YOU DESERVE THE BEST SECURITY

CNAPP:

THE EVOLUTION OF CLOUD-NATIVE RISK REDUCTION

Table of Contents

CloudGuard
CNAPP

Introduction

When it comes to application protection, you have so much data coming in, from telemetry, monitoring, and a range of other data sources. But data alone isn't always enough.

More and more, the main problem isn't extracting data from your applications; it's creating context, breaking down silos, and establishing 100% visibility so you can make the right decisions.

Today, you're not only dealing with faster release cycles than ever before, plus ongoing demand for new features. Economic and business challenges mean that you have to do more work with less. You're also doing your best to steer clear of emerging software supply chain threats. That means you need to eliminate complexity, save resources, and choose tools that let your teams focus on what matters most.

To secure your applications, you need deeper visibility into your entire threat landscape—end to end across applications, APIs, serverless functions, containers, VMs, public cloud assets, and software development pipelines.

So how do you achieve the kind of coverage that lets you leverage enhanced context to gain unexpected insights into some of the biggest security headaches out there, like identity management, workload protection, and code vulnerabilities?

CloudGuard's CNAPP solution gives you enhanced context so you can achieve more secure cloud-native development with less time and effort. Because beyond total holistic coverage at every point in your stack and software development lifecycle (SDLC), only CloudGuard offers effective risk management (ERM), which brings all your security tools together and helps you focus on the alerts that matter.

And that lets your security team take control quickly and easily, with no gaps.

This document is intended to introduce CNAPP, focusing on four advanced capabilities recently introduced by Check Point to provide cloud customers with more context and actionable security for smarter prevention.

Read on to find out what makes Check Point's CloudGuard the most effective CNAPP solution today.

What Goes into a CNAPP Platform?

One of the prime directives of software development is to ensure that your app is secure. The goal of cloud security teams is to secure the entire cloud-native application lifecycle, ensuring high software quality while helping you protect your reputation and avoid fines, data breaches, and other serious negative consequences of vulnerabilities, threats, and secrets in your application.

On top of this, cloud-native development teams are already facing a wide range of unique challenges every single day:

- Large teams in distributed locations
- Massive number of assets, also distributed
- Wider-than-ever range of application types
- Faster-than-ever pace of change
- Supply-chain risk, which has increased with the popularity of open-source

But the need for security and the complexity of today's apps can't bring your organization to a standstill while security teams chase after low-priority alerts and false positives, race to meet compliance regulations, or worse, rush to handle a breach.

Today, your application security products need to evolve to provide actionable insights, which has led to the development of the Cloud-Native Application Protection Platform (CNAPP). First coined by Gartner, the term CNAPP refers to "an integrated set of security and compliance capabilities designed to help secure and protect cloud-native applications across development and production."

A good way to understand CNAPP is by understanding the potential threats in each stage of the SDLC, alongside the CNAPP capabilities that protect organizations. See Figure 1 below.

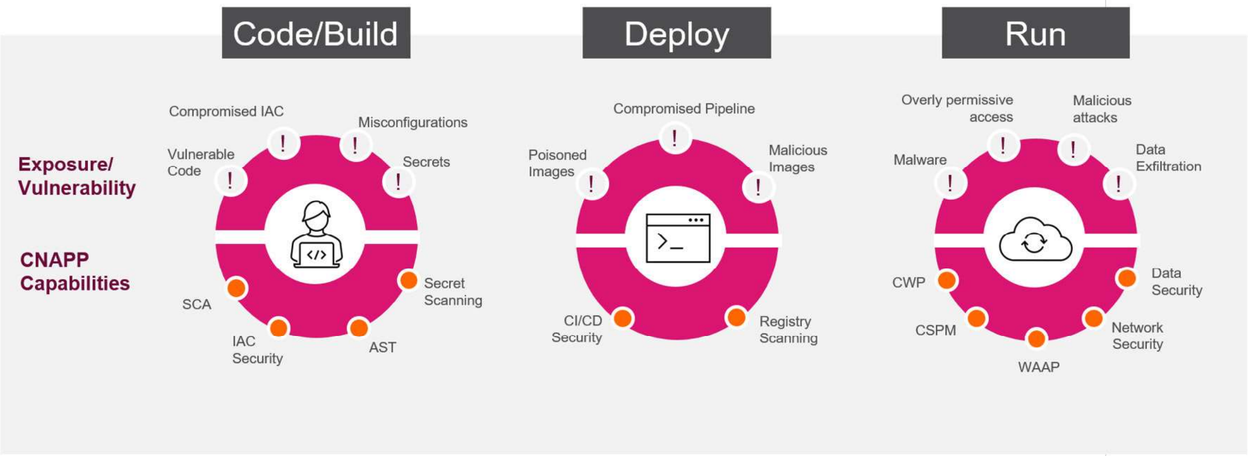


Figure 1: CNAPP capabilities to address relevant cloud threats for each SDLC stage

This is the evolution of application protection. In fact, the very name CNAPP points to the reasons why older tools have become more and more impractical over time:

- **CN = Cloud-native:** Because cloud apps are built for the cloud vendor's native services rather than “lifted-and-shifted,” meaning they also need purpose-built tools

- **AP = Application protection:** Because regular security solutions can't protect your development environment

Cloud can scale exponentially in an instant, driving up the complexity of management overhead. So the only effective security solution is one that's native to the cloud, just like your apps.

