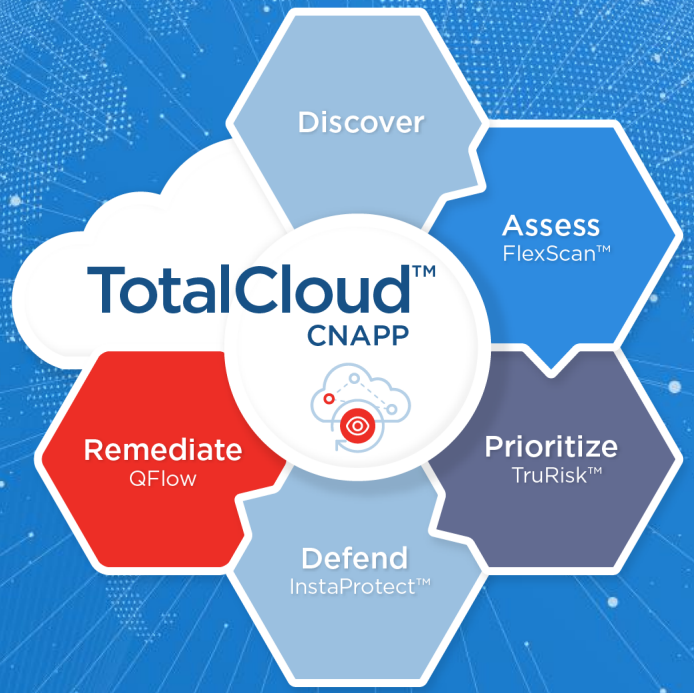
Qualys

Qualys TotalCloud™

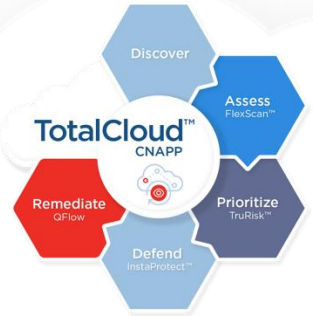
Unified Vulnerability, Threat and Posture Management - From Development to Runtime



Qualys

The Qualys Approach to Cloud Security

Aggregate, Unify, and Contextualize Risk



Cloud Inventory
Attack Surface Risk Management

Detect and Prioritize,
Vulnerabilities, Misconfigurations

Map, Remediate Threats with Remediation
Workflows

Respond and Prevent Threats with Risk, Business Context

Drive Compliance
Monitoring and Reporting

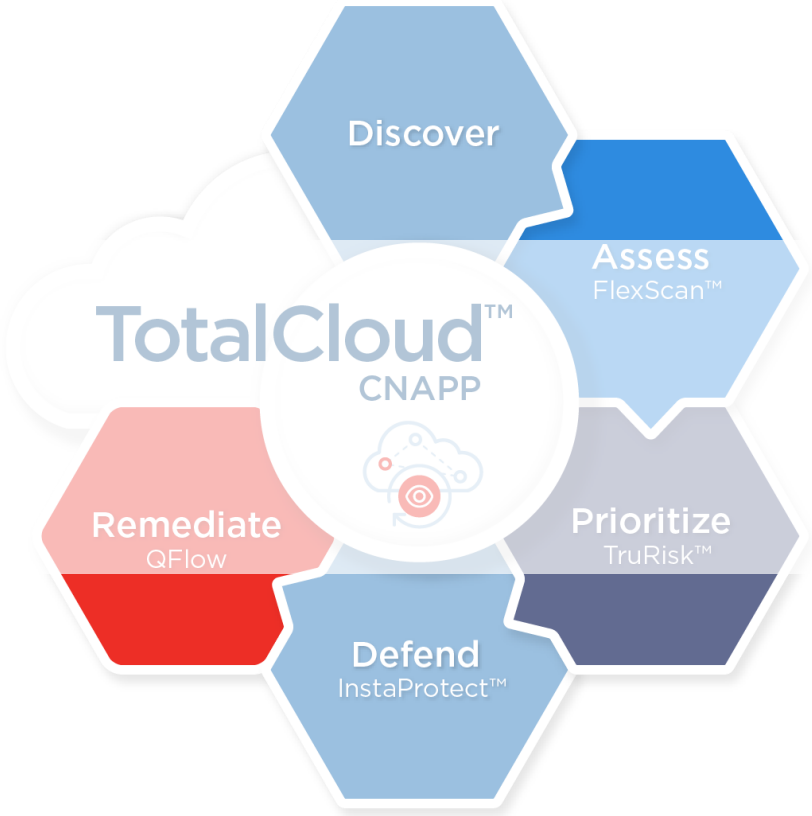
Asset Management → Vulnerability & Configuration Management → Risk Remediation → Threat Detection Response → Compliance

First-Party OSS

API | LIGHTWEIGHT AGENT | PLATFORM SERVICES | SENSORS

3rd Party Data

APPLICATIONS | OPERATING SYSTEMS | CLOUD / CONTAINERS / VMs | IT / WORKSTATIONS / SERVERS | IOT | EXTERNAL DEVICES



Introducing TotalCloud

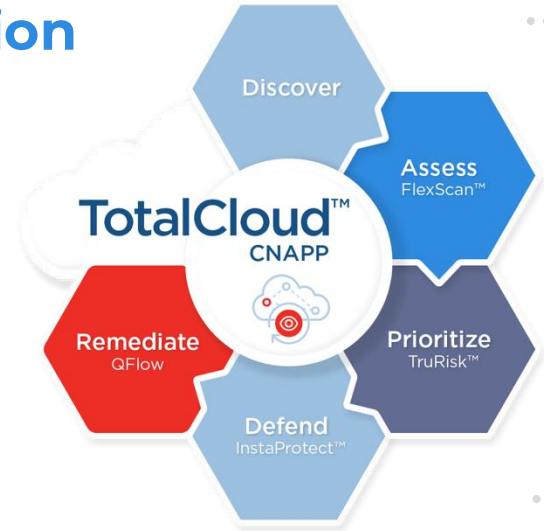
The Qualys Approach to CNAPP

Qualys.

Qualys TotalCloud: AI-powered CNAPP

Unified Vulnerability, Threat and Posture Management

Start secure and stay secure with a real-time AI CNAPP solution



Cloud Security Posture Management (CSPM)
Inventory of public cloud resources. Detection and remediation of misconfigurations and non-standard deployments, including Infrastructure as Code (**IaC**) Security

Cloud Workload Protection (CWP)
Scanning for vulnerabilities in the cloud environment (VMDR with FlexScan).

Cloud Detection and Response (CDR)
Continuous real-time protection of the multi-cloud environment against active exploitation, malware, and unknown threats.

Kubernetes & Container Security (KCS)
Discover, track, and continuously secure containers – from build to runtime.

Cloud Infrastructure Entitlement Management (CIEM)
Discover, track, and continuously manage identities and privileges in cloud environments.

