CloudGuard Spectral - Code

Monitor, classify, and protect your code, assets, and infrastructure for exposed API keys, tokens, credentials, and high-risk security misconfigurations in a simple way, without noise.

CloudGuard Spectral is a developer-centric code security platform that seamlessly monitors, classifies, and protects codes, assets, and infrastructure; simply. With CloudGuard Spectral, organizations can protect against exposed API keys, tokens and credentials, as well as identify and stop security misconfigurations.

CloudGuard Spectral supports more than 500 different stacks and is program language agnostic for the widest range of protection. This allows CloudGuard Spectral to scan code, configuration, binaries, and any other materials in the code base to uncover issues that are often hidden from plain sight. CloudGuard Spectral is able to scan public code hosting platforms (such as Github, Gitlab, etc) to uncover shadow resources and security blindspots, using AI and ML, and allows organizations to identify and resolve issues in their code prior to production.

Best Security From Code To Cloud

Infrastructure as Code (IaC) is a process for configuring and deploying cloud-based infrastructure, and allows organizations to eliminate manual infrastructure configuration through the use of automation, often using tools like CloudFormation and Terraform templates.

This allows infrastructure management and code deployment to become faster and easier.

While IaC simplifies deployment and configuration, it does create new security challenges as the environments are often very complex and expansive, making it difficult to monitor the code for evolving threats. In addition, there are limited IT resources to keep up with the level of diligence needed. To offset these challenges, IaC security solutions look to inspect for configuration and security issues, as well as compliance with company policies and regulatory guidelines. In order to scale this process, automation is a necessity.

Prevent Costly Mistakes

Mitigate secret leaks caused by bad credentials hygiene and human error that can have devastating results.

Integrate with your CI - CloudGuard Spectral integrates with all leading CI systems with built-in support for Jenkins, Azure and others.

Detect as early as a pre-commit - When working with Git, employ our pre-commit, Husky and custom hooks to automate early issue detection.

Install your build systems plugin - Scan during your static builds with native plugins for JAMStack, Webpack, Gatsby, Netlify and more.

Supercharge Your CI/CD

Automate the processes of secret protection at build time. Monitor and detect API keys, tokens, credentials, security misconfiguration and other threats in real time.

Eliminate Public Blindspots

Continuously **uncover and monitor** public deficiencies, supply chain gaps, and proprietary code assets across multiple data sources in a single dev-friendly platform.

Apply & Enforce Your Policies

Seamlessly integrate your own playbooks, build your own detectors, and implement mitigation policies throughout your software development lifecycle.

See What You Can't See

Uncover your organizational blindspots, shadow assets, and supply chain risk in one dashboard, effortlessly.

Monitor out-of-sight assets - Map and monitor hidden sensitive assets such as codebases, logs, and other sensitive intellectual property that belong to your organization, but were left exposed in public facing repositories.

Stay in control- Leverage CloudGuard Spectral's advanced AI backed technology with over 2000 detectors to get extensive coverage, detect issues and keep your organization safe.

Mitigate risks - Maintain balance finding hidden risks and driving organizational change, by using reporting and API to analyze your results.

Developer First Security

CloudGuard Spectral was built from the ground up by developers and for developers. Drive security from your command line, extend and customize.

Scan at record time - We respect your CI so we ensure an average sized repo takes SpectralOps only seconds to scan.

Leverage zero-config - CloudGuard Spectral runs secure by default no special configuration needed. When you need power, it’s available through configuration and extension.

Secure by design - Scan your GitHub, GitLab, Bitbucket, Npm, and more without granting CloudGuard Spectral any permissions of any kind.

Any Stack, Any Language, Anywhere

CloudGuard Spectral scanning technology is programming language agnostic and supports 500+ different stacks

Scan Everything

Scan code, configuration, binaries, or any other material in your codebase. Uncover issues that are visible and hidden from plain sight.

Pinpoint & Resolve

Find and resolve issues in your code and other assets at their exact location and in the correct point in time.

We've Got You Covered

We continuously map developer mistakes, access detail and secret management detection with an ever-growing coverage using AI/ML and our proprietary tech.

Keep Your CI Lightning Fast

Previously building CDNs, we understand low-level file systems, CPU and software optimization and we put it to good use. CloudGuard Spectral scans a typical codebase in seconds.

Scan Your Public Assets

CloudGuard Spectral scans your public Github, Gitlab, Dockerhub, and 30+ other cloud services, and helps you uncover shadow resources and security blindspots.

