

RiskOps For Containers at Scale

Turning Continuous Risk into
Continuous Security





Abhishek R. Singh

Vice President, Product Management
TotalCloud Container Security, CDR,
and SaaS DR



Antonio Anderson

VP, Information Security & IT
Somos



Abhinav Mishra

Director, Product Management,
TotalCloud Kubernetes and Container
Security

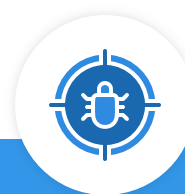
“
Now do you stop with that size
and then keep it up for 180
minutes of creation?
always hanging?”

— Kubernetes Security
— Gartner
Report 2025

”

Challenges with Container RiskOps

Short-lived Assets, Persistent Risk



Explosive Arrival Rate

Excessive vulnerabilities and alerts create an overwhelming influx of findings



Shift Left Isn't Enough

Unclear **ownership** and rebuilt images break **fixes**, continuing, delaying, over elimination and closure

Fix Left is the New Mantra



Moving Risk Baseline

Ephemeral **workloads** and new **detections** constantly reshape your risk surface, making metrics unstable

Get ROC Ready for Containers

**From Noisy Attack
Surface to Quantified
Risk Surface**



**TruRisk
Score**

**Detect Incident Worthy
Toxic Risk Combinations
for Immediate Action**



**TruRisk
Insight**

**Visualize and Break Risk
Chains with Guided
Remediation**

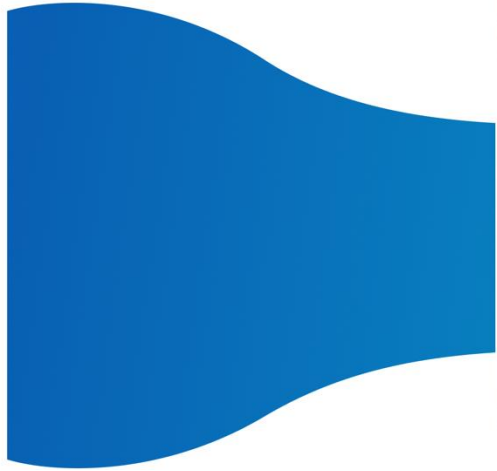


**Attack
Path**

Real-Life Scenario from a Large Financial Customer

Total Containers
Scanned

2M



Complete Build To Runtime Security

Securing 6.5M Containers and over 800+ Customers

Build

Scan Your Dev Builds



CI/CD Scanning

Shift-Left Policy Controls

Context-Driven Shift-Left Security

Release

Scan Your Repositories



Registry Scanning

Continuous Assessment of In-Use Images

Deploy

Scan Your Production Environments

Cluster



Host



Serverless



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

Qualys Kubernetes & Containers Security

Your AI-Powered Risk Operations Center for Containers

Quantify risk, remediate with **attack paths** and full **code-to-cloud** context.

01

Agentless Onboarding, Instant Insights

Block risky **code, builds, deployments**, and runtime privileges with **eBPF**

02

Comprehensive Controls for DevSecOps

Enforce **CIS benchmarks** to secure your Kubernetes control plane(s).

03

Secure the Kubernetes Control Plane

Auto-ticketing workflows along with **auto-assignment, EOL/EOS** tracking.

04

Automate Workflows with ServiceNow

Focus on highest-risk assets to cut the noise, **validate exploits**, apply virtual patches

05

Risk-Minded Detection and Response

Agentless for Containers

Frictionless Deployment, Instant Risk Insights



Discover registries, clusters, and serverless.



Zero Agents, Instant **Risk Insights**.



Incident worthy findings with **attack path**.



Complete **code to cloud** context.

Reduce Risk Instantly With Code To Cloud Correlation

Qualys Cloud Platform

Hi Abhinav

You have just configured your 1st connector!

Congratulations! Your Dashboard is ready to roll!

Configuration Inventory Misconfigurations TruRisk Insights Dashboard

aws

- 10 K8s Clusters
- 05 Repos
- 19 Lambda functions
- 16 EKS Fargate
- [View All](#)

- 10 Cloud Misconfigurations
- 05 IAM Users
- [View All](#)

Need Help? [Watch Tutorials](#) [Quick Start Guide](#) [FAQs](#) [Join Community](#) [Blogs](#)

© 2025

Comprehensive Controls for a Changing World

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

Rule

Rule Type * ⓘ

Image Security

Rule Name *

Limit Vulnerability using Severity

Limit Vulnerability using Severity

Severity Level

Severity 1

Condition

Greater Than

ⓘ Rule fails if image has greater than 1 vulnerabilities with 'level 1'.

