Qualys.
ROCon 25
The Risk Operations Conference
APAC

When Cloud and Container Risk Meets Code!

Fixing Attack Paths at the Source

Qualys.
ROCon 25
The Risk Operations Conference
APAC

Kunal Modasiya

Senior Vice President, Product Management, GTM and Growth

Anmol Parida

Lead Subject Matter Expert
Cloud, Container, Application Security

Shubham Awasthi

SVP, Information Systems & Security,
Axis Bank, Mumbai

Challenges in Cloud Risk Prioritization

Qualys. ROCon 25
The Risk Operations Conference
APAC

Cloud ROC Team

- Remediated Cloud Risks are resurfacing
- **Increased attack surface** generates more findings
- Managing risks in **ephemeral environments** is always challenging.

Compliance Team

- Always **get exception** requests with no concrete plans to remediate
- Unaddressed compliance issues persist for a long duration
- Security Policies are evolving at a later stage

Developers

- **Many security issues** with no context for prioritization.
- Releases are rejected at a very late stage, delaying product rollouts.
- Security concerns are addressed too late in the development process.

Operationalize

The Risk Operations Center (ROC)

Unified Asset Inventory

Risk Factors Aggregation

Threat Intelligence

Business Context

Risk Prioritization

Risk Response Orchestration

Compliance & Executive Reporting

How will you be

ROC Ready from Day 1

For Your Cloud Deployments

Qualys TotalCloud for Multi-Cloud Environments

The Risk-Minded CNAPP

Qualys ROCon 25
The Risk Operations Conference
APAC

Kubernetes and Container Security (KCS)

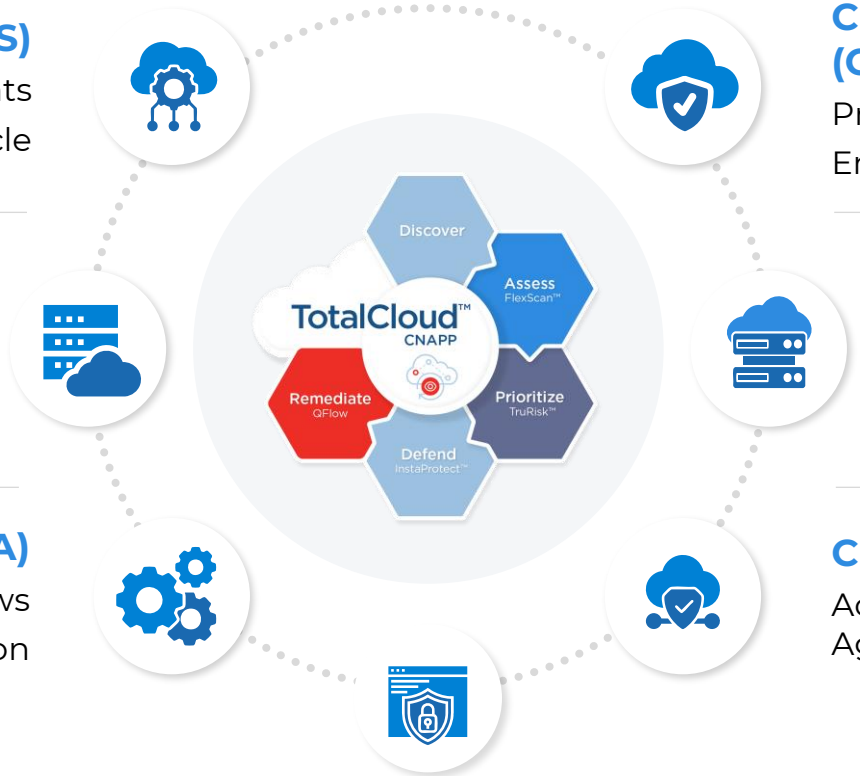
Prioritize Risks In Container Environments
Manage Risk Across The Dev Lifecycle

Cloud Detection & Response (CDR)

Detect Malicious Threats and Malware In Runtime
Integrated Threat Hunting & Anomaly Detection

Cloud Workflow Automation (CWA)

Implement Custom Remediation Workflows
Leverage 200+ Playbooks for Remediation



Cloud Security Posture Management (CSPM)

Prioritize Risk With Attack Path Context
Enforce Compliance From Code To Cloud (IaC)

Cloud Infrastructure and Entitlement Management (CIEM)

Manage Excessive Permissions and Identities
Enforce Least Privilege At Scale

Cloud Workload Protection (CWP)

Achieve Full Vulnerability Coverage With Agent, Agentless, Network, and API Scanning

Application Security (ASPM)

Secure Your Web Apps, APIs, and LLMs

aws Azure Google Cloud ORACLE Cloud

Comprehensive Posture Assessment (CSPM)

Qualys. ROCon 25
The Risk Operations Conference
APAC

Inventory

- Comprehensive, 230+ resource types
- Including cloud native: serverless, storage databases, and more
- Multi-cloud: AWS, Azure, GCP, and OCI

Code to Cloud

- Scan templates like CFT, Terraform, and ARM before deployment
- Run best practices checks
- Detect and prevent misconfigurations before deployment (Shift Left)

Compliance

- 40+ mandates
- Across Industries
- Across geographies
- CIS, PCI, NIST, and more
- Cloud-native frameworks such as AWS FSBP, Azure Policy

Assess, Prioritize, and Monitor

- Determine riskiest misconfigurations
- Best Practices Benchmarks and Compliance frameworks
- Prioritize and generate alerts

Reporting and Remediation

- Service NOW integration
- Jira integration
- Reports and dashboards
- 1 click remediation for many issues
- Automated remediation workflows