Which brings us to the final and most important letter:

- **P = Platform**

Why is that so important?

If you pull back the curtain, you'll discover that most companies are piecing their application security together from a variety of sources, often using “point solutions.” These are individual pieces of software, each of which aim to address a single use case or challenge. And this means more alerts, more dashboards, more need for integration effort, and more room for things to go wrong or fall through the cracks.

So what components should you look for in a CNAPP? At a minimum, you'll want to ensure that you're getting the following:

- **Cloud security posture management (CSPM).** Helps you detect misconfigurations and compliance issues

- **Cloud service network security (CSNS).** Provides optimal network security for the data (traffic) plane; enables network segmentation to secure the dynamic network perimeter

- **Cloud workload protection (CWP)** and **static application security testing (SAST).** Checks source code for vulnerabilities, hardening against security misconfigurations, secret management best practices, and active compromises in cloud workloads (VMs, containers, including Kubernetes, or serverless functions)

- **Cloud infrastructure entitlements management (CIEM)** and **identity and access management (IAM).** Ensures optimal permission configuration of your cloud environment and enforces least privilege

- **Intelligence & threat hunting.** Uses machine learning visualization to provide real-time detection (with context) of threats and anomalies across your cloud environment

- **Developer security tools.** Integrates with your existing development stack to help inculcate a shift-left and least-privilege mindset, including scanning of infrastructure-as-code (IaC) and third-party libraries

But all of these components providing telemetry and intelligence from different sources simply add to data overload—unless you have a way to blend them together, analyzing and extracting the most valuable insights.

Advanced CNAPP Capabilities

Only Check Point gives you a single holistic platform with increased security context and rich functionality backed by Check Point's decades of security experience.

In addition, CloudGuard's CNAPP is designed to work seamlessly with the leading cloud platforms, and includes out-the-box integrations with popular cloud services like AWS Security Hub, Microsoft Defender for Cloud, Google Eventarc, as well as leading third-party solutions like ServiceNow, Splunk and Tenable.

CloudGuard has evolved along with today's best-in-breed software development tools to provide all this and more, giving you deep security intelligence for workloads and users.

CloudGuard's CNAPP solution goes where point solutions can't. Let's take a deep dive into three of CloudGuard's capabilities that not only boost your insights but also make remediation simpler.

Cloud Infrastructure Entitlement Management (CIEM) – Right-Sized Permissions

You've been hearing for years that in the cloud, there's no perimeter, so permissions are more important than ever. But it doesn't end there.

Beyond ordinary users, we're also dealing with ephemeral entities like workloads (including those developed with containers or serverless functions) that spin up and down on demand. Then there are hardworking DevOps teams who sometimes assign excessive entitlements in a bid to remain agile.

How do you know at a glance what access level they all have? How do you know when there are excessive permissions in such a complex environment?

Clearly, old ways of managing access are out of date, struggling to drill down through all those entities and layers of permissions.

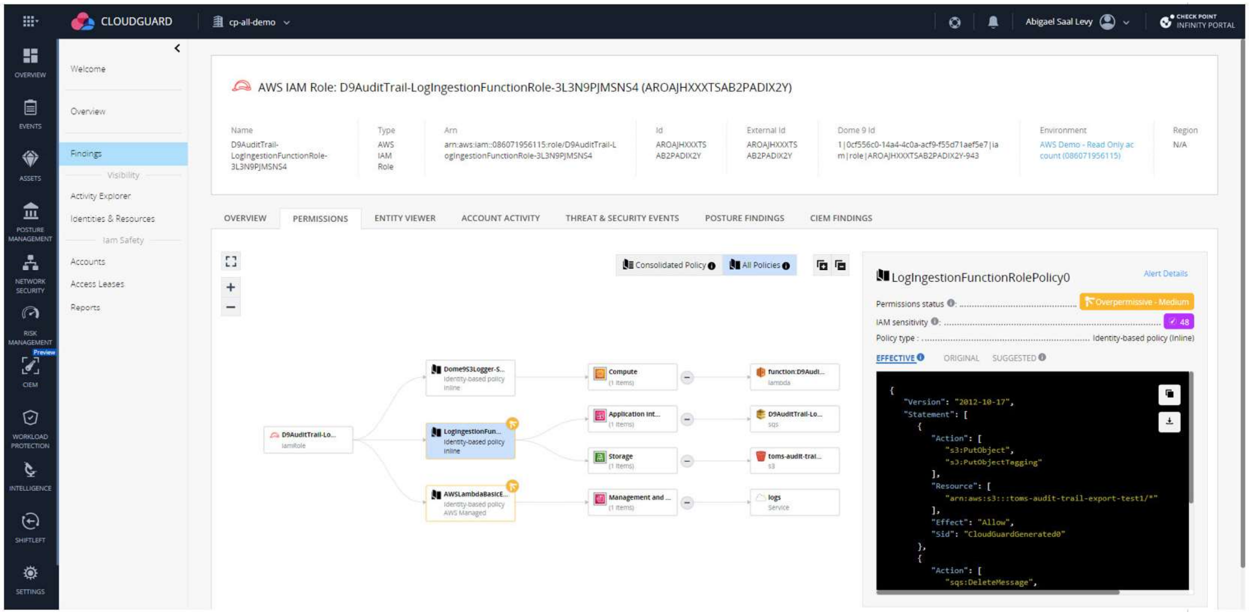
Some security teams manually configure permissions, relying on a lot of guesswork and hoping that the assigned permissions will be "good enough" for the application. Others trust already-configured developer settings so as not to interfere with functionality. Either way, this is a lot of work and leaves you without much insight into effective permissions. If you can't tell which cloud identities have control of your assets, you've just opened a whole new door to attacks.

