Solution Brief

Aqua Security for Amazon Web Services (AWS)

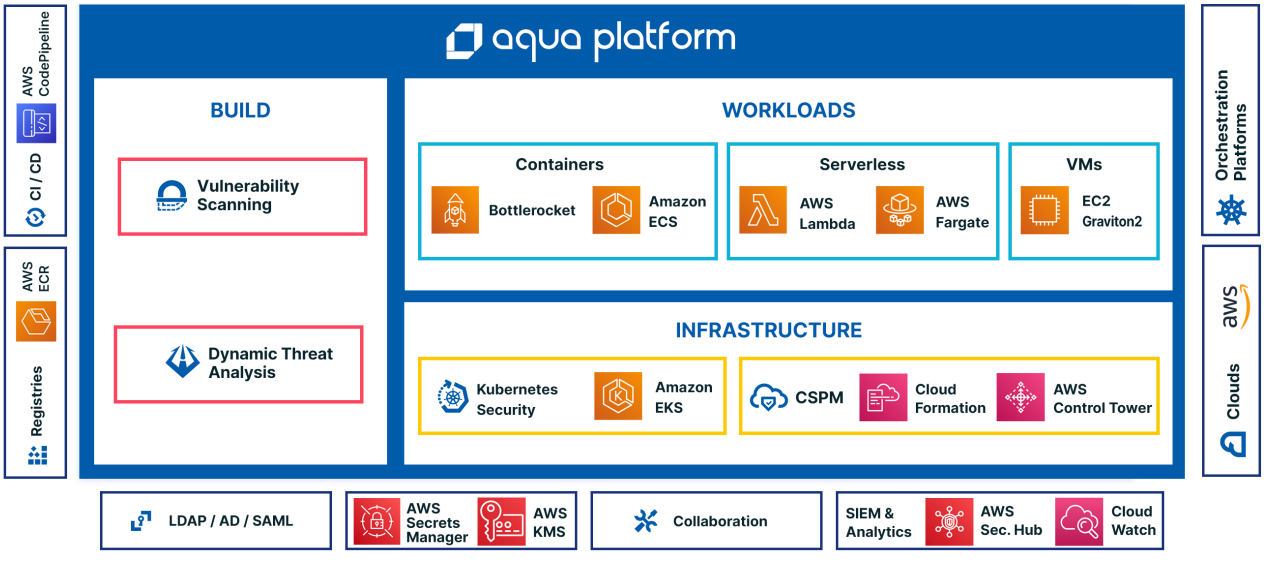
aws partner network
Advanced Technology Partner
Container Competency

Full Lifecycle Security for Cloud Native Applications

Aqua Security enables AWS customers to securely build, scale and automate cloud native applications as well as ensure that controls, configurations and account settings across their environments conform to security best practices and compliance requirements.

Aqua facilitates security and DevOps collaboration for the cloud native journey, embeds security and assurance into AWS build and artifact pipelines, validates and remediates AWS infrastructure configurations, and protects workloads at runtime - including detecting malware, unauthorized changes and supply chain attacks.

With native support for a broad range of AWS compute, container, management & governance, and security services, Aqua's integrated platform provides contextual information that drives more effective security and risk mitigation as part of the shared responsibility model.



End to End Protection for Cloud Native Apps on AWS

The Aqua Enterprise Platform provides comprehensive security for the entire lifecycle of container-based and cloud-native applications, extending from image build to a broad set of cloud-native AWS deployment and runtime services. Aqua also integrates with security and management tools such as AWS Secrets Manager, Control Tower and CloudWatch.
Aqua provides highly-integrated security controls for AWS customers building and deploying applications at scale, including:

- Amazon ECR for storing and managing container images
- Amazon ECS (and ECS Anywhere) for container orchestration
- Amazon EKS for Kubernetes-based deployments
- AWS Fargate for on-demand container scaling
- AWS Lambda for serverless functions
- AWS EC2 VMs running on Graviton2 processors

Aqua's Cloud Security Posture Management delivers centralized visibility across complex cloud native stacks for AWS accounts and services configurations, providing insight into potential risks and controls validation for CIS AWS Benchmarks and AWS Well-Architected Framework security best practices.
The platform can be provisioned as infrastructure as code native resource types from AWS Marketplace through CloudFormation Public Registry templates.
Aqua is an Advanced APN member and Container Competency technology partner.

Secure the Build

- Automatically scan images stored in Amazon ECR and AWS Lambda functions and CloudFormation templates for vulnerabilities, malware, configuration errors, excessive permissions, secrets, and sensitive data
- Scan AWS CodePipeline artifacts for vulnerabilities without disrupting existing build and deploy workflows
- Encrypt and securely distribute secrets stored in AWS Secrets Manager to running containers
- Leverage AWS CloudTrail for real-time events monitoring of high-risk security best practices violations, vulnerabilities, potential compromises, or malicious activity

Secure the Infrastructure

- Validate configurations, access controls, APIs and identify security posture and compliance risks for Amazon EKS, Amazon ECS & other build, orchestration tools
- Maintain continuous auditing of AWS environment configuration and controls against CIS Benchmarks, AWS Well Architected best practices
- Extend Kubernetes-native security capabilities, compatible with Open Policy Agent (Rego expressions) for admission controllers on EKS
- Scan AWS CloudFormation templates for misconfigurations, vulnerabilities including app dependencies and OS packages, and prevent unauthorized changes through Drift Prevention

Secure the Workload

- Protect against run-time attacks for container, VM and serverless workloads with Enforcers purpose-built for Amazon ECS, Lambda BottleRocket, AWS EC2 VMs running on AWS Graviton processors and AWS Fargate containers as a service
- Rapidly detect and automatically respond to exploits, unauthorized changes or injection of code and executable at runtime without stopping all container image processes
- Mitigate known vulnerabilities in running workloads with Aqua vShield by preventing exploits with no code changes
- Protect Lambda functions at runtime with embedded Enforcer with runtime

Available in AWS Marketplace

The Aqua Container Native Security Platform is available as both SaaS and self hosted:

- The full-featured Aqua platform is available for on-demand consumption on the AWS Marketplace, providing security across the application lifecycle, from development to production
- Customers can purchase Aqua on a Pay-As-You-Go basis, through Private Offer, or via Consulting Partner Private Offer as well as SaaS
- Aqua Developer, a free SaaS service for Cloud Security Posture Management (CSPM) for non-production environments

aws marketplace

Aqua Security is the largest pure-play cloud native security company, providing customers the freedom to innovate and run their businesses with minimal friction. The Aqua Cloud Native Security Platform provides prevention, detection, and response automation across the entire application lifecycle to secure the build, secure cloud infrastructure and secure running workloads wherever they are deployed. Aqua customers are among the world's largest enterprises in financial services, software, media, manufacturing and retail, with implementations across a broad range of cloud providers and modern technology stacks spanning containers, serverless functions, and cloud VMs.

aquasec.com
@AquaSecTeam
in/Aqua Security
@Aqua Security
@AquaSecTeam