Contrast Serverless Application Security

The Rise of Serverless is Being Held Back by Security

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.

In addition, serverless architectures lack security visibility due to "no-edge blindness"—functions that have no public-facing endpoint or URL. Abstraction of the infrastructure, network, and virtual machines provides zero context for traditional AST tools to reference, which reduces their accuracy. Deploying traditional AST solutions in serverless environments also tends to take a long time—including complex evaluation and tuning by security experts. Further, non-native testing tools produce a high rate of false positives that must be manually triaged and analyzed before being passed to developers for remediation.

In the place of legacy AST tools, organizations need security testing that is natively designed for the precise demands of serverless development environments—providing the requisite speed, accuracy, and visibility they need into their serverless architectures.

Forrester predicts that 25% of developers will be using serverless technologies by next year. [1]

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. Provides zero false-positive results with vulnerability evidence for true vulnerabilities. Prioritized vulnerability results are based on cloud context and impact. Contextual awareness of issues helps provide developer-friendly remediation support.

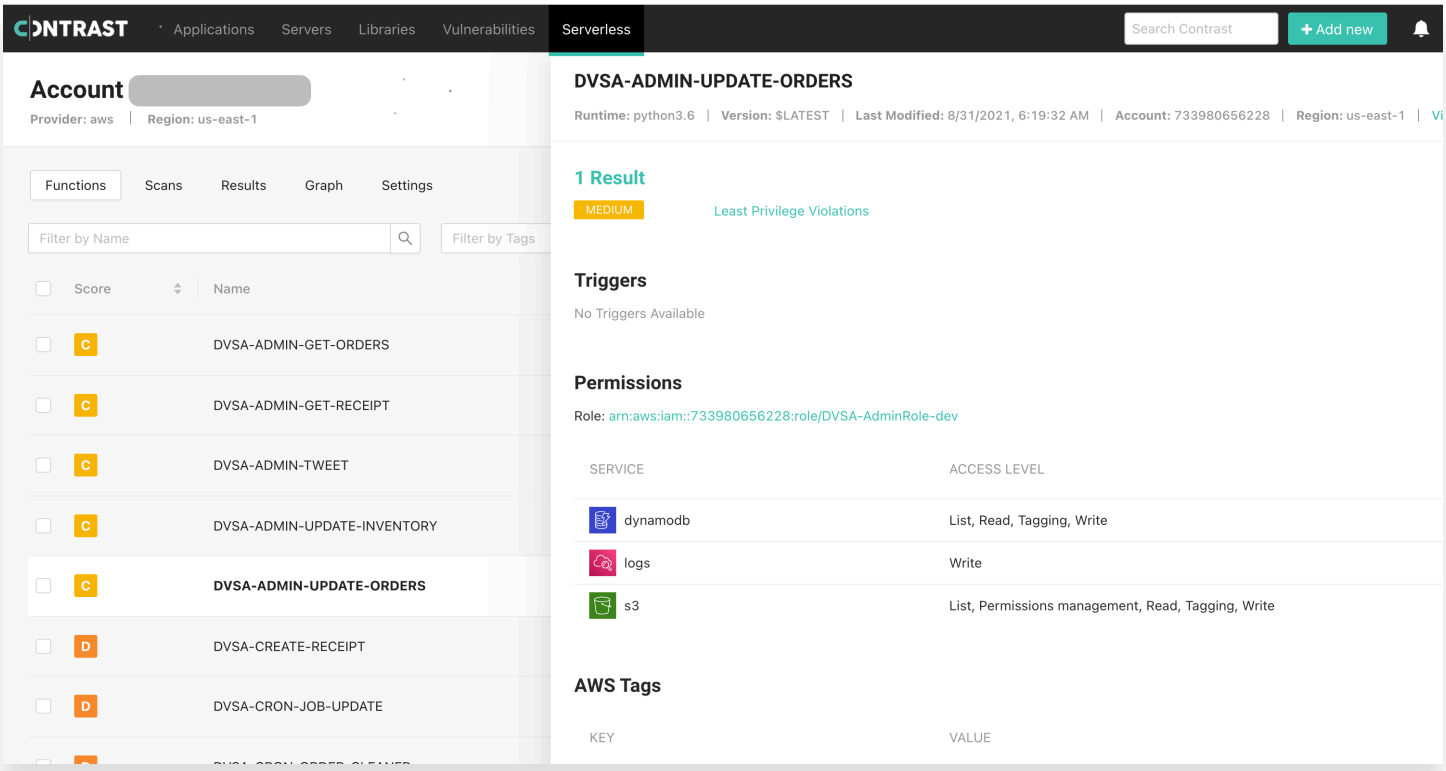

Figure 1: Accurate results, remediation guidance in an easy-to-consume console.

Key Solution Features

Contrast's solution harnesses the power and data of serverless architectures to map all the resources within the environment, execute static code scans, and simulate tailored dynamic attacks. False positives are a large problem with legacy AST tools, with 85% of alerts turning out to be false positives.[2] Contrast Serverless Application Security automatically validates and prioritizes test results with accuracy that eliminates false positives and alert fatigue that plague traditional AST approaches.

