Qualys.
ROCon 25
The Risk Operations Conference
AMERICAS

When Cloud Risk Meets Code!

Recipe to Fix Attack Paths at the Source

Qualys.
ROCon 25
The Risk Operations Conference
AMERICAS

Kunal Modasiya

Senior Vice President, Product Management, GTM and Growth

Terry Barber

Sr. Manager, Cybersecurity Engineering, American Express Global Business Travel

Shrikant Dhanawade

Director Product Management, Cloud Security

Challenges in Cloud Risk Prioritization

Qualys. ROCon 25
The Risk Operations Conference
AMERICAS

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
AMERICAS

Kubernetes and Container Security (KCS)

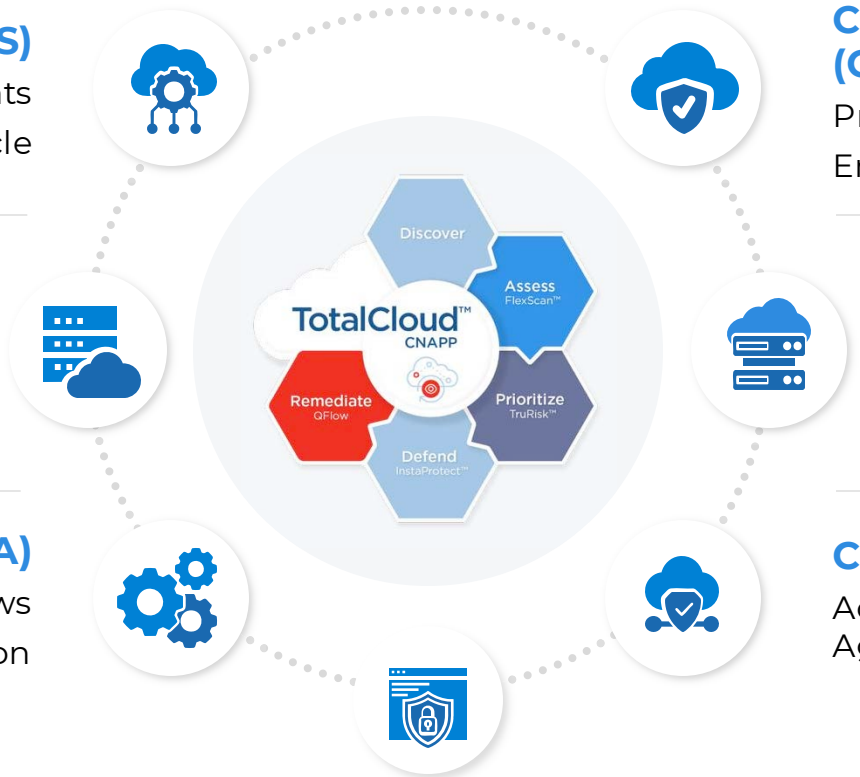
Prioritize Risks In Container Environments
Manage Risk Across The Dev Lifecycle

