5 STEPS TO ZERO TRUST SECURITY on AWS

A practical and holistic approach to implement Zero Trust on AWS

CHECK POINT™

aws PARTNER
Security Software
Competency

Protection from known and unknown threats

Building security infrastructure for the cloud using disparate technologies can lead to complexities and inherent security gaps.

Check Point offers a more practical and holistic approach to implement Zero Trust on Amazon Web Services (AWS) environments, based on single consolidated cyber-security architecture.

Organizations can implement all of the Zero Trust principles that apply to the cloud, focusing on threat prevention, workload protection, and powerful management and visibility tools. With CloudGuard, organizations are empowered to implement Zero Trust maximum security and efficiency.

Check Point brings decades of experience to AWS security solutions, ensuring security is achieved everywhere.

CloudGuard

Available in AWS Marketplace

CLOUDGUARD NETWORK SECURITY
Firewall and threat prevention

Identity Awareness
Granular visibility of users, groups, and machines

CLOUDGUARD POSTURE MANAGEMENT
Visibility, compliance, and consistent policy enforcement

Cloud Identity Entitlement Management (CIEM)
Identity entitlement monitoring, control, and remediation

CLOUDGUARD SPECTRAL
Code and secret scanning

CLOUDGUARD APPSEC
Web application and API protection with contextual AI and no manual tuning
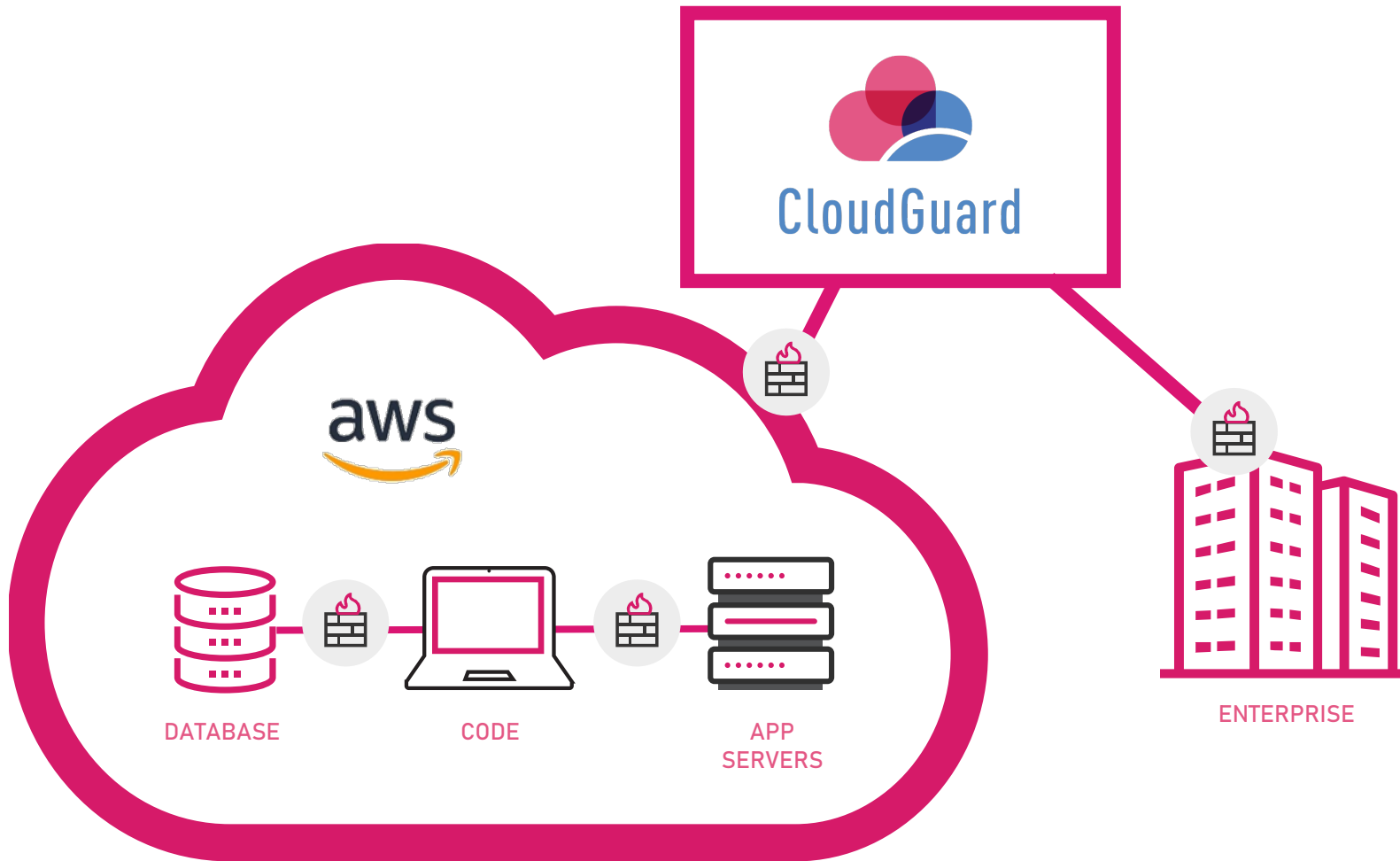
CLOUDGUARD WORKLOAD PROTECTION