We've all heard "enforce least privilege" or "implement zero trust," but how are you supposed to actually get it done?

CloudGuard CIEM (see Figure 2 below) makes it simple, flagging overly permissive entitlements and suggesting remediation steps.

Use case example:

When a software developer grants unnecessary permissions to non-human identities so their code can run quickly, CIEM will alert you about over-privileged access rights and automatically provide a fix to help you avoid a costly data breach.



AWS IAM Role: D9AuditTrail-LogIngestionFunctionRole-3L3N9PJMSNS4 (AROAJHXXXTSAB2PADIX2Y)

Name	Type	Arn	Id	External Id	Dome 9 Id	Environment	Region
D9AuditTrail-LogIngestionFunctionRole-3L3N9PJMSNS4	AWS IAM Role	arn:aws:iam::086071956115:role/D9AuditTrail-LogIngestionFunctionRole-3L3N9PJMSNS4	AROAJHXXXTSAB2PADIX2Y	AROAJHXXXTSAB2PADIX2Y	1|0cf556c0-14a4-4c0a-acf9-f55d71aef5e7|iam|role|AROAJHXXXTSAB2PADIX2Y-943	AWS Demo - Read Only account (086071956115)	N/A

LogIngestionFunctionRolePolicy0

Permissions status: Overpermissive - Medium

IAM sensitivity: 48

Policy type : Identity-based policy (Inline)

```
{
   "Version": "2012-10-17",
   "Statement": [
     {
       "Action": [
          "s3:PutObject",
          "s3:PutObjectTagging"
       ],
       "Resource": [
          "arn:aws:s3:::toms-audit-trail-export-test1/*"
       ],
       "Effect": "Allow",
       "Sid": "CloudGuardGenerated0"
     },
     {
       "Action": [
          "sqs:DeleteMessage",
```

Figure 2: CloudGuard Cloud Infrastructure Entitlement Management helps you right-size permissions

Here's how it works:

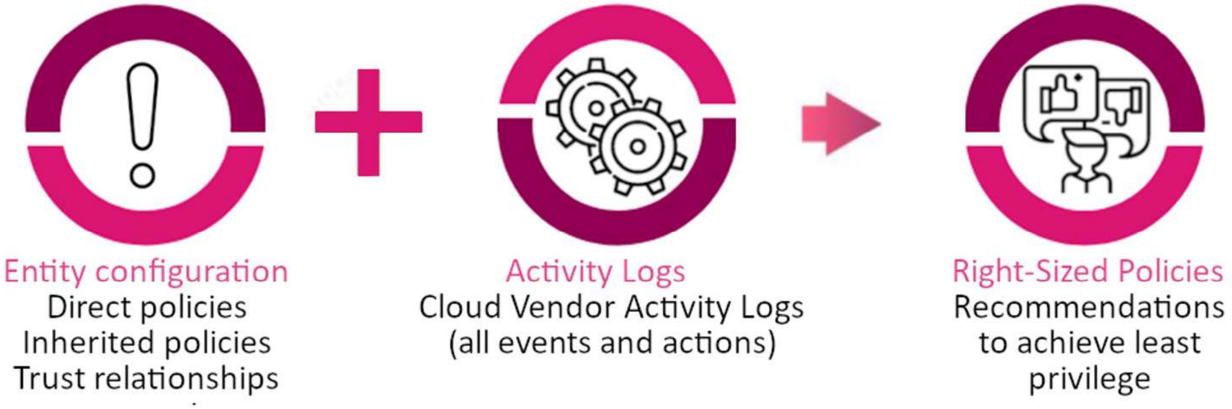


Figure 3: How CloudGuard CIEM combines configuration with usage data to help you enforce least privilege

CloudGuard's CNAPP with CIEM improves your cloud security posture in 3 simple steps:

1. It examines entity configuration and policies, not only directly affecting an entity but also inherited privileges and those based on trust relationships.
2. It assesses activity logs from all your cloud vendors to determine what type of events the entity triggers in a given period (up to 90 days, but CIEM is often able to provide suggestions much earlier).
3. Finally, by comparing permissions granted and actually used, it alerts you about over-permissioned entities, offering you quick-fix policy changes that you can paste in place to ensure compliance with the principle of least privilege.

