CHECK POINT™

Cloud Native Application Protection Platform

The best cloud security is now even smarter

The cloud has revolutionized the ways in which development teams' work, and security teams have strived to keep up at the same velocity and scale. With the exponential increase in distributed assets, changes occur at a rapid pace, and different teams are not always aligned with the security guidelines needed throughout the development lifecycle. This has left security teams unable to stay on top of the risks within their cloud environment, and take action quickly on the alerts most critical.

Organizations need actionable insights to drive pragmatic remediation. Unfortunately, the majority of CNAPP solutions on the market lack the context needed, from across workloads, to operationalize security at cloud speed and scale.

Today's cloud environment needs more context in order to provide smarter security—fast.

More Context. Actionable Security. Smarter Prevention.

From code to cloud, Check Point CloudGuard's CNAPP unifies cloud security, merging deeper security insights to prioritize risks and prevent critical attacks—providing more context, actionable security, smarter prevention. CloudGuard enhances visibility by enriching context, provides actionable remediation insights and speeds up threat mitigation across diverse cloud teams.

More context

Deeper visibility from code to cloud across configurations, identities, vulnerabilities, network exposure and real time security monitoring

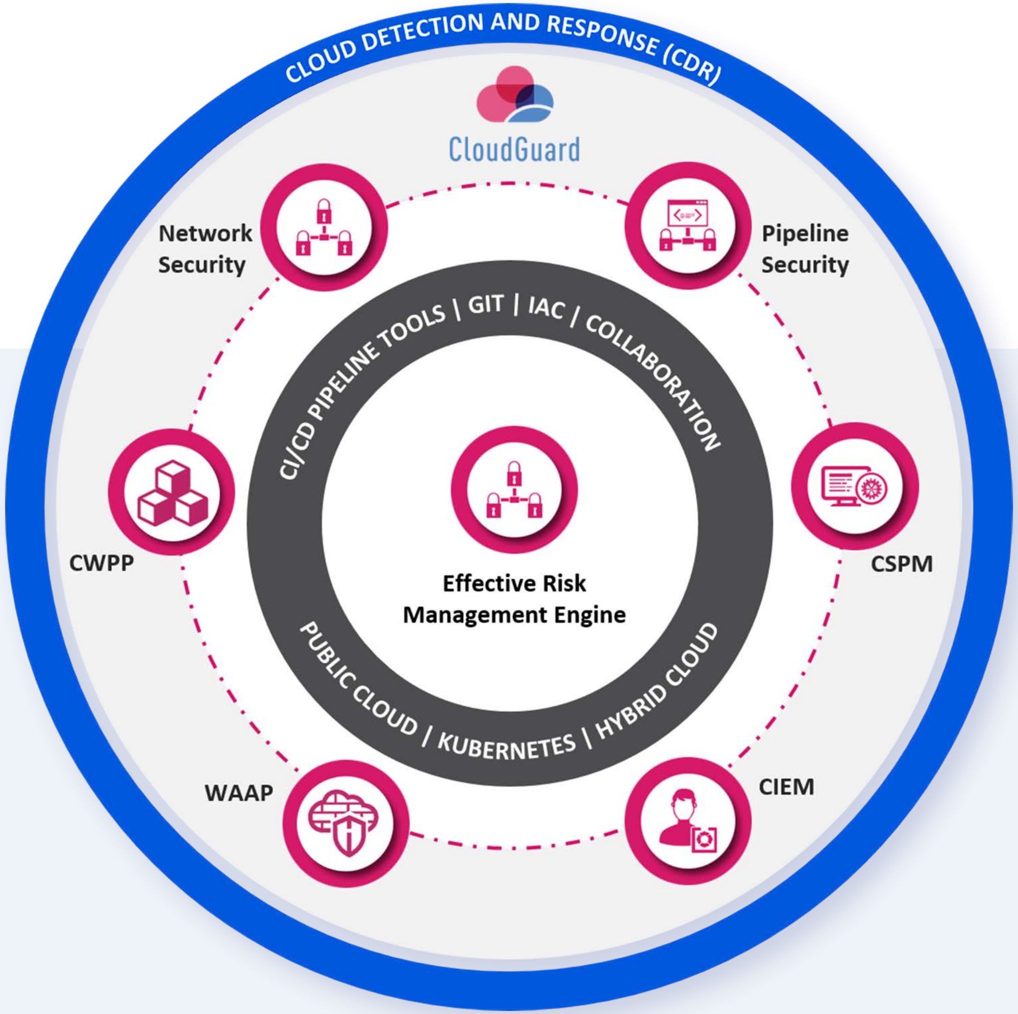
Actionable security

Intelligently prioritize critical risks based on contextual analysis of all elements to focus on the threats that matter most

Smarter prevention

Prevent risks early in the dev pipeline, or stop them in production, while providing actionable remediation guidance for misconfigurations and permissions

