SOLUTION BRIEF

# Accelerating DevSecOps with the Aqua Platform

## A Unified Approach to Cloud Native Security

### Key Benefits

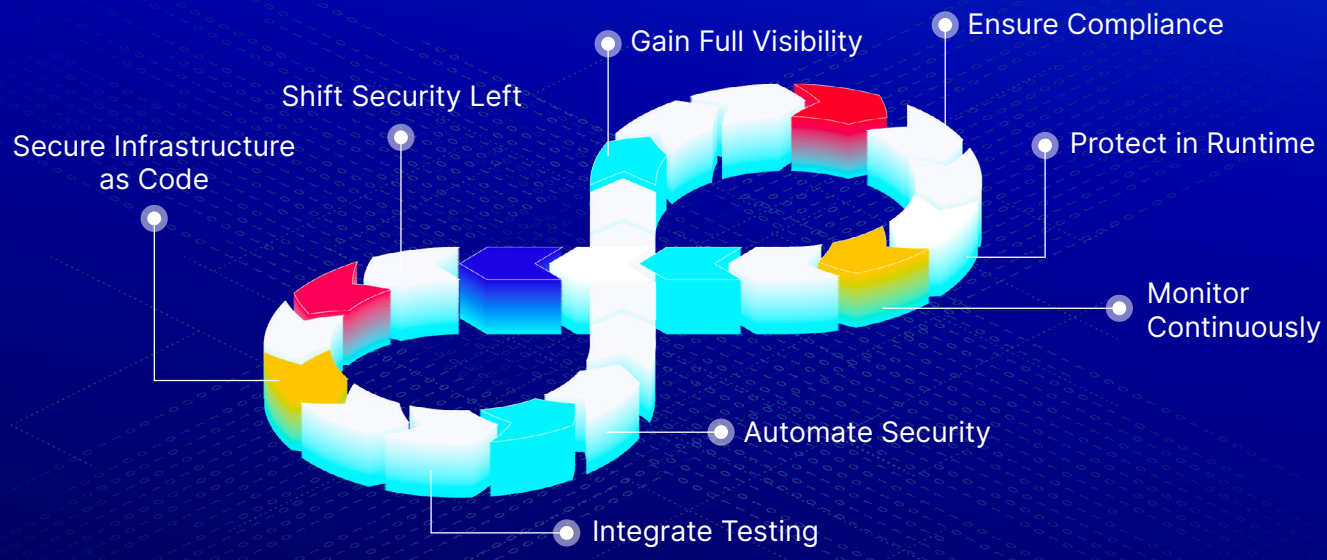
- ✔ Detect and mitigate vulnerabilities across containers, serverless functions, and VMs throughout the entire software development life cycle.
- ✔ Automate security checks at every stage without disrupting existing workflows, integrating with your CI/CD pipeline and tools.
- ✔ Shift left and embed security early in the development process, identifying misconfigurations, exposed secrets, and malware in addition to vulnerabilities, allowing teams to address issues before they reach production, enhancing speed and reducing risks.
- ✔ Secure running workloads with real-time protection and threat detection.
- ✔ Foster close collaboration among Development, Security, and Ops teams to cultivate a security-first mindset.

## Achieve Speed, Security, and Automation with Aqua's Comprehensive Solution

Ensuring security from code to cloud requires embedding security measures, continuous monitoring, and real-time visibility into every stage of the development life cycle. DevSecOps leaders, who aim to deliver applications quickly without compromising on security, continually implement these practices to enhance security posture and maintain compliance. By embedding security early and continuously, they can proactively identify and mitigate security risks, improving both development speed and security.

The Aqua Platform supports DevSecOps by providing a purpose-built solution for cloud native application protection in on-premises, hybrid, and multi-cloud environments. The Aqua Platform safeguards cloud native applications deployed across containers, serverless functions, and VMs.

### A typical DevSecOps workflow



## Embed Security at Every Stage of the SDLC

Automate secure development and deployment of applications in DevOps pipelines by embedding comprehensive security testing and powerful policy-driven controls from the start and across the entire application life cycle.

### Manage open source and third-party risks

Gain visibility into open source and third-party components, surfacing risks and mitigating them. Assess the health of open source libraries with a dedicated score before use and generate SBOMs to identify and update vulnerable packages in your code.