Status

☒ Enabled

☐ Disabled

Cancel

Save and Add another

Add Rule

Cancel

Save and Add another

Add Rule

Rule Sub-Type *

Limit Vulnerability using Severity

Limit Vulnerability using Severity

Block Known Vulnerability using QIDs

Block Known Vulnerability using CVEs

Limit Vulnerability using CVSS

Enforce Qualys Detection Score Threshold

Block Unauthorized Software

Block Images with Secrets

Block Specific Images

Kubernetes Security Posture Management

Continuous Audit-Readiness for Kubernetes Clusters



Secure configuration for
Kubernetes **control plane**.



Support for **cloud managed** and **on-prem**
Kubernetes.

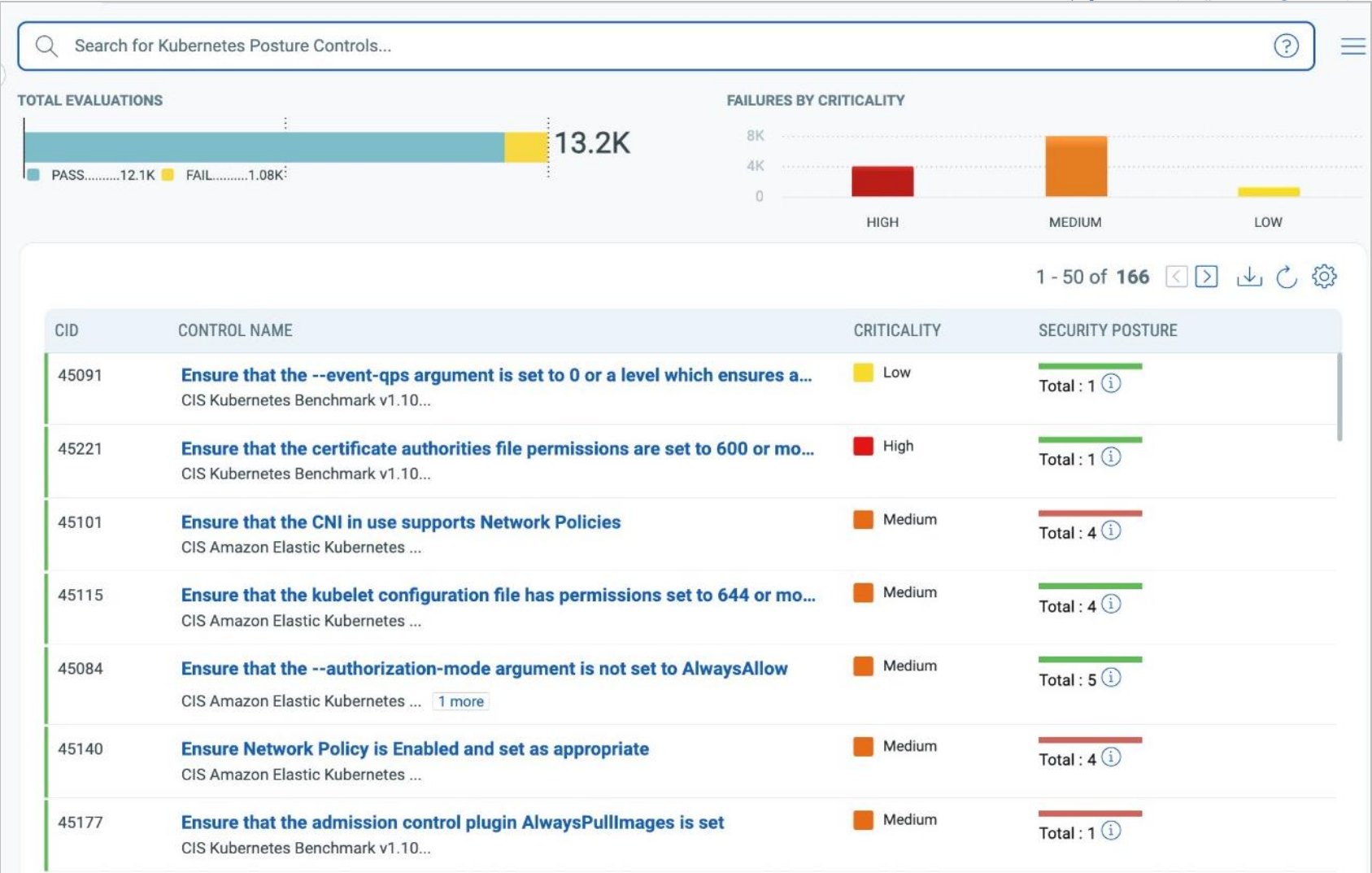


Continuous evaluation
and **drift** management.



