CHECK POINT™

Container Self-Protection

Fully automated protection from CI/CD
through runtime

You Need Security To Outpace DevOps

Cloud native workloads demand cloud native security that understands that dynamic nature of the CI/CD process. CloudGuard automates security from the development stage through runtime, with active threat prevention and continuous code scanning.

Embed Security Into The DevOps Pipeline

Reduce DevOps cycles with early security scanning using CloudGuard's ShiftLeft tool which scans source code, infrastructure-as-a-code, container images and serverless functions.

AUTOMATED SECURITY FROM DEVELOPMENT TO RUNTIME, INCLUDING:

- ShiftLeft Tool
- IAC Scanning
- Automated Runtime Protection

KEY PRODUCT BENEFITS

- **Achieve Zero Trust Security:** Secure containers to achieve zero trust
- **Fully Automated:** Auto-deploy & enforce security controls across every workload with end-to-end context
- **Everywhere:** Security across all clouds and any workloads architecture through the entire application lifecycle

SUPPORT FOR:

Microsoft Azure   aws   kubernetes   docker

Posture Management & Visibility

Understand at a glance what's running in your environment and how it's configured. Visualize K8 data flows and gain visibility of container misconfigurations and anomalies. Build custom compliance rules with intuitive GSL language, and align with NIS & CIS security benchmarks. Gain peace of mind with continuous assessments of cluster & security configurations.

Image Assurance

Ensure security posture without impacting DevOps, with CI tools to scan images in development. Remain secure with continuous runtime scanning to detect newly discovered vulnerabilities. Automatically prevent the deployment of containers which do not meet corporate policy.

Admission Controller

Govern all cluster operations using a central admissions controller. Easily set policies and guardrails for cluster operations using intuitive, human readable policy language. Enforce least privileged access rights and ensure that all images come from trusted sources.

Runtime Protection

Detect and block incidents in real time. Prevent known and unknown attacks with baselining and behavioral signature matching. Ensure container integrity with active threat prevention.

Intrusion Detection

Automatic analysis of all account activity, cluster operations and application traffic flow, in order to continuously detect suspicious behavior.