Qualys ROCon 26
The Risk Operations Conference
EMEA

Autonomous Cyber Risk Operations (ROC) with Qualys Enterprise TruRisk Management (ETM)



Shailesh Athalye
SVP, Product, GTM
& Solutions Architecture



Qualys ROCon 26
The Risk Operations Conference
EMEA

Good Morning — Your Overnight Risk Summary

Your **Frontier Threat Response** agent ran at 02:00 AM. Here's what happened:

New CVEs	Validated Exploitable	Patched	Held	Mitigated	Isolated
127	34	27	1	4	2
	TruConfirm confirmed	High reliability (>90%)	38% reliability — mitigation applied		

127 new CVEs came in overnight → **89** matched your assets → Agent Val TruConfirm validated **34** as exploitable → TruRisk Eliminate: **27 patched** (high reliability), **4 mitigated**, **2 isolated** → **1 patch held** — 38% reliability score, mitigation + JIRA ESC-4891 created instead.

🧠 **AI Decision:** Of 127 overnight CVEs, 34 validated exploitable. Patched 27 (high reliability >90%), held 1 patch (38% reliability — known LDAP restart failures, deployed mitigation + JIRA instead), mitigated 4, isolated 2. AI Patch Reliability trained on 150M+ deployments prevented a production outage on ldap-auth-01.

✅ 33 of 34 findings fully remediated. 1 held patch covered by mitigation — no action required.

Want to see your new agent in the marketplace?

Objectives

Key take aways from Sumedh's Keynote

Qualys ROCon 26 The Risk Operations Conference EMEA

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

Key Challenges

Qualys ROCon 26 The Risk Operations Conference EMEA

01

The CTEM Delusion

Exposure ≠ Exploitability

Exposure visibility without validating real exploitability; slow insights and unproven risk closure.

02

Detection quality -> Risk Program quality

Stale data, False negatives and noise

Poor detection quality creates noise, false positives, and delays in identifying real risks.

03

Remediation Is an Island

Backlog growing faster than teams can fix

Patch backlog grows every month (avg 3k risky vulns remain open) resulting in more time for attackers to exploit and ITOps wasting money on noise

04

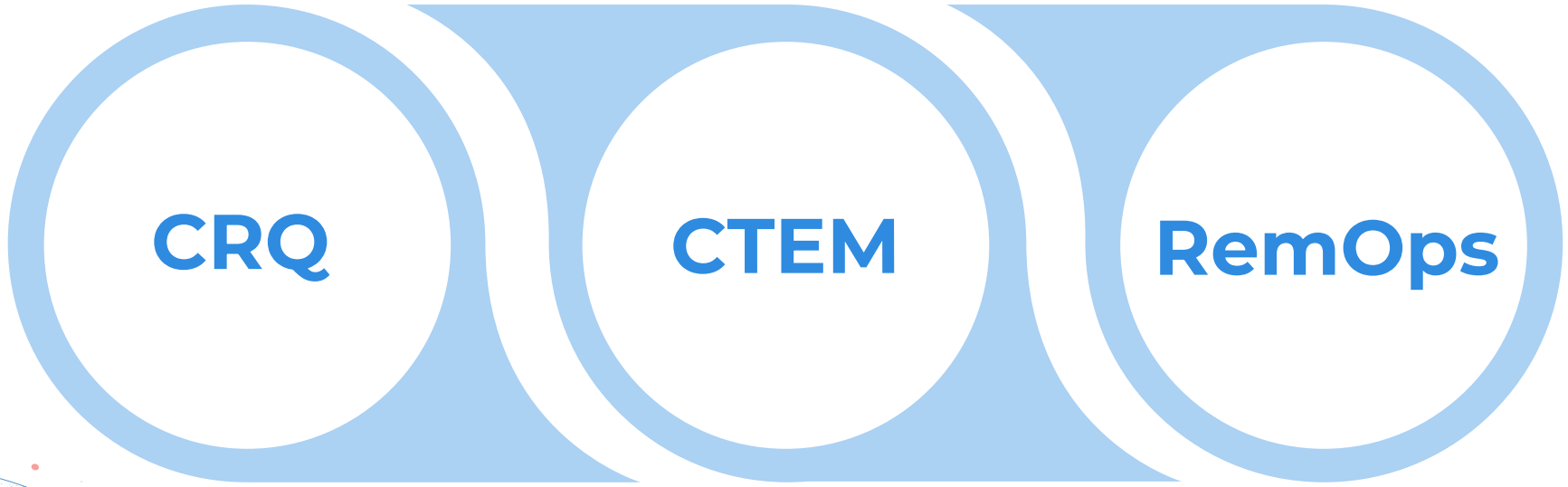
Risk Has No Business Voice

Exec asks 'what's business loss?' — not how many vuln?'

Security metrics don't translate to business impact, leading to weak decision-making and underfunding.

Addressing all four simultaneously is the only path to a programme that scales in the Mythos era.

AI-native ROC



Qualys Approach to ROC – Enterprise TruRisk Management (ETM)

Qualys ROCon 26 The Risk Operations Conference EMEA

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

NON-QUALYS

- Vulnerability Management
- Compliance
- Runtime Security
- Vulnerability Management

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

THREAT INTELLIGENCE

(CMDB, Custom Data Sources)

BUSINESS CONTEXT

MEASURE | Quantify Cyber Risk in Business Terms

COMMUNICATE | Executive Reporting and Ticketing

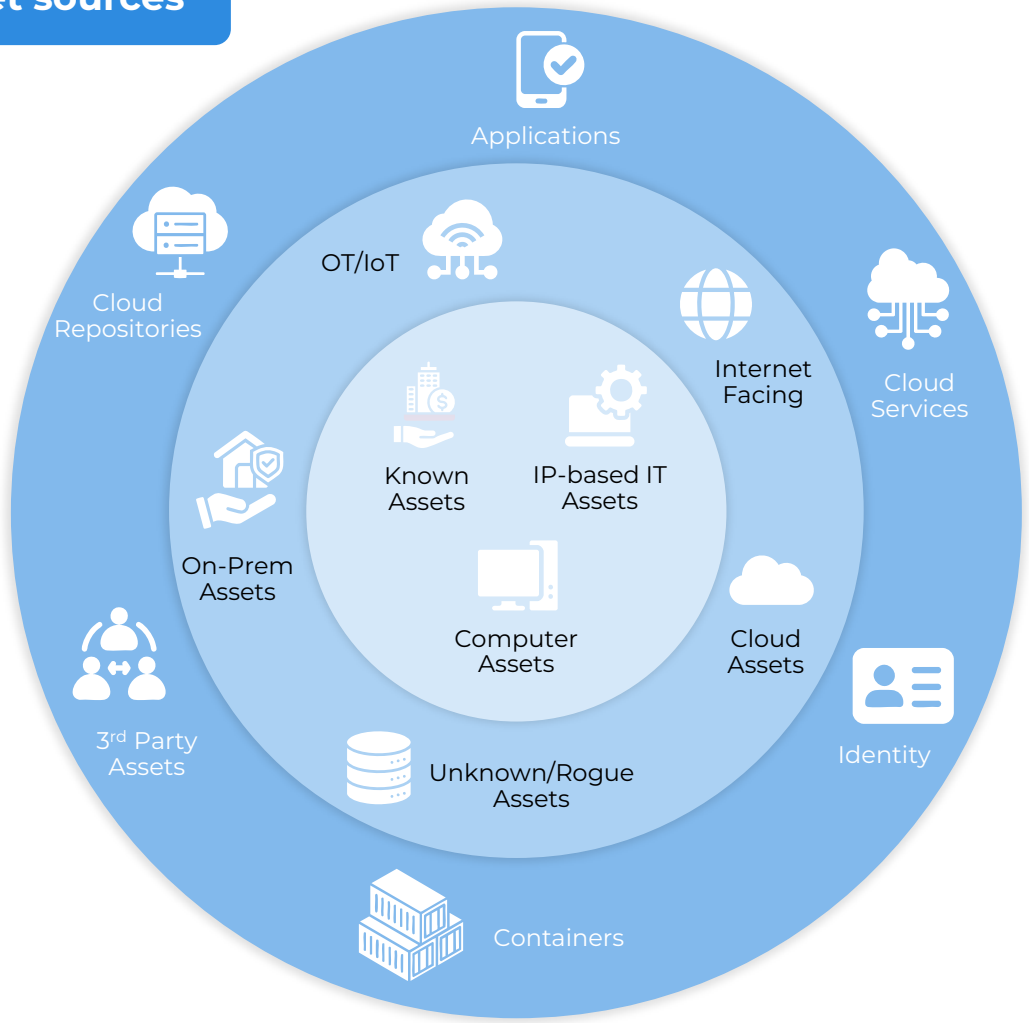
ELIMINATE | Patch Mitigate & Track

Hyper Prioritization

Qualys ROCon 26 The Risk Operations Conference EMEA

Know all your assets & attack surface

Asset sources



Detection method

Qualys Sensors
Agents, Scanners, Cloud

CMDB
ServiceNow, etc.

EASM
External Attack Surface

Passive sensors
unmanaged assets

Security Tools
Third-party integrations

From knowing assets to knowing Business context

Qualys ROCon 26 The Risk Operations Conference EMEA

Aggregation, Normalization & Enrichment

- Business Application, role & Criticality
- Tech Debt (EOS/EOL)
- Software/app Context (mitigation)

Business Entity — **Tier 1 Critical**

Payment Gateway App

i-0abcd1234efgh5678 (EC2)

Holistic Context

Business context:

Value: Critical

Business: Payment Gateway/Acme Capital

Risk Context:

Apache Tomcat: EOL/EOS

Unauthorized software: TeamViewer, Chrome

Mitigation control missing: EDR, DLP

EASM: RDP Open open

Qualys ROCon 26 The Risk Operations Conference EMEA

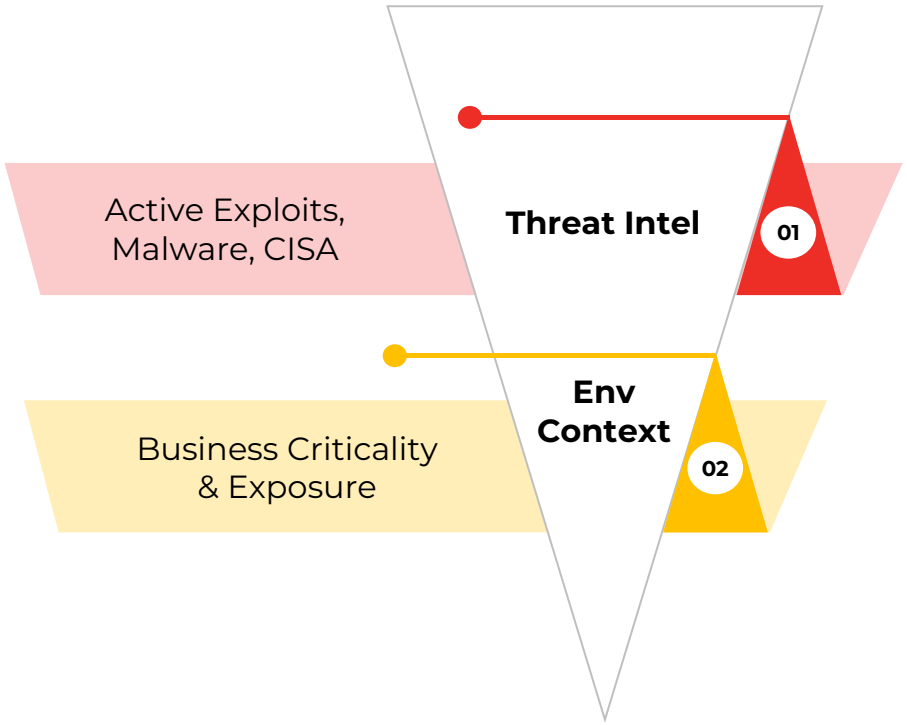
Prioritizing Millions of Exposures at real-time

Security Findings

- Infra Vulns
- Misconfigs
- Certificates
- OSS Vulns
- EOL Software
- Web App
- EASM
- Cloud Posture

In Millions

Threat Feed



Mitigation?
Is it running?

25+ Threat Sources

QVSS

For Vulns + Misconfigs + identities

9.8 Critical

CVE-2024-21887

Talos Google IMMUNITY metasploit

Prioritized Exposures with asset business context

Qualys ROCon 26 The Risk Operations Conference EMEA

Security Findings

- Infra Vulns
- Misconfigs
- Certificates
- OSS Vulns
- EOL Software
- Web App
- EASM
- Cloud Posture

20% of Risky Exposures

Business Asset Context

Asset to business context

Payment Gateway App

EOL Software, Open port	Detected
EDR (mitigation)	Detected
Exposure criticality (QVSS)	9.1

ACME CAPITAL TRURISK

860

Prioritize Exposures now less than 10%

Prioritized Exposures with threat & business context

Qualys ROCon 26 The Risk Operations Conference EMEA



62.5M
ALL FINDINGS

2.17 M (4%)
Prioritized based on threat context

304K (<1%)
Prioritized based on business context

96% Reduction

99% Reduction

THREAT INTELLIGENCE

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

ASSET CONTEXT

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

$3.12 M
Cost of Remediation

$612K
Cost of Remediation

$311K
Cost of Remediation

Qualys ROCon 26 The Risk Operations Conference EMEA

From Reactive to Proactive Action

Knowing the risk to the business from trending threat actors allows us to prioritize high-risk vulnerabilities well before the industry standard.



Qualys ROCon 26 The Risk Operations Conference EMEA

Why Exploit Validation?

Prioritization narrows the focus, but validation proves the risk.

0.74%

Weaponized from 48K CVEs of 2025

52%

of tested exploits bypass default WAF

?

BAS tools don’t get operationalized in Production

Prioritization to Hyper-Prioritization with TruConfirm

Qualys ROCon 26 The Risk Operations Conference EMEA

01

Select

AI picks the right exposures — TruRisk + active threat actor relevance + YOUR business criticality. Not CVSS. Context.

02

Validate

1,700+ production-safe exploit checks. Binary answer: exploitable or not. In YOUR environment. With YOUR controls.

03

AMPLIFY + RELIABILITY

Confirmed exposures get amplified TruRisk. AI Reliability Score (140M+ deployments) pre-clears which patch is safe.

04

Prove

Post-remediation TruConfirm re-validation. Cryptographic proof. SLA stops at "exploit path confirmed closed" — not "ticket closed."

Why It's Different

01 **Validated Risk vs. Other CTEM theoretical risk**

02 **20x cost efficient vs. Manual pen tests**

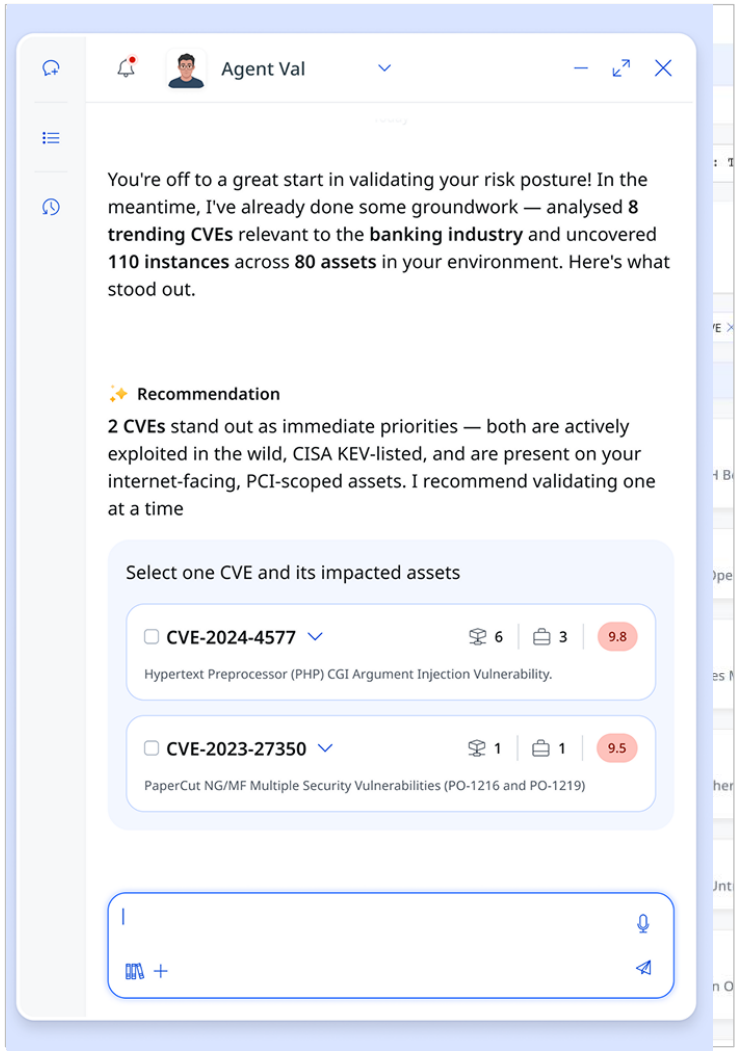
03 **Validates your cyber insights vs. Generic AI**

Agent Val + TruConfirm

Qualys ROCon 26
The Risk Operations Conference
EMEA

Industry's first agentic AI–driven cyber risk agent for safe exploitability validation, powered by ETM TruConfirm

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



Qualys ROCon 26 The Risk Operations Conference EMEA

The Next Era of Exploit Validation

Extending the power of **TruConfirm** to validate exploits natively across Hybrid Infrastructure, IAM, Custom Apps, and Global Grids.

01



Validate Misconfigurations Identities, attack paths

02



Secure Modern Workloads – cloud, container

03



Support for endpoint agent-based validation

04



Protect First party, custom Apps w/ custom exploit kit

Qualys ROCon 26 The Risk Operations Conference EMEA

Exploit validation is a reality in cyber risk operations

8M+

TruConfirm Validations

in last 12 months.

