Qualys ROCon 26
The Risk Operations Conference
EMEA

From Proven Risk Management To Cloud and Container Resilience



Qualys ROCon 26
The Risk Operations Conference
EMEA



Abhinav Mishra
Director of Product Management
Qualys Kubernetes & Containers Security



Matthew Campbell
Senior Security Solutions Architect

Key Takeaways

Qualys ROCon 26 The Risk Operations Conference EMEA



01 **The Problem:** Cloud Has Changed The Scale Of Risk

02 **The Shift:** Need To Move From Alerts To Resilience

03 4 Requirements For Cloud & Container Resiliency

04 How TotalCloud Solves For These Requirements

AI Is Exploding The Cloud Attack Surface

Qualys ROCon 26 The Risk Operations Conference EMEA

Workloads, agents, copilots, and auto-scaled clusters now generate risk signals at a pace no human team was sized to handle.



VMs & Servers

Predictable Attack Surface

- Monolithic Architectures
- Limited Attack Paths

Cloud-Native Workloads

The Expanding Attack Surface

- Kubernetes & Containers, Serverless
- Moving Baseline Shaping Risk Surface
- Vulns Owned By Different Teams

AI-Native Applications

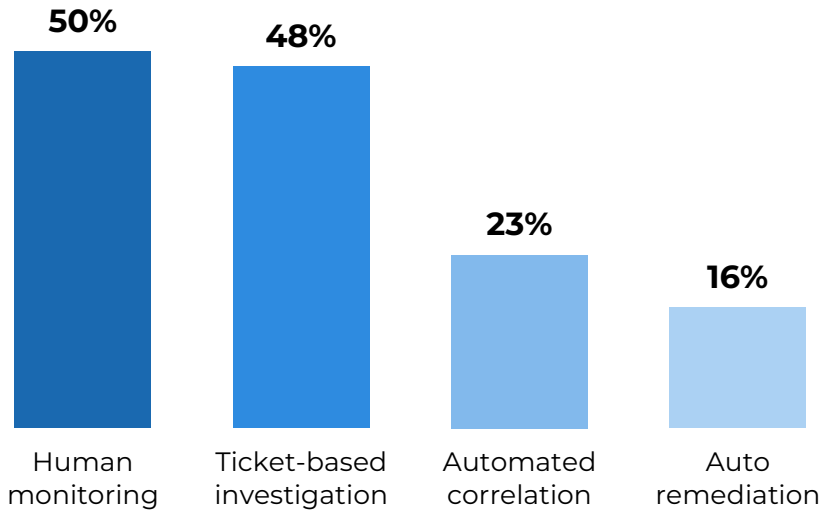
The Unknown Attack Surface

- LLMs and APIs Running on Cloud-Native
- Self-Service Access
- Machine Speed Actions
- Exploitation by Frontier Models At Scale
- Need To Analyze For Runtime Behavior

Human-Driven Security In The Frontier Model Era Will Not Scale

Qualys ROCon 26
The Risk Operations Conference
EMEA

AI is scaling exploit volume faster than human-driven security operations can keep up.







50% Half of Teams Still Rely On Human-Driven Monitoring and Remediation

48% Risk Is Still Process Through Ticket-Based Investigations

23% Minority Using Automated Correlation and Orchestrated Response

16% Automated Remediation Remains Exception Not The Norm

Siloed Context In The Agentic AI Era

Solving Cloud Risk Requires Unified Context, Especially in The AI-Era

Qualys ROCon 26 The Risk Operations Conference EMEA



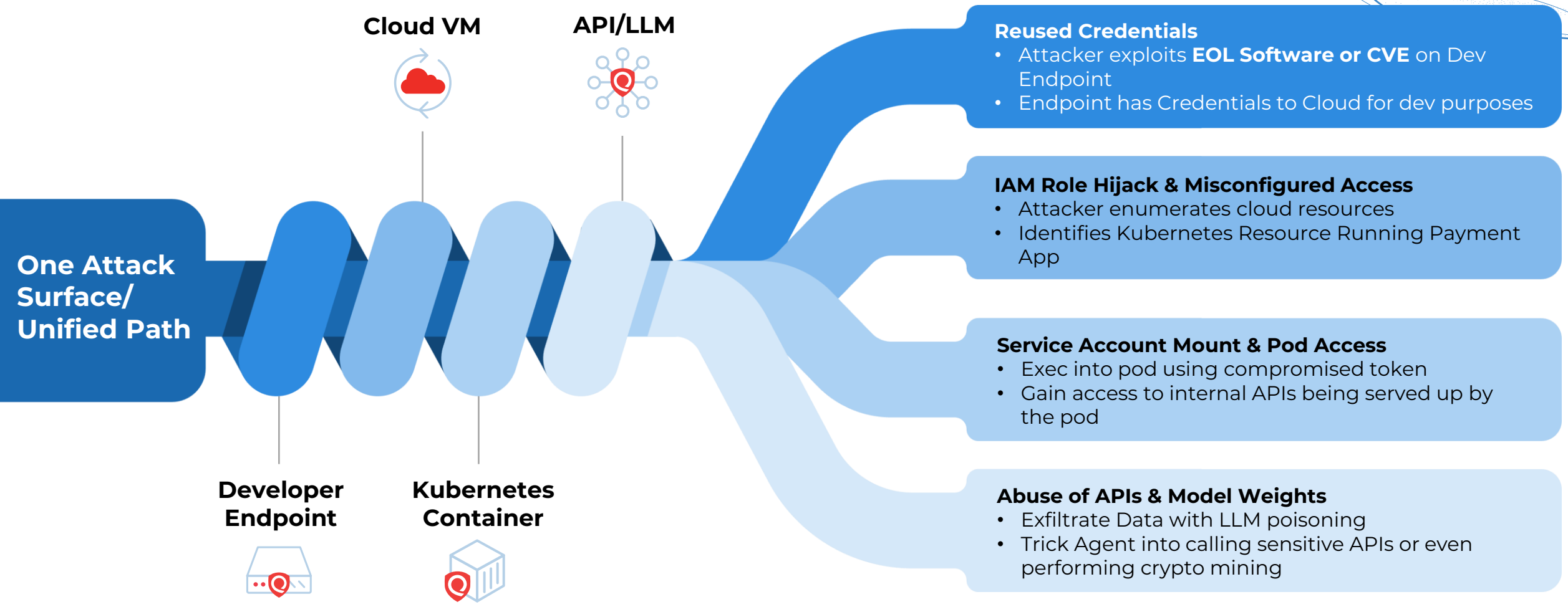
Agents In Point Solutions Lack Visibility and Context

