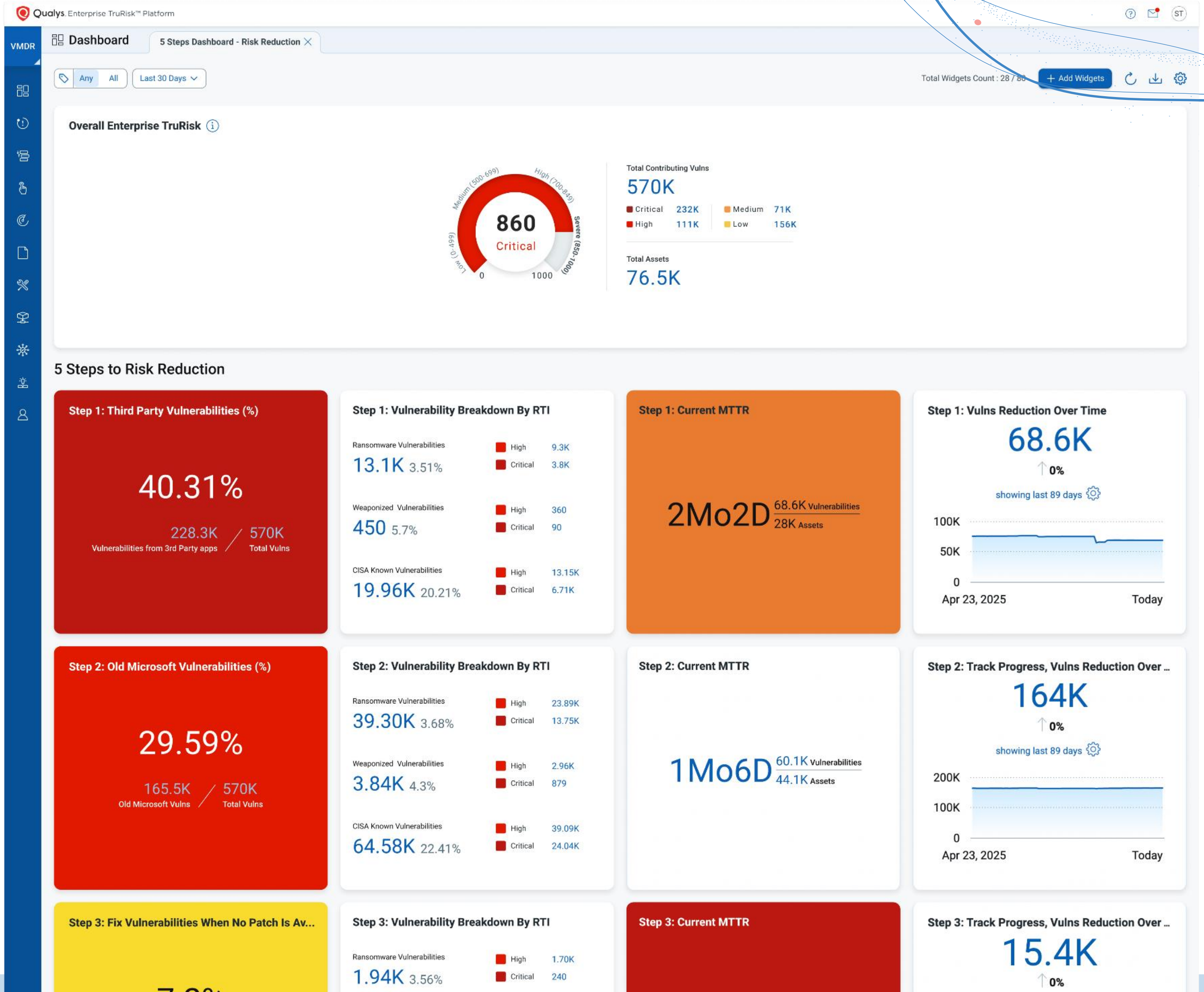
Qualys. ROCon25
The Risk Operations Conference
APAC

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



Qualys. Enterprise TruRisk™ Platform

VMDR | Dashboard | 5 Steps Dashboard - Risk Reduction

Any | All | Last 30 Days

Total Widgets Count : 28 / 80 | + Add Widgets

Overall Enterprise TruRisk

860 Critical (Low (0-499), Medium (500-699), High (700-849), Severe (850-1000); 0 – 1000)

Total Contributing Vulns
570K

Critical	232K	Medium	71K
High	111K	Low	156K

Total Assets
76.5K

5 Steps to Risk Reduction

Step 1: Third Party Vulnerabilities (%)
40.31%
228.3K Vulnerabilities from 3rd Party apps / 570K Total Vulns