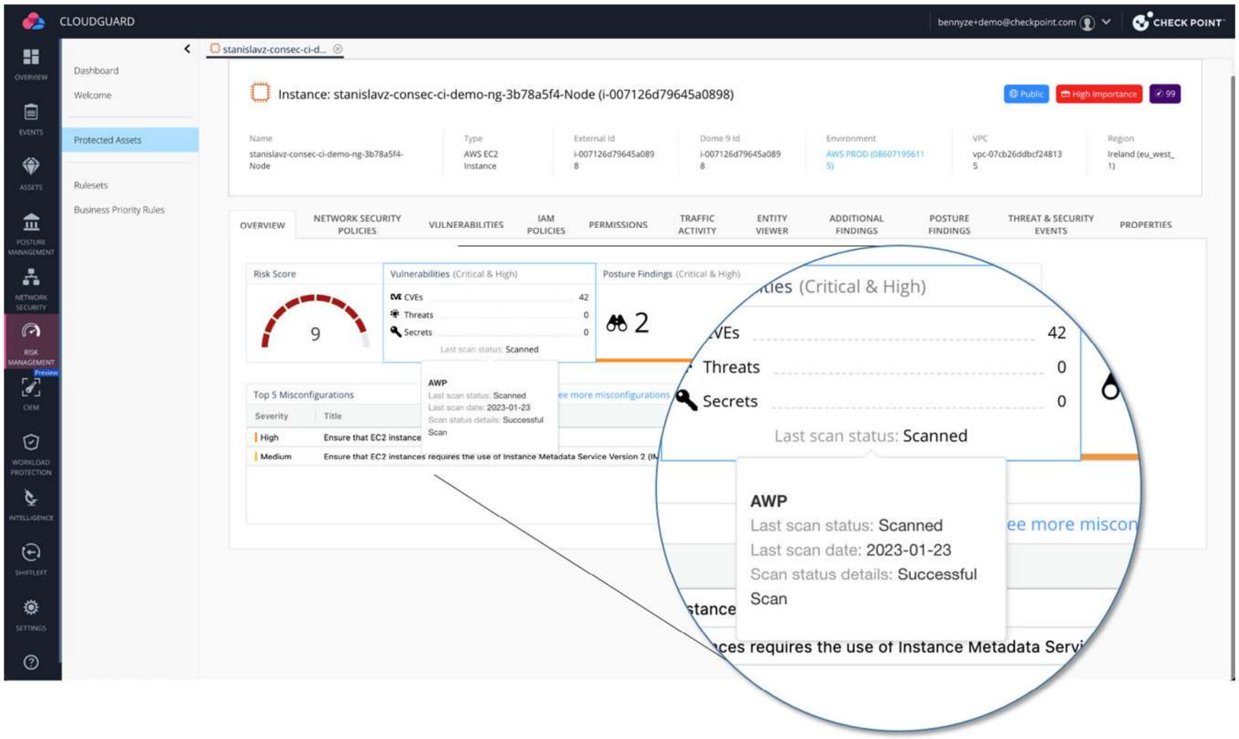
CloudGuard CIEM makes sense of identity risk and provides simplified remediation. That lets you enforce least privilege and eliminate over-permissioning, with automatic oversight and enforcement, eliminating the need to manually find and remove dormant identities and making it easy for your organization to adopt IAM best practices.

Plus, CloudGuard CIEM analyzes permission paths to give you full visibility into entitlements, with a high level of automation to enable greater efficiency from security teams. All without impacting functionality or the pace of development.

Agentless Workload Posture (AWP) – Deeper Visibility, Less Friction

How many times have you heard the phrase “You can’t protect what you can't see”?

But adding agents to workloads to make this visibility possible creates a lot of work for developers, creating friction between security and dev teams and slowing them down. You don’t want to inhibit innovation, but you do need to increase acceptance of security within your dev team.



Instance: stanislavz-consec-ci-demo-ng-3b78a5f4-Node (i-007126d79645a0898)

Name	Type	External Id	Dome 9 Id	Environment	VPC	Region
stanislavz-consec-ci-demo-ng-3b78a5f4-Node	AWS EC2 Instance	i-007126d79645a0898	i-007126d79645a0898	AWS PROD (086071956115)	vpc-07cb26ddbcf248135	Ireland (eu_west_1)

Vulnerabilities (Critical & High)

CVEs	42
Threats	0
Secrets	0

Last scan status: Scanned

AWP
Last scan status: Scanned
Last scan date: 2023-01-23
Scan status details: Successful Scan

Top 5 Misconfigurations

Severity	Title
High	Ensure that EC2 instance
Medium	Ensure that EC2 instances requires the use of Instance Metadata Service Version 2 (IM

Figure 4: CloudGuard gives you deep workload security visibility without the need for software agents

CloudGuard’s AWP provides cloud workload protection (CWP) at the instance level, making security an integral part of your entire SDLC without the need for agents and with no added time or effort.

Use case example:

You are in the cloud security team of a university that needs visibility into various VMs and workloads, but is not in control of what actually runs in the VMs. Faculty, data scientists and students are doing research inside of their cloud environments, but you don’t really know what packages they’re installing and those packages can change from day to day. AWP can give you a baseline every 24 hours and allow you to monitor the security of their machines without having to worry about an agent that needs to be installed or updated.

Here’s how it works:

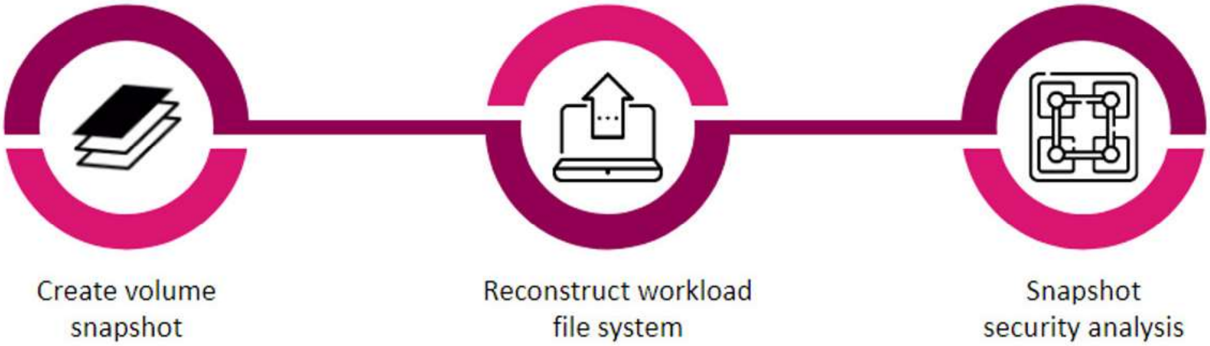


Figure 5: How CloudGuard AWP keeps your workloads secure without impacting performance