Visibility is a Key Part of Risk Management

Comprehensive inventory is crucial for the cloud

Qualys. ROCon 25 The Risk Operations Conference APAC

All environments

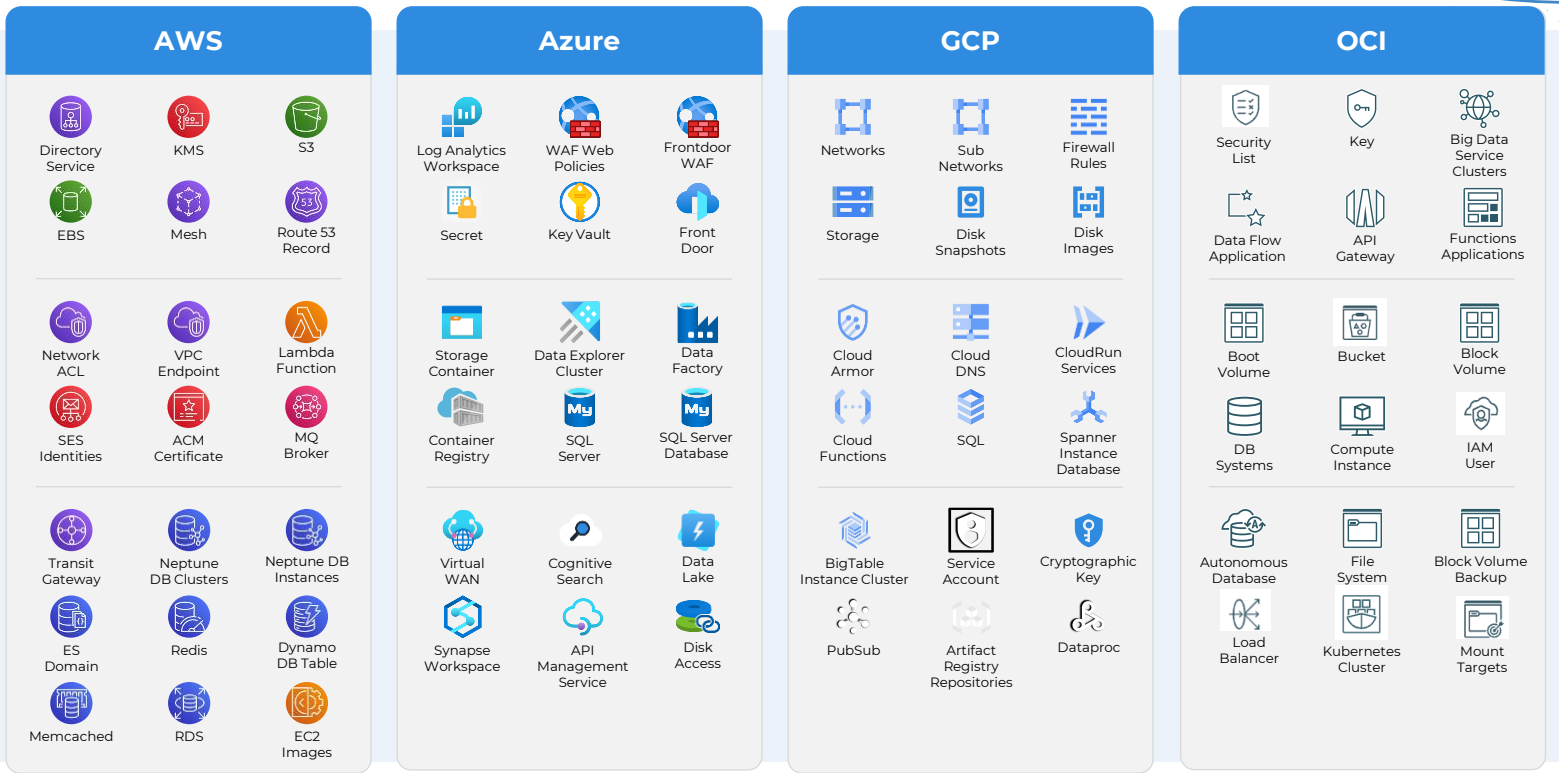
Across all clouds, containers, hybrid workloads

Comprehensive Inventory Including AI Services

Across all inventory and resource types

Accelerated Deployments

Simplified and quick onboarding driving visibility within minutes



aws Azure Google Cloud ORACLE Cloud

TotalCloud CSPM covers ~ 230 services across 4 major cloud providers

TotalCloud CIEM Secures Cloud Identities

Inventory, Hygiene and Risk Assessment

Qualys. ROCon 25 The Risk Operations Conference APAC

Complete **inventory** of identities and entitlements, including users, groups, roles, and policies

Risky identities determined based on analysis. Examples include Administrative privileges, IAM role creation

Risky Identities incorporated into **TruRisk Insights** to further help prioritize risk

TruRisk Insights with CIEM

TruRisk Insights with Identity Issues

CID	INSIGHT TITLE	AFFECTED RESO...
5028	IAM User with privilege escalation or administrative privilege have console acce...	42
5025	Public VM with privilege to create IAM artifacts (User, Group, Role)	41
5031	Public VM allows access to decrypt secrets in secrets manager	41
5026	Security group tampering risk on public and vulnerable VM with 'write' permissio...	40
5029	Public VM with data destructive permissions	40
5030	Public VM with elastic IP hijacking permissions	40

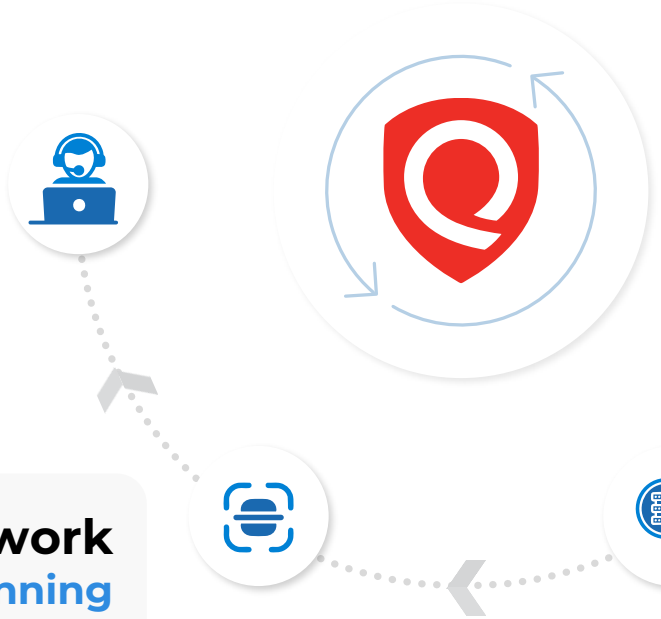
Scale Vulnerability Management with TotalCloud CWP - FlexScan

Continuously monitor cloud workloads, including newly deployed ones

Qualys ROCon 25
The Risk Operations Conference
APAC

Cost-Effective Agentless
Snapshot-Based Assessment

Efficiently capture snapshots and perform vulnerability assessments. Keeps cloud native costs lower.



