Contrast SECURITY

Quickly and Easily Scale and Secure your Serverless Applications with Contrast Serverless Application Security

Executive overview

Forrester predicts that 25% of developers will be using serverless technologies by next year.[1] The term "serverless" refers to a cloud-native development model that allows developers to build and run applications without having to manage servers. Once deployed, serverless applications respond to demand—automatically scaling up or down as needed. However, security concerns about poorly configured or quickly spun-up cloud-native workloads (serverless or container-based) have also increased nearly 10% over the last year to 46%.[2] Legacy application security approaches are inadequate in their coverage for serverless applications and unable to scale to support the speed and accuracy demanded by them.

As a complement to the Contrast Application Security Platform, Contrast Serverless Application Security automatically detects security vulnerabilities directly within serverless environments—helping developers quickly validate and prioritize test results for remediation. Designed to help developers easily create more secure code, Contrast's solution can be deployed in just minutes. There is no burdensome upfront configuration needed and results are immediate. Contrast's developer-friendly approach to serverless application monitoring includes pipeline-native autonomy and automation. Organizations gain complete security visibility for AWS Lambda functions with near-zero false positives.

The global serverless architecture market will reach a reported $25.49 billion by 2026.[3]

Rapid growth of serverless—but security lags

Organizations are turning to serverless environments to help realize the full potential of DevOps/Agile development. Serverless technologies enable instant scalability, high availability, greater business agility, and improved cost efficiency. According to a recent report, serverless adoption in the enterprise has seen a 209% increase in average weekly invocations over the last 12 months.[4]

While serverless is quickly becoming a preferred approach for helping organizations accelerate the development of new applications, their existing toolsets for application security testing (AST) perpetuate inefficiencies that ultimately bottleneck release cycles. And serverless environments themselves present some advantages when it comes to security. There are also some key differences that create some unique challenges.[5] These include:

- **An expanded attack surface.** Serverless has more points of attack to potentially exploit. Every function, application programming interface (API), and protocol presents a potential attack vector.
- **A porous perimeter is harder to secure.** Serverless applications have more fragmented boundaries.
- **Greater complexity.** Permissions and access issues can be challenging and time-consuming to manage.

Serverless architectures also 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 application security tools to reference. This reduces the accuracy of AST results. And while some tools promote static scans for serverless applications, scanning code with zero context is not a real serverless AST solution.

Deployment of traditional AST solutions for serverless applications typically takes a long time—including complex evaluation and tuning by security experts. Similarly, AST operation depends on manual processes between both security and development teams due to a high rate of false-positive results that must be triaged and analyzed before remediation can begin. These complexities and manual dependencies make it very difficult for application security to scale in lockstep with rapid serverless development processes.

Retrofitting traditional security tools for serverless application testing cannot provide the requisite speed, accuracy, or visibility into serverless architectures. For serverless to succeed and deliver the full value that it promises, organizations require AST tools designed for the particular needs of serverless application development environments.

> Compromised applications remain a primary pathway For successful attacks—representing 39% of all data breaches in the last year.[6]

Purpose-built security for serverless application development

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

This new addition to the Contrast Application Security Platform 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.

Key differentiating values of Contrast Serverless Application Security 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 findings 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 recommendations.

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. It automatically validates and prioritizes test results with accuracy that eliminates false positives and alert fatigue that plague traditional application security approaches—with upwards of 85% of alerts turning out to be false positives.[7]

Specific application security functions include:

- **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.

DEPLOYMENT

While the core Contrast Application Security Platform uses an instrumentation-based agent to embed security with the application code itself, 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.

> According to a study that looked at a cohort of companies that have been using aws lambda since 2019, aws lambda functions were invoked 3.5x more often per day than they were two years prior for companies included in the study.[6]

MANAGEMENT

The "Serverless" tab in Contrast TeamServer includes five different screen views for solution management: Functions, Scans, Results, Graphs, and Settings.

Functions. This screen inventories each of the different AWS Lambda functions that make up the serverless application. The left "score" column shows an assigned letter grade (A to F) that rates relative security based on scan findings together with the likelihood and potential impact. This is achieved through Contrast's context-based engine that not only considers the vulnerability but also how the cloud configuration of the function affects the overall severity. For example, if the function is exposed through an unauthenticated API or a public bucket, there is a higher probability of attack. If the function has access to sensitive services and/or resources, like IAM, this makes the potential blast radius bigger; this, in turn, lowers the score.