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

Visibility is a Key Part of Risk Management

Comprehensive inventory is crucial for the cloud

Qualys. ROCon 25 The Risk Operations Conference AMERICAS

All environments

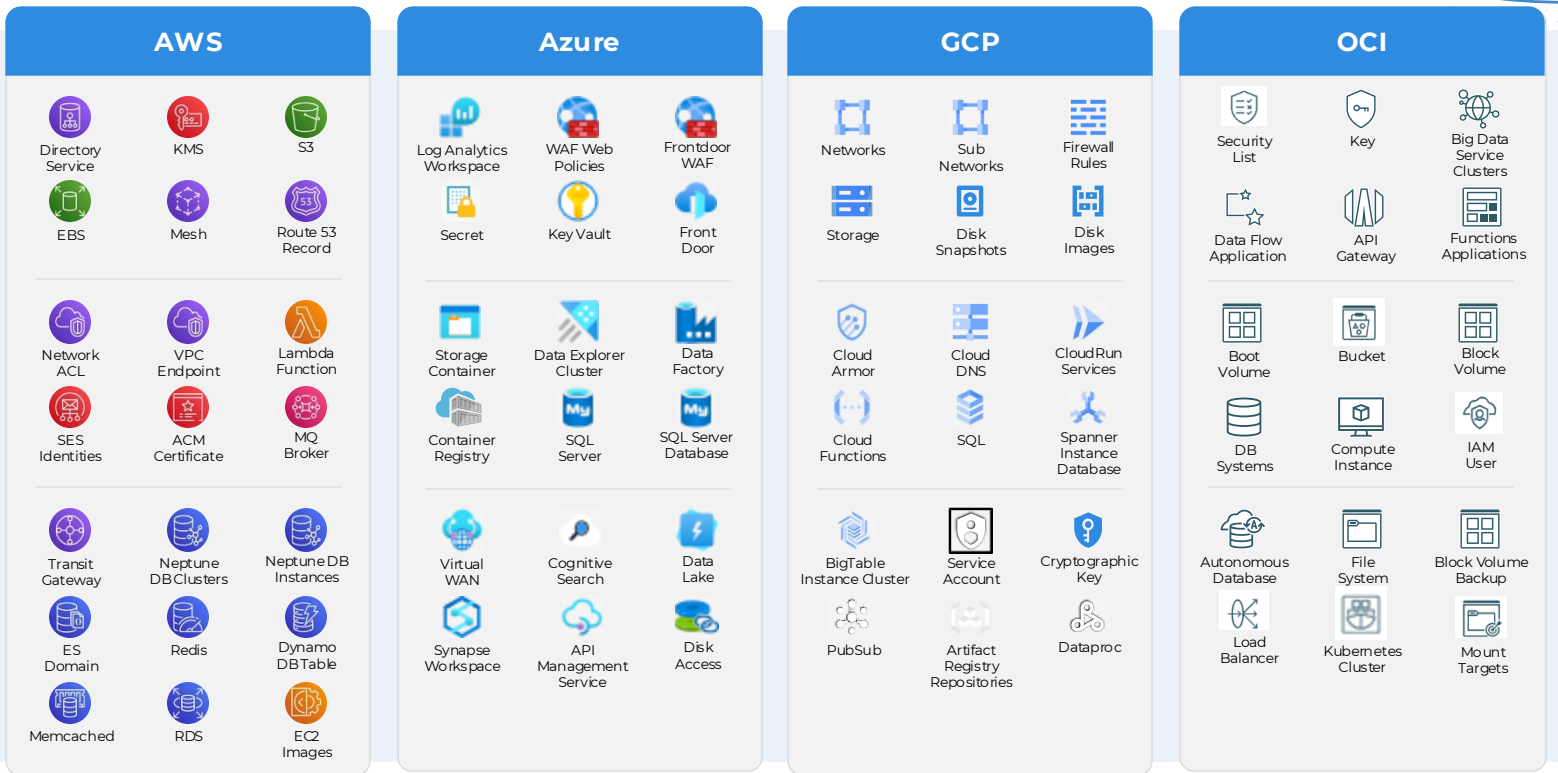
Across all clouds, containers, hybrid workloads

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 AMERICAS

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

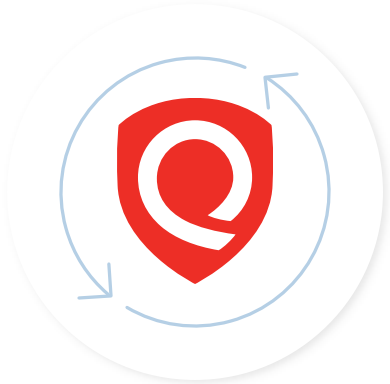
Scale Vulnerability Management with TotalCloud CWP - FlexScan

Continuously monitor cloud workloads, including newly deployed ones

Qualys. ROCon 25 The Risk Operations Conference AMERICAS

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

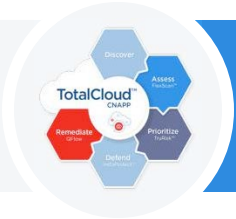
Qualys TotalCloud secures 44 Million cloud workloads across a variety of organizations.

Shift Left in Cloud Security

Evaluate Code before deploying to the Cloud

Qualys. ROCon 25 The Risk Operations Conference AMERICAS

Shift-Left Security
Proactive Approach



Runtime Security
Reactive Approach

Pre-Deployment

Infrastructure as Code (IaC)