Shortest Scan Time
API Based Assessment

CSP-provided APIs collect software inventory for results in 10 min

Scans Entire Network
Network Scanning

Quickly and accurately assess for network-related vulnerabilities

Comprehensive Scan
Qualys Agent Scanning

Real-time comprehensive vulnerability, configuration and security assessments

Qualys TotalCloud secures 44 Million cloud workloads across a variety of organizations.

Kubernetes and Container Security

Securing 6.5M Containers and over 800+ Customers

Qualys. ROCon 25 The Risk Operations Conference APAC

Build

Scan Your Dev Builds

GitHub · GitLab · Jenkins · Bamboo · Azure DevOps

- CI/CD Scanning
- Shift-Left Policy Controls
- Context-Driven Shift-Left Security

Release

Scan Your Repositories

sonatype nexus repository · JFrog CONTAINER REGISTRY · Red Hat Quay · HARBOR · dockerhub

- Registry Scanning
- Continuous Assessment of In-Use Images

Deploy

Scan Your Production Environments

Cluster	Host	Serverless
	docker · aws	

- Contextual Risk Analysis w/TruRisk & Attack Path
- Configuration/Compliance Validation
- eBPF Runtime Protection & Threat Detection
- Behavioral Monitoring & Drift Analysis

Code to Cloud Risk Management – Vulnerabilities, Secrets, Polymorphic Malware

Remediate with servicenow · Jira

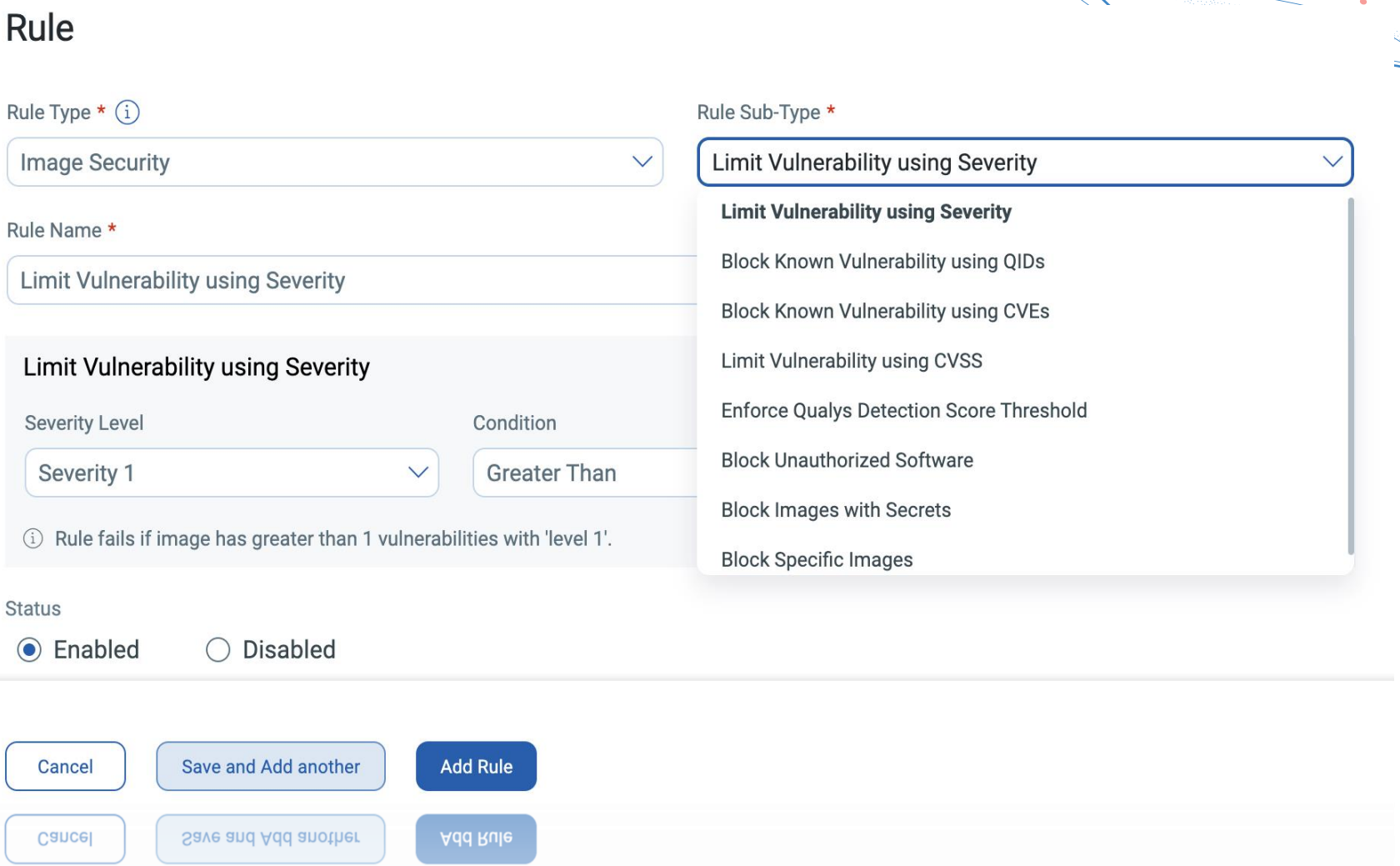
Comprehensive Controls for a Changing World

Qualys. ROCon 25 The Risk Operations Conference APAC

Enforce Secure Gates From Code to Cloud

- Block **deployment** of risky images.
- Fail **build** of risky images.
- Block **commit** of risky code.
- Block **access** to file, network, and process.