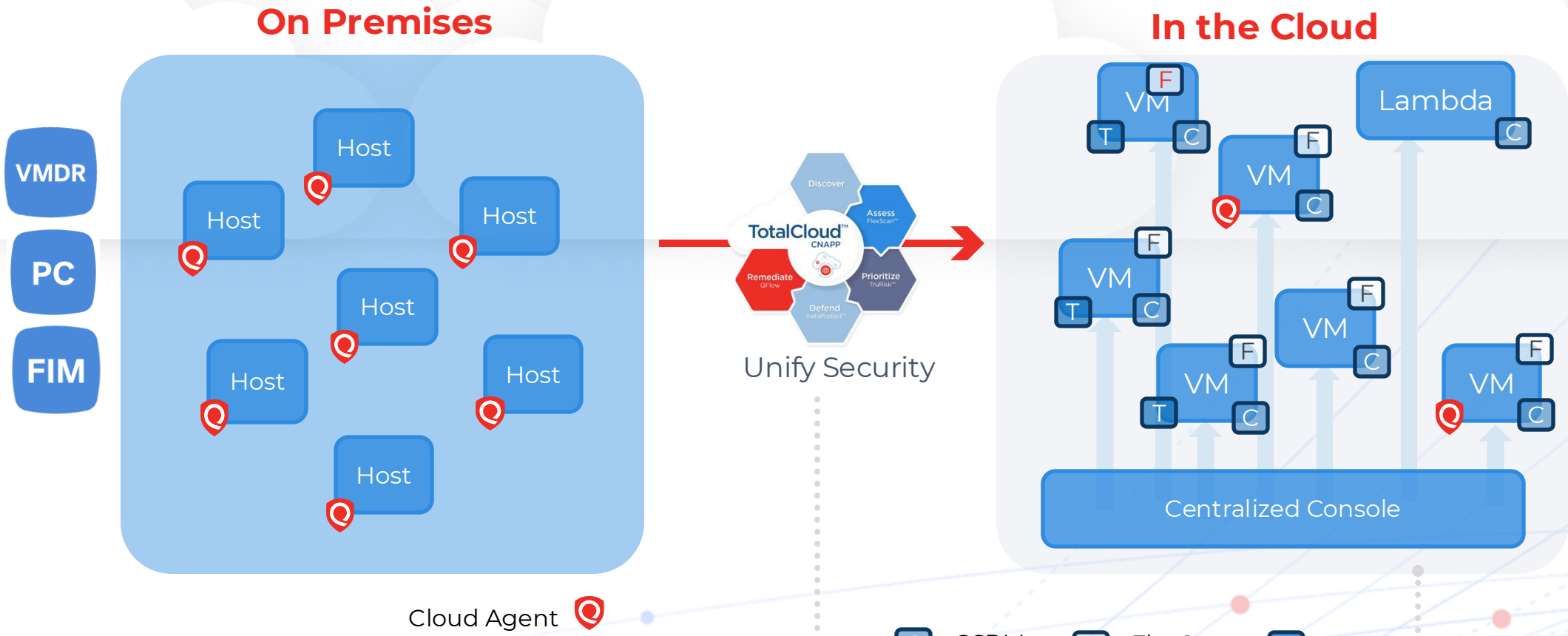
SaaS Security Posture Management (SSPM)
Manage security posture and risk across your entire SaaS application stack

*From **Development** to **Runtime***

1000+ customers are taking advantage of our AI CNAPP solution

On-Prem & Multi-Cloud

Bringing Together On-Prem and Multi-Cloud



Qualys.

Qualys

Identify and fix security risks in Cloud Infrastructure

Cloud Security Posture Management (CSPM)

Cloud Security Posture Management

Comprehensive inventory of cloud assets and their posture

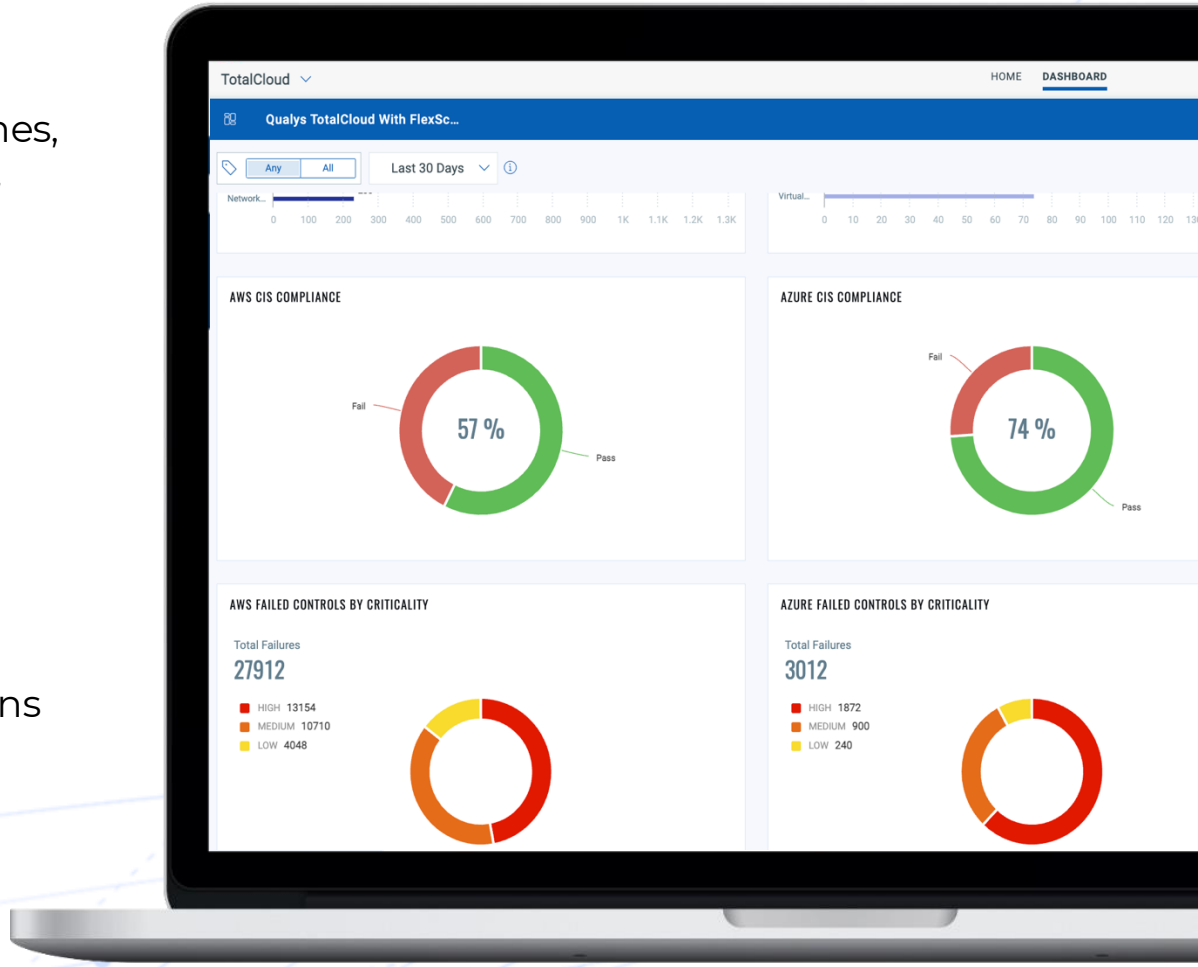
01 **Complete Inventory of all assets** compute (virtual machines, container, serverless) and cloud native (Storage, Database, networks)

02 **Out-of-box Compliance assessments reports for 30+ Mandates** such PCI DSS, HIPAA, GDPR, CIS Benchmarks,. Highest coverage in industry

03 **Shift Left IaC scanning** for misconfigurations, one dashboard.

04 **Automatically alert, ticket, or remediate** misconfigurations

05 **One-click remediation** for many high visibility controls



Qualys.

Cloud Infrastructure and Entitlement Management(CIEM)