CNAPP-only	Sees cloud posture and configuration. Misses deep app behavior and runtime testing.
API and DAST only	Sees API traffic and endpoints. Misses broader app and infra risk.
Container-only	Sees Kubernetes context. Misses blast radius into the cloud
AI- only	Sees AI workloads and LLM models. Misses the surrounding application and API estate.

For Attackers, It Is One Attack Surface

Your Infrastructure May Be Layered, Your Attack Surface Isn't

Qualys ROCon 26 The Risk Operations Conference EMEA



Reused Credentials
- Attacker exploits **EOL Software or CVE** on Dev Endpoint
- Endpoint has Credentials to Cloud for dev purposes

IAM Role Hijack & Misconfigured Access
- Attacker enumerates cloud resources
- Identifies Kubernetes Resource Running Payment App

Service Account Mount & Pod Access
- Exec into pod using compromised token
- Gain access to internal APIs being served up by the pod

Abuse of APIs & Model Weights
- Exfiltrate Data with LLM poisoning
- Trick Agent into calling sensitive APIs or even performing crypto mining

The Shift

Form Alerts to Resilience.

Qualys ROCon 26 The Risk Operations Conference EMEA

The next generation of cloud security is measured by how fast an environment recovers from risk-not by how loudly it reports it.



YESTERDAY

Multi-Attack Surface Detection, Human Triage

Detections and risks flagged from point tools

Humans validated ticketing & triage

NOW

Unified Attack Surface Detection, Autonomous Detection & Remediation

Agents work automatically to remediate risk across the entire attack surface.

Humans involved as necessary



4 Requirements For Cloud & Container Resiliency

Qualys ROCon 26 The Risk Operations Conference EMEA

Cloud native organizations have a new set of concerns moving beyond basic visibility:

01

Full Stack Posture Discovery and Context

Majority of AI runs on cloud and containers. Combine full stack context to discover unknown risk

02

Exploit Validated Workload Protection & Attack Paths

Prioritizes and Validates Real Attack Paths Not Theoretical Ones which are problematic in the cloud

03

Runtime-Powered Threat Detection & Response

Because AI now powers existing and new threat actors and defense-in-depth is required in the new age of AI

04

Autonomous Remediation From Code to Cloud

Because remediation needs to move from manual ticketing to automatic patching & fixing to deal with cloud & AI Scale

Qualys ROCon 26
The Risk Operations Conference
EMEA

How TotalCloud Enables Cloud & Container Resiliency

Supercharging Hyper Risk Operations for Cloud

Qualys Is Built For The Next Wave of AI-Based Exploitation

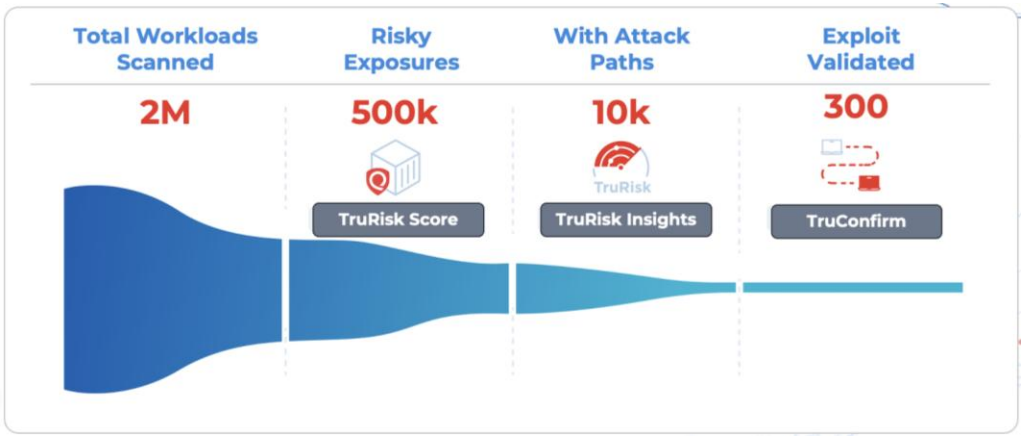
Qualys ROCon 26 The Risk Operations Conference EMEA

