CloudGuard Serverless Security

Threat Prevention at the Speed of Serverless

SERVERLESS SECURITY

Designed for serverless architectures

Product Benefits

- Detects Attacks & Provides Dynamic Protection
- Automatically Remediate Serverless Misconfigurations
- Minimizes Serverless Attack Surface
- "Shift-Left" with Serverless Security Guardrails for CI/CD

Product Features

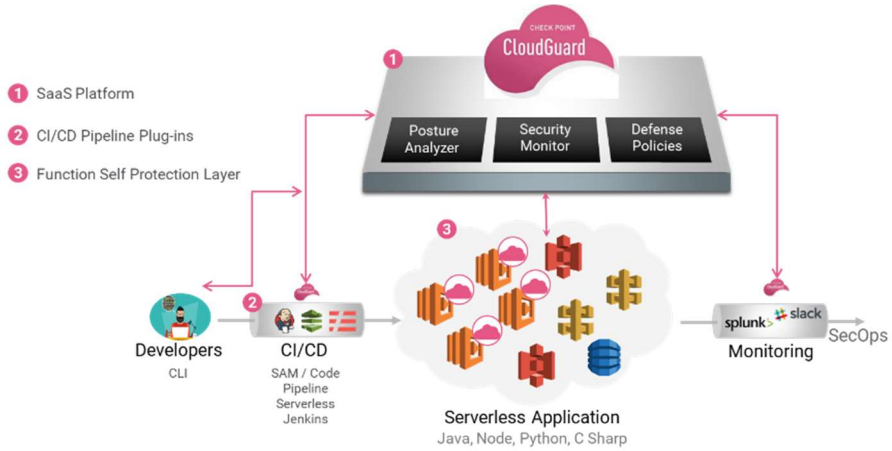
- Automatically generate least privilege IAM roles
- Function Self Protection continuously scans functions for vulnerabilities and potential threats
- Deep Code Flow Analysis for application hardening and least privilege access
- CloudGuard Dome 9 integration for centralized visibility, continuous posture management and integrations alerts
- Third Party integrations with Splunk, Slack, Jira, Amazon CloudWatch, etc. for real-time alerts

INSIGHTS

Serverless applications require a dedicated security approach. Check Point CloudGuard provides unmatched visibility, security, and control over serverless applications from development to runtime.

SOLUTION

Check Point CloudGuard automates the entire security lifecycle of Serverless FaaS applications, from development to runtime. CloudGuard Dome9 detects and alerts on security posture issues, as well as provides corrective remediation prior to deployment – saving developers' time and assuring no vulnerabilities reach the live environment with seamless CI/CD integration. During runtime, CloudGuard Workloads agentless Function-Self-Protection (FSP) layer detects and blocks OWASP TOP 10 attacks at the function level, like injection, broken authentication, excessive permissions, and sensitive data exposure while generating a highly accurate behavioral profile for each function in order to stop anomalies.



PREVENT SERVERLESS MISCONFIGURATIONS - AUTOMATED 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.

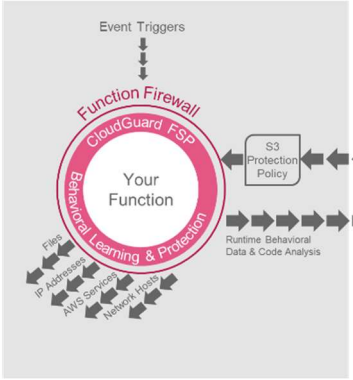
Further, CloudGuard provides a comprehensive, unified view of your entire serverless ecosystem (functions, triggers, third party libraries, etc.) via the intuitive CloudGuard Dome9 interface. The security-focused visualization shows all inputs and triggers along with potential risks.

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.

How Serverless Workload Protection WORKS



AUTOMATICALLY PROFILE FUNCTION AND 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 AND STOP SERVERLESS APPLICATION ATTACKS WITH ACCURACY AND 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.

EXAMPLES OF BLOCKED SERVERLESS ATTACKS WITH CLOUDGUARD

Image of blocked code-injection attack by CloudGuard:

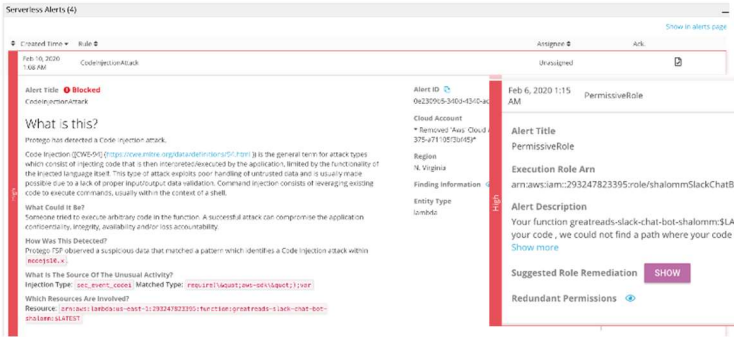


Image of suggested IAM role to remove excessive permissions: