QSC 25 EMEA

Cloudy Attack Paths

Use TruRisk GPS from Code to Cloud

Kunal Modasiya
Senior Vice President, Product Management, GTM and Growth

Challenges in Cloud Risk Prioritization

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.

And breaches are only increasing for this vector of attack.

01

In 2025, Qualys Research Unit identified **that 70% of the Azure resources are misconfigured,** leading to a potential open attack surface.

02

Attackers injected **malicious code** into 1000s of **popular container images** on public registries. 51% of Docker images scanned has a **critical security vulnerability**

03

FTC fined a consumer DNA sequencing company after determining **1000s of customer's DNA information** was stored in **public S3 buckets**

Qualys' CNAPP TotalCloud Platform Overview

Qualys.

Qualys TotalCloud

The Risk-Minded CNAPP

Kubernetes and Container Security (KCS)

Prioritize Risks In Container Environments

Manage Risk Across The Dev Lifecycle

Cloud Detection & Response (CDR)

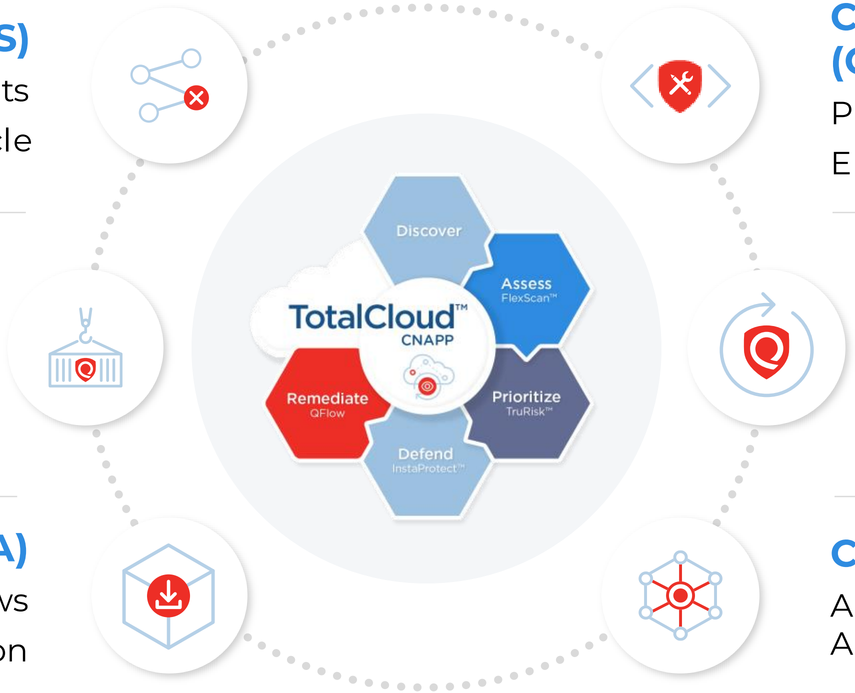
Detect Malicious Threats In Runtime

Respond To Zero-Day Malware

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

aws Azure Google Cloud ORACLE Cloud

DE-RISK YOUR **BUSINESS**

Qualys.

Risk Prioritization with Qualys Enterprise TruRisk Management Platform

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

Visualize critical resource exposure

Identify blast radius enabling proactive threat analysis

Prioritize risk findings w/ security graph

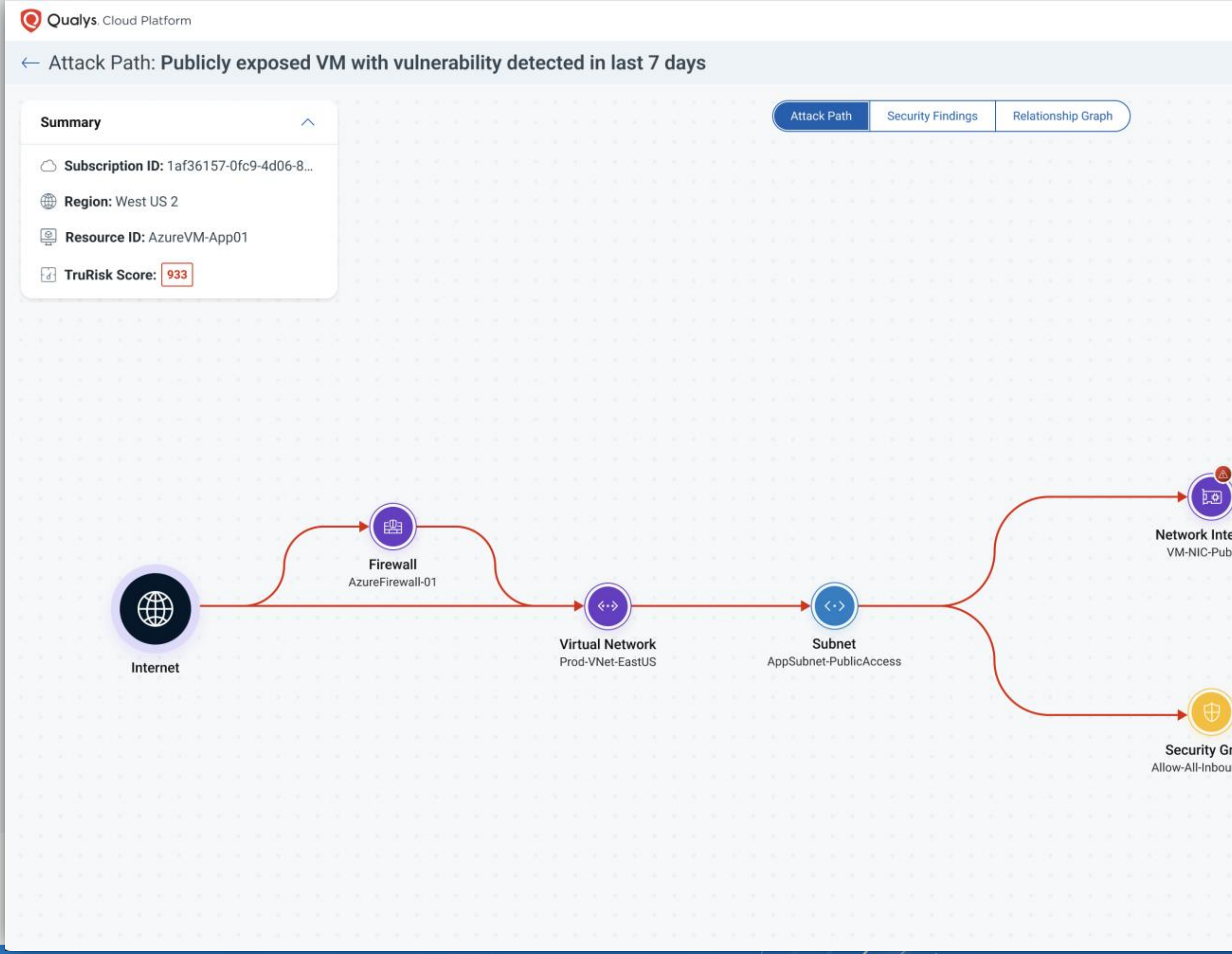
Navigate to important findings on critical resources

Understand resource relationships

Capture communication flows of attached resources

Scale with rapid remediation of risk

Drive accelerated risk-based prioritized threat remediation



Qualys. Cloud Platform

← Attack Path: Publicly exposed VM with vulnerability detected in last 7 days

Summary

- Subscription ID: 1af36157-0fc9-4d06-8...
- Region: West US 2
- Resource ID: AzureVM-App01
- TruRisk Score: 933

DE-RISK YOUR **BUSINESS**

Qualys.

Remediate Risks with Cloud Workflow Automation

No Code / Low Code QFlows

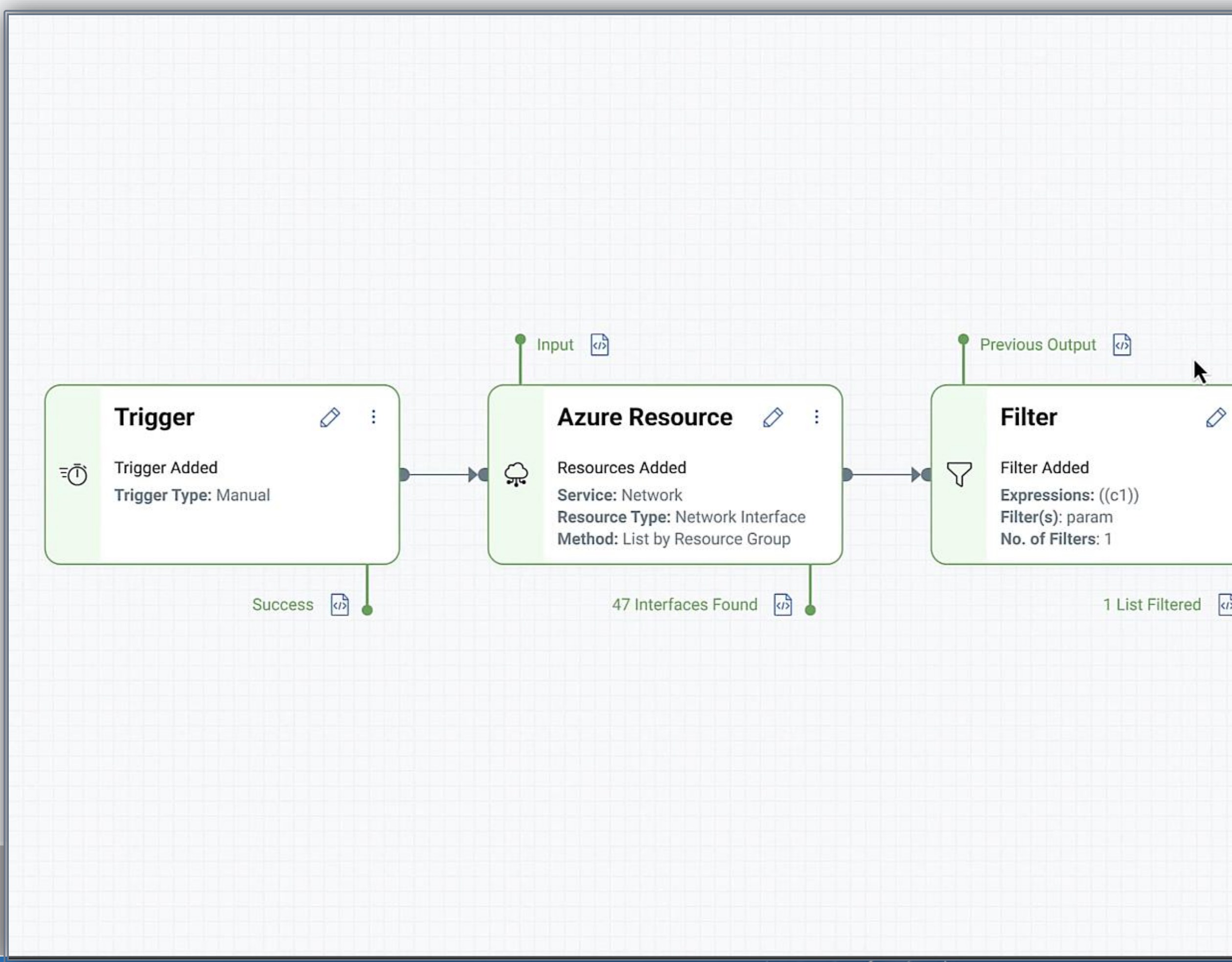
Simplify workflow creation with drag and drop visual nodes and no code

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



Trigger
Trigger Added
Trigger Type: Manual
Success

Input
Azure Resource
Resources Added
Service: Network
Resource Type: Network Interface
Method: List by Resource Group
47 Interfaces Found

Previous Output
Filter
Filter Added
Expressions: ((c1))
Filter(s): param
No. of Filters: 1
1 List Filtered

Announcing New Capabilities

You asked
We are delivering

Qualys®

Qualys Risk Operations Center For Azure

Policy Audit for Cloud, Containers and AI Models

Cloud Security Posture Management (CSPM)

Audit Ready Reporting

- ✓ Compliance monitoring of **35+ global frameworks**
- ✓ Validate with the latest CIS v3.0.0 benchmarks

Attack Path Analysis

- ✓ Public exposure via load balancers, NSG, VNETs, gateways, and Azure Firewall

K8s Security Posture Management (KSPM)

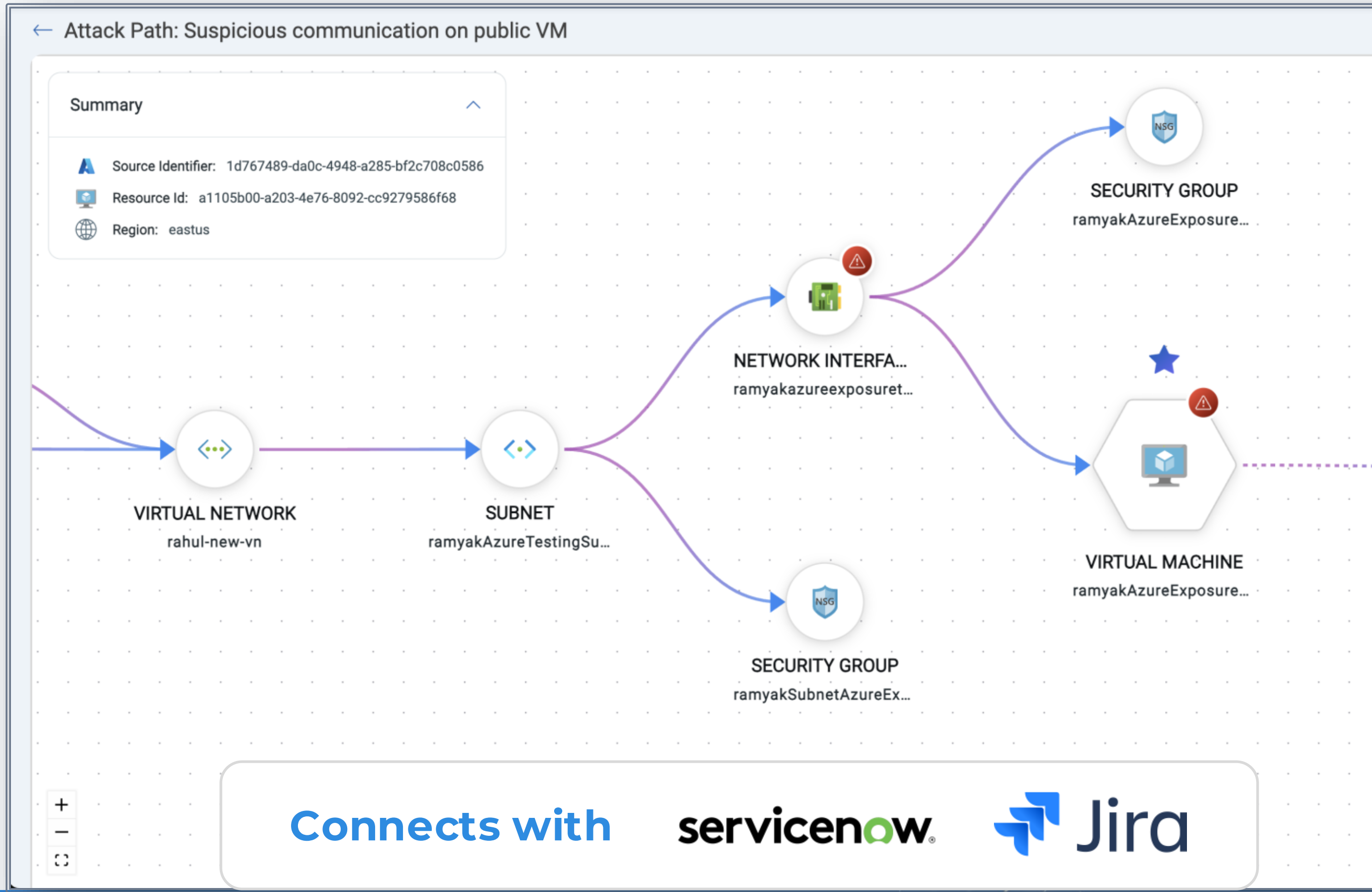
- ✓ CIS for Azure Kubernetes (AKS)

AI Security Posture Management (AISPM)

- ✓ Misconfiguration rules for Azure AI Services and OpenAI

Shift Left – Scan Azure IaC Templates

- ✓ Supports Terraform and ARM Templates
- ✓ Integrates with Azure DevOps pipelines



← Attack Path: Suspicious communication on public VM

Summary

Source Identifier: 1d767489-da0c-4948-a285-bf2c708c0586

Resource Id: a1105b00-a203-4e76-8092-cc9279586f68

Region: eastus

Connects with servicenow Jira

DE-RISK YOUR BUSINESS

Qualys.

