VMDR for Multi-Cloud

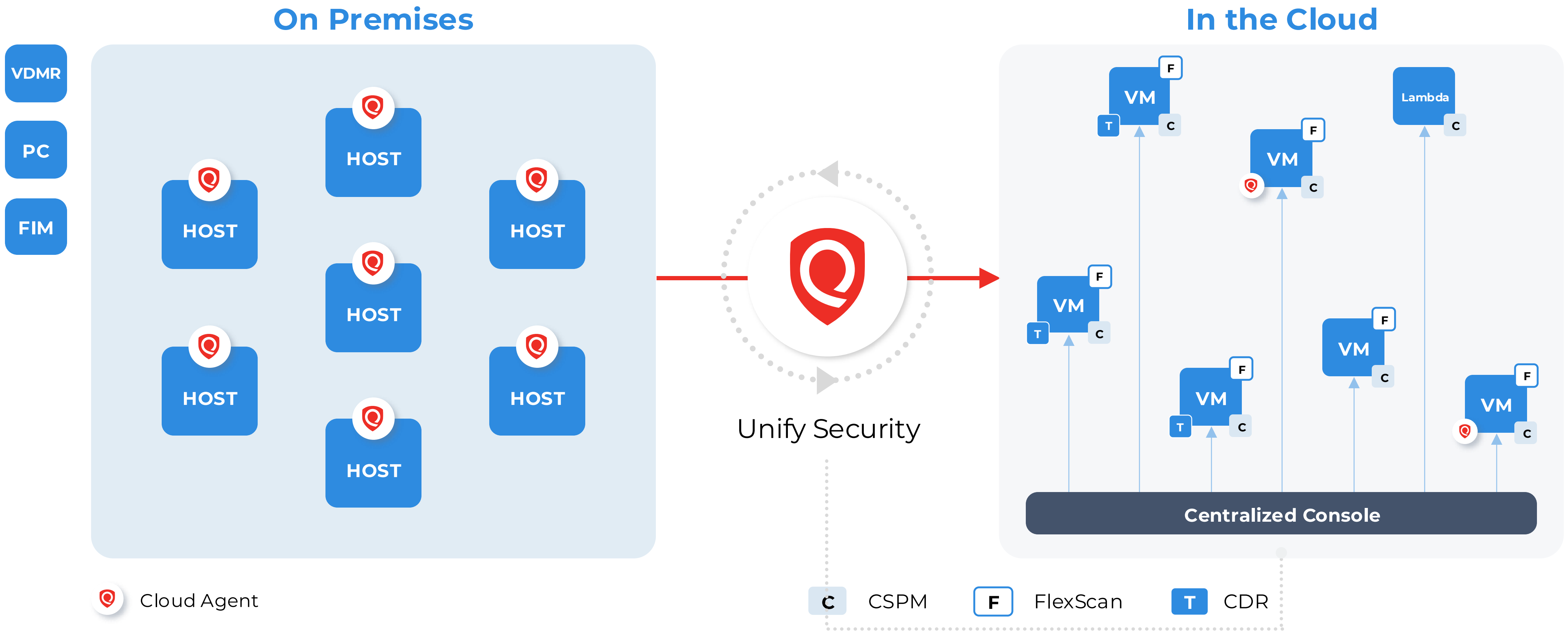
A Single CNAPP Platform for VMDR, CSPM, CWP, KCS, CDR and SaaSPM

Kunal Modasiya
Vice President, Product Management
Cloud & Container Security
Attack Surface Management, Web App & API Security

Thank You VMDR Customers !!!

We want to accelerate your journey to the cloud

It starts with bringing On-Prem and Multi-Cloud together



Cloud migrations are not easy, We understand that !!!

Cloud migrations are leading to challenges for security, vulnerability management and DevOps teams

Cloud Security Challenges

Multi-Cloud Visibility Gaps	Can I inventory my entire infrastructure with **100% visibility across all clouds?**
Identity Proliferation	Can we manage **identities and entitlements** in cloud infrastructure?
Securing dynamic workloads	Can we balance **development agility and security** effectively in our VMs and container orchestration?
Fragmented DevSecOps	Can we integrate security tooling within our rapid deployment cycles, and **shift left at scale**?
Shared Responsibility Model Confusion	Can we ensure all security aspects are adequately covered between us and the **cloud provider**?

And breaches are only increasing for this vector of attack.

01 In 2023, a F500 organization disclosed that a **cloud misconfiguration** had **exposed** the data of approximately **200,000+ customers**