Full Stack Discovery

- Flex Scanning – Agent & Agentless
- Full Stack Discovery – Cloud, API, AI
- Code To Runtime Context

Discover Your Interconnected Attack Surface

Exploit-Validated Risk Prioritization



Focus on the few risks that are actual exploits with agentic powered exploit validation

Threat Detection & Response + Autonomous Remediation

Vulnerability Response

Qscanner Auto-Patch From Code To Cloud

Risk Response

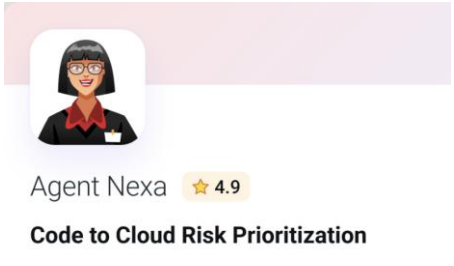
QFlow Powered No-Code Playbooks Across Cloud Stack

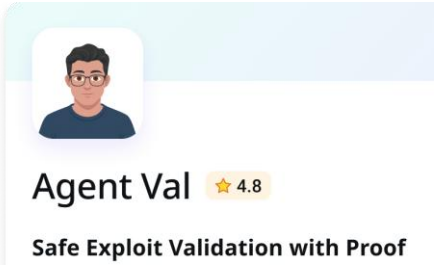
Threat Response

Runtime Powered Containment

Respond In Real-Time. Ticketing and Manual Response Is No Longer An Option





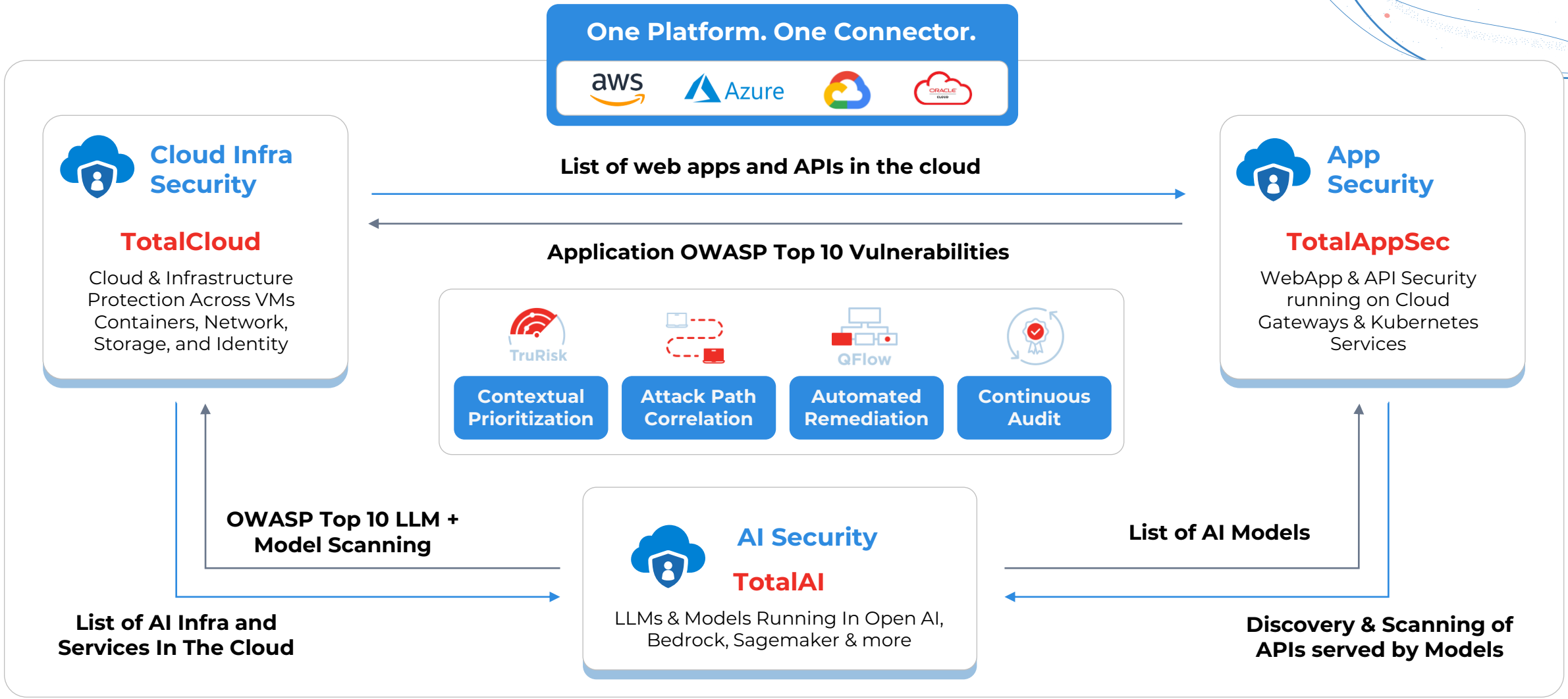




Full Stack Discovery and Context

