

# Journey from ASM to RSM

Cyber Risk Management  
in an AI-powered world



**Sumedh Thakar**  
President & CEO, Qualys Inc





---

An identity that carried our vision for 20+ years

---



is now



Qualys®

# ROCon<sup>®</sup> 25

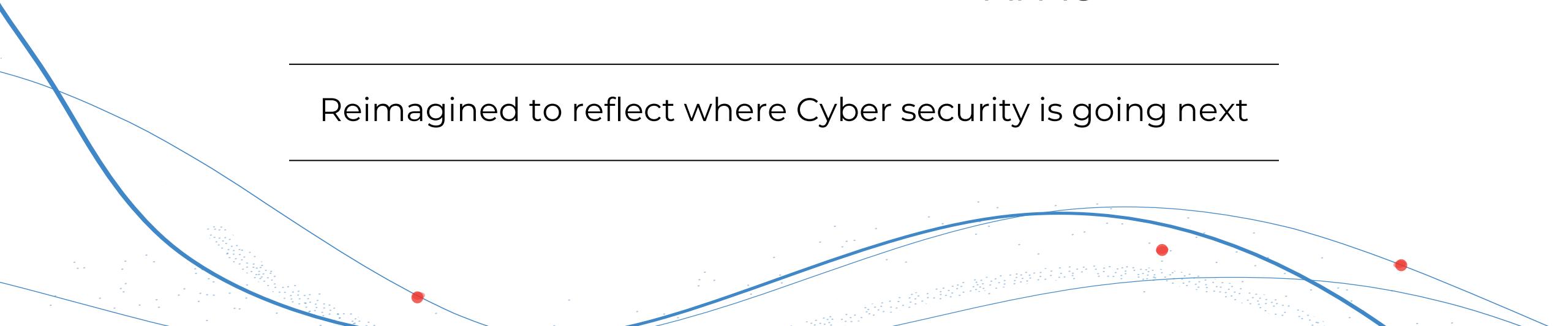
The Risk Operations Conference

---

APAC

---

Reimagined to reflect where Cyber security is going next



# Attack Surface Management

---



# Risk Surface Management

---



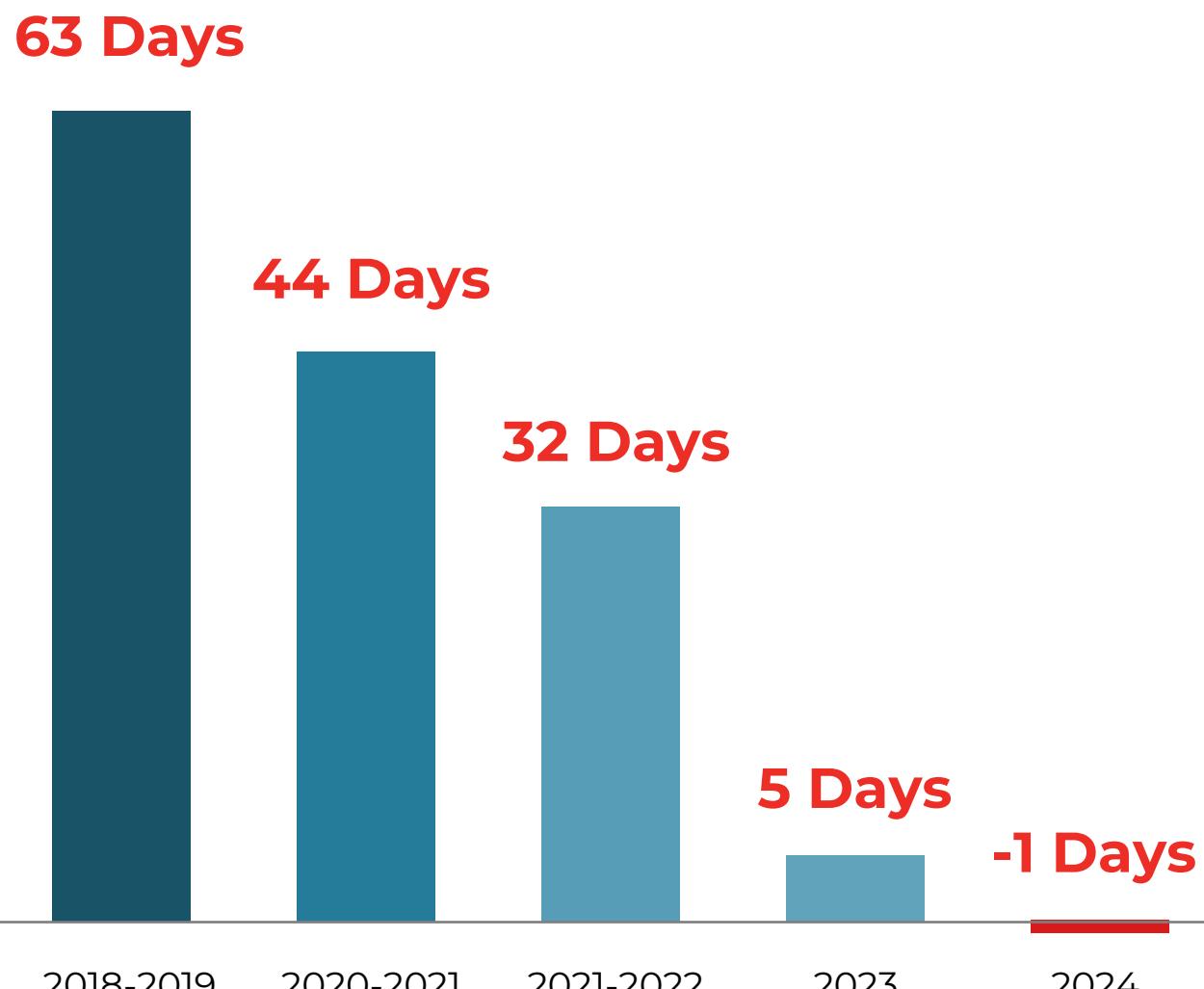
# Attack Surface is expanding and so is the Alert Surface