Qualys Risk Operations Center For Azure

Extending VMDR to Azure Cloud

Azure Workload Protection

Unmatched Accuracy of Detections

- ✓ Best in class Six Sigma Accuracy powered by VMDR
- ✓ Correlates with 25+ external threat feeds

Agentless and Agent-based Scans

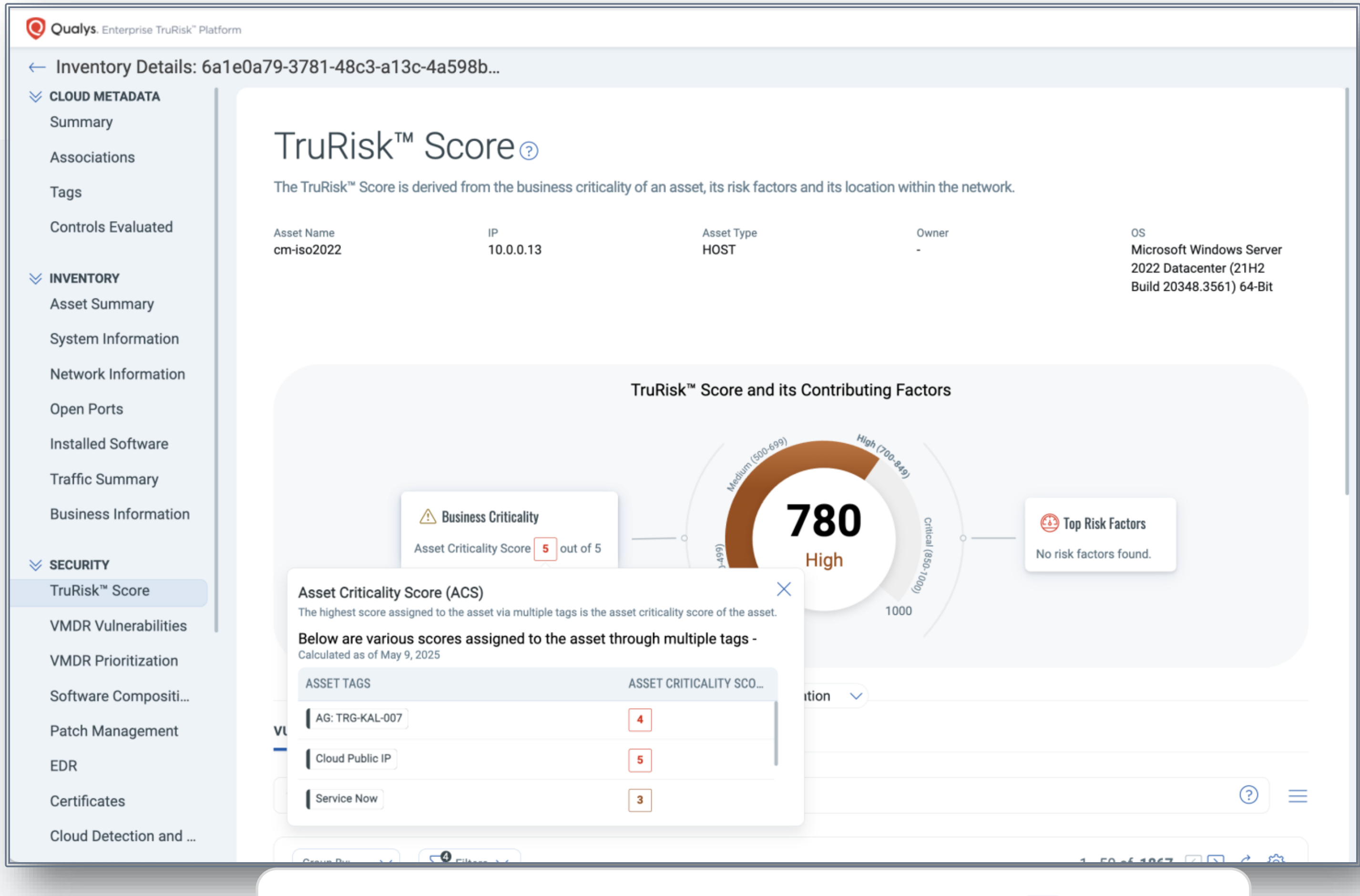
- ✓ Ensures all your cloud workloads are scanned
- ✓ Covers agents, network, and snapshot-based scans

Launching new - Azure Linux

- ✓ Cloud Agent and Container Sensor support for new Azure Default Operating System

Scan VM Scale Sets

- ✓ Ensures all your dynamic workloads are scanned before they vanish to get visibility



Inventory Details: 6a1e0a79-3781-48c3-a13c-4a598b...

TruRisk™ Score

The TruRisk™ Score is derived from the business criticality of an asset, its risk factors and its location within the network.

Asset Name	IP	Asset Type	Owner	OS
cm-iso2022	10.0.0.13	HOST	-	Microsoft Windows Server 2022 Datacenter (21H2 Build 20348.3561) 64-Bit

TruRisk™ Score and its Contributing Factors

Business Criticality

Asset Criticality Score 5 out of 5

780 High

Top Risk Factors

No risk factors found.

Asset Criticality Score (ACS)

The highest score assigned to the asset via multiple tags is the asset criticality score of the asset.

Below are various scores assigned to the asset through multiple tags -

Calculated as of May 9, 2025

ASSET TAGS	ASSET CRITICALITY SCO...
AG: TRG-KAL-007	4
Cloud Public IP	5
Service Now	3

Connects with servicenow Jira

DE-RISK YOUR BUSINESS

Qualys.

Qualys Risk Operations Center For Azure

CDR for Azure Virtual Machines and Containers

Azure Threat Detection and Response

Powered by AI/ML Framework

- ✓ Detects known and unknown threats in real-time
- ✓ Ability to detect the mutated malwares