Terraform
Cloud Formation
ARM Template

Repository and Registries

GitHub
Bitbucket
Gitlab

CI/CD

Jenkin
Bamboo

Post-Deployment

Cloud

AWS
Azure

Instance/ Containers/ Serverless/ WebApp

Amazon EC2
Web App

Resources

SQL
NSG

Identities

Developers | **GitOps** | **DevOps** | **CloudOps**

Risk Aggregation to Prioritization

With Qualys Enterprise TruRisk Management Platform

Qualys. ROCon 25
The Risk Operations Conference
AMERICAS

Asset Level Risk Score

Complete 360 Context with Threat Intel

TruRisk Score

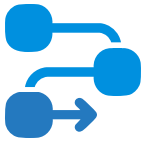
Correlate signals from many source

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
AMERICAS

Visualize critical resource exposure

Identify blast radius enabling proactive threat analysis

Prioritize risk findings w/ security graph

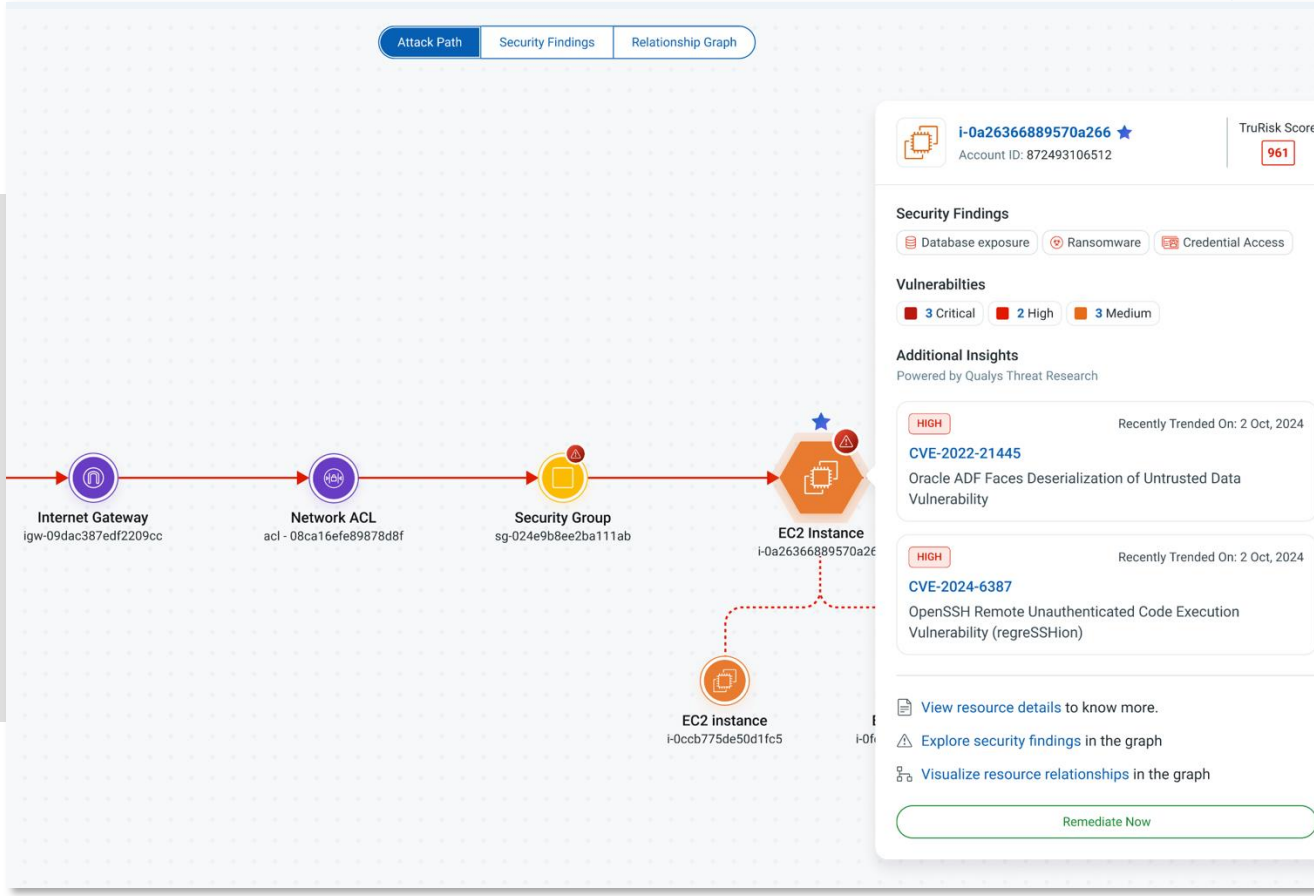
Navigate to important findings on critical resources