Clicking on any individual function listed opens a detailed set of results with specific prioritized scan alerts, any associated service triggers (such as a dependent API), and a list of relevant permissions for that function. It also lists any AWS Tags and a graded Posture Score summary for both the parts and the whole of that specific Lambda function. These details can help developers isolate critical problems that need to be remediated.

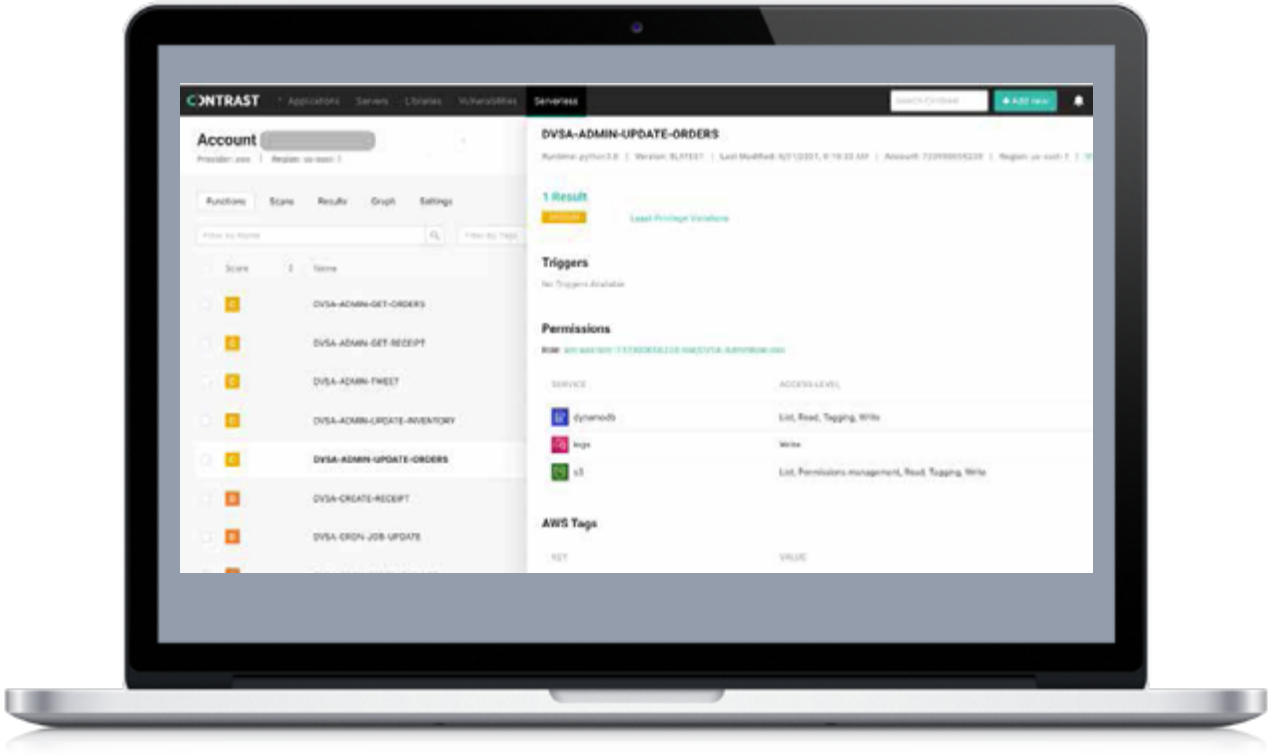

Figure 1: Contrast Serverless "Functions" screen provides detailed per-function summaries.

Scans. This screen provides a historical list of executed scans (including currently running scans) performed on a given application. Each scan contains a list of all scanned resources. After the solution's initial scan establishes a baseline of all the different functions, Contrast Serverless Application Security continuously tracks any changes and additions to the application. This happens automatically as developers write and revise their code—thus eliminating the need to stop and run new scans as things change within the application. Contrast's approach to serverless application security happens seamlessly in the background as an integrated part of the development pipeline.