### Protect your CI/CD toolchain

Harden your CI/CD pipeline by quickly identifying and correcting misconfigurations across your various DevOps platforms and tools. Implement a zero-trust DevOps environment to always maintain a robust CI/CD security posture.

### Accurately detect risks

Comprehensively scan container images, VMs, and functions for known vulnerabilities, hidden malware, embedded secrets, open source license issues, configuration issues, and more with the highly accurate and universal Aqua scanner, powered by Aqua Trivy.

### Uncover sophisticated malware

Discover hidden malware and suspicious behavior in your CI/CD pipeline by running a container image in an isolated sandbox to check its runtime behavior before it goes to production with Aqua DTA (Dynamic Threat Analysis).

### Protect in runtime

Detect and prevent active attacks on your running containers, VMs, and serverless workloads in real time with granular controls to instantly identify and stop known and unknown threats, fileless malware, zero-day attacks, cryptocurrency mining, and more.

## Operate at Cloud Native Speed

Accelerate speed to software delivery without sacrificing security by ensuring that security policies are enforced across development, staging, and production. This reduces risks early and enables teams to adopt DevSecOps practices without slowing development.

### Enable developers to fix issues fast

Empower developers to embrace a security-first mindset, automatically tracing issues to the exact line of code, generating a pull request to the responsible owner, and enabling quick resolution — saving developers time and effort.

### Focus on the biggest risks

Use a risk-based approach to automatically filter thousands of vulnerabilities and determine top-priority issues that pose the greatest risk and require action. Analyze the impact of CVEs by a variety of granular factors such as code reachability, EPSS, actively running packages, remote exploitability, available exploits in the wild, and more.

### Control your risk tolerance

Speed up your DevOps processes and manage risk effectively by setting the level of accepted risk and having multiple image-assurance policies as guardrails for varying security and compliance requirements across applications.

### Protect workloads faster

Quickly protect workloads at runtime with zero configuration, out-of-the-box protection against advanced threats based on behavioral detections, eliminating the need for specialized cloud native expertise. Prevent exploitation attempts and mitigate vulnerabilities without a fix by applying compensating controls such as vShield.

### Achieve compliance without compromise

Ensure continuous compliance with automatic monitoring of cloud native environments against industry standards (such as PCI-DSS, HIPAA, and GDPR), access to real-time reports, and enforcement of security policies to maintain compliance throughout the application life cycle.

## Maximize DevSecOps Efficiency

Automate security tasks to free up DevOps and Security teams from manual processes. Combine multiple previously disparate security capabilities into a single, integrated platform to save limited resources and ensure streamlined operations.

### Improve collaboration across teams

Streamline security processes between development and security teams, ensuring alignment on risk thresholds and action plans with Aqua assurance policies, which set clear tolerance levels for your environment's security posture.

### Tailor policies and rules

Set up highly flexible assurance policies as guardrails at multiple stages of the software development life cycle based on the security needs of different applications or pipelines. The rules can apply to various factors, such as risk score, vulnerability severity, root privileges, embedded secrets, malware, and more.

### Optimize application stability and security

Improve application stability and performance with eBPF technology for less intrusive, lightweight runtime security, enhancing user experience and efficiency.

### Define once and run anywhere

Establish a universal set of granular runtime security rules to save time and ensure consistency across hybrid and multi-cloud environments, enhancing your overall security posture and reducing the risk of threats due to inconsistent enforcement.