Step 1: Vulnerability Breakdown By RTI

Ransomware Vulnerabilities 13.1K 3.51%	High	9.3K
	Critical	3.8K
Weaponized Vulnerabilities 450 5.7%	High	360
	Critical	90
CISA Known Vulnerabilities 19.96K 20.21%	High	13.15K
	Critical	6.71K

Step 1: Current MTTR
2Mo2D 68.6K Vulnerabilities / 28K Assets

Step 1: Vulns Reduction Over Time
68.6K
0%
showing last 89 days
100K, 50K, 0; Apr 23, 2025 – Today

Step 2: Old Microsoft Vulnerabilities (%)
29.59%
165.5K Old Microsoft Vulns / 570K Total Vulns

Step 2: Vulnerability Breakdown By RTI

Ransomware Vulnerabilities 39.30K 3.68%	High	23.89K
	Critical	13.75K
Weaponized Vulnerabilities 3.84K 4.3%	High	2.96K
	Critical	879
CISA Known Vulnerabilities 64.58K 22.41%	High	39.09K
	Critical	24.04K

Step 2: Current MTTR
1Mo6D 60.1K Vulnerabilities / 44.1K Assets

Step 2: Track Progress, Vulns Reduction Over ...
164K
0%
showing last 89 days
200K, 100K, 0; Apr 23, 2025 – Today

Step 3: Fix Vulnerabilities When No Patch Is Av...

Step 3: Vulnerability Breakdown By RTI

Ransomware Vulnerabilities 1.94K 3.56%	High	1.70K
	Critical	240

Step 3: Current MTTR

Step 3: Track Progress, Vulns Reduction Over ...
15.4K
0%

Impact of Qualys TruRisk Eliminate

140M

Patches + Mitigations Deployed in last 12 months

- Mitigation + Isolation
- No VPN
- Rollback
- RBAC
- Patch via SCCM
- Smart Chaining
- ServiceNow Integrated

40%

Faster MTTR than traditional patch

5%

Customers in 0-5 days MTTR

9%

Customers in 6-10 days

32%

Customers in 11 to 17 days

How Proactive is your Risk Remediation...

TruRisk Eliminate integrated with TruRisk Prioritization Remediates Risky Exposures 27 days before they are added in CISA KEVs...

The **patch** can break my **critical assets**

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

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.

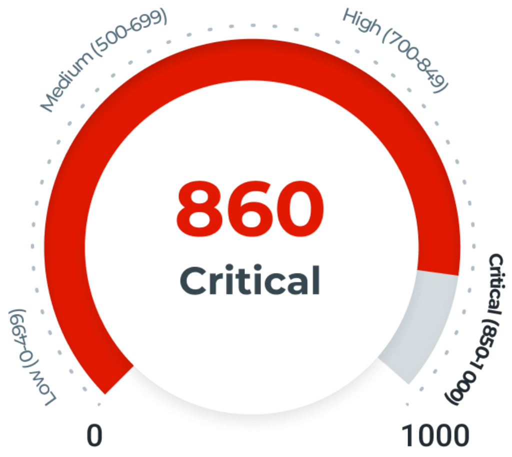
Accelerate MTTR with Patch Reliability Score

	Avg Risky Vulnerabilities per customer		**With Patch Reliability**
01	Existing on **Non-Critical** Assets	10.2K	High Reliability (82%) **Patch Automation**
02	Existing on **Critical** Assets	30K	High Reliability (78%) **Staged Patch rollout** with minimal testing delays
03	Not Patched due to **Business Impact**	16.3K	
04	Exist on Critical Assets with **No Patch Available**	6K	**Deploy Permanent Fixes** Created by Qualys Research Team