Protect baseline with
admission controller.

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



ServiceNow Container Vulnerability Response

Accelerate MTTR With Seamless Ticketing and Automation



Fewer, high-quality tickets that track your **risk** surface.



Automatic ticket **lifecycle** management.

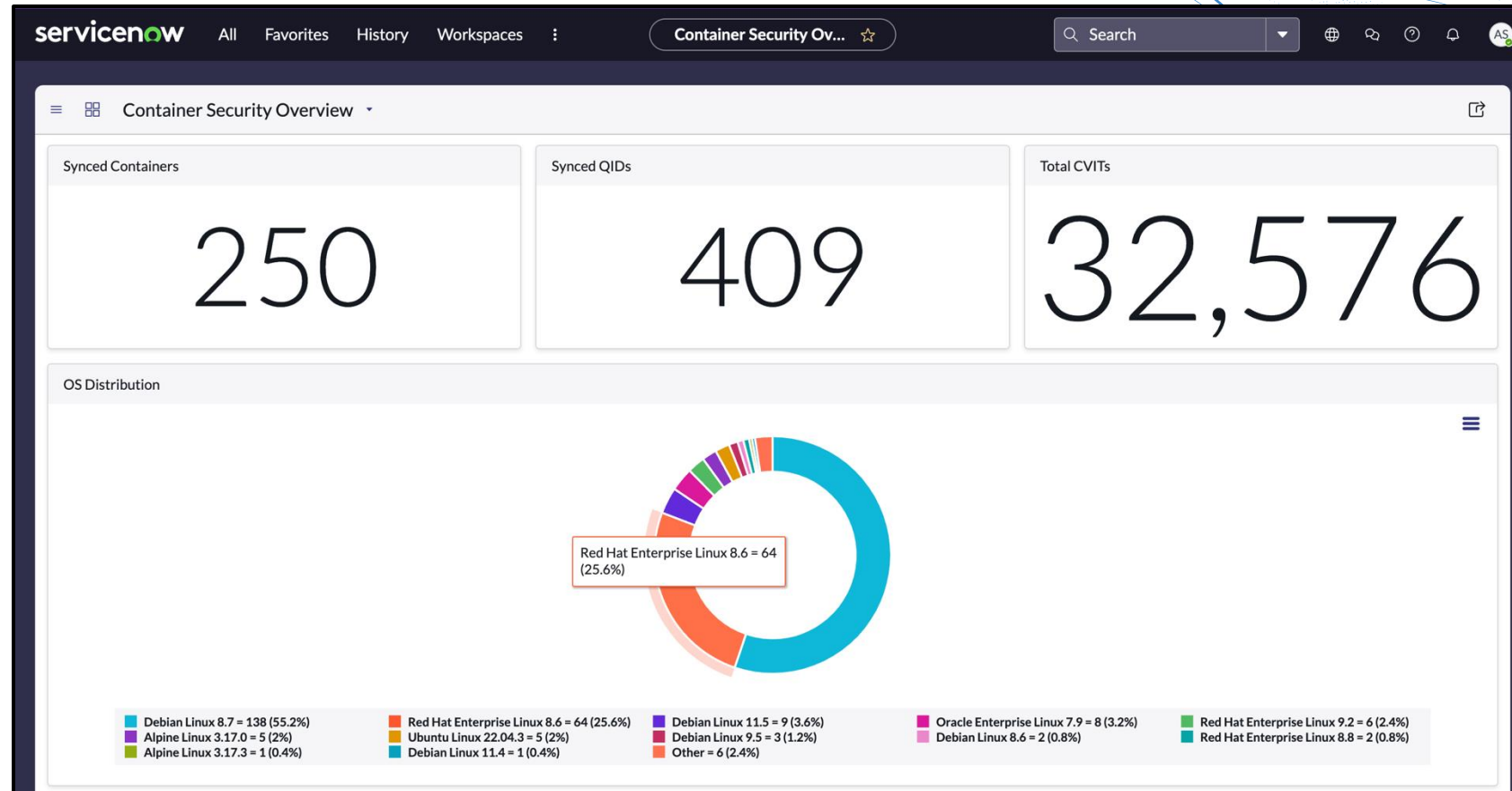


Automatic ticket **assignment** with code to cloud context.



Automatic remediation workflows and **exception** management.