Zero service disruption

Production environment

Qualys ROCon 26 The Risk Operations Conference EMEA

Detection to Prioritization to Hyper-prioritization



62.5M
ALL FINDINGS

$3.12 M
Cost of Remediation

2.17 M (4%)
Prioritized based on threat context

96% Reduction

THREAT INTELLIGENCE

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

$612K
Cost of Remediation

304K (<1%)
Prioritized based on business context

99% Reduction

ASSET CONTEXT

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

$311K
Cost of Remediation

With TruConfirm

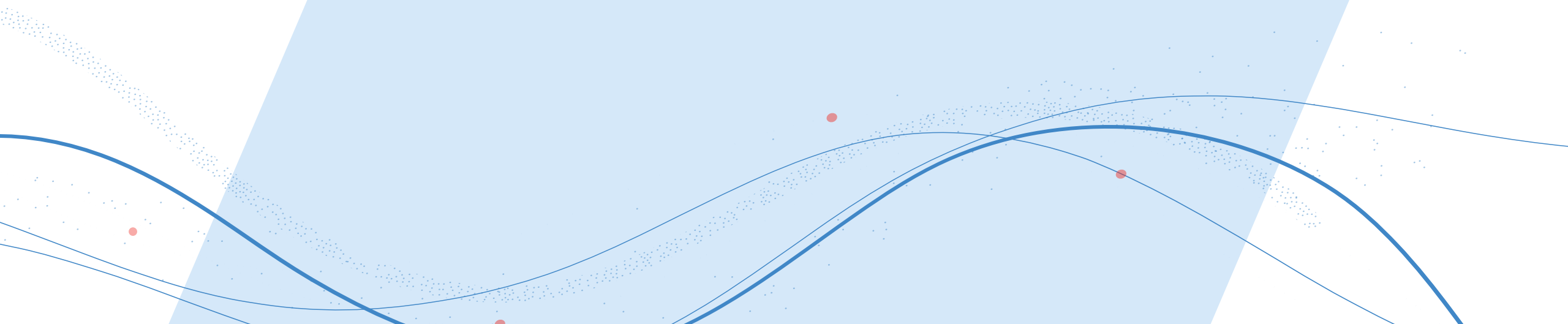
60K (<0.1%)
Prioritized based on compensating controls

Validating exploitability by using modified harmless network payloads

$31K
Cost of Remediation

Qualys ROCon 26
The Risk Operations Conference
EMEA

Autonomous Remediation



Qualys ROCon 26 The Risk Operations Conference EMEA

The Reality Check

Manual Remediation Is Dead

30+ Days

Human Speed

Average Window of Exposure before manual patching completes.

The Mythos Avalanche

-7 Days

Machine Speed

Attacker exploitation window using AI-generated tooling.

If Vuln & Patch count increases 2x or 3x, you cannot outrun an AI-driven pace of detection & exploitation with human speed.

Remediation must become autonomous. But we must address the three systemic fears:

Trust. Confidence. Backup Plan.

Qualys ROCon 26 The Risk Operations Conference EMEA

The English Cricket Inflection Point

In 2022, English Cricket faced the exact same **trust crisis for Abandoning survival-first approach for aggregative style**—until their win rate jumped from **39%** to **61%** **with aggressive approach.**



Addressing **Trust**

Change in Pitches

Creating flatter, faster pitches built the environment for success, rather than blaming players for failing in survival mode.

Addressing **Confidence**

T20 Success Transfer

Leveraging the proven muscle memory and aggressive success from T20 cricket leagues at scale.

Addressing **Backup Plan**

Keep Playing Joe Root

The fundamental rock. Even in an aggressive system, you keep the reliable anchor to ensure a total collapse is impossible.

They only succeeded because they built the trust infrastructure first.

Qualys ROCon 26 The Risk Operations Conference EMEA

Enterprises are already on the Autonomous Journey

TruRisk Eliminate

01

Proven Scale

Total patches deployed:

150M+

Zero-touch autonomous:

40M+

Rollback rate:

<0.1%

02

Confidence

Live mitigations executed:

1M+

Options:

Mitigate, Isolate, Uninstall, Fix

03

Backup with Autonomy

Roll back driven by snapshots:**

Before / After

AI-planned waves:

Today / Weekend / CAB

Qualys ROCon 26 The Risk Operations Conference EMEA

Where should Remediation go from the ITOps Lens

ITOps doesn't speak "TruRisk 847". They speak **"Will this patch break production?“**
We show how operational patch discipline eliminates security debt silently.

AI-Planned Sequencing

Agent Sara studies 6 months of your patch jobs and builds the plan that runs itself.

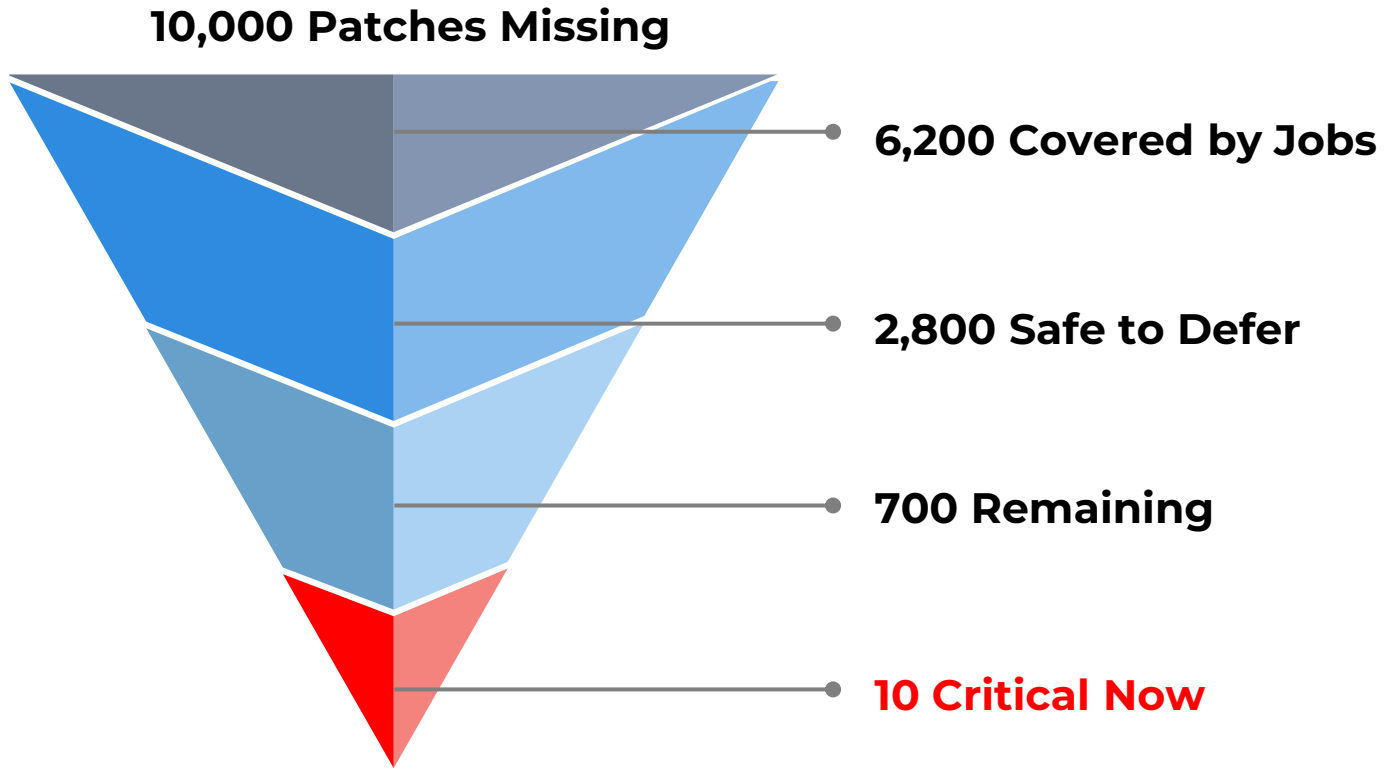
Wave 1: Deploy Today
High Reliability Score, non-critical tier. Clears 60-70% of backlog automatically.