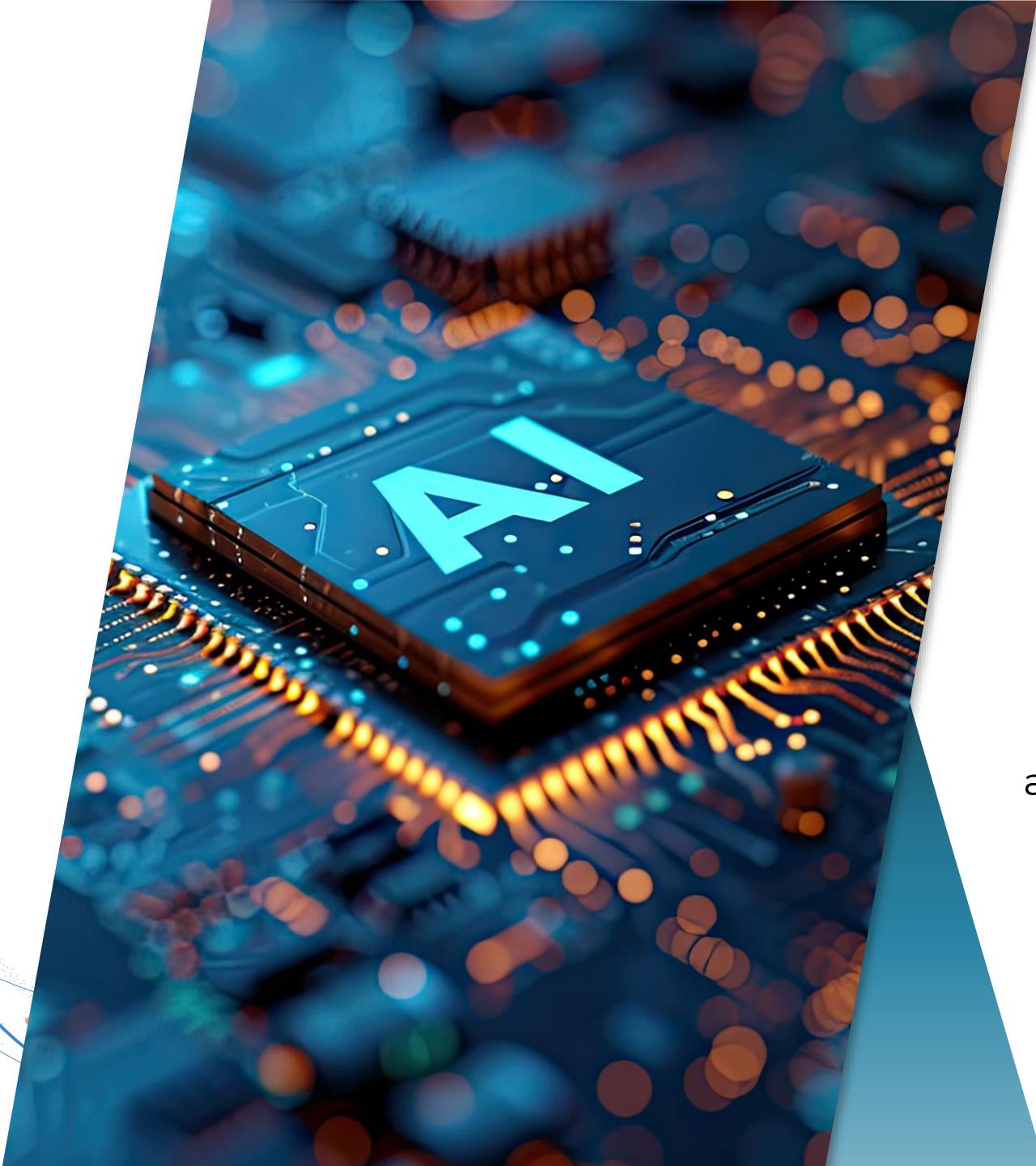
# Time to exploit is compressing

---

Historical time-to-exploit timeline



Source: Mandiant

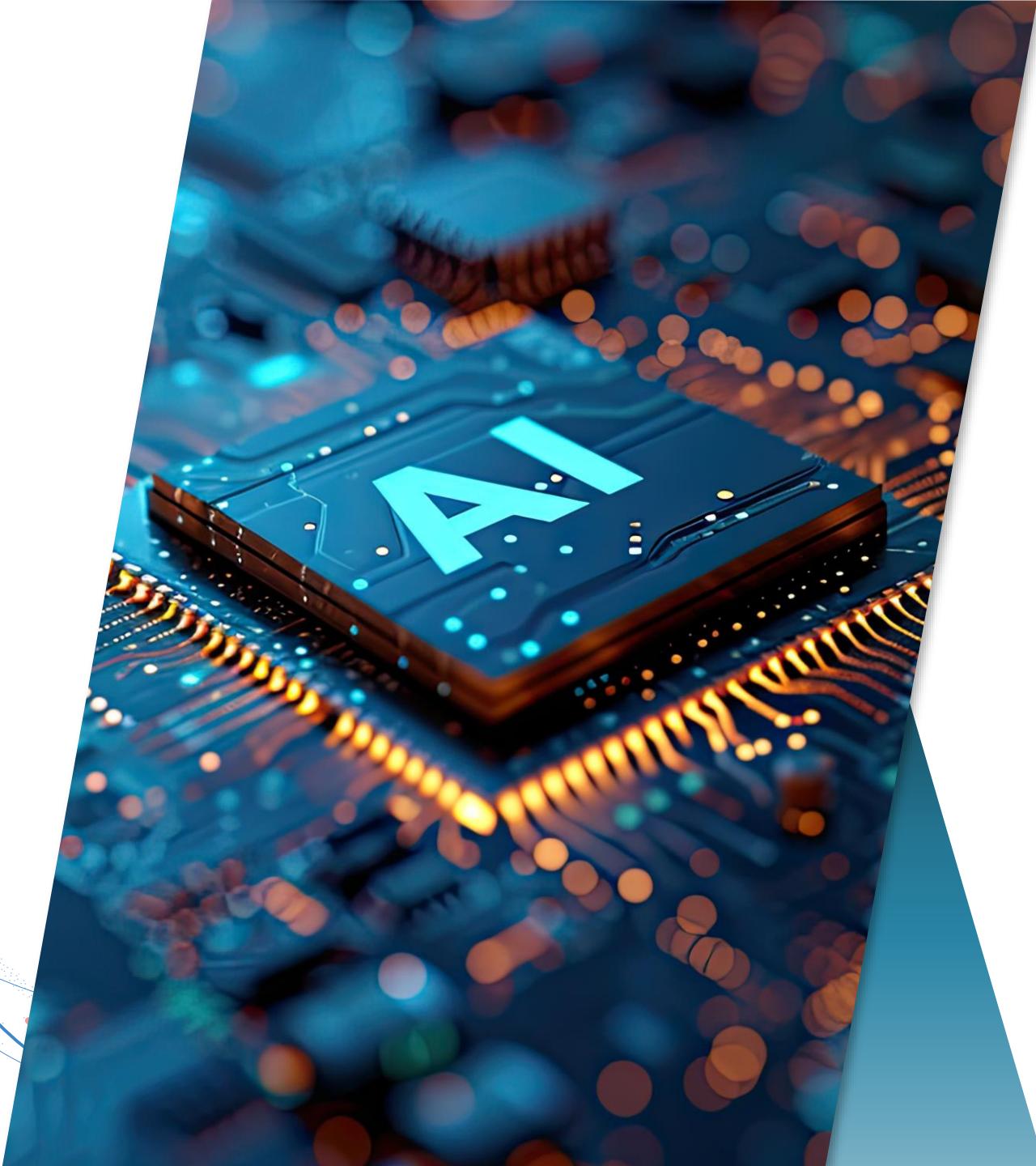
A close-up photograph of a computer processor. The letters 'AI' are prominently displayed in blue on the surface of the chip. The processor is surrounded by a complex network of glowing blue and orange lights, representing circuitry and data flow. The overall aesthetic is futuristic and high-tech.

