

TotalCloud™ for Government

Accelerating Secure Cloud Adoption: Eliminating Critical Attack Paths across Hybrid-Cloud and Container Architectures.

GovCloud. De-risked.

TotalCloud enables agencies, defense contractors, and public-sector suppliers to continuously assess, monitor, and secure their cloud workloads, containers, and applications in Government Community Cloud (GCC), AWS GovCloud, Azure Government, and Google Cloud Platform (GCP) environments. Built on the FedRAMP High (FedRAMP Certified Class D) authorized platform aligned with NIST SP 800-53 Rev. 5 controls, TotalCloud provides risk-based visibility, automated remediation, and continuous compliance to support FISMA, OMB A-130, EO 14028, and the CISA Zero Trust Maturity Model.





Prioritize Real Risk With FlexScanCoverage

Continuously discover and assess authorized cloud and hybrid resources using FlexScan™, supporting agent, API, and snapshot methods. Findings are scored with TruRisk™, helping prioritize vulnerabilities that pose the highest mission impact and satisfy NIST 800-53 RA-5 and SI-2 requirements.



Contextualize The Impact With Attack Path Analysis

Visualize how vulnerabilities and misconfigurations can propagate through critical systems. Attack Path Analysis maps potential lateral movement and privilege escalation to identify assets and mission-essential functions affected. Supports NIST 800-53 CA-7 and PM-9.



Secure Kubernetes and Containers From Build To Runtime

Detect and remediate container and Kubernetes risks. Integrate security into CI/CD pipelines to meet NIST SP 800-218 (SSDF).



Stay Resilient Against Malicious Threats

Identify and correlate anomalous cloud activity using advanced behavioral analytics and threat intelligence. Continuous monitoring supports requirements in NIST 800-53 IR-4 and SI-4, enabling zero-day containment.



Achieve Audit-Readiness With Continuous Compliance

Maintain real-time visibility into compliance status with automated mapping to NIST 800-53, CIS Benchmarks, and agency-specific security plans.



Remediate With No-Code Automation Playbooks

QFlow™ low-code automation orchestrates patching, isolation, and ticketing to satisfy CA-7 and IR-5.

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

SaaS Security Posture Management (SSPM)

Manage the Compliance and Posture of Your SaaS Apps



Cloud Security Posture Management

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.

Cloud Detection and Response

Inspect 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.

Kubernetes and Container Security

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.

Cloud Workflow Automation

Build and play automated remediation workflows with a no-code orchestration platform (Qualys Flow) with enterprise-grade precision. Achieve use case-based requirements and build automation and response playbooks through a drag-and-drop interface of nodes within minutes.

Cloud Workload Protection

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.

SaaS Security Posture Management

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.

Infrastructure as Code 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, Terraform, and ARM) before deploying.

Cloud Identity and Entitlement Management

Continuous visibility, control, and automated least-privilege access for every identity across your cloud environments. Detect risky identities and access privileges across multi-cloud environments, providing visibility, control, and enforcement of least-privilege access.





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. Focuses remediation on exploitable risks that affects mission operations.



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. Supports Continuous ATO (cATO), enables automated evidence collection and control monitoring.



Continuous Scanning to Reduce Exposure to Vulnerabilities

Flexible, multi-vector scanning with no-touch, agent, agentless snapshot, API- and network-based scanning for in-depth assessment. Meets NIST 800-53 Rev. 5 controls protecting CUI and agency data.



Real-Time Threat Detection With Deep Learning AI

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



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.



