aqua

SOLUTION SHEET

The Comprehensive Security Platform
for Containers, Serverless, 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 and serverless workloads** providing IT security with **full visibility and control** over application activity across the lifecycle, while remaining transparent and unobtrusive to DevOps.

Enabling DevSecOps

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

Protecting Cloud Native Workloads

Automated runtime protection against attacks, including zero-day threats

Full Visibility and Control

Gain visibility into application activity and improve compliance and forensics

Run Only Trusted Code

Scan images and functions for vulnerabilities, configuration, and permissions issues, and enforce their integrity across the lifecycle.

Next-Gen Runtime Protection

Automated profiling and whitelisting of capabilities, dev-to-prod drift prevention, integrity monitoring & network segmentation.

Full Stack Security

Harden and protect functions, containers, VM hosts, and Kubernetes against misconfiguration and attacks.

Security Automation at Scale

Zero-touch deployment and management, using APIs and integrations with orchestrators and cloud configuration.

Fine-Grained User Access Control

Role-based privileges and permissions across applications for specific services, images, clusters and hosts.

Secure Once, Run Anywhere

Seamlessly works across Linux and Windows environments, all orchestrators, and private, public or hybrid clouds.

The End-to-End Platform for Cloud Native Security

Image and Function Assurance

- Scan images and functions for known vulnerabilities, malware, secrets, open source licenses, configuration and permissions issues
- Scan OS packages (RPM and Deb) and language packages, curated from multiple sources
- Integrate with CI/CD to automate security testing in the pipeline
- Encrypt container images to protect data and intellectual property
- Block images and functions that violate security policy from running

Container Runtime Protection

- Monitor container activity, detect and granularly block suspicious processes
- Use automated Vulnerability Shields to detect and prevent CVE exploits
- Enforce immutability by preventing drift between containers and their originating images
- White-list only container capabilities that are used based on behavioral machine-learned profiling
- Protect the OS kernel using automated syscall profiling

Serverless Runtime Protection

- Enforce immutability by preventing code injection and writing into /tmp directory
- Monitor functions for abnormal activity patterns
- Use honeypots to detect malicious activity in functions

Microservices Firewall

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

User Access Control

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

Secrets Management

- Securely inject secrets into containers with no downtime
- Leverage secrets vaults for lifecycle controls, includng HashiCorp Vault, CyberArk EPV and Conjur, AWS KMS and Azure Vault

Auditing & Compliance

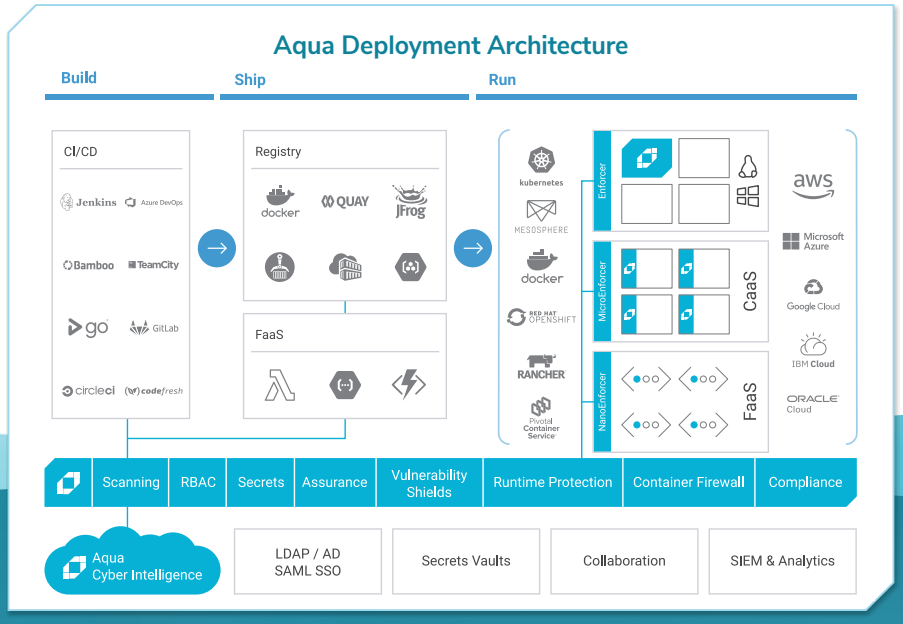
- Visualize cluster security posture by namespace deployment, pod, and host
- Automate CIS certified Benchmark tests for Linux, Kubernetes and Docker
- Monitor hosts for vulnerabilities, malware, user activity and login attempts
- Out-of-the-box runtime policies for PCI, HIPAA, NIST and GDPR
- Maintain history of scan results, policy changes, secrets rotation
- Granular event logging and reports

Integrations

- CI/CD: Jenkins, Azure DevOps, CircleCI, Bamboo, GitLab, GoCD, TeamCity, and Codefresh
- Identity Mgmt: Active Directory / LDAP, SAML Single Sign-On, Okta
- SIEM, Analytics and Alerts: ArcSight, AWS CloudWatch, Datadog, ElasticSearch, Google CSCC, Logentries, Loggly, Microsoft OMS, Splunk, Sumo Logic, Syslog

Supported Environments

- Linux (Docker, CRI-O, containerd) and Windows containers
- Registries: DockerHub, Amazon ECR, Azure ACR, Google GCR, Red Hat Quay, JFrog Artifactory, Harbor, Sonatype Nexus
- Orchestrators: Kubernetes (incl. Red Hat OpenShift, Amazon EKS, Azure AKS, Google GKE, Pivotal Container Service - PKS, Rancher, Docker EE, Mesosphere DC/OS, IBM Cloud Private), Amazon ECS, Mesos, and Docker Swarm
- Clouds: AWS, Azure, Google Cloud, IBM Cloud, Oracle Cloud



Contact

contact@aquasec.com www.aquasec.com

US HQ: 800 District Avenue, Suite 510,Burlington, MA 01803
Intl. HQ: 2 Ze'ev Jabotinsky Rd., Ramat Gan, Israel 52520