Detection using Azure Flow Logs

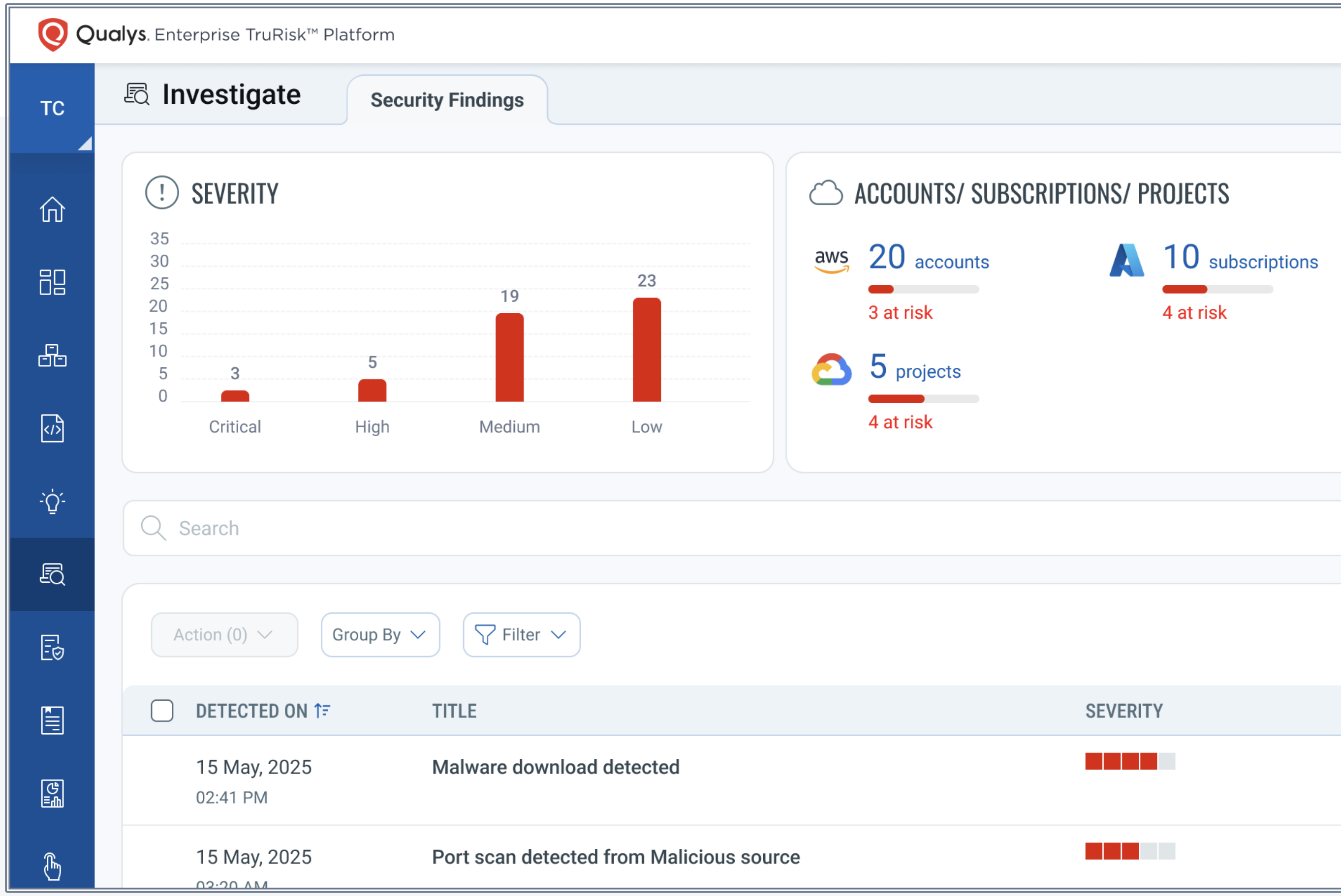
- ✓ Monitor and analyze network traffic
- ✓ Detects suspicious patterns, and indicators of compromise

Detection using Azure VTAP Traffic

- ✓ Mirror network traffic from Azure virtual machines
- ✓ Deploy appliances using simple terraform commands

Detect Zero-Day Malware

- ✓ In Azure Virtual Machines and Containers registry
- ✓ Detect runtime threats on AKS containers with EBPF



aws 20 accounts — 3 at risk

10 subscriptions — 4 at risk

5 projects — 4 at risk

☐ DETECTED ON	TITLE	SEVERITY
15 May, 2025 02:41 PM	Malware download detected	🟥🟥🟥🟥⬜
15 May, 2025 03:20 AM	Port scan detected from Malicious source	🟥🟥🟥⬜⬜

DE-RISK YOUR **BUSINESS**

Qualys.

Qualys Risk Operations Center For Azure

No code workflow automation using Qualys Flow

Azure Cloud Workflow Automation

Build custom checks in minutes

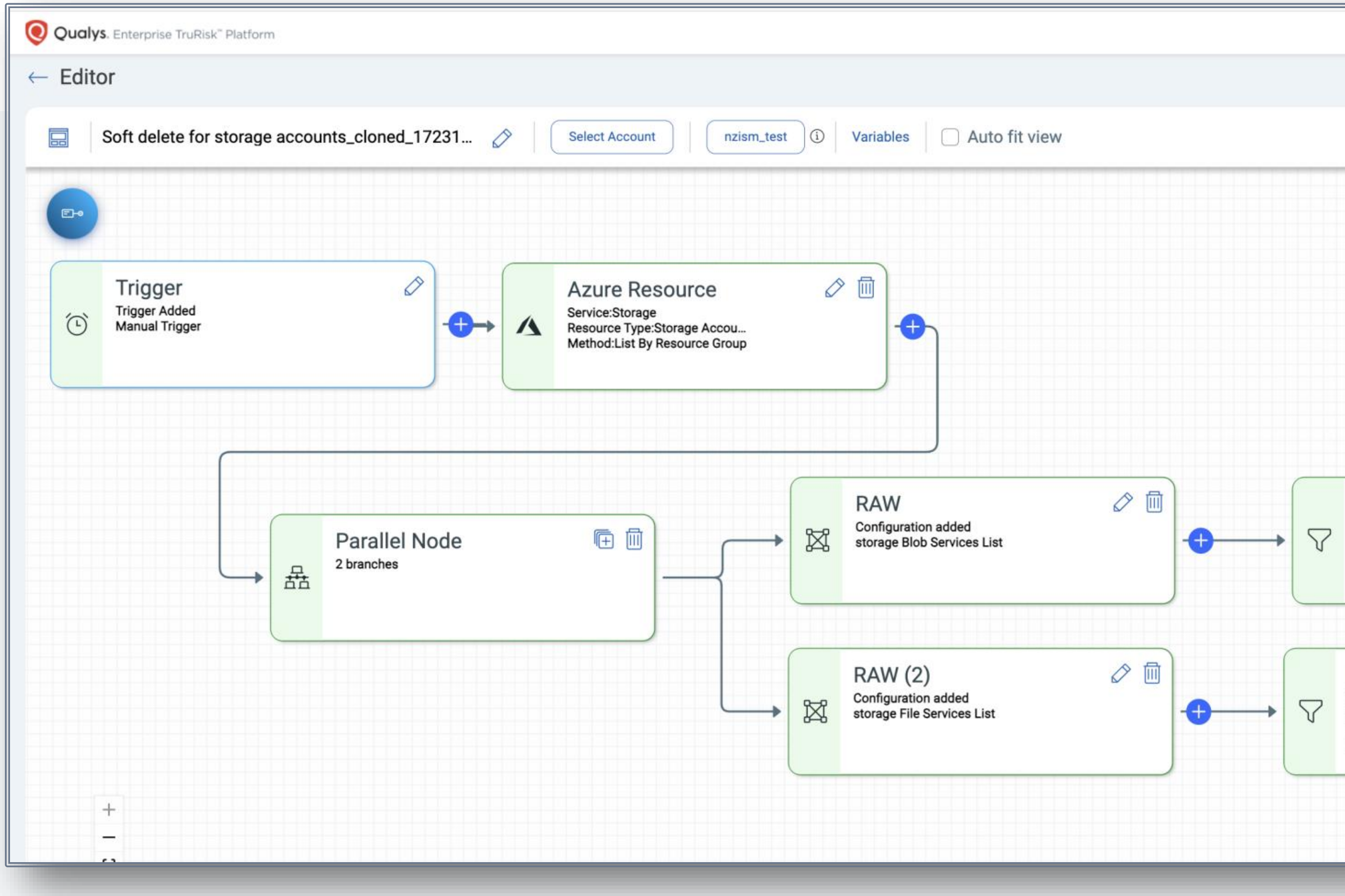
- ✓ Handles all custom compliance use cases
- ✓ Integrates with TotalCloud CSPM for continuous assessments

Custom Remediations to reduce risks

- ✓ Build custom remediation workflows to address specific security issues
- ✓ Vulnerability scanning, patching, quarantine, and triggering change control workflows.

100+ Azure Cloud Playbooks

- ✓ Best practices out-of-the-box workflows
- ✓ Based on real-world scenarios requested by users



Qualys. Enterprise TruRisk™ Platform

Editor

Soft delete for storage accounts_cloned_17231...

