Qualys ROCon 26
The Risk Operations Conference
EMEA

Cyber Risk Management in the AI Era

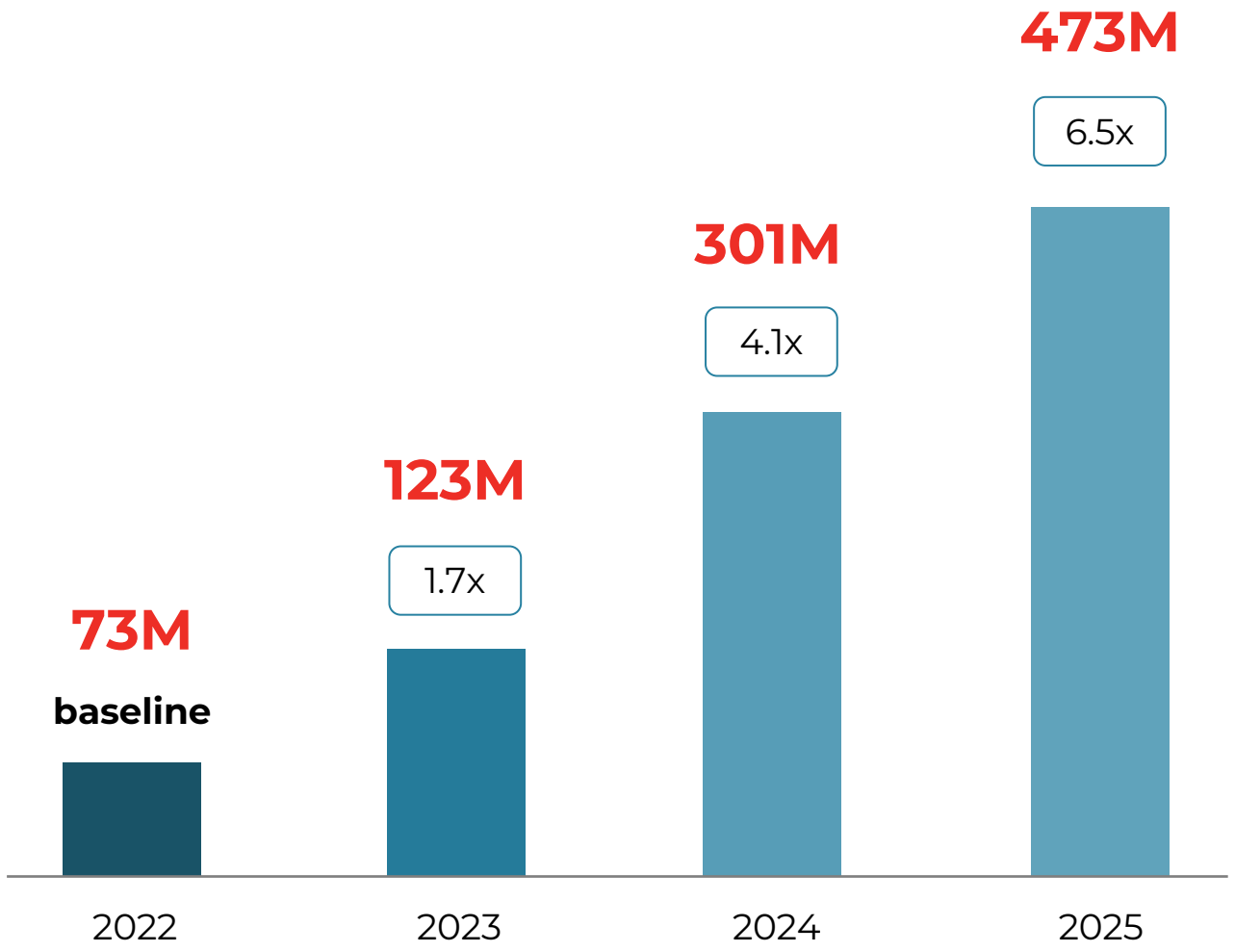


Sumedh Thakar
President & CEO, Qualys Inc



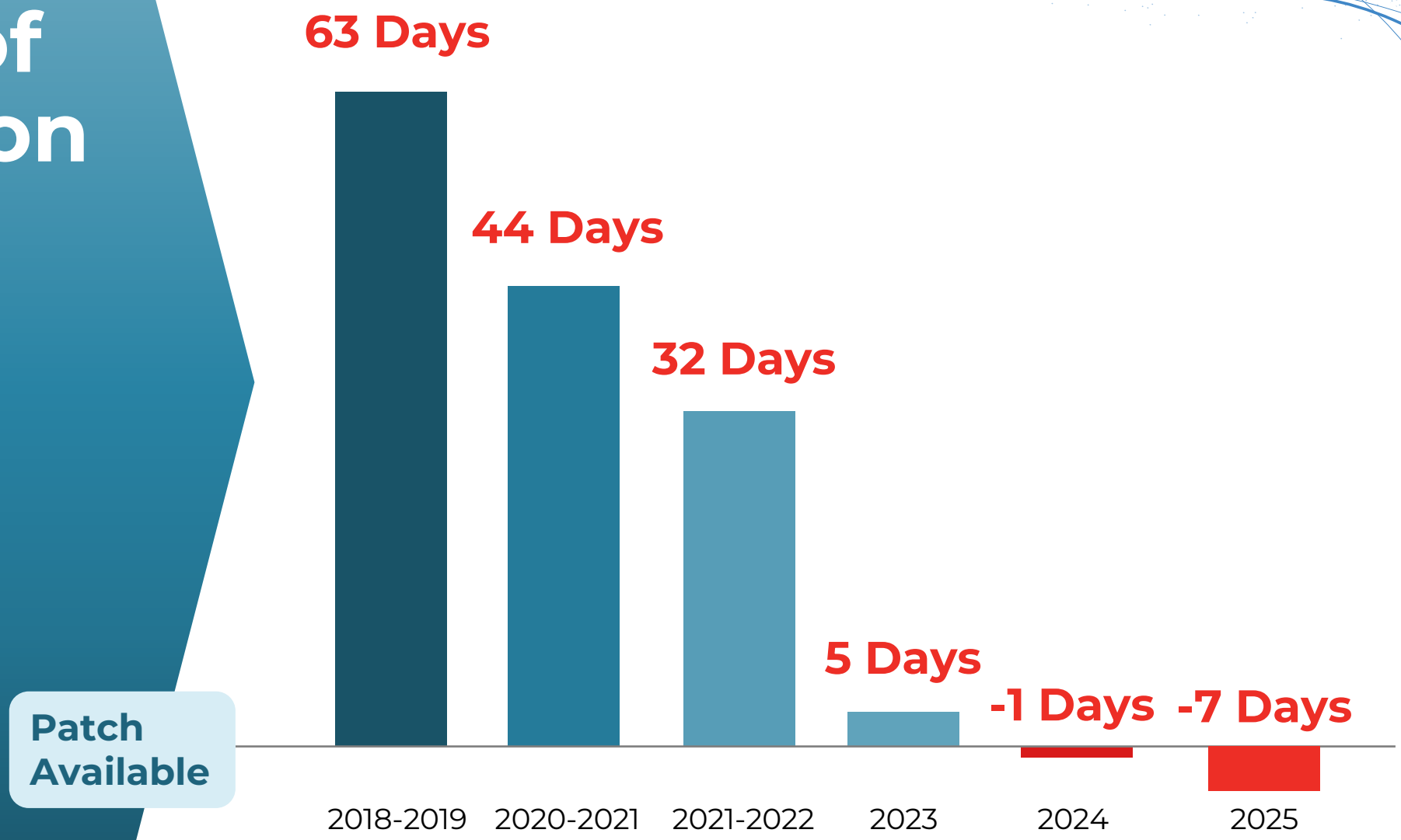
The CISA KEV Volume Explosion

6.5x	Growth in 4 years
+400M	Additional events managed
1.57x	Jump from 2024 alone



Vulnerability events closed per year across 10,000+ organizations.
Research by Qualys TRU.

