Qualys

Cloud & Container Security Buyer's Guide

The capabilities and tools you need for comprehensive cloud security

Table of Contents

Introduction

Organizations are increasingly moving to the cloud to win in the digital sphere by harnessing its power to innovate and grow faster than the competition. The most successful companies also understand that moving to the cloud is not without risk and have put the right tools and technologies in place to help properly allocate this risk. This guide will give you the guidance you need to choose the proper technologies that can mitigate these risks, empowering your organization to fully capture the value of the cloud.

The State of the Cloud

As your business connects to more exciting services and applications in the cloud, you're unlocking new, powerful capabilities that could drive levels of productivity like never before. Unfortunately, the benefits aren't always without cost. With every connection, your attack surface expands and risks multiply.

Many organizations are realizing their security doesn't line up with the risks they're facing in the cloud. Resource-strapped security teams are left grappling with blind spots, fragmented tools, and an expanding attack surface they can't fully monitor. While teams may not be fully aware of the extent of these gaps, cybercriminals certainly are. That means businesses need solutions that safeguard their operations and assets, without hindering productivity or leaving gaps exposed.

More than 1 in 4 (28%) admitted their organizations had been the victim of a cloud- or SaaS-related data breach in the past year.

— QUALYS | THE STATE OF CLOUD AND SAAS SECURITY REPORT

Many challenges with multi-cloud and hybrid environments can be boiled down to three key obstacles

1. An expanding attack surface in the cloud

Now that the cloud includes a complex mix of multi-cloud and hybrid environments with an array of workloads across containers, serverless, VMs, databases, and more external-facing assets; as well as a plethora of services spanning multiple cloud service providers—many of which are inadequately monitored—it's easy to lose track of what's really at risk. Only 9% of organizations believe they have complete visibility into their attack surface.

2. A visibility crisis

Nearly 80% of security incidents stem from unknown or unmanaged assets. Without a unified view of risk, security teams struggle to connect the dots, which leaves them reactive instead of strategic and allows low-priority noise to mask real threats and vulnerabilities.

3. Rising costs and fragmented compliance

Cloud complexity is driving up both security risk and operational cost. With compliance frameworks like PCI DSS 4.0, HIPAA, and ISO evolving rapidly, maintaining continuous adherence across multi-cloud and container environments is resource-intensive—especially when using disconnected point tools. Many organizations are forced to stitch together vulnerability scanners, CSPM tools, identity governance platforms, and third-party automation—creating gaps, inefficiencies, and skyrocketing TCO. The result: more spend, more risk, and less control.

Teams' pain points with the cloud

- Limited visibility into cloud and hosting environments
- Growing attack surface
- Relentless advanced threats
- Lack of optimal resources and automated workflows
- Too many alerts
- Misconfigurations of cloud controls
- Unpatched vulnerabilities
- Cloud complexity
- Ephemeral nature of the cloud
- Shared responsibility model
- Maintaining compliance
- Shortage of skilled security workers
- Cloud and SaaS cost inefficiency
- System reliability

What you need to solve those pain points

- A single platform for unified visibility across all workloads, services, and environments
- Risk-based vulnerability management that prioritizes what matters most
- Built-in container and Kubernetes security aligned with zero trust principles
- Automated workflows and playbooks for remediation
- Layered threat protection with behavioral analytics and attack path tracing
- Developer-ready security with visibility from build to runtime
- Continuous compliance enforcement with real-time audit readiness
- Identity-aware controls that go beyond traditional IAM boundaries
- Code-to-cloud traceability to correlate risk across the entire DevOps lifecycle
- Integrated protection for APIs and AI/LLM workloads with unified risk scoring