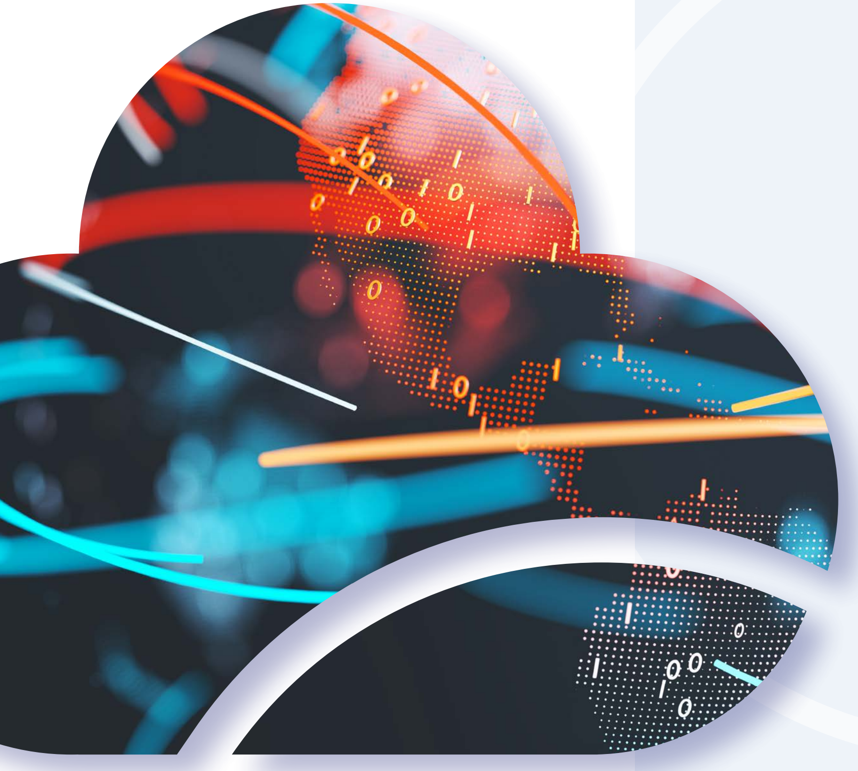
> "Check Point enables us to maximize our cybersecurity posture with a fixed level of investment. As we need new capabilities, we simply add them. Check Point's unique flexibility gives us agility for business growth with service continuity for our partners and customers."
>
> — Brian Chan, Information Technology Director of Jebsen Group


CLOUD DETECTION AND RESPONSE (CDR)
CloudGuard
Network Security
Pipeline Security
CI/CD PIPELINE TOOLS | GIT | IAC | COLLABORATION
CWPP
CSPM
Effective Risk Management Engine
PUBLIC CLOUD | KUBERNETES | HYBRID CLOUD
WAAP
CIEM

Take advantage of industry-leading Pipeline Security, Cloud Security Posture Management (CSPM), Cloud Infrastructure Entitlement Management (CIEM), Workload Protection (CWPP), Web Application and API Protection (WAAP), and Cloud Detection and Response (CDR) technologies all integrated with an AI-driven Effective Risk Management engine (ERM) for a unified experience and single point of decision-making.

CloudGuard's CNAPP provides customers actionable security insights covering public clouds, workloads, identities and applications, covering the entire development lifecycle from code-to-cloud. CloudGuard delivers a smooth experience for agile teams that can rely on agentless deployments and seamless integrations to provide actionable security guidance from build through runtime.

- New Deep workload security visibility at scale with no agents
- New Understand your permissions and enforce least privilege across your clouds
- New Shift CNAPP left & secure your cloud applications from the start
- New Focus on the 1% of risks and threats that matter by putting cloud security in context



Enhanced Cloud Security Posture Management

More context across cloud workloads and users for greater insights

One of the great things about cloud computing is the ability to collect telemetry from a wide variety of sources. Monitoring, intelligence and other data sources provide a wealth of information when it comes to application protection. But data extraction is not the main problem anymore, it's establishing 100% visibility, creating synergies, ending fragmentation, and understanding security posture in context, so you can make the right decisions. Check Point CloudGuard combines context from workloads and user activity to gain deeper security insights.

Gain visibility and stay compliant with CSPM

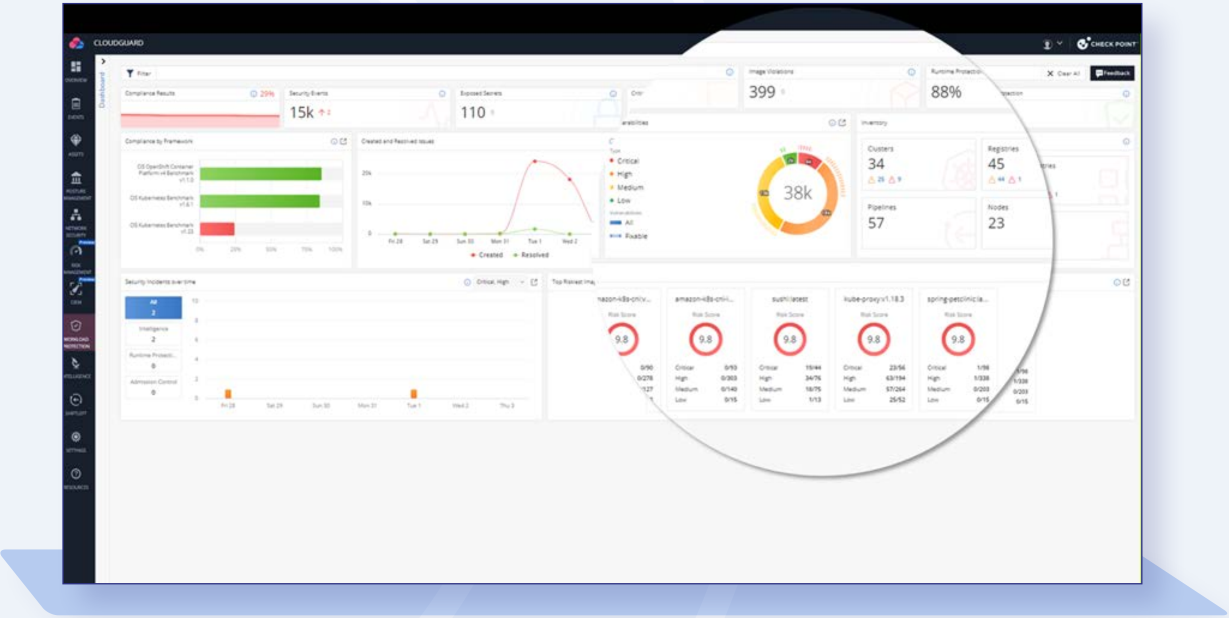
From one unified platform, you can visualize and assess security posture, detect misconfigurations, model and enforce gold standard policies, protect against attacks and insider threats, and comply with regulatory requirements and best practices. With CloudGuard, cloud security operations are faster and more effective, compliance and governance are easier, and DevSecOps practices are frictionless.

