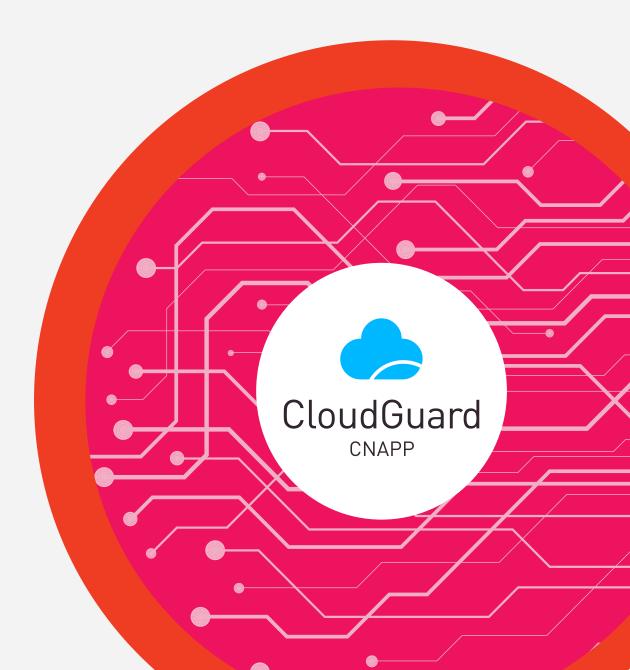


Cloud Native Application Protection Platform

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

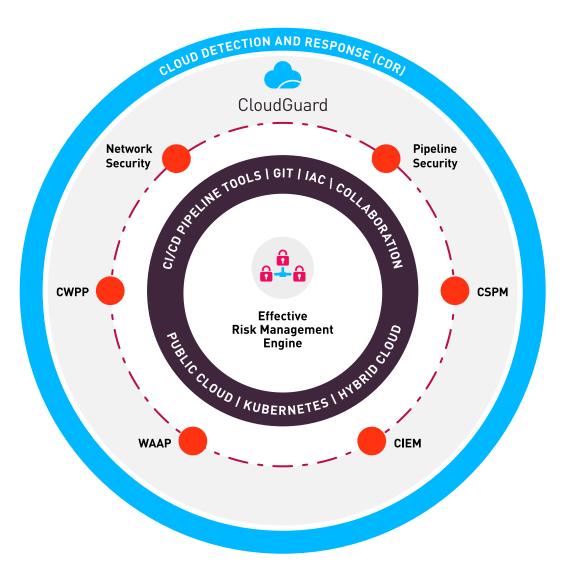


Smarter prevention

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 s 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 Chanw, Information Technology Director of Jebsen Group

•••••



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

CLOUD NATIVE APPLICATION

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.

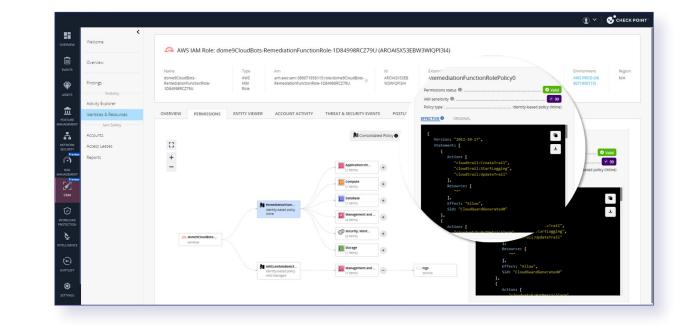
Agentless Workload Posture (AWP) extends CloudGuard's agentless infrastructure visibility into workloads. AWP scans and identifies risks including misconfigurations, malware detection, vulnerabilities and secrets across all cloud workloads including Virtual Machines, Containers and Serverless Functions:

- 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)

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.