Wave 2: Maintenance Window
Medium-criticality, sequences reboots to maintain quorum. Auto-rollback pre-staged.

Wave 3: Mitigate Now
Critical infra with Low Reliability Score. Apply compensating control instantly, CAB for patch later.

No patch surprises. Risk debt repaid in waves.

The Patch Funnel



Qualys ROCon 26 The Risk Operations Conference EMEA

Closing Risk at Machine Speed.
While keeping Production Alive.

Cyber Risk Lens

Average Window of Exposure (AWE)

~~~37 Days~~ → <10 Days

KEV-to-Patched Time

~~Weeks~~ → Hours

Remediation Options

~~1 (Patch)~~ → 5+ (Mitigate, Isolate, etc.)

Exploitability Noise Reduction

~~100% Volume~~ → 99% Filtered

IT Ops Lens

First-Pass Patch Success	↓ 98.2%
Rollback Rate	↓ 83%
SLA Compliance	↓ 91%
TruRisk Points Eliminated	↓ 142K
Production Outages (Auto)	0
~~~

Prioritize — Validate — Remediate at Machine Speed

Qualys ROCon 26 The Risk Operations Conference EMEA

Rich Context Inputs

- **Exposure**
- **Asset Context**
- **Exploit Validation**
- **Remediation Context**

Bi-Directional ITSM Sync

Jira | ServiceNow | Real-Time Closure

Rich Context Inputs

Real-World Autonomous Workflow

- **PRIORITIZE**
- **VALIDATE**
- **MITIGATE (INSTANT)**
- **REMEDIATE (SCHEDULED)**

Rich Context Inputs

LEGACY MTTR

~~35+ Days~~

TM MACHINE SPEED

< 4 Hrs

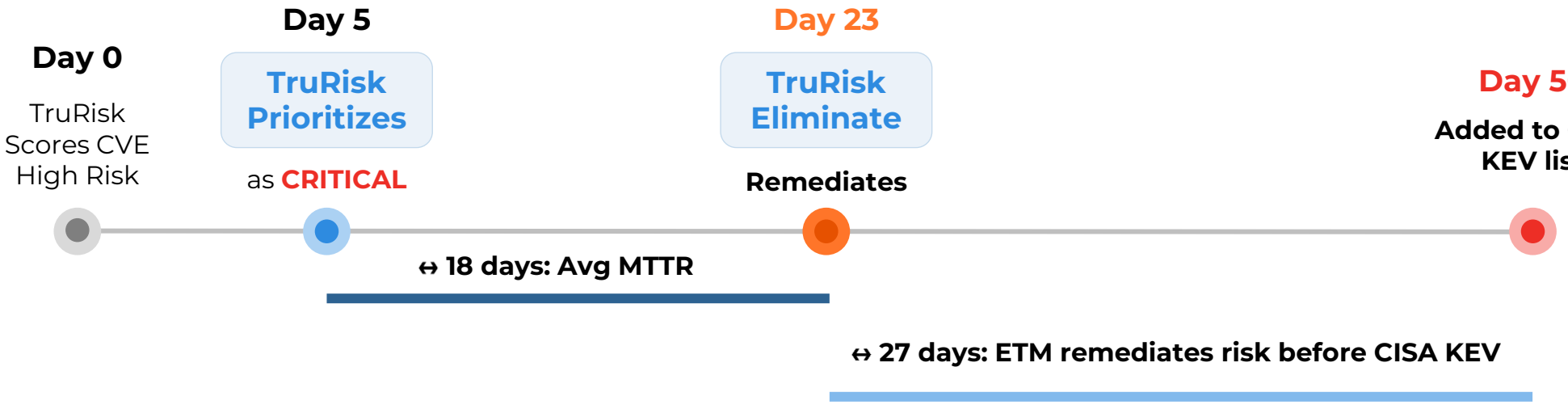
Outcomes Unlocked

- Zero-day exposure neutralized instantly via autonomous mitigation tools.
- Zero-touch automated patching drastically reduces manual IT overhead.
- Continuous audit-readiness with bi-directional syncing of all events.

Qualys ROCon 26 The Risk Operations Conference EMEA

How Proactive is Your Risk Remediation?
You're Fixing a risky exposures 27 Days Before CISA KEV

You fix it 27 days BEFORE it's on CISA KEV



AI-native approach...