Serverless Security
Security of Lambda functions with automated runtime protection and posture management

Container Security
Image assurance and least-privilege access control for Kubernetes clusters and more

CLOUDGUARD INTELLIGENCE
Real-time visibility and threat response

Powered by THREATCLOUD
Accurate prevention against the most advanced attacks using AI technology and big data threat intelligence

2

Protect against unauthorized users

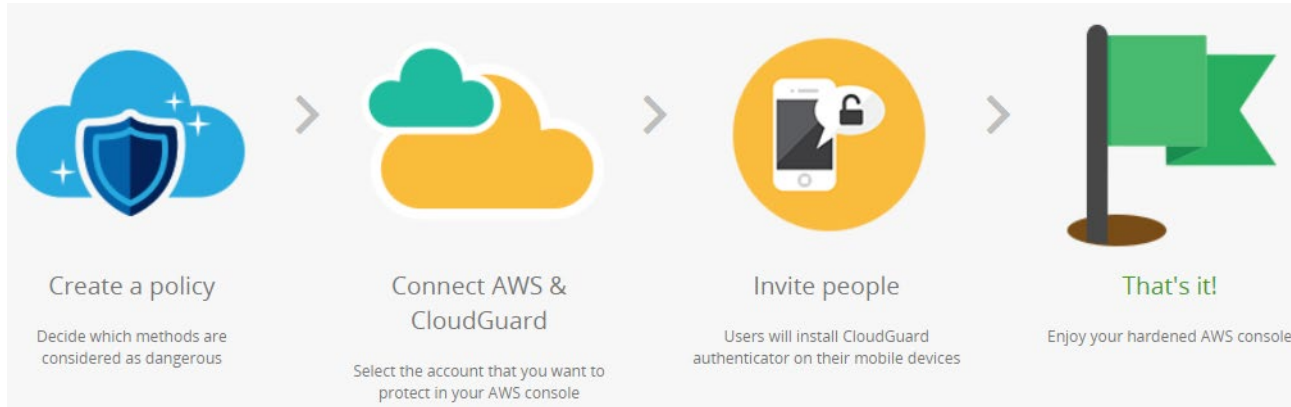Compare actual behavior vs permissions
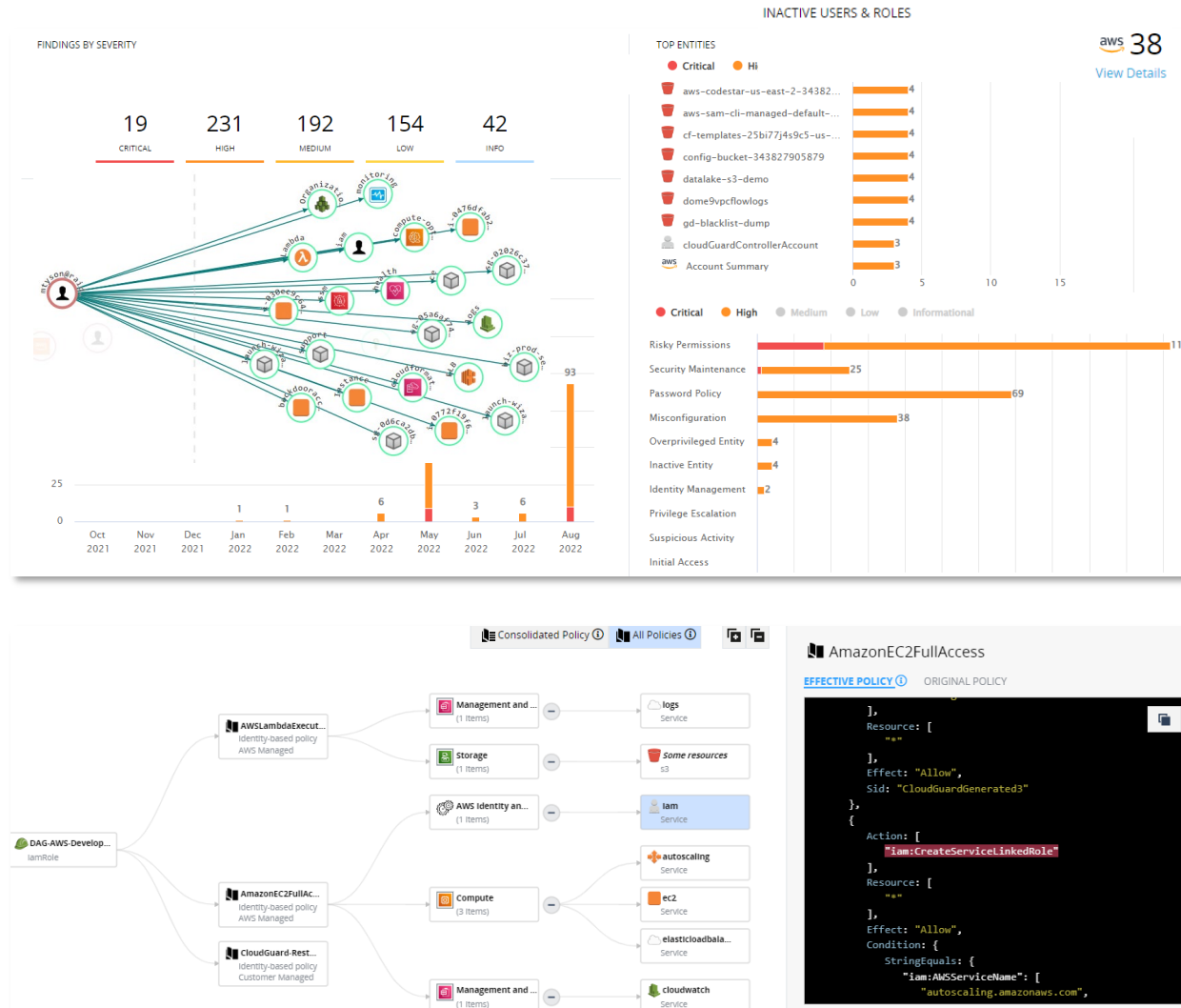
**CLOUDGUARD
POSTURE MANAGEMENT**
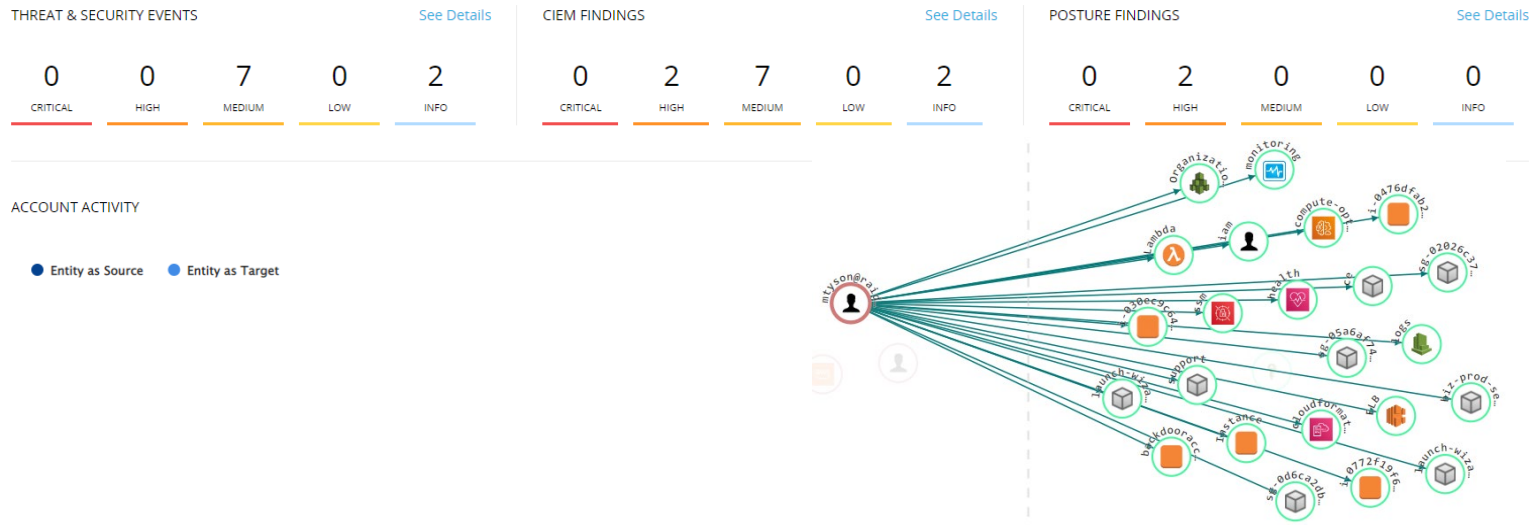CIEM functionality provides identity entitlement monitoring, control, and remediation