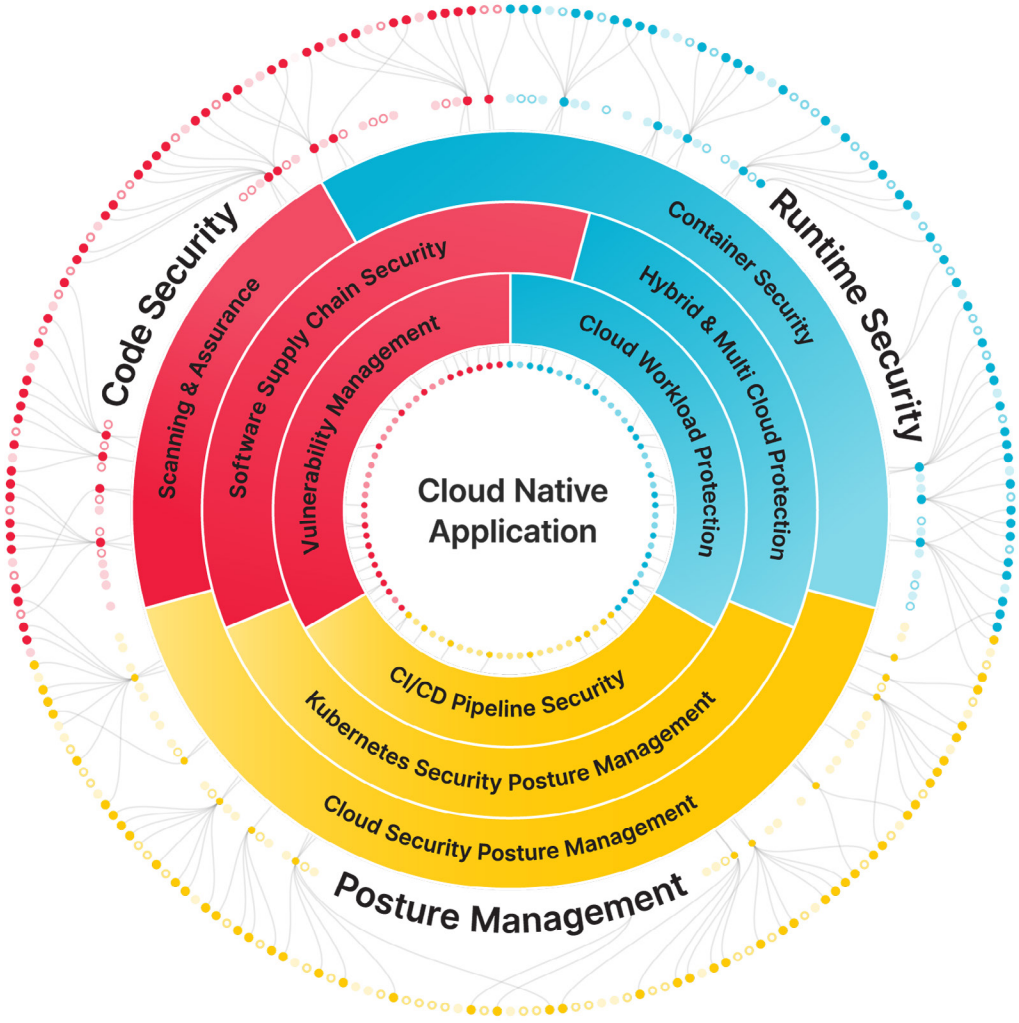
### Consolidate scanning tools

Streamline security and risk management by leveraging a single unified scanner, powered by Aqua Trivy, across all application life-cycle stages. This unified approach boosts scanning accuracy and consistency, replaces multiple tools with one, and facilitates early issue detection and resolution, empowering your organization to scale efficiently in the cloud.

# The Aqua Platform

## Secure Every Cloud Native Application Everywhere

**Aqua Security's Cloud Native Application Protection Platform (CNAPP) enables DevSecOps by integrating security throughout the software development life cycle. It provides automated code to cloud vulnerability management, continuous compliance monitoring, and runtime protection for applications deployed in containers, serverless functions, and VMs. The Aqua Platform ensures that security controls are enforced across development, staging, and production, reducing risks early and enabling teams to adopt DevSecOps practices without slowing development.**




aqua

Aqua Security is the pioneer in securing containerized cloud native applications from development to production. Aqua›s full lifecycle solution prevents attacks by enforcing pre-deployment hygiene and mitigates attacks in real time in production, reducing mean time to repair and overall business risk. The Aqua Platform, a Cloud Native Application Protection Platform (CNAPP), integrates security from Code to Cloud, combining the power of agent and agentless technology into a single solution. With enterprise scale that doesn't slow development pipelines, Aqua secures your future in the cloud. Founded in 2015, Aqua is headquartered in Boston, MA and Ramat Gan, IL protecting over 500 of the world's largest enterprises.
For more information, visit https://www.aquasec.com

**Schedule a demo ›**