Shrinking Window of Exploitation



Source: Google Threat Intelligence Group

Key Metric: Exposure Window

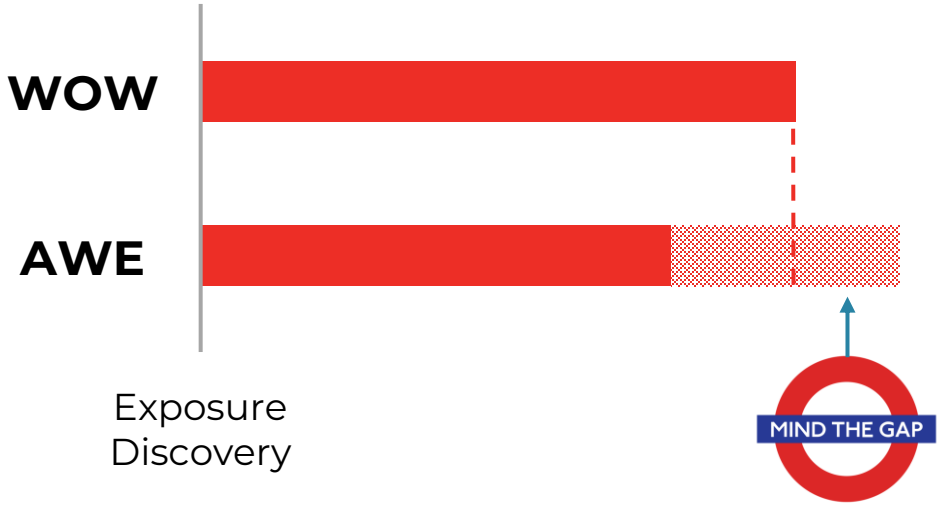
WOW

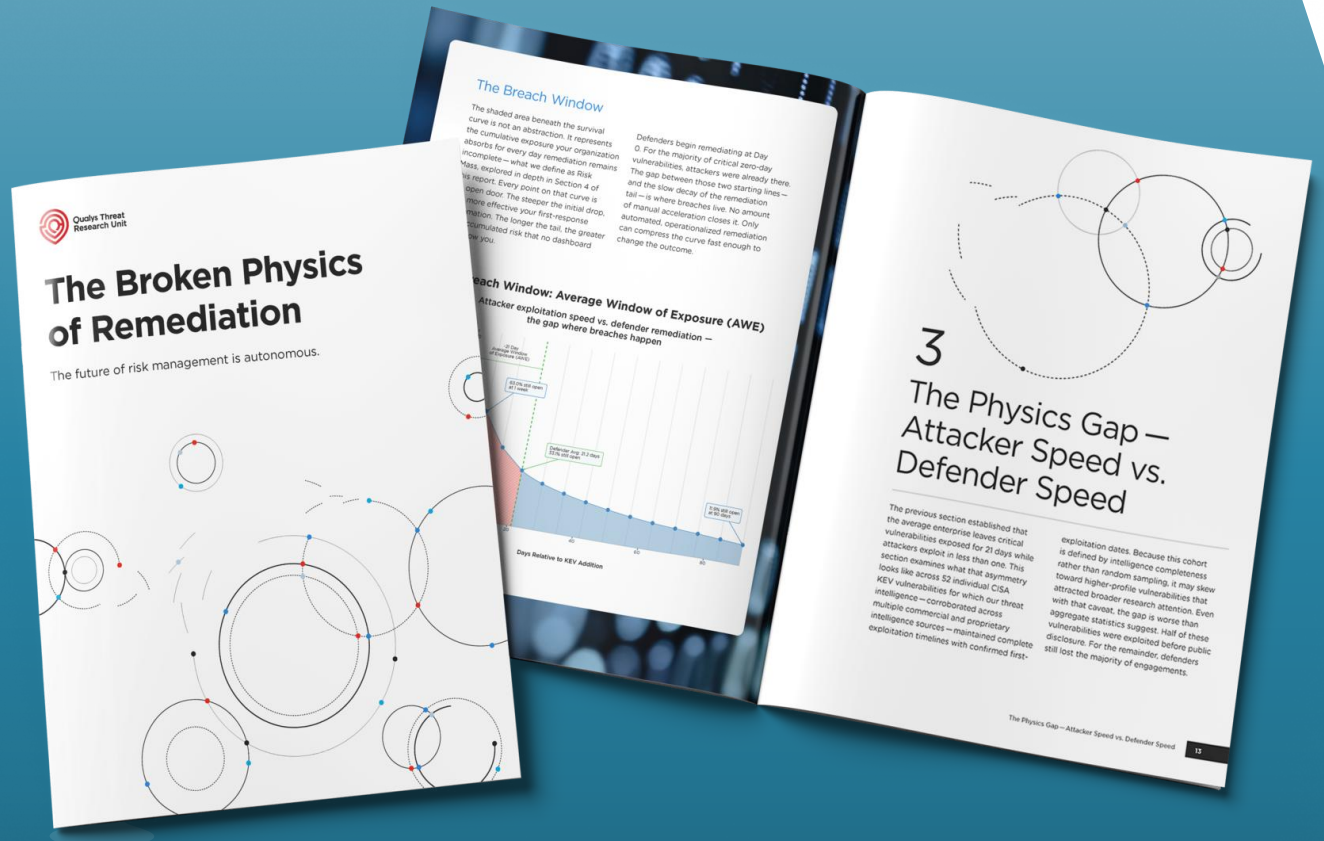
Window of Weaponization

AWE

Average Window of Exposure

To Prevention Exploitation AWE needs to be smaller than WOW

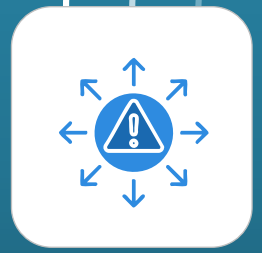




Largest study of its kind based on one billion CISA KEV Remediation records spanning 10,000 organizations over four years

Download the report

The AWE is Already Aweful



01

The Physics Gap

88% of weaponized vulnerabilities were patched slower than they were exploited. AI multiplies this.

02

The Wasted Head Start

Even with **70+** day head starts, organizations took **178–242** days to patch. AI will now hunt these long-tail assets at scale.

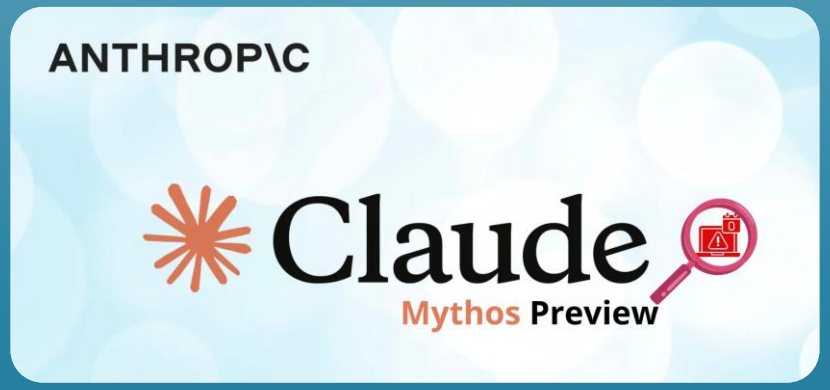
03

The Perimeter Problem

The devices that enforce hardening are themselves the hardest to patch. The hardening layer is the weakest link.

Analysis of 52 high-profile weaponized CISA KEV vulnerabilities with confirmed exploitation timelines — across 10,000+ organizations and four years of data

The Coming AI Tsunami of **Vulnerabilities**



- Frontier model from Anthropic, other Frontier models not far behind
- Good in identifying and exploiting new vulnerabilities. Found 1000s of zero days
- Over 99% of the vulnerabilities they found have not yet been patched

Project Glasswing

Project to harden widely deployed software and the most common source of exploited vulnerabilities

43% of CISA KEVs come from Glasswing launch partners

PROXYSHELL · MICROSOFT EXCHANGE · AUGUST 2021

Patches existed.
Thousands of servers fell anyway.

Three separate Exchange vulnerabilities — each patched the day it was disclosed — were chained into one of the most destructive **unauthenticated RCE** exploits of the decade. This is how the chain worked, and how **any one patch** would have broken it.

Patch one link, break the chain.

ProxyShell · Microsoft Exchange · 2021

Three CVEs. One takeover.

Patch any single link and the chain collapses.

Three independent Exchange bugs. Individually serious, but **none grants system takeover on its own**.

CVE #1

ENTRY POINT

CVE-2021-34473

Pre-auth path confusion

AutoDiscover URL parser flaw strips auth checks. Frontend forwards request to backend as **NT AUTHORITY\SYSTEM** .

CVSS 9.1 CRITICAL

QVSS 10 CRITICAL

- CISA KEV
- Associated with ransomware

CVE #2

PRIVILEGE ESCALATION

CVE-2021-34523

PowerShell backend privilege escalation

SID injection in HTTP headers impersonates an **Exchange Admin** , unlocking the Remote PowerShell interface.

CVSS 9.0 CRITICAL

QVSS 10 CRITICAL

- CISA KEV
- Associated with ransomware

CVE #3

REMOTE CODE EXECUTION

CVE-2021-31207

Arbitrary file write via mailbox export

New-MailboxExportRequest writes an **.aspx** webshell to a web-accessible path. Browsing it executes code as SYSTEM.

CVSS 6.6 MEDIUM

QVSS 9.5 MEDIUM

- CISA KEV
- Associated with ransomware

THE SETUP

Three Microsoft Exchange flaws disclosed in 2021. Each patched the day it was released. None is a full compromise in isolation.

Patch one link, break the chain.

ProxyShell · Microsoft Exchange · 2021

Three CVEs. One takeover.

Patch any single link and the chain collapses.

Step 1 — Entry. CVE-2021-34473 bypasses the frontend auth and lands inside the backend as SYSTEM.

CVE #1

ENTRY POINT

CVE-2021-34473

Pre-auth path confusion

AutoDiscover URL parser flaw strips auth checks. Frontend forwards request to backend as **NT AUTHORITY\SYSTEM** .

CVSS 9.1 CRITICAL

QVSS 10 CRITICAL

- CISA KEV
- Associated with ransomware

CVE #2

PRIVILEGE ESCALATION

CVE-2021-34523

PowerShell backend privilege escalation

SID injection in HTTP headers impersonates an **Exchange Admin** , unlocking the Remote PowerShell interface.

CVSS 9.0 CRITICAL

QVSS 10 CRITICAL

- CISA KEV
- Associated with ransomware

CVE #3

REMOTE CODE EXECUTION

CVE-2021-31207

Arbitrary file write via mailbox export

New-MailboxExportRequest writes an **.aspx** webshell to a web-accessible path. Browsing it executes code as SYSTEM.

CVSS 6.6 MEDIUM

QVSS 9.5 MEDIUM

- CISA KEV
- Associated with ransomware

STEP 1 · ENTRY POINT

A crafted AutoDiscover URL confuses the frontend parser. Authentication is stripped; the request is forwarded straight to the backend, running as **NT AUTHORITY\SYSTEM.**

OUTCOME

Unauthenticated backend access

Patch one link, break the chain.

ProxyShell · Microsoft Exchange · 2021

Three CVEs. One takeover.
Patch any single link and the chain collapses.

Step 2 — Escalate. CVE-2021-34523 downgrades SYSTEM into a valid **Exchange Admin** token.

CVE #1

ENTRY POINT

CVE-2021-34473

Pre-auth path confusion

AutoDiscover URL parser flaw strips auth checks. Frontend forwards request to backend as **NT AUTHORITY\SYSTEM** .

CVSS 9.1 CRITICAL

QVSS 10 CRITICAL

- CISA KEV
- Associated with ransomware

GRANTS SYSTEM CONTEXT



CVE #2

PRIVILEGE ESCALATION

CVE-2021-34523

PowerShell backend privilege escalation

SID injection in HTTP headers impersonates an **Exchange Admin** , unlocking the Remote PowerShell interface.

CVSS 9.0 CRITICAL

QVSS 10 CRITICAL

- CISA KEV
- Associated with ransomware

CVE #3

REMOTE CODE EXECUTION

CVE-2021-31207

Arbitrary file write via mailbox export

New-MailboxExportRequest writes an **.aspx** webshell to a web-accessible path. Browsing it executes code as SYSTEM.

CVSS 6.6 MEDIUM

QVSS 9.5 MEDIUM

- CISA KEV
- Associated with ransomware

STEP 2 · PRIVILEGE ESCALATION

SYSTEM can't run admin mailbox commands. By injecting a chosen SID into HTTP headers, the attacker impersonates an Exchange Administrator and unlocks the Remote PowerShell interface.

OUTCOME

Exchange Admin context

Patch one link, break the chain.

ProxyShell · Microsoft Exchange · 2021

Three CVEs. One takeover.

Patch any single link and the chain collapses.

Step 3 — Takeover. CVE-2021-31207 drops an **.aspx webshell.**

CVE #1

ENTRY POINT

CVE-2021-34473

Pre-auth path confusion

AutoDiscover URL parser flaw strips auth checks. Frontend forwards request to backend as **NT AUTHORITY\SYSTEM** .

CVSS 9.1 CRITICAL

QVSS 10 CRITICAL

- CISA KEV
- Associated with ransomware

CVE RELEASED
Jul 13, 2021

PATCH AVAILABLE
Same day

GRANTS SYSTEM CONTEXT



CVE #2

PRIVILEGE ESCALATION

CVE-2021-34523

PowerShell backend privilege escalation

SID injection in HTTP headers impersonates an **Exchange Admin** , unlocking the Remote PowerShell interface.

CVSS 9.0 CRITICAL

QVSS 10 CRITICAL

- CISA KEV
- Associated with ransomware

CVE RELEASED
Jul 13, 2021

PATCH AVAILABLE
Same day

ENABLES ADMIN POWERSHELL



CVE #3

REMOTE CODE EXECUTION

CVE-2021-31207

Arbitrary file write via mailbox export

New-MailboxExportRequest writes an **.aspx** webshell to a web-accessible path. Browsing it executes code as SYSTEM.

CVSS 6.6 MEDIUM

QVSS 9.5 MEDIUM

- CISA KEV
- Associated with ransomware

CVE RELEASED
May 11, 2021

PATCH AVAILABLE
Same day

COMPROMISE — WITH PATCHES ALREADY SHIPPED

With admin PowerShell, the attacker abuses New-MailboxExportRequest to write an **.aspx** webshell into a web-accessible directory — **unauthenticated RCE as SYSTEM.**

OUTCOME

Remote code execution

Patch one link, break the chain.

ProxyShell · Microsoft Exchange · 2021

Patch **any single link** and the entire takeover chain collapses.

Three CVEs. One takeover.

Patch any single link and the chain collapses.

CVE #1

ENTRY POINT

CVE-2021-34473

Pre-auth path confusion

AutoDiscover URL parser flaw strips auth checks. Frontend forwards request to backend as **NT AUTHORITY\SYSTEM** .

CVSS 9.1 CRITICAL

QVSS 10 CRITICAL

- CISA KEV
- Associated with ransomware

CVE RELEASED	PATCH AVAILABLE
Jul 13, 2021	Same day

GRANTS SYSTEM CONTEXT



CVE #2

PRIVILEGE ESCALATION

CVE-2021-34523

PowerShell backend privilege escalation

SID injection in HTTP headers impersonates an **Exchange Admin** , unlocking the Remote PowerShell interface.

CVSS 9.0 CRITICAL

QVSS 10 CRITICAL

- CISA KEV
- Associated with ransomware

CVE RELEASED	PATCH AVAILABLE
Jul 13, 2021	Same day

ENABLES ADMIN POWERSHELL



CVE #3

REMOTE CODE EXECUTION

CVE-2021-31207

Arbitrary file write via mailbox export

New-MailboxExportRequest writes an **.aspx** webshell to a web-accessible path. Browsing it executes code as SYSTEM.

CVSS 6.6 MEDIUM

QVSS 9.5 MEDIUM

- CISA KEV
- Associated with ransomware

CVE RELEASED	PATCH AVAILABLE
May 11, 2021	Same day

CHAIN BROKEN

Apply the patch for **any one** of these three CVEs and ProxyShell cannot complete. No entry, or no escalation, or no file-write primitive — means no webshell, no RCE, no compromise.

OUTCOME

Chain broken

THE DEFENDER'S TAKEAWAY

Patch any single link and the entire chain collapses.

Every CVE in this chain had a patch available the day it was disclosed.
Closing **any one** of them stops ProxyShell cold.

The Path Forward

Need:
Speed of remediation needs to match speed of detection.



The Solution to Keep
AWE Smaller than WOW

Autonomous Remediation



Autonomous Remediation Needs:

- ✓ Hyper Prioritization
- ✓ Operational Resilience
- ✓ Agentic AI



If everything is critical, nothing is.

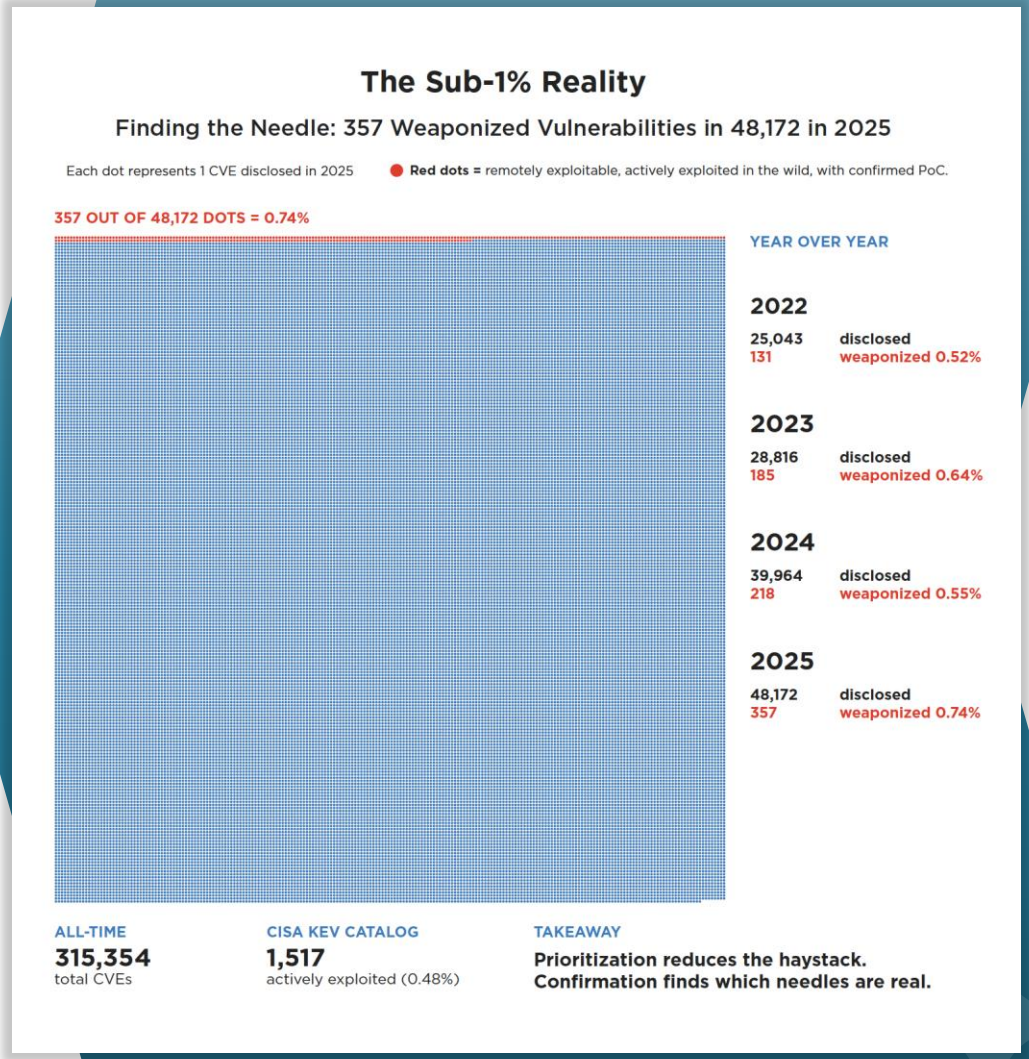
Too many **threats.**
Too many **patches.**
Too many **alerts.**
Too many **vulnerabilities.**



The Case for Hyper Prioritization

- Most orgs are burning cycles on theoretical risk.
- Even within the 0.74%, not all are exploitable in your environment.