10 Must-Have Capabilities of Cloud and Container Security

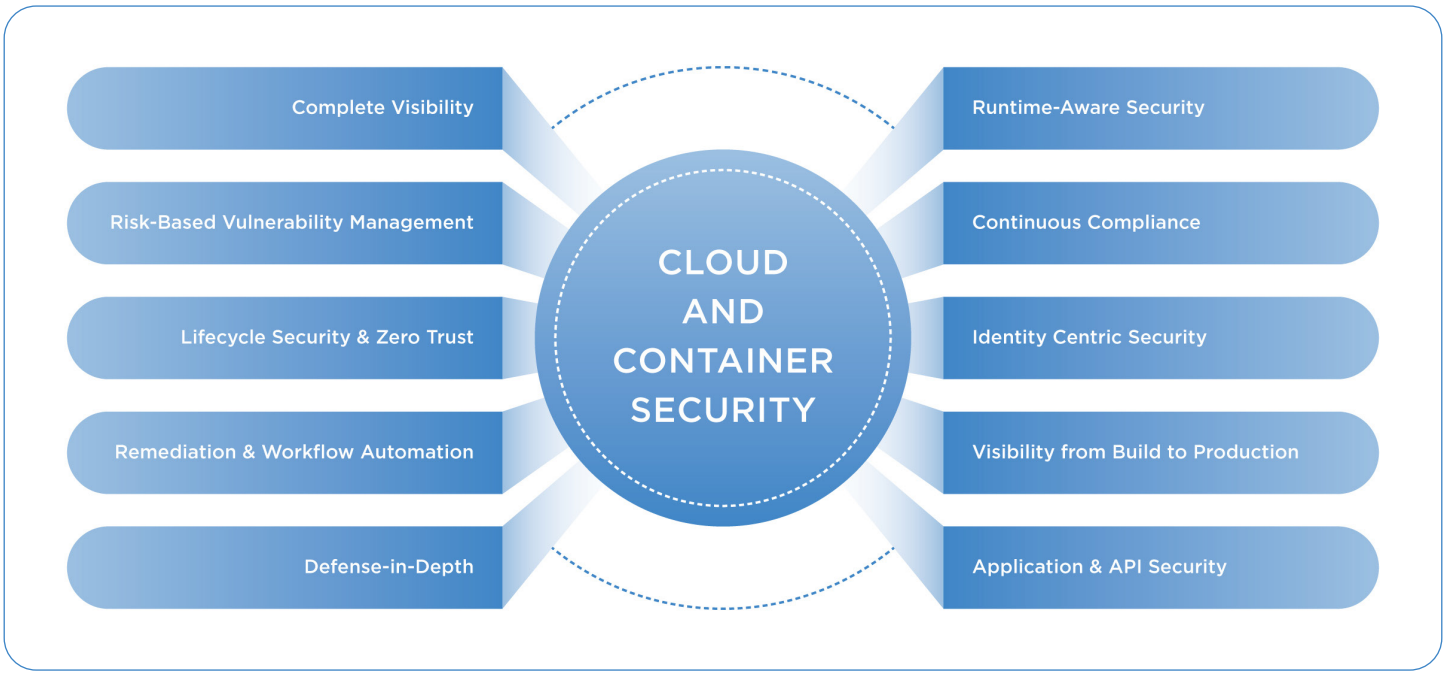
Siloed, legacy tools just can't keep up with the demands of today's cloud-native and hybrid environments. The complexity of interconnected workloads, APIs, applications, and identities requires a more integrated approach, one that moves beyond mere visibility to correlate misconfigurations, vulnerabilities, permissions, connected endpoints, and runtime behavior. Fragmented signals often obscure true risk, while the inability to respond swiftly—particularly to threats emerging in production—can leave critical assets exposed.

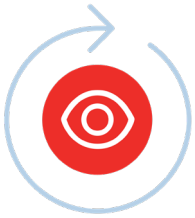
The evolution toward unified, context-aware security platforms capable of seamless remediation reflects a necessary shift in safeguarding modern environments.

As organizations consider their options, an effective cloud and container security solution must combine these nine fundamental capabilities in one comprehensive architecture, empowering security teams to stay ahead of evolving cloud threats.

