aqua

Solution Sheet

The Comprehensive Security Platform for Containers and Cloud-Native Applications

With the agility, scale and flexibility they bring, cloud-native applications require a new approach to security. Aqua's platform is **natively architected for containers**, providing IT security with **full visibility and control** over application activity across the lifecycle, while remaining transparent and unintrusive to DevOps.

Full Visibility and Control

Gain visibility into container activity and enforce security policies

Protecting Cloud-Native Workloads

Automated runtime protection against attacks, including zero-day threats

Enabling DevSecOps

"Shift left" security with automated tests and controls within the CI/CD pipeline

Continuous Image Assurance

Scan images for known vulnerabilities, detect malicious code, and enforce image integrity throughout the lifecycle.

Runtime Protection

Advanced threat detection and mitigation, with container activity controls, network segmentation, and host integrity controls.

Intelligent Security Policy

Automated policy creation using machine learning that understands contextual container behavior.

Security Automation at Scale

Zero-touch deployment and management, with APIs and integrations with orchestration tools.

Fine-Grained User Access Control

Role-based permissions per specific container, image, host, cluster, namespace, network and storage volume.

Cross-Platform

Supports Docker and Kubernetes environments, Linux and Windows Containers, on-prem or on public cloud.

aqua

Solution Sheet

The End-to-End Platform for Cloud-Native Security

Continuous Image Assurance

- Scan images and AWS Lambda functions for known vulnerabilities, malware, hard-coded secrets, based on a continuous feed correlated across multiple source
- Scans OS packages (RPM and Deb) and language packages: Java, NodeJS, Ruby, PHP, Python, C/C++
- Integrates with CI/CD to automate security testing in the pipeline, and with Jira for developer feedback

User Access Control

- Role-based privilege definition per container/host/application/network/storage volume
- Allow/disallow specific user actions, e.g. start/stop, log access, read/write access, volume access

Secrets Management

- Securely inject secrets into containers with no downtime
- Integrates with HashiCorp Vault, CyberArk Password Vault, AWS KMS and Azure Vaults

Runtime Protection

- Monitor container activity, detect and granularly block suspicious processes
- Behavioral machine-learned profiles that whitelist required capabilities
- Prevent changes in running containers compared to original image
- Protect the OS kernel using automated syscall profiling

Microservices Firewall

- Visualize container networking
- Firewall container networking based on orchestrator concepts (pod name, namespaces), IP/CIDR addresses, and DNS

Auditing & Compliance

- Automated CIS Benchmark tests for Kubernetes and Docker
- Monitor hosts for vulnerabilities, malware, and login attempts
- Out-of-the-box runtime policies for PCI, HIPAA, NIST and GDPR
- Maintain history of scan results, policy changes, secrets rotation
- Granular event logging and reports

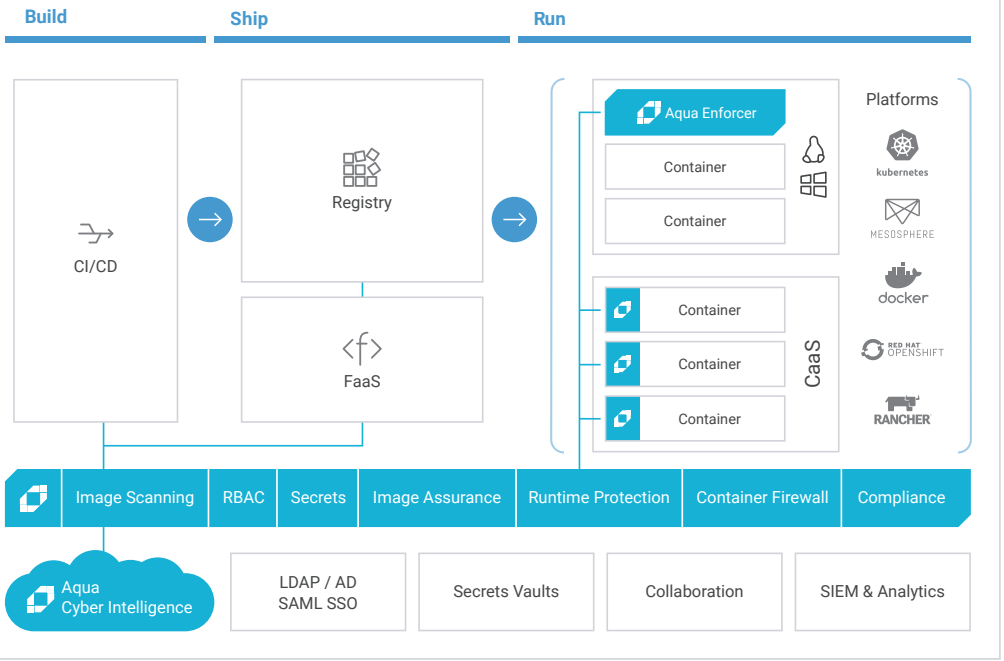
Integrations

- CI/CD tools: Jenkins, GoCD, TeamCity, Bamboo, GitLab and Microsoft VSTS
- Identity Mgmt: Active Directory / LDAP, SAML Single Sign-On
- SIEM, Analytics and Alerts: ArcSight, AWS CloudWatch, ElasticSearch, Google CSCC, Logentries, Loggly, Microsoft OMS, Splunk, Sumologic, Syslog

Supported Environments

- Linux (Docker, CRI-O, containerd) and Windows containers
- Registries: DockerHub, Amazon ECR, Google GCR, CoreOS Quay, JFrog Artifactory, Azure ACR or any v1/v2 registries
- Orchestrators: Kubernetes, Mesos, Docker Swarm, Red Hat OpenShift, Amazon ECS, Rancher
- AWS (inc. Fargate and Lambda), Azure (inc. ACI), Google Cloud, IBM Cloud

Aqua Deployment Architecture



About Aqua

Aqua Security enables enterprises to secure their cloud-native applications from development to production, accelerating container adoption and bridging the gap between DevOps and IT security.

Aqua's Container Security Platform provides full visibility into container activity, allowing organizations to detect and prevent suspicious activity and attacks, providing transparent, automated security while helping to enforce policy and simplify regulatory compliance.

Contact

contact@aquasec.com

www.aquasec.com

@aquasecteam

linkedin.com/company/aquasecteam

US HQ:
800 District Avenue, Suite 310,
Burlington, MA 01803

Intl. HQ:
2 Ze'ev Jabotinsky Rd.,
Ramat Gan, Israel 52520