From Infra To App to AI

Qualys ROCon 26 The Risk Operations Conference EMEA



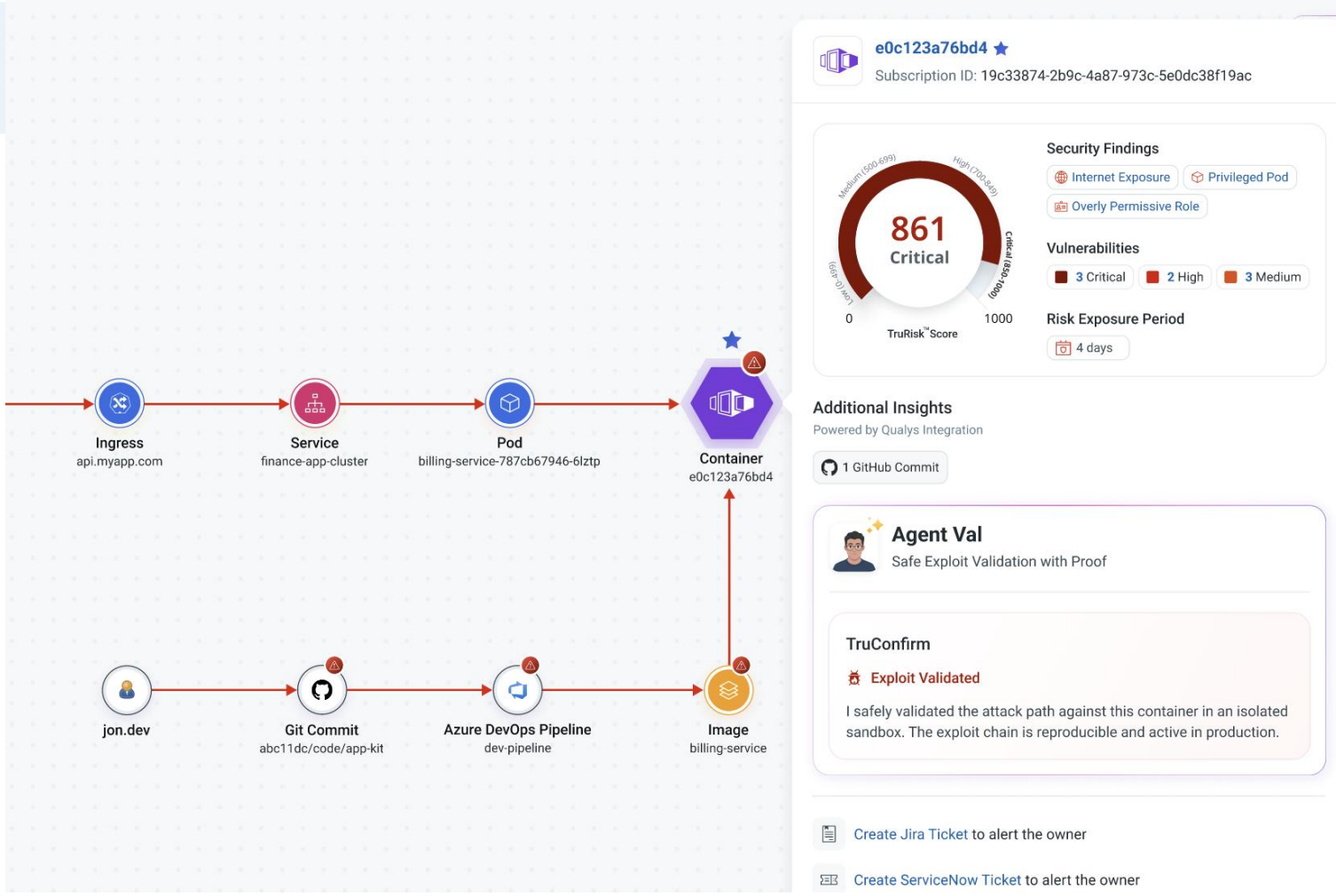
Exploit Validated Risk Prioritization

Turbocharge the risk prioritization with Exploit-Validated **Code to Cloud Attack Paths**

Qualys ROCon 26 The Risk Operations Conference EMEA

Developers receive **prioritized findings and context** to address critical issues **first.**

- **Combined Business, Exposure Runtime and Code Context**
- **Correlate runtime risks** to vulnerable code
- **TruConfirm : Real-Time Exploit Validation**
- **Runtime-Powered:** Correlate Attack Paths With Real-Time Threat Events
- **DSPM Aware:** Correlate Blast Radius To Crown Jewel Storage Assets Which Have Sensitive Data (e.g. PHI or PII)



