Contrast Serverless Application Security
Secure AWS Lambda and Microsoft Azure Functions

While serverless applications are gaining traction due to their instant scalability, high availability, greater business agility, and improved cost efficiency, traditional application security testing (AST) tools cause workflow inefficiencies that ultimately bottleneck serverless release cycles.

Challenges with serverless security today:

Visibility. Not all attacks come via HTTP. Serverless applications may have integrations to APIs or external services.

Large attack surface. Complex serverless functions may have multiple dependencies and external integrations.

Shared resources. Functions may share resources with other functions or services within the same cloud platform provider account which can increase the security risk if one of these resources is compromised.

Permissions are overwhelming. Functions require permissions to access other services, and these permissions must be set up correctly. Misconfigured permissions can lead to unauthorized access to sensitive data or services. With hundreds and thousands of functions, manually setting permissions for each is not practical.

Shared security model. Organizations are still responsible for their own code, while cloud providers manage much of the underlying infrastructure.

Contrast Serverless Application Security

Contrast Serverless Application Security is designed specifically for serverless development. This purpose-built solution ensures that security and development teams get the testing and protection capabilities they need without legacy inefficiencies that delay release cycles.

Contrast's approach uses context-based static and dynamic engines to automatically detect vulnerabilities within serverless environments. It then empowers developers to validate and prioritize alert test results for remediation—improving operational efficiency of serverless security by 50% while accelerating development release cycles. The solution's differentiating values include:

Visibility. Gain complete security visibility across your serverless architecture.

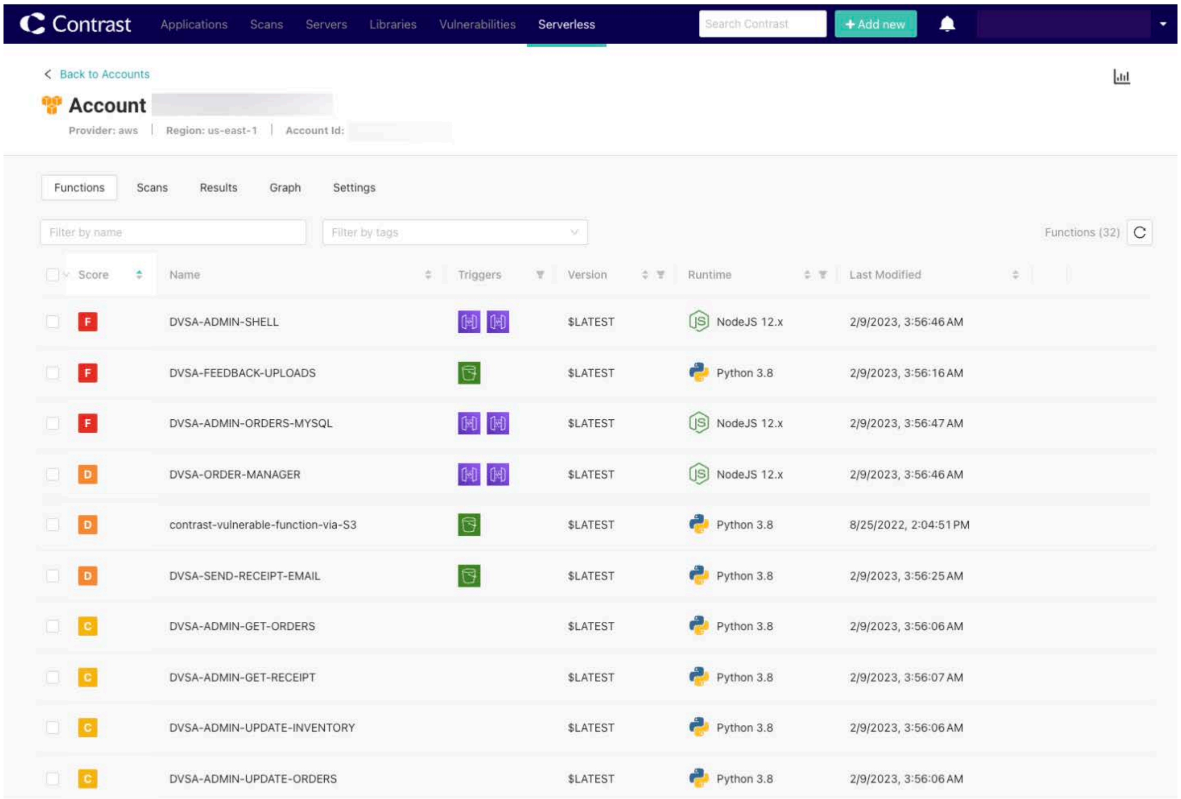
Speed. Onboarding only takes a few minutes, with zero configuration and immediate results after scanning.

