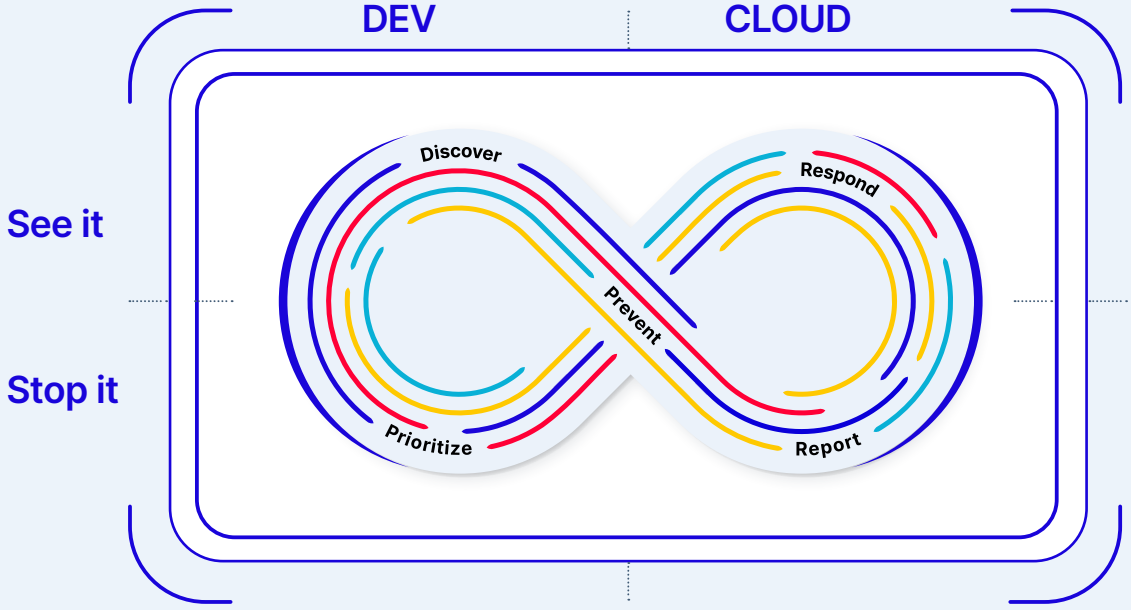
Aqua CNAPP

Secure your cloud native applications across the full life cycle

The Aqua Cloud Native Application Protection Platform (CNAPP) unifies your cloud security so that you can see and stop attacks from code to cloud and back. Its single source of truth enables seamless collaboration across teams, giving everyone the context to prioritize and fix what's most important. The platform's fully integrated set of security and compliance capabilities allow you to prioritize and manage discovered risks in minutes across the full software development lifecycle (SDLC). It also helps you automate the prevention of known risks from making it to production, as well as the detection and response to issues found after deployment.

Aqua Unifies

- **Software Supply Chain Security**
- **Vulnerability and Risk Scanning**
- **Cloud / Kubernetes Security Posture Management (CSPM / KSPM)**
- **Cloud Workload Protection Platform (CWPP)**
- **Cloud Detection and Response (CDR)**



Discover and prioritize risk in minutes

Automatically discover all your assets and artifacts with a searchable inventory. Go one step further to combine issues discovered during scans with runtime alerts to gain context-based insights into the highest risks to your cloud native applications. The Aqua Platform unifies asset and risk visibility from code to cloud, on any cloud, across VMs, containers, serverless functions and the entire software development life cycle (SDLC).

Code security

Write code securely with automated Static Application Security Testing (SAST) that uncovers issues. Safely use open source components with Software Composition Analysis (SCA) that integrates directly into the IDE.

IaC scanning

IaC further blurs the distinction between applications and their underlying infrastructure. Scan IaC files for misconfigurations that could leave your environment vulnerable to attack.

Image scanning

Minimize your attack surface by connecting to your image registries to detect vulnerabilities, embedded secrets, and other security issues in proprietary and third-party container images.