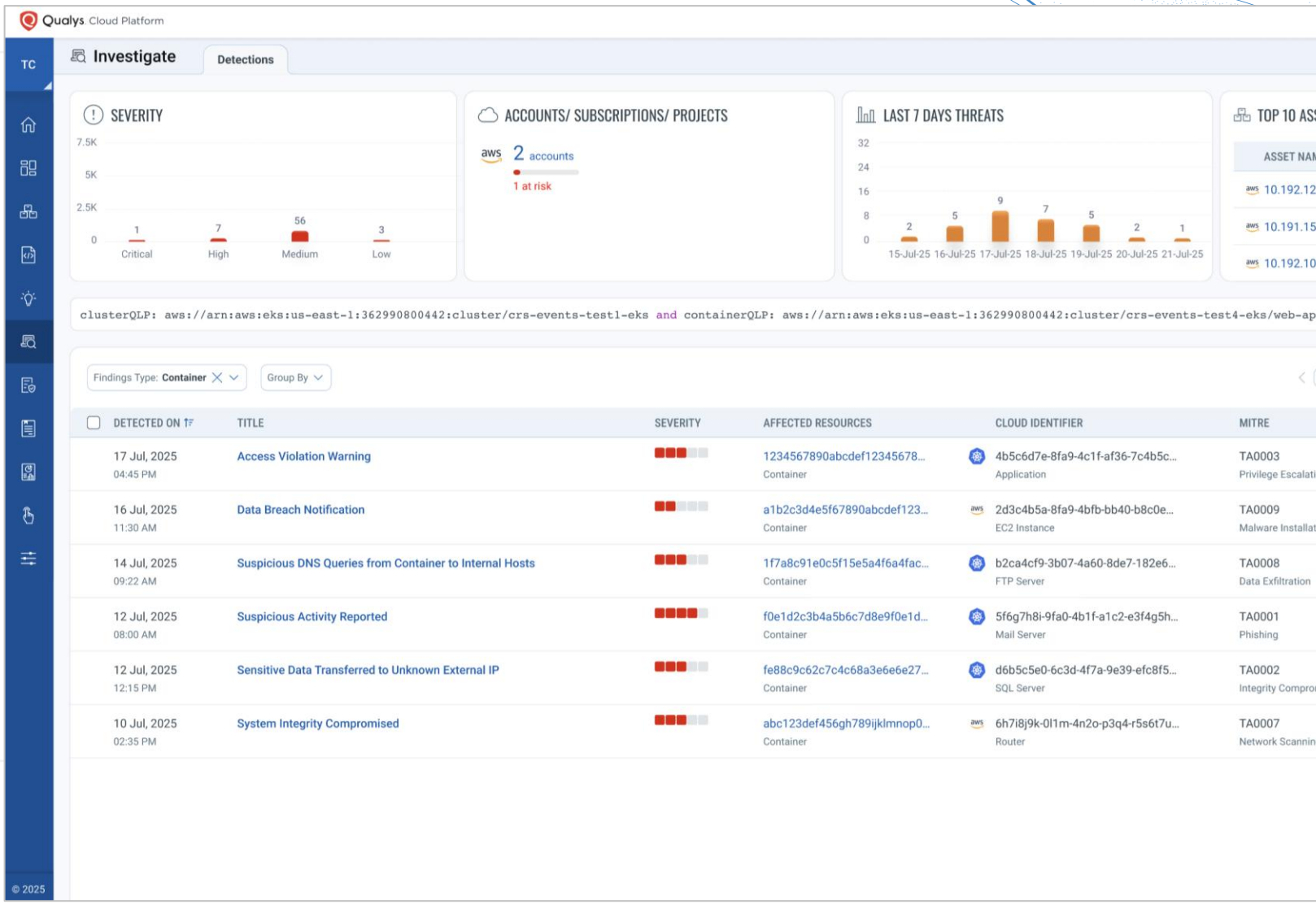
Threat Detection & Response

Build Resilience Against The Unknown With Zero-Day Malware and Threat Detection

Qualys ROCon 26
The Risk Operations Conference
EMEA

- Detect Threats With Agents (eBPF) and Agentlessly (Flow Logs, Cloud Trail, Network Logs)
- **Detect Threats, Anomalies and Drift** Across Process, Network, DNS and File Events
- **Integrated Response Actions:** including process quarantine and file access locking
- Zero-Day Malware Detection To Detect Next-Gen AI Attacks in Supply Chain

Defense-In Depth Against The Unknown



Autonomous Remediation

Validate and Remediate Attack Path Exploitability From Code to Cloud

Qualys ROCon 26 The Risk Operations Conference EMEA



Runtime-Driven Validation & Response

TruConfirm Validates Vulnerability Exploitability Based on Running Processes Detected With Ability To Automatically Enforce with Runtime Sensors.



AI-Powered Code Patching

QScanner Runs as an MCP Server To Perform Direct Auto-Patching of Code In IDEs, CI/CD Pipelines and Code Repositories.



Custom Cloud Playbooks With AI

Leverage LLM Powered Custom Control Creation To Orchestrate Different Remediation Playbooks and Last Mile Customization In The Cloud

TotalCloud CNAPP

A Unified Platform For Cloud & Container Resilience

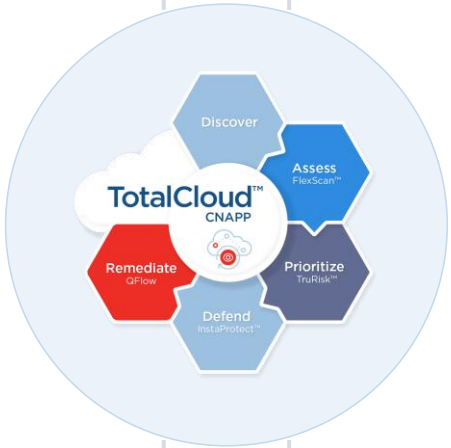
Qualys ROCon 26 The Risk Operations Conference EMEA

Posture Management

CSPM – 230+ Cloud Services Across All 4 Clouds
CIEM – Cloud Identities & Entitlements
DSPM – Databases, Object Storage
ASPM – Applications including WebApps + APIs
AI-SPM – LLMs, MCP Servers and AI Infra

Workload & Runtime Protection

CWP – Flexible Agent/Agentless Scanning
KCS – Secure The Kubernetes & Container Lifecycle From Build to Runtime
AI Workload Protection – Automatic Discovery & Scanning of LLMs and MCP Servers in Cloud



Autonomous Remediation

QFlow – Agentic-Powered Remediation Playbooks & Workflows
Qscanner – Automated Patching of Code in IDEs, Repositories, & CI/CD Pipelines
Eliminate – Patch & Mitigation for Cloud Workloads