Frictionless. Automatically discovers any new change deployed to the monitored environment, issues new tailored security tests, and validates finding in close to real time. The result is that Contrast's solution is completely transparent for developers.

Accuracy. Secure imported libraries and custom code. Prioritized vulnerability results are based on cloud context and impact. Contextual awareness of issues helps provide developer-friendly remediation support.

Permissions. Establish least-privilege access policies for deployed functions.

For more information about Contrast Serverless Application Security, visit www.contrastsecurity.com/contrast-serverless-application-security.



Account [redacted]

Provider: aws | Region: us-east-1 | Account Id: [redacted]

Score	Name	Triggers	Version	Runtime	Last Modified
F	DVSA-ADMIN-SHELL		$LATEST	NodeJS 12.x	2/9/2023, 3:56:46 AM
F	DVSA-FEEDBACK-UPLOADS		$LATEST	Python 3.8	2/9/2023, 3:56:16 AM
F	DVSA-ADMIN-ORDERS-MYSQL		$LATEST	NodeJS 12.x	2/9/2023, 3:56:47 AM
D	DVSA-ORDER-MANAGER		$LATEST	NodeJS 12.x	2/9/2023, 3:56:46 AM
D	contrast-vulnerable-function-via-S3		$LATEST	Python 3.8	8/25/2022, 2:04:51 PM
D	DVSA-SEND-RECEIPT-EMAIL		$LATEST	Python 3.8	2/9/2023, 3:56:25 AM
C	DVSA-ADMIN-GET-ORDERS		$LATEST	Python 3.8	2/9/2023, 3:56:06 AM
C	DVSA-ADMIN-GET-RECEIPT		$LATEST	Python 3.8	2/9/2023, 3:56:07 AM
C	DVSA-ADMIN-UPDATE-INVENTORY		$LATEST	Python 3.8	2/9/2023, 3:56:06 AM
C	DVSA-ADMIN-UPDATE-ORDERS		$LATEST	Python 3.8	2/9/2023, 3:56:06 AM

Figure 1: AWS Lambda functions security findings prioritized by risk score.

Key Solution Features

Contrast's solution maps all the resources within the environment, executes static code scans, and can optionally dynamically instrument AWS Lambda functions.

Rapid deployment.
Connecting the Contrast web console to Microsoft Azure Functions or AWS Lambda accounts is simplified via guided installation and low-touch configuration.

Dynamic environment scanning.
In AWS accounts, instrumented dynamic analysis uncovers all exploitable AWS Lambda functions. Uncover OWASP Top Ten vulnerabilities including injections, cross site scripting (XSS) and local file inclusion (LFI).

Supports latest AWS Lambda services.
Uncover security issues in AWS Step Functions – a service that coordinates multiple Lambda functions into flexible workflows.

Incorporate AWS Inspector static analysis findings with Contrast Serverless results for comprehensive visibility.

AWS account observability.
Improved observability increases security coverage in AWS Lambda accounts by uncovering all serverless account assets including unused/outdated functions (shadow functions).

Resource map.
Automatically discovers and presents a visualized graph of all resources and their relationships within tested environments in a few short minutes per session. This helps security teams quickly identify weak spots and potential risks.

Language support.
Java, .NET, Python, Node.js

For more information about Contrast Serverless Application Security, visit www.contrastsecurity.com/contrast-serverless-application-security.

Code scanning. Automatically executes assessments of relevant code and configurations to discover new vulnerabilities in near real time with context-rich remediation guidance and without manual help. Vulnerability types covered include:

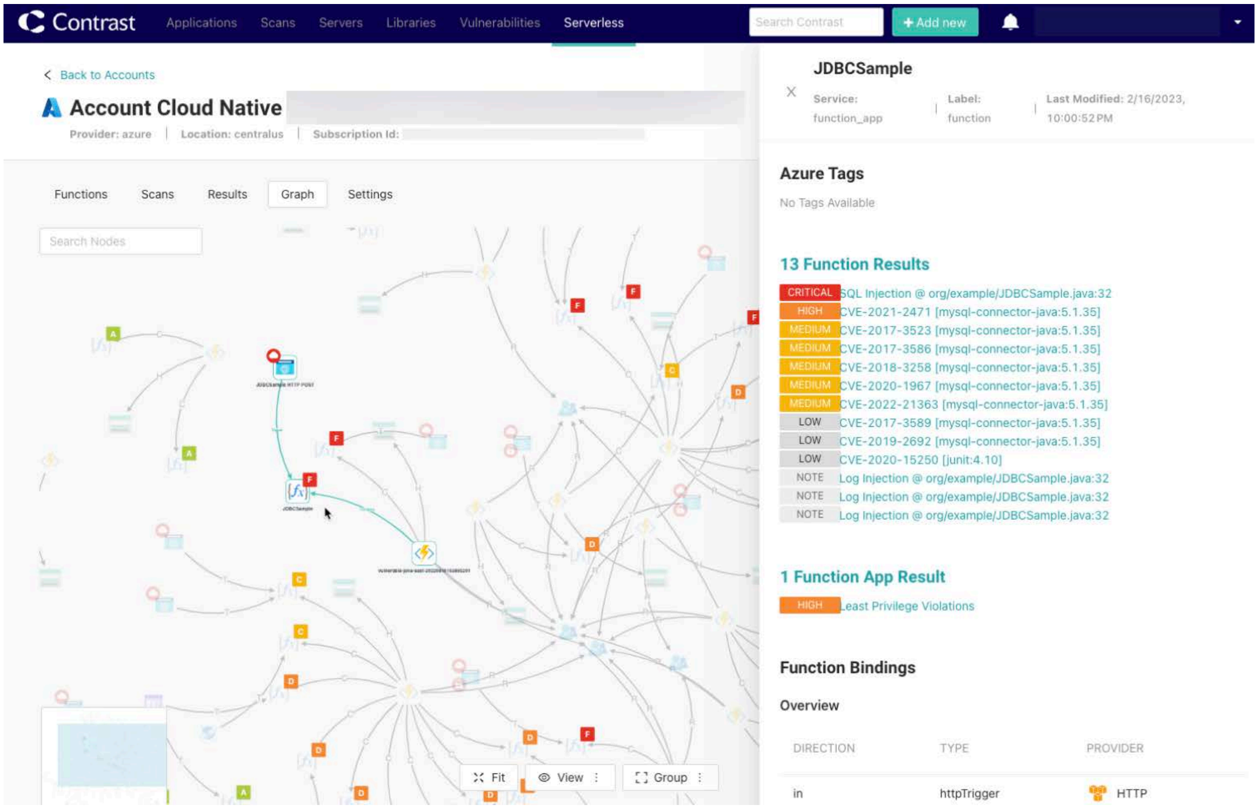
Least privilege. These include identity and access management (IAM) vulnerabilities (over permissive functions) within serverless workload prior to deployment. The solution suggests a tailored least-privilege policy for each Lambda based on its actual needs.

Custom code. The solution finds vulnerabilities in custom code and provides remediation recommendations.

Open-source libraries. The solution provides software composition analysis (SCA) of open-source libraries using Contrast's unique open-source security engine.

Instrumented dynamic analysis (AWS only). Accurately detect exploitable AWS Lambda functions including new services such as AWS Step Functions. When identifying a vulnerability, a real exploit with evidence is provided as well as the potential impact (Lateral Movement/ Blast Radius).

Inspector CVE Integration. Seamless integration with Amazon Inspector CVE reports, boosting contextualization of flagged threats, providing further tailored insights for each specific function vulnerability, allowing AppSec teams to prioritize remediations based on their applicability, and unique potential impact on their particular apps, maximizing the effectiveness of their security efforts.



Account Cloud Native

Provider: azure | Location: centralus | Subscription Id:

JDBCSample

Service: function_app | Label: function | Last Modified: 2/16/2023, 10:00:52 PM

Azure Tags

No Tags Available

13 Function Results

CRITICAL	SQL Injection @ org/example/JDBCSample.java:32
HIGH	CVE-2021-2471 [mysql-connector-java:5.1.35]
MEDIUM	CVE-2017-3523 [mysql-connector-java:5.1.35]
MEDIUM	CVE-2017-3586 [mysql-connector-java:5.1.35]
MEDIUM	CVE-2018-3258 [mysql-connector-java:5.1.35]
MEDIUM	CVE-2020-1967 [mysql-connector-java:5.1.35]
MEDIUM	CVE-2022-21363 [mysql-connector-java:5.1.35]
LOW	CVE-2017-3589 [mysql-connector-java:5.1.35]
LOW	CVE-2019-2692 [mysql-connector-java:5.1.35]
LOW	CVE-2020-15250 [junit:4.10]
NOTE	Log Injection @ org/example/JDBCSample.java:32
NOTE	Log Injection @ org/example/JDBCSample.java:32
NOTE	Log Injection @ org/example/JDBCSample.java:32

1 Function App Result

HIGH	Least Privilege Violations

Function Bindings

Overview

DIRECTION	TYPE	PROVIDER
in	httpTrigger	HTTP

Figure 2: Interactive graph visualization shows relationships between functions and other application components.

Contrast Secures and Accelerates Serverless Development

Contrast Serverless Application Security empowers organizations to unleash the full potential of serverless applications. In doing so, organizations can shift smart by delivering higher-quality applications without delays attempting to use legacy testing tools. Contrast Serverless Application Security seamlessly integrates with native serverless deployment platforms.

For more information about Contrast Serverless Application Security, visit www.contrastsecurity.com/contrast-serverless-application-security.