Deep workload security visibility at scale with no agents

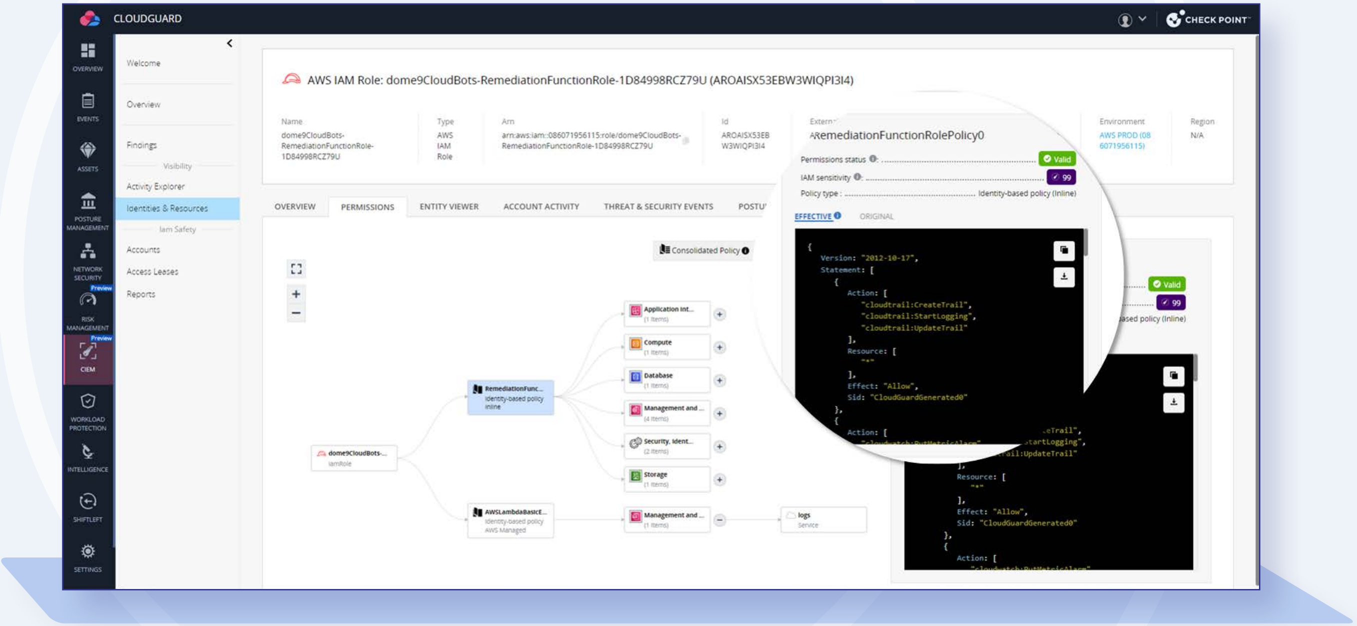
Don’t rely on other teams to deploy security – Gain deep visibility with agentless deployments to understand what is happening within your cloud workloads.

Agentless Workload Posture (AWP) extends CloudGuard’s agentless infrastructure visibility into workloads. AWP scans and identifies risks including misconfigurations, malware detection, vulnerabilities and secrets across all cloud workloads including Virtual Machines, Containers and Serverless Functions:

- Immediate visibility into workloads including VMs, containers, and serverless functions at scale
- Detect and alert on risks such as misconfigurations, malware, vulnerabilities and secrets
- WP findings feed into CloudGuard’s contextual risk engine (ERM) and XDR platforms



Understand Your Permissions & Enforce Least Privilege Across Your Clouds with Cloud Infrastructure Entitlement Management (CIEM)



AWS IAM Role: dome9CloudBots-RemediationFunctionRole-1D84998RCZ79U (AROAISX53EBW3WIQPI3I4)

Name	Type	Arn	Id	Extern	Environment	Region
dome9CloudBots-RemediationFunctionRole-1D84998RCZ79U	AWS IAM Role	arn:aws:iam::086071956115:role/dome9CloudBots-RemediationFunctionRole-1D84998RCZ79U	AROAISX53EBW3WIQPI3I4		AWS PROD (086071956115)	N/A

ARemediationFunctionRolePolicy0

Permissions status: ✓ Valid

IAM sensitivity: 99

Policy type: Identity-based policy (Inline)

```
{
  Version: "2012-10-17",
  Statement: [
    {
      Action: [
        "cloudtrail:CreateTrail",
        "cloudtrail:StartLogging",
        "cloudtrail:UpdateTrail"
      ],
      Resource: [
        "*"
      ],
      Effect: "Allow",
      Sid: "CloudGuardGenerated0"
    },
    {
      Action: [
        "cloudwatch:PutMetricAlarm"
```

In today's complex cloud environment, you need to ensure that user and workload access is optimized with the perfect dose of permissions, while quickly addressing over permissive roles.

With Check Point CloudGuard CIEM functionality you get full visibility of effective permissions to quickly identify over-permissive entitlements. CloudGuard identifies exposure and risks quickly to automatically generate least privilege role recommendations to reduce access and revoke unused permissions—helping you reach a state of zero-trust.

