Qualys.

TotalCloud™ 2.0 with TruRisk™ Insights

AI-Powered Cloud-Native Application Protection Platform (CNAPP) for Cloud Infrastructure and SaaS Environment

Your Cloud. De-risked.

TotalCloud 2.0 with TruRisk Insights provides a holistic view of risk by correlating unique indicators from diverse Qualys sources such as Six Sigma vulnerability detection, AI-powered threat detection, externally exposed assets, and asset criticality, and combines them with SaaS and cloud infrastructure posture. By bringing these unique indicators together, TruRisk Insights offers a singular, prioritized view of your cloud risk landscape.

Complete posture visibility in under 10 minutes

Rapidly assess all your cloud resources, including transient and ephemeral resources, for vulnerabilities and misconfigurations with a risk-based view in under 10 minutes.

Continuous scanning to reduce exposure to vulnerabilities

Continuous, multi-vector scanning with no-touch, agentless, API- and snapshot-based scanning and agent- and network-based scanning for in-depth assessment.

Manage security posture and risk across your entire SaaS application stack

Provides a protective shield for your favorite enterprise SaaS apps like Microsoft 365, Salesforce, Zoom, Google Workspace, and more, keeping them just as secure as your core cloud environment.

Detect vulnerabilities that other solutions miss

Six Sigma (99.99966%) accuracy with any scanning method avoids alert fatigue to reduce the risk of breaches.

85% time saving with a unified view of risk

One prioritized view of risk to fix what matters most instead of looking at siloed data.

Real-time threat detection with deep learning AI

Continuous detection of known and unknown threats - ransomware, malware, and active exploitation in real-time.

Qualys TotalCloud 2.0 includes:

SSPM

SaaS Security Posture Management (SSPM)

Helps you protect your SaaS applications from cyberattacks and ensure compliance with industry regulations. It manages users and data access rights effectively, identifies misconfigurations in your SaaS applications (Microsoft 365, Salesforce, Zoom, Google Workspace, and more), monitors user activity and data access to detect suspicious behavior, and provides one-click remediation.

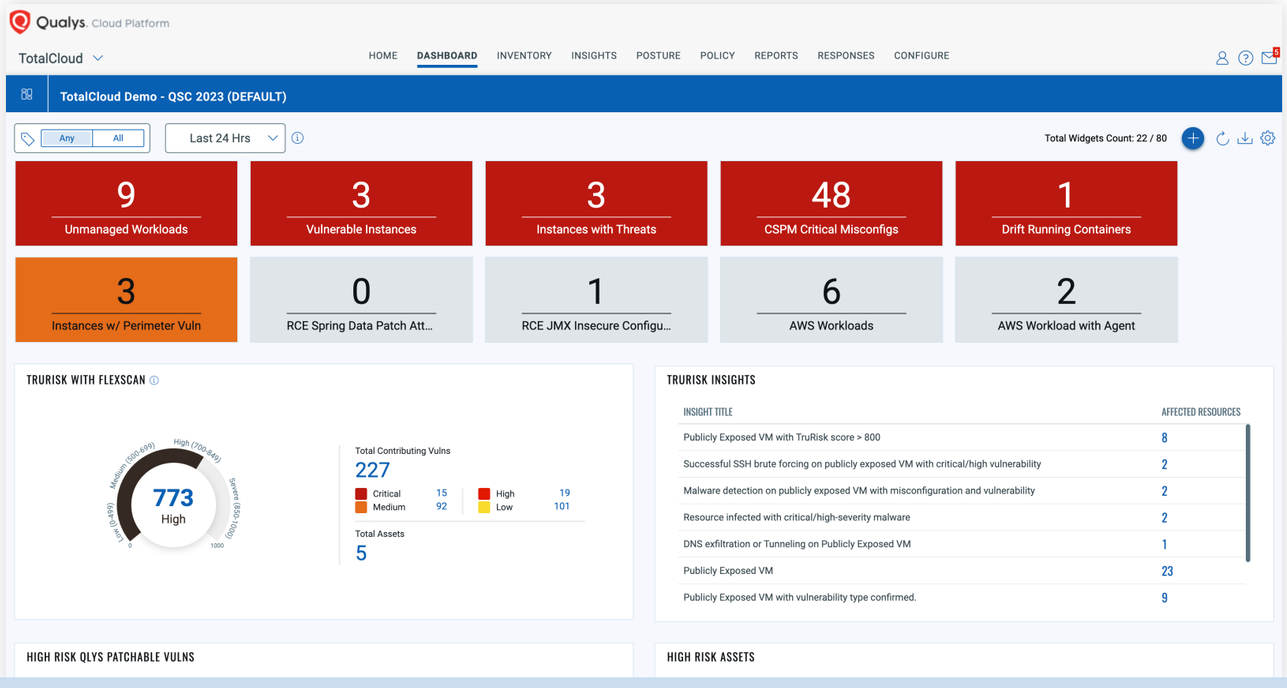
- Complete visibility by automatically inventorying all your SaaS application users and user groups.
- Powerful access controls to manage users and data access rights effectively.
- Data exposure insights by identifying security weaknesses.
- Continuous and automated security posture and configuration assessments of your SaaS applications.
- Unified, real-time, context-based alerts that help determine the actual risk.