Qualys ROCon 26 The Risk Operations Conference EMEA

Not Just a Chatbot; out of box agents for risk outcomes

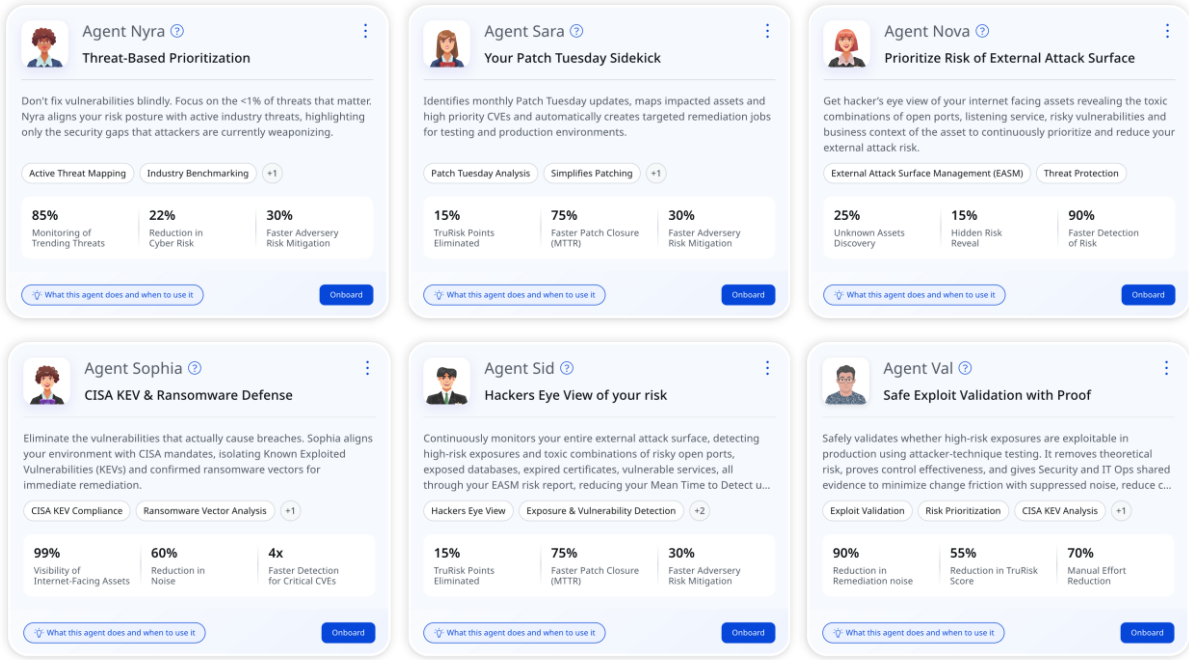
Customer Outcome: If you already know what to ask, humans would have figured out a workflow. Agentic AI is not just generating reports, it's unlocking autonomous, measurable risk reduction.

What It's Not

- Just a chatbot interpreting manual commands.
- A shiny overlay creating tactical dashboards.
- A reactive tool waiting for a prompt.

What Agentic AI needs to look like

Out of Box Cyber Risk Agents for specific risk outcomes



Qualys ROCon 26 The Risk Operations Conference EMEA

Not Just a Chatbot; Decision in your risk operations

Customer Outcome: If you already know what to ask, humans would have figured out a workflow. Agentic AI is not just generating reports, it's unlocking autonomous, measurable risk reduction.

What It's Not

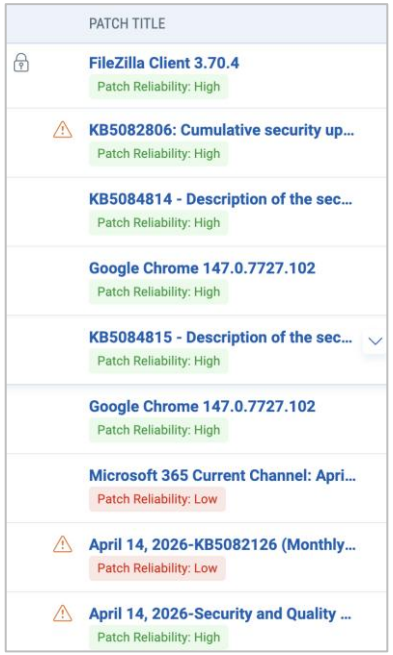
Just a chatbot interpreting manual commands.

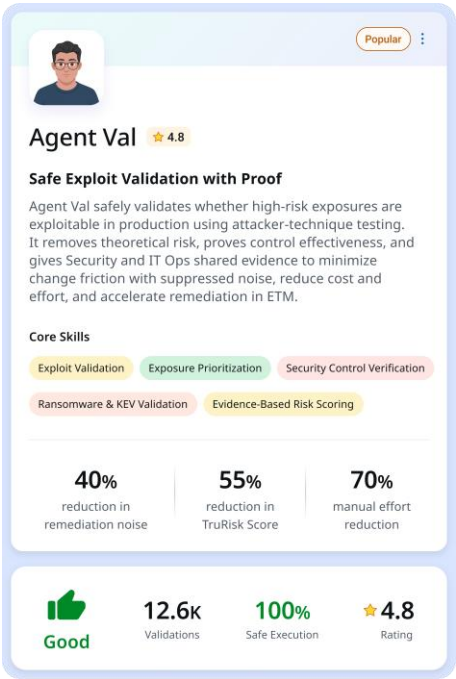
A shiny overlay creating tactical dashboards.

A reactive tool waiting for a prompt.

What Agentic AI needs to look like

AI Baked In Every Cyber Risk decision making





Qualys ROCon 26 The Risk Operations Conference EMEA

Not Just a Chatbot; driving cyber risk tasks

Customer Outcome: If you already know what to ask, humans would have figured out a workflow. Agentic AI is not just generating reports, it's unlocking autonomous, measurable risk reduction.

What It's Not

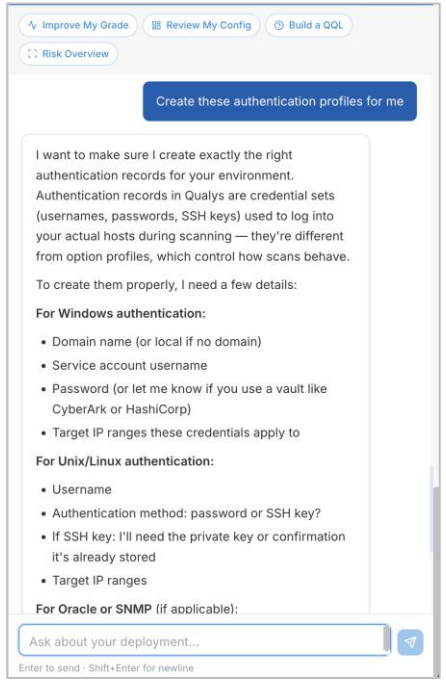
Just a chatbot interpreting manual commands.