With TruRisk Eliminate

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

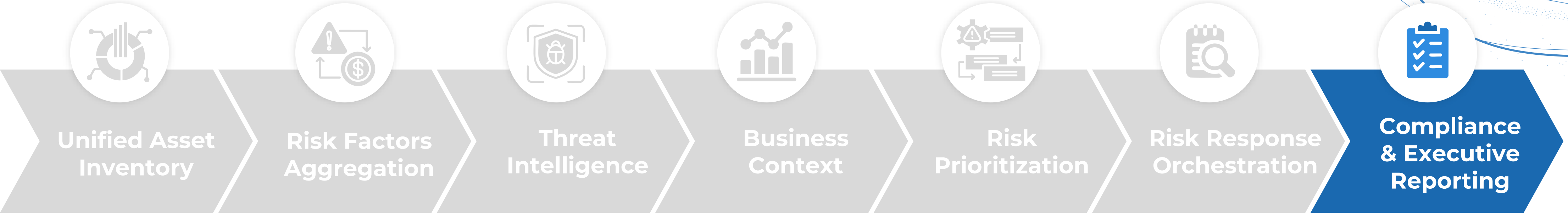
Have Permanent Fixes Provided by
TruRisk Eliminate

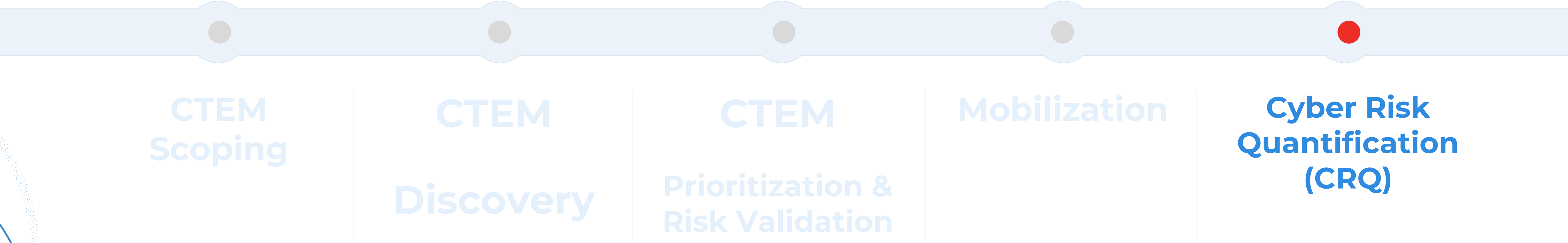
TruRisk Eliminate ensures the reduction of Cyber Risk and MTTR through focused Risk Elimination Strategies

|

ETM: Compliance & Executive Reporting

Qualys. ROCon 25 The Risk Operations Conference APAC




CTEM Scoping
CTEM
Discovery
CTEM
Prioritization & Risk Validation
Mobilization
Cyber Risk Quantification (CRQ)