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 buckers**

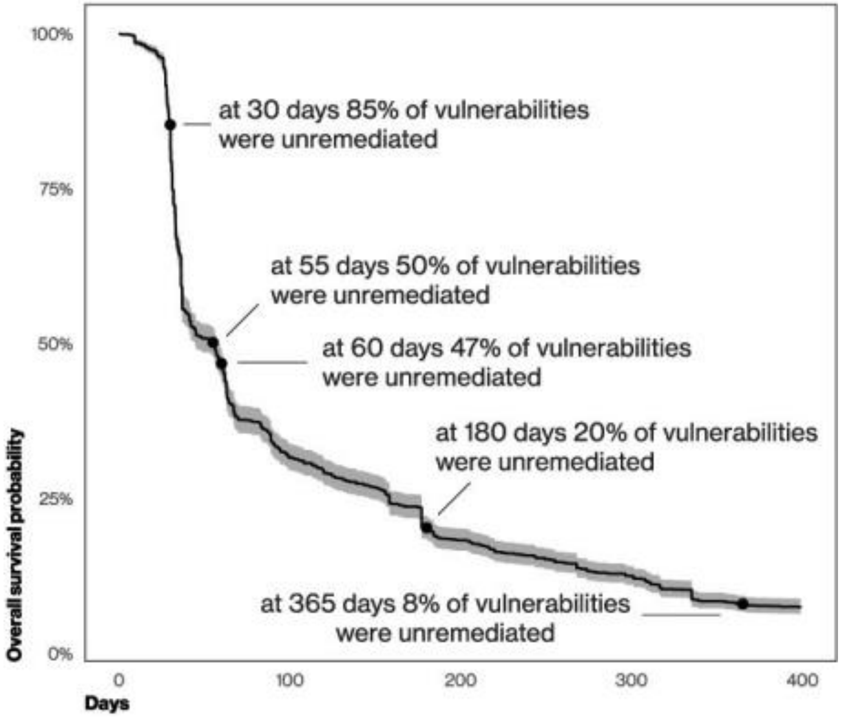
These are not isolated instances - Its pervasive

65% **Misconfiguration and unauthorized access** are their top cloud security concern

56% Having a more **complex multi-cloud** environment than expected

57% Maintaining **compliance in cloud environments** as challenging

44% Have delayed or slowed application deployment due to **container security concerns**



at 30 days 85% of vulnerabilities were unremediated

at 55 days 50% of vulnerabilities were unremediated

at 60 days 47% of vulnerabilities were unremediated

at 180 days 20% of vulnerabilities were unremediated

at 365 days 8% of vulnerabilities were unremediated

Figure 19. Survival analysis of CISA KEV vulnerabilities

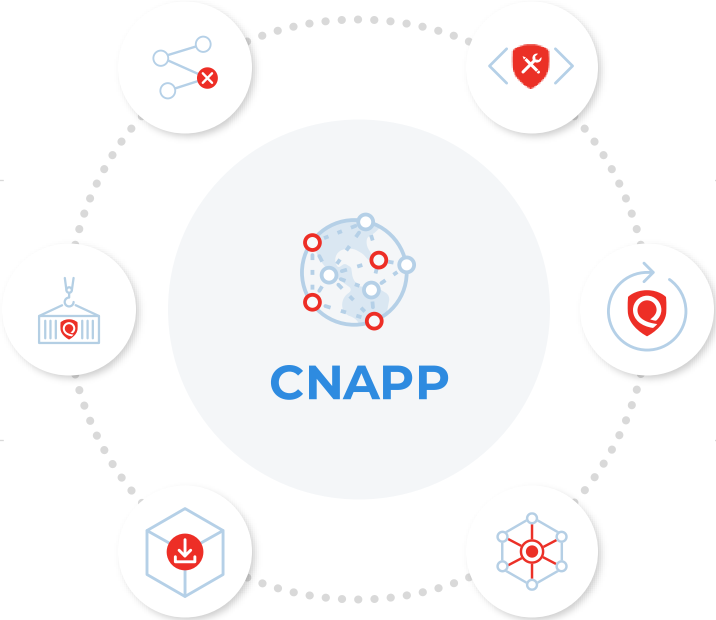
Source: Verizon DBIR Report 2024

Cloud Security is a key component for a comprehensive risk management strategy

...as new attack vectors continues to emerge

Cloud Native Application Protection Platform (CNAPP) are critical for your risk management

Core Cloud Security Functions in One Solution



Vulnerability Assessments (CWP)

Kubernetes and Container Security (KCS)

Runtime Threats (CDR)