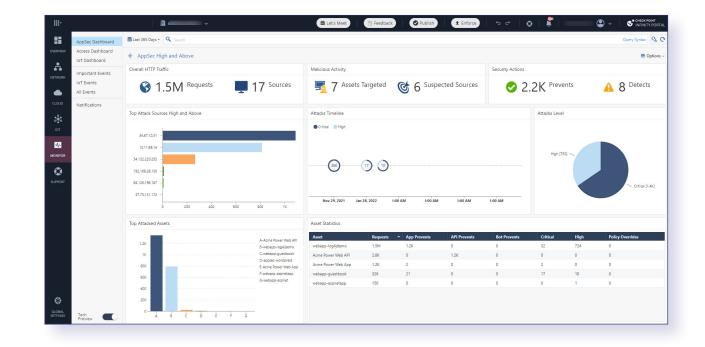
- Achieve zero trust security across applications, APIs, K8s and serverless functions
- Auto-deploy & enforce security controls
- Remain cloud & architecture agnostic with protection on multi and hybrid cloud deployments

											CHECK P
55	Viecome			isk Score	Wenerabilities						
DAEBAICH		+ Add Filter -		sk Score		Malware				₽ Search × Clear	All * Saved
Ē.	Deshooers (Preview)	Snowing 267 of 267 results	.4-aws (19401c10-c		0 0 0 0 0	0	~			Autofit Columns Reset Columns De Export - ()	
DENS .	A0980	second to a to come	-g-kube-aws (19401c10-c		0 0 0 0 0	0	•			water commit	
	Envronments	🗄 Drag here to set row grow	11 .chung-kube-aws (1940)c10-c	9.8	90 278 127 13 76	0	0				
٠	Workloads	Image	mchung-kube-aws (540fc10-c		0 0 0 0 0	0	0	Ratus Registry	Image Tag	Image M Digest	Is Ranning
ASSETS	images	é consec nuntime policy	mchuno-kube-avs (540h:10-c	0.1	4 25 10 0 0	0	0	evapie/deckpoint	1.0.0	0126e4026e6e3Mdb128021e8545603723480x 456058148e72ec8cebee965752e68	
	Image Accurator	Consec-Imagentan-	mchung-kube-avs (\$940%:10-c		15 52 53 13 1	0	0	quay lo (medipoint	2.5.0	Tock20276500564/b500549950024694977 40x0a7210cbc0480b141905a440ar	
1 alian		🖝 amazon-kda-chi		80	0 0 0 0 0			602401143452.dkr.ect.us-east	v1.10.1-eksbuild.1	401533463c87vox29uo4559v0850vc792s1_3stob805524243456491x34481	
NACEMENT	Vuinerabilities	é consec-invento	mchung-kube-aws (1940):10-e			0	0	quay io/theopoint	1.43	41001433c00d7b452aa2140140332743ca7td 7881d0927b8c64a4389969bd035e	
	Rulesets	🖝 consec-admir 🔘	mchung-kube-aws (1940fc10-c		0 0 0 0 0	0	0	quay is/checkpoint	13.0	12454-09193556-0744210-0644-0843-0 86247126685466444197254	
n	Polces	é lube prov O	mchung-kube-avs (1940)c10-c	9.2	2 10 9 1 0	0	0	5 602401143452.dir.ectus-east-	v1212-eksturid2	\$505605645645645656669745844238 0ea6717ec1442764822e/56652e88	
ACCURITY	Acceptment History	é consec-fue O	mchung-kube-aws (1940fc10-c	9.8	93 303 140 15 78	0	0	Sc quaylio/checkpoint	1.6.9-cp	64ed1484829cb364990479821earSa4571eaes 110e526282cb79154c7757c757285	
0	00, Buller	e consecuti	mchung-kube-aws (1940)(:10-c		0 0 0 0 0	0	0	evay lo/theckpoint	1.0.2	945a2b6xa89x2c50c8as4668221724c0x59x a614c823a8cscx9005ba798b4c4a0x	
REK.		e consec-run			0 0 0 0 0	0	0	evay is/thedipoint	0.0.677	9/76a1ccc893aec64c37546172a0664a1/7178a 182eber0a220/3a21eb8/135cr06b8/	
NACEMENT	CI-CD Tool	· Amazon-43	mchung-kube-aws (1940)(c10-c		0 0 0 0 0			34 602401143452.dkr.ecr.us-east	v1.10.1-eksbuild.1	MSM1+ch3902or1+c334+cfb1+d53+edfa0821 6c70af7b/257712105a83+896b2afb	
8		👉 constra 🤘 🔘	mchung-kube-aws (1940fc10-d			0	0	Sc 602401143452.dkr.ecrup-east	v1.84-eksbuild.1	6958c0997ex0360217eb36641d6dc13040_tcd0ebc008ec23ebe46d5d0t8K	
CEM	Rulesets	🖝 consec-flowA	mchung-kube-aws (1940fc10-c		0 0 0 0 0	0	0	g quay is the sport	0.5.2	c124342487443345533686570834r137815_em39c22a821x8b95c99c55445433	
-	Polices	🖝 consec-images 🛛 🔘	mchung-kube-aws (1940fc10-c		0 0 0 0 0	0	0	quey lo/checkpoint	250	exaal/1527e7660308e66254dec36028c157m d02e795ea88c60977e00e79ec325	
0	00, Buller	é consec-surtime	chapp-demp (ec5al541-@19-/	0.0	0 0 0 0 0	0	0	quay is the dipoint	0.27.1-cp-1	059cmc66426315634839674225973c58139 67426729ea0043a41e103836639e	
ORIEGAD		👉 consec-admission-		0.0	0 0 0 0 0	0	0	quay is the oppint	13.1	fa3c10025287da746685bae56573e04895087 101ca15fa186688a15373aae20d15c	
	Excusions	· addon-resper			0 0 0 0 0		v	eugrinigia-release-staging	1.8.10-gim0	063c412851871326256396699647aabelicbk e89971901081c38d89ec46c81687al	
2	Seceness	é fuetit ?	chapp-demo (ec5a0541-6019-4	0.0		0	0	d giagorio	v1.57-pi#2	244aee000773c3478a05ee53x348tee134279 60313%163c77ccs8883Q0348c63c1	
and the second second	Serveriess Runctions	👉 cli-node-driver-registrar	rapp-demo (ecSa8541-4819-4	0.0	0 0 0 0 0	0	•	ed gikegorio	v210-gke3	24/942422236498644453807829438299 fbe94a64fbe5488c7829438217cbd	
(-)	Serveriess CHCD	🖨 consec-imagescan-shim	-demo (ec5a0541-6019-4	0.0	0 0 0 0 0	0	0 Scan	ed quayio/checkpoint	210.0	27)c215dbarkc04x04e81db1x160000e8v 5d81de2282784da3416376dp7b2	
HITLET		🖆 dutter-proportional-autor	cale 0 0 (ec5al541-619-4	92	3 21 12 3 1	0	C Scare	ed giagorio	18.4-pix1	46eec7474718c5457453795c0b286a7c5905 0932ba18663345a33925662242#9	
		👉 Ma-dra-Aube-dra	0 0400	0.4	6 26 16 7 1	0	Stav		1,21,0-gkm0	5440604e13a/Se3660cm1a/Sc570an3a048_6566662ma36666c0349546cc66ee	
۲		 kube-proxy-amd64 	O crapp-dend		0 0 0 0 0		Scarr		v1.21.10-gite 2000	SIC3/738ec1e5773cb/Sbbc53bc0531d80ffe3t	
ETTINGS.		 consec-inventory-agent 	O crapp-dente (ecSalS211)			0 0	Scarv		148	61056414376484571748540508708054566 4da70c62cc607a8e14c74906475e6	
~		prometheus-to-sd	O chapp-demo (ec5a8541-819-	00	00000		Scene		v0.4.2	626686869028139916/7226c5822901683e4666 acabe#03a75e830*10582e87066481	
0		🐓 consec-fluentbit	O chapp-demo (ec5al541-819-		0 0 0 0 0	0 0			1.6.9-cp	64ec81448229cb864bbid75921eaf3a4571eaec 1104/26282cb79154c7757c757285	
ISOURCES		 Outer-proportional-autor 			0 0 0 0 0	0 0			18.1-pix0	6x6dc22b2045b262celbeelb60e985254144 3b600d2e5ee1e6d5fcedbd783b289	
		 gla-metrics-agent 	O chapp-demo (actal/541-619-	0.0	0 0 0 0 0				1.2.0-gka.1	s266732ed0963167sd74246/fe1c432a68d.eB95c82cfs7638c7748a6dosc3eda	
		consec-imagescan-engine	O chapp-demo (ec5al541-819-4		0 0 0 0 0	0 0			2.10.0	a4c377933e0c534c4480ac40ae8087%a4abd 2ct/bee39356eee50c5c5995957498	
		metrics-server-and54	Chapp-demo (acSall541-819-		0 0 0 0 0	0 0	Scen		v0.4.5-gke.0	a4c84005490457ed0359343954b8556da 6e400705456b84080474e8dar	
		é secepte	O chapp-demo (ecSa8541-4819-		0 0 0 0 0	5. 0	Scarv		v03.5-gka.0	aed1o48e882dd0feea264083c0813729966rg_08e808d7ea0020%7cc1279cae4fox	
		prometheus-to-ad	C chapp-demo lacSall541-819-4	0.0	0 0 0 0 0	A (Scent	ed okeoptio	v0.100-pix/0	65010x7601602845x7c17265c36936412dk die12580a401990d5e08ed248dda4	

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.



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
- 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 exposure 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.

shboard Ieta	Scan Summary > fabriziav/spectral-goat			
2708	Asset			canned I
sora dinga GR	fabrizian/spectral-goat Presser & Polec	Issues	Scanned Files	50
	Scan History The table below includes issues that were discovered during this specific scan (angeshot).	102	554	
	Finding	26 32 44	4.667 sec(s)	
	API Key Audit, scclefnahut.ih ● meniptet			/
	Ensure that you are using authorized IP address ranges in order to secure access to the API server uctimuticioud/azure/main.joon		ee live issues	
	Visible AVIS Key Incibackerdi sploader.go Investigate		[61001]	
	Visible Google API Key sc/lefra/google-splj.con • Investgate	1	code/infra	
	Ensure EBS volume encryption is enabled scrimulicioud/cloud/invalues/sent	1	code/infra CLEFRMOR	1

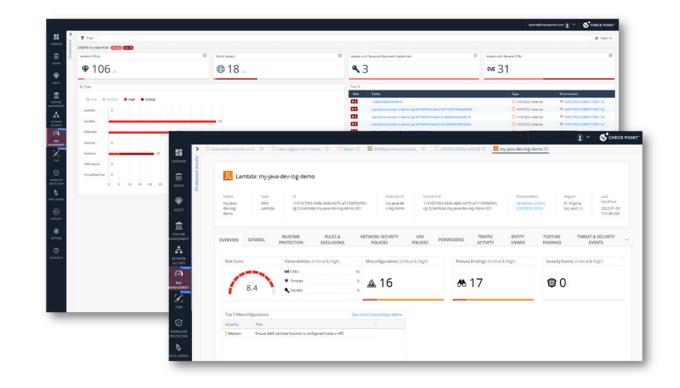
CloudGuard shift-left functionality seamlessly integrates seamlessly integrates into the CI/CD pipeline to scan code, automate protection, detect malware, and eliminate blind spots.

- 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

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.