Cloud Security Posture Management (CSPM)

Continuously audit cloud accounts and services for security risks and misconfigurations.

Agentless cloud workload scanning

Scan snapshots of running workloads for a quick view into risk factors that could leave the door open to an attack.

Automate shift-left prevention

Reduce the attack surface with automated pre-production acceptance gates throughout your CI/CD pipelines that prevent malicious source code, non-compliant images, IaC templates and misconfigured Kubernetes workloads from getting into production.

Kubernetes Security Posture Management (KSPM)

Scan for misconfigurations that could lead to attacks on your Kubernetes (K8s) clusters. Use the results and your pre-defined assurance policies to automate the secure deployment of K8s applications at K8s admission controllers.

Dynamic Threat Analysis

Run and test images in a secure, pre-production sandbox environment to identify hidden and sophisticated risks.

Assurance policies

Assurance policies automate security policies for artifacts across the code, build, and deploy phases of development. You can automatically block source code commits, the usage of misconfigured IaC templates, and keep non-compliant images and misconfigured Kubernetes workloads from making their way into production.

Software Supply Chain Security

Identify and remove risks in proprietary and third-party code, generate Software Bills of Materials (SBOMs), ensure integrity of images through build pipelines, and secure the tools and processes used to build your applications.

Protect in real time

Immediately stop attacks in progress that others cannot see using behavioral indicators derived from real-world attacks. Runtime policies provide surgical, real-time protection for containers, VMs and serverless workloads while malicious activity in the build is detected and stopped.

Real-time in-workload visibility

Agentless workload scanning alone leaves gaps in your ability to see and prioritize risks. Real-time in-workload visibility provides in-depth context and risk-based insights for faster and more effective risk-based prioritization.

Cloud Detection & Response (CDR)

Identify unknown attacks that nobody else can see in real time using eBPF and behavioral indicators curated by the Aqua Nautilus threat research team.

Virtual Machine (VM) security

Scan and monitor cloud VMs with a lightweight solution to block known vulnerabilities and malware, check OS configurations against CIS Benchmarks, and ensure that the security posture of your cloud VMs is aligned with compliance policy.

Runtime controls

Enforce immutability, mitigate vulnerabilities that could be exploited but can't be patched, block known threats (e.g. malware, cryptocurrency), and further reduce attackers' ability to operate with runtime policies for containers, VMs and functions.

Serverless security

Scan your serverless functions for cloud provider-specific keys and secrets and prevent their accidental exposure. Ensure least-privilege permissions that, if left unchecked, could allow a potential attacker access to your resources.

The power of the platform

Cloud native application protection requires a holistic end-to-end approach to secure applications across their full lifecycle, from dev to runtime and back. This is possible only with a comprehensive and tightly integrated platform that provides full context across diverse and complex environments, improves operational efficiency, and reduces friction between teams.

AI-guided remediation

Automatically generate prescriptive remediation steps for issues across container images and other artifacts, multiple clouds, and multiple workload types.

Cloud-to-code tracing

With one source of security truth for dev and cloud, quickly trace cloud security issues back to the original code and user to improve efficiency and speed resolution.

Compliance reporting

Out-of-the-box reports make auditing for compliance simple.

Platform integrations

Our full life cycle security approach provides consolidated visibility, insights and protection across clouds, development pipelines, infrastructure and workloads - with broad and deep cloud native ecosystem integrations.

Seamless integration with your cloud tech stack

Registries | CI/CD | DevOps Tools | Container Platforms | Service Mesh
Serverless | Cloud Providers | Vaults | Security & SIEM

The Aqua Platform

The Aqua Cloud Security Platform protects the entire development life cycle from dev to cloud and back and is the industry's most integrated cloud native application protection platform (CNAPP). After expanding its platform with fully integrated Software Supply Chain Security, Aqua is the only solution with the end-to-end context to accurately identify and stop threats in any phase of the application life cycle.

Schedule a demo ›