Protect Your Baseline — From Build to Runtime



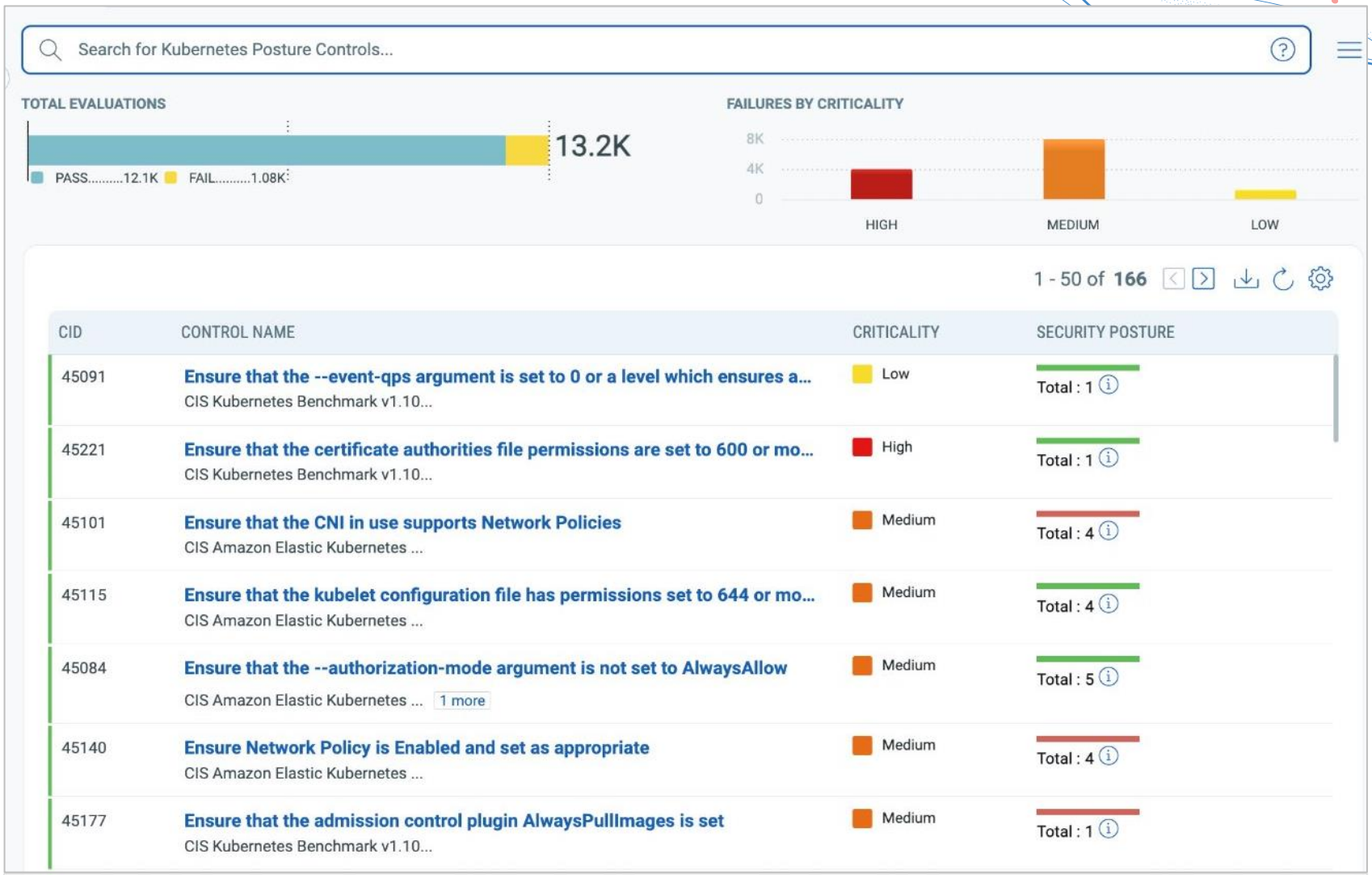
Kubernetes Security Posture Management

Continuous Audit-Readiness for Kubernetes Clusters

Qualys. ROCon 25
The Risk Operations Conference
APAC

- Secure configuration for Kubernetes **control plane.**
- Support for **cloud managed** and **on-prem** Kubernetes.
- Continuous evaluation and **drift** management.
- Protect baseline with **admission controller**.

CIS Benchmark Coverage with 200+ Controls Across Cloud, Kubernetes, and OpenShift Environments



Risk-Minded Detection and Response

Combine Risk Context with Threat Detection

Qualys. ROCon 25
The Risk Operations Conference
APAC

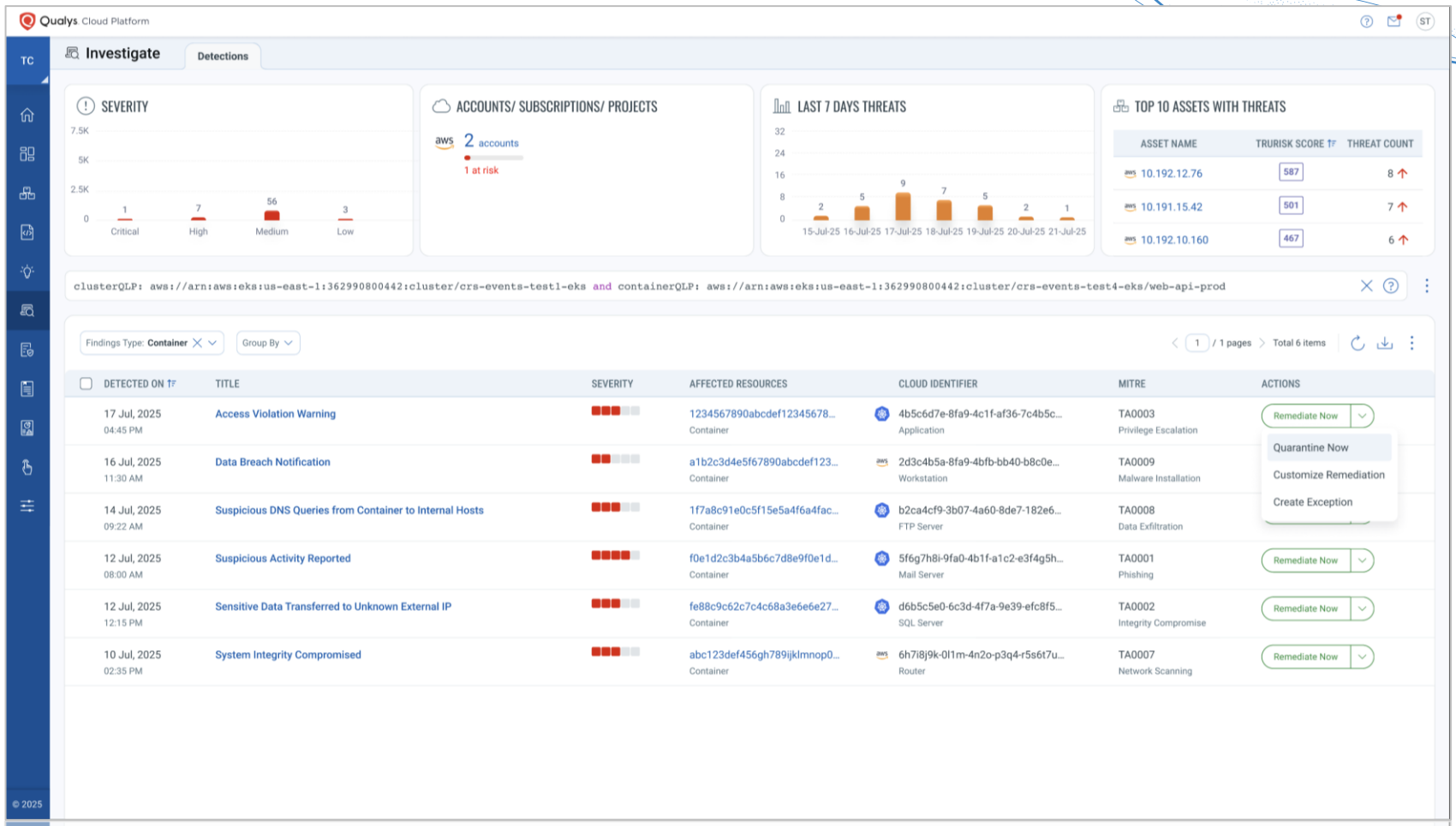
Findings grouped by **Assets**, ranked by Risk.