Understand resource relationships

Capture communication flows of attached resources

Scale with rapid remediation of risk

Drive accelerated risk-based prioritized threat remediation



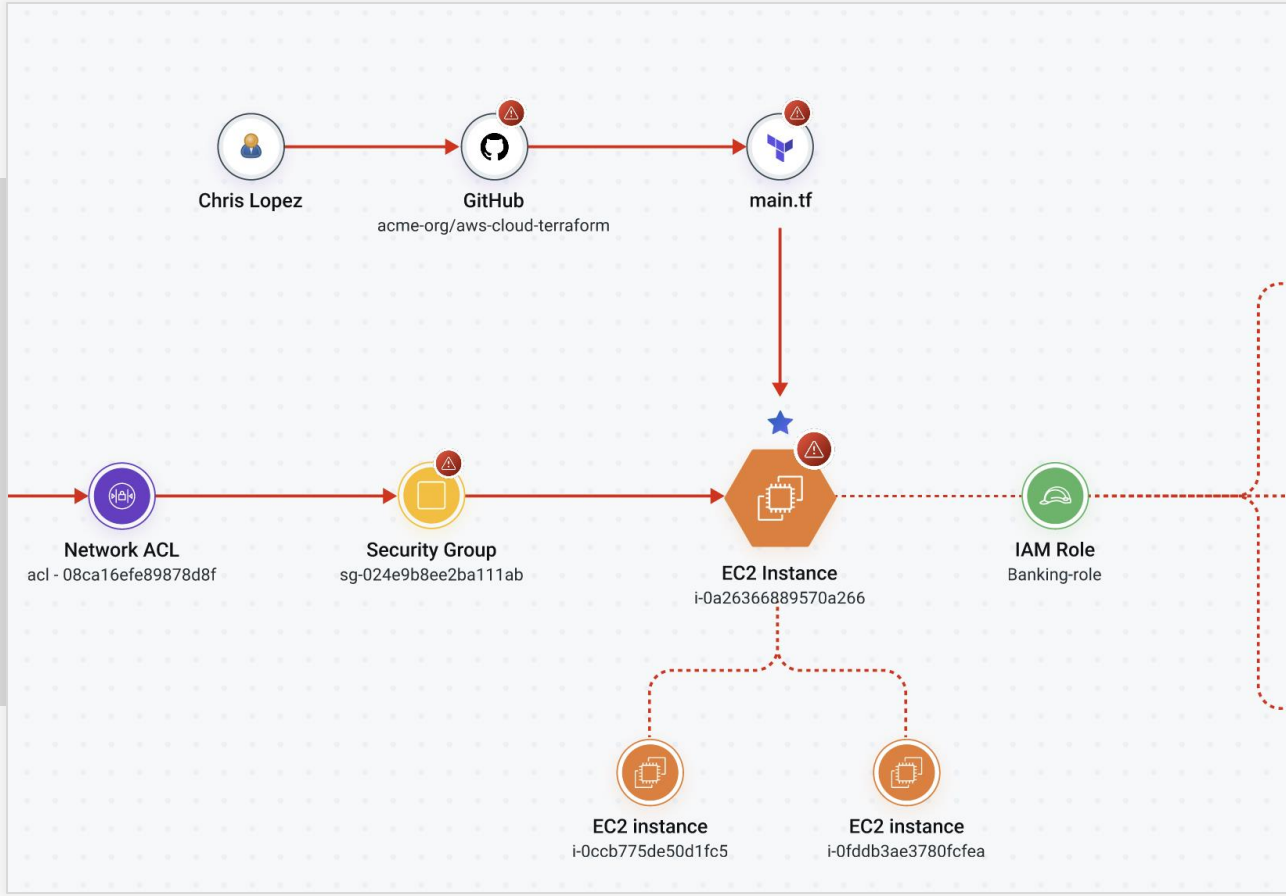
Provide Runtime Risk Context to Code

Turbocharge the risk prioritization with **Code to Cloud**

Shift Left and Fix Left