Rapid deployment. Contrast Serverless Application Security is deployed as another AWS Lambda function by connecting Contrast TeamServer to the organization's AWS Lambda environment. The solution supports developer-friendly deployment via three-click installation, zero configuration, and automated operations. It takes only a few minutes to get up and running, with immediate full results provided.

Dynamic environment scanning. Automatically initiates tailored, dynamic security assessments based on any specific updates introduced to the tested environment in real time. This greatly improves the ease of pentesting versus legacy manual approaches. Dynamic scans are based on the interpretation of OWASP Top Ten benchmarks that include vulnerabilities such as injections, security misconfiguration, different code failures, and broken access controls.

Resource map. Automatically discovers and presents a visualized graph of all resources (e.g., S3 bucket, API Gateway, DynamoDB) and their relationships within tested environments in a few short minutes per session. This helps security teams quickly identify weak spots and potential risks.

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

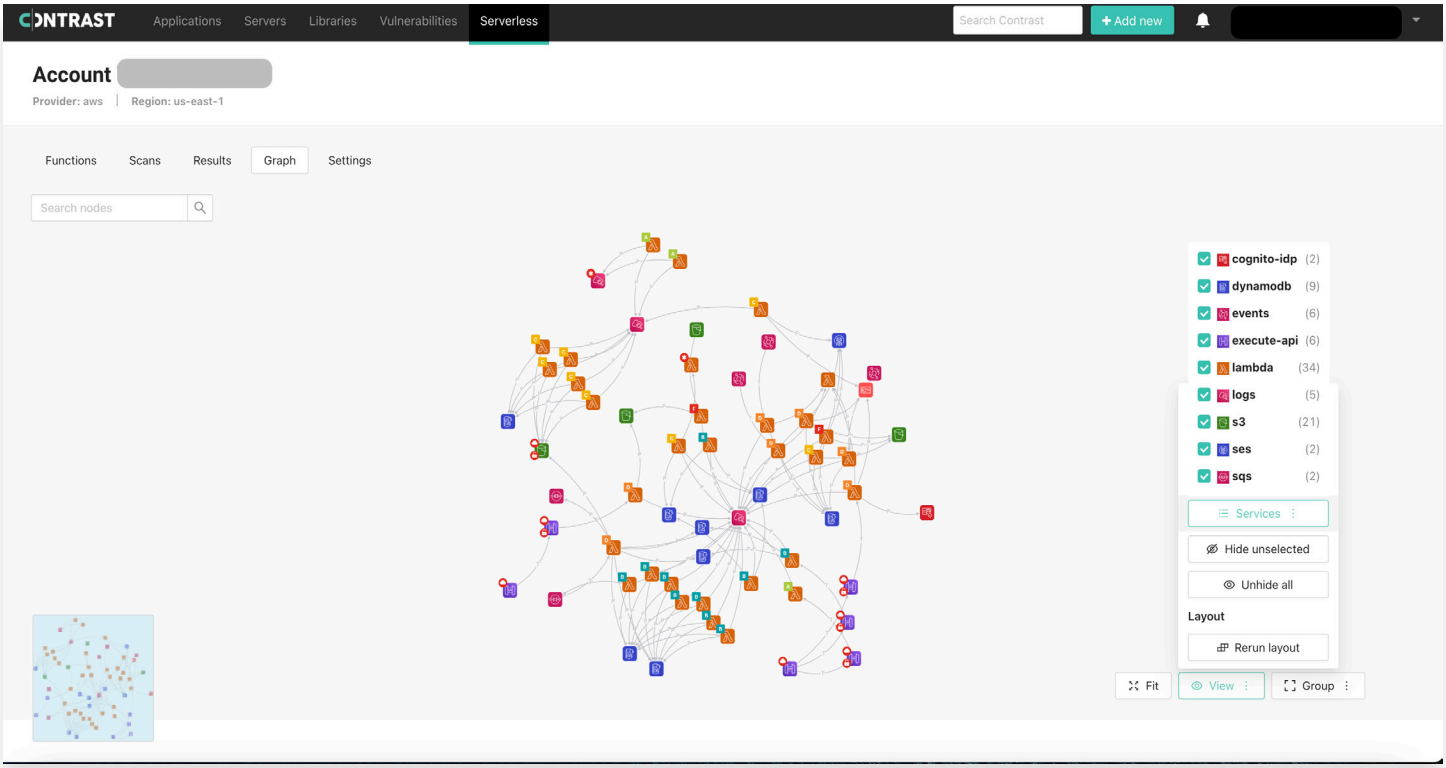

Figure 2: Interactive graph visualization shows relationships between functions and other application components.

Contrast Secures and Accelerates Serverless Development

Contrast Serverless Application Security is a revolutionary approach to AST, empowering organizations to unleash the full potential of serverless applications. In doing so, organizations can shift left by delivering higher-quality applications without delays that come with legacy AST tools. Contrast Serverless Application Security is able to do so due to the fact that it seamlessly integrates within native tools and workflows of serverless deployment platforms.

1 Dave Bartoletti, "Cloud computing will power pandemic recovery in 2021," ZDNet, October 21, 2020.

2 "Digital Transformation Thwarted: When Your AppSec Tools, Scanning, and Resources Become Your Mr. Hyde," Contrast Security, July 2020.