100 m 1 1									
AWS Default	Search		Search Environment	s 👻 🐣 Home Dashboard 👻					
Azure Default	~ INVENTORY								
GCP Default	MONITORED ENVIRONMENTS	INVENTORY O	TOP PROTECTED ASSETS	PROTECTED ASSETS PER PLATFORM					
Home Dashboard				GCP					
Kubernetes Default	aws 37 🔥 11	236,424	1. 9 GCP IAM Role 219,968	• AWS					
Serveriess Default	🔷 191 🛛 🥘 34		2. 🕈 Azure Role Definition 2,615	Azure					
Favorites	C) 1 (+) 57	Total Protected Assets	3. X GCP Route 1,631	Kubernet Alibaba					
	d 15		4. 🔯 AWS Log Group 1,321	▲ 1/2 ▼					
	TOP ENTITIES BY HIGH SEVERITY ALERTS COUNT	ENVIRONMENTS WITH HIGH SEVERITY ALERTS	STORAGE WITH HIGH SEVERITY ALERTS	SECURITY GROUP WITH HIGH SEVERITY ALERTS					
			17	11					
	1. 🔹 guay.io/siamaksade/spring-petclinic:latest(1,330	1. Openshift-cta (c6090906-a3a0-4b9d-b4d823,784	1. esti-bucket (esti-bucket) 113	1. ① dome9-exercise-sg (sg-0423d72d8180e8dcb)					
	2 602401143452.dkr.ecr.us-east-2.amazona 1.250		2. d9d9permissionsbucket5 (d9d9permissionsb 81	2 default (se-Occab4c8c4bc2b3e4)					
	 602401143452.dkr.ecr.us-east-2.amazona 1.211 	3. 509	3. dentless-demo-bucket (agentless-demo-buck77	3. 🕥 launch-wizard-3 (sg-f377348a)					
	4	4. 201 Ililei-Dev (196159408806) 3,468	4. test-open-write-all-roy (test-open-write-all-roy) 74	4. 1 launch-wizard-9 (sg-63acd713)					
	5. Checkpoint.azurecr.io/container-demo:v1(51 791	5. M AWS Stage (726853184812) 3,067							
	 6. rolandopcp/testcentosapp:v1(7f5b34059cfb 444 	6. G GCP prod (tullenv-149408) 3,038	USER WITH HIGH SEVERITY ALERTS	COMPUTING WITH HIGH SEVERITY ALERTS					
	7. ghcr.io/christophetd/log4shell-vulnerable-ap 398		1. A N/A 347	1. 🖸 i-0338fbde03510fd8f (i-0338fbde03510fd8f) 8					
	gncr.io/cnristopnetd/log4snell-vulnerable-ap598 i-0f995fed0a188f655 (i-0f995fed0a188f655) 395	 7. mcnung-kube-aws (1940tc10-d9ec-43/1-ad 2,776 8. Morocco (549639478491) 2.404 	2. A Leonid (AIDARICSJ2KJVD673DB5E) 43	2. 🖸 i-0f995fed0a188f655 (i-0f995fed0a188f655)					
	9. 8 N/A 347	 Morocco (549639478491) 2,404 Azure prod (6863828a-3f21-4624-9b05-4e52,213 	3. A Hillel (AIDAS3LADBKTK53KHQQCL) 39	3. 🖸 i-0338fbde03510fd8f					
			1. A daboss (AIDAVWWGTFUBJB7QP3XTW) 28	4. 🖸 i-0f995fed0a188f655					
	10. 🥗 N-A (N-A) 333	10. M Serverless_Demo (293247823395) 1,910							
	~ INTELLIGENCE								
	TOP CRITICAL ALERTS	TOP ENTITIES WITH CRITICAL ALERTS	ALERTS TRENDLINE	Jamle from Check Point CloudGuard					
			ALERTS TRENDLINE	Hi Andrei, Check Point continues to develop i					
	1. ACME-Malicious 20	1. Comparing 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1.		1. de features to enhance our customers' experient					

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.





"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 lifecyle, 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

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

© 2024 Check Point Software Technologies Ltd. All rights reserved.

