SOLUTION SHEET

aqua

aws partner network
Advanced Technology Partner
Containers Competency
Marketplace Seller

# 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 functions.

Lack of visibility into which functions are being used and where, vulnerabilities may contain over-provisioned permissions on AWS Lambda, and embedded secrets such as AWS access and secret keys. This increases the attack surface and creates risks that must be discovered, assessed, and mitigated.

Additionally, extremely short runtime durations of serverless functions mean that security controls must be as preemptive and preventative as possible, while minimizing impact on function performance 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, as well as the operational and performance constraints of serverless functions.

#### 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 vulnerabilities, overprovisioned and unused permissions, and embedded secrets, and prevent risky functions from being executed in runtime.

#### Runtime Protection

Block malicious code injection from being added to a running function, basically whitelisting what the function was invoked with and blocking any attempt to run new code.

#### Honeypots

Detects malicious intent by luring attackers to exploit what is perceived to be "low hanging fruit" embedded into the function code or its environment variables

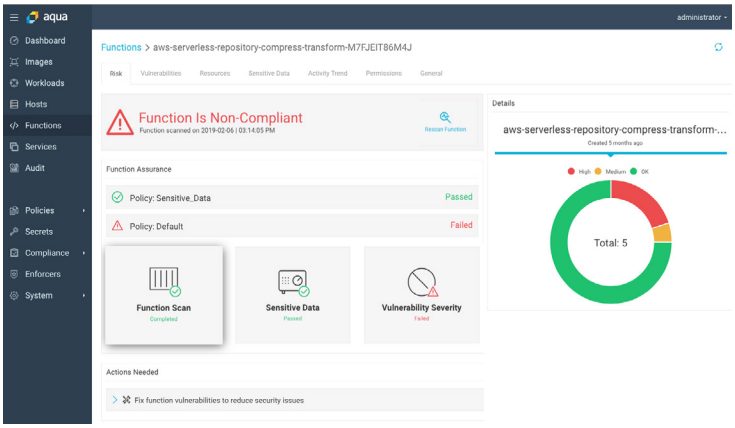
#### Auditing and Compliance

Track suspicious activities and risk-related events, get notified with alerts or view within your existing SIEM and analytics solutions, via one of Aqua's many integrations.

aqua

# 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 policies, ensuring that your serverless applications are both performant and secure in runtime.
Using 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 AWS accounts

**Get single pane-of-glass** visibility of your Lambda functions risk posture

**Send scan results** and security event 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 or administrator roles that should be reduced or eliminated

**Discover AWS-specific** sensitive data (access credentials, keys) embedded in functions or in their environment variables

## Runtime Protection

**Deploy Aqua's NanoEnforcer** by adding it as a Lambda Layer with no modifications to the function code or its runtime

**Protect the function's "/tmp"** directory against unauthorized abuse, blocking code injection

**Control the types** of executables that developers are allowed to include in 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, Bamboo, CircleCI, TeamCity, Gitlab, and more

## Function Assurance

**Prevent execution** of Lambda functions that present unacceptable risk

**Define assurance policies** based on vulnerability scores, malware and AWS Lambda permissions and triggers

**Get notifications** and generate audit events when functions were blocked from executing

## Honeypot Malicious Actors

**Insert fake AWS** account credentials into Lambda functions where attackers would likely seek them

**Constantly monitor** the environment to detect attempts to use the credentials

**Use detection** as a clear indicator of compromise of your Lambda environment

Contact
contact@aquasec.com
www.aquasec.com
@aquasecteam
linkedin.com/company/aquasecteam

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