P.29 - The Filter — From Prioritization to Confirmation
The Broken Physics of Remediation, Research Report from Qualys TRU



Exploitable ≠ Exploitable

Less than 20% of the prioritized exposures are exploitable against compensating controls

Validating exploitability in your environment reduces remediations required

Confidence in Operational Resilience

- ✓ Patch reliability score
- ✓ Patchless remediations
- ✓ Deployment waves
- ✓ Ability to Rollback



Current State of Risk Management

Dashboard Tourism



It seems like today we're all playing **"Risk Whack-A-Mole"**



Budgets

aren’t growing at the same rate as the attack surface and pace of attacks

4-6%	Growth of security budgets over last 5 years
650%	Growth in volume of vulnerabilities in last 4 years
-7 Days	Mean-time-to-exploit (exploitation before patch availability)

Frontier models are going to make this worse with more vulnerabilities and faster exploits



From
Attack Surface Management
to
Risk Surface Management





Risk management

is about **reducing the likelihood of a major financial loss** to the business

Risk Factors

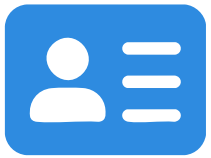
Vulnerabilities



Misconfiguration

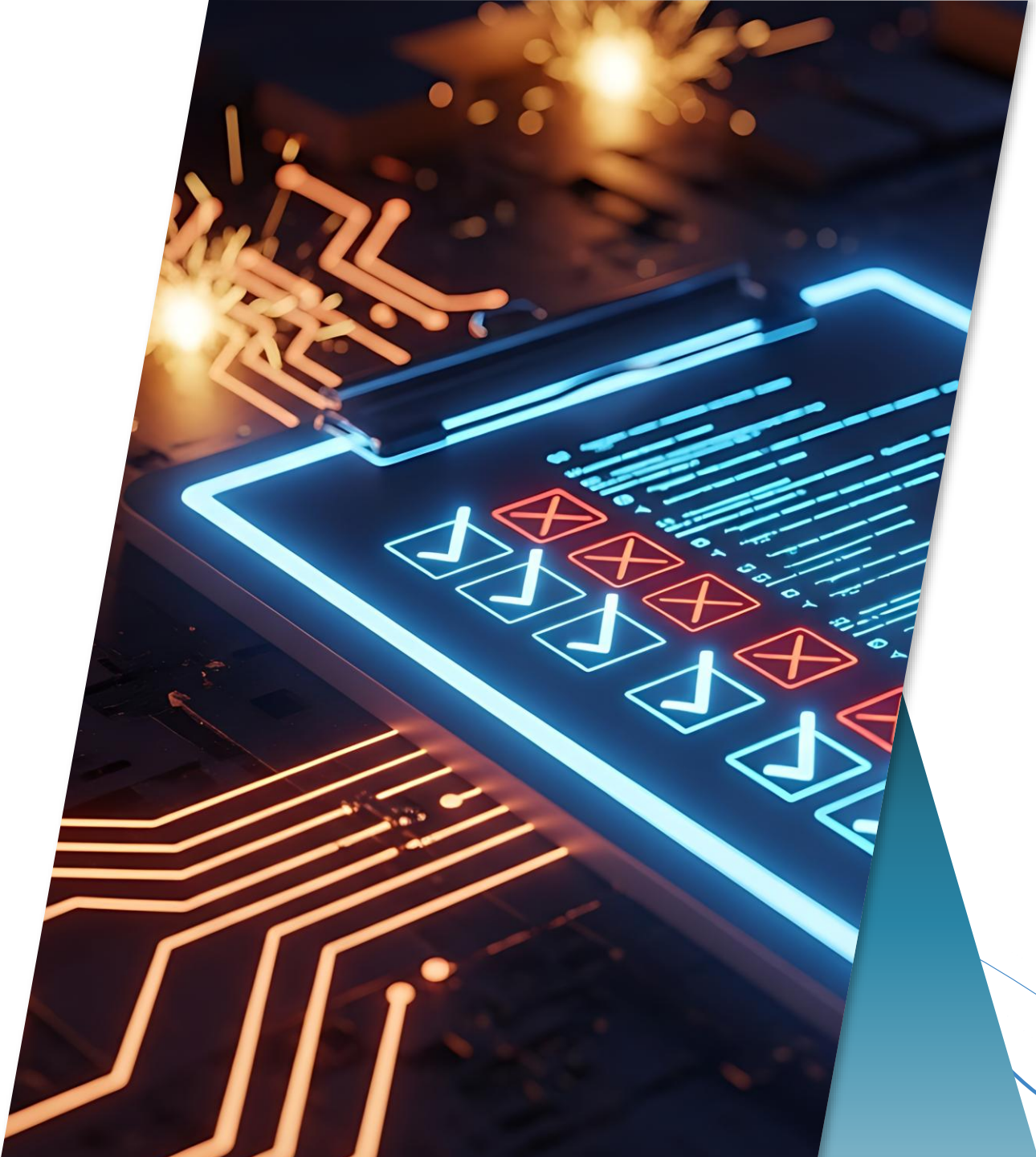


Identities



LLMs & Agentic AI





Need for an **operationalized process** for cyber risk management

Introducing the

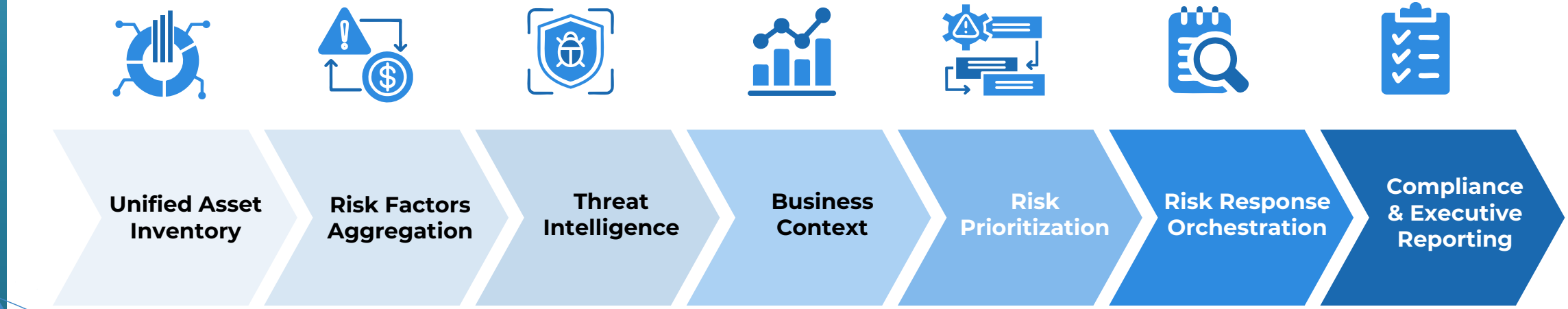
ROC

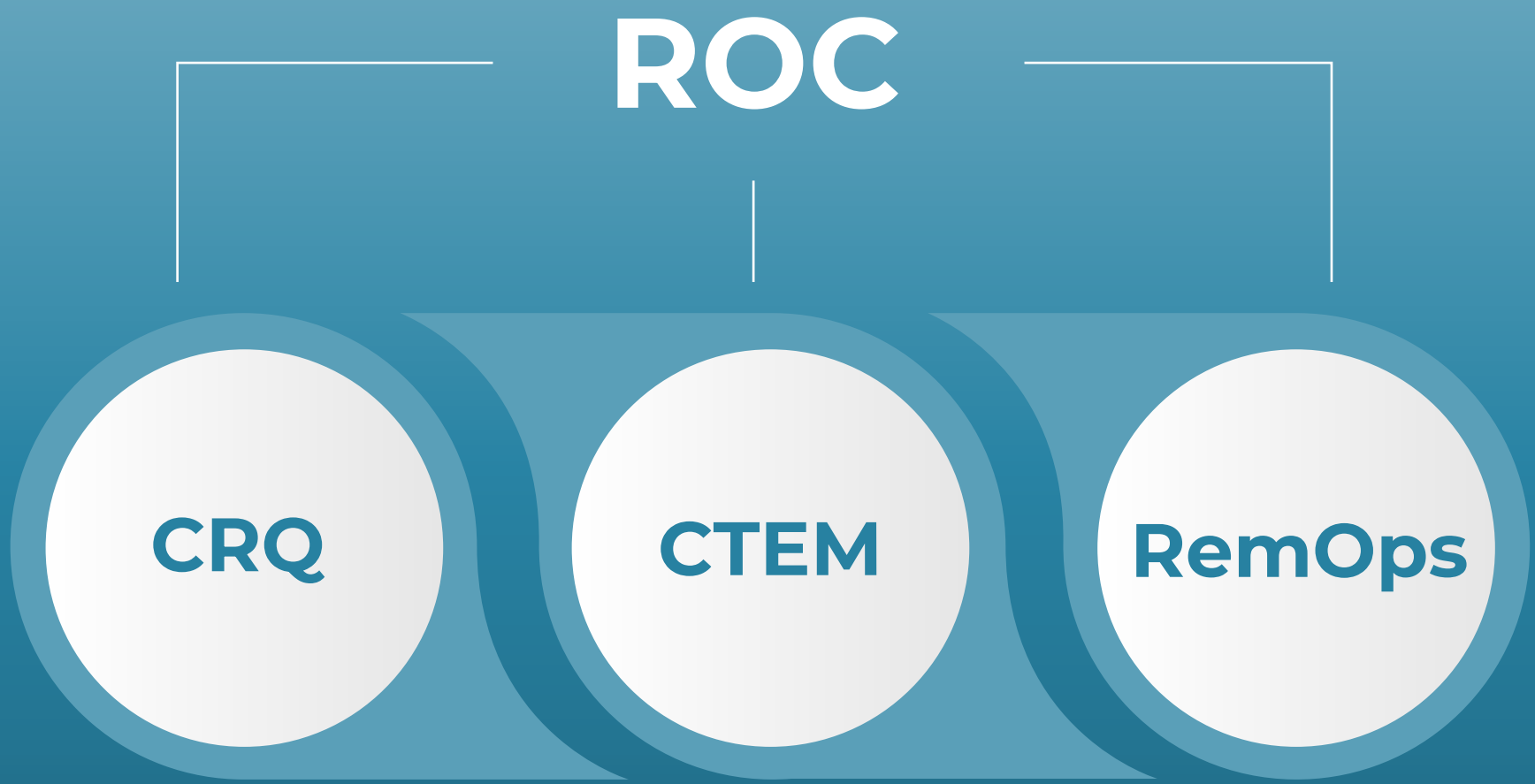
Risk Operations Center



The Risk Operations Center

Operationalize




ROC
CRQ
CTEM
RemOps



Cyber Fusion Center ROC

It integrates SOC and ROC functions to create an intelligence-driven, unified hub for proactive threat detection, response, and organizational resilience