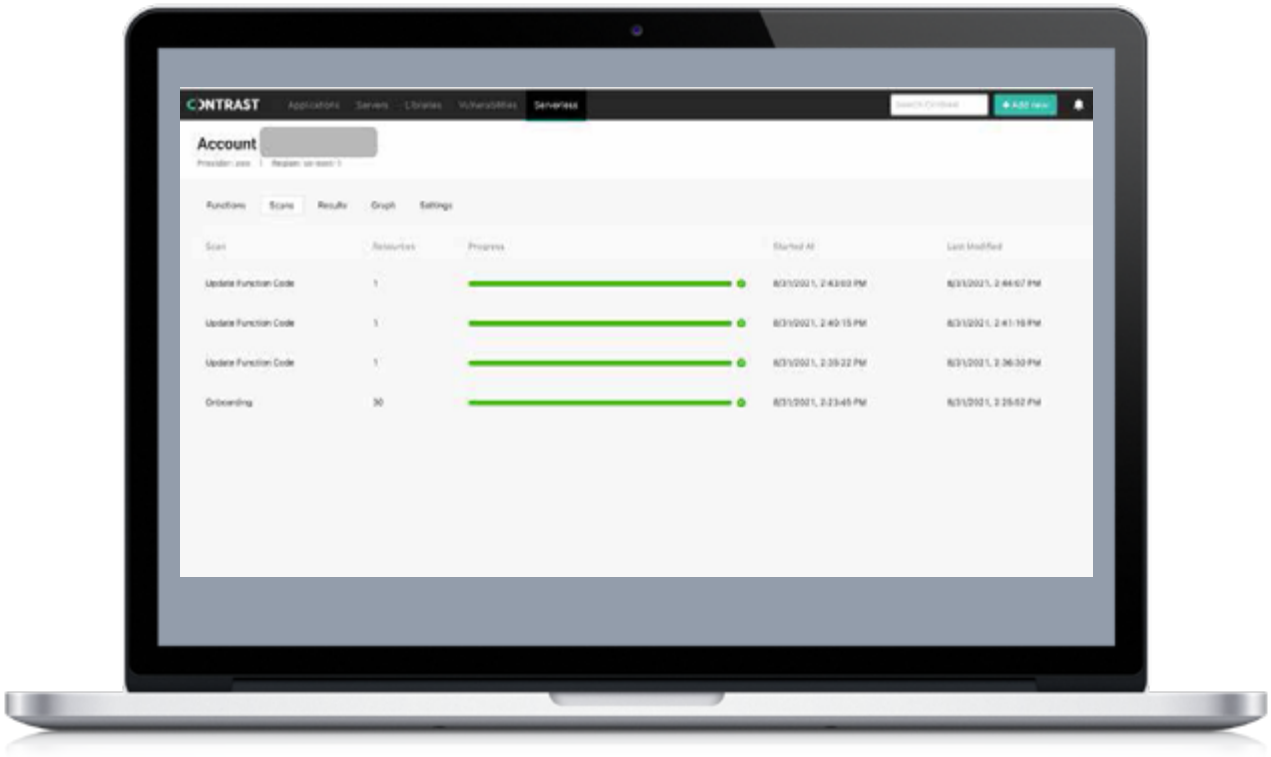

Figure 2: Contrast Serverless "Scans" screen.

Results. This screen provides a list of all the scan alerts for potential problems in the application. The left column assigns a "severity" rating (critical, high, medium, low) to each result. Clicking on an individual result brings up a detailed summary—including a description of the vulnerability or issue, a code-level view of what happened, and (best of all) contextual remediation guidance to help the developer quickly fix the problem. In some cases, Contrast's remediation guidance will even include sample code that makes the repair go even faster. Contrast also automatically tracks other AWS services and functions that will be impacted within the blast radius.