Trigger
Trigger Added
Manual Trigger

Azure Resource
Service:Storage
Resource Type:Storage Accou...
Method:List By Resource Group

Parallel Node
2 branches

RAW
Configuration added
storage Blob Services List

RAW (2)
Configuration added
storage File Services List

Integrates with ServiceNow

Vulnerability/Misconfiguration Assignment and Remediation

ServiceNow Modules

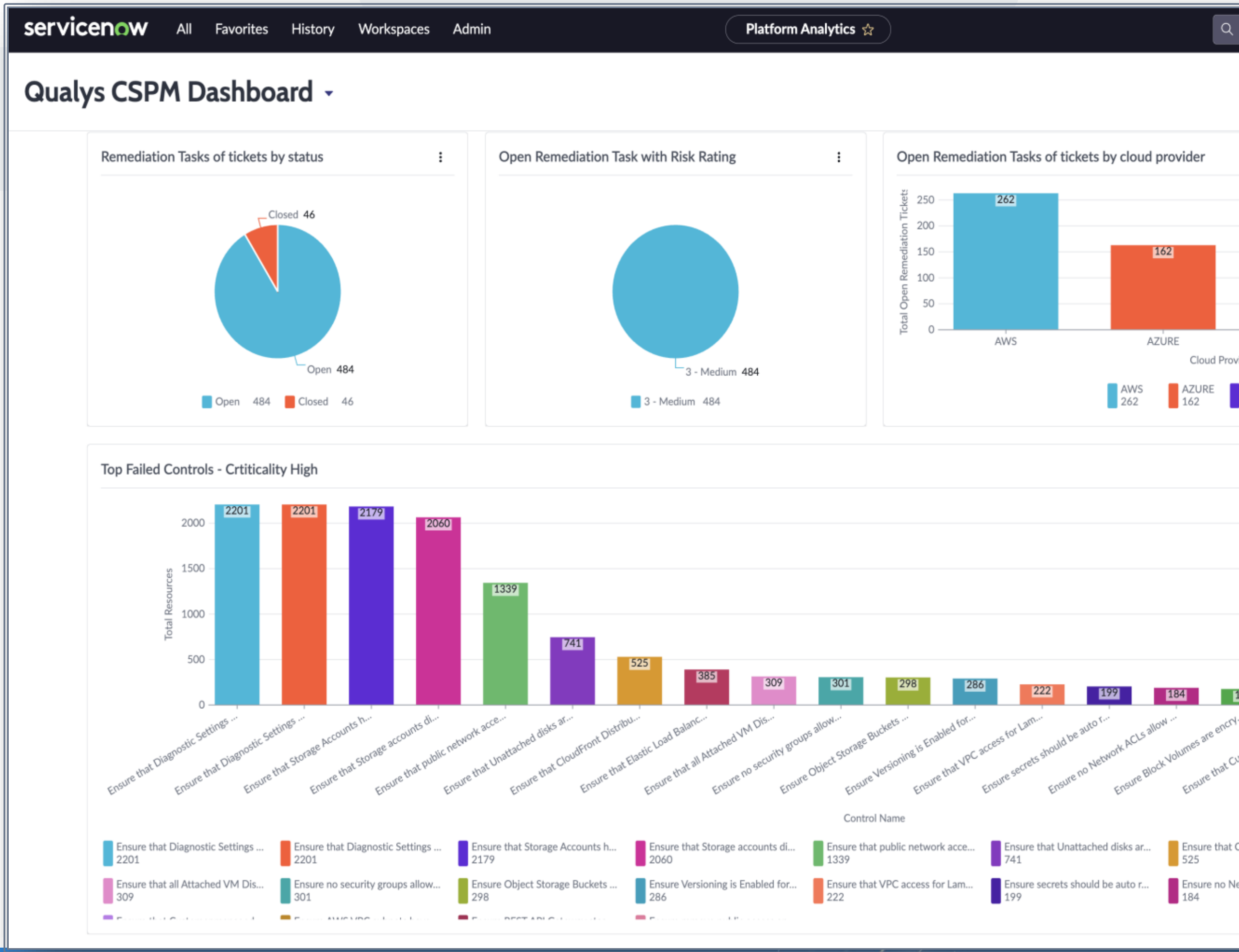
Vulnerability Response
Container Vulnerability Response
Configuration Compliance

Many Qualys customers use ServiceNow

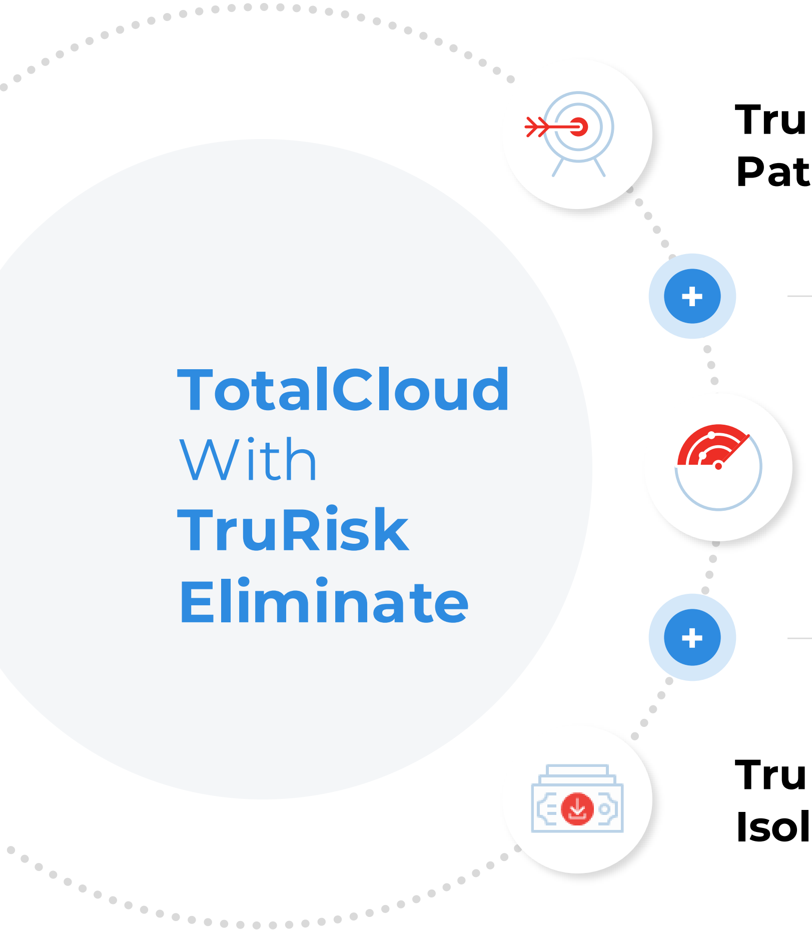
Comprehensive Tracking and Action: Enable extensive coverage of findings in ServiceNow so that the IT team can efficiently track and take timely action.

Automated Vulnerability Assignment: Utilize automated workflows to assign vulnerability fixes to developers based on asset ownership seamlessly.

Wide Adoption of Key Capabilities: Many Qualys customers leverage these essential integration features for enhanced vulnerability and misconfiguration management.


servicenow
All
Favorites
History
Workspaces
Admin
Platform Analytics ☆
Qualys CSPM Dashboard
Remediation Tasks of tickets by status
Closed 46
Open 484
Open 484
Closed 46
Open Remediation Task with Risk Rating
3 - Medium 484
3 - Medium 484
Open Remediation Tasks of tickets by cloud provider
Total Open Remediation Tickets
250
200
150
100
50
0
262
162
AWS
AZURE
Cloud Prov
AWS 262
AZURE 162
Top Failed Controls - Crtiticality High
Total Resources
2000
1500
1000
500
0
2201
2201
2179
2060
1339
741
525
385
309
301
298
286
222
199
184
Ensure that Diagnostic Settings ...
Ensure that Diagnostic Settings ...
Ensure that Storage Accounts h...
Ensure that Storage accounts di...
Ensure that public network acce...
Ensure that Unattached disks ar...
Ensure that CloudFront Distribu...
Ensure that Elastic Load Balanc...
Ensure that all Attached VM Dis...
Ensure no security groups allow...
Ensure Object Storage Buckets ...
Ensure Versioning is Enabled for...
Ensure that VPC access for Lam...
Ensure secrets should be auto r...
Ensure no Network ACLs allow ...
Ensure Block Volumes are encry...
Ensure that C
Control Name
Ensure that Diagnostic Settings ... 2201
Ensure that Diagnostic Settings ... 2201
Ensure that Storage Accounts h... 2179
Ensure that Storage accounts di... 2060
Ensure that public network acce... 1339
Ensure that Unattached disks ar... 741
Ensure that C 525
Ensure that all Attached VM Dis... 309
Ensure no security groups allow... 301
Ensure Object Storage Buckets ... 298
Ensure Versioning is Enabled for... 286
Ensure that VPC access for Lam... 222
Ensure secrets should be auto r... 199
Ensure no Ne 184

Cloud Exploitability Prevention



TotalCloud With TruRisk Eliminate

TruRisk Patch

- Automatic Playbooks For CISA KEVs
- Fully automate patch deployment based on attack paths
- Full support for any host, on-prem or cloud

TruRisk Mitigate

- Leverage Qualys Flow Playbooks to apply compensating controls while waiting for patch
- Includes ability to limit privileges, restrict network access, and any API supported by your CSP
- Apply Admission Control Policies in Kubernetes

TruRisk Isolate

- Isolate hosts/VMs to ensure vulns cannot be exploited
- Allow exceptions to ensure workloads and images can be patched and managed

We secure your ORACLE Cloud too!