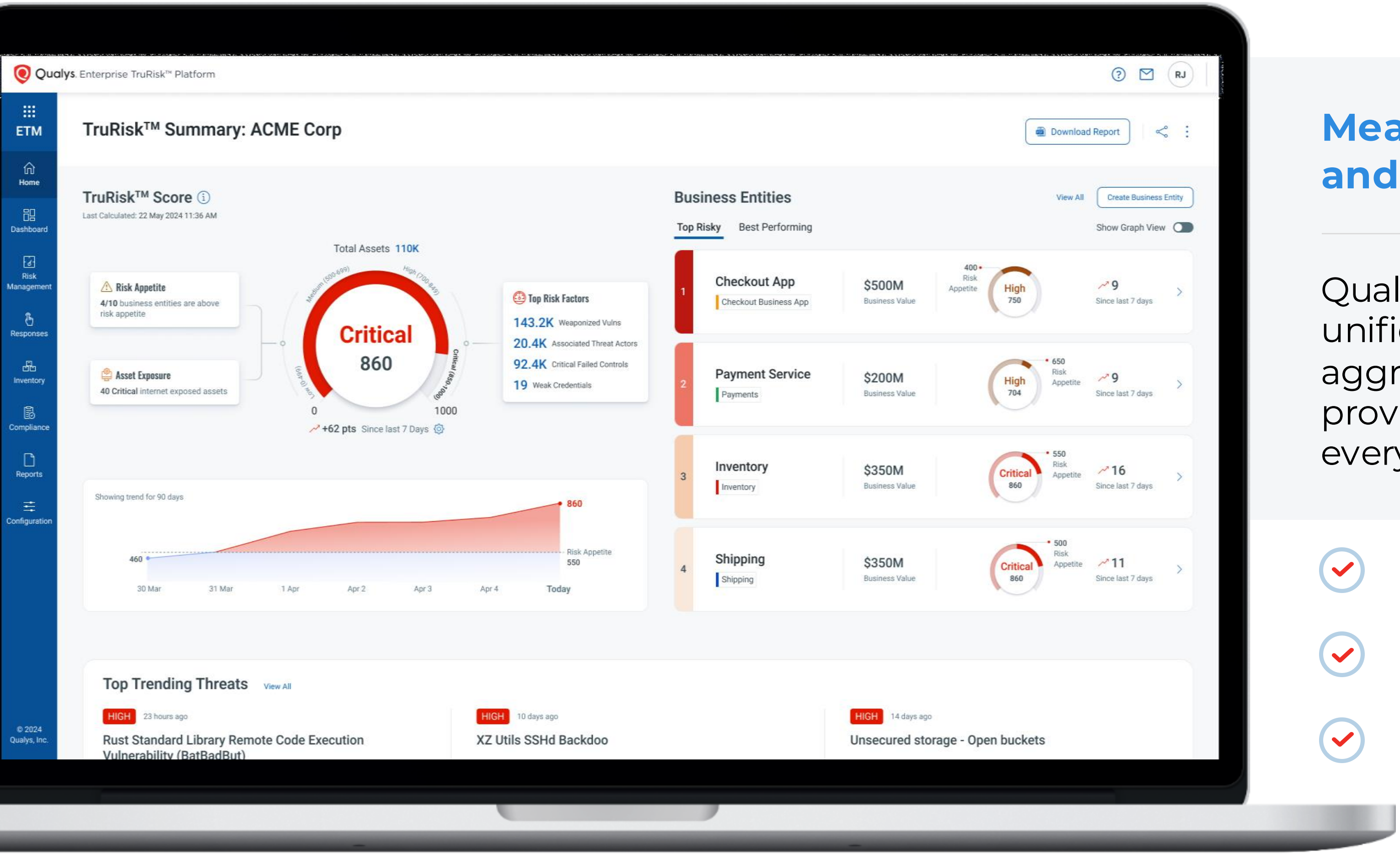
Misconfiguration (CSPM)

Cloud Infrastructure and Entitlement Management (CIEM)

Cloud Workflow Automation (CWA)

Qualys Enterprise TruRisk Management (ETM)

World's First **Risk Operations Centre** in the Cloud



TruRisk™ Summary: ACME Corp

TruRisk™ Score

Last Calculated: 22 May 2024 11:36 AM

Total Assets 110K

Critical 860

+62 pts Since last 7 Days

Risk Appetite: 4/10 business entities are above risk appetite

Asset Exposure: 40 Critical internet exposed assets

Top Risk Factors

- 143.2K Weaponized Vulns
- 20.4K Associated Threat Actors
- 92.4K Critical Failed Controls
- 19 Weak Credentials

Business Entities

	Entity	Business Value	TruRisk	Risk Appetite	Since last 7 days
1	Checkout App Checkout Business App	$500M	High 750	400	9
2	Payment Service Payments	$200M	High 704	650	9
3	Inventory Inventory	$350M	Critical 860	550	16
4	Shipping Shipping	$350M	Critical 860	500	11

Top Trending Threats

- HIGH 23 hours ago: Rust Standard Library Remote Code Execution Vulnerability (BatBadBut)
- HIGH 10 days ago: XZ Utils SSHd Backdoo
- HIGH 14 days ago: Unsecured storage - Open buckets

Measure, Communicate, and Eliminate Risks

Qualys Enterprise TruRisk Management (ETM) unifies asset management, vulnerability aggregation, risk assessment in one platform, providing real-time, contextual risk insights across every environment.

- ✓ Unified View of Risk Posture
- ✓ Enriched & Prioritized Risk Data
- ✓ Automated Risk Orchestration

With Qualys TotalCloud CNAPP, you can create a single prioritized view of risk for your Multi-cloud, container and SaaS environments

...and turbocharge your ROC Journey

Qualys TotalCloud CNAPP

Unified Cloud Security, Vulnerability, Compliance, and Threat Management

Vulnerability Assessments (CWP)

