

Serverless Function Self-Protection

Security automation & threat prevention at the speed of serverless functions



Serverless Applications Require Dedicated Security

Check Point CloudGuard provides unmatched visibility, security, and control over serverless applications on AWS and Azure, from development through runtime.

Auto Deploy Self-Protecting Functions

CloudGuard automates the entire security lifecycle of Serverless FaaS applications, from development to runtime, with detection and alerts on security issues. During runtime, the agentless Function-Self-Protection (FSP) layer detects and blocks OWASP TOP 10 attacks at the function level, like injection, broken authentication, and sensitive data exposure.

Gain Function Level Granularity Within FunctionApps

CloudGuard is the only solution to provide visibility at the function level. An industry first, CloudGuard allows you to transcend the FunctionApp and where necessary, set controls for individual Azure functions. With the CloudGuard Layer 7 Firewall, set access control rules at the HTTP level as well as at Layer 3/4. Prevent the misuse of serverless functions by setting rules and exclusions for files, processes and network within the scope of the FunctionApp or account.

AUTOMATED SECURITY FROM DEVELOPMENT TO RUNTIME, INCLUDING:

- Function Level Visibility (AWS & Azure)
- Behavior Control
- Third party integration with real-time alerts

KEY PRODUCT BENEFITS

- Zero Trust Security: Including Protection From OWASP Top 10
- Automated by Design: Automatically Minimize Serverless Attack Surface
- **Protection On Any Public Cloud:** Prevent Function Misuse on AWS & Azure

SUPPORT FOR:







Serverless Misconfigurations: Automatic Application Hardening

CloudGuard analyzes your serverless application code before and after deployment, and helps you maximize your application's security posture, minimize the attack surface, and simplify governance. Furthermore, CloudGuard provides a comprehensive, unified view of your entire serverless ecosystem (functions, triggers, third party libraries, etc.) via the intuitive CloudGuard interface. The security focused visualization shows all inputs and triggers along with potential risks.

Minimize Attack Surface

CloudGuard's breakthrough Deep Code Flow Analysis technology detects configuration risks and automatically generates least-privilege function permissions. The solution clearly outlines recommended steps for remediation, enabling you to drive remediation of security posture at scale. In addition, CloudGuard detects and alerts on configuration issues, such as unlinked triggers and over provisioned function timeout configurations. It will continuously scan your functions for known vulnerabilities and embedded secrets ensuring your applications are not exposed to attacks.

Automatically Profile Function & Application Behavior

CloudGuard continuously scans your serverless infrastructure, code, and runtime environment. Utilizing machine based analysis and deep learning algorithms, CloudGuard builds a model of normal application and function behavior, including automatic creation of a white list of actions on a resource level. You can further define custom policies and enforce behavior on a per function level.

Detect & Stop Serverless Application Attacks With Accuracy & Speed

Based on learned function context, CloudGuard provides dynamic protection along with automatic protection from the time of invocation. CloudGuard's Function Self Protection (FSP) detects, alerts, and stops application layer attacks such as the Serverless OWASP Top 10 and anomalous activity independent of the attack trigger.

 Worldwide Headquarters

 5 Ha'Solelim Street, Tel Aviv 67897, Israel | Tel: 972-3-753-4555 | Fax: 972-3-624-1100 | Email: info@checkpoint.com

 U.S. Headquarters

 959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 800-429-4391; 650-628-2000 | Fax: 650-654-4233

 www.checkpoint.com