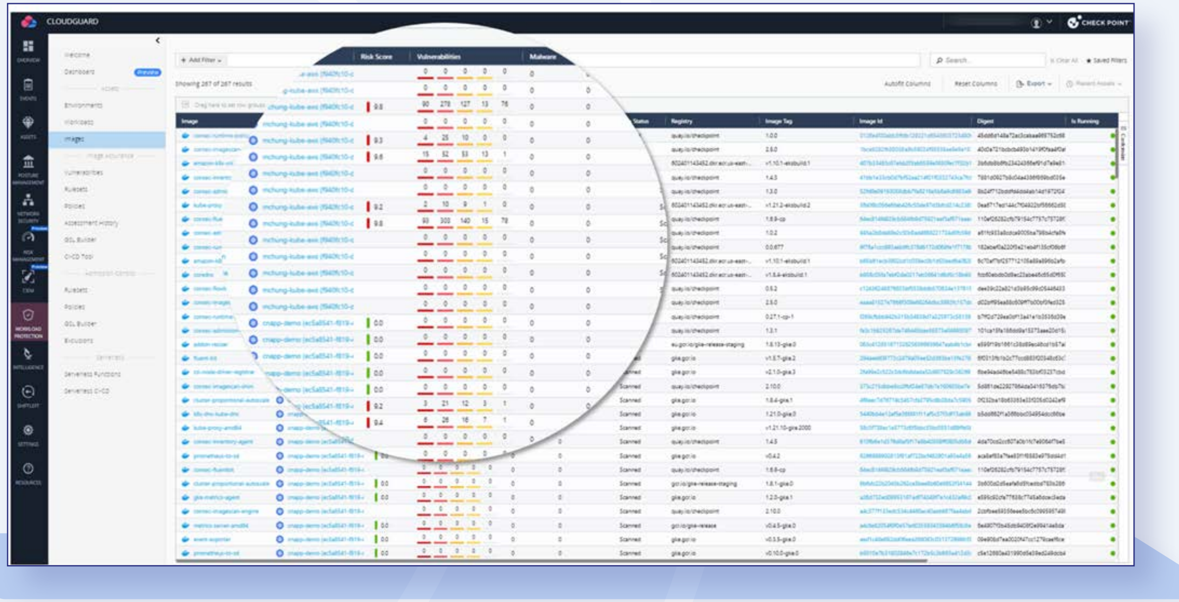
- Visualize effective permissions of users and cloud services
- Detect unused roles, over-permissions and risky entitlements that can put you at risk
- Automatically generate least privilege roles recommendations based on actual usage

Runtime Protection for Your Cloud Workloads (CWPP)

CloudGuard provides fully automated, cloud-native workload protection. It allows unified visibility, compliance and threat prevention across applications, APIs and microservices (K8s containers & serverless functions), from development through runtime. Protect workloads during runtime, and profile and enforce function, container, and application behavior. CloudGuard allows you to block malicious activity with behavioral signature matching and easily set security policies and guardrails for K8s cluster operations with admission control.

CloudGuard unifies workload protection, providing visibility, security controls and scanning across the entire cloud workload from the first line of code through to runtime.

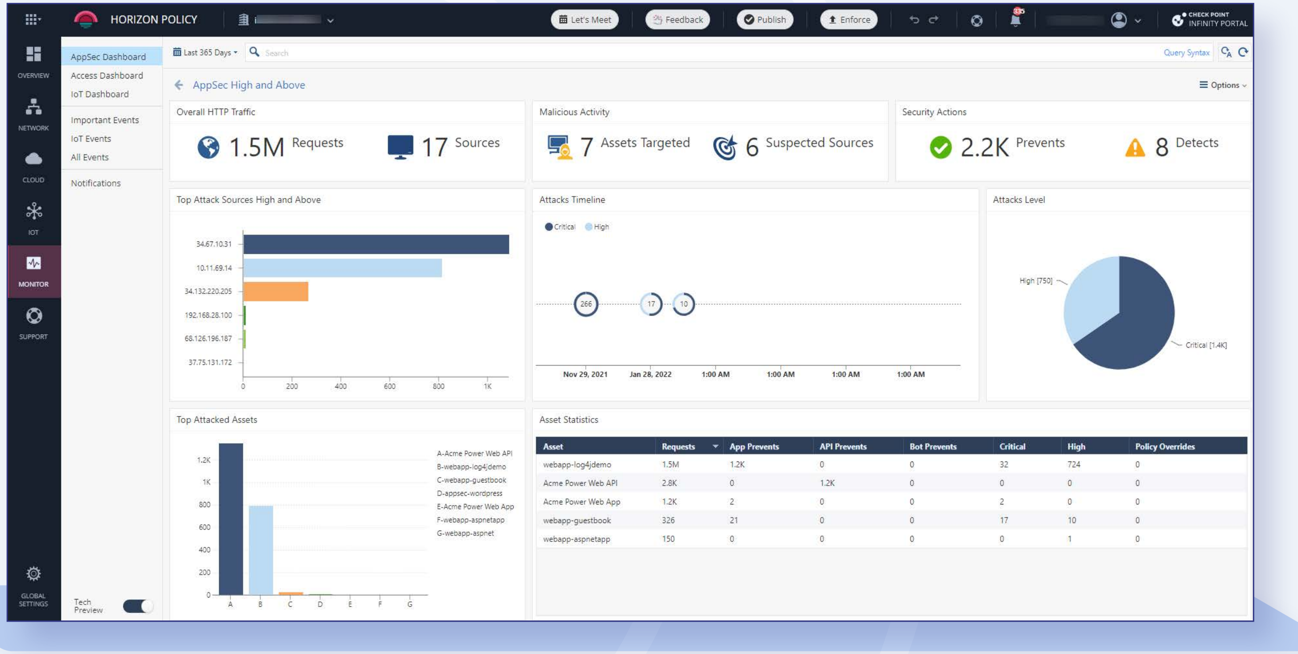
- Achieve zero trust security across applications, APIs, K8s and serverless functions
- Auto-deploy & enforce security controls
- Remain cloud & architecture agnostic with protection on multi and hybrid cloud deployments



Context-Based Web Application and API Protection (WAAP)

As a revolutionary paradigm in application security, CloudGuard replaces legacy Web Application Firewalls, which only work well if an excessive amount of management resources are devoted to maintaining them.