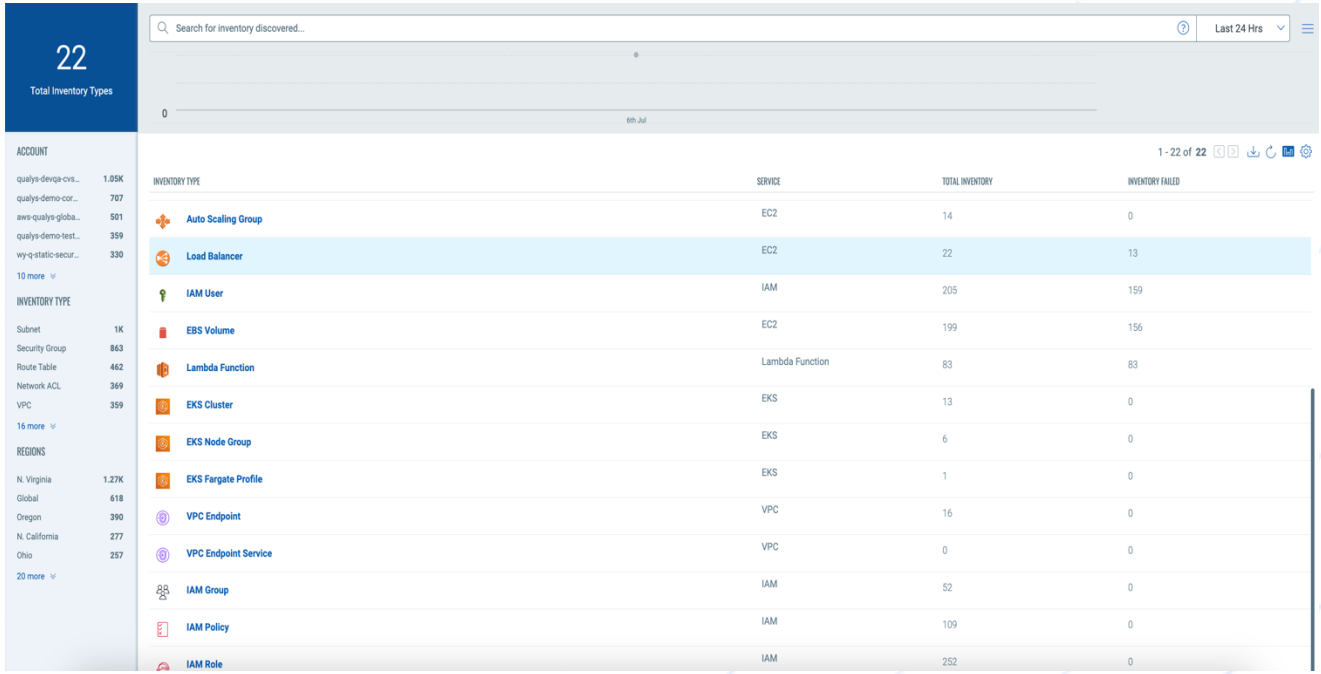
Identity and Permissions Management

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

02 Risky identities **determined based on analysis: e.g. administrator privileges, or privileges to create IAM artifacts**

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

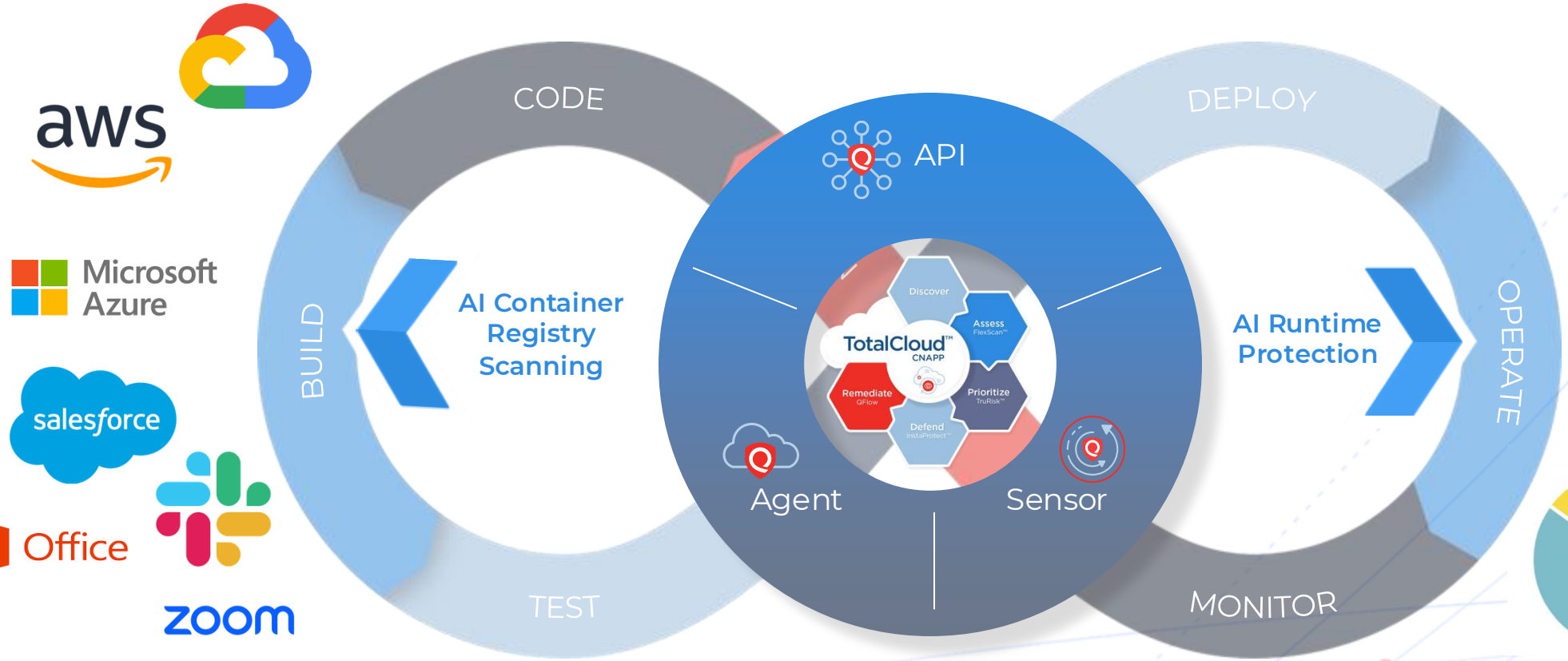
04 **Remediate**



Qualys.

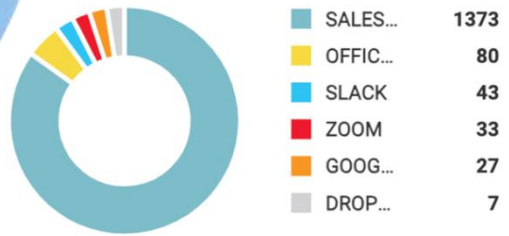
Comprehensive Inventory Functions

Users, Resources and SaaS Applications



INVENTORY TYPE	SERVICE
Instance	EC2
VPC	VPC
RDS	RDS
Subnet	VPC

INTERNAL USERS



Industry-leading inventory resource coverage across Multi-Cloud

Qualys.

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

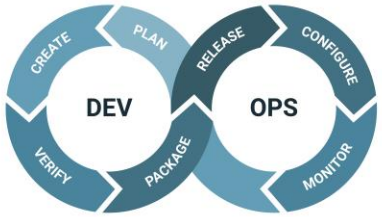
- IRDAI Guidelines On Information and Cyber Security for Insurers
- Reserve Bank of India (RBI) - Baseline Cyber Security and Resilience Requirements (Annex 1)

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)

Compliance for Any Mandate

By Vertical across SecOps, DevOps and Beyond



General / Sweeping Mandates

- 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy
- ANSSI 40 Essential Measures for a Healthy Network
- Australian Signals Directorate - Essential Eight Maturity Model
- CIS Controls Version 8
- General Data Protection Regulation (GDPR)
- ISO/IEC 27001:2013 / 27001:2022
- NCSC Basic Cyber Security Controls (BCSC)
- NESA UAE Information Assurance Standards (IAS)
- NIST 800-53 (Special Publication)
- NIST Special Publication 800-171
- The NIST Cybersecurity Framework (CSF)
- Sarbanes-Oxley Act: IT Security

Banking / FinTech

- Reserve Bank of India (RBI) - Baseline Cyber Security and Resilience Requirements (Annex 1)
- Payment Card Industry Data Security Standard (PCI-DSS) v3.2.1 / v4.0
- APRA Prudential Practice Guide (PPG): CPG 234 - Management of Security Risk in IT
- MAS - Notice 834: Cyber Hygiene Practices
- SWIFT Customer Security Controls Framework - Customer Security Programme v2021
- Technology Risk Management (TRM) Guidelines

Government / Federal

- Federal Risk and Authorization Management Program (FedRAMP L / LI-SaaS / M)
- IRS Publication 1075
- New Zealand Information Security Manual (NZISM)

Energy

- NERC Critical Infrastructure Protection (CIP)

Healthcare

- HIPAA Security Rule 45 CFR Parts 160/164, Subparts A/C:1996
- Minimum Acceptable Risk Standards for Exchanges (MARS-E)

Insurance

- IRDAI Guidelines On Information and Cyber Security for Insurers

Law / Legal

- CJIS Security Policy

Qualys.