# AI is accelerating the exploit timeline

---

Charcoal Typhoon and Salmon Typhoon (China-affiliated), Crimson Sandstorm (Iran-affiliated), Emerald Sleet (North Korea-affiliated), and Forest Blizzard (Russia-affiliated)

Used OpenAI services for querying open-source information, translating, finding coding errors, and running basic coding tasks

A close-up photograph of a computer processor. The letters 'AI' are prominently displayed in blue on the surface of the chip. The processor is surrounded by a complex network of glowing blue and orange lights, representing circuitry and data flow. The overall aesthetic is futuristic and high-tech.

# AI is accelerating the exploit timeline

---

Attackers used Anthropic's Claude Code to automate end-to-end ransomware

Low-skill actors using Claude for extortion workflows and selling AI-assisted ransomware kits

# Not every vulnerability matters — but the right 1% matters **a lot**

~4–6% of all known vulnerabilities are exploited in the wild

~1–2% are weaponized within days after disclosure

<1% account for the majority of real-world breaches

And fixing those at the speed of  
light matters **the most**

# Budgets

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

---





To stay ahead,  
we need more  
than just visibility  
We need **prioritization**  
We need fast **remediation**

We need  
**Risk Surface  
Management**

---



WHAT IS CYBER SECURITY?

---

**Cybersecurity**  
is a risk management  
function

What is Risk Management?

---

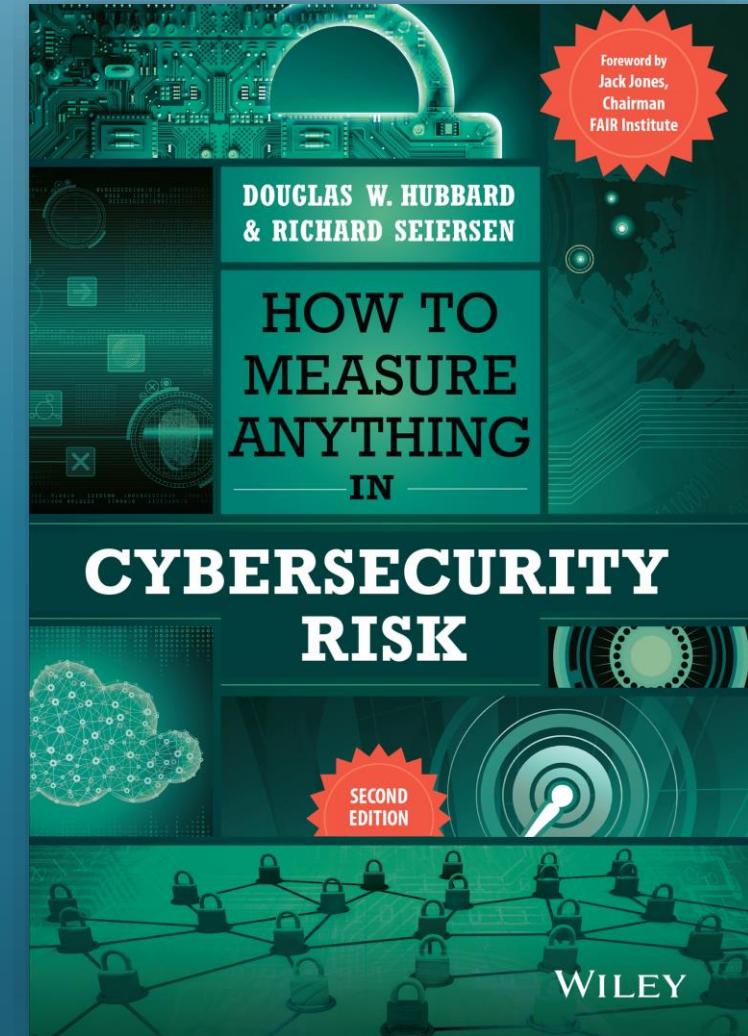
## Risk Management

is the mitigation or transfer of risk for the most plausible losses that could impact the business.”