Discovery and Inventory

Cloud Connectors to Oracle Cloud Tenancy

Discovers from all global regions of the OC-1 realm

Configuration Assessment (CSPM)

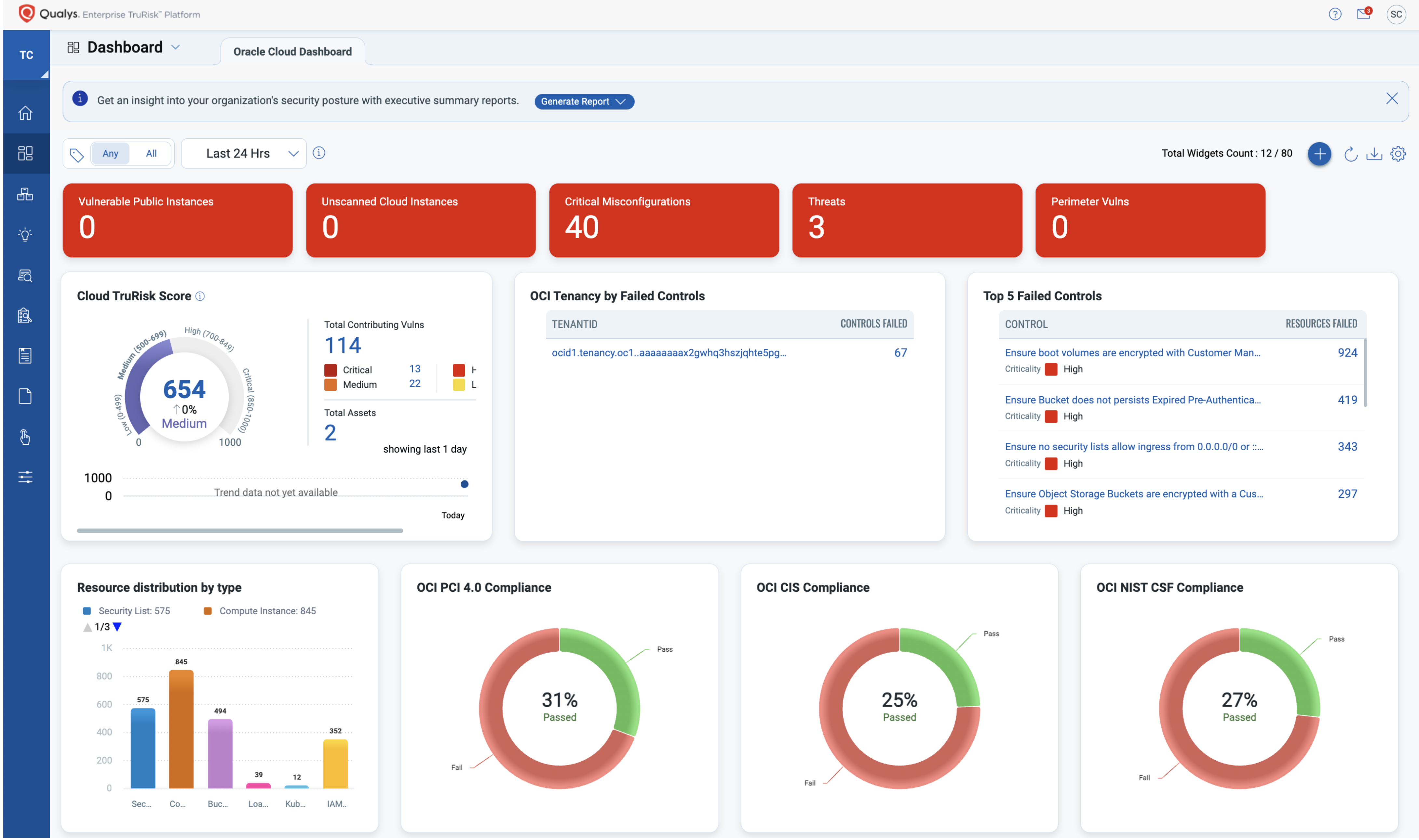
Extensive coverage of the security controls

CIS Foundation Benchmarks v2.0.0 and 40+ Global Compliance mandates.

Know and Eliminate the Risk

Build Custom Dashboard and Reports

Supports Alert Rule configurations – Email, PagerDuty, Slack, MS Teams



Qualys. Enterprise TruRisk™ Platform

TC

Dashboard

Oracle Cloud Dashboard

Get an insight into your organization's security posture with executive summary reports. Generate Report

Any All

Last 24 Hrs

Total Widgets Count : 12 / 80

Vulnerable Public Instances	Unscanned Cloud Instances	Critical Misconfigurations	Threats	Perimeter Vulns
0	0	40	3	0

Cloud TruRisk Score

654
↑0%
Medium

Total Contributing Vulns
114

🟥 Critical	13	🟥 H	
🟧 Medium	22	🟨 L	

Total Assets
2

showing last 1 day

Trend data not yet available

Today

OCI Tenancy by Failed Controls

TENANTID	CONTROLS FAILED
ocid1.tenancy.oc1..aaaaaaaax2gwhq3hszjqhte5pg...	67

Top 5 Failed Controls

CONTROL	RESOURCES FAILED
Ensure boot volumes are encrypted with Customer Man... Criticality 🟥 High	924
Ensure Bucket does not persists Expired Pre-Authentica... Criticality 🟥 High	419
Ensure no security lists allow ingress from 0.0.0.0/0 or :... Criticality 🟥 High	343
Ensure Object Storage Buckets are encrypted with a Cus... Criticality 🟥 High	297

Resource distribution by type

🟦 Security List: 575 🟧 Compute Instance: 845

1/3

OCI PCI 4.0 Compliance

31% Passed

OCI CIS Compliance

25% Passed

OCI NIST CSF Compliance

27% Passed

DE-RISK YOUR **BUSINESS**

Qualys.

We are Delivering Customer Commitments!

Shift Left VMDR in Cloud

- Scan AWS AMIs for vulnerabilities.
- Verify image hygiene and shift risk prioritization and remediation to the left.

Software Composition Analysis (SCA) using Agentless

- Extend vulnerability detections to Open-Source Software using Agentless Scans
- Elevate the cloud workload security with more detections