Manage Risk in Your Cloud Infrastructure

...with Cloud Security Posture Management (CSPM)

Automate compliance with audit-ready compliance reports

- Both on-screen and printable reports out-of-box
- Persona-centric reports
- Compliance reporting from pre deployment(IaC Scanning) to run-time

Scalability (Enterprise-ready)

- Comprehensive multi-cloud support
- Scalable Multi cloud support for AWS, Azure, GCP and OCI
- Rapid M&A and Multi-site deployment

Qualys.

Qualys

Secure Cloud Workloads, Faster

Cloud Workload Protection (CWP)

Cloud Workload Protection

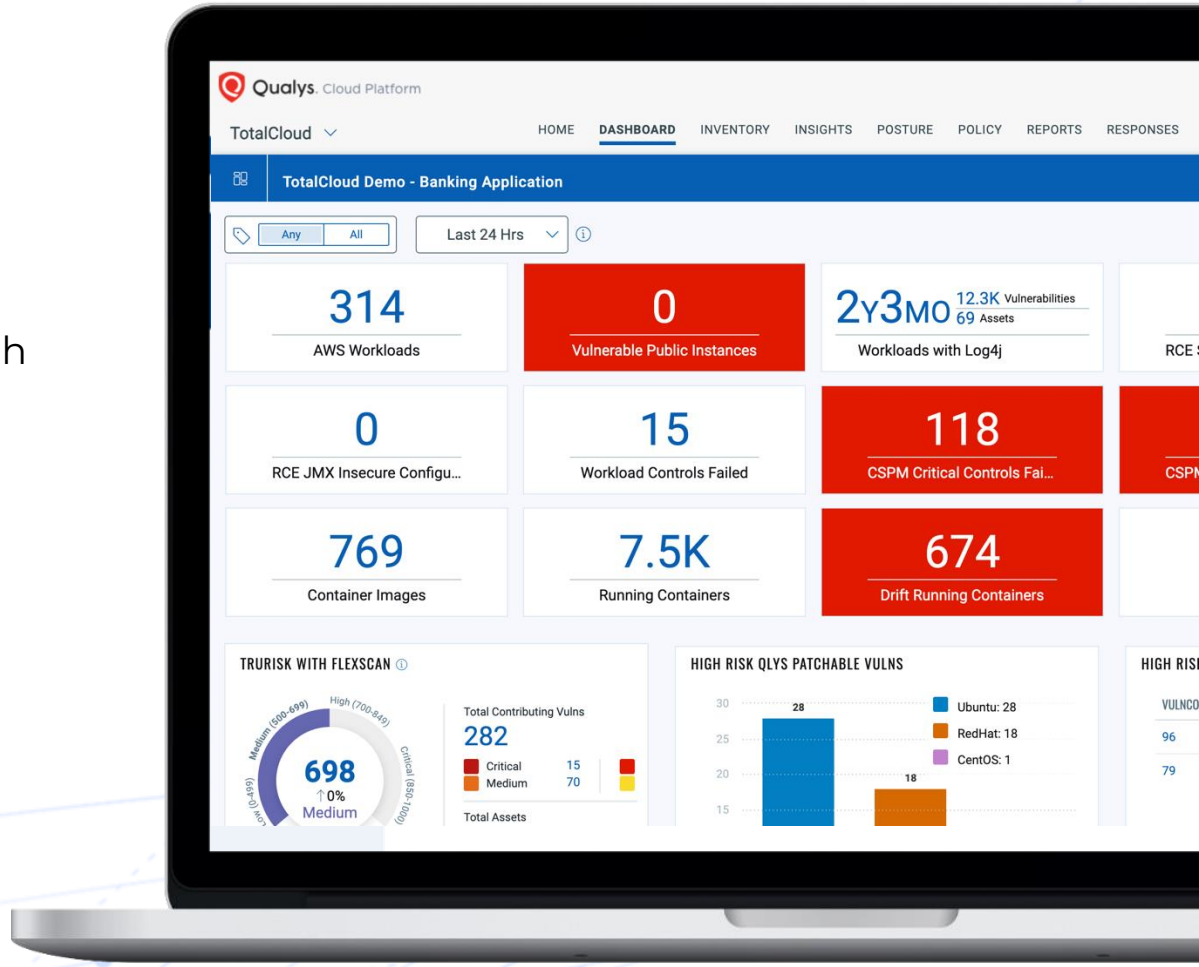
Eliminate blind spots and collapse attack path analysis mitigations

01 **100% continuous, coverage of all cloud workloads** using multiple agent and agentless vulnerability assessment methods

02 **Six sigma 99.9996% vulnerability detection accuracy** with 80K+ vulnerability signatures

03 Understand, manage, and **prioritize cybersecurity risk with TruRisk**

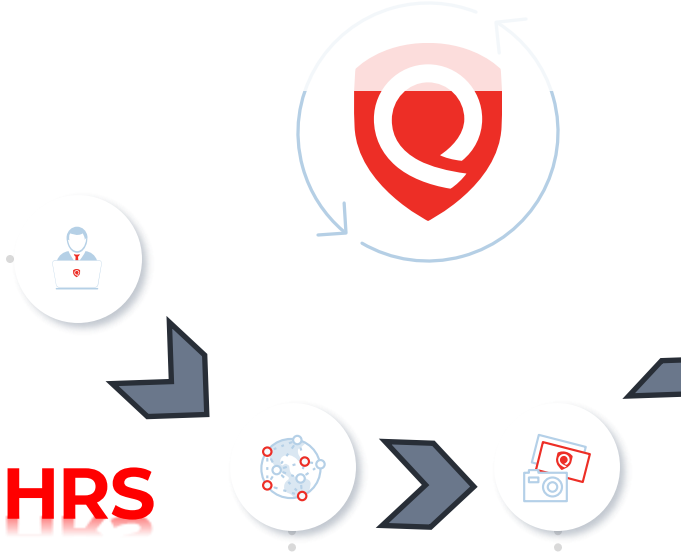
04 **Remediate threats faster** using patch management and building custom no-code workflows



Qualys.

How? No Blind Spots with FlexScan™

Scan Everything, Continuously, without Latency Implications



10 MIN

API Assessment

CSP-provided APIs collect software inventory for results in 15 min vs. 24 hours

4 HRS

Agent Scanning

Real-time comprehensive vulnerability, configuration and security assessments

12HRS

Network Scanning

Quickly and accurately assess for network-related vulnerabilities

24HRS

Snapshot Assessment

Efficiently capture workload snapshots and perform vulnerability assessments

Qualys.

Overview of Different Scanning Methods

Assessment Method	Strengths	Limitations
API-based Use CSP-provided APIs to collect software inventory and perform assessments	• **Fastest setup and assessment** • Ephemeral instances • Quick assessment on startup • Orchestrate as a part of CI/CD pipeline	• **Lack of OSS coverage**
Snapshot-based Take snapshot of the workload and perform vulnerability assessment on it	• **Fast and easy setup without access to the workload** • Quick assessment • Can scan suspended instances • M&A, Cloud migration, large scale deployment	• Less coverage as it looks at snapshots, from CSP's runtime block storage and then scans them • Expensive from resource standpoint • Does not work for hybrid environment, only public cloud • **Periodic scanning, 24 hrs. due to resource limitations**
Agent-based Real-time comprehensive vulnerability, configuration and security assessment	• Long-running workloads • **Detect runtime threats** • Workloads on which high accuracy vulnerability coverage is desired	• **Getting access to all workloads to run agents** • Difficult to deploy agent to ongoing deployments (shutdown workloads to deploy new agent)
Network-based Assess for network-related vulnerability related	• Easy to deploy • **Continuous, no need to stop the workload to inspect it.** • Detect runtime threats	• Getting access to all workloads to run agents • **Being able to access workloads at run time**

Secure Cloud Workloads, Faster.