**CLOUDGUARD
NETWORK SECURITY**
Identity awareness functionality integrates with AWS IAM to allow access only to specific users

Protect against unauthorized users (continued)

With IAM Safety, you can harden your AWS console and protect it against theft, man-in-the-browser attacks, and more. After you activate IAM Safety, users will be asked to authorize possibly harmful actions using their mobile device.

Create a policy

Decide which methods are considered as dangerous

Connect AWS & CloudGuard

Select the account that you want to protect in your AWS console

Invite people

Users will install CloudGuard authenticator on their mobile devices

That's it!

Enjoy your hardened AWS console

CIEM:
Cloud Infrastructure Entitlement Management

THREAT & SECURITY EVENTS					See Details
0	0	7	0	2	
CRITICAL	HIGH	MEDIUM	LOW	INFO	

CIEM FINDINGS					See Details
0	2	7	0	2	
CRITICAL	HIGH	MEDIUM	LOW	INFO	

POSTURE FINDINGS					See Details
0	2	0	0	0	
CRITICAL	HIGH	MEDIUM	LOW	INFO	

ACCOUNT ACTIVITY

● Entity as Source   ● Entity as Target

CLOUDGUARD POSTURE MANAGEMENT
CIEM functionality provides identity entitlement monitoring, control, and remediation

CLOUDGUARD NETWORK SECURITY
Identity awareness functionality integrates with AWS IAM to allow access only to specific users