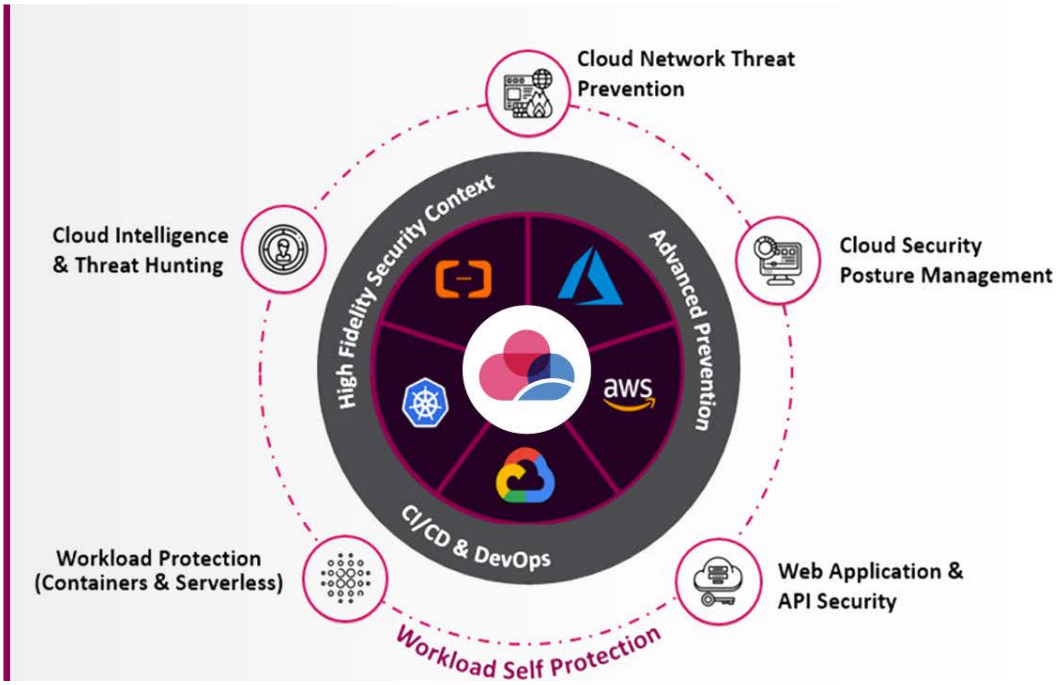
Keep Your Code Private

Your code and data is safe with CloudGuard Spectral. We never copy, send or store any of it. We don't even connect with your Github.