...with Cloud Workflow Protection (CWP)

Unified Vulnerability Management on On-Prem and Cloud

- Comprehensive vuln scanning across hybrid and multi-cloud environment with industry leading VM solution

Eliminate blind-spots across all workloads (Built-in FlexScan™)

- Purpose-built FlexScan™ solution to support vuln scanning for all types of workloads across multi-cloud environment
- Out-of-box support for agent, agentless, snapshot, network based, and API based scan technologies

Fast MTTR in the Cloud

- Improve MTTR with ITSM integration – SNOW and JIRA
- QFlow based (Drag-and-drop) support for building remediation playbook

Qualys.

Securing Containers

Container Security (CS)

Kubernetes and Container Security (KCS)

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

Modes: Container Sensor

CICD | Registry | General

Network Scanner

Cloud Agent

Support for all cloud service provider Build Tools, Registries, and Kubernetes implementations

Qualys.

Connects with servicenow Jira

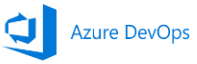
DevOps Pipeline Integrations

Orchestrators

Public Registries

Private Registries

CICD



Remediation

Qualys: Comprehensive Container Security

Container Discovery

- Container images running on hosts and clusters
- Container images in repository (registry)
- Container images built in official builds (CICD)
- Container images built in dev builds

Risk Assessment

- Code – vulnerable first party and third-party code in images; malware in images
- Config - CIS for docker, secrets in images
- TruRisk for K8s clusters
- TruRisk Insights for the Riskiest Containers

Threat Management

- Detect zero-day Malware in Kubernetes cluster nodes with Deep-learning
- Detect zero-day Malware in containers
- Respond to Malware detected in containers (eBPF)

Risk Remediation

- Service NOW integration
- Jira integration
- Reports and dashboards

Policy Compliance

- CIS for Docker
- PCI 4.0 (Risk Based Vulnerability Management)
- PCI 4.0 (FIM for containers)

Qualys: Applying Proven VMDR and Policy Compliance Methodology to Containerized Applications

Key Capabilities in Qualys KCS

Effective Management of Risks from Containerized Workloads

Runtime Prioritized

Package and vulnerability drift, in-use images using cluster inventory

Zero-day Malware Capable

Deep learning based zero-day malware detection – shifted left to handle supply chain problems

Performance Optimized

Highly scalable architecture, low overhead and low operational cost

VMDR Powered

Risk based Vulnerability Management – detection accuracy, noise reduction, threat informed, TruRisk based on asset criticality

Compliance Ready

CIS for Docker containers and images, PCI 4.0/ FIM.

Enforce compliance in CICD and Kubernetes runtime (admission controller)

Qualys.

Qualys: Runtime Security Evolution

Agent Based

- ✓ Docker runtime instrumentation
- ✓ Intrusive, RASP like problems
- ✓ Container Runtime Security 1.0

Agentless

- ✓ Snapshot and best effort
- ✓ Shallow context, more suited for inventory
- ✓ API integration with K8s – Cluster sensor, Admission controller

eBPF Based

- ✓ Lightweight, kernel safe, application agnostic
- ✓ Deep application context and behavior monitoring
- ✓ Container Runtime Security 2.0

Expanded coverage with Agentless and **eBPF**-Based Solutions

Container Use Case Processes

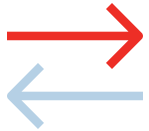
...with Cloud Workflow Protection (CWP)

Run:
Assess Risky Instances

- Assess your production environment for high-risk containers

Release:
Asses Risky Images

- Assess your container registry for high-risk images
- Shift security **left**



Build:
Fail Risky Builds

- Identify and fail risky images at the build stage itself
- Shift security **further left**

Threat:
Detect Zero-day Malware

- Signature free zero-day malware detection with deep learning

Compliance:
Detect Exposed Secrets

- Scan images for exposed secrets.
- The Google Cloud's 2023 Threat Horizons Report found that 86% of breaches involve stolen credentials.

Qualys.

Proactive and Reactive Risk Mitigation

...Shift Left and Right with CS

Risk Reduction from Development to Runtime

- Scan in the CI/CD pipeline, Scan registries, and sca running containers
- Support both on-prem and multi-cloud deployment

Enterprise-grade Vulnerability Scanning

- Industry leading Container Scanning solution powered by Threat research team

Reduce MTTR through integration

- JIRA, SNOW integrations improve remediation workflows

Qualys.

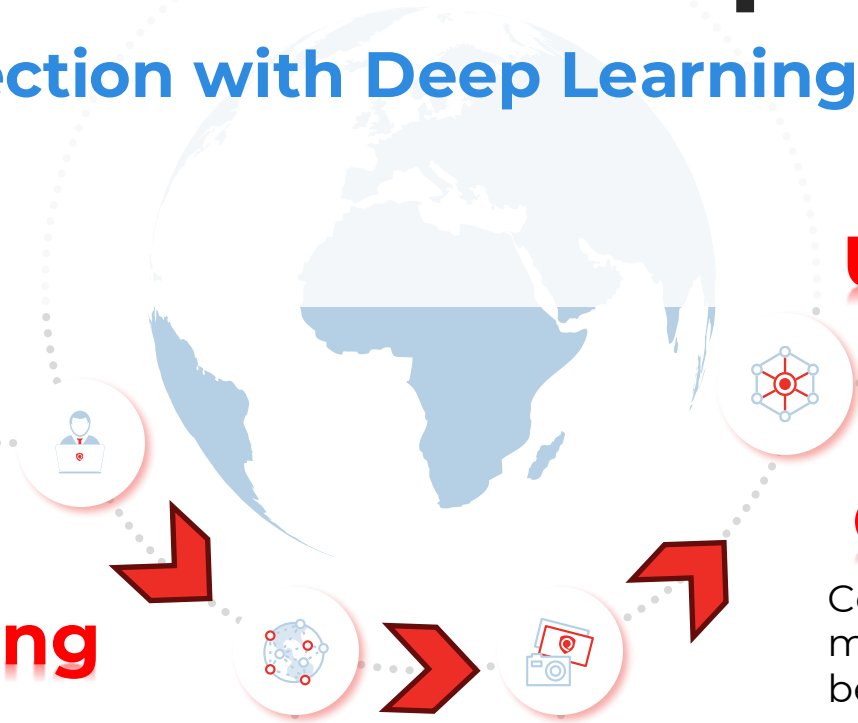
Qualys

Detecting Threats

Cloud Detection and Response (CDR)

Cloud Detection and Response (CDR)

Real Time Threat Detection with Deep Learning AI



Malware

Detect known and unknow malware,.
Classification of malware such as infostealcer, ransomware, trojans, etc ,

Cryptomining

Detection of cytrominers hijacking compute resources

Suspicious Communications

Port Scan, Vertical and Horizontal

Unauthorized Activity

SSH bruteforcing, RDP access..