**Richard Seiersen**

Chief Risk Technology Officer, Qualys





# Risk management

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

---



What is your  
**Value at Risk (VAR)?**

---

**CEO, CISO, CIO, CFO  
and the Board should  
collaborate to define  
value at risk**

# Risk Factors

**Vulnerabilities**



**Misconfiguration**



**User Identities**



# State of **Security Posture** Management today

---



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

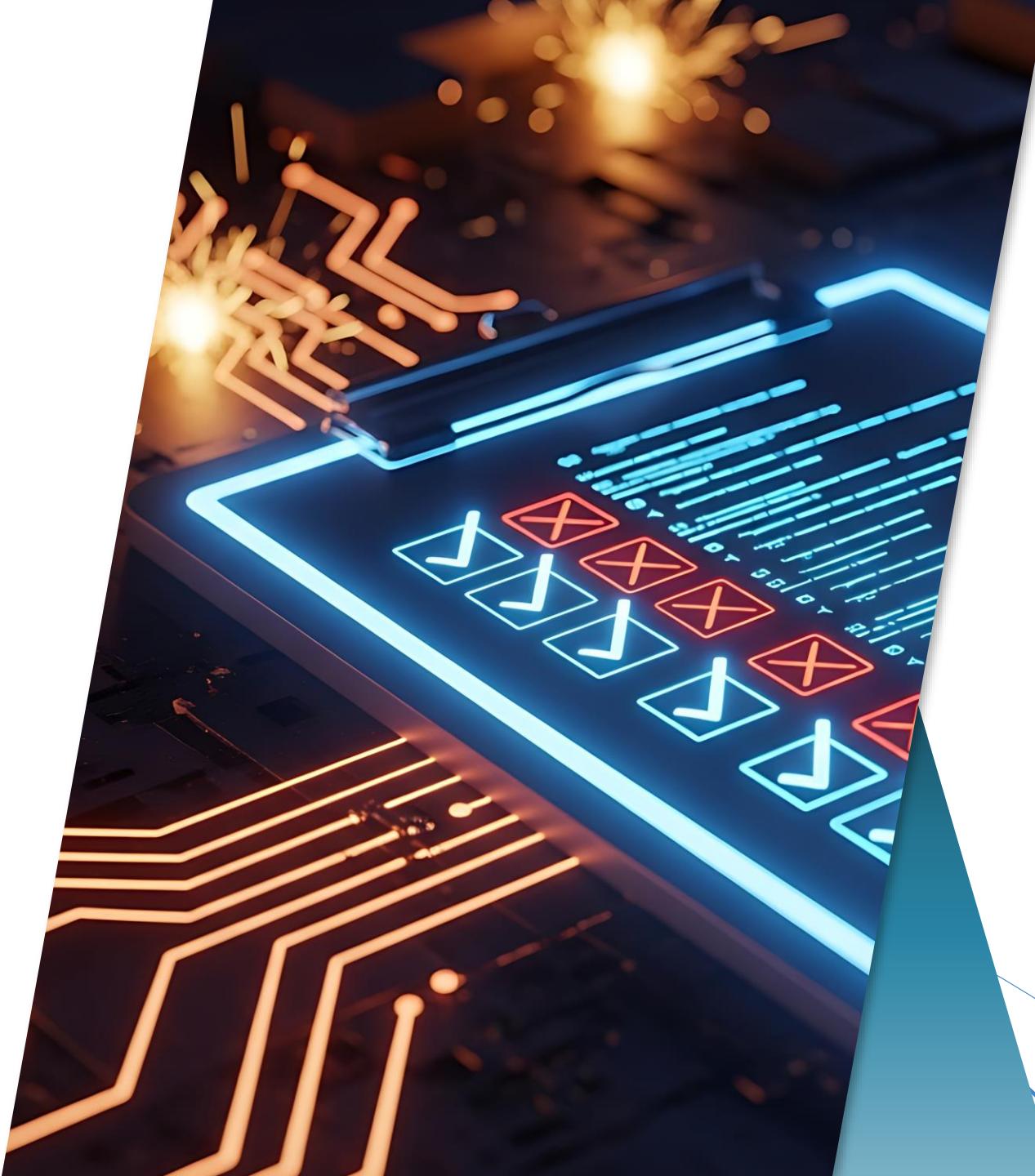
---



# Dashboard Tourism

---





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

---

In 2024, we  
introduced the

**ROC**

**Risk Operations  
Center**

---



# The Risk Operations Center

—  
Operationalize

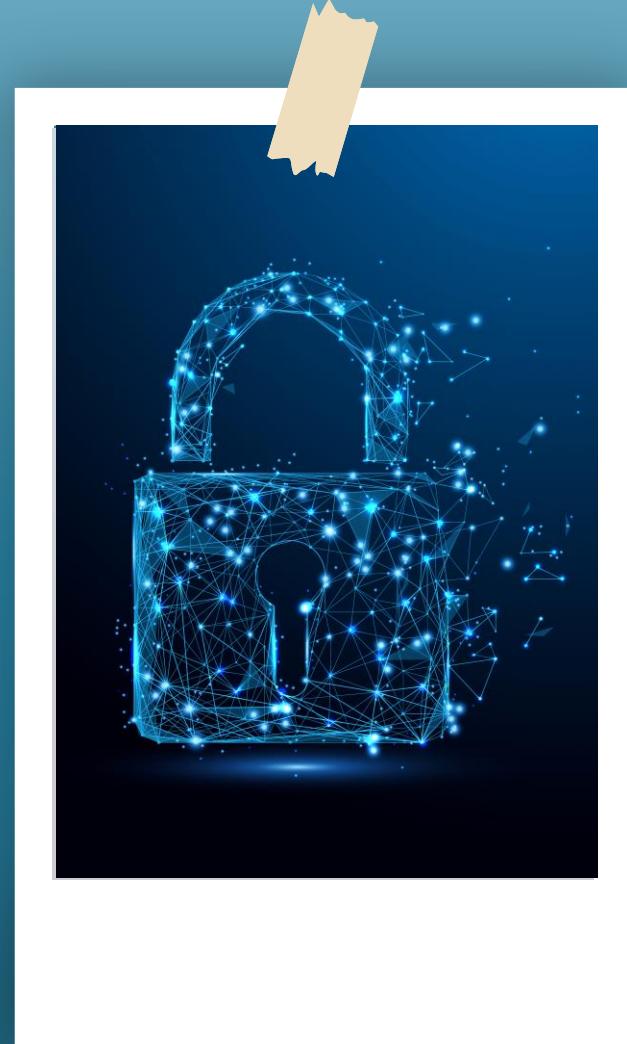


# CTEM Solutions

## Overexpose

### your exposure

---



# 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  
ROC in the Cloud  
**QUALYS ETM**

# Enterprise TruRisk Management

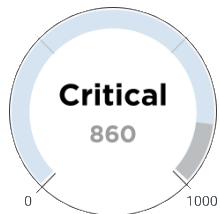
---



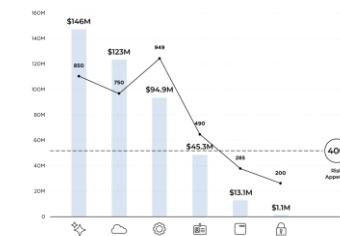
# Qualys ETM



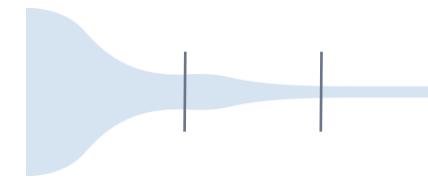
## Measure



## Communicate



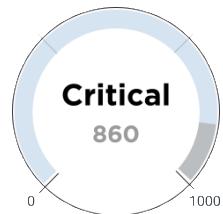
## Eliminate



# Qualys ETM



## Measure



## Communicate



## Eliminate



ETM



Hi Mayuresh, here's the risk summary for your organization. Dive in and de-risk now!



Search here

All Business Entities

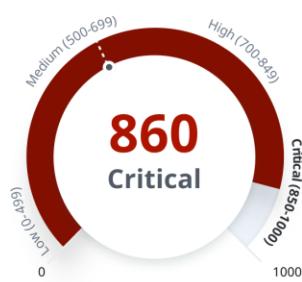


## ACME Corporation

Revenue \$15B

Industry Retail

## TruRisk Score

Last Calculated  
30 Sep 2025  
01:24 PM Your score is **lower** than 88.2% of the peers in your Industry

## Trend of TruRisk Score



## Risk Overview

## Critical Assets

851

&lt;1% of Total 965K Assets



## Critical Vulnerabilities

304K

3.87% of 213M Total Findings (304 Unique)