With CloudGuard, every incoming request is analyzed in context. The patent-pending AI engine analyzes risk by examining user profiles, patterns observed in user sessions, and how other users interact with the application. The score assigned to each request determines how likely it is to be malicious. Through continuous profiling of the user, application, and content, the engine adapts automatically to changes in the application. This approach has proven to eliminate false positives while maintaining the highest standards of application security.



Asset Statistics

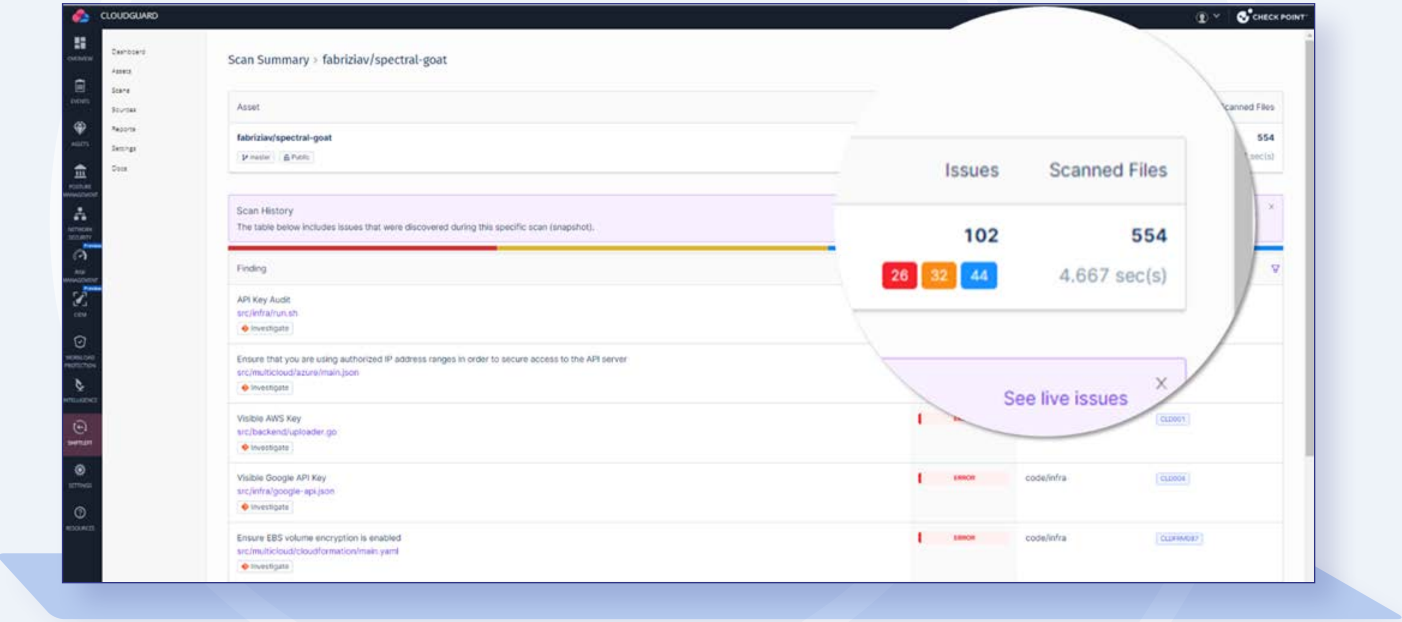
Asset	Requests	App Prevents	API Prevents	Bot Prevents	Critical	High	Policy Overrides
webapp-log4jdemo	1.5M	1.2K	0	0	32	724	0
Acme Power Web API	2.8K	0	1.2K	0	0	0	0
Acme Power Web App	1.2K	2	0	0	2	0	0
webapp-guestbook	326	21	0	0	17	10	0
webapp-aspnetapp	150	0	0	0	0	1	0

With deployment to protection in a matter of hours, maintain application security with a solution that can keep up even with the fastest Devops teams.

- Stop attacks against applications including site defacing, information leakage, digital theft, and user session hijacking

Shift CNAPP Left to Secure Applications from the Start in Your CI/CD Pipeline

As applications are developed faster, they often contain hard-coded secrets or vulnerabilities erroneously left behind, and too often reaching your production environment. CloudGuard prevents these exposures from reaching production and shifts CNAPP left to streamline your application protection at its creation. With CloudGuard enforce security policies throughout the software development lifecycle without creating friction for developers.



Scan Summary › fabriziav/spectral-goat

Asset

fabriziav/spectral-goat

Scan History

The table below includes issues that were discovered during this specific scan (snapshot).