CWP

Cloud Workload Protection (CWP)

CWP with FlexScan offers agent-based and agentless scan techniques to continuously discover and monitor all your workloads, detect software vulnerabilities, and scan container images across a multi-cloud environment.

- Zero-touch, agentless, cloud service provider API-based scanning for fast analysis.
- Snapshot assessment that mounts a workload's Snapshot for periodic offline scanning, including vulnerability and open-source scanning (OSS).
- Virtual appliance-based scanning to assess unknown workloads over the network for open ports and remotely- exploitable vulnerability detection.
- Comprehensive vulnerability configuration, assessment with Qualys cloud agents
- Six Sigma-level accuracy.
- Insights from over 180k vulnerabilities sourced from over 25+ threat sources.



CSPM

Cloud Security Posture Management (CSPM)

Monitor, analyze, and assess the status of your multi-cloud assets and resources to identify misconfigurations and non-standard deployments to remediate issues and proactively enforce best practices automatically.

- Continuous discovery and inventory of multi-cloud resources.
- Identify threats caused by misconfigurations and non-standard deployments.
- Continuous compliance monitoring of 35+ global compliance mandates.
- No code automation for custom controls and remediation.
- 1000+ out-of-the-box security controls.
- Coverage of CIS foundation benchmarks, cloud service provider benchmarks, and Qualys best practices, including Kubernetes.

IaC

Infrastructure as Code (IaC) Security

Integrate existing CI/CD tools to assess Infrastructure as Code (IaC) artifacts continuously. Prevent misconfiguration in your cloud accounts by scanning your deployment IaC templates – CloudFormation and Terraform – before deploying.

- Support popular IaC formats like Terraform, CloudFormation, Azure ARM, etc.
- Integration with popular git repositories to Identify issues during the development cycle.
- Integration with CI/CD pipelines to catch issues before deployment.
- Bring your cloud developers and DevOps in security by integrating IaC scan in their tool sets at Git and CI/CD.
- Detailed reporting of misconfigurations detected in IaC templates.
- A centralized dashboard to manage and view all results.

CDR

Cloud Detection and Response (CDR)

IInspect multi-cloud network traffic for suspicious communications, unauthorized activity, crypto mining, malware, zero-day threats, and more. Identify assets that are being actively exploited in real-time using deep learning AI.

- Support cloud-native traffic mirroring deployments and cloud flow log analysis.
- Support traffic mirroring from all supported workload types in the cloud service provider.
- Detects both known and unknown malware in exe, elf, pdf, and docx file types.
- Detect Command and control communication from cloud workload to malicious domains.
- Detection of unauthorized access to workloads using IAM user/Role credentials.