## Critical Misconfigurations

13K

&lt;1% of 213M Total Findings



# Qualys ETM



Measure



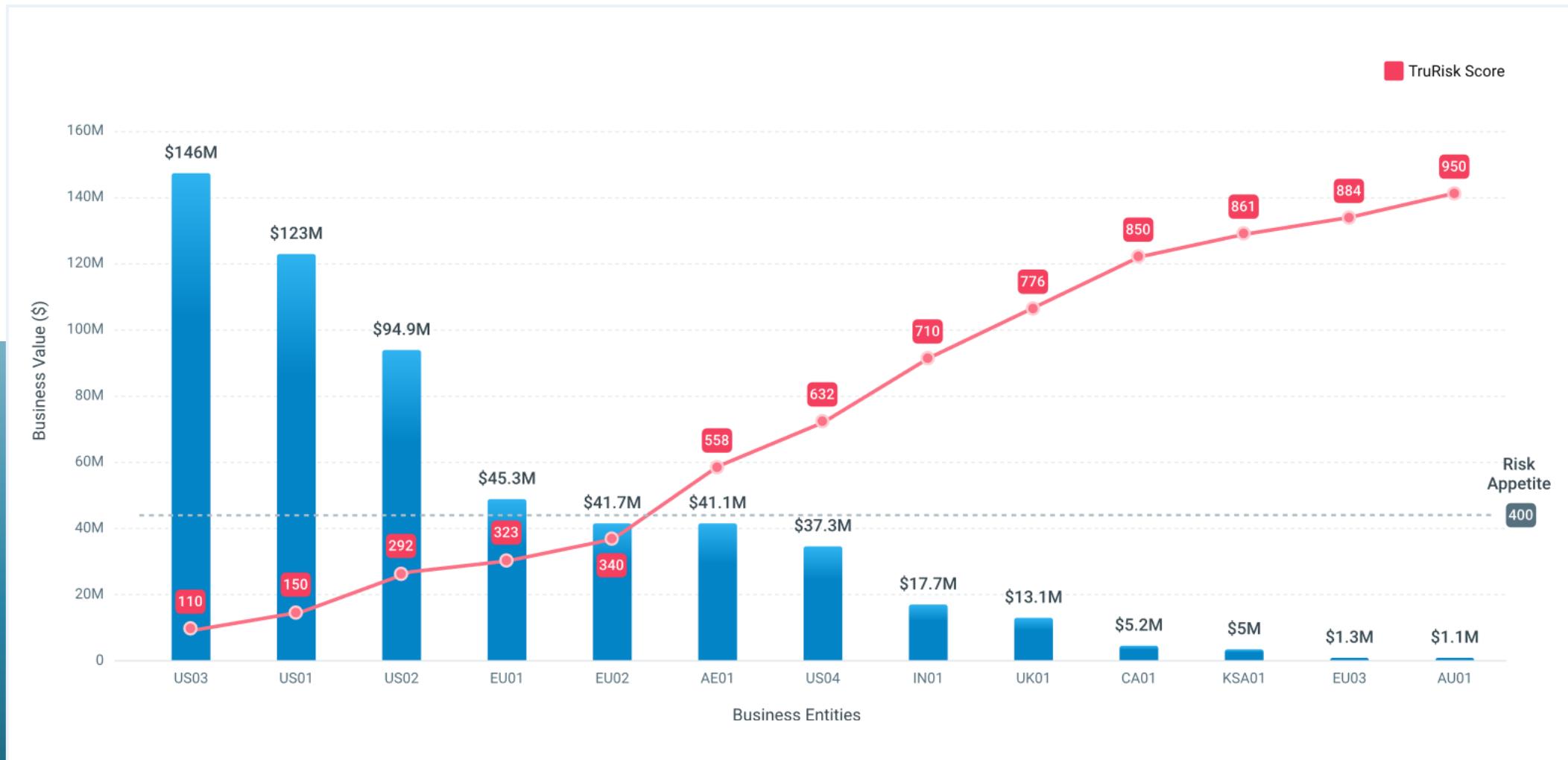
Communicate



Eliminate

# Your Partner in **Cyber Risk Management**

## Aligns Cyber Risk to Business



# Qualys ETM



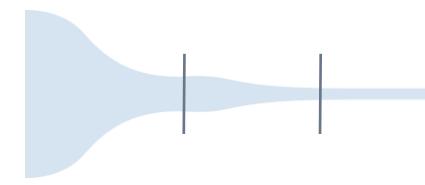
**Measure**



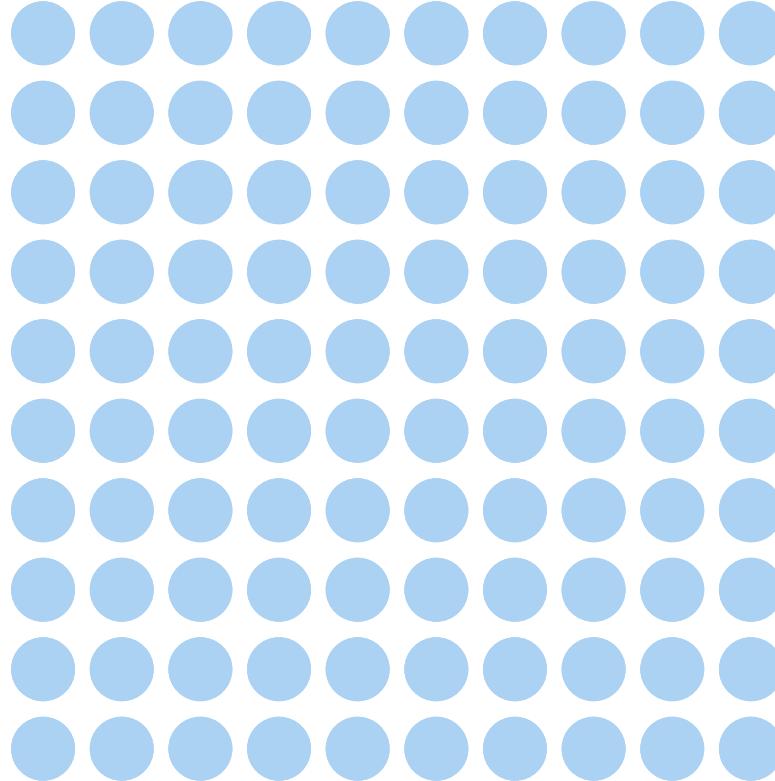
**Communicate**



**Eliminate**

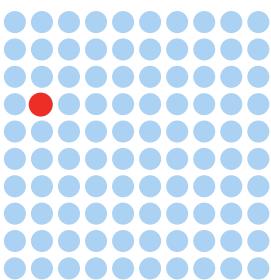


Bring **every exposure** from every  
security tool

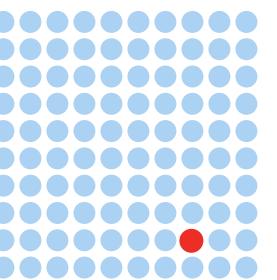


# Millions of Fragmented Exposures coming together

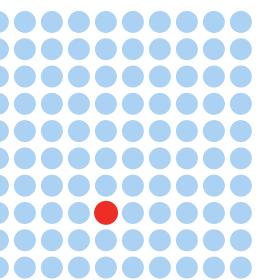
16.5M



9.5M

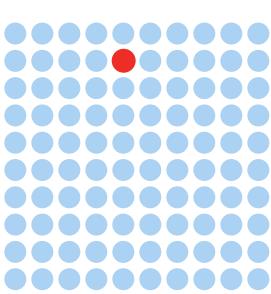


7M

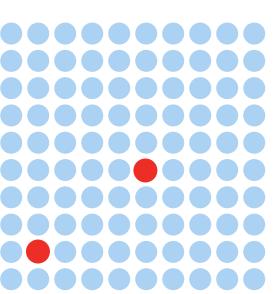


Aggregating All Findings

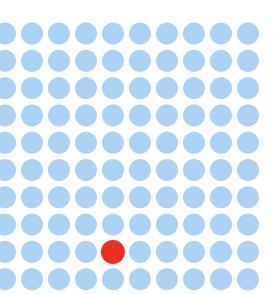
5.5M



11M



13M

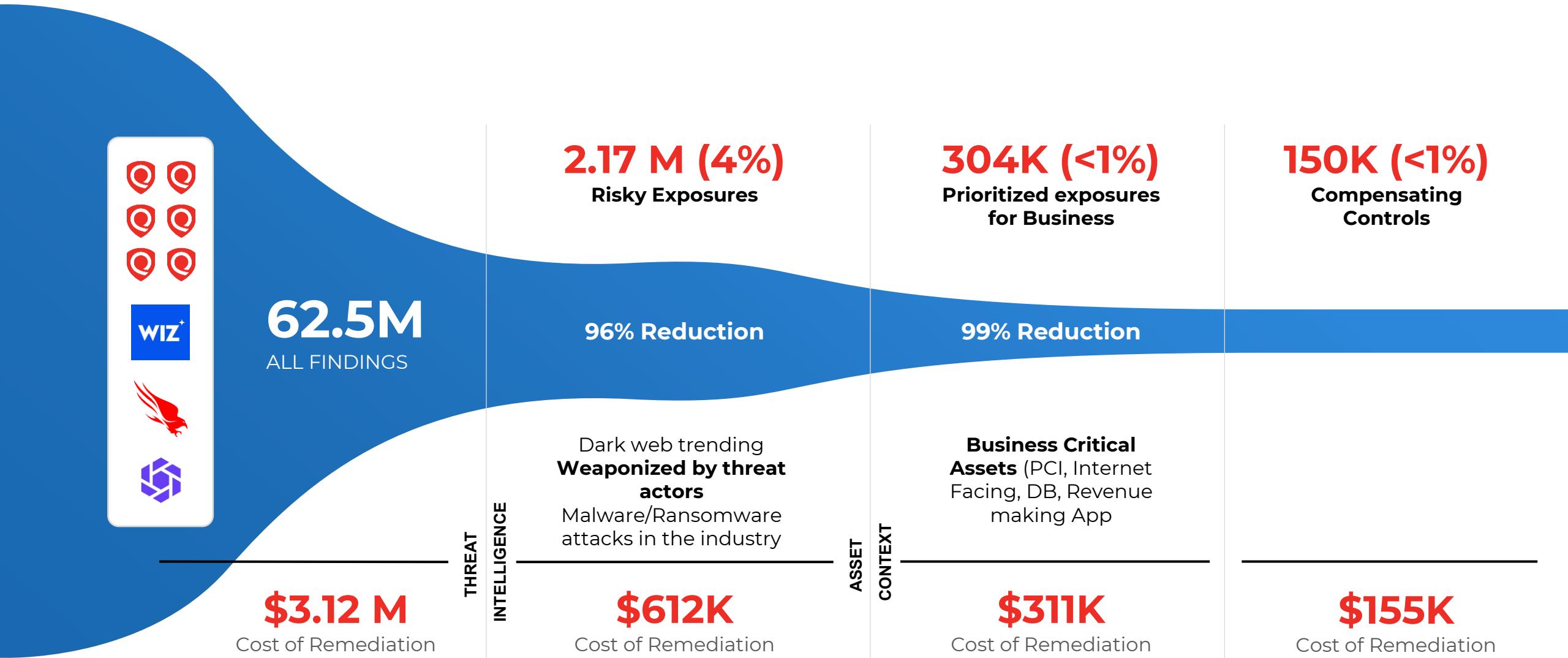


**62.5M**

ALL FINDINGS

# Prioritizing Risk which Matters, Increases Efficiency

## Risk Operations Center (ROC)



# Eliminate Risk With, or Without a Patch

TruRisk Eliminate – Reduce Risk, Reduce Cost of Remediation