Finding

API Key Audit
src/infra/run.sh

Ensure that you are using authorized IP address ranges in order to secure access to the API server
src/multicloud/azure/main.json

Visible AWS Key
src/backend/uploader.go

Visible Google API Key
src/infra/google-api.json

Ensure EBS volume encryption is enabled
src/multicloud/cloudformation/main.yaml

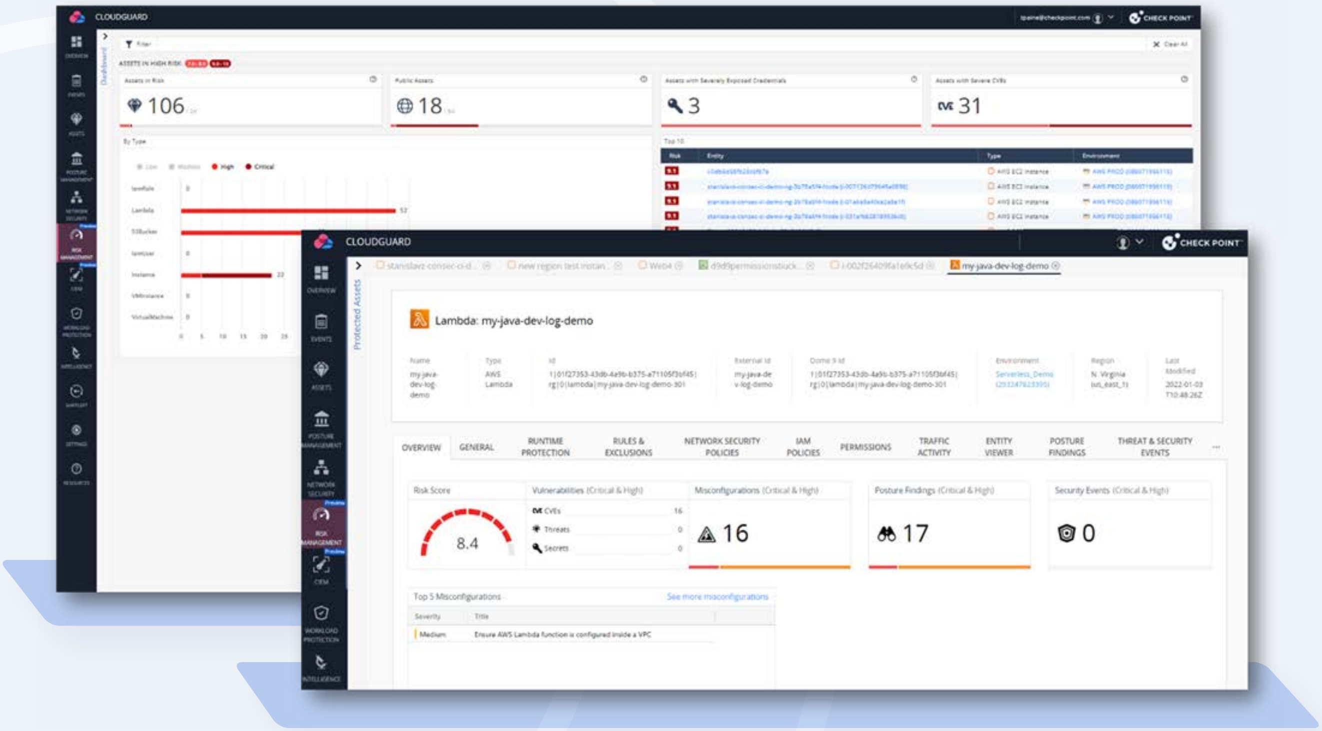
CloudGuard shift-left functionality seamlessly integrates into the CI/CD pipeline to scan code, automate protection, detect malware, and eliminate blind spots. In addition, CloudGuard automates open source governance and SBOM creation to stop malicious and faulty OSS packages with a software composition analysis tool made for high-velocity development teams. Keeping malicious open source software packages out of your applications.

- Empower developers to fix vulnerabilities, misconfigurations, and exposed secrets proactively before code deployment
- Identify and remediate supply chain risks across your pipeline tools including Git, Jenkins & more
- Extend workload protection throughout the CI/CD pipeline to remediate issues prior to production

Focus on the 1% of Risks That Matter and Fix Faster with Effective Risk Management (ERM)

Staying on top of the flood of security alerts requires smarter action, not harder work. CloudGuard's Effective Risk Management (ERM) engine prioritizes risks and provides actionable remediation guidance based on the full context including workload posture, network exposure, identity permissions, attack path analysis and the application business value.

Take action quickly by focusing on the 1% of risks that are the most critical to your business, while automating security throughout your cloud environment, with actionable insights from a contextual engine which uses AI and risk scoring to reduce the attack surface.



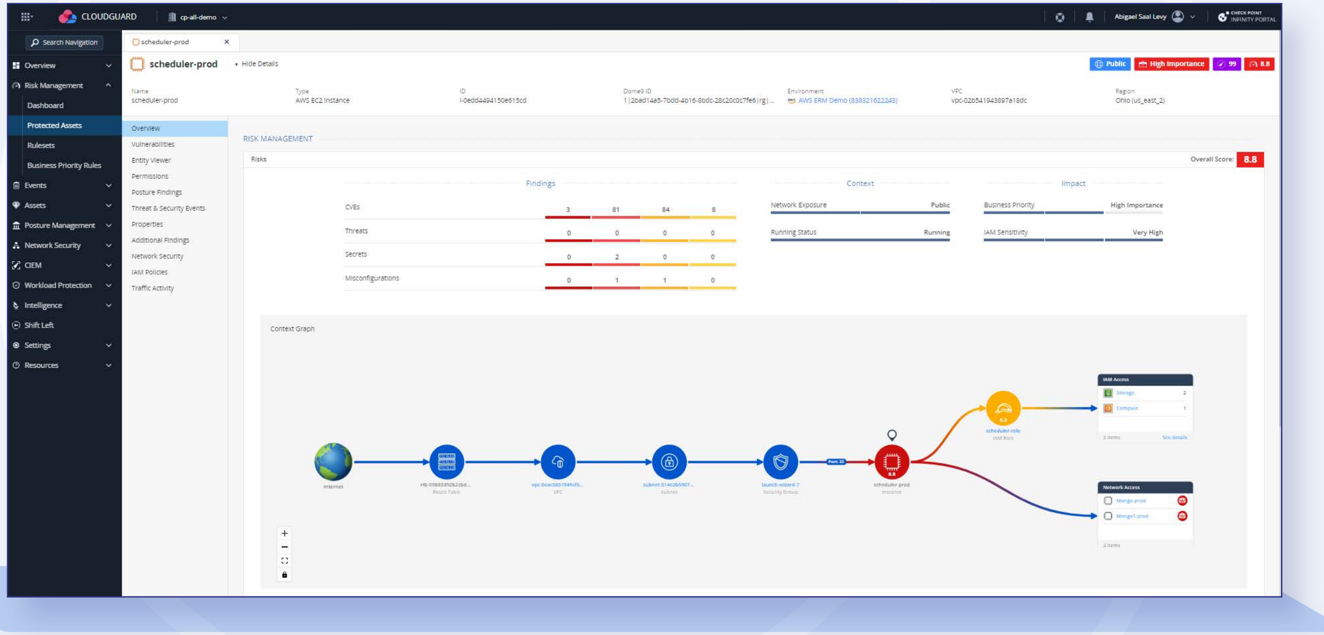
- Prioritize risks based on full context — on figuration risks, workload posture, network exposure, permissions, attack path, and business priorities
- Focus on the threats that matter across clouds, workloads and code
- Deliver optimized remediation guidance based on the fastest path to risk reduction