Speaking the language of the executives…

Financial Impact

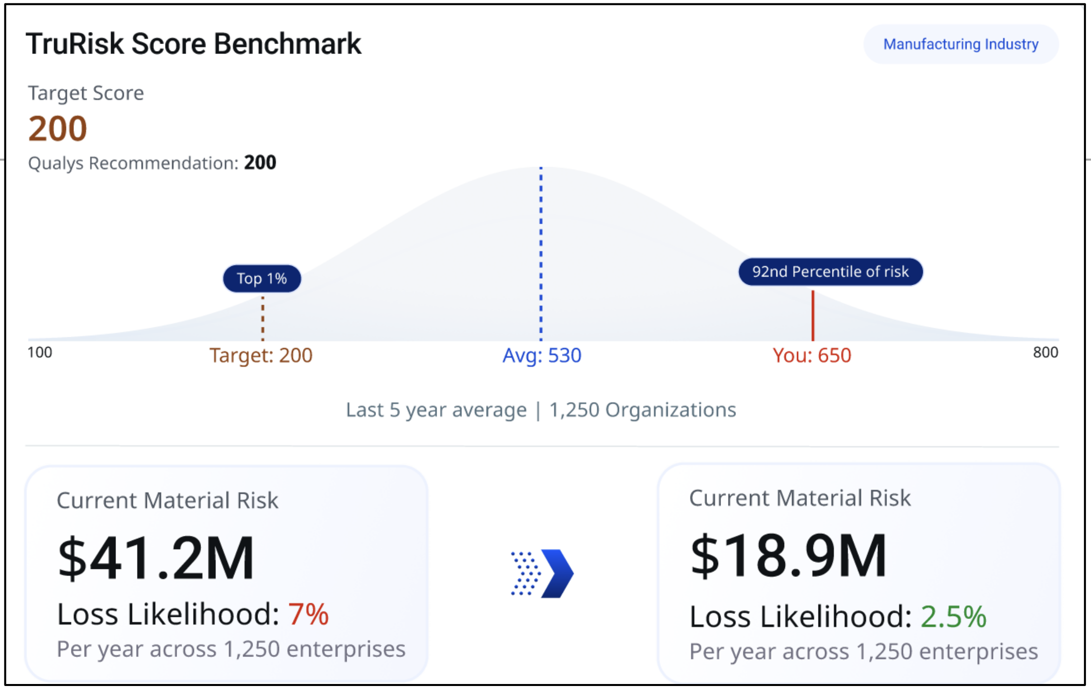
Industry risk

Executives wanting to know financial impact for budget decisions

Cyber risk and security teams managing exposures and risk

TruRisk

TruRisk Cohort



TruRisk Score Benchmark

Manufacturing Industry

Target Score

200

Qualys Recommendation: **200**

Last 5 year average | 1,250 Organizations

Current Material Risk

$41.2M

Loss Likelihood: 7%

Per year across 1,250 enterprises

Current Material Risk

$18.9M

Loss Likelihood: 2.5%

Per year across 1,250 enterprises

Compliance Assessment and Reporting

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

Regulations

ISO GDPR

NIST PCI DSS v4.0

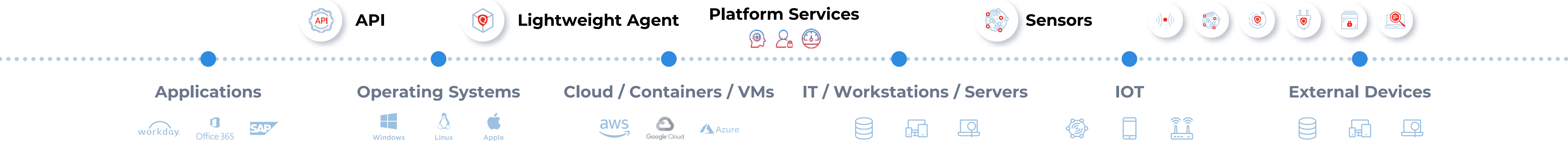
...and many more!

✗ Asset discovery & management

✗ Identities: passwords and accounts

✗ Access control and permissions

✗ System and file integrity



Compliance Assessment and Reporting

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

Regulations

ISO GDPR

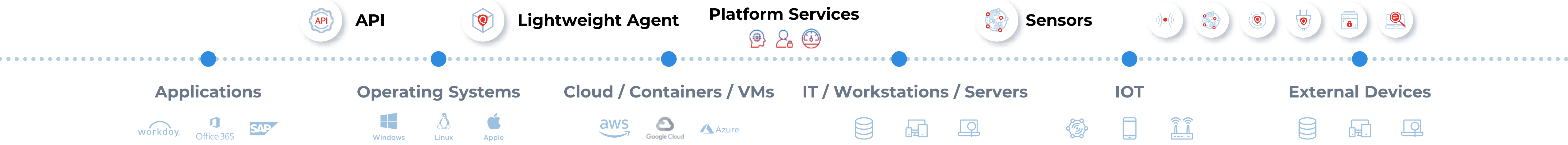
NIST PCI DSS v4.0

...and many more!