Confirm whether a vulnerability is **exploited**.

Noise cancelling response with **eBPF policy**.

Prevent exploit with virtual patching.

Turn Threat Detections into Risk-Informed Action



Qualys.
ROCon25
The Risk Operations Conference
APAC

We are always on the
Expressway of Risk Prioritization and Elimination!

Risk Aggregation to Prioritization

With Qualys Enterprise TruRisk Management Platform

Qualys. ROCon 25
The Risk Operations Conference
APAC

Asset Level Risk Score

Complete 360 Context with Threat Intel

TruRisk Score

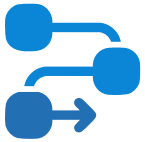
Correlate signals from many source

Toxic Combination

TruRisk Insight

Visualize Attack Path exposure

Blast Radius impact analysis



Attack Path

Visualize Risks with Attack Path

Multi-Dimensional Approach to Cloud Security

Qualys. ROCon 25
The Risk Operations Conference
APAC

Visualize critical resource exposure

Identify blast radius enabling proactive threat analysis

Prioritize risk findings w/ security graph

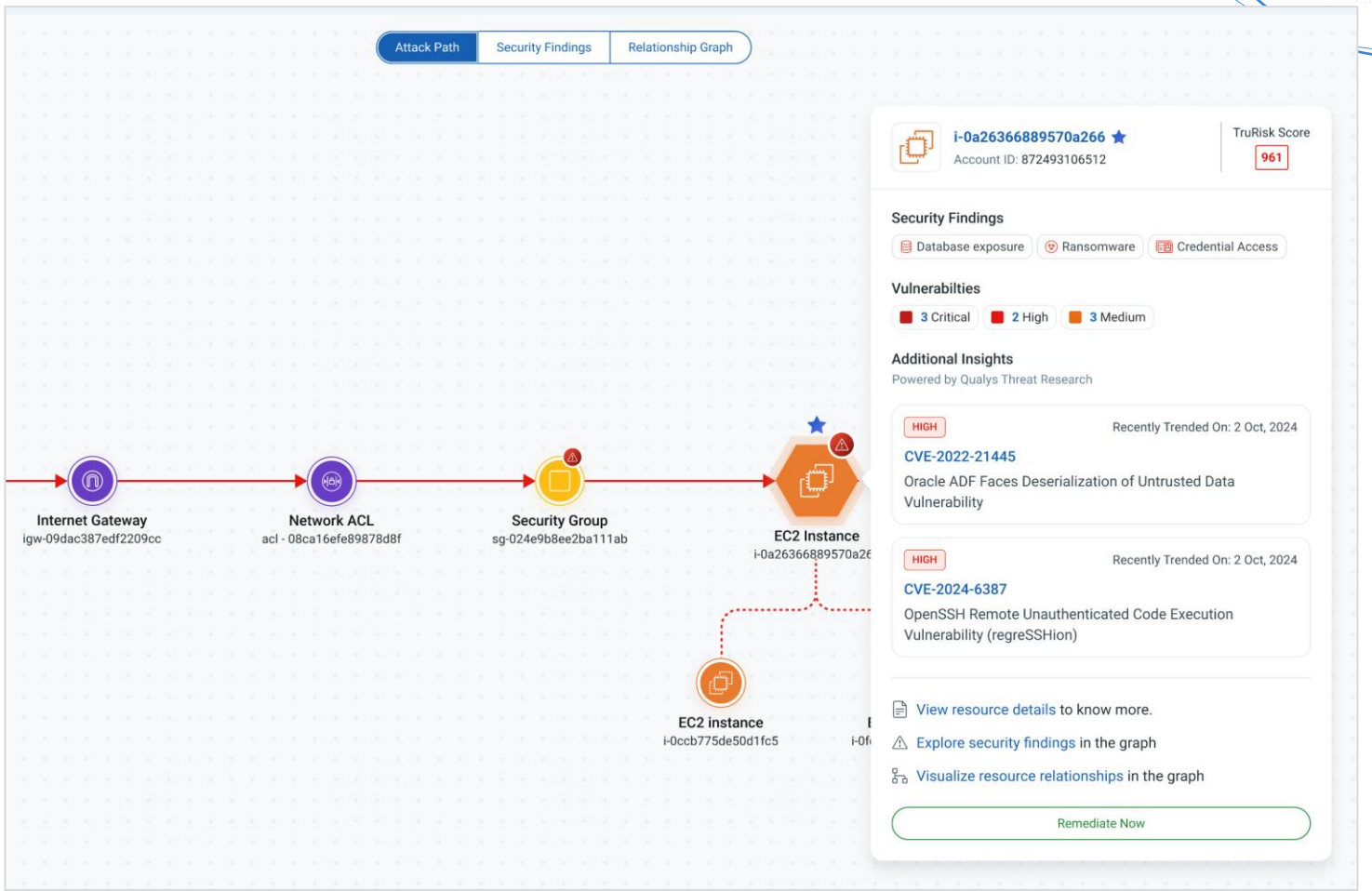
Navigate to important findings on critical resources

