The Complete Cloud Native Security Platform

Unleash the full potential of your cloud native transformation and accelerate innovation with the confidence that your cloud native applications are secured from start to finish, at any scale. Aqua Platform protects your entire stack, on any cloud, across VMs, containers, and serverless.

Secure the **Build**

Accelerate development by detecting security issues in your artifacts early and shortening time to remediate.

"Shift left" security into the CI/CD pipeline, get full visibility into the security posture of your pipeline and reduce the application attack surface before application deployment.

Secure the **Infrastructure**

Enforce compliance across the stack, gain real-time visibility and control over your security posture.

Monitor, detect, and automatically remediate configuration issues across public cloud services and Kubernetes clusters.
Ensure conformity with CIS benchmarks, PCI-DSS, HIPAA, GDPR and other regulations.

Secure the **Workloads**

Protect applications in runtime using a zero trust model, with granular controls that accurately detect and stop attacks.

Unify security across VMs, containers, and serverless on any cloud, orchestrator, and operating system. Leverage micro-services concepts to enforce immutability and micro-segmentation.

Aqua's full lifecycle security approach provides coverage for all clouds and platforms, integrating with your existing infrastructure and the cloud native ecosystem.

Aqua Cloud Native Security Platform Key Features

Cloud Native Posture Management (CSPM)

- Continuously audit cloud accounts and services for security risks and misconfigurations
- Get actionable remediation advice, auto-remediate selected service settings
- Scan infrastructure-as-code templates (Terraform, AWS CloudFormation) for security issues
- Achieve consistent security across AWS, Azure, Google and Oracle cloud

Vulnerability Scanning

- Scan CI pipelines and registries, container images, VM images, and functions
- Find known vulnerabilities, malware, embedded secrets, OSS licensing, configuration, and permissions issues
- Filter and prioritize vulnerabilities based on risk factors such as exploitability, remote access, and running workloads

Dynamic Threat Analysis

- Detect and mitigate hidden malware in container images using a secure sandbox
- Thwart supply chain attacks before images are deployed in production

Container Security

- Use scan results to set policies for image deployment and prevent the use of unapproved images
- Mitigate known vulnerabilities with Aqua vShield, preventing exploits with no code changes
- Enforce container immutability by preventing drift against their originating images
- Use machine-learned behavioral profiles to narrow down capaiblities including syscalls
- Securely inject secrets into containers with no downtime while leveraging your existing vaults
- Protect Linux and Windows containers, TAS (PCF) containers, and CaaS (AWS Fargate, ACI)

Kubernetes Security

- Get real-time discovery and visualization of risks across your Kubernetes clusters
- Kubernetes Security Posture Management (KSPM) ensures ongoing secure configuration with built-in CIS benchmarks, least privilege RBAC, pen-testing, and pod deployment policies
- Secure Red Hat OpenShift, TKGI, Rancher, Amazon EKS, Azure AKS, Google GKE, and more

Cloud VM Security

- Use vulnerability and malware scan results to set policies for VM compliance
- Continuously use File Integrity Monitoring (FIM), system and registry integrity, and user activity
- Protect both Linux and Windows-based cloud instances

Serverless Security

- Use vulnerability and permission scan results to set policies for function compliance
- Track usage patterns for unused permissions and runtime anomalies
- Protect AWS Lambda functions at runtime, prevent code injections and use honeypots to detect indications of compromise

Identity-Based Segmentation

- Establish zero-trust networking between workloads of the same application identity
- Discover network connections across containers, VMs, and functions to create rules
- Firewall connections seamlessly within and across Kubernetes clusters and cloud providers

Regulatory Compliance

- Automate CIS benchmark tests for Cloud Fundamentals, Linux, Kubernetes, and Docker
- Out-of-the-box policies for PCI-DSS, HIPAA, NIST, and GDPR
- Maintain history of scan results, policy changes, secrets rotation, runtime events, user logins

Multi-Application RBAC

- Maintain separation of duties across teams and applications
- Grant least privilege permissions by role to specific cloud native artifacts, assets, and workloads
- Leverage existing identity management infrastructure and security groups to assign roles

Platform and Integrations

- Manage users with LDAP/Active Directory and Single-Sign-On
- Send events to SIEM, analytics and monitoring solutions
- Collaborate across teams with Slack, PagerDuty and Jira integrations
- Run as self-hosted solution or consume as SaaS

aqua

aquasec.com

contact@aquasec.com

@Aqua Security

@AquaSecTeam

in/Aqua Security

@AquaSecTeam