Protect AWS workloads

- Seamless integration with AWS
- Detect over-permissive roles, vulnerabilities, and embedded threats
- Multi layer security, leveraging machine learning to profile and protect workloads
- Enforce granular security policies during CI/CD and production for all workloads
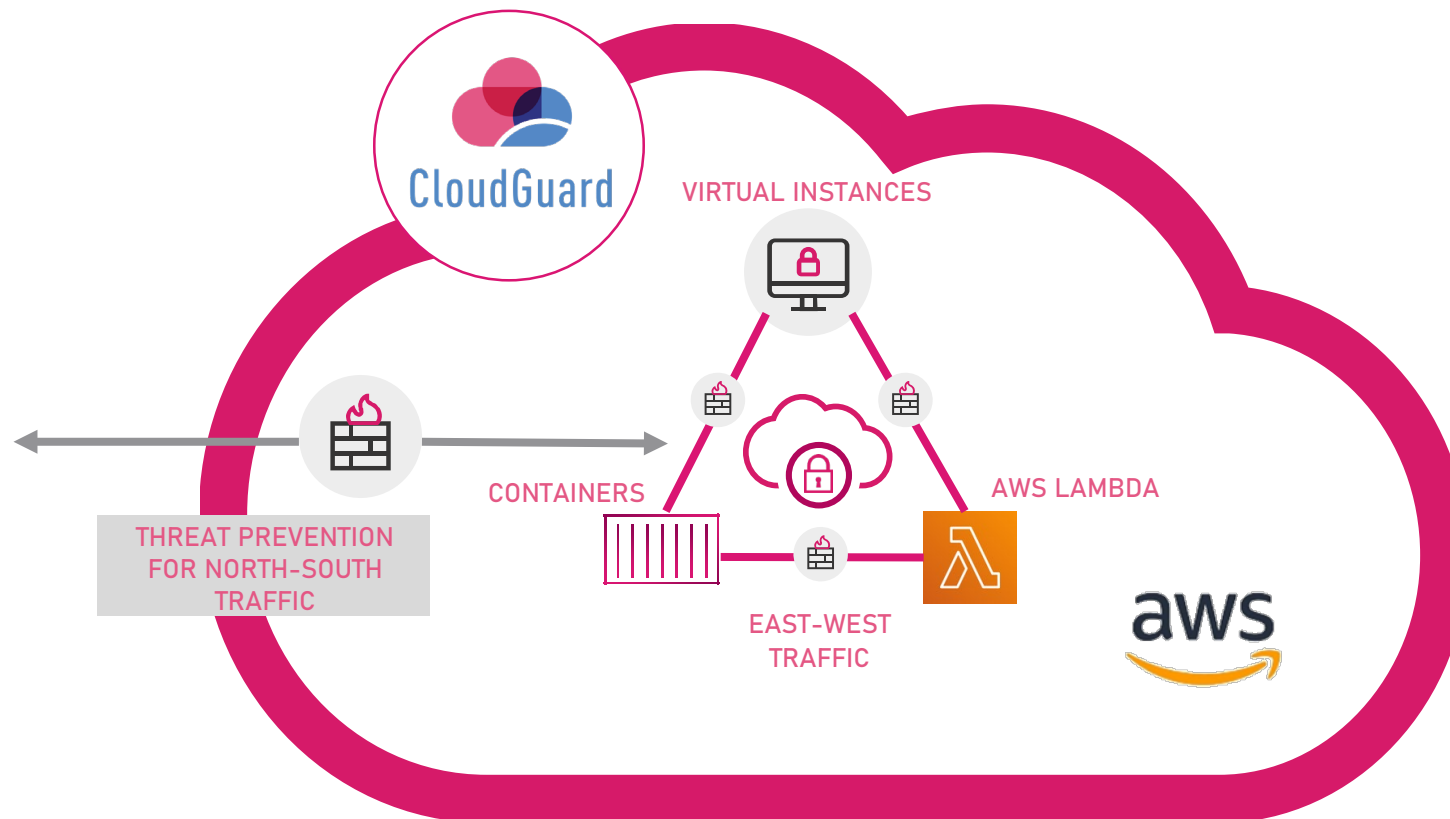
CloudGuard