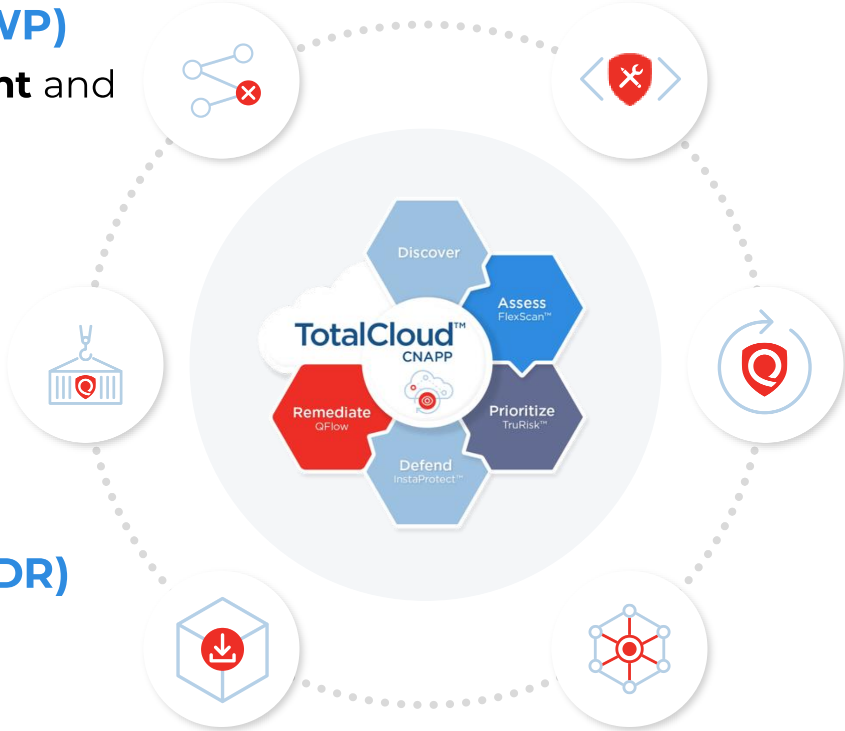
Flexible Vulnerability scanning (**agent** and **agentless**) with six sigma accuracy

Kubernetes and Container Security (KCS)

Container Security from
Development to Runtime

Runtime Threats Detection (CDR)

- Detect Runtime Threats
- **Deep Leaning AI**



Cloud Security Posture Management (CSPM)

- Multi-Cloud Inventory
- **Compliance**
- IaC Scanning

Cloud Infrastructure and Entitlement Management (CIEM)

- Identity Inventory
- Managing **Excessive Permissions**

Cloud Workflow Automation (CWA)

- **Custom Control**
- Automated Remediation

So how does TotalCloud CNAPP help with risk prioritization?

Comprehensive Multi-Cloud Visibility

Complete visibility across all cloud and containerized workloads

Scale Cloud Posture Assessments

Enriched cloud posture and vulnerability management

Secure Cloud Identity and Entitlements

Comprehensive view of cloud infrastructure entitlements and inventory

Secure Kubernetes and Containers

Discover, monitor and secure your Kubernetes and container environments

Drive risk prioritization with context and correlation with TruRisk Insights

Visibility is a key part of Risk Management

Comprehensive inventory crucial for the cloud

All environments

Across all clouds, containers, hybrid workloads

Comprehensive Inventory

Across all inventory and resource types

Accelerated Deployments

Simplified and quick onboarding driving visibility within minutes

AWS

- Directory Service
- KMS
- S3
- EBS
- Mesh
- Route 53 Record
- Network ACL
- VPC Endpoint
- Lambda Function
- SES Identities
- ACM Certificate
- MQ Broker
- Transit Gateway
- Neptune DB Clusters
- Neptune DB Instances
- ES Domain
- Redis
- Dynamo DB Table
- Memcached
- RDS
- EC2 Images

Azure

- Log Analytics Workspace
- WAF Web Policies
- Frontdoor WAF
- Secret
- Key Vault
- Front Door
- Storage Container
- Data Explorer Cluster
- Data Factory
- Container Registry
- SQL Server
- SQL Server Database
- Virtual WAN
- Cognitive Search
- Data Lake
- Synapse Workspace
- API Management Service
- Disk Access

GCP

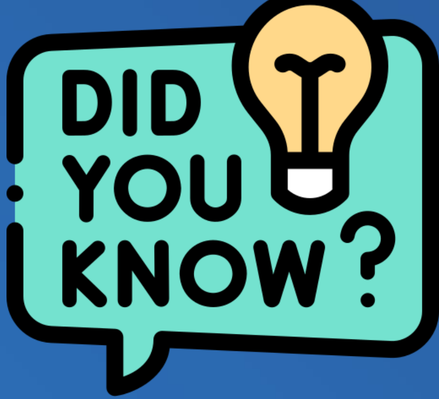
- Networks
- Sub Networks
- Firewall Rules
- Storage
- Disk Snapshots
- Disk Images
- Cloud Armor
- Cloud DNS
- Cloud Run Services
- Cloud Functions
- SQL
- Spanner Instance Database
- BigTable Instance Cluster
- Service Account
- Cryptographic Key
- PubSub
- Artifact Registry Repositories
- Dataproc

OCI

- Security List
- Key
- Big Data Service Clusters
- Data Flow Application
- API Gateway
- Functions Applications
- Boot Volume
- Bucket
- Block Volume
- DB Systems
- Compute Instance
- IAM User
- Autonomous Database
- File System
- Block Volume Backup
- Load Balancer
- Kubernetes Cluster
- Mount Targets

and many more...