Achieve Audit-Readiness With Continuous Compliance

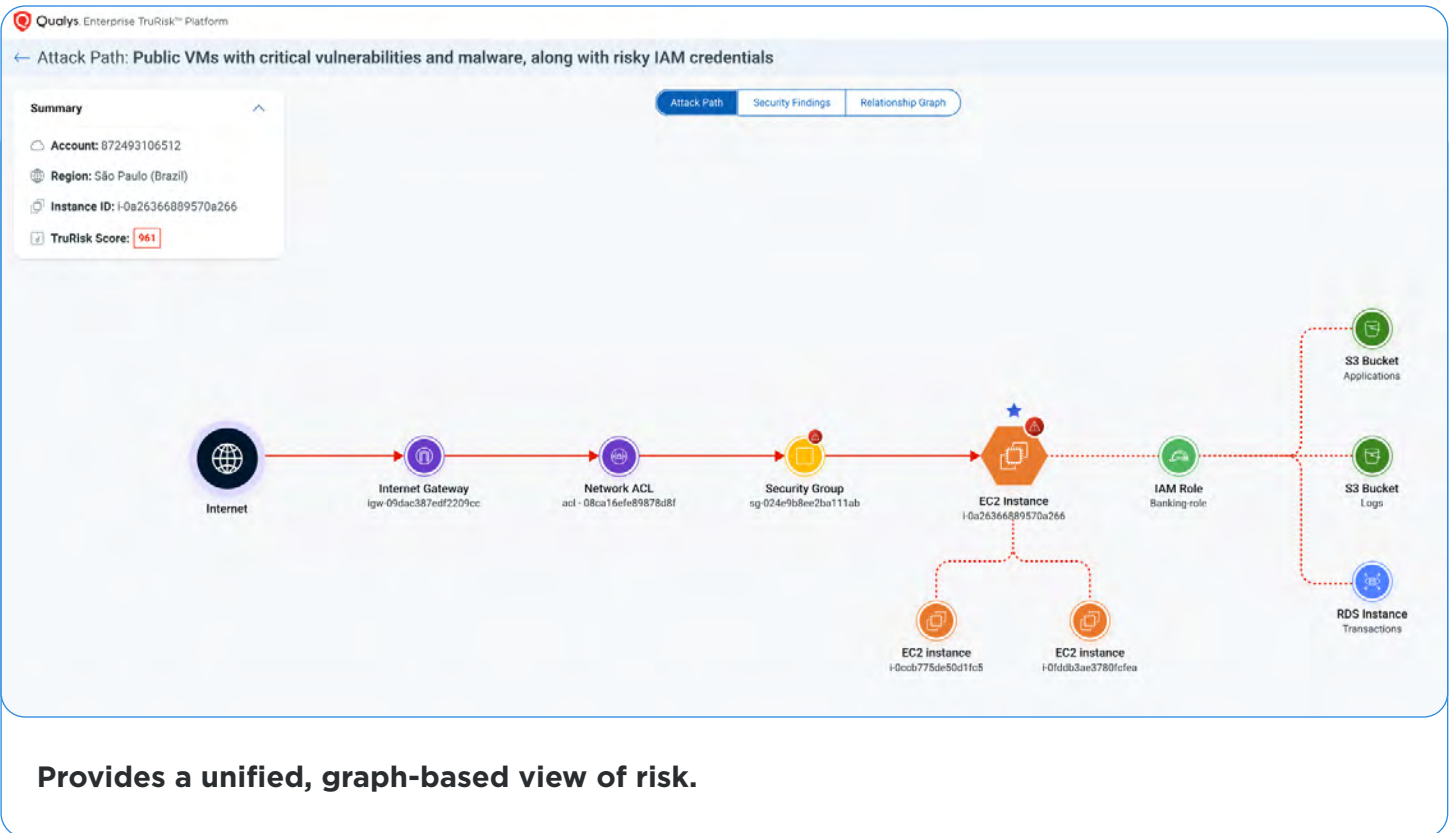
Support for over 40+ mandates including FISMA, OMB A-130, and Zero Trust Maturity Model goals, as well as IaC to ensure you deploy safely and securely.



Detect Vulnerabilities That Other Solutions Miss

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

Understand Potential Impact with Attack Path Analysis



Ready to take the next step
to de-risk your cloud?



Visit Now

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