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

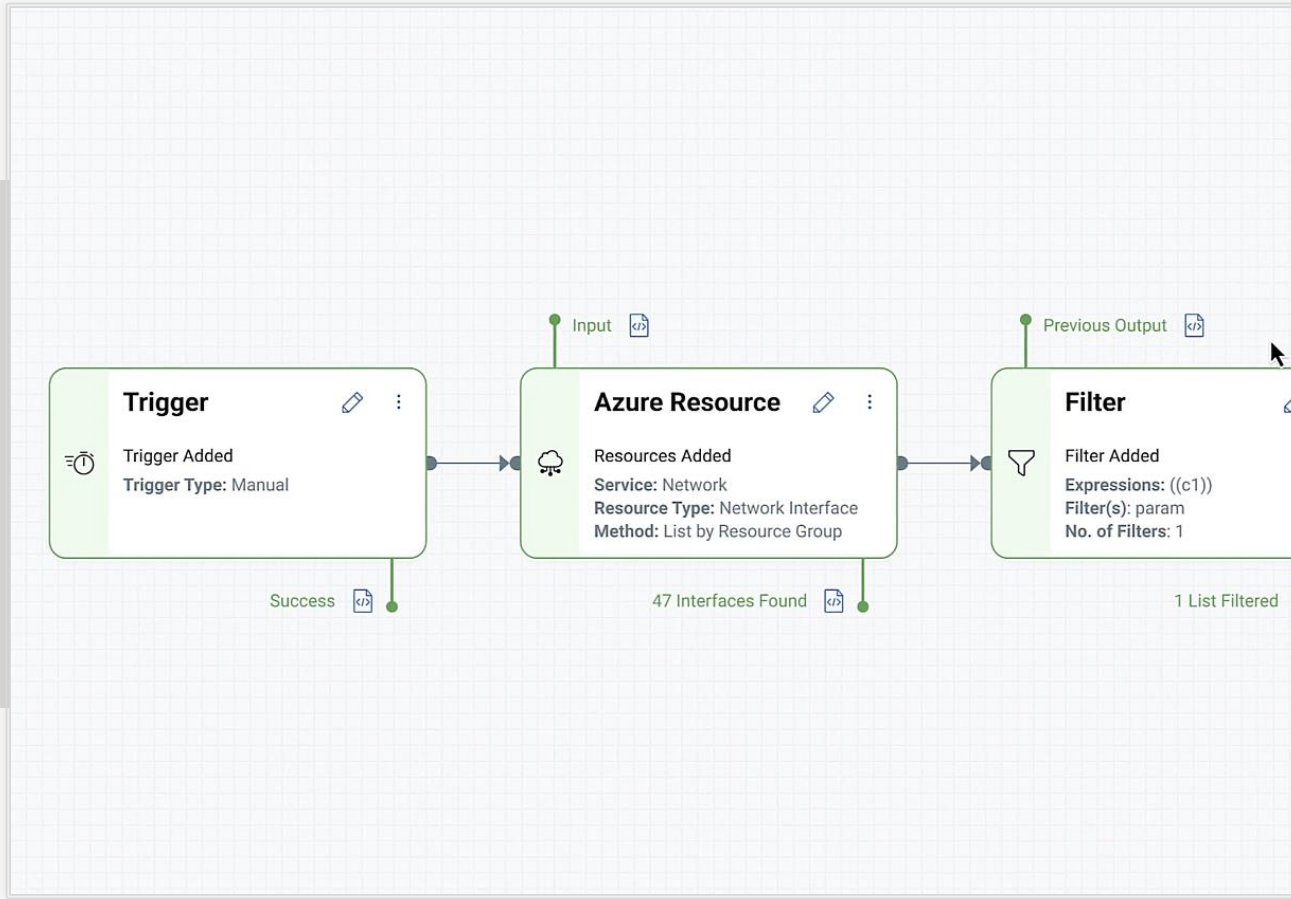
Qualys. ROCon 25
The Risk Operations Conference
AMERICAS

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
AMERICAS

Meet Your Response SLAs

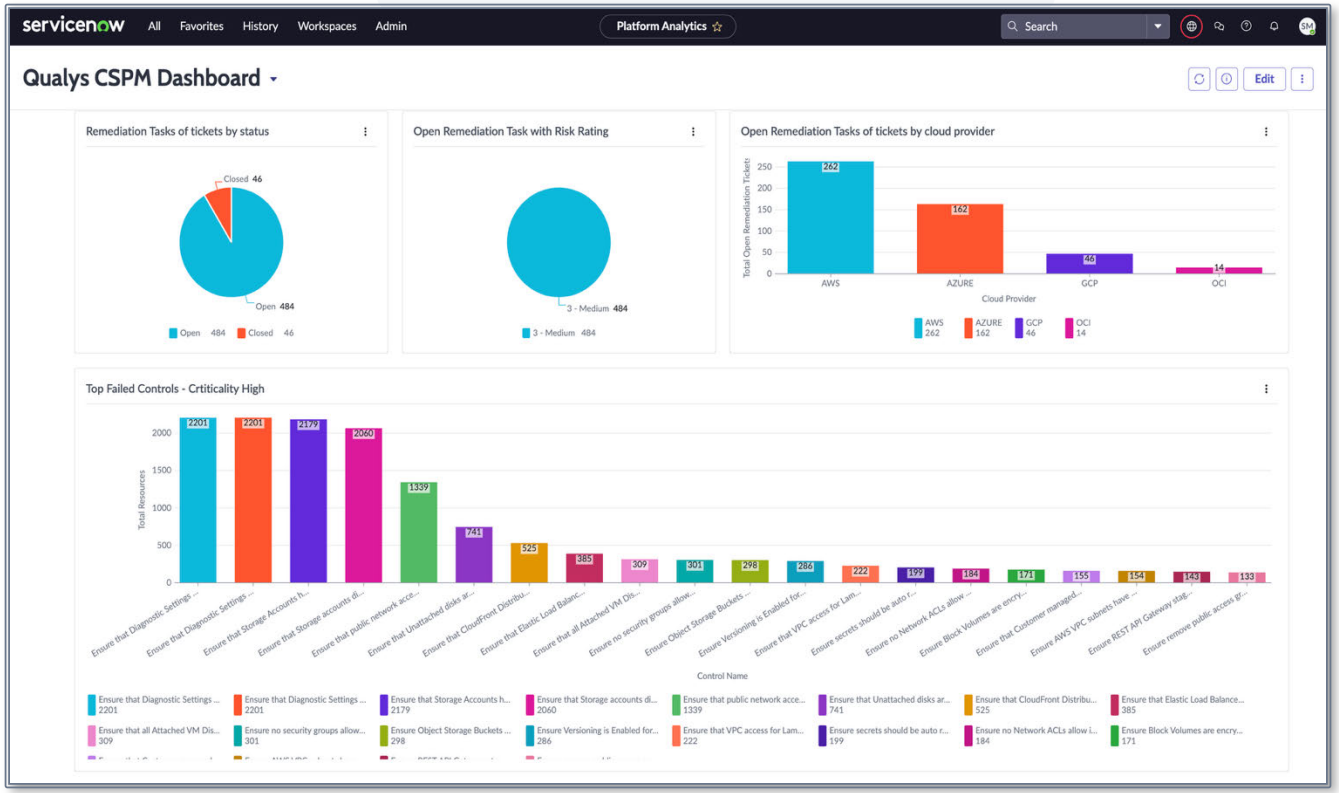
Comprehensive Tracking and Action:
Enable IT team to efficiently track and take timely action.