Analyze Attack Paths with Context Graph Visualization

A picture is worth a thousand words. Leverage CloudGuard's Context Graph to gain comprehensive insights into the risks associated with a cloud asset based on its exposure and context. Gain a holistic view of the asset's exposure to the Internet and factors contributing to its overall risk profile. The Context Graph considers various elements such as the asset's configuration, network connections, and interdependencies, allowing you to visualize the asset's position within your cloud environment.

Comprehensive insights: Understand the risks associated with a cloud asset within its relevant context.

Impact assessment: Assess the potential impact of a vulnerable asset on your cloud environment.



scheduler-prod

Name: scheduler-prod
Type: AWS EC2 Instance
ID: i-0edd4494150e615cd
Dome9 ID: 1 |2bad14a5-7bdd-4b16-8bdc-28c20c0c7fe6 |rg |...
Environment: AWS ERM Demo (838321622243)
VPC: vpc-02b541943897a18dc
Region: Ohio (us_east_2)

RISK MANAGEMENT

Risks — Overall Score: 8.8

Findings

CVEs	3	81	84	8
Threats	0	0	0	0
Secrets	0	2	0	0
Misconfigurations	0	1	1	0

Context

Network Exposure	Public
Running Status	Running

Impact

Business Priority	High Importance
IAM Sensitivity	Very High

Context Graph

Proactive risk management: Identify weak points and potential avenues of exploitation and take preemptive measures to mitigate risks before they are exploited.

Informed risk mitigation: Make informed decisions regarding risk mitigation like fine-tuning IAM policies etc.

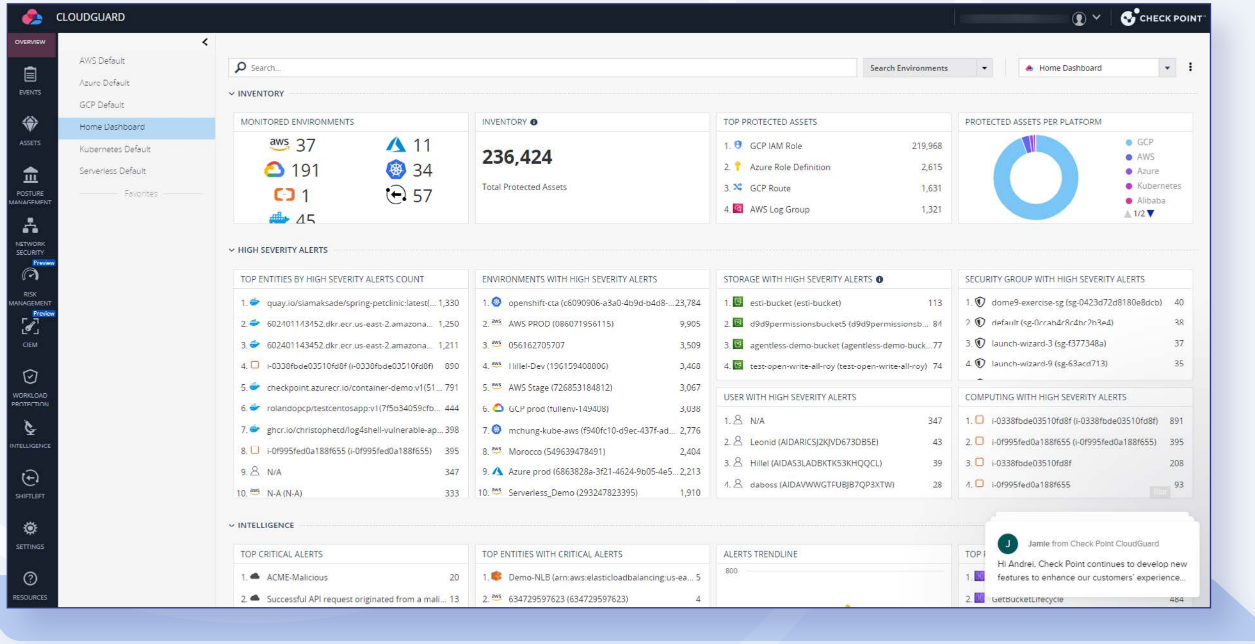
Safeguard your critical cloud assets, data and infrastructure with the Context Graph. By analyzing the asset's IAM (Identity and Access Management) permissions, you can understand the extent of its privileges and the potential ramifications of unauthorized access. Moreover, the Context Graph goes beyond the scope of a single asset by also considering its communication with other assets. This analysis enables you to evaluate the potential chain reaction that could occur if the asset is compromised, thereby allowing you to anticipate and mitigate the cascading effects of an exploit.