Threat Detection & Response

CDR – Deep Learning-Based Threat Detection Across Cloud & Network Events
eBPF Runtime Security – Agent-Based Threat Detection, Response, & Monitoring
Zero-Day Malware– Supply Chain Detection

aws Azure Google Cloud ORACLE Cloud

Qualys ROCon 26
The Risk Operations Conference
EMEA

Why TotalCloud CNAPP

CNAPP + AppSec + AI – Differentiated Bundle

Transparent Pricing Based on Total Asset Count

Qualys ROCon 26 The Risk Operations Conference EMEA

- **Compute Instance**
- **Virtual Machines**
- **Containers & Kubernetes**
- **Web Apps & APIs**
- **Serverless**
- **LLMs & MCP Servers**
- **Cloud Identities (CIEM)**
- **Agents**

Discover Everything. Count What You Scan

Counted across: | AWS | GCP | Azure | OCI | Kubernetes

Discovery → Risk & Exposure Management → Vulnerability Prioritization → Detection & Response → Remediation & Automation

No additional SKUs. No module sprawl. No procurement friction.

Leadership Spotlight

2026 Forrester Wave For CNAPP – Only leader with positive customer feedback

Qualys ROCon 26 The Risk Operations Conference EMEA

FORRESTER®

Key Highlights:

- **Only 1 of 2 vendors** to lead in both agent and agentless Cloud Workload Protection/Vuln Mgmt
- Recognized For Best Transparency and Flexibility In Pricing With Qualys QFlex
- **5/5 top scores** for leading Agentic AI, CSPM, and Container Runtime capabilities powered by robust Enterprise TruRisk Platform



*A halo indicates above-average customer feedback. A double halo indicates that the vendor is a Customer Favorite.

© Forrester Research, Inc. Unauthorized reproduction, citation, or distribution prohibited.

Read The Report Here

TotalCloud Analyst Recognition

Established Leadership and Trust In All Leading Categories

Qualys ROCon 26
The Risk Operations Conference
EMEA



Top 3 Leader
in Forrester Wave CNAPP 2026



CNAPP Marketspace 2025
Top 5 in Capabilities
Recognized as Major Player



Best Cloud Security – SC Awards US & UK





Product and Market Leadership in Cloud Security, CTEM, and Hybrid Cloud Ecosystem

GIGAOM

2025 Leader and Outperformer – CNAPP, CWS, Container Security
2026 Fast Mover - CIEM

Built For AI-Native Tooling & Ecosystems

Qualys ROCon 26 The Risk Operations Conference EMEA

Code
Scan In-Code & IDE

Repository





IDE







Local Dev Scanning – CLI & IDE

Scan Local & Remote Code Repos

MCP Server For Dev Scanning & AI-Driven Auto-Patching

CI/CD
Scan in Pipelines and Registries







Continuous Assessment of Images

Authenticated App & API Testing

Policy-Based Release Gates

Automated & On-Demand Scanning

Deploy & Runtime
Scan Your Production Environments

Cloud



Container



API



Live Attack Surface Discovery

Exploit Validation of Exposures

Business-Prioritized Prioritization

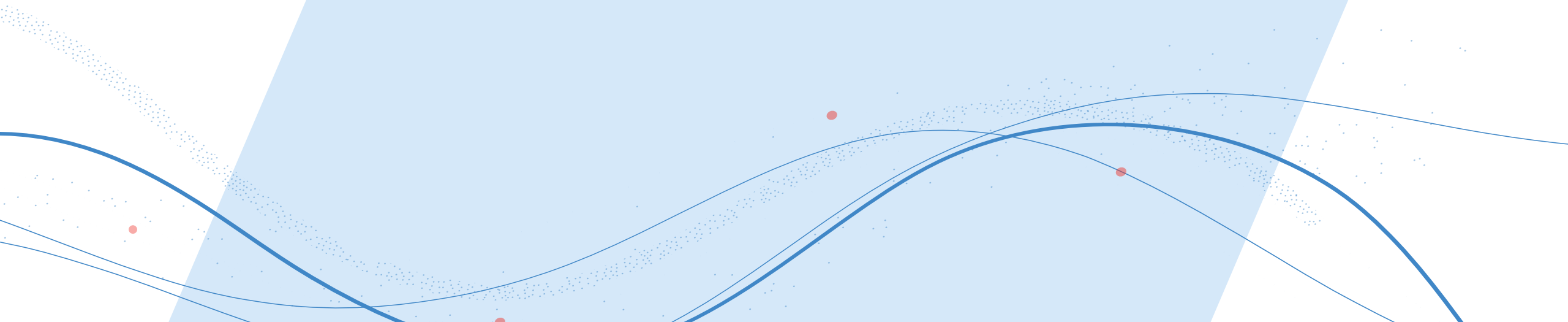
Cloud Workflow Automation For Last-Mile

Vulnerabilities, Secrets, SCA for 9+ Languages (Java, Node, Python, Go. etc)
Scan Anywhere In The Development Lifecycle
Code to Cloud Traceability