VIRTUAL INSTANCES

CONTAINERS

AWS LAMBDA

EAST-WEST TRAFFIC

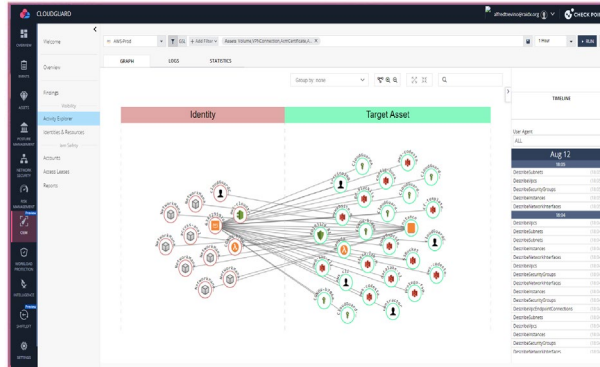THREAT PREVENTION FOR NORTH-SOUTH TRAFFIC

aws

CLOUDGUARD NETWORK SECURITY
Threat prevention for north-south traffic
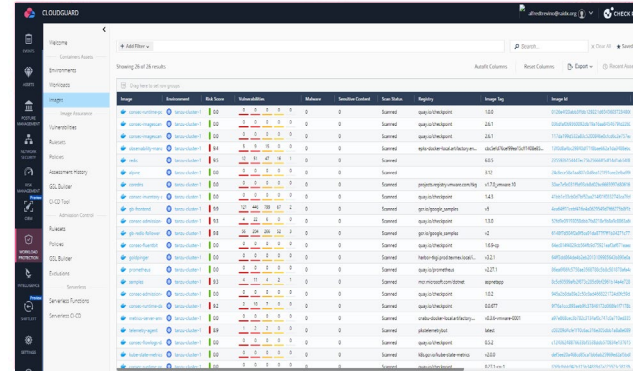Full control over east-west traffic

CLOUDGUARD POSTURE MANAGEMENT
Full visibility into AWS infrastructure, identity misconfigurations and security gaps, and adaptive access policy
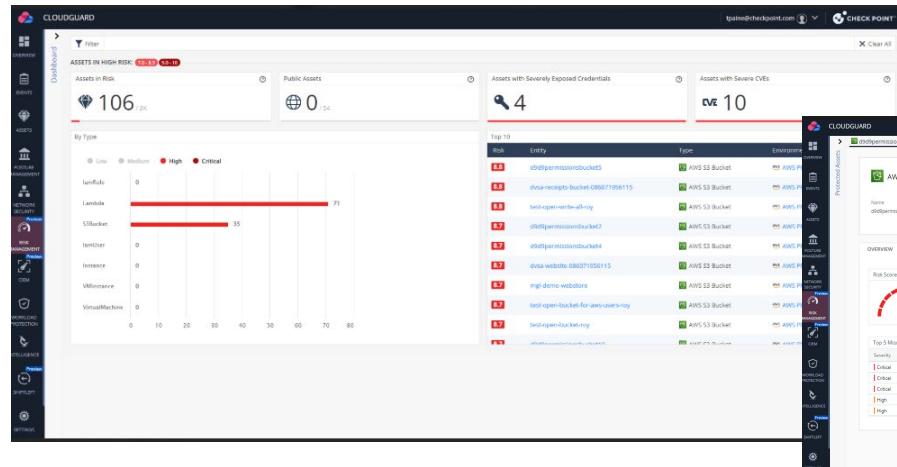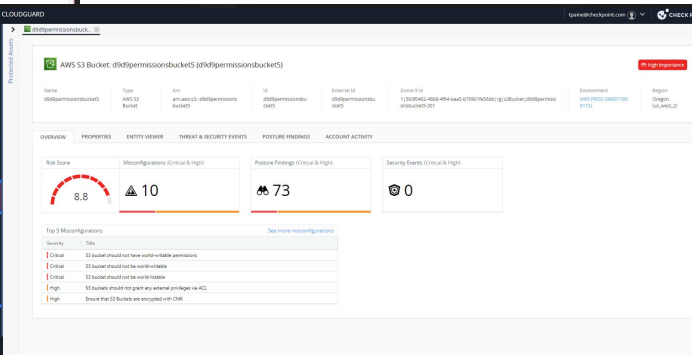
Visibility and analytics