Prevent Threats Proactively with Cloud Detection and Response

Enhance findings with CloudGuard to improve threat hunting, and remediation. By integrating information from cloud inventory and configuration, account activity, network traffic logs, and threat feeds such as Check Point ThreatCloud and IP reputation databases, CloudGuard provides a complete and accurate picture for SecOps and SOC teams.

With the added intelligence layer, you can:

- Prevent security breaches and unauthorized activity before any vulnerabilities can be exploited. Leveraging AI and UEBA, CloudGuard continuously analyzes account activity and monitors network traffic for signs of anomalies and cyber threats.
- Receive automatic alerts on rule infringement. Pre-built rules are comprised of industry best practices, in-depth cybersecurity research, the MITRE ATT&CK framework and more.
- Turn enriched data into actionable insights! Retrieve historical data and perform advanced incident analysis to drive data-informed decisions.
- Take a visual exploration tool that interprets account activity and network traffic logs, and provides rich contextual information.



INVENTORY

MONITORED ENVIRONMENTS

aws 37	11
191	34
1	57
45	

INVENTORY

236,424

Total Protected Assets

TOP PROTECTED ASSETS	
1. GCP IAM Role	219,968
2. Azure Role Definition	2,615
3. GCP Route	1,631
4. AWS Log Group	1,321

PROTECTED ASSETS PER PLATFORM

HIGH SEVERITY ALERTS

TOP ENTITIES BY HIGH SEVERITY ALERTS COUNT	
1. quay.io/siamaksade/spring-petclinic:latest(...	1,330
2. 602401143452.dkr.ecr.us-east-2.amazona...	1,250
3. 602401143452.dkr.ecr.us-east-2.amazona...	1,211
4. i-0338fbde03510fd8f (i-0338fbde03510fd8f)	890
5. checkpoint.azurecr.io/container-demo:v1(51...	791
6. rolandopcp/testcentosapp:v1(7f5b34059cfb...	444
7. ghcr.io/christophetd/log4shell-vulnerable-ap...	398
8. i-0f995fed0a188f655 (i-0f995fed0a188f655)	395
9. N/A	347
10. N-A (N-A)	333

ENVIRONMENTS WITH HIGH SEVERITY ALERTS	
1. openshift-cta (c6090906-a3a0-4b9d-b4d8-...	23,784
2. AWS PROD (086071956115)	9,905
3. 056162705707	3,509
4. Hillel-Dev (196159408806)	3,468
5. AWS Stage (726853184812)	3,067
6. GCP prod (fullenv-149408)	3,038
7. mchung-kube-aws (f940fc10-d9ec-437f-ad...	2,776
8. Morocco (549639478491)	2,404
9. Azure prod (6863828a-3f21-4624-9b05-4e5...	2,213
10. Serverless_Demo (293247823395)	1,910

STORAGE WITH HIGH SEVERITY ALERTS	
1. esti-bucket (esti-bucket)	113
2. d9d9permissionsbucket5 (d9d9permissionsb...	84
3. agentless-demo-bucket (agentless-demo-buck...	77
4. test-open-write-all-roy (test-open-write-all-roy)	74

SECURITY GROUP WITH HIGH SEVERITY ALERTS	
1. dome9-exercise-sg (sg-0423d72d8180e8dcb)	40
2. default (sg-0ccab4c8c4bc2b3e4)	38
3. launch-wizard-3 (sg-f377348a)	37
4. launch-wizard-9 (sg-63acd713)	35

USER WITH HIGH SEVERITY ALERTS	
1. N/A	347
2. Leonid (AIDARICSJ2KJVD673DB5E)	43
3. Hillel (AIDAS3LADBKTK53KHQQCL)	39
4. daboss (AIDAVWWGTFUBJB7QP3XTW)	28

COMPUTING WITH HIGH SEVERITY ALERTS	
1. i-0338fbde03510fd8f (i-0338fbde03510fd8f)	891
2. i-0f995fed0a188f655 (i-0f995fed0a188f655)	395
3. i-0338fbde03510fd8f	208
4. i-0f995fed0a188f655	93

INTELLIGENCE

TOP CRITICAL ALERTS	
1. ACME-Malicious	20
2. Successful API request originated from a mali...	13

TOP ENTITIES WITH CRITICAL ALERTS	
1. Demo-NLB (arn:aws:elasticloadbalancing:us-ea...	5
2. 634729597623 (634729597623)	4

ALERTS TRENDLINE

TOP	
1.	
2. GetBucketLifecycle	484

Jamie from Check Point CloudGuard

Hi Andrei, Check Point continues to develop new features to enhance our customers' experience...

CloudGuard provides the tools to filter out false positives, speed up triage, and simplify incident analysis. Check Point's world-renowned team of experts is constantly expanding and improving alerts. Further, with the power of CloudBots technology, automatically revert risky configuration changes, and create responses to any type of network alert or audit trail, running entirely within your environment.

CloudGuard
CNAPP

> “Check Point CloudGuard CNAPP delivers a well-rounded, **industry-leading approach to cloud and DevOps security**. Best of all, we can manage the entire environment from one place instead of having multiple management interfaces for different parts.”
>
> — Mark Nix, National Information Security, Risk & Governance Manager

More Context, Actionable Security, Smarter Prevention with CloudGuard

From code to cloud, Check Point CloudGuard delivers automated cloud native security, unified across your applications, workloads, and network to manage risk, maintain posture, and prevent threats, in context, at cloud speed and scale. CloudGuard's prevention-first approach protects applications and workloads throughout the software development lifecycle, and includes an effective risk management engine, with automated remediation prioritization, to allow users to focus on the security risks that matter. For more information on CloudGuard, visit www.checkpoint.com/cloudguard

CHECK POINT™

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