28% of orgs suffered a cloud or SaaS data breach last year. Of those, over a third were hit more than once.

— DARK READING STATE OF CLOUD & SAAS SECURITY REPORT





Complete Visibility into Cloud Workloads and Services

A comprehensive CNAPP solution delivers unified visibility across all your cloud environments, whether AWS, Azure, GCP, OCI, Red Hat OpenShift, and beyond. It covers every resource type—VMs, containers, serverless functions, databases, managed services—and normalizes them for consistent insight across providers. To eliminate blind spots, it offers agentless discovery via CSP APIs while enriching visibility with real-time data on vulnerabilities, network exposure, identities, malware, secrets, and sensitive data. The result? Security teams get a complete, actionable view of risk.

Risk-Based Vulnerability Management With Multi-Dimensional Prioritization

Not all risks are created equal, and treating them as such results in wasting valuable time and resources. Multi-dimensional risk prioritization combines vulnerability severity with real-world exploitability, asset importance, runtime context, and threat intelligence to surface the issues that truly matter.
By aligning these signals into a unified risk score or attack path, security teams can stop chasing noise and instead focus on the small subset of vulnerabilities that represent actual risk to the business. This approach reduces mean time to remediation (MTTR) and ensures effort is spent where it drives the most impact.

Full-Lifecycle Security and Zero Trust for Containers and Kubernetes

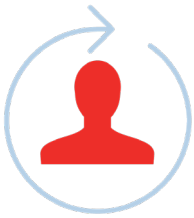
Containers and Kubernetes introduce powerful agility, but also a rapidly shifting attack surface. Enforcing Zero Trust in these environments requires visibility and control across the entire lifecycle: from scanning images in CI/CD, to validating configurations and dependencies pre-deploy, to enforcing runtime policies with admission controllers and drift detection. A mature CNAPP should not only surface vulnerabilities and misconfigurations early but also ensure that only trusted workloads run in production, detect unexpected behavior post-deploy, and block malicious actions in real time. Whether securing EKS, AKS, GKE, or OpenShift, organizations need consistent container security that aligns with workload identity, RBAC policies, and cluster-level posture. This provides the guardrails and visibility required to prevent lateral movement, privilege abuse, and supply chain risk in modern Kubernetes environments.

Contextual Remediation and Workflow Automation

Identifying risk is only the starting point. True value comes from fast, precise, and scalable remediation. A comprehensive CNAPP should bridge the last-mile gap with automated workflows that reduce manual effort and ensure consistent action. This includes integrating with cloud-native APIs to remediate misconfigurations and vulnerabilities, aligning with frameworks like CISA KEVs for patch prioritization, and pushing contextual guidance—complete with runtime insights—into developer tools and ticketing systems.
To fit seamlessly within any organization, the platform must offer flexible, customizable automation that works across third-party systems, enabling security teams to tailor response actions that match their operational tempo and compliance needs.

Defense-in-depth and Protection Against the Unknown

Cloud-native threats like cryptominers hidden in packages, ransomware targeting storage, and data exfiltration via exposed containers or IAM roles demand a defense-in-depth strategy. A robust CNAPP must correlate signals across the stack, linking cloud activity (CloudTrail, VPC flow logs) with deep runtime visibility via eBPF or agents to detect threats as they move from cloud to cluster to container. Deep learning and behavioral analytics are key to uncovering zero-days, long dwell times, and supply chain anomalies that evade traditional tools. Crucially, the platform must go beyond detection, enabling automated response actions like killing malicious processes, quarantining hosts, restricting file access, or closing exposed security groups —so teams can act fast and contain threats before they escalate.



