Solution Brief

stop cloud native attacks with the aqua platform

Stop cloud native attacks from day one and in real-time with **the Aqua Platform, a Cloud Native Application Protection Platform** (CNAPP). Its fully integrated set of security and compliance capabilities visualize, prioritize, and eliminate risk in minutes across the full software development life cycle. Automated policies for shift-left prevention and runtime detection and response reduce your attack surface and mitigate active attacks—before damaging losses can occur. Aqua empowers you to unleash the full potential of your digital transformation and accelerate innovation with the confidence that your cloud native applications are secured from start to finish, at any scale.

Aqua Unifies

- Software Supply Chain Security
- Vulnerability and Risk Scanning
- Cloud Security Posture Management (CSPM)
- Cloud Workload Protection Platform (CWPP)
- Cloud Native Detection and Response (CNDR)

aqua platform

Secure from Day 1 | **Protect in real-time**

Code > Build > Deploy > Run

Prioritize Risk in Minutes

Automate Prevention

Stop Attacks Immediately

Secure from day one

Effective cloud native security requires a view into the assets and artifacts across the entire application life cycle as well as a way to quickly prioritize risk. You must have a way to automate prevention so protection can quickly scale across your teams and applications.
With Aqua, security can become an integral part of the life cycle itself from the very start.

Prioritize risk in minutes

View the top risks for your cloud native applications in minutes with a searchable asset inventory and context-based insights from across the software development life cycle (SDLC). The Aqua Platform protects your entire stack from code to runtime, on any cloud, across VMs, containers, and serverless functions.

Source code scanning
Connect your Source Code Management (SCM) tools to scan source code repositories for vulnerabilities, embedded secrets, and other security issues.

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

Unified risk visibility
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 insights into the highest risk threats to your cloud native applications.

Cloud workload scanning
Scan snapshots of running workloads for a quick view into risk factors that could leave the door open to an 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, services for security risks and misconfigurations.

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

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.

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.

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.

Dynamic Threat Analysis

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

Cloud Native Detection & Response (CNDR)

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.

Software Supply Chain Security

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

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.

Managing the Aqua Platform

Role-Based Authentication Control (RBAC)

Define access using your enterprise directory to permit or deny users access to the Aqua Platform. Within the platform, you can grant granular access to roles and individuals based on artifacts, workloads, and infrastructure objects. This allows you to prevent threats from insiders or unauthorized access to user accounts.

Secrets Management

Integrate the Aqua Platform with your secrets key store or third-party key vault to securely inject secrets, like passwords, connection strings, and tokens into containers. You can also define granular access to secrets for only authorized users, allowing you to enforce principles of least privilege.

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 stack across the cloud native ecosystem

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

Aqua Security stops cloud native attacks, preventing them before they happen and stopping them when they happen. With Aqua, DevOps and Security teams prioritize risk in minutes across the entire development lifecycle while automating prevention to secure their cloud native applications on day one. Real cloud native attacks are stopped immediately without killing workloads. With a platform built on the most loved open source cloud native community and innovation from dedicated threat research, Aqua is a complete solution to cloud native security for transformational teams. Founded in 2015, Aqua is headquartered in Boston, MA and Ramat Gan, IL with Fortune 1000 customers in over 40 countries.

Aquasec.com