TotalCloud CNAPP covers ~ 200 services across 4 major cloud providers



VMDR Customers: You have access to free *TotalCloud connectors* for full cloud inventory as part of your subscription

Drive posture assessments to the cloud with our Cloud Security Posture Management (CSPM)

Ensure complete visibility across your stack

- Continuous discovery and inventory of **multi-cloud** resources
- Setup in minutes using **cloud provider APIs**

Continuously assess risk and prioritize threats

- **1000+ out of the box** security controls
- **No code automation** for remediation and custom controls

Qualys TotalCloud CSPM

Cloud Posture Assessments

- Identify threats caused by **misconfigurations** and non-standard deployments
- Validate with latest **CIS v3.0.0** benchmarks

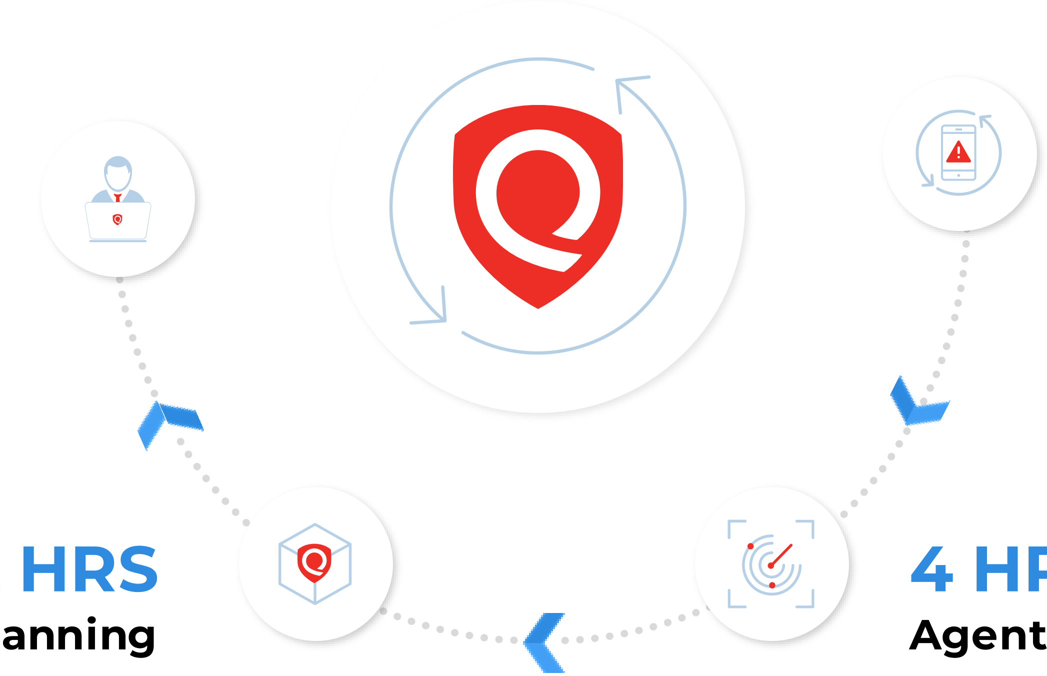
Ensure reporting and compliance

- Prevent fines due to compliance violations (e.g., **GDPR, PCI**)
- **Compliance monitoring of 35+** global compliance mandates

Three Fortune 50 banks use TotalCloud CSPM to scale compliance and be Audit Ready

Scale Vulnerability Management with our Cloud Workload Protection (CWP)

Enterprise-grade Vulnerability Scanning for On-Prem and Cloud Infrastructure



24 HRS

Snapshot Assessment

Efficiently capture workload snapshots and perform vulnerability assessments

10 Min

API Assessment

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

12 HRS

Network Scanning

Quickly and accurately assess for network-related vulnerabilities

4 HRS

Agent Scanning

Real-time comprehensive vulnerability, configuration and security assessments

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

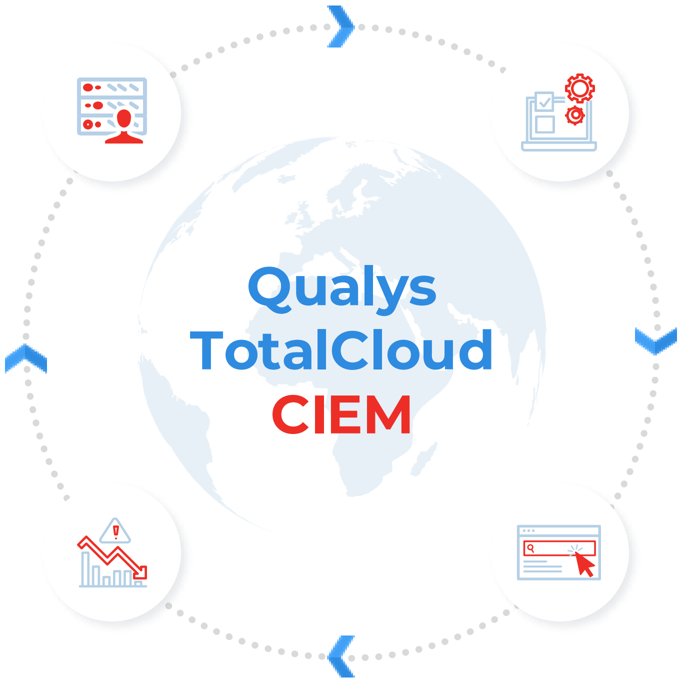
Secure cloud identity with our Cloud Identity and Entitlement Management (CIEM)

Discover Identities and Permissions

- Inventory of **users, roles, and cloud services** using the identities
- Permissions and entitlements

Remediate to reduce Risk

- **Reduce permissions** with overly permissive identities
- Use **automation workflows** to scale response



Assess and Monitor

- **Overly permissive entitlements** and unused identities
- Monitor **new identities, permissions, and events** from cloud provider