**150K (<1%)**

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

## Patch

Qualys + SCCM/Intune  
Integrated

## Mitigate

Patchless  
patching

## Cloud Exploitation Prevention

## Isolate

Non-compliant

## Uninstall

Unused

**\$155K (<10%)**

Cost of Remediation

# High Quality Threat Intel is the brain of Risk Operations Center (ROC)

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



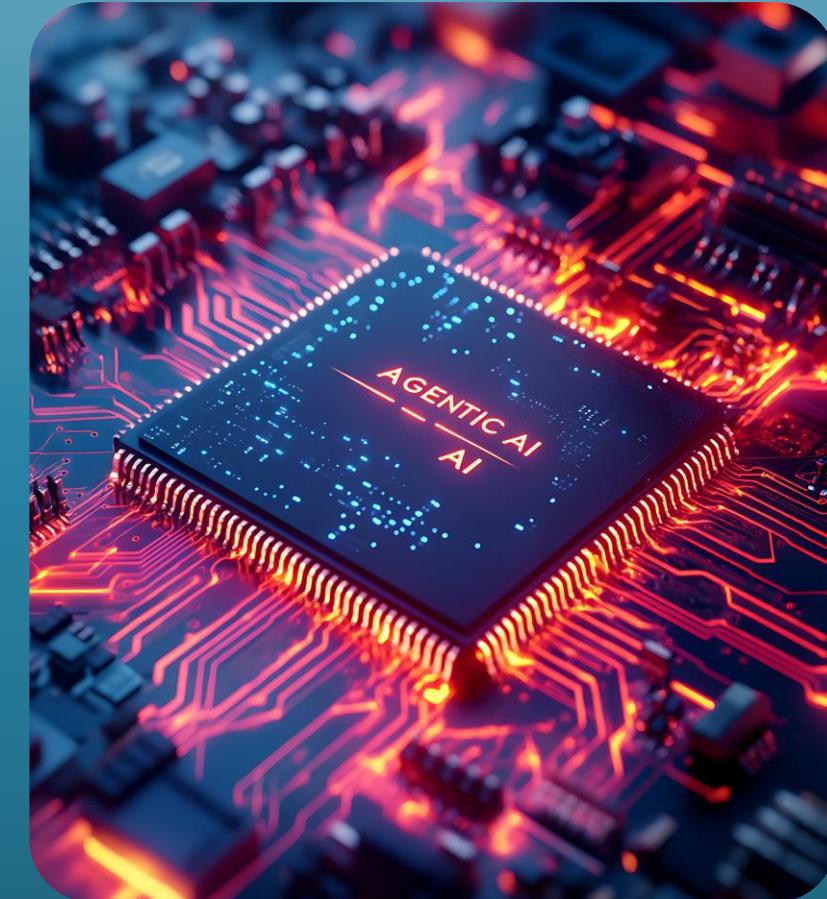
25+ Threat Sources



You can't fight  
**machine-speed**  
**threats** with **human-**  
**speed response**

Human + AI  
Collaboration

**Agentic AI**  
changes the game



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

---



# Qualys Marketplace of Cyber Risk Agents

Your skilled, digital  
workforce for  
autonomous risk  
management

The Qualys Marketplace of Cyber Risk Agents is a digital platform for managing a skilled, digital workforce. It features a grid of agent profiles, each with a unique name, rating, and a brief description of their capabilities. Each profile includes a 'Core Skills' section, a 'Projected Agent Impact' section, and a 'Employ' button.