Understand resource relationships

Capture communication flows of attached resources

Scale with rapid remediation of risk

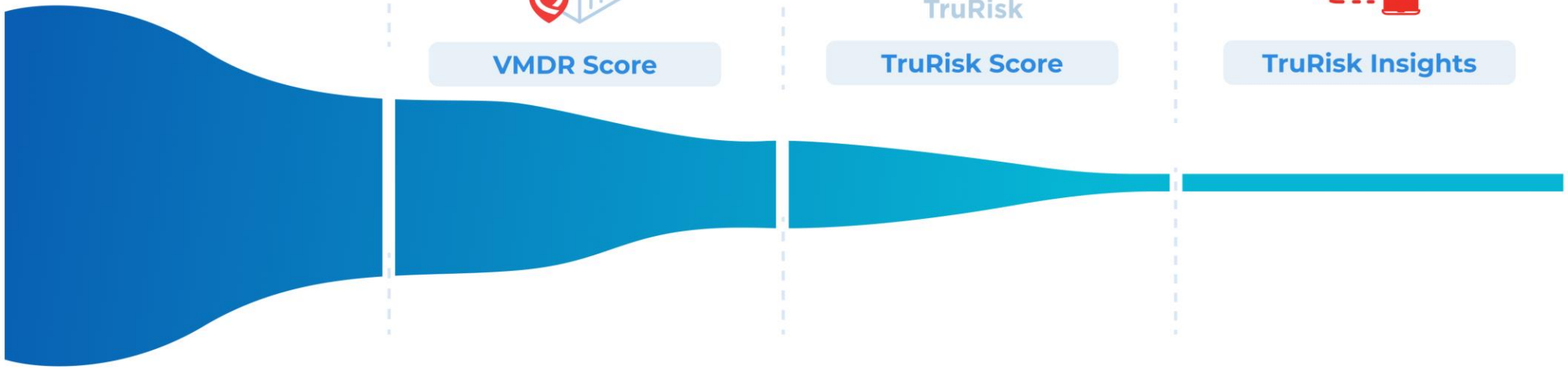
Drive accelerated risk-based prioritized threat remediation



Real-Life Scenario from a Large Financial Customer

Qualys. ROCon 25 The Risk Operations Conference APAC

Total Workloads Scanned	Risky Exposures	Business Critical	With Attack Paths
2M	500k	30k	300
	VMDR Score	TruRisk Score	TruRisk Insights



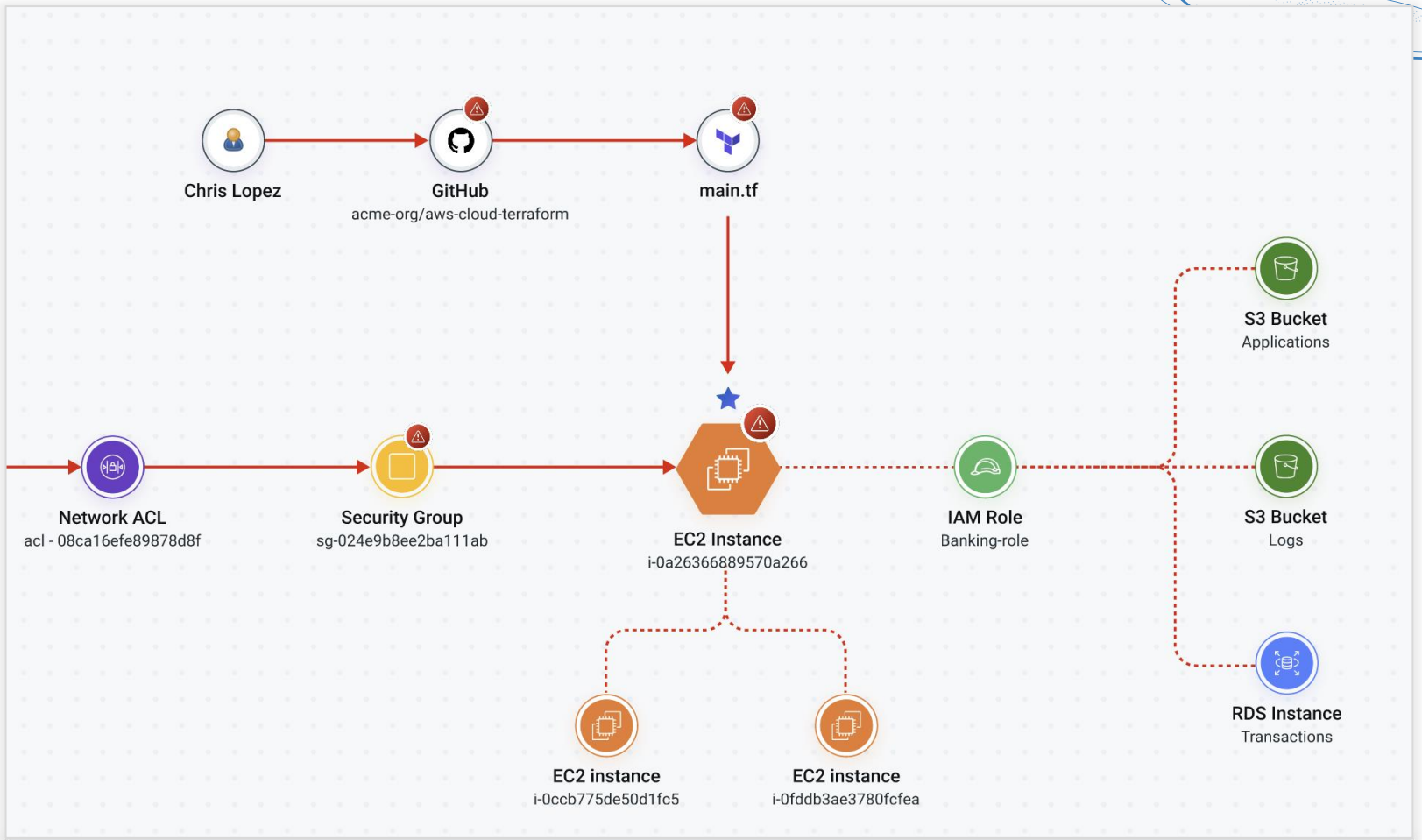
Provide Runtime Risk Context to Code

Turbocharge the risk prioritization with **Code to Cloud Shift Left and Fix Left**

Qualys. ROCon 25
The Risk Operations Conference
APAC

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

- **Empower developers** with proactive, in-workflow security
- **Correlate runtime risks** to vulnerable code
- **Enable scalable,** automated security remediation.
- **Prioritize and resolve cloud risks** using actionable insights.
- **Strengthen security posture** through informed, effective risk management strategies.