Prioritize with TruRisk Insights

- Identify the impacted resources and **potential lateral movements**
- **Prioritize response** and drive remediations at scale

Large industrial manufacturer in Europe enhances cloud identity context with TotalCloud CIEM

Secure your DevOps cycle with our Kubernetes and Container Security (KCS)

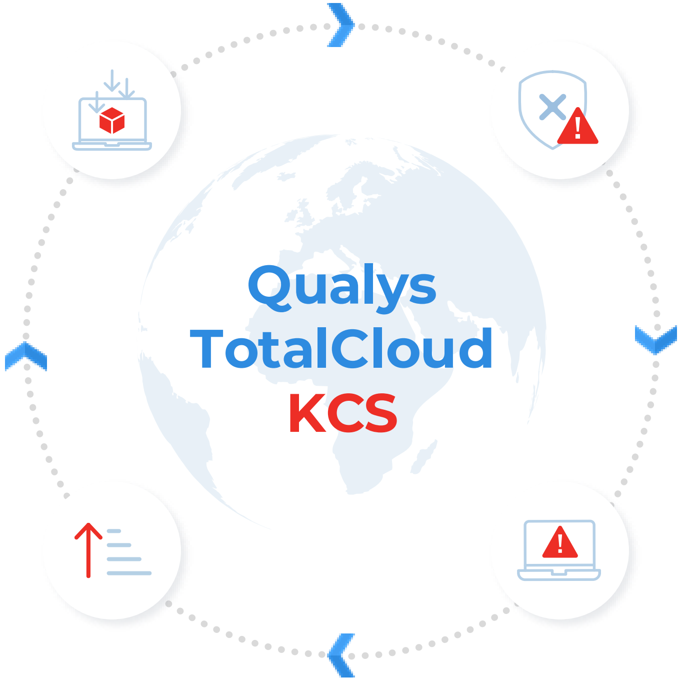
Manage and Mitigate Risk end-to-end for the entire DevOps Pipeline

Container Discovery and Inventory

- Manage and **inventory container images on hosts, clusters, registry**
- Manage and inventory container images built in **official builds (CI/CD)**

Drive Policy Compliance

- **CIS for Docker**
- PCI 4.0 (Risk based Vulnerability Management & File Integrity Monitoring for Containers)



Risk Assessment

- **Identify vulnerable first party and third-party code**, and malware in images
- **TruRisk for K8s clusters** and risky containers

Threat Management

- **Detect zero-day malware** in containers using deep learning
- Respond and manage threats with **workflow automation, and integrations**

Fortune 10 bank uses TotalCloud KCS to secure from development to runtime, scanning 6.5 Million container images per month

Drive automated risk correlation with TruRisk Insights

Contributing factors

- Internet Exposure
- Vulnerabilities
- Active Threats
- Misconfigurations
- Access Permissions

TruRisk Insights

TruRisk Insights

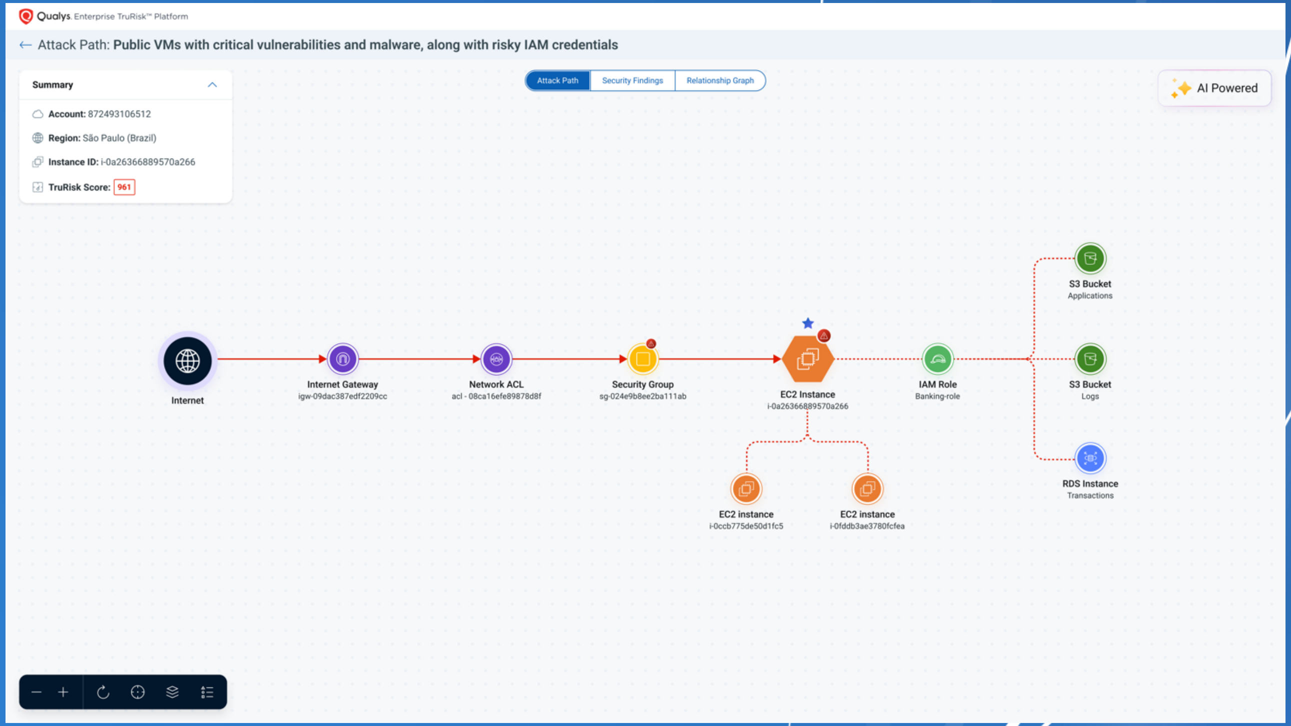
- ✓ Public VM with write access on database
- ✓ Public VM with privilege to create IAM artifacts (User, Group, Role)
- ✓ Critical exploitable vulnerability on public VM with destructive permissions for AWS KMS
- ✓ Public VM with the privilege to create IAM artifacts (User, Group, Role)