- Agent Nyra** (4.8, Reliable): Threat-Informed Risk Prioritization. Monitors trending high-profile threats. Core Skills: Threat Intelligence, Threat Prioritization, MITRE Attack. Impact: 85% Monitoring of Trending Threats, 22% Reduction in Cyber Risk. Employ button.
- Agent Sara** (4.8, Popular): Autonomous Patch Tuesday Lifecycle. Automates Patch Tuesday from CVE mining to patch mapping. Core Skills: Patch Tuesday, Vulnerability Management. Impact: 15% TruRisk Points Eliminated, 75% Faster Patch Closure (MTTR). Employ button.
- Agent Nova** (4.9, Trending): Discover & Prioritize Risk of External Attack Surface. Provides a hacker's eye view of internet-facing assets. Core Skills: External Attack Surface Management (EASM), Threat Protection. Impact: ~25% Unknown Assets Discovery, ~15% Hidden Risk Reveal, 90% Faster Detection of Risk. Employ button.
- Agent Chang** (4.6, Popular): Audit-readiness Assessment & Reporting. Keeps assets audit-ready with continuous evidence collection. Core Skills: Compliance Management, Audit Management. Impact: 85% Less Time, 22% Less Audit Gaps. Employ button.
- Agent Sophia** (4.6, Reliable): Self-Healing Autonomous VM. Self-heals VMs by identifying security vulnerabilities. Core Skills: Continuous Discovery, Risk Based Detection. Impact: 99% Visibility of Internet-Facing Assets, 60% Reduction in Noise, 4x Faster Detection for Critical CVEs. Employ button.
- Agent Vikram** (5, Reliable): Adaptive Cloud Risk Assessment. Discovers unknown and unmanaged cloud assets. Core Skills: CWPP, CNAPP, Cloud Security. Impact: 100% Visibility into Cloud Assets, 6 Mins To Define Flexible Scan Strategies in Cloud, 22% Less Cyber Risk in Cloud. Employ button.



Agent Sara ★ 4.8

### Autonomous Patch Tuesday Lifecycle

Automates Patch Tuesday from CVE mining to patch mapping, enabling faster remediation, reduced risk and exposure, and greater focus on high-value security priorities.

#### Core Skills

Patch Tuesday

Vulnerability Management

+1

#### Projected Agent Impact

15%

TruRisk Points  
Eliminated

75%

Faster Patch Closure  
(MTTR)

Employ

Popular

## Current Posture

20.92K of 112K

Assets (18.67%)

45.73K of 410K

Finding Instances (11.15%)

59

Unique Vulnerabilities

6.1K

Critical Vulnerabilities



56D

MTTR



Agent Sara ★ 4.8

### Autonomous Patch Tuesday Lifecycle

Automates Patch Tuesday from CVE mining to patch mapping, enabling faster remediation, reduced risk and exposure, and greater focus on high-value security priorities.

#### Core Skills

Patch Tuesday

Vulnerability Management

+1

#### Projected Agent Impact

**15%**

TruRisk Points  
Eliminated

**75%**

Faster Patch Closure  
(MTTR)

Employ

Popular

## 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



Agent Sara ★ 4.8

### Autonomous Patch Tuesday Lifecycle

Automates Patch Tuesday from CVE mining to patch mapping, enabling faster remediation, reduced risk and exposure, and greater focus on high-value security priorities.