Remediate Risks with Cloud Workflow Automation

No Code / Low Code QFlows

Qualys. ROCon 25 The Risk Operations Conference APAC

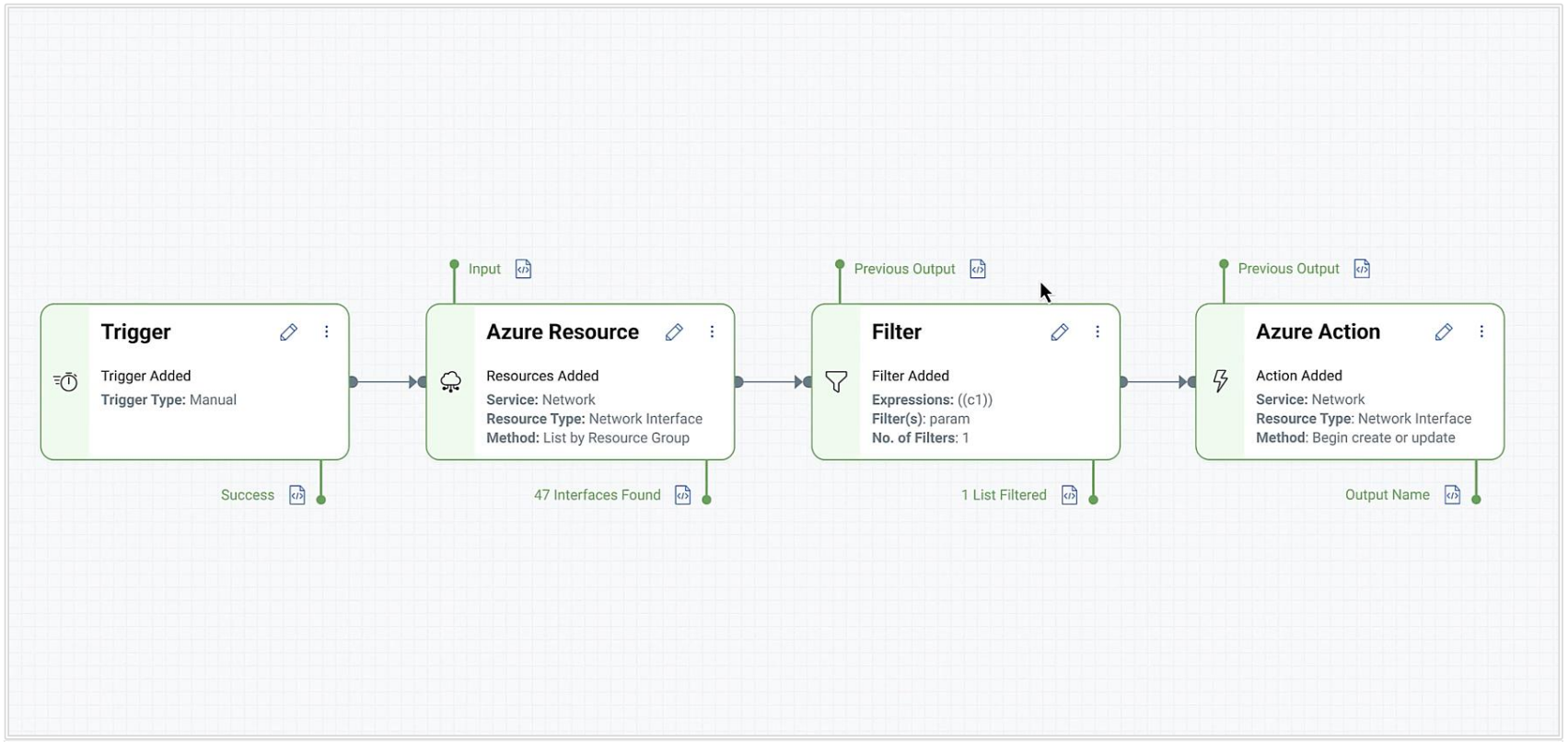
Simplify workflow creation with drag and drop visual nodes and no code