TruRisk Insights creates a single prioritized view of risk

TruRisk Insights provides comprehensive risk prioritization

We are excited to enhance it by visualizing and analyzing context

Announcing TotalCloud Attack Path



Attack Path: **Public VMs with critical vulnerabilities and malware, along with risky IAM credentials**

Summary

Account: 872493106512

Region: São Paulo (Brazil)

Instance ID: i-0a26366889570a266

TruRisk Score: 961

Why Attack Path?

TruRisk Insights prioritizes risks with context

Attack path helps visualize the context and **understand risk propagation**

Prioritize with **TruRisk Insights**

Analyze with **Attack Path**

Remediate with **Workflow Automation**

TotalCloud 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

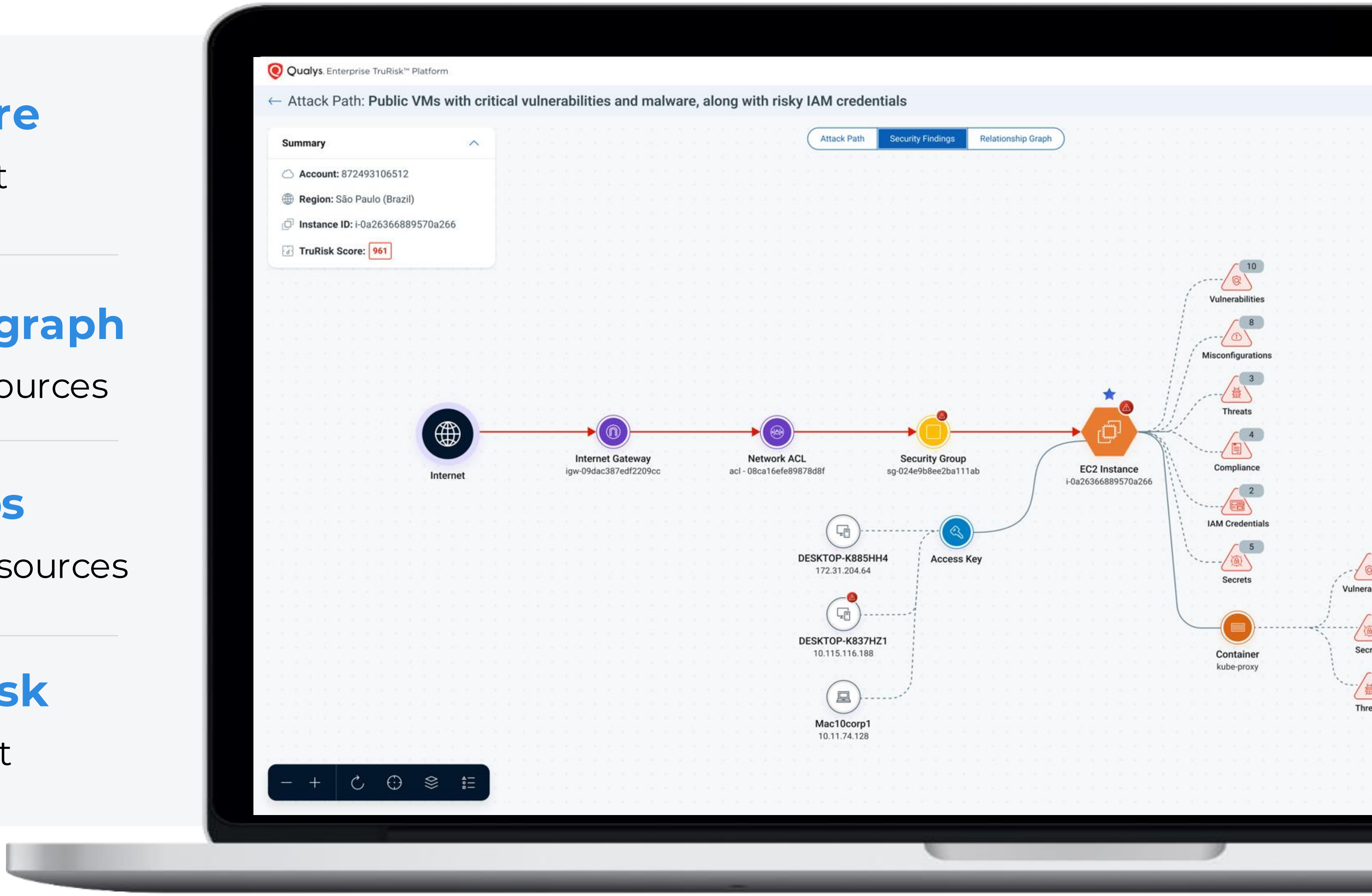
Navigate to important findings on critical resources