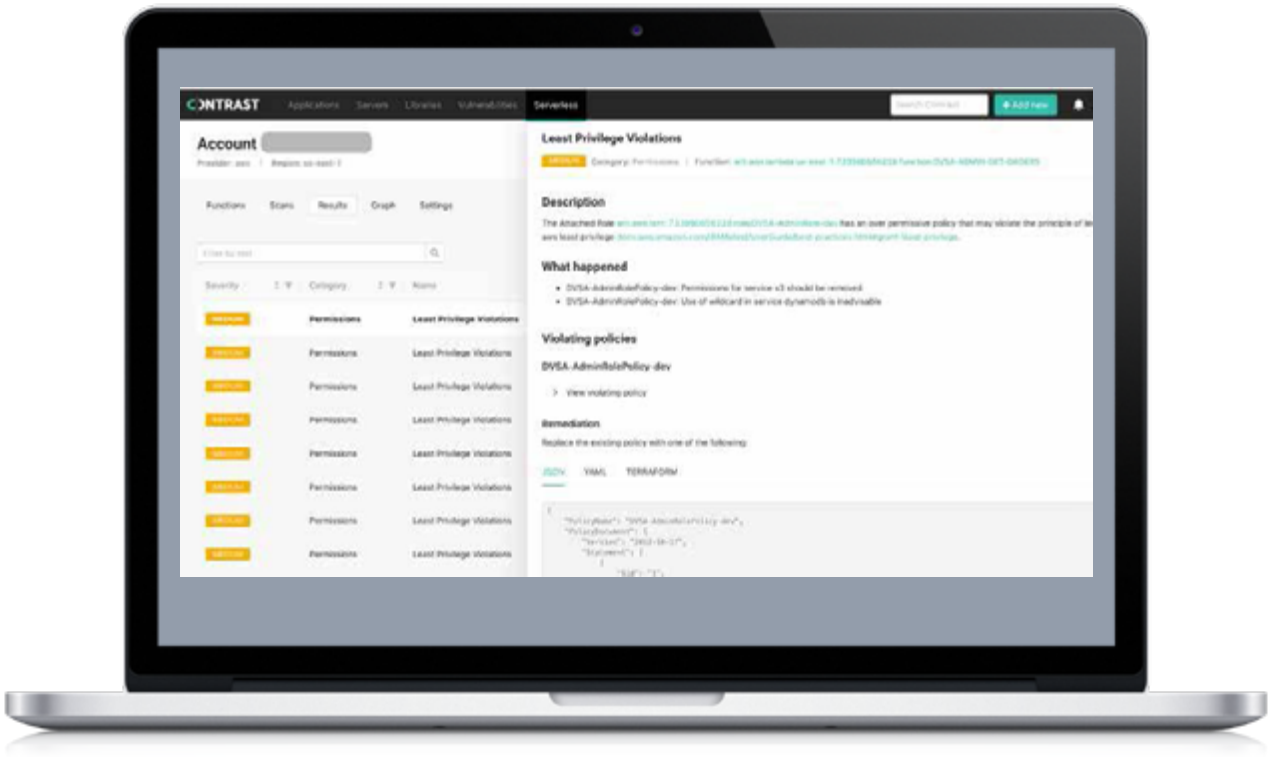

Figure 3: Contrast Serverless "Results" screen with contextual remediation guidance details.

Graphs. This screen visualizes the relationships between functions and resources across the entire application.

Figure 4: Contrast Serverless “Graphs” visualize the relationships between functions and services.

Clicking on a graph element, such as a specific Lambda function, shows its connections and reveals a risk score. This view helps users to understand the blast radius of a potential exploit easily and the associated application elements that may be impacted as a result.