01 Auto discover your audit scope

02 Collect and map Evidence to get Audit Readiness report

03 Know and automatically fix prioritized audit gaps



API

Lightweight Agent

Platform Services

Sensors

Applications: workday, Office 365, SAP

Operating Systems: Windows, Linux, Apple

Cloud / Containers / VMs: aws, Google Cloud, Azure

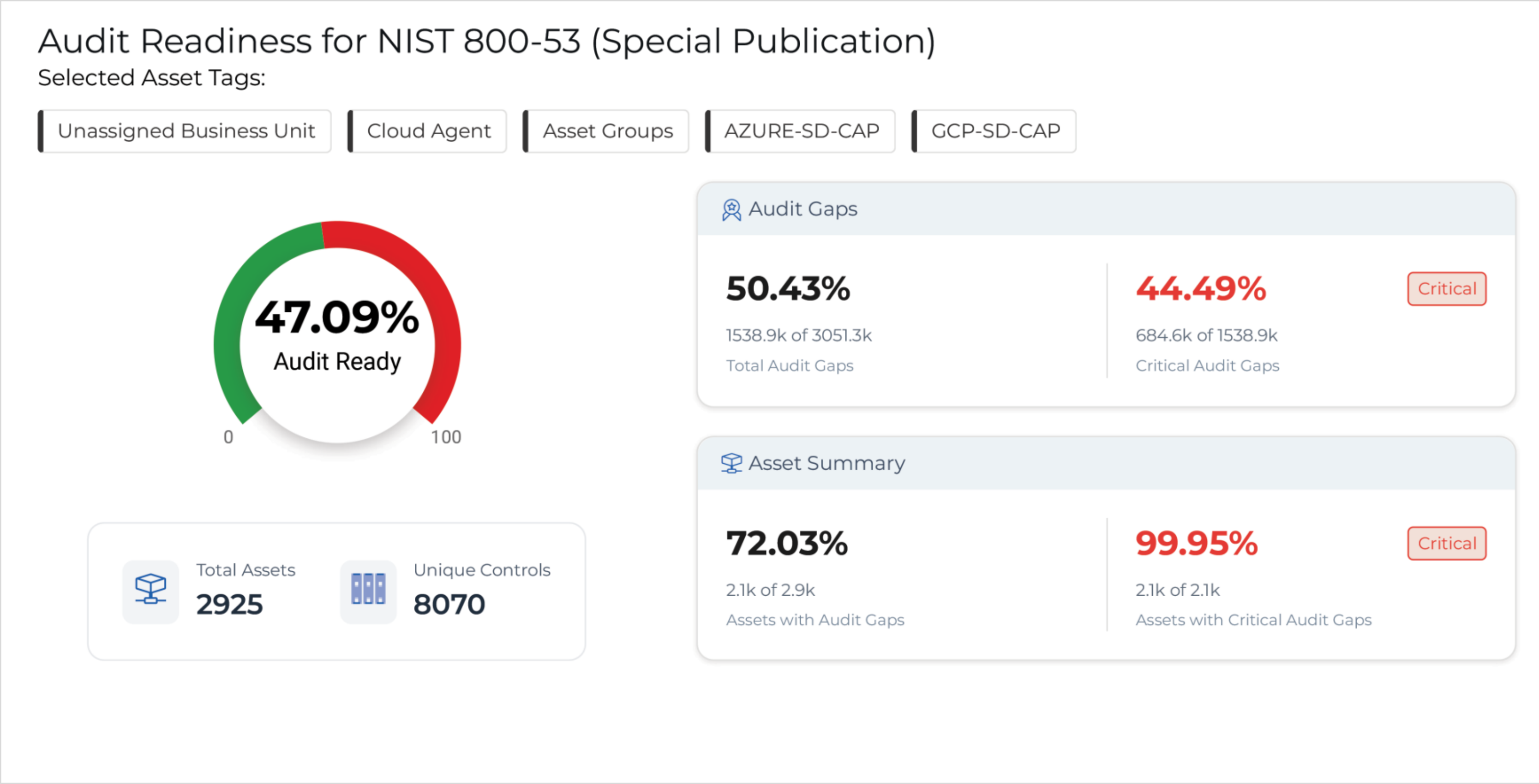
IT / Workstations / Servers

IOT

External Devices

Compliance Assessment and Reporting

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



Audit Readiness for NIST 800-53 (Special Publication)

Selected Asset Tags:

Unassigned Business Unit | Cloud Agent | Asset Groups | AZURE-SD-CAP | GCP-SD-CAP