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



Compliance for Any Mandate

Compliance by Region

Global

- CIS Controls Version 8, Cloud Controls Matrix (CCM), / ISO/IEC 27001:2013, ISO/IEC 27001:2022 / Payment Card Industry Data Security Standard (PCI-DSS) v3.2.1 / Payment Card Industry Data Security Standard (PCI-DSS) v4.0 / SWIFT Customer Security Controls Framework - Customer Security Programme v2021

Americas

- NERC CIP (Energy)
- 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy
- CJIS Security Policy
- Cybersecurity Maturity Model Certification (CMMC) Level 1-5
- Federal Risk and Authorization Management Program (FedRAMP L / LI-SaaS / M)
- HIPAA Security Rule 45 CFR Parts 160/164, Subparts A/C:1996
- IRS Publication 1075
- Minimum Acceptable Risk Standards for Exchanges (MARS-E)
- NIST 800-53 + Special Publication 800-171
- Sarbanes-Oxley Act: IT Security
- The NIST Cybersecurity Framework (CSF)
- US Cybersecurity Maturity Model Certification (CMMC) 2.0 Level 1 and 2

Europe and Middle East

- ANSSI 40 Essential Measures for a Healthy Network
- General Data Protection Regulation (GDPR)
- NESA UAE Information Assurance Standards (IAS)
- NCSC Basic Cyber Security Controls (BCSC)

India

- IRDAI Guidelines On Information and Cyber Security for Insurers
- Reserve Bank of India (RBI) - Baseline Cyber Security and Resilience Requirements (Annex 1)

AsiaPac / Oceana

- APRA Prudential Practice Guide (PPG): CPG 234 - Management of Security Risk in IT
- Australian Signals Directorate - Essential Eight Maturity Model
- MAS - Notice 834: Cyber Hygiene Practices
- Technology Risk Management (TRM) Guidelines
- New Zealand Information Security Manual (NZISM)

When Cloud Security Meets App Security?

Qualys. ROCon 25
The Risk Operations Conference
AMERICAS

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

TotalCloud

Cloud Security

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

TotalAppSec

Application Security

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

New Announcement

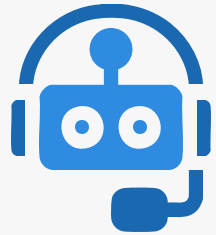
Qualys. ROCon 25
The Risk Operations Conference
AMERICAS

Qualys Agentic AI

AI fabric to drive real-time, autonomous **response to risk signals** and deliver **board-ready insights** at machine speed

AI Agent Marketplace

Specialized AI Agents trained for autonomous risk prioritization and remediation.
Built-In & Build Your Own Agents



Cyber Risk Assistant

Democratize access to security data with natural language interface for adaptive, self-learning decision support.