C2

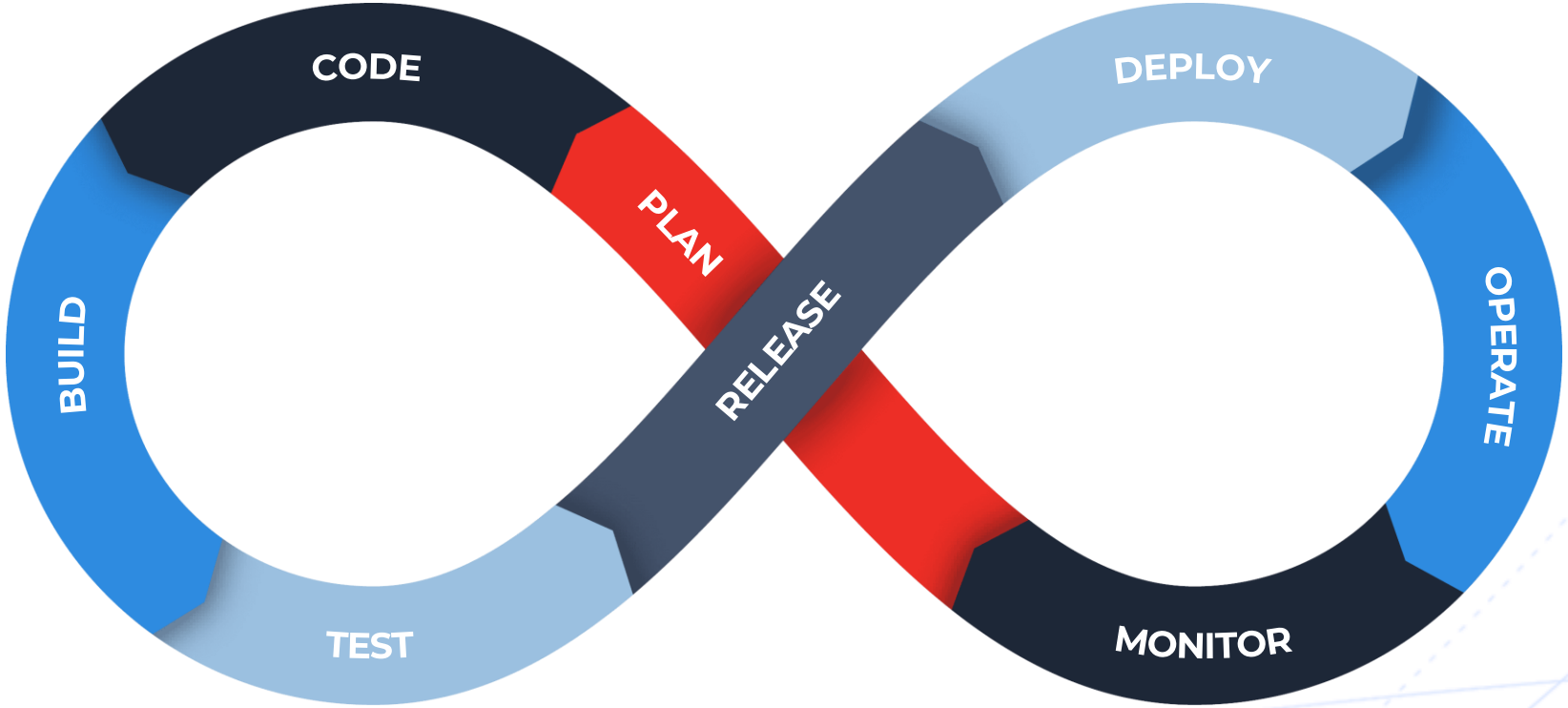
Command and control activity to a malicious server including stealthy beaconing activity.

Deep learning AI for Inspecting Network Traffic and Cloud Activity Logs

Prioritize and Remediate the Threats That Matters Most

Qualys TotalCloud Secures workload from Build to Runtime

End-to-end AI-based Threat Detection : Start Secure and Stay Secure



AI Container Registry Scanning

- Malware

AI Runtime Protection

- Malware
- Unauthorized communications
- Suspicious communications
- Cryptomining
- C2C (Beaconing)

Qualys.

Proactive Threat Detection using Deep Learning AI

Detect new unknown threat

- Monitor network traffic and cloud logs to detect threats at runtime

Instant Signature less detection

- Detect threats in milli seconds and deter a breach

MTTD dramatically reduced due to no manual triage

- AI does the analysis to detect threats so you do not have to

Qualys.

Qualys

SaaS Security Posture Management

SSPM

SaaS Security Posture Management (SSPM)

Secure the SaaS Apps and Data that help drive your business

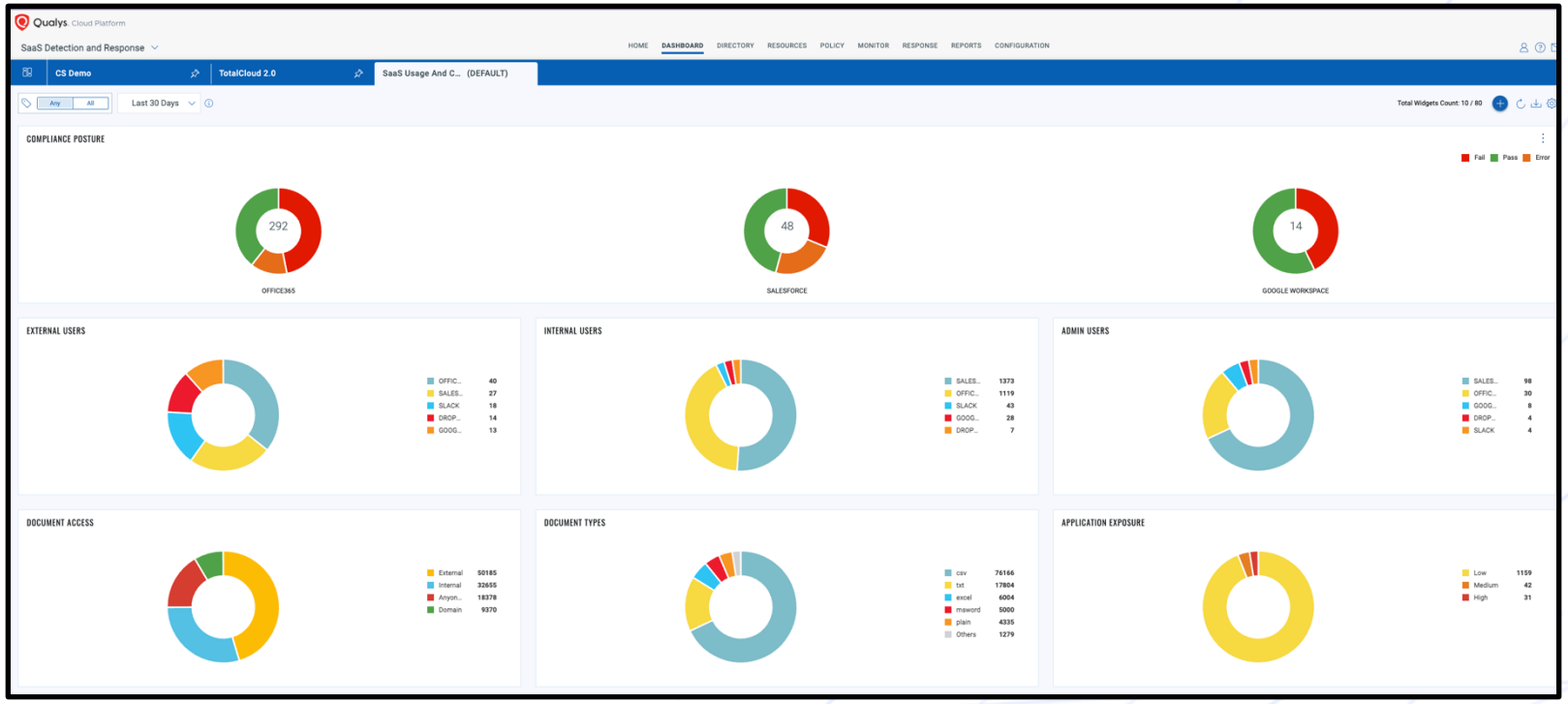
01 **Compliance for Key Apps:** Microsoft 365, Salesforce, Zoom, Google Workspace, Dropbox, Slack

02 **Automated Remediation:** Auto-fix security issues when possible

03 **Comprehensive User and File Directory:** Detailed tracking of users and files

04 **External and Admin Audits:** Regular audits of external users and admin privileges

05 **Third-Party Plugin Security:** Manage and secure third-party plugins



The recent SEC regulation mandates that all public companies are now obligated to disclose cyber incidents and meet cybersecurity readiness requirements for data stored in SaaS systems.