With its scanning-as-a-service model, there's nothing to install, and the onboarding process is simple to perform e.g. via an AWS CloudFormation Template (CFT). Onboarding covers your entire environment, meaning your entire cloud account, rather than per virtual machine.

Once you've onboarded CloudGuard AWP, it gets to work in 3 simple steps:

1. It creates a snapshot of the running workload volume and encrypts it; AWP does this every 24 hours. Note also that snapshots remain encrypted throughout the process and are promptly deleted after scanning is completed.
2. It attaches the snapshot to a virtual machine instance and reconstructs the workload's file system, operating system, applications, and data in a read-only view.
3. Lastly, AWP performs security analysis using scanner tools on the offline snapshot rather than in production to ensure zero impact on service and performance.

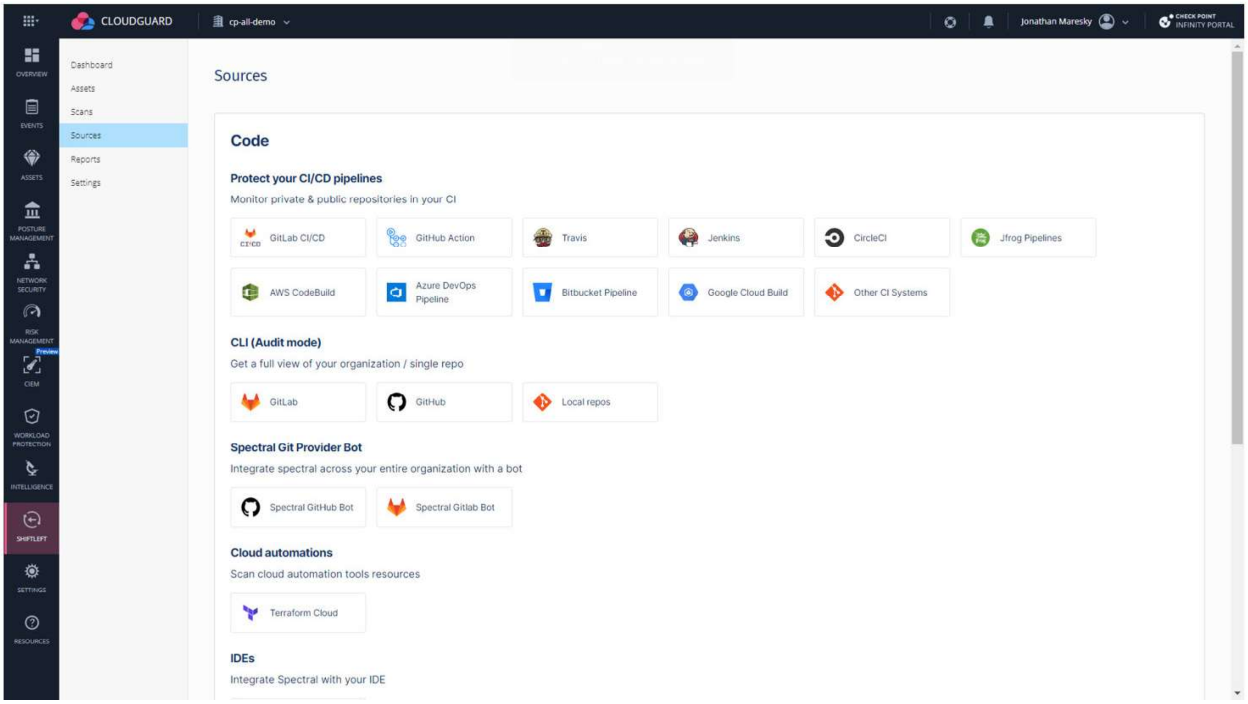
CloudGuard AWP assesses all packages installed for known vulnerabilities; it also searches for secrets, such as exposed credentials, using Check Point's proprietary algorithms. This approach makes AWP completely developer-friendly. Because it works on a snapshot of your volumes, it will never interfere with running workloads. So your developers don't even need to know it's there, working in the background.

While most users will want to use CloudGuard AWP through its simple SaaS model, if sensitive workloads and data protection are a concern, Check Point does offer the option to run it within your own environment.

With CloudGuard AWP, there is nothing to install on each workload (after onboarding), and you gain complete visibility into vulnerabilities, exposed credentials, malware, OS-level compliance, intrusion detection, and file integrity. Operational efficiency is improved for both teams: developers can get back to work while your security team can rest assured that you're covered.

Pipeline Security – Building Transparency Across the SDLC

The software development process has been completely transformed in recent years. Today's cloud-native applications are rarely hand-coded line by line. Instead, they're assembled from a wide range of resources found in open-source repositories, services, libraries, and APIs. This transformation has made development faster, but it also leaves you vulnerable to weaknesses in any components your applications may be using from anywhere in the software supply chain.