#### Core Skills

Patch Tuesday +1 Vulnerability Management

#### Projected Agent Impact

**15%**  
TruRisk Points Eliminated

**75%**  
Faster Patch Closure (MTTR)

Employ

Popular

## Task: Patch Critical Vulnerabilities on Non-Critical Assets

### Outcome

#### TruRisk Score Impact



-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

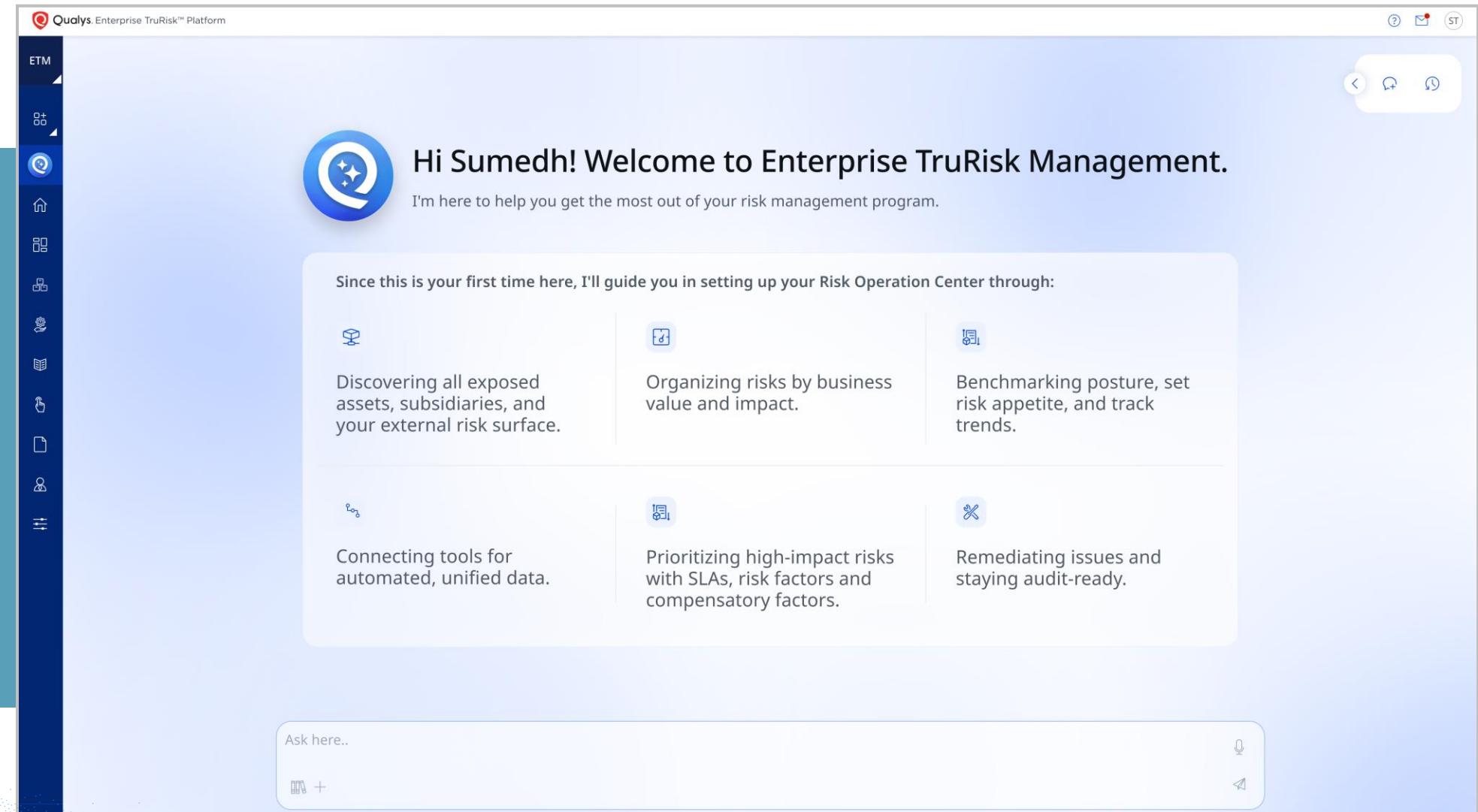


**4%** Remaining findings

Patch not available, Mitigation can be Applied

# Cyber Risk Assistant

Helps users navigate and evaluate their risk posture with a NLQ



The screenshot shows the Qualys Enterprise TruRisk Platform interface. At the top, it says "Hi Sumedh! Welcome to Enterprise TruRisk Management." Below this, a message reads: "I'm here to help you get the most out of your risk management program." A central callout box states: "Since this is your first time here, I'll guide you in setting up your Risk Operation Center through:" followed by six numbered steps:

- Discovering all exposed assets, subsidiaries, and your external risk surface.
- Organizing risks by business value and impact.
- Benchmarking posture, set risk appetite, and track trends.
- Connecting tools for automated, unified data.
- Prioritizing high-impact risks with SLAs, risk factors and compensatory factors.
- Remediating issues and staying audit-ready.

At the bottom, there is a search bar with the placeholder "Ask here.." and a "Ask" button.

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**

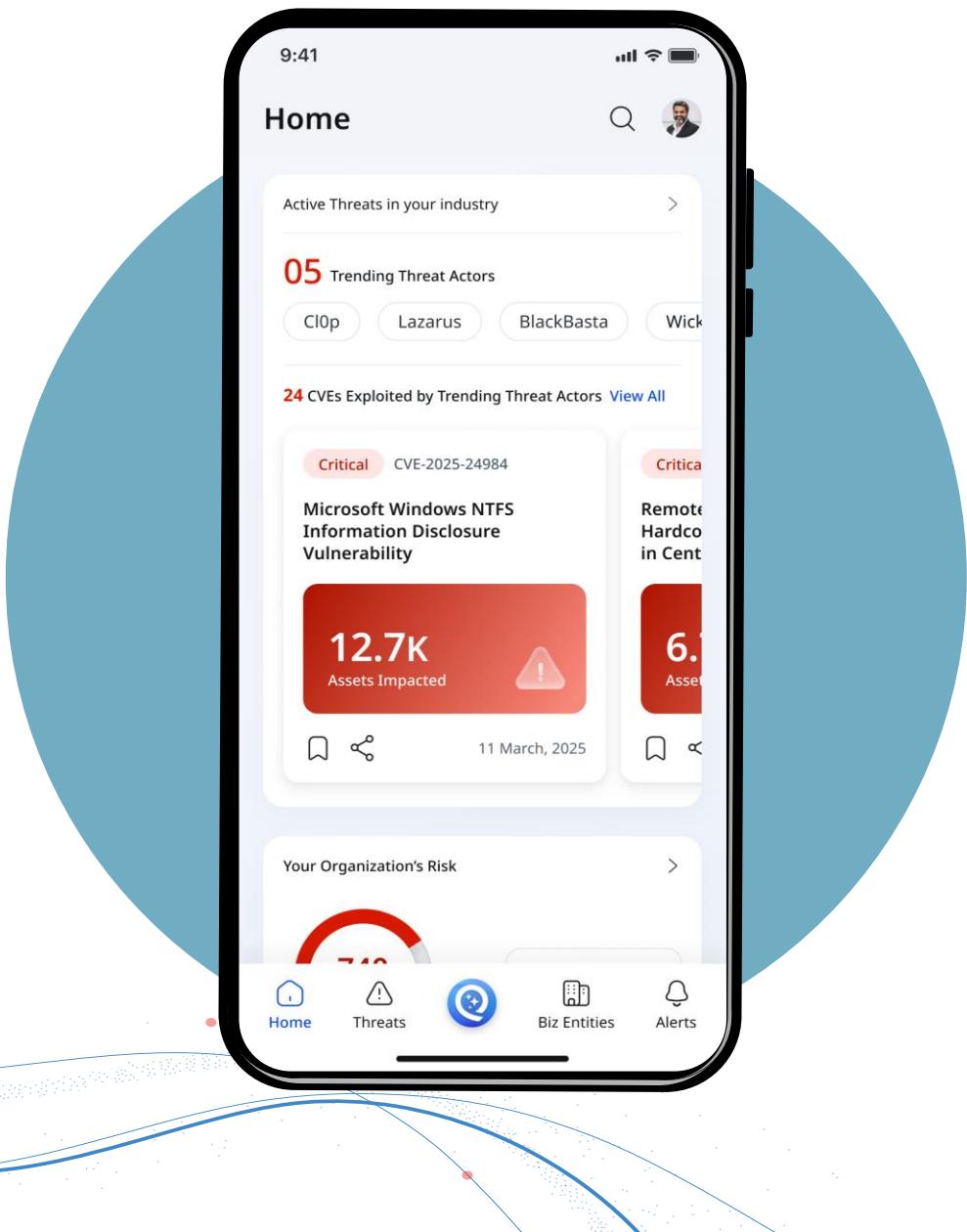
Global Mercantile Corporation, San Francisco, CA



👉 Would you like me to **save this as your Company Profile**?

Chatting with Agent Sid X





# Democratize

access to diverse  
security data

---

# Introducing mROC

# managed Risk Operations Center

---



**mROC  
Partners**



**Qualys®**

**ETM**

**Cyber  
Insurance**



---

## **Enterprise TruRisk™ Management**

Measure, communicate and eliminate cyber risk

---

**De-risk your business**  
with the **Risk Operations Center**



# DEMO



Qualys®

# ROCon<sup>25</sup>



The Risk Operations Conference

---

APAC