Qualys®

Prioritize Risk Under a Unified View

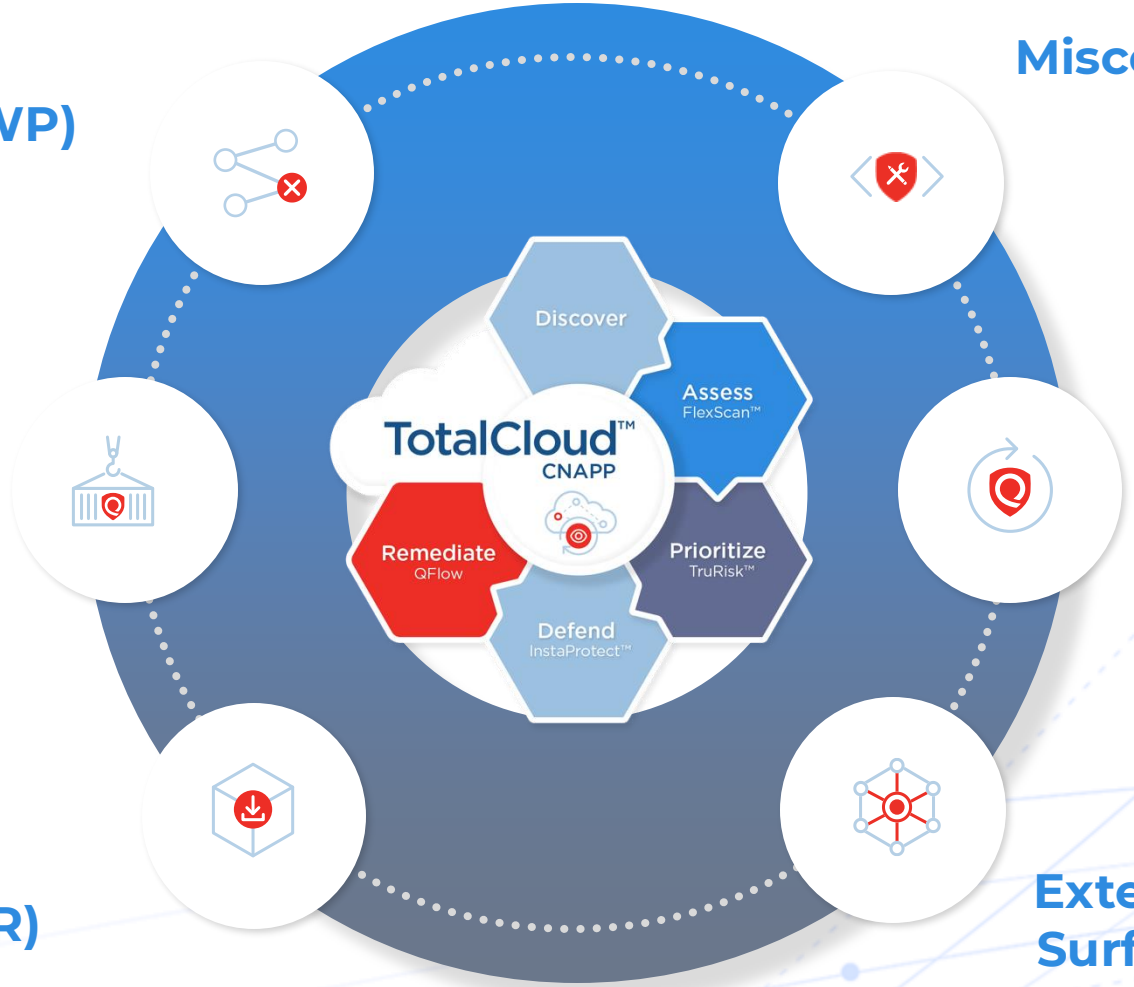
The Benefits of **TruRisk Insights** in the Cloud

Combining Data from Many Sources

Many Cloud Security Functions in One Solution

Vulnerability Assessments (CWP)

Misconfiguration (CSPM)



Container

SSPM + CIEM

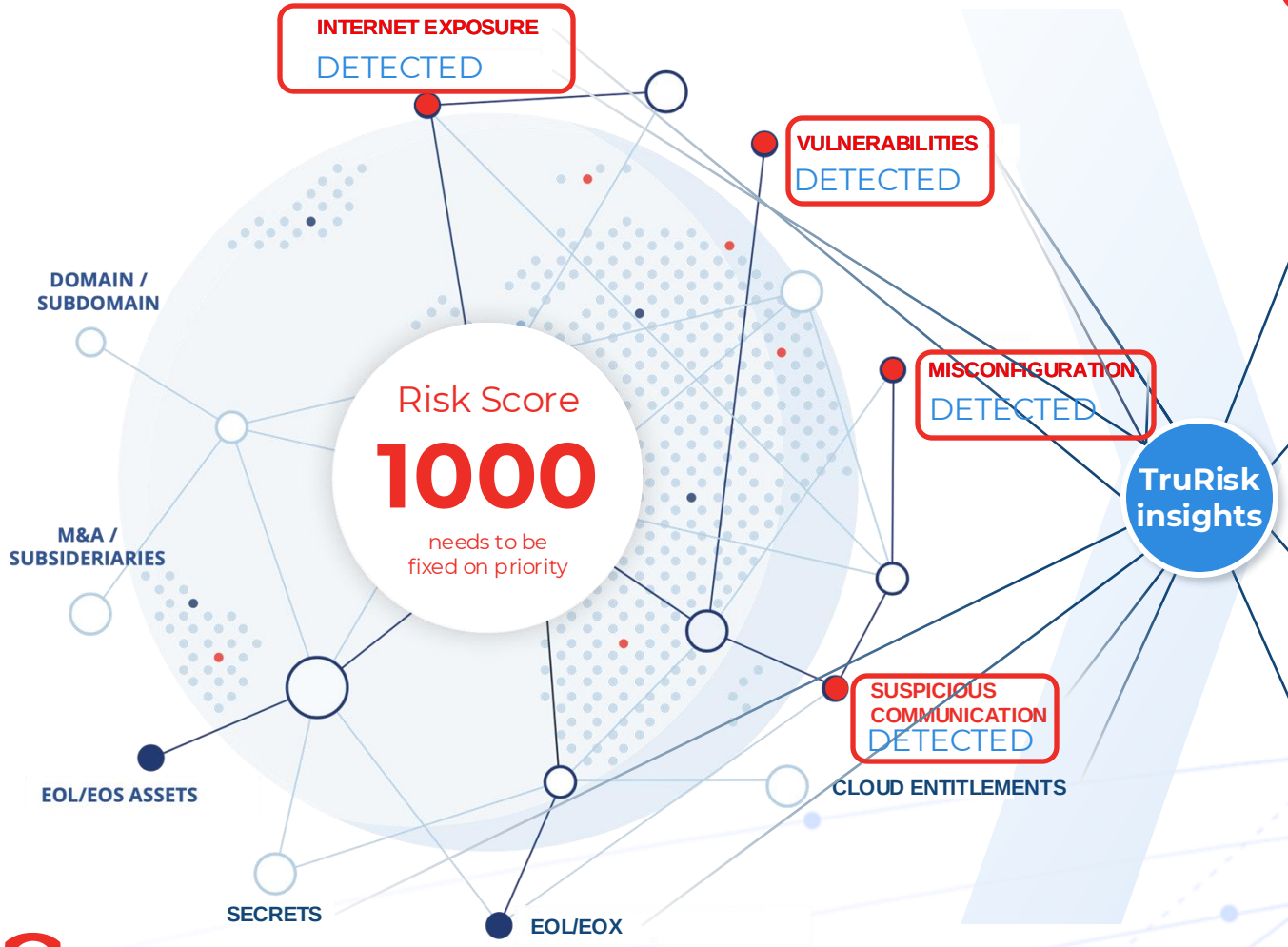
Runtime Threats (CDR)

External Attack Surface (EASM)

Qualys.

Correlating Contributing Factors

....With TruRisk™ Insights to create a single view of risk



Correlating Risk Factors

- Critical vulnerability with a known exploit found on Publicly Exposed VM
- Asset with Vulnerability and C2 beaconing to malicious IP
- High permission publicly exposed critical vulnerabilities
- Endpoints with vulnerabilities, EOL software, and cloud secrets

Qualys.