Sources

Code

Protect your CI/CD pipelines

Monitor private & public repositories in your CI

CLI (Audit mode)

Get a full view of your organization / single repo

Spectral Git Provider Bot

Integrate spectral across your entire organization with a bot

Cloud automations

Scan cloud automation tools resources

IDEs

Integrate Spectral with your IDE

Figure 6: CloudGuard lets developers scan source code and IaC quickly and efficiently

Pipeline Security (see Figure 6 above) is a simple, lightning-fast, and efficient way to enable you to build secure applications while making sure vulnerabilities are fixed early in the pipeline. It combines secret scanning, software composition analysis for open-source vulnerabilities, and infrastructure-as-code (IaC) scanning to ensure that vulnerabilities won't make it into your production and runtime environments:

- Frictionless development with end-to-end application protection from code to cloud
- Peace of mind thanks to simplified routine scans of code and repositories and uniform policy enforcement
- Developer-first approach with automated detection of hard-coded secrets, malware, and vulnerabilities detection throughout the SDLC
- Tighter security through identification and elimination of blind spots and supply chain risks
- Applies all CloudGuard security policies from the very beginning of the SDLC, ensuring faster time to remediation

Pipeline Security was created with developers in mind, so—as with the entire CloudGuard CNAPP suite—its focus is on letting them do their job. It integrates quickly and scans entirely in memory, ensuring that no data is sent to the backend to help you comply with data security standards.

Use case example:

API keys and tokens are used to access data and resources from another application or service. They are typically used to connect two applications to share data. If an attacker is able to steal an API key or a token, they can gain access to the data and resources that key is meant to protect. Pipeline Security is able to detect an API key or token that was left by a developer by mistake in their code or repository.

Here's how it works:

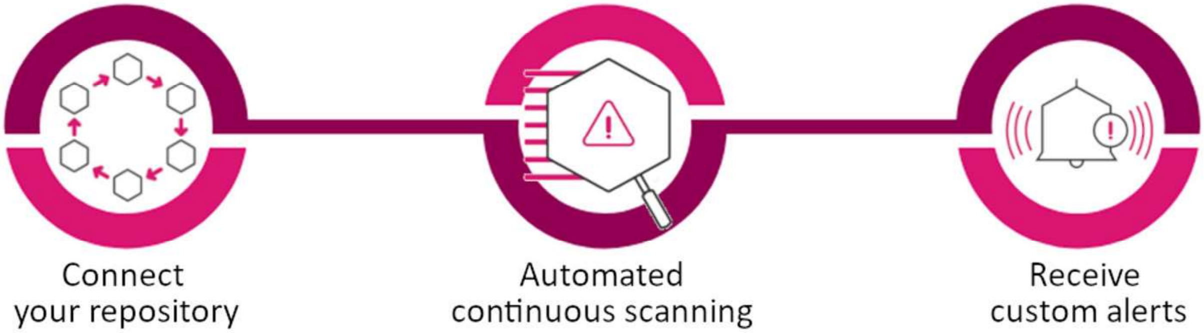


Figure 7: CloudGuard Pipeline Security automates code security in three steps

Setting up in just three minutes, with no special configuration needed, Pipeline Security left-shifts your protection against hard-coded secrets and other vulnerabilities in just a few simple steps:

1. First, connect your repository or CI/CD. Pipeline Security integrates seamlessly with every leading CI system, including Jenkins, Azure, and more.
2. Pipeline Security automatically begins scanning your code using hundreds of custom detectors and proprietary machine learning models, uncovering problems in near real time.
3. Custom alerting can be configured to meet your own policies and KPIs, using built-in AI-backed detectors or custom detectors created around your own needs.

Pipeline Security works fast, usually in 5-7 seconds. And as you can see, it does more than simply flag problems—it gives developers the information they need to resolve them fast. With Pipeline Security on your team, you'll spend less time fixing security issues because potential problems are flagged as soon as developers create the code or check it in. And with only seconds for each scan, it gives you total control over security with greater efficiency and without getting in the way of your developers' workflows. Plus, Pipeline Security integrates into your existing source control, CI/CD pipelines, and IDEs. It works behind the scenes to make sure insecure code never reaches production, keeping you, your customers, and your reputation safe.