Building Developer Harmony Through Runtime-Aware Security

To truly accelerate remediation, security needs to work with developers, not against them. That means shifting left in a way that learns from runtime—surfacing only what matters, not flooding the developers with hundreds of CVEs. A strong CNAPP integrates directly into developer workflows with shift-left tools across CSPs (such as AWS CodeBuild, Azure DevOps, Google Artifact Registry, and more) as well as 3rd party integrations such as GitHub, GitLab, Jenkins, JFrog Artifactory, etc., providing clear, actionable guidance tied to actual runtime risk: what to fix, why it matters, and which patches to apply. Guardrails must be flexible, enforcing policy without blocking innovation. That includes runtime-informed exceptions for newly disclosed vulnerabilities or unpatchable risks, and the ability to scope enforcement by environment, such as stricter controls in production vs. more lenient rules in development. The result: a developer experience built not on noise but on context and collaboration, one that drives faster, more efficient remediation without creating friction.

Always-On Compliance Monitoring and Audit Readiness

Continuous compliance in the cloud requires more than just point-in-time scans. It demands real-time visibility, policy enforcement, and monitoring across every layer of your environment. Traditional agents often miss blind spots in the cloud control plane or Kubernetes API layer, where misconfigurations and drift can quietly introduce risk. With evolving mandates like PCI DSS 4.0 requiring continuous monitoring of both hosts and containers, capabilities like File Integrity Monitoring (FIM) and Kubernetes Security Posture Management (KSPM) are essential. A comprehensive CNAPP should not only audit configurations across AWS, Azure, and GCP but also enforce custom policies by environment (e.g., dev vs. prod), support exceptions, and ensure consistent governance at scale, helping teams prove compliance while actively reducing risk.

Identity Centric Security That Goes Beyond IAM

In cloud environments, identities—not just infrastructure—are the new perimeter. With thousands of human and machine identities, excessive permissions and lateral movement risks often go undetected. A comprehensive CNAPP must include Cloud Infrastructure Entitlement Management (CIEM) to continuously analyze permissions, detect toxic combinations (e.g., public access + admin rights), and highlight over-privileged identities. CIEM should also help enforce least privilege by integrating with IAM policies across AWS, Azure, and GCP, and provide clear remediation paths—ensuring access is scoped appropriately based on risk, role, and environment.

Code to Cloud Risk Correlation and Traceability

Human error remains the leading cause of cloud breaches—often introduced early in the development lifecycle through insecure configurations or vulnerable code. A CNAPP should connect runtime risk and compliance issues back to their origin in infrastructure as code (IaC), application code, or CI/CD misconfigurations. By combining IaC scanning with SAST/SCA tools and mapping findings to runtime exposure, security teams can pinpoint which code changes introduced real-world risk. This end-to-end visibility from build-time misconfigurations to production impact enables smarter shift-left practices, helping developers fix issues early while maintaining a clear understanding of their potential blast radius.

Unified Security For APIs and AI-Powered Workloads

Securing cloud workloads is more than just about the infrastructure; it is also about the applications and APIs that attackers actually target. A complete CNAPP must extend runtime protection to APIs and web apps, detecting and blocking threats like web malware, API abuse, and logic attacks that traditional WAFs or infrastructure tools miss. This requires connecting signals across the stack, linking infrastructure vulnerabilities and misconfigurations to application-layer exploits and even LLMs running in on prem and cloud workloads in real time. By correlating API behavior, file access patterns, and inbound traffic with known risks and vulnerabilities, security teams gain the context they need to stop attacks before they cause damage. This full-stack approach—from VM to container to API to even LLM—ensures that the services powering your business are protected not just during deployment, but also continuously during runtime, where it matters most.

Why CNAPP Is the Foundation of Modern Cloud Security

To secure today's dynamic cloud environments, organizations need more than siloed tools stitched together with manual effort. They need a **unified platform** that delivers end-to-end security from posture management and compliance to threat detection and fast, automated remediation. At the center of this strategy is the **Cloud Native Application Protection Platform (CNAPP)**—a modern approach that brings all critical cloud security functions into one cohesive solution.