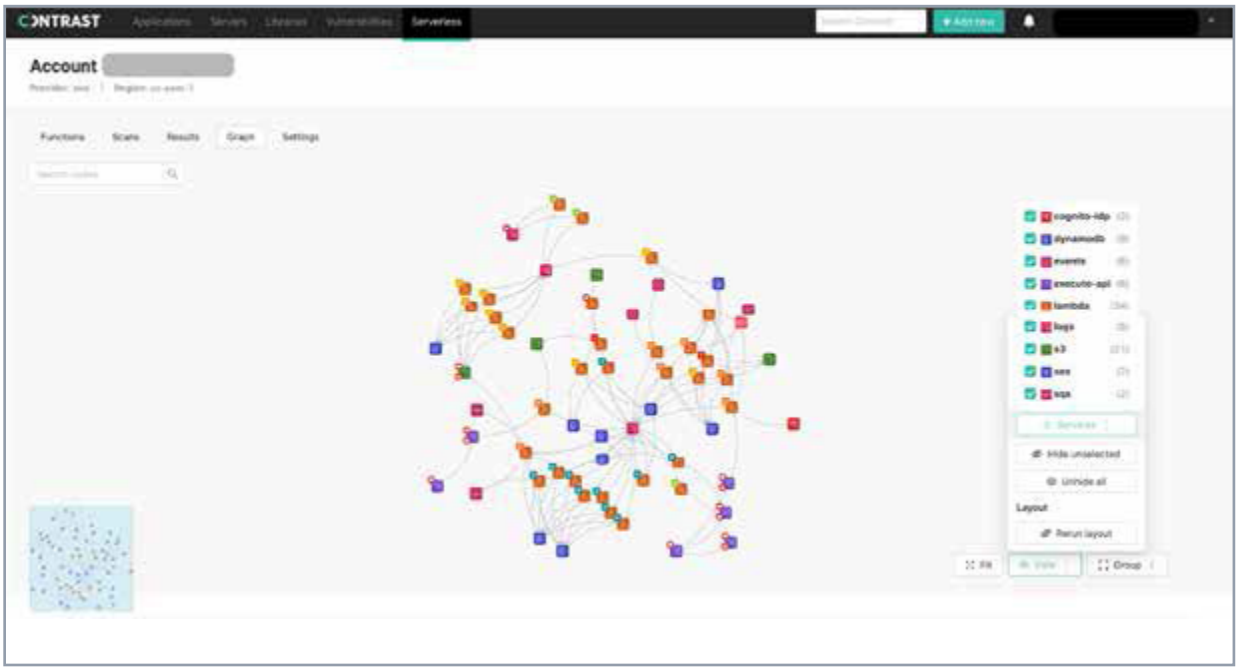

Figure 5: Select or unselect various services to reveal more or less information.

Users can hide and reveal services as well as group and sort them in different ways to customize views that are most meaningful to the organization.

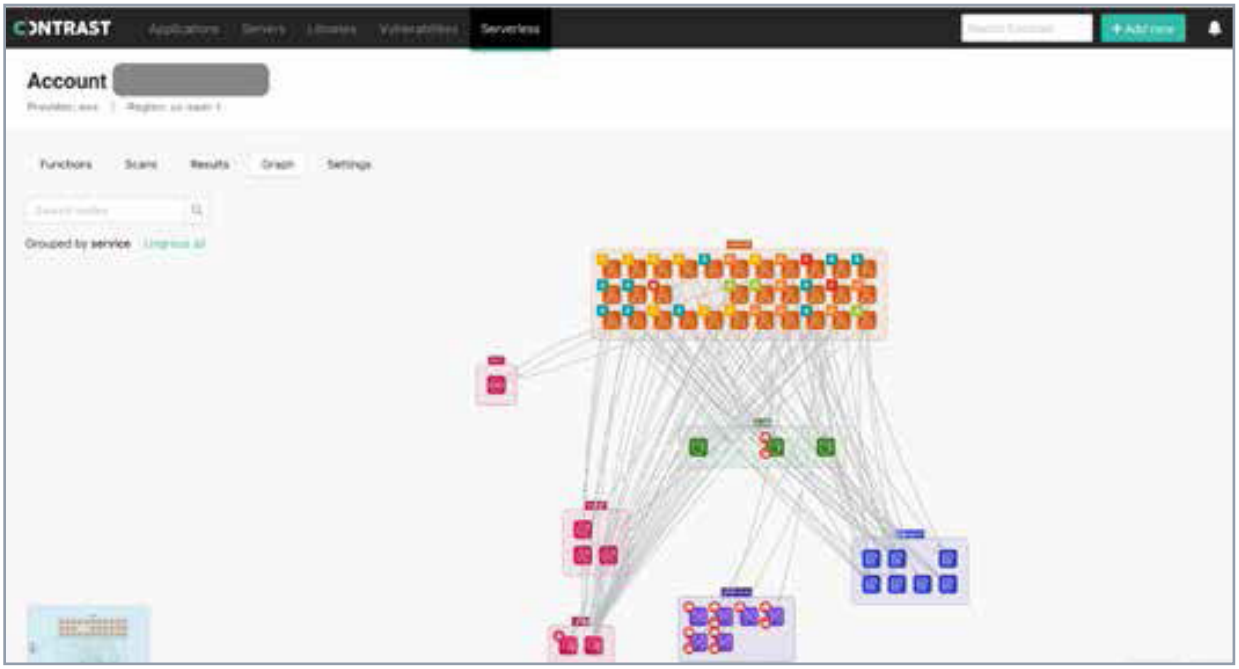

Figure 6: Graph grouping by service.

Settings. After the initial solution setup, users can make customized changes to adjust their inventory and scan controls as needed. For example, a subset of the AWS account can be set up to work with Contrast Serverless Application Security. Additionally, application security teams can also configure which security scans run continuously for every change.