4

Identify suspicious activity and track trends

Real- time visibility into billions of log records

Follow real-time forensic alerts on your CSPM dashboard…

…and get full visibility to risks as well as mitigation options

CLOUDGUARD INTELLIGENCE
Intuitive visualization, querying, intrusion alerts, and notifications

CLOUDGUARD POSTURE MANAGEMENT
Quickly detect and mitigate threats with a single view into security risks

Protect from known and unknown threats

CloudGuard

- Prevention first: highest security effectiveness score with 100% block rate*
- 0% false positives*: Fewer alerts and tickets for security administrators and uninterrupted user productivity

Advanced threat prevention

Provides North-South and East-West protection of cloud assets

Automated network security

Supports rapid deployment, agility and automation of CI/CD workflows

Unified management across AWS environments

Consistent policy to manage security across AWS and hybrid-cloud environments

CLOUDGUARD NETWORK SECURITY
Threat prevention for north-south traffic
Full control over east-west traffic

THREATCLOUD

Combines the latest AI technologies with big data threat intelligence to prevent the most advanced attacks while reducing false positives

* Objective third-party lab tests show CloudGuard Network Security has <u>highest security effectiveness score</u> with 100% block rate, 100% malware prevention, 100% exploit resistance and 0% false positives; Check Point is ranked as a Leader for 22 consecutive years on the <u>Gartner Magic Quadrant for Network Firewall</u>, and has a <u>Recommended rating by NSS Labs.</u>

For more information

For nearly thirty years, Check Point has set the standard for cyber security. Across the ever-evolving digital world, from enterprise networks through cloud transformations, from securing remote employees to defending critical infrastructures, we protect organizations from the most imminent cyber threats.

www.checkpoint.com/cloudguard/amazon-aws-security
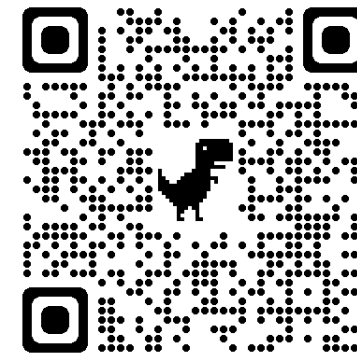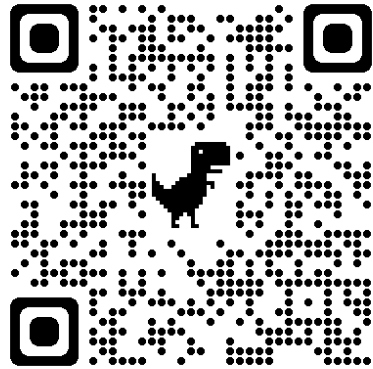
CHECK POINT™

aws Available in AWS Marketplace

**CLOUDGUARD
NETWORK SECURITY**
Firewall and threat prevention

**CLOUDGUARD
POSTURE MANAGEMENT**
Visibility, compliance, and consistent policy enforcement

CLOUDGUARD CIEM
Identity entitlement monitoring, control, and remediation

CLOUDGUARD SPECTRAL
Code and secret scanning

CLOUDGUARD APPSEC
Web application and API protection with contextual AI and no manual tuning

**CLOUDGUARD
WORKLOAD PROTECTION**

Serverless Security
Security of Lambda functions with automated runtime protection and posture management

Container Security
Image assurance and least-privilege access control for Kubernetes clusters and more

CLOUDGUARD INTELLIGENCE
Real-time visibility and threat response

**CHECK POINT
IDENTITY AWARENESS**
Granular visibility of users, groups, and machines

THREATCLOUD
Accurate prevention against the most advanced attacks using AI technology and big data threat intelligence