aqua

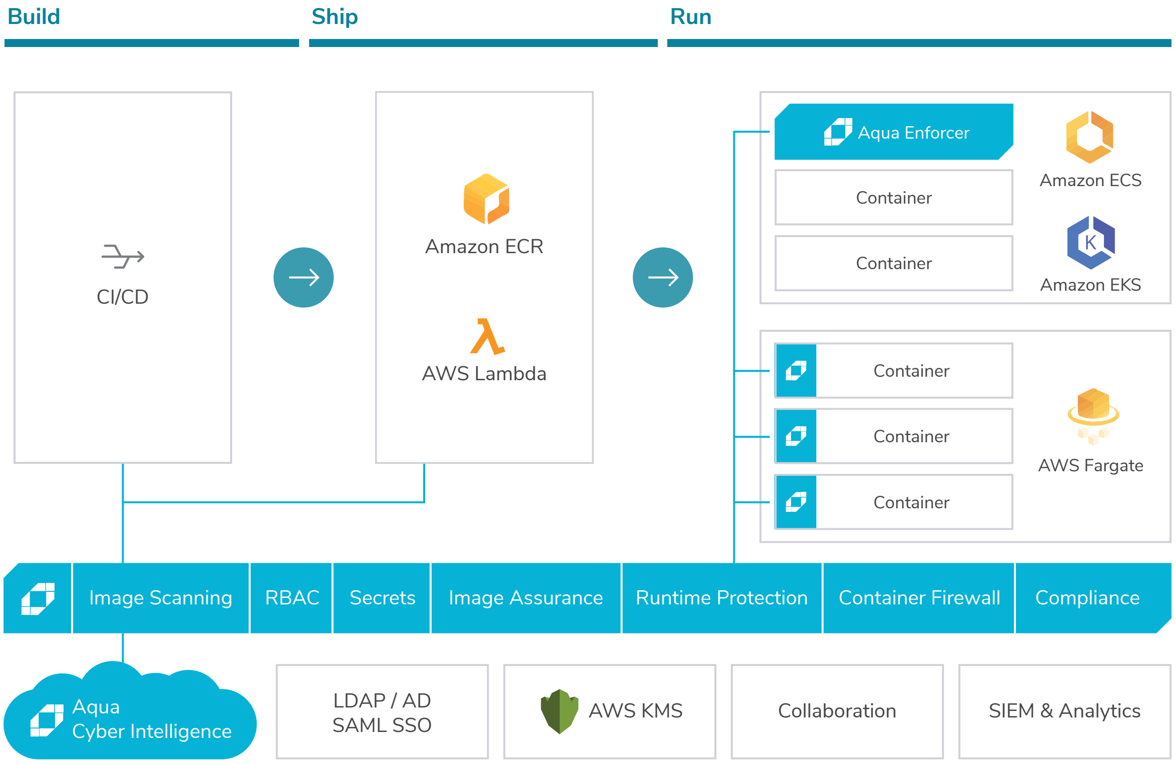
Solution Sheet

Aqua Security for Amazon Web Services (AWS)

Full Lifecycle Security for Cloud Native Applications

AWS offers a range of services for developing and deploying cloud-native applications, including Amazon Elastic Container Service (Amazon ECS) for container orchestration; Amazon Elastic Container Service for Kubernetes (Amazon EKS) based deployment; AWS Fargate for on-demand container scaling; AWS Lambda for serverless functions; Amazon Elastic Container Registry (Amazon ECR) for storing, managing and deploying Docker container images; and AWS Key Management Service (AWS KMS) for securely storing and managing keys.

The solution provides comprehensive security for the entire lifecycle of container-based and cloud-native applications, with consistent policies and controls, from image build to any type of cloud-native AWS deployment and runtime.



Aqua Security's image scanner is available in AWS Marketplace, on a pay-per-scan basis:

- Full-featured security scanning for container images, on Amazon ECR or other registries
- Pay only for what you scan
- Easy to deploy and use
- Supports AWS PrivateLink for use within VPCs

Available in AWS Marketplace

www.aquasec.com

Secure Images on Amazon ECR and Functions on AWS Lambda

Automatically scan images stored in Amazon ECR and AWS Lambda functions for vulnerabilities, malware, configuration-errors, secrets, open-source licenses, and sensitive data:

- Discover and maintain up-to-date image inventory
- Scan for malware and known vulnerabilities based on multiple public, vendor-issued and proprietary sources
- Scan OS packages (RPM, Deb, Alpine), language packages (Java, C++, NodeJS, PHP, Ruby, Python and more)
- Detect and amend over-provisioned function privileges
- Generate image bill of materials (packages, layer history, OSS license information)
- Conduct custom compliance checks (SCAP, shell scripts)
- Get actionable guidance for fast and effective remediation
- Integrate with CI/CD tools to automate security scanning in the build phase
- Integrate with Jira, Slack and PagerDuty to provide developers with immediate feedback

Protect Workloads on Amazon ECS, Amazon EKS, and AWS Fargate

Secure runtime workloads running across Amazon's container-based services Amazon ECS, Amazon EKS, and AWS Fargate. Employ both passive and active runtime controls to ensure that applications are secure, detect and stop attacks.

Image Integrity Validation and Drift Prevention

- Lock down and prevent unauthorized images from running, whether due to policy violations or attempts to run unchecked or spoofed images
- Cryptographic digest of images allows tracking of images from creation to runtime
- Prevent changes to running containers including binaries, executables and files

Granular Role-Based User Access Control

- Role-based privileges that limit user access per container, host, application, network, storage volumes
- Allow/disallow specific user actions, e.g. start/stop, log access, read/write
- Log all user privilege escalation attempts

Container Runtime Profiles

- Automatically create container security profiles based on runtime parameters
- Block unneeded executables, network connections, ports and file paths
- Centrally manage and enforce SECCOMP profiles
- Out-of-the-box runtime profiles for popular Docker images

Runtime Workload Protection

- Rapidly detect and automatically respond to suspicious activity via whitelisting of normal Behavior, blocking specific activities and attacks without killing the container
- Block bad reputation IP addresses
- Visualize and automatically map container network connections, create microservice-level firewall rules to prevent network traversal
- Monitor and log resources activity and consumption, including network connectivity
- Send policy violations and activity data to 3rd party SIEM

Inject Secrets from AWS KMS

- Encrypt and securely distribute secrets stored in AWS KMS to running containers
- Maintain secrets visibility only inside the intended containers, with no visibility on hosts or persistence on disk
- Easily update/revoke/rotate secrets with no need to restart containers and no downtime

Enable Regulatory Compliance

- Check Amazon EKS and Amazon ECS instances against the CIS Kubernetes and Docker benchmarks
- Scan Amazon ECS instances for malware and known vulnerabilities
- Ensure segregation of duties using granular RBAC

aws partner network

Advanced
Technology Partner

Container Competency

About Aqua

Aqua Security enables enterprises to secure their container-based 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