Understand resource relationships

Capture communication flows of attached resources

Scale with rapid remediation of risk

Drive accelerated risk-based prioritized threat remediation



Qualys. Enterprise TruRisk™ Platform

← Attack Path: **Public VMs with critical vulnerabilities and malware, along with risky IAM credentials**

Summary

Account: 872493106512

Region: São Paulo (Brazil)

Instance ID: i-0a26366889570a266

TruRisk Score: 961

DE-RISK YOUR **BUSINESS**

Qualys.

Want to see how you can break organizational silos, and scale remediation with automation?

Qualys Cloud Workflow Automation (QFlow)

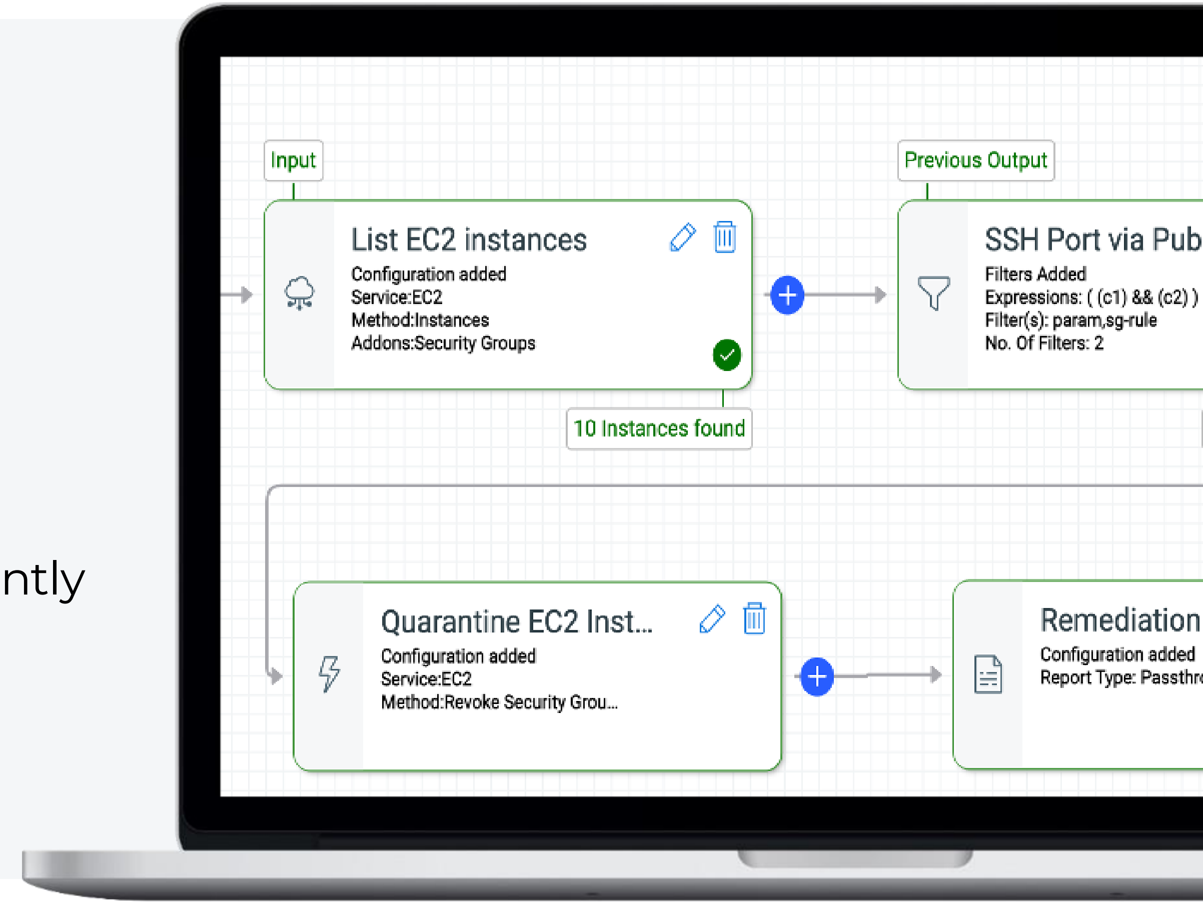
No Code / Low Code

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 programs efficiently

Orchestrate remediation workflows and integrate with DevOps and ITSM tools



Input

List EC2 instances
Configuration added
Service:EC2
Method:Instances
Addons:Security Groups

10 Instances found

Previous Output

SSH Port via Pub
Filters Added
Expressions: ((c1) && (c2))
Filter(s): param,sg-rule
No. Of Filters: 2

Quarantine EC2 Inst...
Configuration added
Service:EC2
Method:Revoke Security Grou...

Remediation
Configuration added
Report Type: Passthr

Demo

Can I deploy and Operationalize this in minutes?

Now, lets hear from, Syntax, on how they scaled up their cloud security program

…and drove vulnerability management and compliance to the cloud