aqua

Solution Sheet

aws partner network

Advanced Technology Partner

Container Competency

Aqua Security for AWS Lambda Functions

The Challenge of Securing Serverless Functions

As organizations move to architectures that incorporate serverless functions (FaaS), they need to implement granular security and compliance controls suited to the unique challenges of managing serverless. Lack of visibility into which functions are being used and where, vulnerabilities they may contain, over-provisioned permissions on AWS Lambda, and embedded secrets such as AWS access and secret keys all increase the attack surface and create risks that must be discovered, assessed, and mitigated.

Functions typically run for extremely short durations. Aqua's runtime protection solution is performance-optimized, with minimal impact on function invocation time and resource use.

The Aqua Approach: Dedicated Security for AWS Lambda Functions

Aqua's solution for securing AWS Lambda functions uses dedicated controls that address the unique risks and operational constraints of serverless functions, while being highly optimized for performance and speed:

Discovery and Visibility

Discover and inventory stored AWS Lambda functions, providing visibility into your overall risk posture, in the CI/CD pipeline and in AWS accounts

Risk Assessment & Mitigation

Assess functions for risk factors including known vulnerabilities, overprovisioned and unused permissions, embedded secrets, and suspicious behavior.

Advanced Runtime Protection

Prevent code injection into running function, use serverless firewall to restrict outbound connections, and insert tripwire to detect malicious activity.

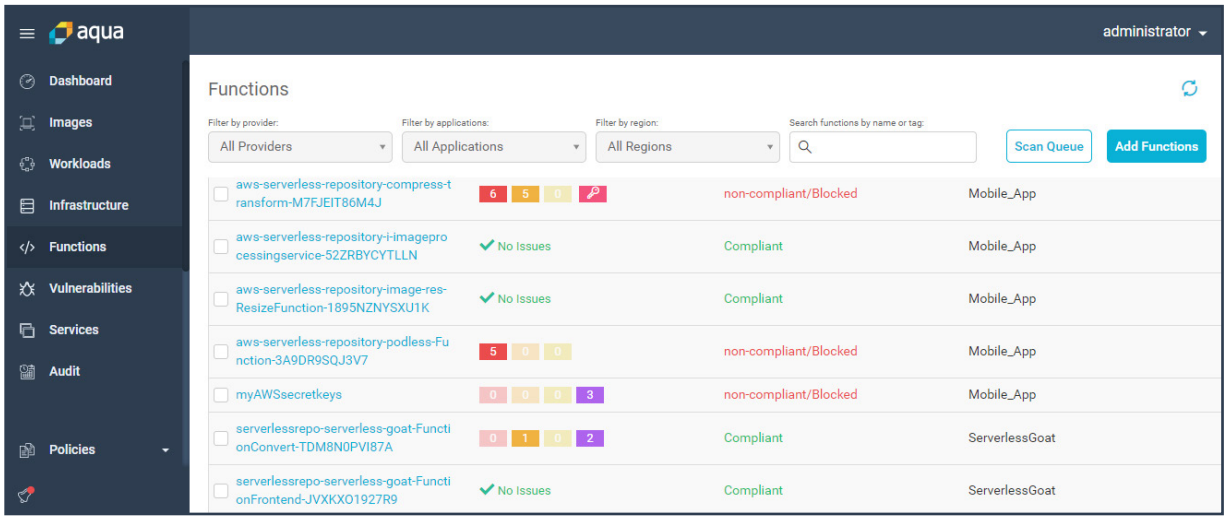
Auditing and Compliance

Track events and policy violations for Lambda functions, use your existing SIEM or analytics tools to for single-pane-of-glass view.

Solution Sheet

End-to-End Security for AWS Lambda
from Development to Runtime

Aqua provides granular visibility and controls for securing AWS Lambda functions, reducing their attack surface and enforcing your organization's security and compliance policy.
As part of Aqua's market leading cloud native security platform, you can enhance the security of your entire cloud native stack on AWS, from containers running on Amazon EKS and ECS, to AWS Fargate and AWS Lambda.



Risk Posture Discovery

- **Automatically retrieve** and scan inventory of functions from your AWS accounts
- **Get single pane-of-glass** visibility of your Lambda functions risk posture
- **Send scan results** and security events data to your existing SIEM and analytics tools

Function Risk Assessment

- **Scan for malware** and known vulnerabilities based on multiple public, vendor-issued and proprietary sources
- **Detect over-provisioned**, unused, and shared permissions and roles
- **Discover AWS-specific** credentials and keys embedded in functions or their environment variables

Advanced Runtime Protection

- **Block execution** of functions that present unacceptable risk
- **Prevent code injection** into running functions, block write access to /tmp directory
- **Limit functions' outbound** connections with serverless firewall
- **Embed tripwires** to detect malicious attempts to exploit functions

CI/CD Integration

- **Scan functions** as they are built in your CI pipeline, providing feedback to developers on security issues
- **Automatically** fail the build of functions based on a preconfigured policy
- **Supports** Jenkins, CircleCI, TeamCity, Gitlab, and more

contact@aquasec.com
www.aquasec.com
@AquaSecTeam
AquaSecTeam