Aqua Enterprise Security Platform

Cloud Native Security Platform for AWS

Why Aqua?

- Comprehensive cloud native security platform with deep integration into AWS infrastructure & services
- Consolidated, scalable approach to securing, protecting, mitigating risk and monitoring the cloud native application lifecycle
- Centralized visibility, insight into potential risks and controls validation for CIS Benchmarks and AWS Well-Architected Framework security best practices across complex cloud native stacks
- Consistent policies, unified security enforcement to reduce risks for DevOps from build, orchestration and runtime for AWS services
- Leverage AWS CloudTrail for real-time events monitoring of high-risk security best practices violations, vulnerabilities, potential compromises, or malicious activity.
- Flexible vulnerability and controls remediation options– assisted, automated & manual options
- Extensible architecture based on open source technologies

aws partner network

Advanced

Technology Partner

Containers Competency

Marketplace Seller

Aqua Enterprise Overview

Aqua's cloud native security platform empowers security, operations, and DevOps teams to securely scale application delivery, enforce infrastructure protection policies and automate security best practices without impeding workflows and processes. As an Advanced Technology and Container Competency partner, Aqua delivers security coverage, policy enforcement, workload integrity, remediation and runtime monitoring via AWS CloudTrail for key Amazon Web Services services, encompassing: Amazon ECS for container orchestration, Amazon EKS for Kubernetes-based deployments, AWS Fargate for on-demand container scaling, AWS Lambda for serverless functions, Amazon ECR for storing and managing container images and AWS Graviton for EC2 VMs. Aqua's protection extends to infrastructure as code with scanning for AWS CloudFormation and Terraform templates for vulnerabilities, malware or exposed secrets.

Product Features

Automate DevSecOps

- Shift left security early into the DevOps pipeline - accelerate application delivery, remove obstacles and mitigate risk for digital transformation
- Embed and integrate comprehensive security testing and powerful policy-driven controls into DevOps pipelines for secure scaling of app delivery
- De-risk adoption at scale of advanced AWS services with consistent control validation, monitoring and auditing

Automate Regulatory Compliance

- Automate CIS benchmark tests and validation for Cloud Fundamentals, Linux, Kubernetes and Docker.
- Out-of-the-box policies for PCI-DSS, HIPAA, EU GDPR and the NIST framework.
- Maintain history of scan results, policy changes, remediation actions, secrets rotation, runtime events & user logi

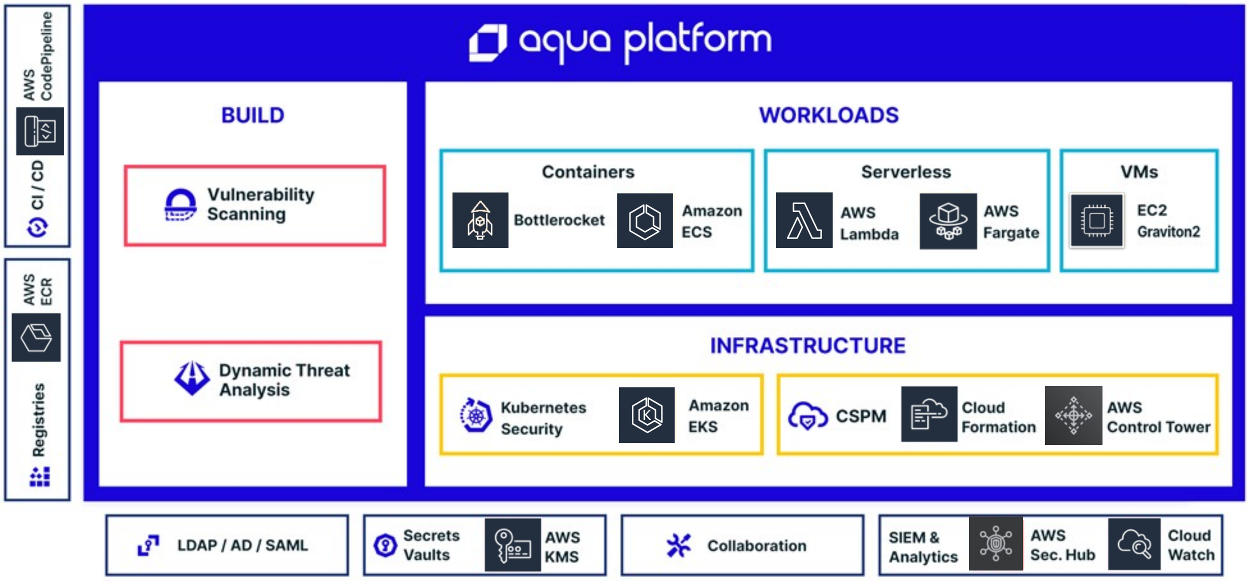
Secure Cloud-Native Apps

- Enforce container immutability by preventing drift against their originating images
- Rapidly detect and automatically respond to suspicious activity via enforcement of allowed behavior, blocking specific activities and attacks without stopping all container processes
- Mitigate known vulnerabilities with Aqua vShield, preventing exploits with no code changes

How It Works

The Aqua Enterprise Platform provides comprehensive security for the entire lifecycle of container-based and cloud-native applications, with consistent policies and controls, from image build for a broad set of cloud-native AWS deployment and runtime services. The platform is deployed as infrastructure as code package from AWS Marketplace through CloudFormation templates.

- Automatically scan images stored in Amazon ECR and AWS Lambda functions for vulnerabilities, malware, configuration errors, secrets, open-source licenses, and sensitive data
- Secure runtime container, VM and serverless workloads running across Amazon's services including Amazon ECS, BottleRocket, AWS EC2 using AWS Graviton processors and AWS Fargate
- Employ both passive and active runtime controls to ensure that applications are secure, detect and stop attacks via Aqua vShield for identified vulnerabilities that have not yet been patched.
- Scan, validate access controls, configurations, APIs and identify security posture and compliance risks for Amazon EKS, Amazon ECS and other build, orchestration tools
- Maintain continuous auditing of configuration and controls through CIS Benchmark, best practices comparison



Aqua Security SaaS Options

Aqua Wave for Cloud Security Posture Management

Aqua Wave provides a SaaS-based, cloud security posture management (CSPM) solution that continually audits your cloud accounts for security risks and misconfigurations. This is performed across hundreds of configuration settings and compliance best practices, enabling consistent, unified multi-account security. It also provides self-securing capabilities to help ensure your cloud accounts do not drift out of compliance by leveraging a policy-driven approach. Aligning with your multi-account strategy, Aqua CSPM integration for AWS Control Tower accelerates the onboarding process by employing automation and enables your organization to start from a secure foundation right out the gate. Learn more here.

Solution available in AWS Marketplace