Rather than relying on loosely integrated point products, a CNAPP consolidates capabilities like posture and compliance monitoring, identity protection, container and Kubernetes security, shift-left analysis, API protection, and complete asset visibility—into a **single pane of glass**. This gives teams consistent control and insight across cloud workloads, SaaS applications, and hybrid environments alike.

As Gartner notes, "CNAPP offerings allow an organization to use a single integrated offering to identify risk across the entire life cycle and disparate elements of a cloud-native application"—which streamlines operations, improves accuracy, and reduces complexity.

When teams don't unify around a CNAPP, the consequences are clear:

- **Increased compliance risk** from fragmented visibility and inconsistent controls
- **Higher costs and inefficiencies** due to redundant tools and workflows
- **Security burnout** from contextless alerts and disconnected findings
- **Delayed response times** and missed SLAs due to the last-mile gap in remediation

A modern CNAPP addresses these issues by integrating automated and contextual remediation workflows directly into its risk management process. Whether it's pushing guided fixes into developer pipelines, remediating misconfigurations via cloud APIs, or applying policy-based controls in production, CNAPP helps teams act on what matters—fast.

By unifying capabilities like CSPM, CWPP, KSPM, and CIEM, a CNAPP provides the flexibility to secure diverse workloads across the full application lifecycle—from code to cloud.

Capabilities to look for in a modern CNAPP:

Cloud Security Posture Management (CSPM)
Part of CNAPP

As a major component of CNAAP, CSPM tools continuously discover, monitor, and analyze your cloud assets for misconfigurations and any deviations from best practices. With real-time risk insights, CSPM offers fast, effective remediation capabilities for minimizing misconfigurations and compliance failures in cloud environments and helping your team take quick, informed actions.

Cloud Infrastructure Entitlement Management (CIEM)
Part of CNAPP

CIEM primarily focuses on managing identities and permissions in the cloud. It helps organizations gain visibility into their cloud identities and ensures that they adhere to the principle of least privilege —meaning users are only given the minimum level of access necessary to perform a task.

Cloud Workload Protection (CWP)
Part of CNAPP

Also known as Cloud Workload Protection Platforms (CWPPs), CWPs secure workloads like virtual machines, containers, and serverless applications across cloud environments. Its main purpose is to protect your runtime infrastructure and applications targeting cloud-based assets through vulnerability management, runtime protection, and monitoring.

Kubernetes and Container Security (KCS)
Part of CNAPP

The risk of vulnerabilities in your blind spot is greatly reduced with KCS' enhanced visibility and security controls for Kubernetes clusters and containerized applications. Security teams are better able to detect vulnerabilities and misconfigurations early by identifying and addressing risks well before they escalate. Container Runtime Security leverages the power of eBPF to detect and respond against malicious threats, malware, and anomalies.

Infrastructure as Code (IaC)
Part of CNAPP

IaC security tools help prevent security flaws from being introduced at key developmental stages. IaC tools scan infrastructure code for misconfigurations, assist in remediating security gaps within IaC templates, and detect potential security threats before deployment, ensuring risk operations from code to cloud.

Cloud Detection And Response (CDR)
Part of CNAPP

CDR provides real-time monitoring and threat detection across all cloud environments. Teams can quickly identify and respond to malicious activity—like active exploitation and malware—reducing the impact of potential known and unknown attacks.

Cloud Workflow Automation (CWA)
Part of CNAPP

In order to streamline processes and increase efficiency, CWA allows users to tie together a sequence of tasks or processes across cloud environments, driving automation and removing unnecessary manual tasks.

Application Security (ASPM)

ASPM provides continuous visibility, correlation, and control over application security risks across the entire software development lifecycle—from code to runtime. By integrating and analyzing data from tools like SAST, SCA, DAST, and cloud runtime environments, ASPM helps security teams prioritize vulnerabilities based on exploitability and business impact, enforce security policies, and ensure only secure code reaches production.