CloudGuard

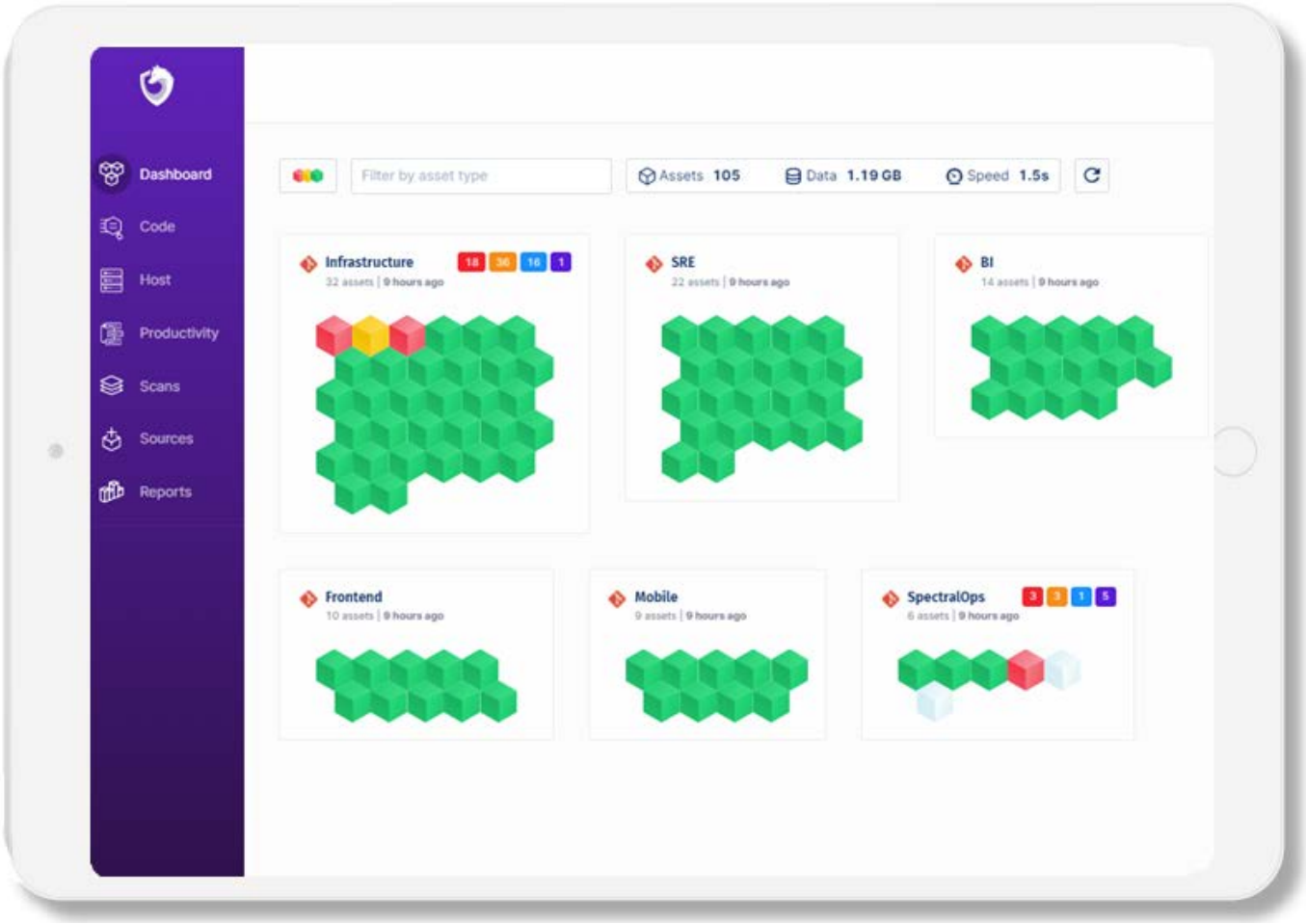
SECURE THE CLOUD

Secure the Cloud with a unified cloud native security platform from code to cloud



IaC USE CASES

IaC CODE SCANNING	Scan code, configuration, binaries, or any other material in your codebase. Uncover issues that are visible and hidden from plain sight
CODE TAMPERING PREVENTION	Easy and safe shift-left provenance, verifying runnable scripts and binaries. Plug your own malware/threat detection
SOURCE CODE LEAKAGE DETECTION	Mitigate secret leaks caused by bad credentials hygiene and human error
SOURCE CONTROL AND CI/CD SECURITY	Ensure a secure development process for a dev team enforced by CI. Harden CI/CD processes by eliminating common mistakes.
HARD CODED SECRET DETECTION	Map & monitor hidden sensitive assets, codebases, logs, and other sensitive intellectual property that was left exposed in public facing repositories.



SUPPORTED ENVIRONMENTS

CLOUD
- Amazon Web Services (AWS)
- Google Cloud Platform (GCP)
- Microsoft Azure

CONTAINERS
- Docker
- Kubernetes

*IaC
- Cloudformation
- Terraform
- Kubernetes
- Dockers
- Microsoft Azure
- GCP

*INCLUDED FREE FOR 90 DAYS

PROTECTION CATEGORIES

SECRETS & MISCONFIGURATIONS
- Passwords
- API Keys
- Tokens
- Credentials
- PCI
- PII
- PHI

OWASP TOP 10
- A2:2017 - Broken Authentication
- A3:2017 - Sensetive Data Exposure
- A5:2017 - Broken Access Control
- A6:2017 - Security Misconfiguration

DESCRIPTION	SKU
CloudGuard Spectral scans your code for security risks such as secrets, keys and misconfigurations. 100 Developers for 1 year	CP-CGSP-CNT-100-1Y
CloudGuard Spectral scans your code for security risks such as secrets, keys and misconfigurations. 25 Developers for 1 year	CP-CGSP-CNT-25-1Y
CloudGuard Spectral scans your code for security risks such as secrets, keys and misconfigurations. 100 Developers for 2 year	CP-CGSP-CNT-100-2Y
CloudGuard Spectral scans your code for security risks such as secrets, keys and misconfigurations. 25 Developers for 2 year	CP-CGSP-CNT-25-2Y
CloudGuard Spectral scans your code for security risks such as secrets, keys and misconfigurations. 100 Developers for 3 year	CP-CGSP-CNT-100-3Y
CloudGuard Spectral scans your code for security risks such as secrets, keys and misconfigurations. 25 Developers for 3 year	CP-CGSP-CNT-25-3Y

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