Remediate with



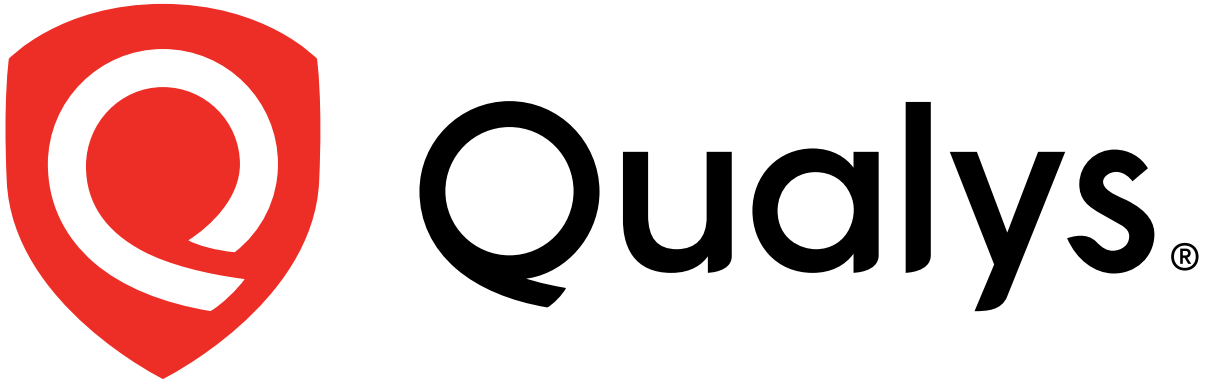
Demo



Qualys ROCon 26
The Risk Operations Conference
EMEA

Thank You!




Qualys®

Qualys

ROCon 26

The Risk Operations Conference

EMEA

Qualys ROCon 26
The Risk Operations Conference
EMEA

Blind Spot Discovery With Agent Vikram

Qualys ROCon 26
The Risk Operations Conference
EMEA

Multi-Cloud Posture & DSPM

Qualys ROCon 26
The Risk Operations Conference
EMEA

Container Security – Auto-TruRisk Scoring & Securing AI Workloads

Qualys ROCon 26
The Risk Operations Conference
EMEA

Attack Path & TruConfirm With Agent Nexa

Qualys ROCon 26
The Risk Operations Conference
EMEA

Autonomous Remediation – QFlow & Developer Auto-Patch

Qualys ROCon 26
The Risk Operations Conference
EMEA

You Asked We Delivered

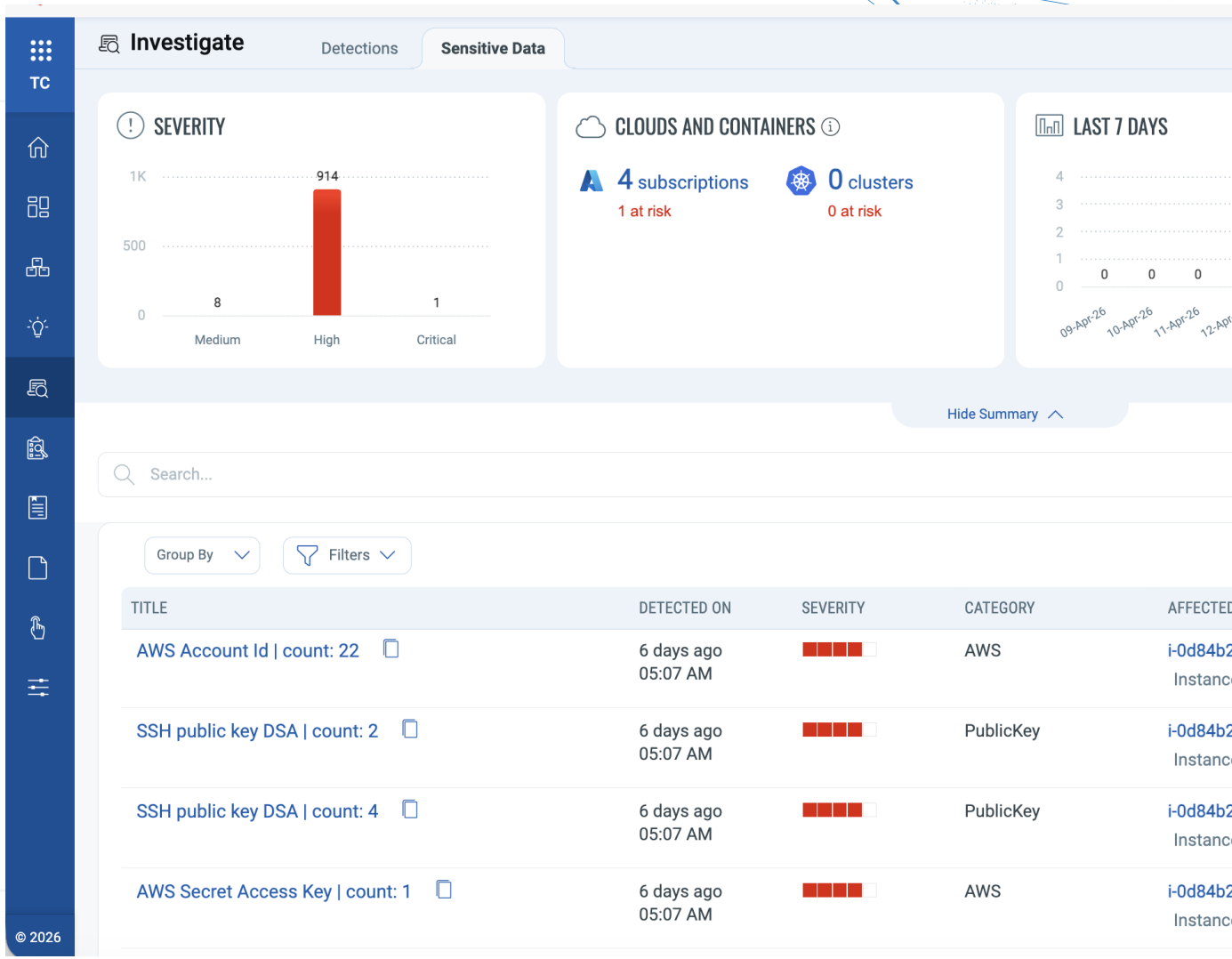
Data Security Posture Management (DSPM)