The World's First
AI-ROC

QUALYS

Enterprise TruRisk Management



ETM: Powering The 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
- Application Security

THREAT INTELLIGENCE

BUSINESS CONTEXT

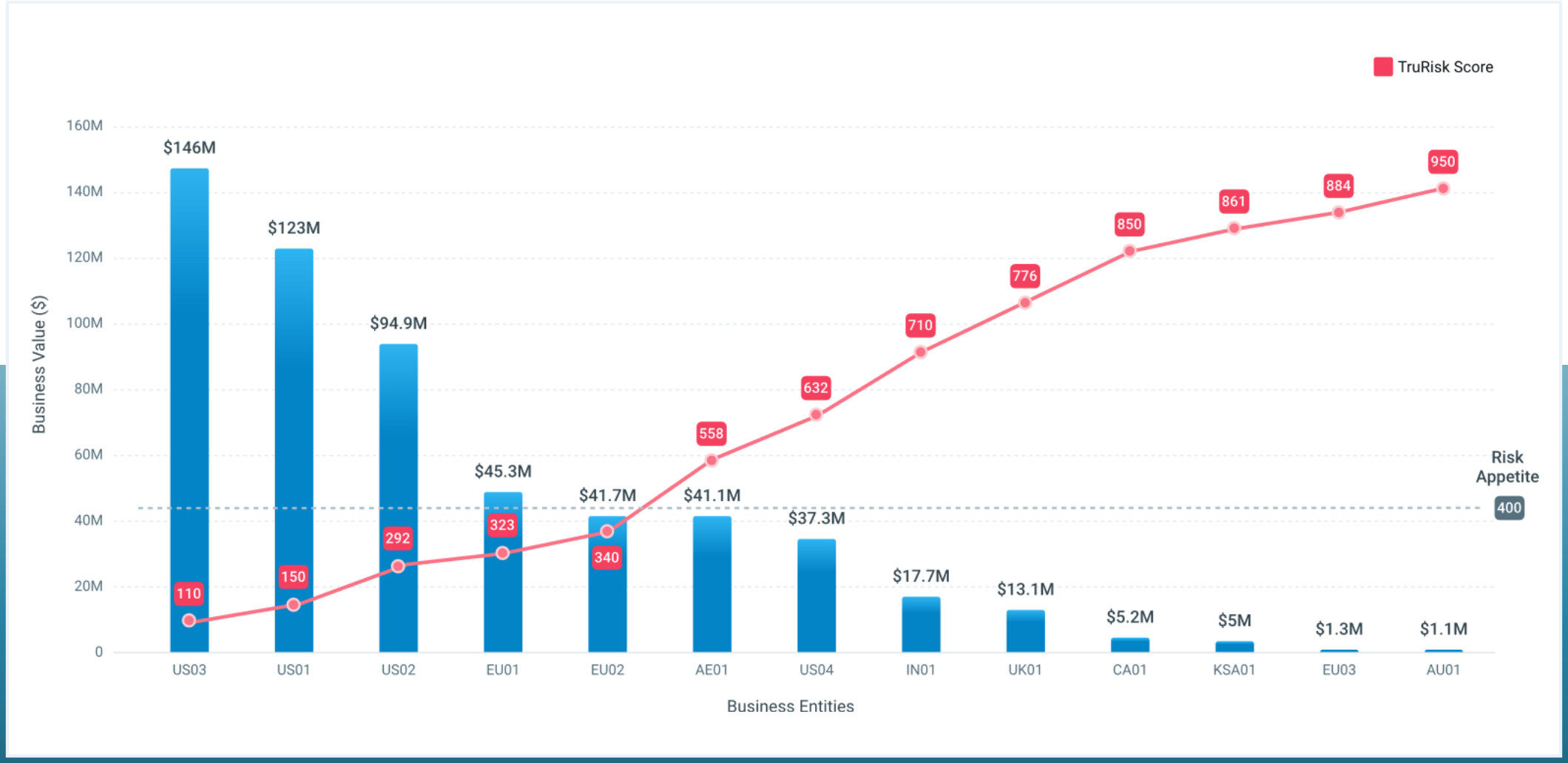
MEASURE | Quantify Cyber Risk in Business Terms

COMMUNICATE | Executive Reporting and Ticketing

ELIMINATE | Patch Mitigate & Track

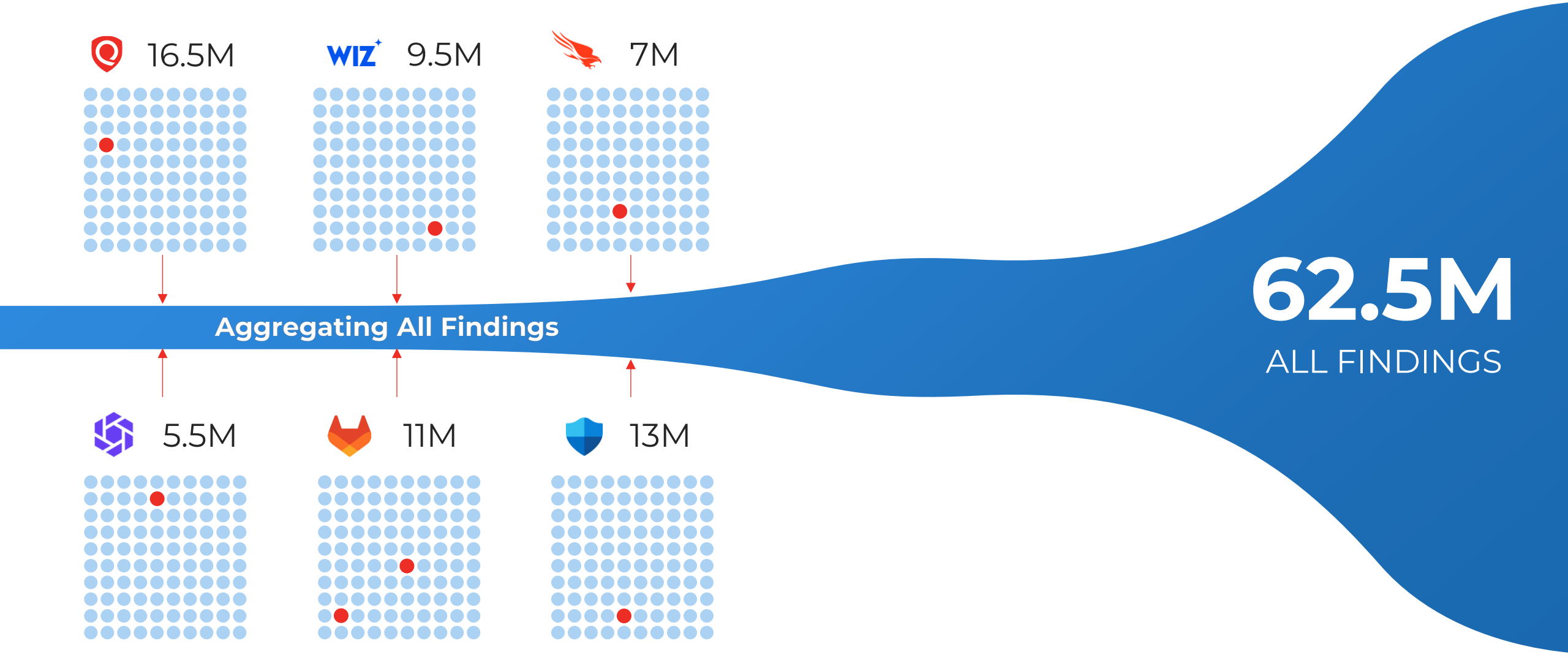
Your Partner in **Cyber Risk Management**