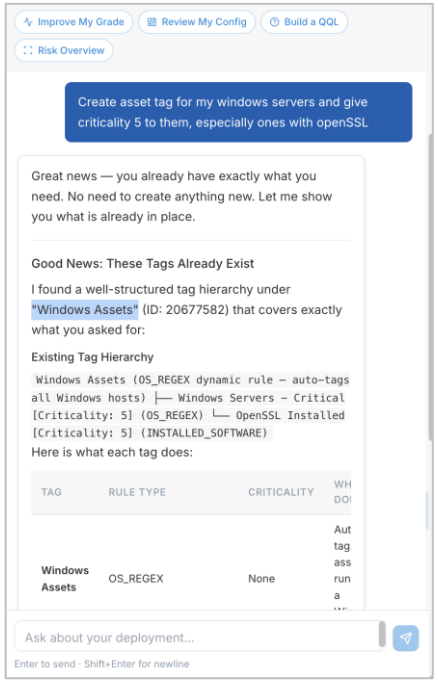
A shiny overlay creating tactical dashboards.

A reactive tool waiting for a prompt.

What Agentic AI for ETM Looks Like

Cyber Risk Assistant (ROCky) for driving risk operations



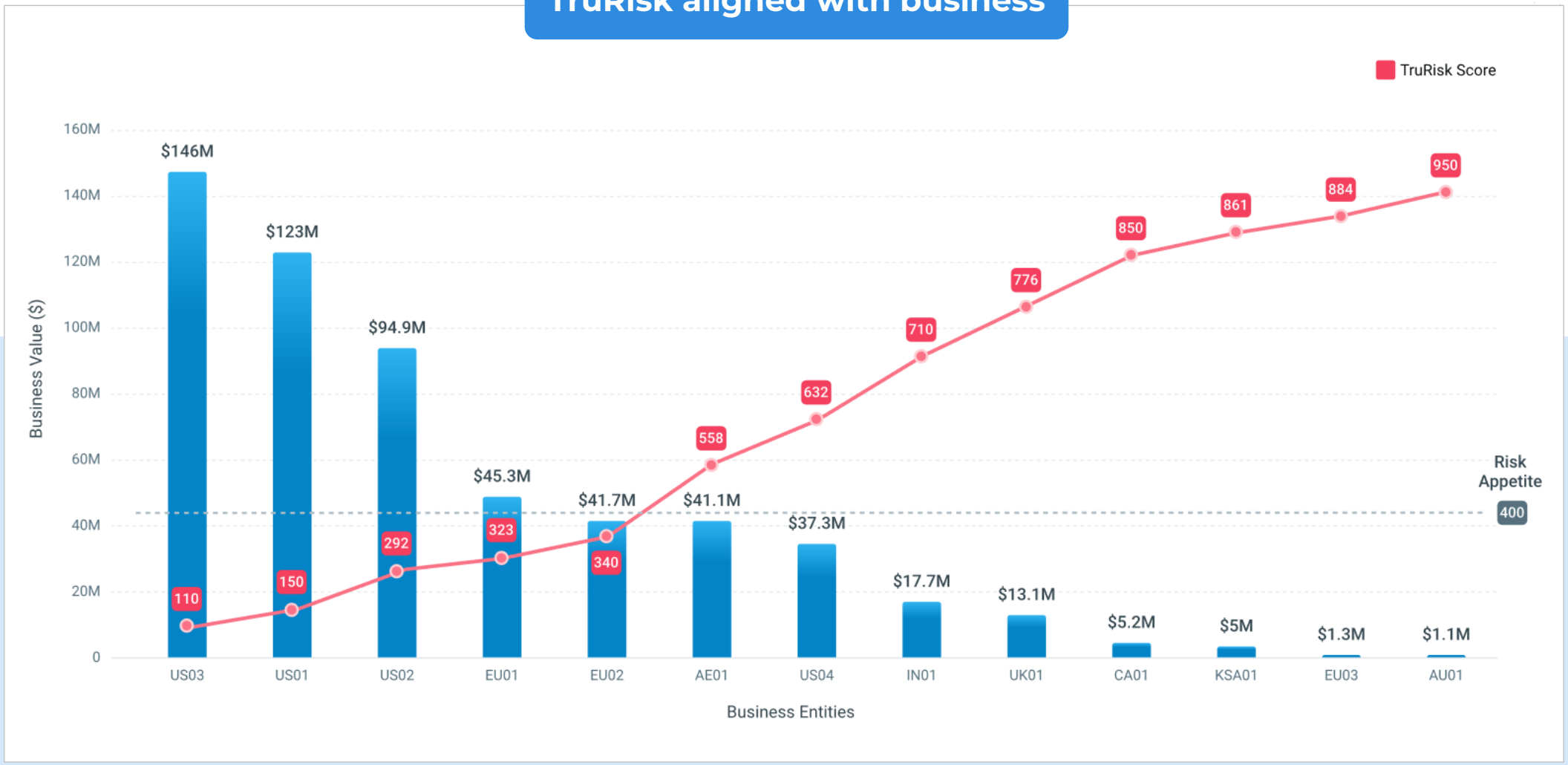


Qualys ROCon 26
The Risk Operations Conference
EMEA

Communicating Cyber Risk for Business Value

Communicating Cyber Risk for Business Value

TruRisk aligned with business



Qualys ROCon 26 The Risk Operations Conference EMEA

Cyber Risk Quantification from bottoms up Cyber TruRisk

Security Speaks in Tech

“We have 14,000 critical CVEs unpatched, a CVSS average of 8.4, and our cloud workload misconfigurations have increased by 20%”

Not actionable for the business

The Board Speaks in Dollars

"What is our mathematical probability of a catastrophic financial loss this quarter, and is it fully covered by our cyber insurance policy?"

Missing empirical data

The Legacy FAIR Problem

The FAIR framework is mathematically sound, but universally fails in practice because it is **starved of operational data.** It relies on manual estimates rather than continuous, real-time telemetry from the endpoints.

Qualys ROCon 26 The Risk Operations Conference EMEA

Cyber Risk Quantification from TruRisk score

The **Controls** and their **Effectiveness** are the common bridge between actual Cyber Risk (**TruRisk**) and the **Financial impact** on the business.