Detect Secrets using Agentless

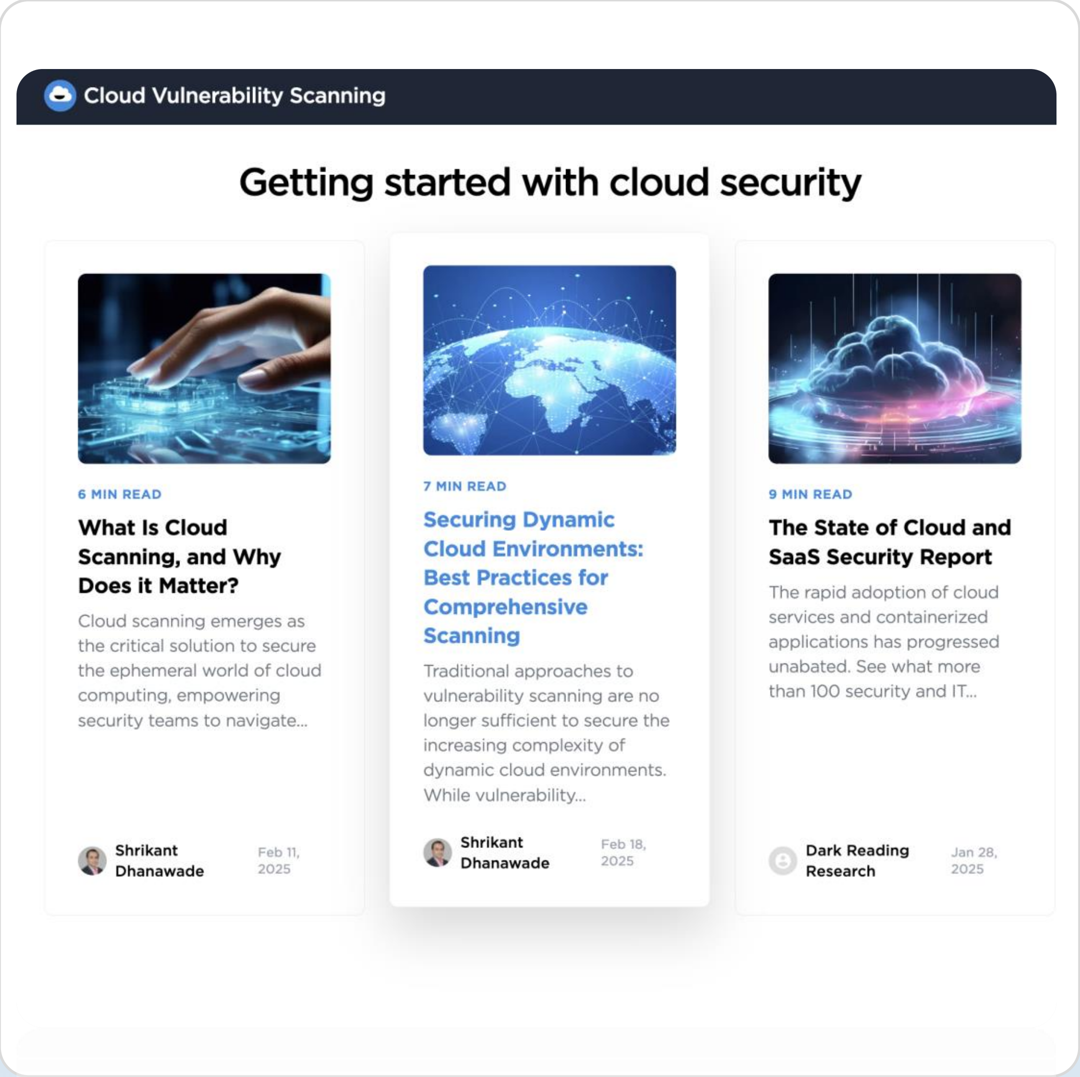
- Covers secrets of Cloud and SaaS providers
- Correlate the secrets on the exposed assets with vulnerabilities and misconfigurations

Qualys's Cloud Vulnerability Scanner

Website that showcases our expertise

https://www.cloudvulnerabilityscanner.com/

- **Updates on the latest cloud threats**
  How experts address them?
- **Statistics on the most common cloud security issues**
  How many do you have?
- **Dive in with more cloud scanning articles**
  Elevate your knowledge in specific areas



Cloud Vulnerability Scanning

Getting started with cloud security

6 MIN READ

What Is Cloud Scanning, and Why Does it Matter?

Cloud scanning emerges as the critical solution to secure the ephemeral world of cloud computing, empowering security teams to navigate...

Shrikant Dhanawade — Feb 11, 2025

7 MIN READ

Securing Dynamic Cloud Environments: Best Practices for Comprehensive Scanning

Traditional approaches to vulnerability scanning are no longer sufficient to secure the increasing complexity of dynamic cloud environments. While vulnerability...

Shrikant Dhanawade — Feb 18, 2025

9 MIN READ

The State of Cloud and SaaS Security Report

The rapid adoption of cloud services and containerized applications has progressed unabated. See what more than 100 security and IT...

Dark Reading Research — Jan 28, 2025

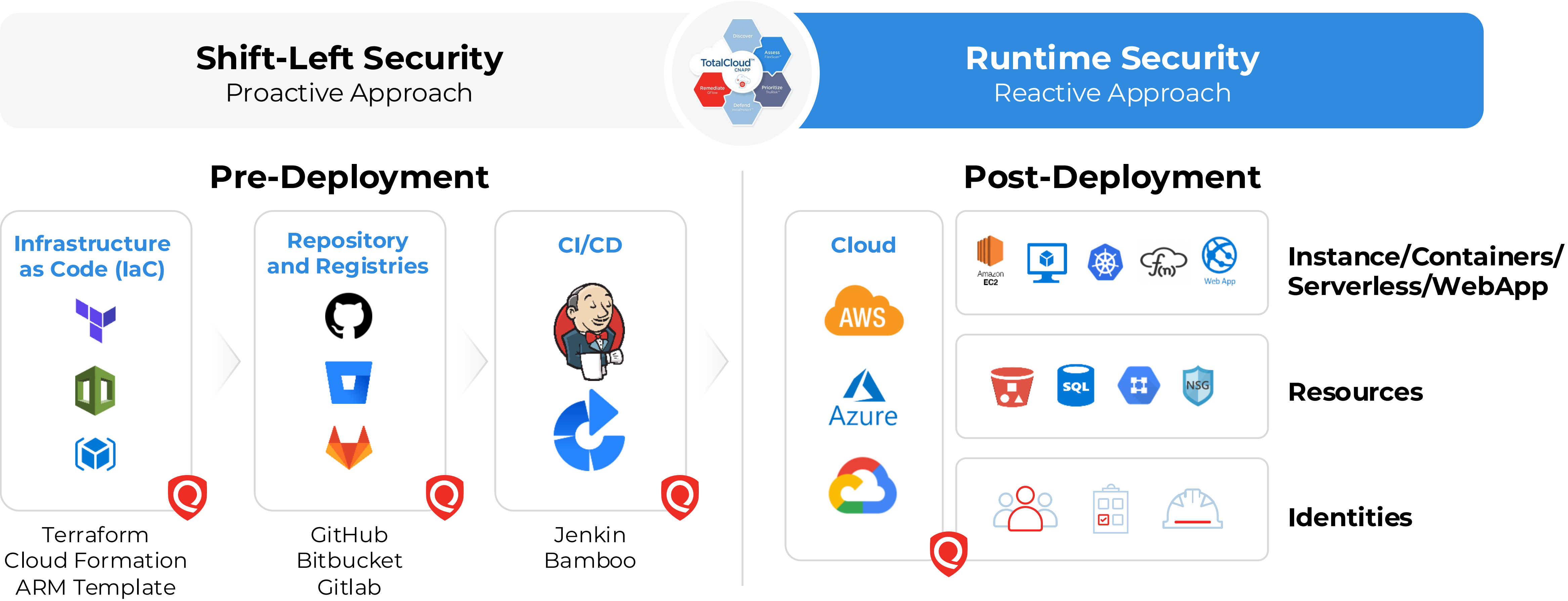
Qualys offers a Free customized TruRisk Insights Report.

We continue the Innovation Journey!