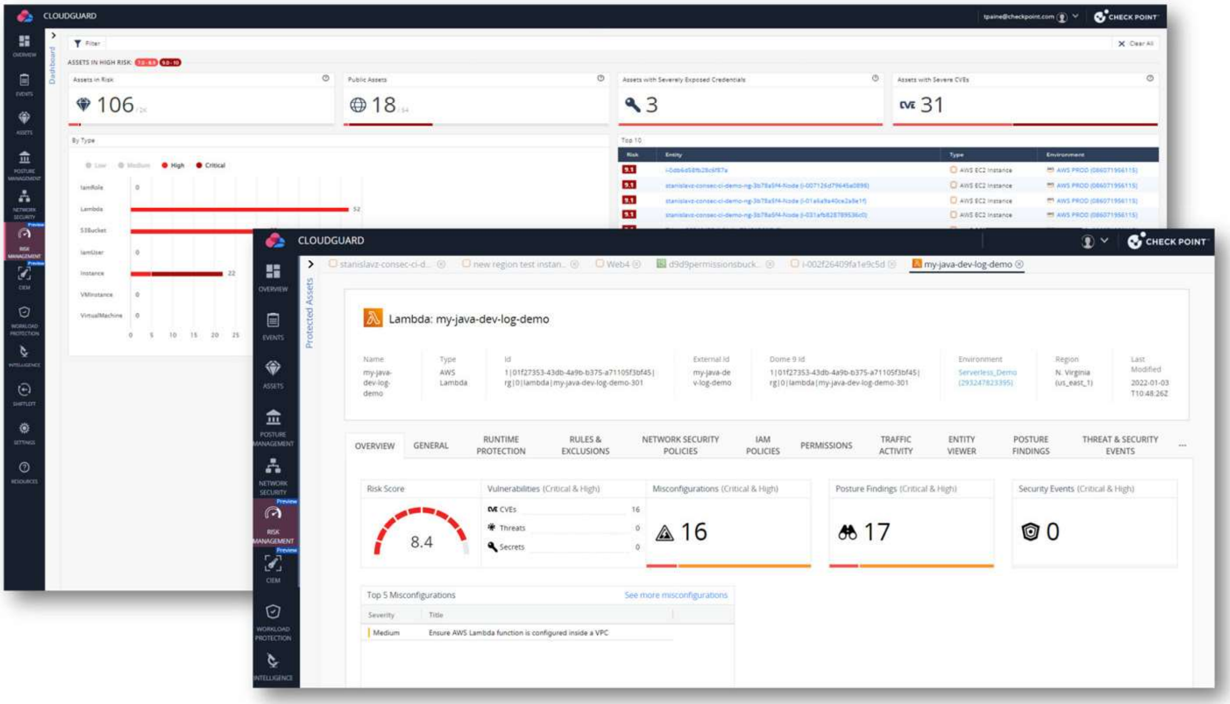
Effective Risk Management (ERM) – Focus on the 1% of Risks That Matter

Almost all security teams feel overloaded and overwhelmed. With so many moving parts, all the components that go into CNAPP solutions can generate a massive volume of alerts. This, in turn, keeps your security team in a rut where they're on constant high alert, having to task-switch, and not making efficient use of the personnel available—at a time when highly qualified cloud security engineers are scarce.

CNAPP should relieve your burden, not add to your burden, so you need a CNAPP platform that lets you focus on the 1% of essential tasks that cannot be overlooked.

That's why Check Point has built effective risk management (ERM) into its CloudGuard CNAPP solution, letting you leverage enhanced context to decide what is important and what is not. ERM brings data together from all CloudGuard CNAPP components, combining it with deep context to provide actionable reporting across the entire environment.

CloudGuard ERM makes it easier to assess risks and follow up with automated remediation. You'll get more than security intelligence for workloads and users, you'll also have deep context so you don't miss a beat. ERM is designed to help you turn data into action, prioritize the risks that matter to your business, and bring down time to remediation.



Risk	Entity	Type	Environment
9.1	i-0db6d58fb28c6f87a	AWS EC2 Instance	AWS PROD (086071956115)
9.1	stanislavz-consec-ci-demo-ng-3b78a5f4-Node (i-007126d79645a0896)	AWS EC2 Instance	AWS PROD (086071956115)
9.1	stanislavz-consec-ci-demo-ng-3b78a5f4-Node (i-01a6a9a40ce2a8e1f)	AWS EC2 Instance	AWS PROD (086071956115)
9.1	stanislavz-consec-ci-demo-ng-3b78a5f4-Node (i-031afb828789536c0)	AWS EC2 Instance	AWS PROD (086071956115)

Lambda: my-java-dev-log-demo

Name	Type	Id	External Id	Dome 9 Id	Environment	Region	Last Modified
my-java-dev-log-demo	AWS Lambda	1|01f27353-43db-4a9b-b375-a71105f3bf45|rg|0|lambda|my-java-dev-log-demo-301	my-java-dev-log-demo	1|01f27353-43db-4a9b-b375-a71105f3bf45|rg|0|lambda|my-java-dev-log-demo-301	Serverless_Demo (293247823395)	N. Virginia (us_east_1)	2022-01-03 T10:48:26Z

Top 5 Misconfigurations

Severity	Title
Medium	Ensure AWS Lambda function is configured inside a VPC

Figure 8: CloudGuard ERM lets you focus on the risks that matter for faster prevention and time to remediation

.

In other words? You need insights, not just more alerts.

To let your team focus on the risks that matter to your business and avoid being distracted by lower-priority issues, ERM gives you:

- Simplified big-picture views of your environment thanks to contextual AI and risk scoring
- A unified approach that reduces complexity, letting you focus on the highest-priority risks
- Actionable insights with a clear framework for automated remediation

Plus, ERM offers a "minimal effective dose" approach to remediation. This means it won't send your team chasing labor-intensive fixes that have little relevance to your overall security posture. With precise remediation recommendations, you'll get the most ROI possible with the least possible effort.

ERM puts you in the driver's seat, with total control over your security and reduced operational overhead, adapted to your priorities.

Use case example:

Your QA team is using a cloud resource to test a feature with mock data. At the same time, your in-production payment application has misconfigurations and vulnerabilities. ERM will help your security team focus on fixing the instance at risk in the payment application before they get distracted by the alerts generated by your QA team's testing resource.