Web App Scanning and Malware Detection

Part of ASPM

Web and API-based applications are one of attackers' favorite targets. To help teams rapidly identify and remediate infections, Web Malware Detection leverages deep learning to scan public -facing sites for hidden malware, injected scripts, or malicious content.

API Security

Part of ASPM

Digital transformation has led to the increasing use of both microservices and APIs to power innovation. Organizations with modern application development require solutions like API Security to detect misconfigurations and malicious payloads in real time, thereby protecting sensitive data and application integrity.

AI Security

Part of ASPM and CNAPP

AI security and workload protection focuses on safeguarding AI/LLM models and their supporting infrastructure across cloud and on-prem environments. It includes visibility into deployed models, risk analysis, and policy enforcement to identify vulnerabilities, misconfigurations, and compliance gaps. As organizations adopt platforms like Amazon Bedrock, Azure AI, and Hugging Face, securing these AI workloads becomes critical to managing risk posture, ensuring responsible AI use, and protecting the integrity of the software supply chain.

Attack Surface Management (ASM)

ASM helps organizations identify, analyze, and mitigate potential risks across their entire digital footprint—both known and unknown. It continually monitors and assesses the evolving threat landscape, focusing on inventory and risk assessment of every cyber asset within the organization. True attack surface management includes the risk context that drives stronger vulnerability management and remediation.

Cybersecurity Asset Management

With external attack surface management

CSAM helps security teams quickly identify at-risk assets, assess complex IT environments, and take timely action to mitigate risks across hybrid environments by continuously discovering, monitoring, tracking, and securing an organization's hardware, software, and cloud assets. For robust attack surface management, CSAM should be combined with external attack surface management.

External Attack Surface Management

To complement cybersecurity asset management

External attack surface management helps organizations identify and reduce the risk of internet-facing assets that they potentially did not even know they had, but that are visible and potentially exploitable by external attackers.

Why Qualys: Risk-Minded Cloud Security For Any Attack Surface

Cloud security is a complex landscape requiring complex capabilities—delivered streamlined. Here's how Qualys enables comprehensive, scalable security capabilities purpose-built to handle the complexities of modern cloud environments —efficiently and at scale.

With a single purchase of a Qualys Licensing Unit – you get all of the capabilities out of the box. With everything enabled, you can reallocate units across different use cases and attack surfaces enabling you to accelerate your cloud journey and build resilience.

Find out more about Qualys' solutions

TotalCloud™

Unified Cloud Risk Visibility across code, config, and runtime with TruRisk™ and attack path context.

Built-in Remediation with automated playbooks, controls, and runtime threat mitigation.

TotalAppSec™

8+ Million: Critical issues remediated across APIs, LLMs, and Applications thanks to integrated and automated workflows.

CyberSecurity Asset Management

Unmatched Visibility: Find all internet-facing assets —known and unknown—with built-in EASM.

Smarter Coverage: Expand scan reach with risk-based tagging and prioritization across hybrid environments.

RESOURCES

Case studies and reports

2025 Gartner® Voice of the Customer for Cloud-Native Application Protection Platforms

2023 Qualys TruRisk Threat Research Report

2024 Gartner® Market Guide for CNAPP

The State of Cloud and SaaS Security Report

Securing Dental Patient Data in the Cloud Customer Success Story

Solution briefs

VMDR and CyberSecurity Asset Management with External Attack Surface Management (EASM)

TotalCloud™ - The Risk-Minded CNAPP

The Good, the Bad, and the Ugly of Cloud-Native Application Protection Platforms (CNAPPs)

eBooks

The 6 Essential Must-Haves: Cloud-native Application Protection Platform (CNAPP)

5 Questions To Ask Your Cloud Security Provider Before It's Too Late

Blogs

Our Takeaways From 2024 Gartner Market Guide for Cloud-Native Application Protection Platforms (CNAPP): Insights and Market Evolution

Best Practices for Cloud Compliance

From Vulnerability Scanning to Risk Management: The Complete VMDR Advantage

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

v250721