Agent Vikram for TotalCloud

Qualys. ROCon 25
The Risk Operations Conference
AMERICAS

< 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

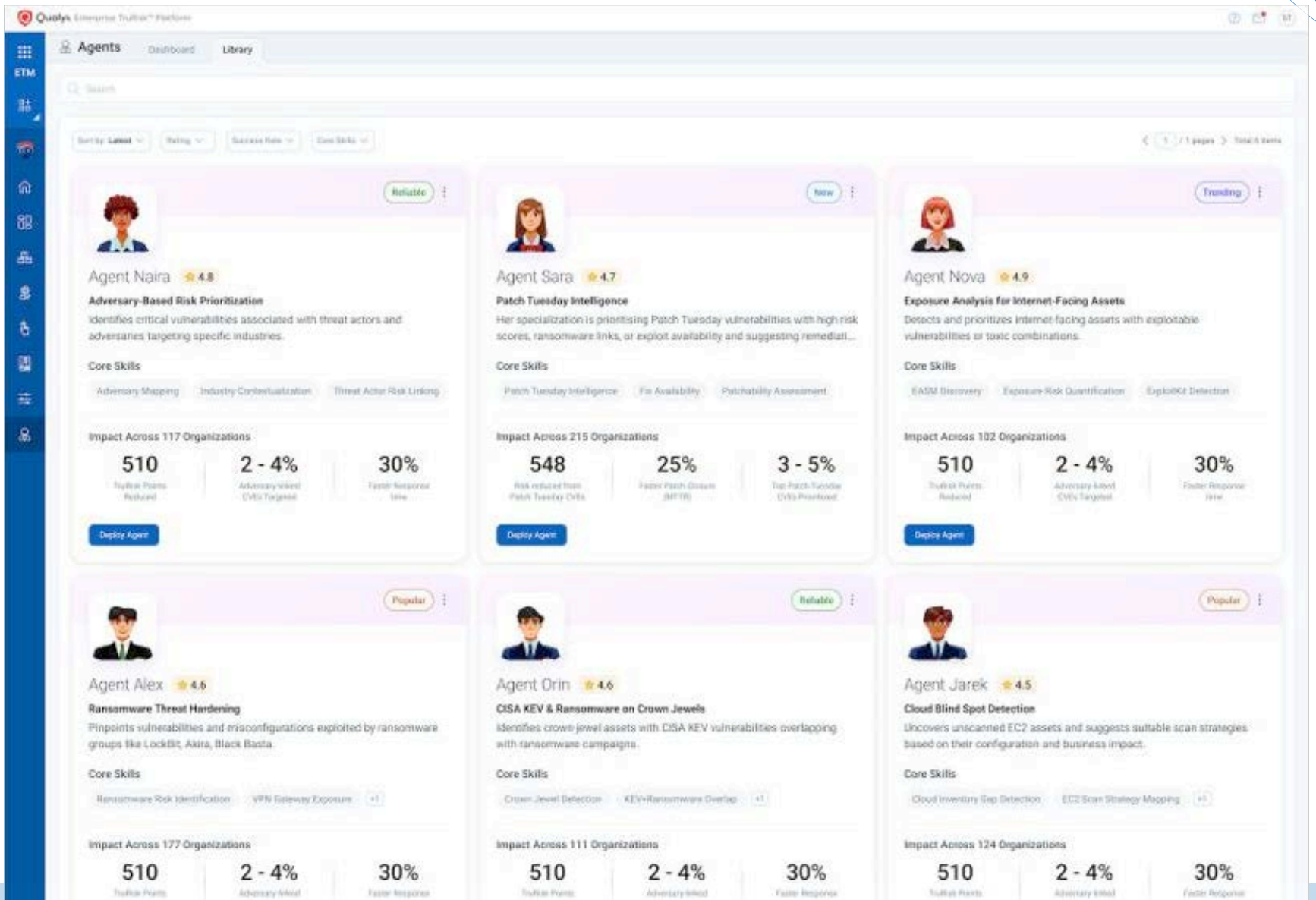
100%	6 Mins	22%
Visibility into Cloud Assets	To Define Flexible Scan Strategies in Cloud	Less Cyber Risk in Cloud

Employ

Agentic AI

Your skilled, digital workforce for autonomous risk management

Qualys. ROCon 25
The Risk Operations Conference
AMERICAS



Cloud-native Security

Discover, Assess, Remediate Cloud Accounts Effectively

Qualys' Cloud Implementation Provides Insights Into Maturing Internal Processes For Cloud-native Security

Terry Barber,
Sr. Cyber Security Manager
Cybersecurity Engineering
American Express Global Business Travel

- Sr. Cybersecurity Manager – Cybersecurity Engineering
- 9+ Years with American Express Global Business Travel
- Broad Experience Across Multiple Platforms
- Computer Science Program, California State University, Northridge
- Helping To Protect The Personal Information of AMEX Global Business Travelers

Terry Barber

CISSP

AMERICAN EXPRESS GLOBAL BUSINESS TRAVEL

Inventory

Assessment

Prioritize

Remediate

Inventory

- Deploy Cloud Connectors
- Tag Assets for Responsibility Matrix
- Assess Each Account's Assets
- Prioritize Findings
- Remediate