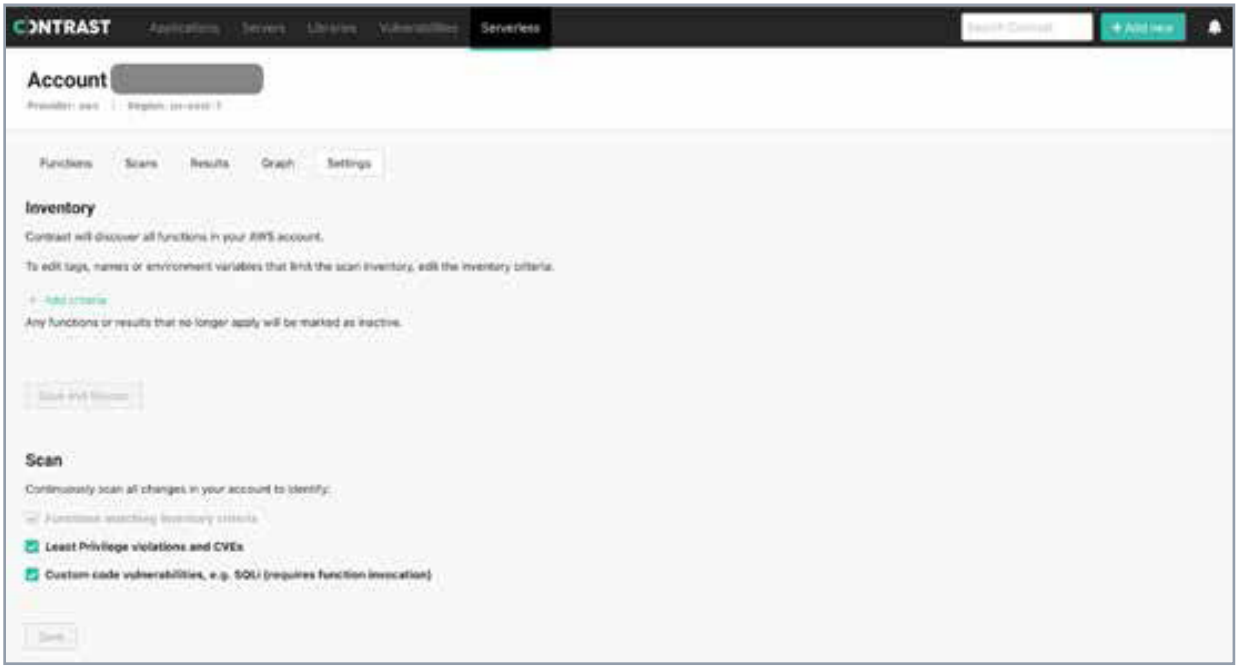

Figure 7: Contrast Serverless “Settings” screen.

Contrast secures and accelerates serverless development

Bringing new applications to market faster is one of the key drivers behind serverless adoption. But development speed at the expense of application security only creates new problems, costs, and delays downstream. It costs much more to fix problems later in the software development life cycle (SDLC) while exposing users to a higher risk of application attacks.

> Fixing a vulnerability gets more expensive as the development process gets further from where the error was introduced.[9]

Contrast's unique solution for serverless AST not only provides accurate scan results, it enables developers to "shift left" by delivering higher-quality applications without delays or bottlenecks. And it does this seamlessly within the native tools and workflows of serverless development platforms.

Contrast SECURITY

[1] Dave Bartoletti, "Cloud computing will power pandemic recovery in 2021," ZDNet, October 21, 2020.
[2] Lawrence E. Hecht, "Misconfiguration Worries Grow," The New Stack, April 29, 2021.
[3] "Serverless Architecture Market Size, Revenue Growth Trends, Company Strategy Analysis, 2020-2026," MarketWatch, August 25, 2021.
[4] "For the Love of Serverless," New Relic, February 14, 2020.
[5] Hillel Solow, "Why Serverless Architectures Are the New Cloud," The New Stack, August 9, 2021.
[6] "2021 Data Breach Investigations Report," Verizon, May 2021.
[7] "Digital Transformation Thwarted: When Your AppSec Tools, Scanning, and Resources Become Your Mr. Hyde," Contrast Security, July 2020.
[8] "The State of Serverless," Datadog, May 2021.
[9] Jeff Williams, "How To Start Decluttering Application Security," Forbes, January 27, 2021.

Contrast SECURITY

Contrast Security provides the industry's most modern and comprehensive Application Security Platform, removing security roadblocks inefficiencies and empowering enterprises to write and release secure application code faster. Embedding code analysis and attack prevention directly into software with instrumentation, the Contrast platform automatically detects vulnerabilities while developers write code, eliminates false positives, and provides context-specific how-to-fix guidance for easy and fast vulnerability remediation. Doing so enables application and development teams to collaborate more effectively and to innovate faster while accelerating digital transformation initiatives. This is why a growing number of the world's largest private and public sector organizations rely on Contrast to secure their applications in development and extend protection in production.

240 3rd Street
2nd Floor
Los Altos, CA 94022
Phone: 888.371.1333
Fax: 650.397.4133

Contrast SECURITY

contrastsecurity.com