Qualys®

Shift Left in Cloud Security

Evaluate Code before deploying to the Cloud



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

Instance/Containers/ Serverless/WebApp

Resources

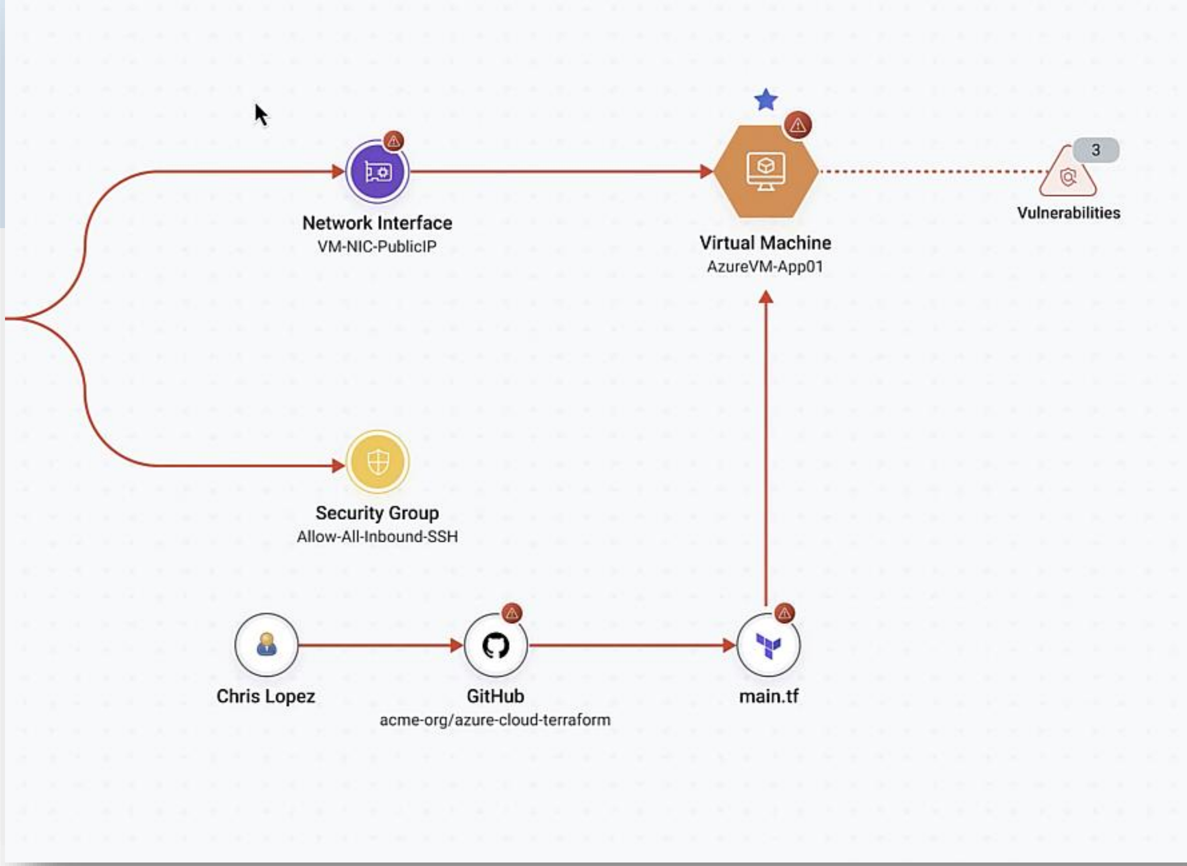
Identities

Bringing Risk Remediation to the Code

Turbocharge the code prioritization with run time security risk insights

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.



Industry and Customer Recognition

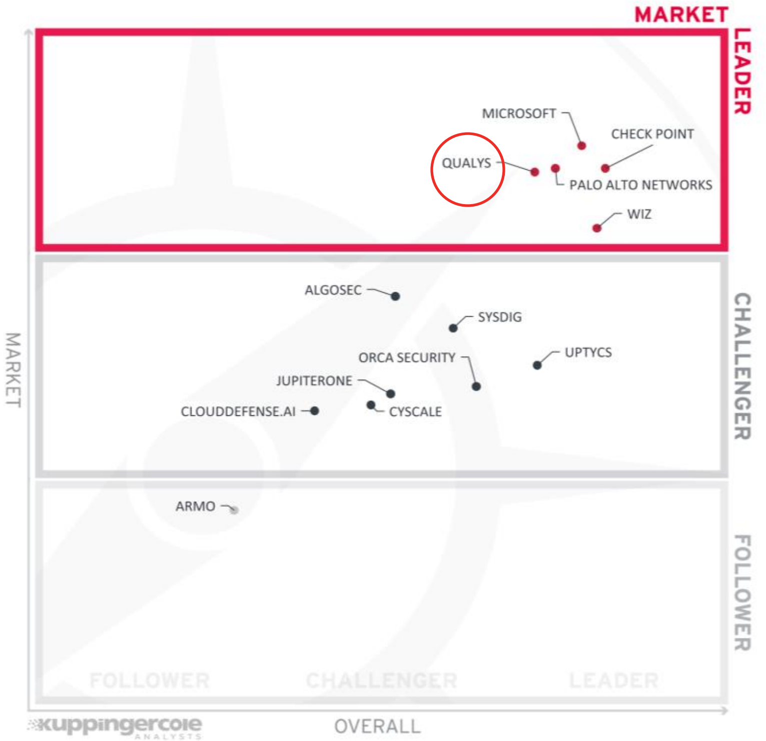
Qualys®

Cloud Security Market Recognition

Recognized By Analysts. Trusted By Enterprises.

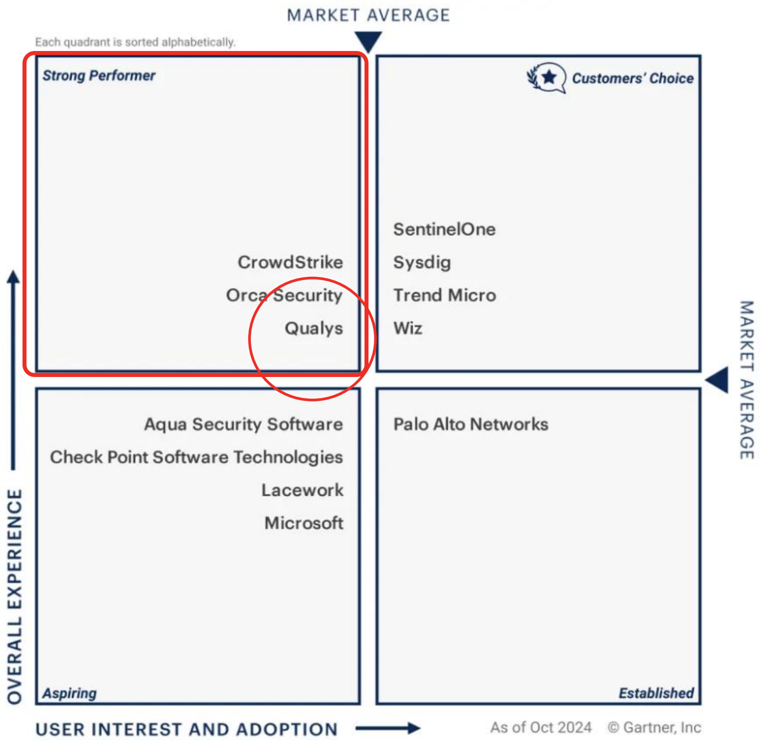
KuppingerCole

2024 Leadership Compass for CSPM



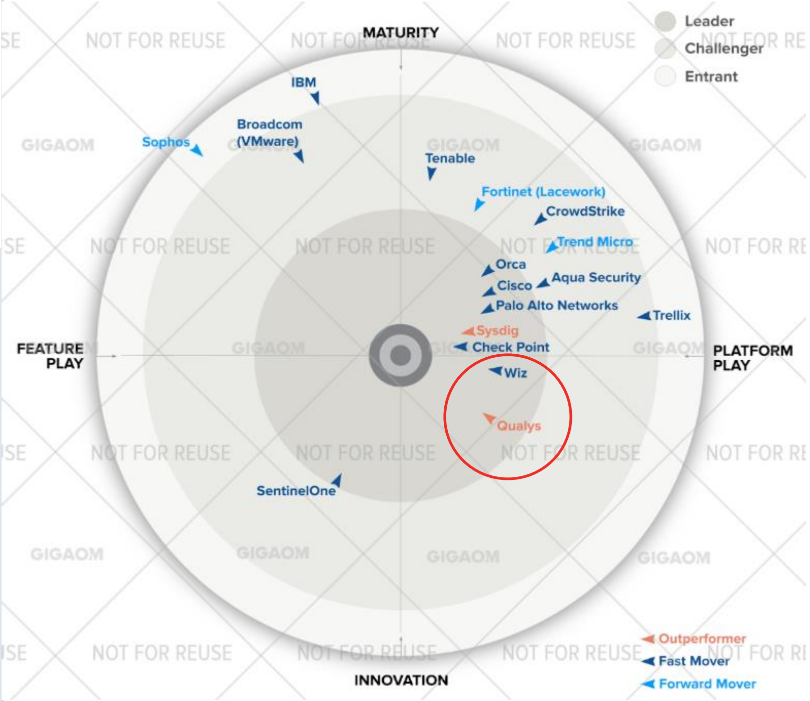
Gartner

2024 Peer Insights Voice Of The Customer - CNAPP



GigaOm

2025 Cloud Workload Security Radar



Demo

Qualys.

Free Custom Report

Do you know the biggest risk to your multi-cloud and container environment?

Get your free custom assessment today!

Qualys®

Enterprise TruRisk™ Platform

Measure, communicate, and eliminate cyber risk.

De-risk your business.