01

Deploy
Qualys Connectors

Discover and
Populate Inventory

02

Tag Assets,
Assess, Prioritize
And Remediate

AMERICAN EXPRESS GLOBAL BUSINESS TRAVEL

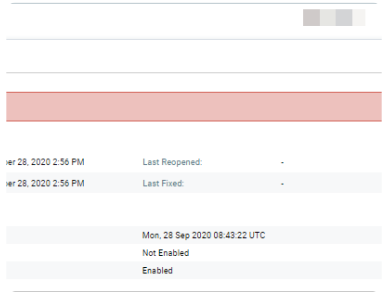
CSPM

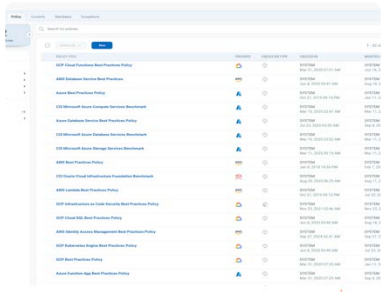
Cloud Security Posture Management

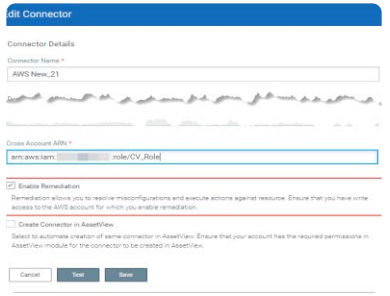
Activating CSPM On The Qualys Connector Enables Visibility And Assessment Of The Account.

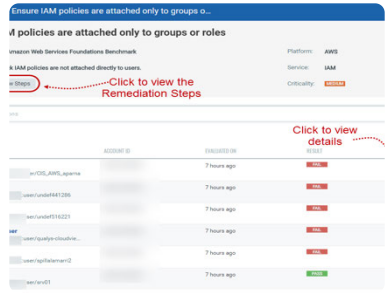
- Adding CSPM to the Connector Provides Configuration Data
- TotalCloud Applies CSPM Configuration through the Connector.
- Providing Posture, via Policies, TotalCloud Helps Identify Misconfigurations.
- A Dashboard for Control Assessment with TruRisk Insights.
- Insights – Visibility into Critical Risks such as Publicly Exposed VM's with Vulnerabilities.

Configuration Assessment









Misconfigured Cloud Accounts Introduce Risk

Assess Cloud Accounts to Discover These Misconfigurations

Remediation of Misconfigured Settings can be Automated

Use Policy Assessment to Define Security Policies, Eliminate Risk, and Quickly Assess New Environments

Vulnerabilities

Utilize Multiple Scanning Strategies For Complete Coverage

Multi-layered Approach To Vulnerability Detection

Cloud Agent

Network Scanner Appliances

External Scans

Snapshot Scans

API Scans

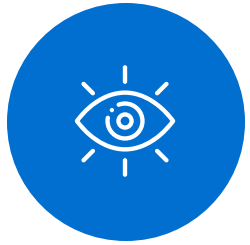
Qualys Scanning

FlexScan Flexibility Awaits

- Review your cloud environment to determine which scanning methodology to implement
- Cloud Agents – Operating system coverage
  Perimeter Scans – Scan public facing assets
- API Scans – scan package inventories
  Snapshot Scans – scan workload snapshots
- Tailor the scanning strategy for cost effectiveness
  and gap reduction

Containers

Container Environments can be Fluid



CI/CD Pipeline Visibility

Shift Left

Responsibility Matrices

GLOBAL BUSINESS TRAVEL

Streamlining Process & Managing Cost

Container Environments Create Unique Issues for Remediation Teams. Who's Responsible?

Shift Left is a Trend That Assists in the Early Definition of Vulnerabilities.

Stop Vulnerabilities at Build Time, Ensure Secure Runtime.

TruRisk

Attack path – Public facing?
Sensitive data?

Connected assets, EC2 to S3

Once compromised attack path vulns become worse

Utilize Automation to Speed Response

Zero Touch Scanning

QFlow Initiated Scanning

Configuration Remediation

Multi-faceted approach

Build a Strategy

01 Discover

02 Assess

03 Secure

04 Remediate

05 Automate

In Closing

When building a cloud strategy review all your capabilities in your tool set and deploy your security solution in a manner that:

Discovers inventory in your environment

Deploys tools to assess the environment and prevents gaps

Allows the use of Automation to speed the efficiency and response

Qualys. ROCon 25
The Risk Operations Conference
AMERICAS

Demo - Code to Cloud

Recipe to Fix Attack Paths at the Source

Qualys®

Enterprise TruRisk™ Platform

Measure, communicate, and eliminate cyber risk.

De-risk your business.