Core Capabilities

TruRisk score cohort to Control effectiveness

Financial loss cohort due to control effectiveness

How We Do It: The Bridge

Cyber Risk
(TruRisk Cohort)

Controls Effectiveness

Financial Impact
(Public Data & Loss Prob.)

"Instead of abstract guessing, we use the **same customer base cohort** and their public data to **map real TruRisk scores to actual probability of financial loss.**

Qualys ROCon 26 The Risk Operations Conference EMEA

A Change in Language

Moving from technical jargon to business risk context.

Attack Surface/CTEM

- 150K CVEs, 78K CIS misconfigs, 51K EASM exposures (risk prioritized).
- Zero-day heard of; we have a critical vulnerability.
- Debt of 12K patches.

Focuses on technical counting

Risk Surface/ROC (ETM - CRQ)

- Payment Gateway (value of $12M/year at risk.
- We have validated 13 ransomware exposures, which require 2 high reliability remediations
- Need to invest in a $100/year tool for continuous risk reduction for Payment gateway

Focuses on business outcomes

Security at Machine Speed. Your Audit?

Qualys ROCon 26 The Risk Operations Conference EMEA

The Real-World Audit Drag

40%

Security Team Burnout

Of highly-paid security engineering time is wasted manually collecting screenshots and evidence for auditors.

82%

Point-in-Time Failures

Of organizations rely on static spreadsheet assessments, meaning they fall out of compliance the day the auditor leaves.

Legacy GRC

By the time your audit report is ready, your evidence is already stale

Audit at Questionnaire speed

SaaS Compliance Tools

Great at checking basic policy boxes, but lacks operational evidence (why!). Technical evidence mapping is still hard!

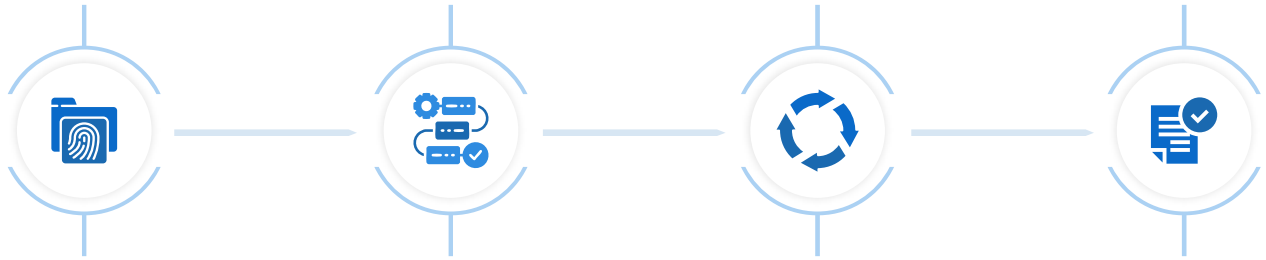
No technical continuous control evidence

Qualys ROCon 26 The Risk Operations Conference EMEA

ETM Audit: Continuous Audit Readiness

Extending ETM's power for continuous audit-readiness

The Autonomous Evidence Engine, extended with ETM



Single Source of Truth for Cyber Risk & Audit

The exact same asset & exposure context for compliance

Qualys ROCon 26 The Risk Operations Conference EMEA

UK NCSC Board Toolkit

How the Qualys ETM platform directly maps to and comprehensively addresses the UK National Cyber Security Centre's directives for corporate boards.

Mods 1, 2 & 3

Governance & Culture

CRQ & Financial Impact

Mods 4

Establishing a Baseline

Asset Criticality (ACS)

Mods 5

Threat Landscape

TruLens Benchmarking

Mods 6

Cyber Risk Management

TruRisk Prioritization

Mods 7

Technical Measures

Zero-Touch Automation

Mods 8

Suppliers & Partners

3rd-Party Consolidation

Mods 9

Planning for Cyber Incidents

TruConfirm & ROC Automation

Demo

Question isn't whether your program becomes autonomous, Question is when does it.

Qualys ROCon 26
The Risk Operations Conference
EMEA

3 Measurable Outcomes This Quarter

01

Stop spending on ghosts

How: Agent Val + TruConfirm on top 20 exposures.

Measure
>95% are noise — know your **validated risk**

02

Get below 18-day Window of Exploitation

How: TruRisk Eliminate + AI pre-screens patch wave.

Measure
Target: **AWE** <18 days within 30 days.

03

Walk into board with a number

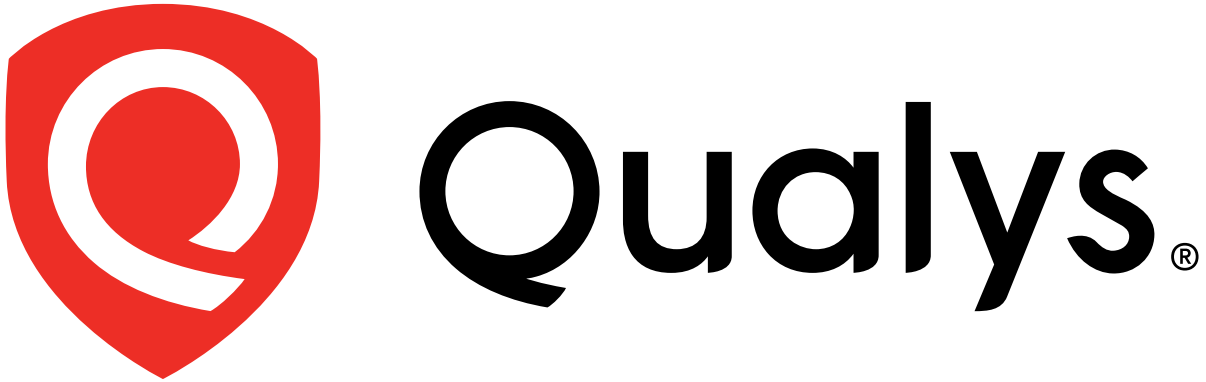
How: Run CRQ on TruRisk. Board-ready in one coffee.

Measure
show **TruRisk for a business unit**

Qualys ROCon 26
The Risk Operations Conference
EMEA

Thank You!




Qualys®

Qualys

ROCon 26

The Risk Operations Conference

EMEA