Total Assets
2925

Unique Controls
8070

Audit Gaps

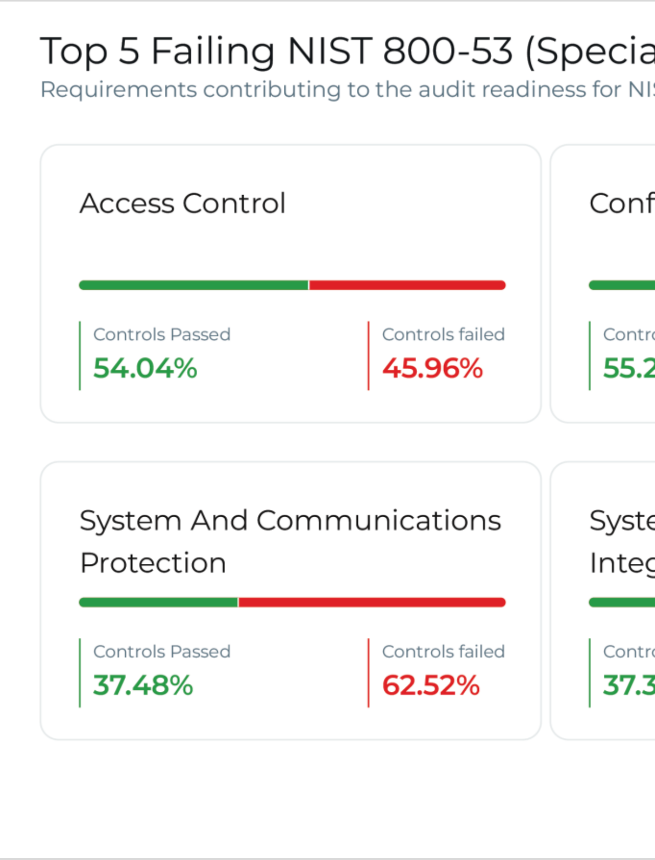
50.43%
1538.9k of 3051.3k
Total Audit Gaps

44.49% Critical
684.6k of 1538.9k
Critical Audit Gaps

Asset Summary

72.03%
2.1k of 2.9k
Assets with Audit Gaps

99.95% Critical
2.1k of 2.1k
Assets with Critical Audit Gaps



Top 5 Failing NIST 800-53 (Specia

Requirements contributing to the audit readiness for NI

Access Control

Controls Passed
54.04%

Controls failed
45.96%

Conf

Contr
55.2

System And Communications Protection

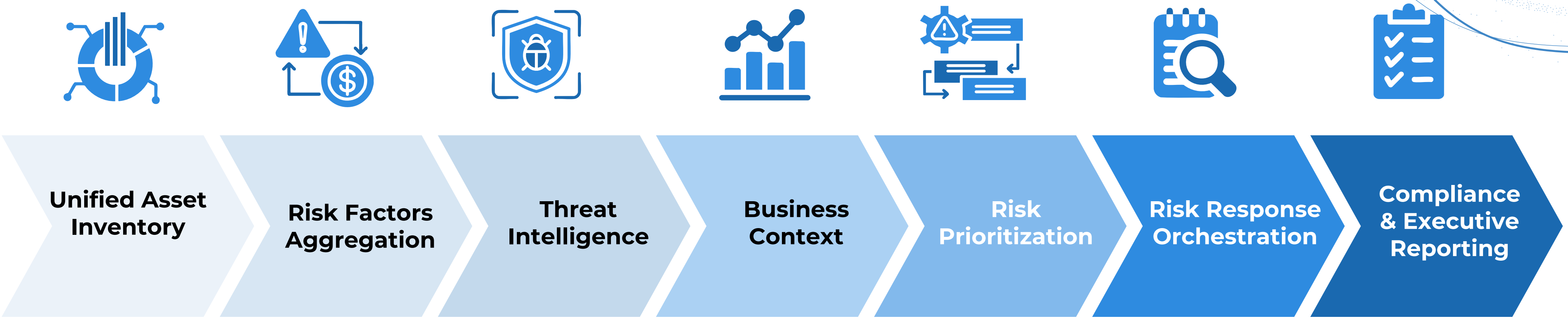
Controls Passed
37.48%

Controls failed
62.52%

Syste Integ

Contro
37.3

Risk enrichment on top of your exposure data



Unified Asset Inventory

Risk Factors Aggregation

Threat Intelligence

Business Context

Risk Prioritization

Risk Response Orchestration

Compliance & Executive Reporting

Which assets are unknown risk surface

Which Assets mapped to my critical business app?

Which Exposures (Vulnerabilities, Misconfigs, Identities) are causing the most risk

TruLens

Whats my risk to the trending threats in my industry?

Cyber Risk Rationalizer

What's the impact of TruRisk on business?

TruConfirm

Which exposures are validated as exploitable?

Eliminate/Remediate

Remediate exposures – patch or Mitigate or custom workaround

Audit-ready report

Mapped to 100+ mandates to get compliance friendly report

Qualys.

ROCon 25

The Risk Operations Conference

APAC

Thank You