Auto-Classification and Posture Assessment of Sensitive Data Assets

Qualys ROCon 26
The Risk Operations Conference
EMEA

- Auto-Discovery and Classification of Data Assets for PII, PHI
- Correlate Attack Path Blast Radius To Sensitive Data Assets For Prioritization
- Continuous Compliance Monitoring And Auto-Ticket Creation in SNOW CC/JIRA
- Customizable Sensitive Data Detectors

Protect Your Crown Jewels With Deeper Data Analysis

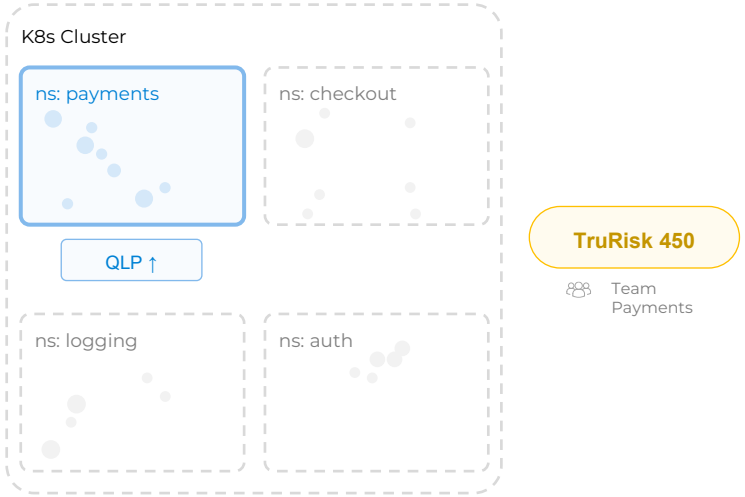


Auto TruRisk Scoring with Ephemeral Workloads

Stable identity, ownership, and risk prioritization across ephemeral containers

Qualys ROCon 26 The Risk Operations Conference EMEA

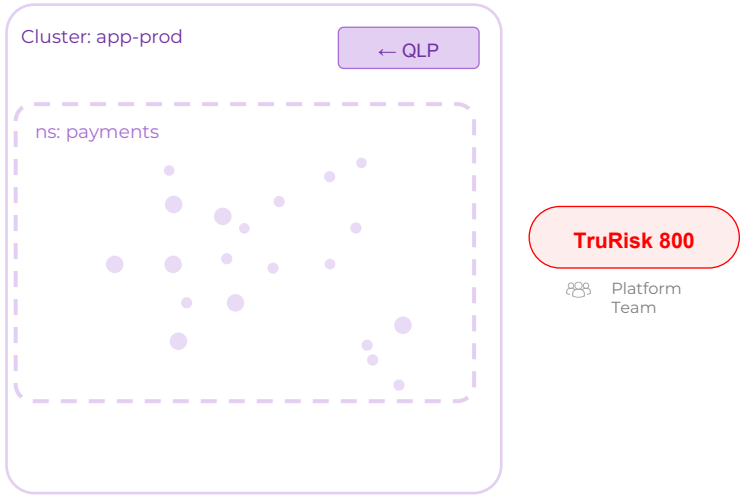
Shared Cluster Environment



QLP at Namespace Level

Ownership: Team-based
Risk grouped by namespace boundaries

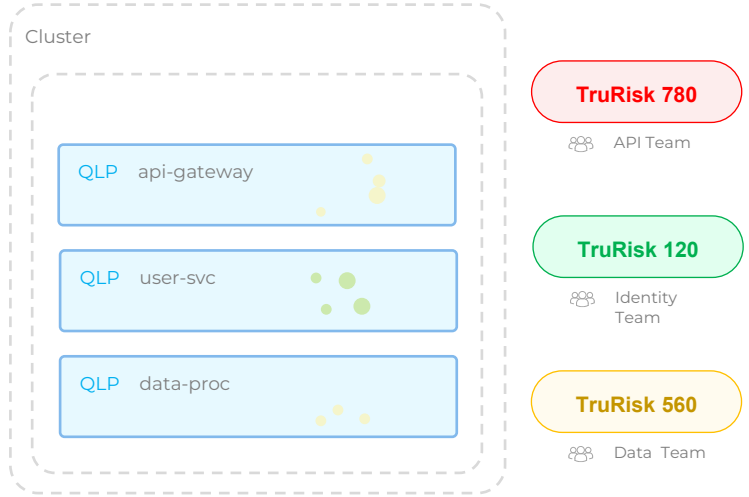
Dedicated Cluster Environment



QLP at Cluster Level

Ownership: Single team
Risk aggregated at cluster boundary

Granular Workload Ownership



QLP at Workload Level

Ownership: Service-level
Fine-grained prioritization

Auto Creation and TruRisk Scoring of Groups That Match Organizational Hierarchies