From Manual Ticket Management to Fully Automated Remediation Workflows



Risk-Minded Detection and Response

Combine Risk Context with Threat Detection



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



Confirm whether a vulnerability is **exploited**.

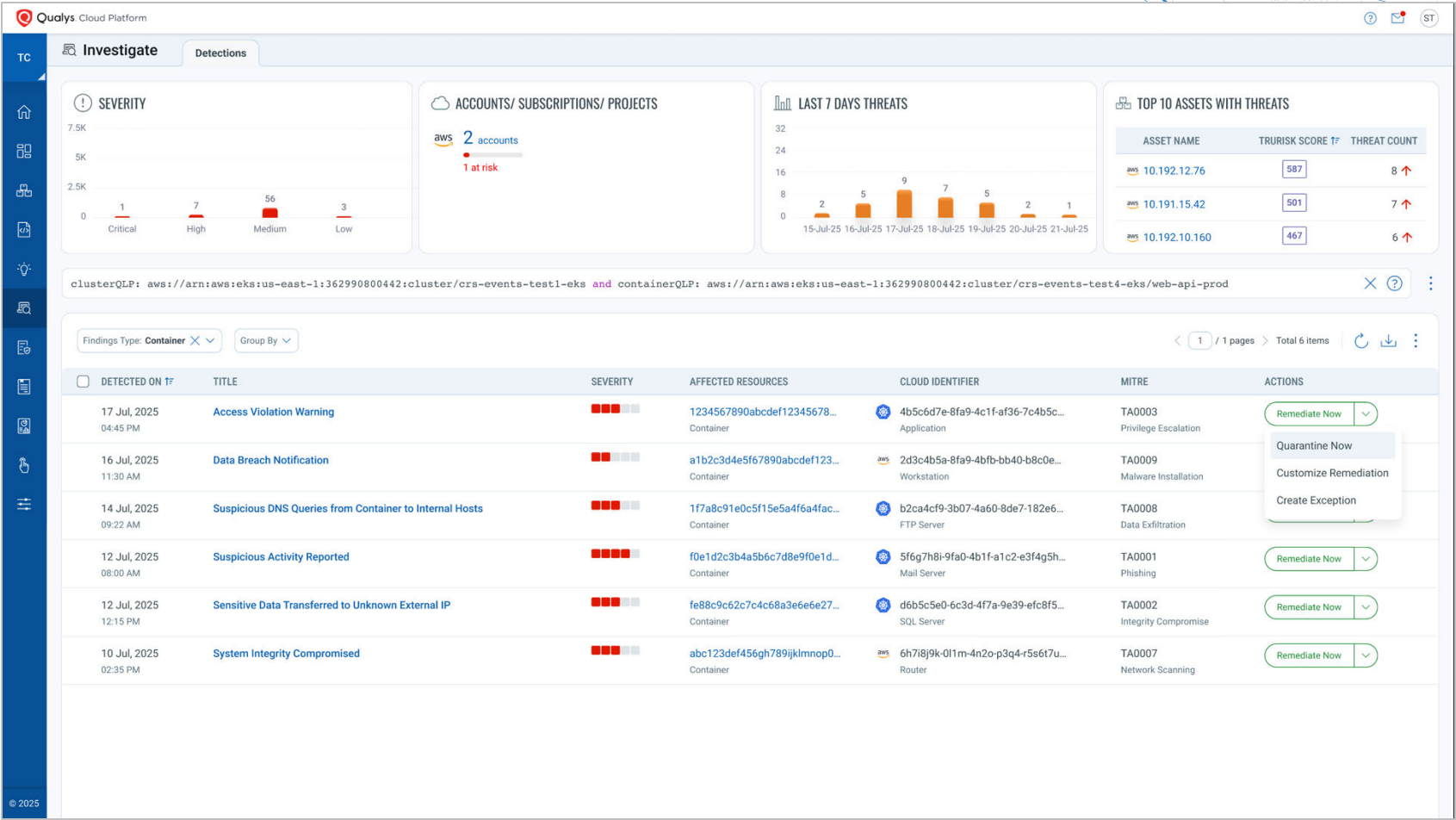


Noise cancelling response with **eBPF policy**.



Prevent exploit with virtual patching.

Turn Threat Detections into Risk-Informed Action



Container FIM for PCI-DSS 4.0 Compliance

Audit Your Sensitive PCI Data Running on Containers



Customize FIM/ FAM Policies



Prioritize investigation with Kubernetes context











Remediate in real time



Out of the box Audit **Reporting**

Stay Audit-Ready for Cloud-Native Workloads – now in Scope for PCI 4.0!