Aligns Cyber Risk to Business

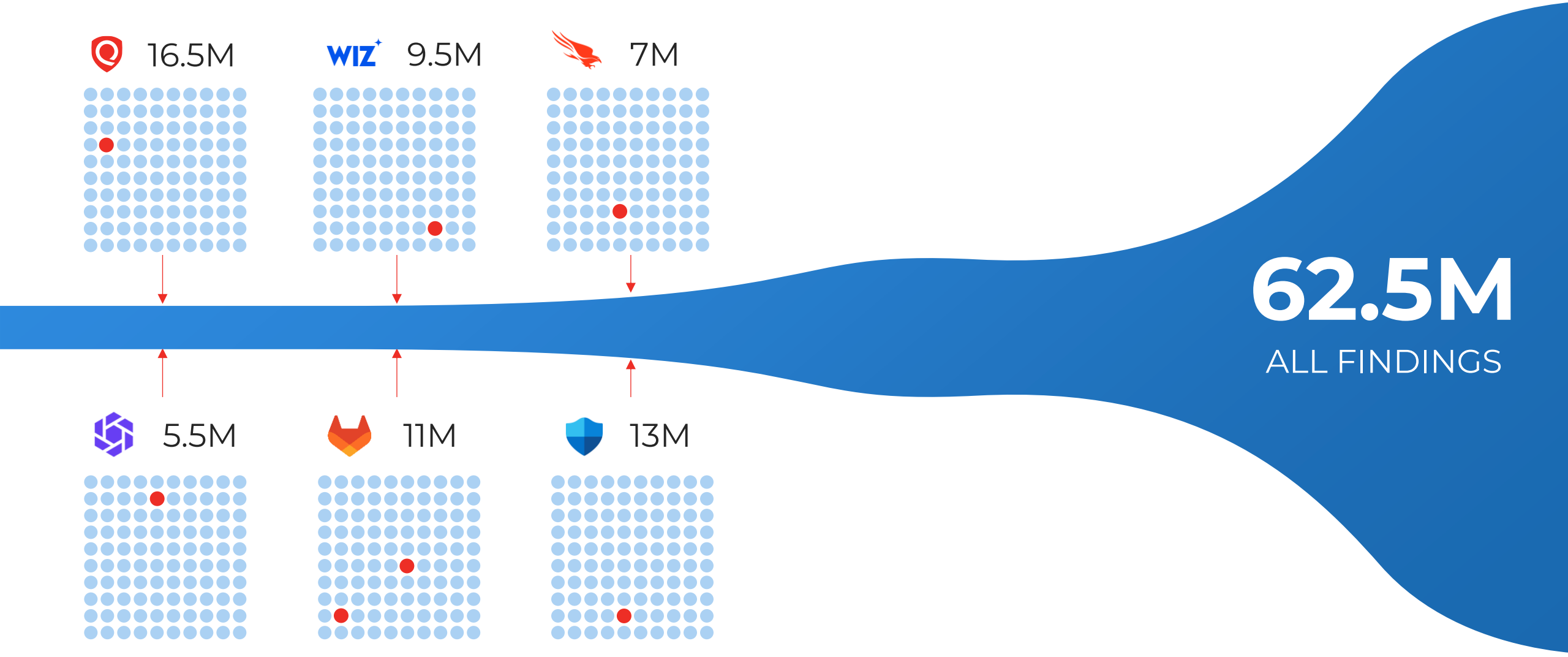


Bring **every exposure** from every security tool

Millions of Fragmented Exposures coming together

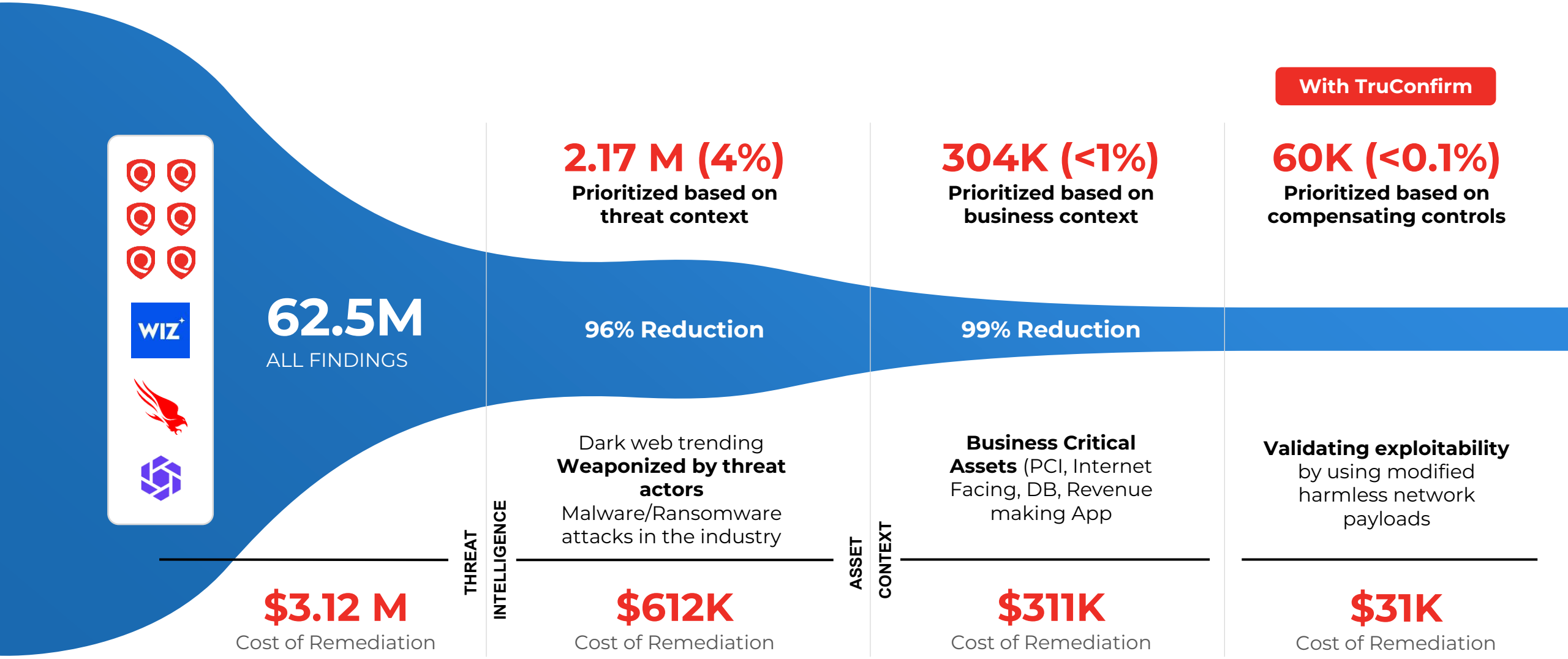


Millions of Fragmented Exposures coming together



Prioritizing Risk which Matters, Increases Efficiency

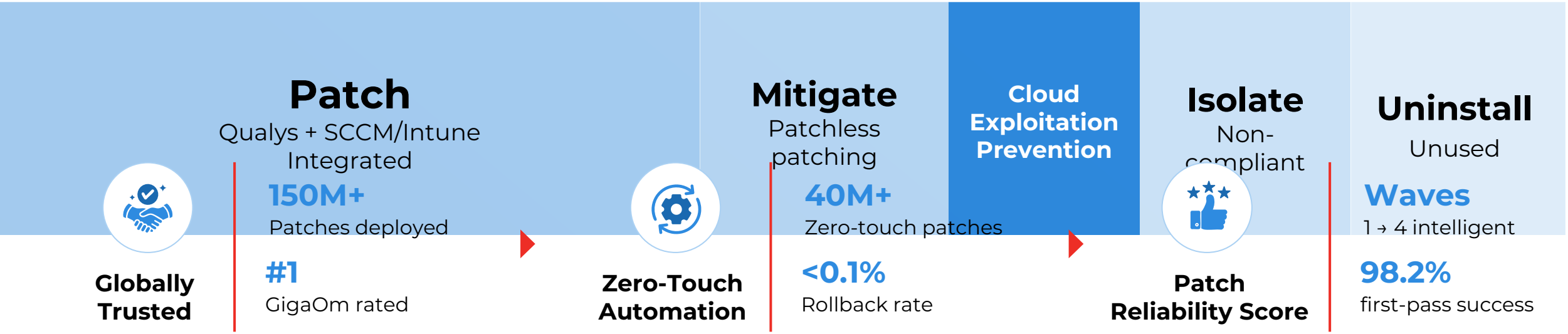
Risk Operations Center (ROC)



TruRisk Eliminate
Eliminate Risk With, or Without a Patch



TruRisk Eliminate
Eliminate Risk With, or Without a Patch



Qualys **Unveils Agentic AI** to Power the Industry's First **AI-ROC**



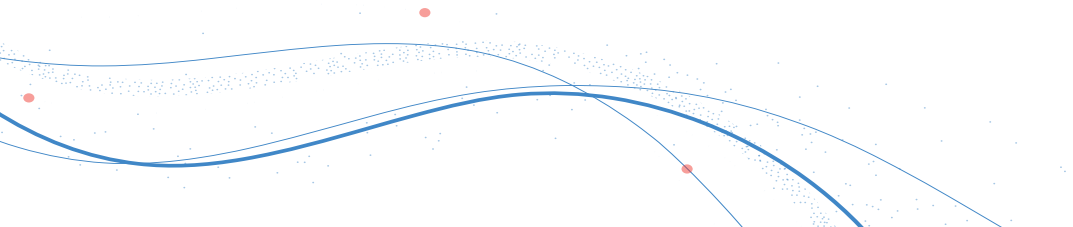
Need for AI Agents to:

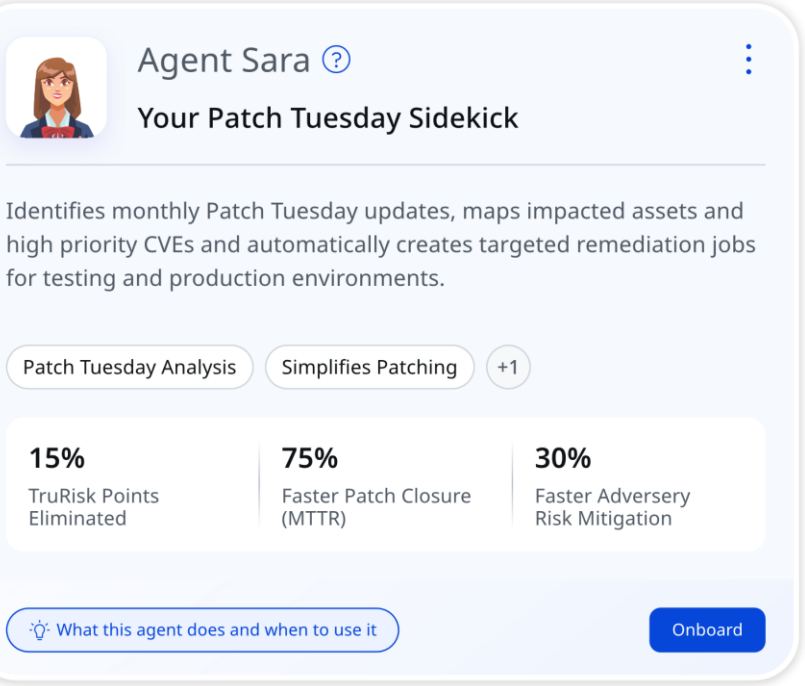
- ✓ Prioritize
- ✓ Validate exploitability
- ✓ Remediate
- ✓ Re-validate exploitability



