aqua

Solution Sheet

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.

Additionally, extremely short runtime durations of serverless functions mean that security controls must be as preemptive and preventative as possible, mitigating risk well before the function is executed and preventing its execution if a new risk is discovered.

aws partner network

Advanced
Technology
Partner

Container Competency

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:

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

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

Risk Mitigation

Prevent Lambda functions with unacceptable risk from being executed in your AWS environment, applying least privilege and reducing the attack surface.

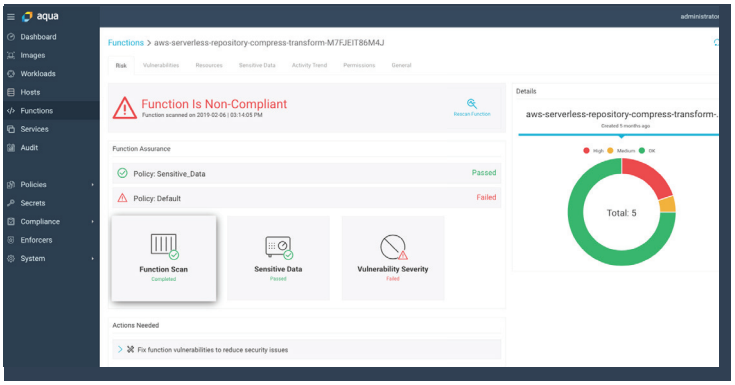
Auditing and Compliance

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

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 to ensure that high-risk functions will not be allowed to execute.

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 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 Assurance

- Prevent execution of Lambda functions that present unacceptable risk
- Define assurance policies based on vulnerability severity and score, the presence of embedded secrets, malware, open source license types, AWS Lambda permissions and triggers
- Get notifications and generate audit events when functions were blocked from executing

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 shouldn't be assigned to functions
- Discover AWS-specific sensitive data (access credentials, keys) embedded in functions or in their environment variables

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

About Aqua

Aqua Security enables enterprises to secure their container and cloud native applications from development to production, accelerating application deployment 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 in real time. Integrated with container lifecycle and orchestration tools, the Aqua platform provides transparent, automated security while helping to enforce policy and simplify regulatory compliance. Aqua was founded in 2015 and is backed by Lightspeed Venture Partners, Microsoft Ventures, TLV Partners, and is based in Israel and Boston, MA.

For more information, visit www.aquasec.com or follow us on twitter.com/AquaSecTeam.

Contact

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