FIM



Events

Event Insights

All Events

Event Review

Ignored

5

Total Events

Search for events...

Last 30 Days

22 Apr

24 Apr

26 Apr

28 Apr

30 Apr

2 May

4 May

6 May

8 May

10 May

12 May

14 May

16 May

18 May

20 May

22 May







Host Based











Scan Based

Container Based

Group by

1 - 5 of 5



TIME	TARGET	ACTION	ACTOR	CONTAINER NAME	SEVERITY
May 6, 2025 04:23 AM	 shadow1 /etc/shadow1	Delete	rm root	nginx 192.168.31.234	
May 6, 2025 04:23 AM	 shadow /etc/shadow	Rename	mv root	nginx 192.168.31.234	
May 6, 2025 04:22 AM	 passwd1 /etc/passwd1	Delete	rm root	nginx 192.168.31.234	
May 6, 2025 04:22 AM	 passwd /etc/passwd	Rename	mv root	nginx 192.168.31.234	
May 6, 2025 04:21 AM	 passwd /etc/passwd	Rename	mv root	sshd 192.168.31.234	

© 2025

3052



You ~~will~~ ~~fail~~ ~~love~~ ~~love~~ ~~MDR~~..
Container Security



+



Consolidating Cloud-Native Workloads Securely with Qualys

October 2025



Antonio Anderson, VP, Information Security & IT



> **Building trust through innovation:**

I lead our Information Security and IT teams with one goal in mind, making sure every digital interaction earns our customers' trust. Security isn't just about protection; it's about confidence in how we do business.

> **Turning security into a business advantage:**

Too often, security is seen as a blocker. I see it as a catalyst. We use it to drive growth, win deals, and create value; because when done right, security accelerates innovation, it doesn't slow it down.

> **Empowering people to make technology work for them:**

I'm passionate about building teams that don't just manage systems; they transform them. When you give smart, motivated people the right tools and trust, they turn challenges into real business impact.

Somos is the Global Provider of Telephone Number Management & Information Services

Telephone Number Administration Services

On behalf of U.S. F.C.C., manages over 7 billion telephone numbers across 1,400+ Service Providers



North American
Number Plan
Administrator



Toll-Free Number
Administrator



Reassigned
Numbers
Administrator

Global Telephone Number Intelligence Solutions

Telephone Number Intelligence for 200+ countries and Identity Management Solutions



Fraud Mitigation,
Compliance &
Data Integrity



Routing
Optimization



Connected
Asset
Management

Business Challenges



Siloed Tools

Fragmented systems create blind spots and inefficiencies.



Too Much Noise

Overwhelming alerts make it hard to focus on real threats.



Poor Prioritization

Lack of threat context leads to wasted remediation effort.



False Positives

Inaccurate findings drain analyst time and reduce trust.

Business Solution



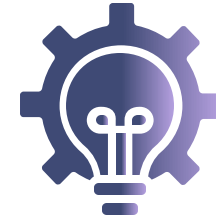
Unified Platform

End-to-end visibility
and streamlined
workflows.



Threat-Informed Prioritization

Focus on vulnerabilities
that truly matter
(QID-driven).



Noise Reduction

Actionable insights,
fewer false positives,
faster response.

Business Outcomes – Key Improvements with Qualys

Enhanced Visibility

Deployed Qualys sensors revealed large numbers of unused container images

Cleanup efforts led to an 80% reduction in clutter, improving focus on active images and vulnerabilities

Streamlined Remediation

Shifted from CVE-based to QID-based vulnerability tracking

Achieved a 90% reduction in duplicate checks, helping engineers clearly see which patches apply to which CVEs

Expanded Fargate Coverage

Previous tools lacked Fargate insights; Qualys enables on-demand scanning

Gained nearly 100% visibility into Fargate images, eliminating blind spots

What's Next



Advancing Container Security

Excited about agentless approaches for Lambda and Fargate at scale, plus EOL/EOS integration and WAS support to improve API visibility and remediation ownership.



Risk-Driven Approach

Moving toward TruRisk-based CDR to rank assets with attached findings, reducing alert fatigue.



Shift-Left & Continuous Assessment

Expanding CI/CD/dev integrations and enabling continuous assessment without rescanning registries for updated detections.

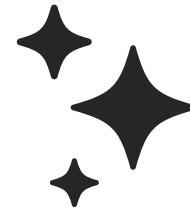
Demo

Thank You!





Qualys®



ROCon 25

The Risk Operations Conference

AMERICAS