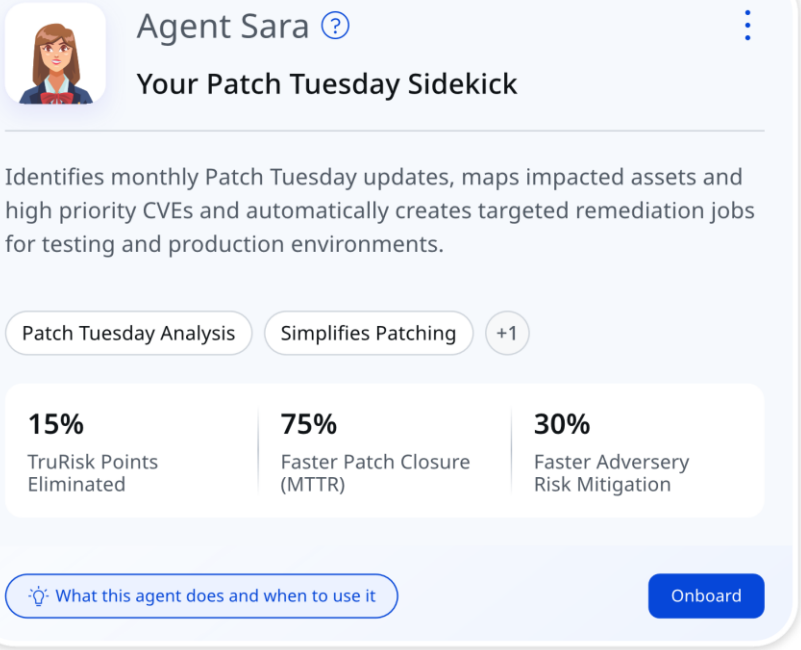
Qualys Marketplace of Cyber Risk Agents

Your skilled, digital workforce for autonomous risk management




Agent Sara
Your Patch Tuesday Sidekick
Identifies monthly Patch Tuesday updates, maps impacted assets and high priority CVEs and automatically creates targeted remediation jobs for testing and production environments.
Patch Tuesday Analysis
Simplifies Patching
+1
15%
TruRisk Points Eliminated
75%
Faster Patch Closure (MTTR)
30%
Faster Adversery Risk Mitigation
What this agent does and when to use it
Onboard


Current Posture
20.92K of 112K
Assets (18.67%)
45.73K of 410K
Finding Instances (11.15%)
59
Unique Vulnerabilities
6.1K
Critical Vulnerabilities
950
Critical
TruRisk Score
56D
MTTR



Plan

Patch Critical risk on Non-critical Assets

- **30%** critical risks on non-critical assets open **56 days**
- **85%** are patchable, with no reboot required

Action

Create Patch Job

Potential TruRisk Reduction 950 → 450

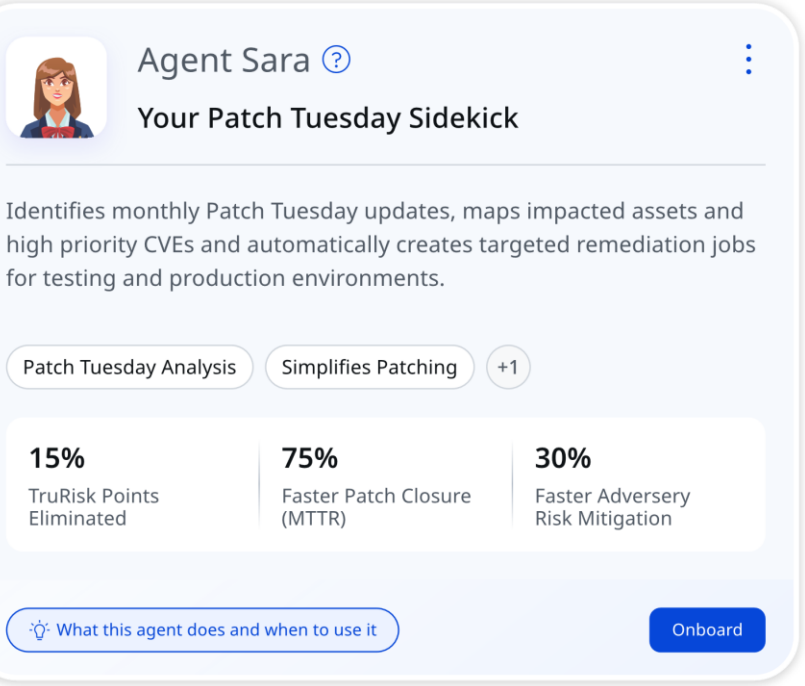
Mitigate the Risk on Critical Assets with No Patch

- **20%** remain unpatched **>180 days** on crown jewel servers
- **75%** are mitigable by applying **17 mitigations**

Action

Create Mitigation Job

Potential TruRisk Reduction 950 → 670



Task: Patch Critical Vulnerabilities on Non-Critical Assets

Outcome

TruRisk Score Impact

950 Critical → 302 Low

-47% Improvement

Reduced MTTR

56 Days → 27 Days

-48% Faster remediation

Patch Coverage

96% Patch Tuesday CVEs Remediated within 14 days

-60.7% Faster remediation

Residual Patch Tuesday Risk

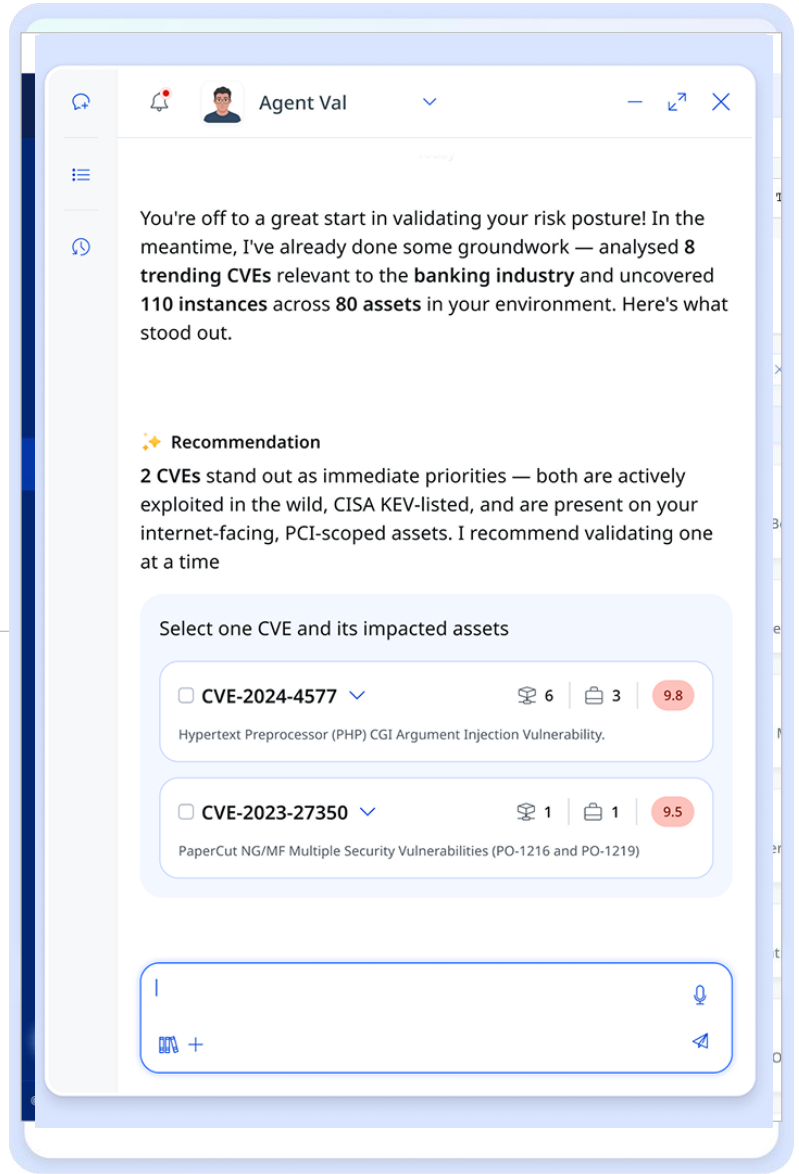
4% Remaining findings

Patch not available, Mitigation can be Applied

Introducing Agent Val

Industry's first agentic AI to run safe exploitability validation with ETM TruConfirm