Here's how ERM works:

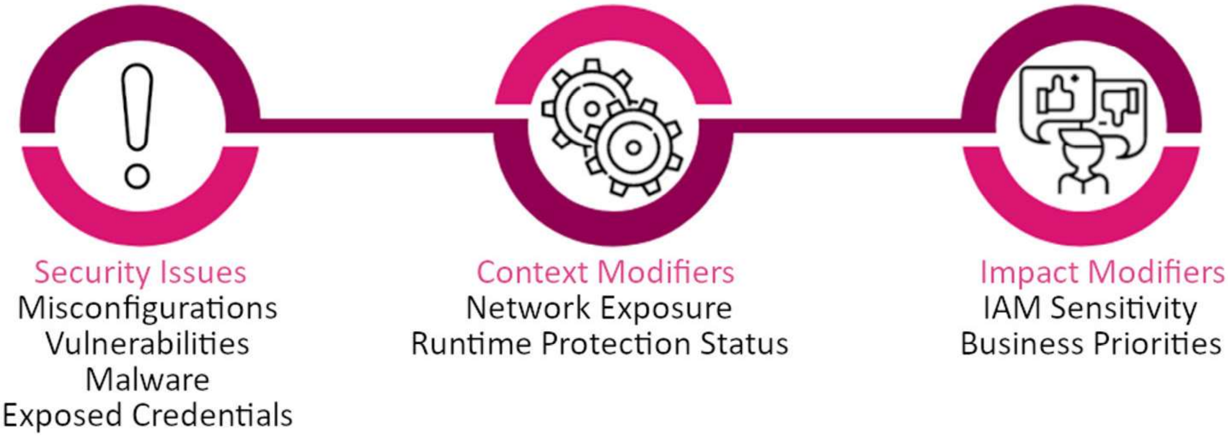


Figure 9: The three risk score components of CloudGuard ERM give you the context you need to protect your most mission-critical workloads

CloudGuard's ERM gets you up and running quickly, analyzing three distinct risk score components to offer you a comprehensive security context:

1. It profiles input from misconfigurations, CVEs, malware, and exposed credentials across all cloud assets to identify known security issues along with their severity.
2. ERM assesses context modifiers such as internet exposure and active protections in place.
3. It weighs a range of impact modifiers such as IAM sensitivity, i.e., the potential damage the entity could cause due to its cloud entitlements, and business priority, which is the criticality of a given asset to your business's operations, letting you differentiate between ordinary and "crown jewel" assets.

Armed with this deep context, ERM provides a clear and understandable risk score per cloud asset, as well as clear and prioritized remediation steps that empower your team to focus on the real risks, bringing down time to remediation and ensuring greater application security.

As you can see, CloudGuard's CNAPP solution helps you understand your true risk posture—which is more than just a number. ERM helps you reduce risk by letting your security team focus on the 1% of alerts that pose 99% of your security risk.

CloudGuard CNAPP: Where All Your Teams' Needs Meet

When it comes to cloud-native application security, it's essential to get all your departments on the same page so you can speed up threat mitigation across diverse cloud teams and avoid vulnerabilities during runtime by fixing them early in the pipeline. One of the most challenging aspects of this is reconciling the tension between your developers and DevOps teams and your security teams:

- **DevOps:** Fast and furious by nature, they want to move quickly, build great features, and fix problems fast. They can maximize revenue through agility and developer-friendly features, such as AWP, which runs on a mirror image of the data, so it doesn't affect their processes.

- **Security:** Careful and steady by nature, they want to slow things down and ensure safety before release. They maximize revenue through reducing risk and ensuring a solid reputation, trust, and compliance.

Three Simple Ideas: More Context, Actionable Security, Smarter Prevention

CloudGuard's CNAPP represents the next evolution of cloud security, giving all your departments exactly what they need.

CloudGuard is your best way to achieve more context, including deep security intelligence on workloads and users, for better and actionable application security. Its new contextual risk engine separates the 1% of alerts that matter from the 99% that don't. So you get smarter prevention capabilities in less time, thanks to the effective remediation engine built into CloudGuard's CNAPP that helps you choose the most effective actions to maximize risk reduction. Plus, we've built CloudGuard to address the four most urgent areas of modern cloud application security complexity. Each component helps you move quickly from risk to resolution with the least possible impact.

Risk	CloudGuard Component	Resolution
Developer team resistance to workload agents	AWP	See what's really going on beneath the surface without impeding developer velocity.
New vulnerabilities, malware, and secret leakage	Pipeline Security	Build security into the SDLC painlessly to protect applications from day one.
Misconfigurations and excessive permissions	CIEM, ERM	Start with deep insights and flag potential issues to resolve them fast.
Unattended security issues	ERM	Set auto-prioritization to tailor remediation to your business's priorities.

Figure 10: How CloudGuard's components address your most critical cloud security needs

At Check Point, we know that an effective CNAPP solution is more than the sum of its parts, bringing together best-in-breed tools and unifying them through a single powerful platform, built for the way modern software organizations work. With powerful guardrails for your cloud security teams, high levels of automation to enable much greater operational efficiency, and unprecedented agility for your developers, CloudGuard gives you a true enterprise-grade security platform, backed by Check Point's industry-leading reputation.

To get started, read more about CloudGuard's CNAPP, or schedule a personalized demo.

Worldwide Headquarters
5 Shlomo Kaplan Street, Tel Aviv 6789159, Israel | Tel: +972-3-753-4599

U.S. Headquarters
959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 1-800-429-4391

www.checkpoint.com