Customize security control workflows and scale inventory discovery

Enrich the security teams by automating efforts to manage security efficiently

Orchestrate remediation workflows and integrate with DevOps and ITSM tools

Over 300 out-of-the-box remediation playbooks



Integrates with ServiceNow

Vulnerability/Misconfiguration Assignment and Remediation

Qualys. ROCon 25
The Risk Operations Conference
APAC

Meet Your Response SLAs

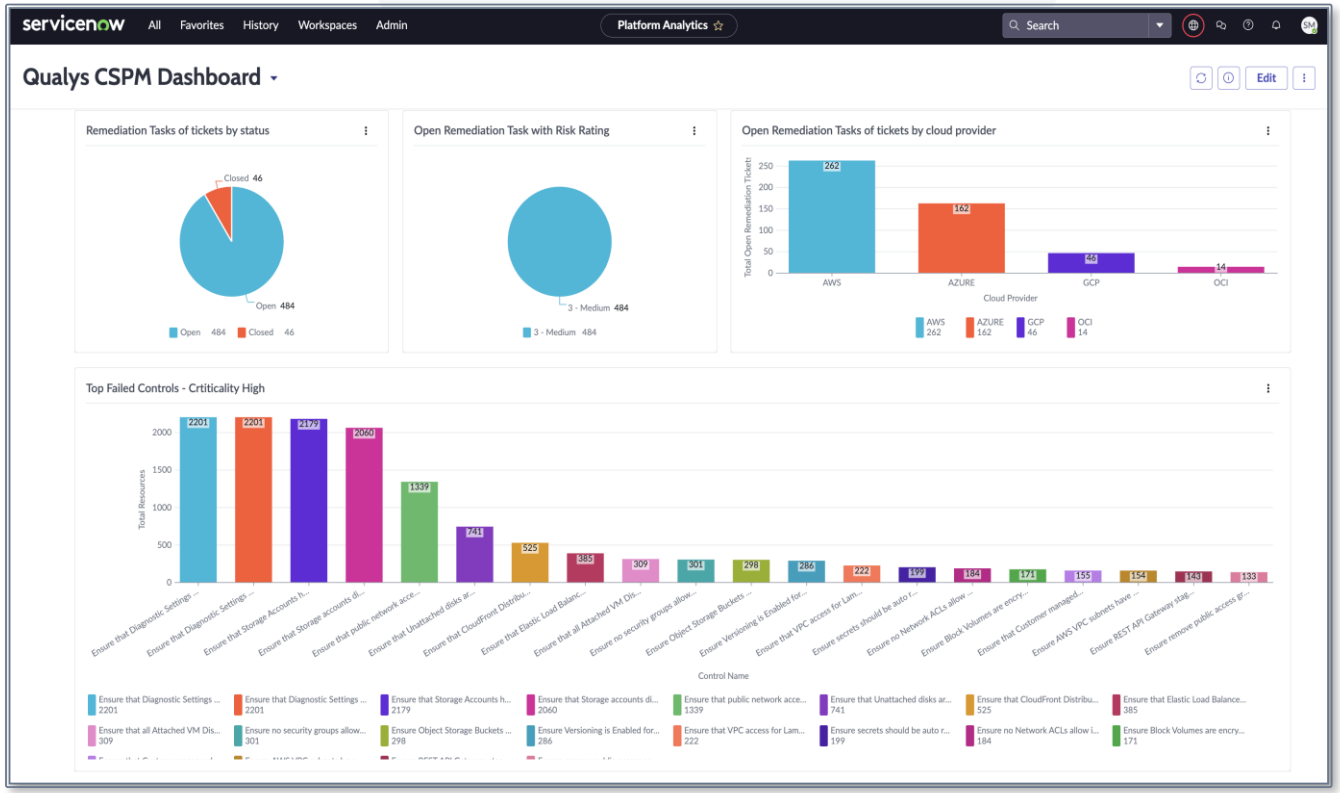
Comprehensive Tracking and Action:
Enable IT team to efficiently track and take timely action.

Automated Vulnerability Assignment:
Assign vulnerability fixes to developers based on asset ownership seamlessly.

Wide Adoption of Key Capabilities:
Enhanced vulnerability and misconfiguration management.

ServiceNow Modules

Vulnerability Response
Container Vulnerability Response
Configuration Compliance



Agent Vikram for TotalCloud

Qualys ROCon 25
The Risk Operations Conference
APAC

< Blog Home

How Agentic AI Helps with Adaptive Cloud Risk Assessment with Agent Vikram

Kunal Modasiya, Senior Vice President, Product Management, GTM and Growth
August 19, 2025 - 4 min read

In fast-moving cloud environments like AWS, security teams face an uncomfortable truth: not every EC2 instance is being scanned, existing tools don't work across a diverse environment that includes long-lived and ephemeral assets, and visibility is never complete. Qualys research found that over 30% of virtual machines have high or critical vulnerabilities, and with blind spots in your scanning, you may miss these critical risks.

Cloud Blind Spots Are Everywhere

The reason not all instances are being scanned is workloads:

- Are missing agents
- Lack SSM integration
- Have encrypted volumes
- Are so ephemeral that they spin up and disappear before traditional tools can catch them

Reliable

Agent Vikram ☆ 5

Adaptive Cloud Risk Assessment

Discovers unknown and unmanaged (for cyber risk) cloud workloads and resources and assesses their risk with FlexScan strategies of agent & agentless scanning in cloud, making sure you never have a cloud asset without visibility into its risk

Core Skills

CWPP | CNAPP | Cloud Security

Projected Agent Impact

100%	6 Mins	22%
Visibility into Cloud Assets	To Define Flexible Scan Strategies in Cloud	Less Cyber Risk in Cloud

Employ

When Cloud Security Meets App Security?

Qualys. ROCon 25 The Risk Operations Conference APAC

List of Web Apps and APIs in the cloud

Location of Applications (regions, servers, PAAS)

Exposure and metadata such as ports, protocols, owners

Application OWASP Top10 Vulnerabilities

Application Owners and Business Use

Application Source Code Location

Cloud Security

TotalCloud

Discover and scan all cloud resources, including Compute, Storage, Network, Databases, Web Applications, API gateways, across multi-cloud environments

Application Security

TotalAppSec

Instantly detect and scan APIs and Web Applications for vulnerabilities, malware, and advanced threats using deep learning

TotalCloud Analyst Recognition

Established Leadership and Trust In All Leading Categories

Qualys. ROCon 25 The Risk Operations Conference APAC

Gartner

2024 Voice of The Customer
Strong Performer

IDC

CNAPP Marketspace 2025
Top 5 in Capabilities
Recognized as Major Player

SC awards EUROPE 2025 WINNER

Best Cloud Security (TotalCloud)

Best Vuln Management 3x in a row (VMDR)

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

2025 Leader and Outperformer in CNAPP, Workload and Container Security

Qualys.
ROCon 25
The Risk Operations Conference
APAC

Customer Success Story

A Decade of Innovation and Protection with Qualys!

Cloud Agents for VAPT Automation

- **Over 95% deployment success** across multi-cloud platforms
- **One agent, one platform**, simplifies cloud security operations

Proactive Alerts for Public Exposures

- **Instant notification** of externally exposed assets
- **Reduced escalations** significantly, improved security posture

Risk Prioritization with TruRisk

- **Six Sigma–accurate** findings
- **Powered by Threat Feeds** from authorized sources

Cloud Security Posture Elevated

Reduced Blind Spots

- **100% infrastructure is auto-onboarded** to Qualys using Cloud Connectors
- **Auto-scan continuously** with no manual intervention

Audit Ready Reports

- Always prepared for **evolving auditor** and central governance requirements
- Significantly **reduced hours spent** on manual monitoring

Remediation Ready Play

- **Faster and easier** remediation of vulnerabilities
- **Eliminated misconfigs significantly,** improving security posture

What Next?

When extending a cloud security strategy, review all capabilities and deploy the TotalCloud solution

Leverage Qualys Agents for API Discovery – Easy onboarding for AppSec team

Expand the footprints to container security to secure unknowns

Attack Paths to Assess the impact beyond the internet exposure – know blast radius and act

Qualys. ROCon 25
The Risk Operations Conference
APAC

Demo - Code to Cloud

Recipe to Fix Attack Paths at the Source