KCS

Kubernetes & Container Security (KCS)

Discover, track, and continuously secure containers – from build to runtime. Discover vulnerabilities across the entire lifecycle of your container images and running containers with out-of-the-box integrations.

- Vulnerability detection for images and running containers.
- Drift detection of the running containers from the corresponding images.
- Comprehensive metadata for every image, including labels, tags, installed software, and layers.
- Integration into popular CI/CD and registry tools.
- Support for self-managed Kubernetes, including EKS, AKS, and GKE.
- Software Composition Analysis support to detect vulnerabilities in application language packages.

KEY BENEFITS

A unified solution for managing the security posture and risk across your entire SaaS application stack and cloud infrastructure:

Qualys TotalCloud 2.0 offers a unified solution for managing security posture and risk, seamlessly integrating cloud infrastructure and SaaS applications into one comprehensive platform. It simplifies the complex landscape of cloud security by providing a singular, holistic view of risks across the entire digital ecosystem, from cloud infrastructure to popular SaaS platforms like Microsoft 365, Zoom, and Slack.

Flexible, continuous, and quick scanning capabilities to detect vulnerabilities in minutes:

TotalCloud 2.0 FlexScan provides continuous scanning for vulnerabilities using agentless techniques and agents. It supports multiple scanning methods, including API-, Snapshot-, Agent-, and Network-based scanning to provide continuous, quick, and comprehensive visibility into vulnerabilities across a multi-cloud environment. This flexible approach allows security teams to identify potential vulnerabilities within minutes in a continuous manner.

Highest level of vulnerability detection accuracy:

TotalCloud 2.0 provides Six Sigma (99.99966%) accuracy with any scanning method, avoids alert fatigue, and reduces the risk of breaches.

- Low false positive rates avoid alert fatigue, wasting time and resources chasing after vulnerabilities that do not exist.
- Low false negative rates prevent exposing the organization to potential attacks and data breaches.

For more information, please visit:
qualys.com/apps/totalcloud/

One prioritized view of risk with TruRisk Insights:

TruRisk Insights consolidates critical indicators from diverse Qualys sources, such as Cloud Workload Protection (CWP), Cloud Security Posture Management (CSPM), and Cloud Detection and Response, into a cohesive, actionable dashboard. TruRisk Insights offers a singular, prioritized view of your cloud risk landscape by correlating these unique factors.

Deep learning AI to detect known and unknown threats in real-time:

Qualys' AI-based approach can detect both known and unknown malware in real-time across the entire cloud kill chain, including reconnaissance, exploitation, installation, command and control, actions on objectives, and lateral movement. Its ability to continuously self-learn from new data makes it more efficient at identifying false positives over time, reducing the burden on security teams and allowing them to focus on genuine threats.

Automated, one-click, and custom remediations and ITSM tool integration:

Qualys offers a variety of remediation options, including automated, one-click, and custom remediation. Qualys offers integrations with ITSM tools to automatically assign tickets and enable orchestration of remediation to reduce MTTR. Qualys also provides complete evidence and clear steps to drive remediation.

Flexible licensing provides lowe r total cost of ownership (TCO) and higher return on investment (ROI):

Qualys delivers a modular and flexible licensing model that gives customers the flexibility to deploy what they want and when they want and the ability to move licenses when they want and how they want. This results in lower TCO and higher ROI because customers start with what they need without unused licenses going to waste. It also allows moving licenses without opening new POs or getting finance approval.

About Qualys

Qualys, Inc. (NASDAQ: QLYS) is a pioneer and leading provider of disruptive cloud-based Security, Compliance and IT solutions with more than 10,000 subscription customers worldwide, including a majority of the Forbes Global 100 and Fortune 100. Qualys helps organizations streamline and automate their security and compliance solutions onto a single platform for greater agility, better business outcomes, and substantial cost savings. Qualys, Qualys VMDR® and the Qualys logo are proprietary trademarks of Qualys, Inc. All other products or names may be trademarks of their respective companies.

For more information, please visit **qualys.com**