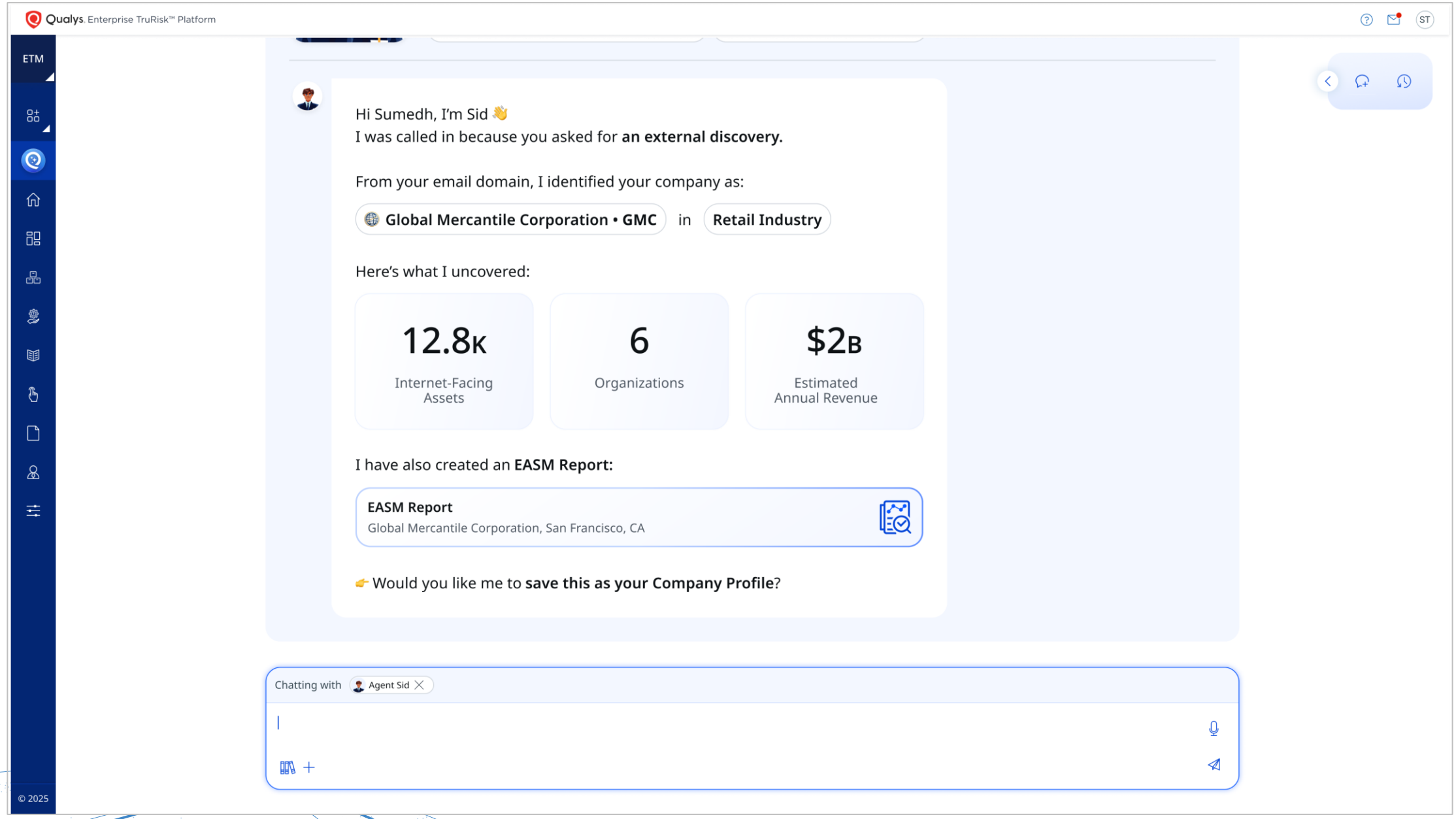
Continuous validation **based on your environmental and Risk Context** so exploitable exposures are never left untested.

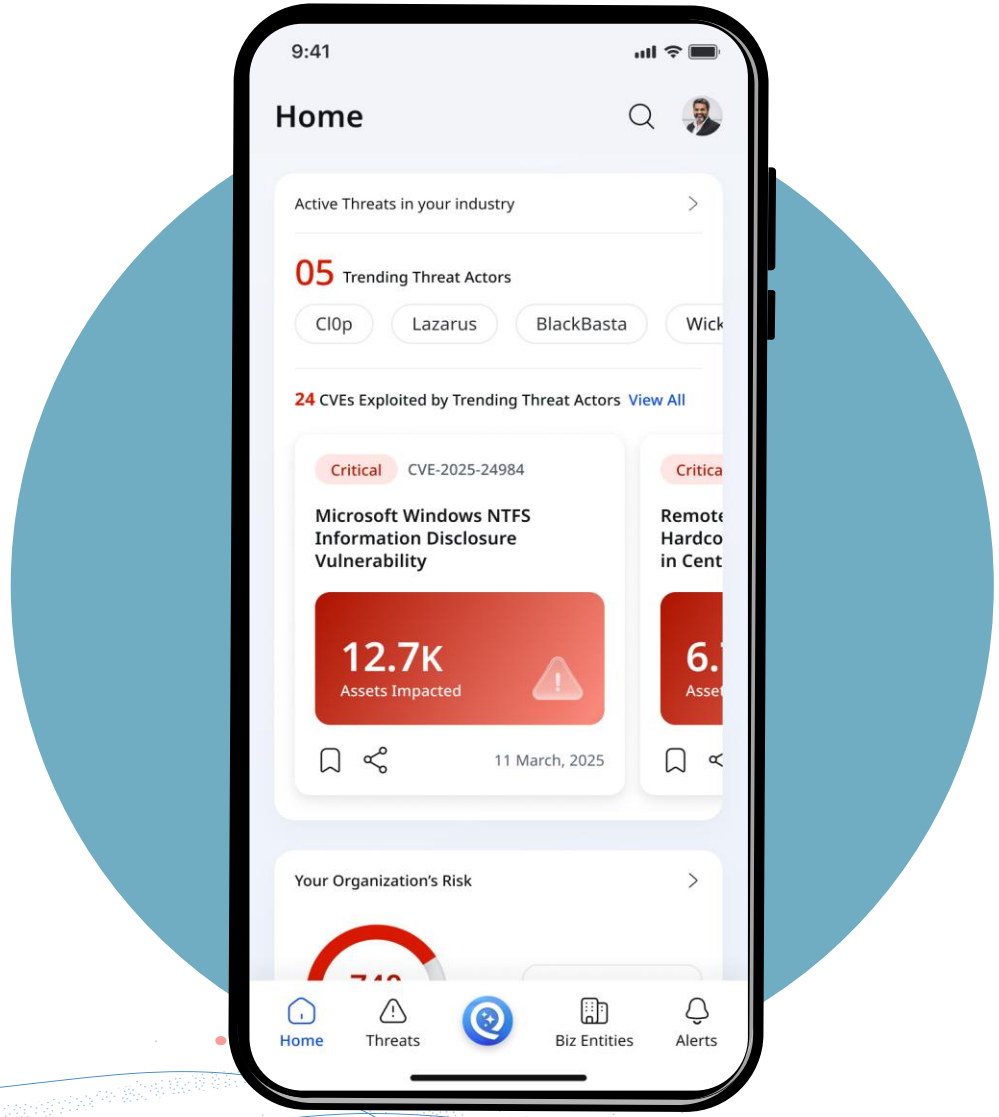


Cyber Risk Assistant

Helps users navigate and evaluate their risk posture with a NLQ




Qualys. Enterprise TruRisk™ Platform
ST
ETM
Hi Sumedh, I'm Sid 👋
I was called in because you asked for an external discovery.
From your email domain, I identified your company as:
Global Mercantile Corporation • GMC
in
Retail Industry
Here's what I uncovered:
12.8K
Internet-Facing Assets
6
Organizations
$2B
Estimated Annual Revenue
I have also created an EASM Report:
EASM Report
Global Mercantile Corporation, San Francisco, CA
👉 Would you like me to save this as your Company Profile?
Chatting with
Agent Sid
© 2025



Democratize

access to diverse security data

Operationalize Risk Management for the AI Era

01

Exposure Avalanche

Hyper Prioritization

Drive continuous resiliency through validation and autonomous workflows.

02

Manual Remediation is Dead

Autonomous Remediation

Need mechanism for autonomous validation & remediation of cyber risk driven from trust, confidence and a backup plan.

03

Attack Surface to Risk Surface

Cyber Risk Quantification

Start measuring cyber risk in terms of business impact and communicate in terms of business loss

Dashboard Tourism in 2028

Good Morning – Here's What Happened Overnight

New CVEs Disclosed
127
Frontier AI | 14 CISA KEV | 90 NVD

Match Your Environment
89
Across 2,847 assets

Confirmed Exploitable
34
TruConfirm validated at 02:00 AM

Agentic AI Remediated
28
Patches deployed automatically

AI Decision: Of 127 overnight CVEs, AI filtered to 89 matching your assets, validated 34 as exploitable, patched 28, mitigated 4, and isolated 2 internet-facing assets with no fix. 55 flagged CVEs were dismissed — not exploitable in your config.

What happened while you slept:

Action	Count	Status	JIRA	Detail
Patched	28	✓ **Complete**	28 tickets created	TruRisk Patch via Cloud Agent, rollback available
Mitigated	4	✓ **Complete**	4 tasks created	TRU scripts: registry mod (2), port block (1)
Isolated	2	⚠ **Active**	2 escalations	Internet-facing, no patch/mitigation — quarantined, awaiting vendor fix
Not exploitable	55	— **Dismissed**	—	Compensating controls, segmentation, or config prevent exploitation

Your morning queue: **6 items need human review** — 4 mitigations to verify and 2 isolated assets awaiting vendor patches. Everything else was handled automatically.

Show me the 6 items that need my attention


Qualys
ROCon 26
The Risk Operations Conference
EMEA