Prioritize Risk

...with a Single Unified view

Rapid and accurate risk prioritization

- Reduced threat exposure with faster MTTR
- Reduce manual threat analysis of correlating multiple threat vectors into one prioritized TruRisk Insight

Collapse attack paths and identify *true* risk

- Mitigate more threats faster, with precise and concise information on risky assets, rather complex listings of cloud assets (as opposed to attack paths)
- Identify actual risks, rather inferred possible one (as opposed to attack path analysis)

Qualys.

Subscription Model

Select what you want and when you want

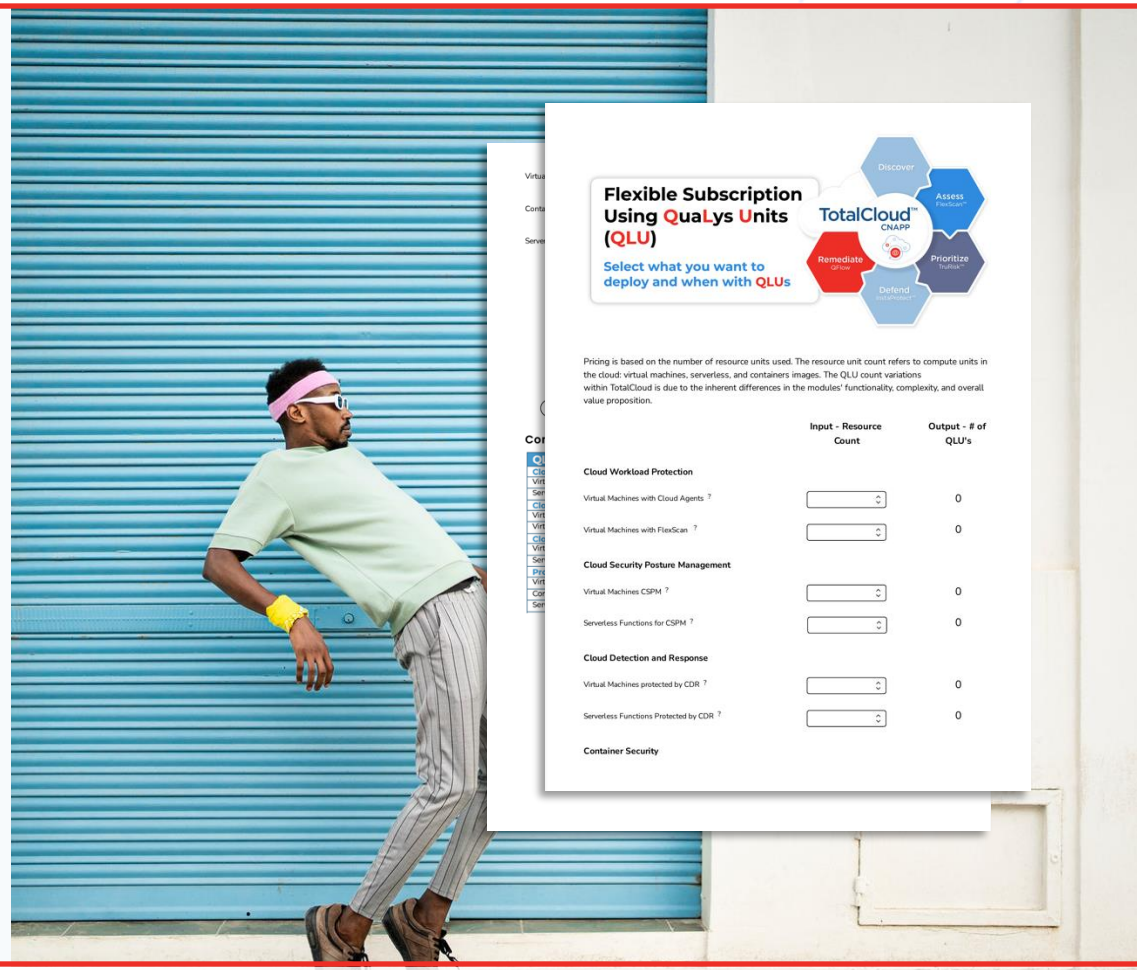
Flexible Subscription Using Qualys Units (QLU)

Ability to select different features (CWPP, CDR, CS, CSPM) as part of the same subscription

No need to re-license to select different features

Qualys Units (QLU) **can be reallocated** to enable preference

One QLU = One VMDR



Qualys.

URL: https://www.qualys.com/qlu-pricing/

A More Complete CNAPP

Meeting Unmet Needs for Cloud and Security Leaders with Qualys

01

Complete Risk Insights in the Cloud

Contextual correlation of cyber risk across all cloud security functions with business implications with **TruRisk™ Insights**

02

No blind spots with continuous scanning

Discover vulnerabilities and compliance controls w/ **API**, **Snapshot**, **Agent-based** and **Network-based scanning** via **FlexScan™**

03

Unified View of Risk Across Entire Infrastructure

One consolidated view of risk across your multi-cloud, hybrid infrastructure, **including external assets**

04

Ability to Action on Findings

Natively-integrated patch management and mitigation actions with **AI-risk-informed workflows with InstaProtect™**

Qualys.

Overview of Different Scanning Methods

Assessment Method	Strengths	Limitations
API-based Use CSP-provided APIs to collect software inventory and perform assessments	• **Fastest setup and assessment** • Ephemeral instances • Quick assessment on startup • Orchestrate as a part of CI/CD pipeline	• **Lack of OSS coverage**
Snapshot-based Take snapshot of the workload and perform vulnerability assessment on it	• **Fast and easy setup without access to the workload** • Quick assessment • Can scan suspended instances • M&A, Cloud migration, large scale deployment	• Less coverage as it looks at snapshots, from CSP's runtime block storage and then scans them • Expensive from resource standpoint • Does not work for hybrid environment, only public cloud • **Periodic scanning, 24 hrs. due to resource limitations**
Agent-based Real-time comprehensive vulnerability, configuration and security assessment	• Long-running workloads • **Detect runtime threats** • Workloads on which high accuracy vulnerability coverage is desired	• **Getting access to all workloads to run agents** • Difficult to deploy agent to ongoing deployments (shutdown workloads to deploy new agent)
Network-based Assess for network-related vulnerability related	• Easy to deploy • **Continuous, no need to stop the workload to inspect it.** • Detect runtime threats	• Getting access to all workloads to run agents • **Being able to access workloads at run time**

Three Ways We're Better Than the Rest

Scalable, Continuous, and Actionable

Features / Capabilities	Conventional Standalone CNAPP	TotalCloud with TruRisk Insights
Single, Prioritized view of Risk	No business context or aggregation of CVEs = more CVEs without context and perhaps without a remediation. Attack paths show possible path of exploitation but no view of risk.	**Reduces CVEs through QID consolidation and TruRisk Insights**, allowing users to address less alerts with aggregated remediation workflows
Flexible, Continuous Scanning	Only conducts agentless periodic scanning, typically every 24 hours.	**FlexScan™, allows users to conduct continuous scanning** via **networking**, **snapshot**, **passive / agentless,** and **agent-based** scanning
AI-enabled Threat Analysis	Signature-based threat detection cannot detect unknown and 0 day threats	**Qualys AI learning model leverages over 13 Trillion Indexed data-points and 30+ Petabytes of storage** to better classify critical assets and preemptively take action to block attacks.

What this Means for You

01 **Less time spent managing and analyzing CVEs** that potentially don't matter, **faster MTTR**, and **more informed remediation actions with TruRisk Insights**

02 **No blind spots. Less risk.**

03 **Reduces risk on custom software and OSS**

Qualys.

Qualys Named a Leader

Gartner

Gartner Market Guide for Cloud-Native Application Protection Platforms, 2023: Representative Vendor

FORRESTER®

Forrester Landscape for Cloud Workload Security, 2023: Representative Vendor

kuppingercole ANALYSTS

KuppingerCole Leadership Compass for Cloud Security Posture Management Solutions, 2023: Leader

GIGAOM

GigaOm Radar for Container Security, 2023: Challenger

Qualys.


Qualys®