



Por que o gerenciamento e visibilidade na nuvem é necessário?

Henrique Sauer e Helio Leite

Security Engineers - Brasil

Abril 2024

YOU DESERVE THE BEST SECURITY

Agenda

- Sobre a Check Point;
- Cloudguard;
- CNAPPP;
- Demo;

Sobre a Check Point

Check Point: The Leading Global Cyber Security Company

Global Leader

100,000+ Customers,
88+ Countries, 6,200+ Partners

Cutting-Edge Technologies

Over 30 Years Of Expertise,
Industry's Most Visionary Player

Innovation Leadership

Highest Number Of AI Real-time
Prevention Techniques

6,500+

Employees Worldwide, Top
Talent

Traded on Nasdaq

1996 | CHKP

World's Best Employer

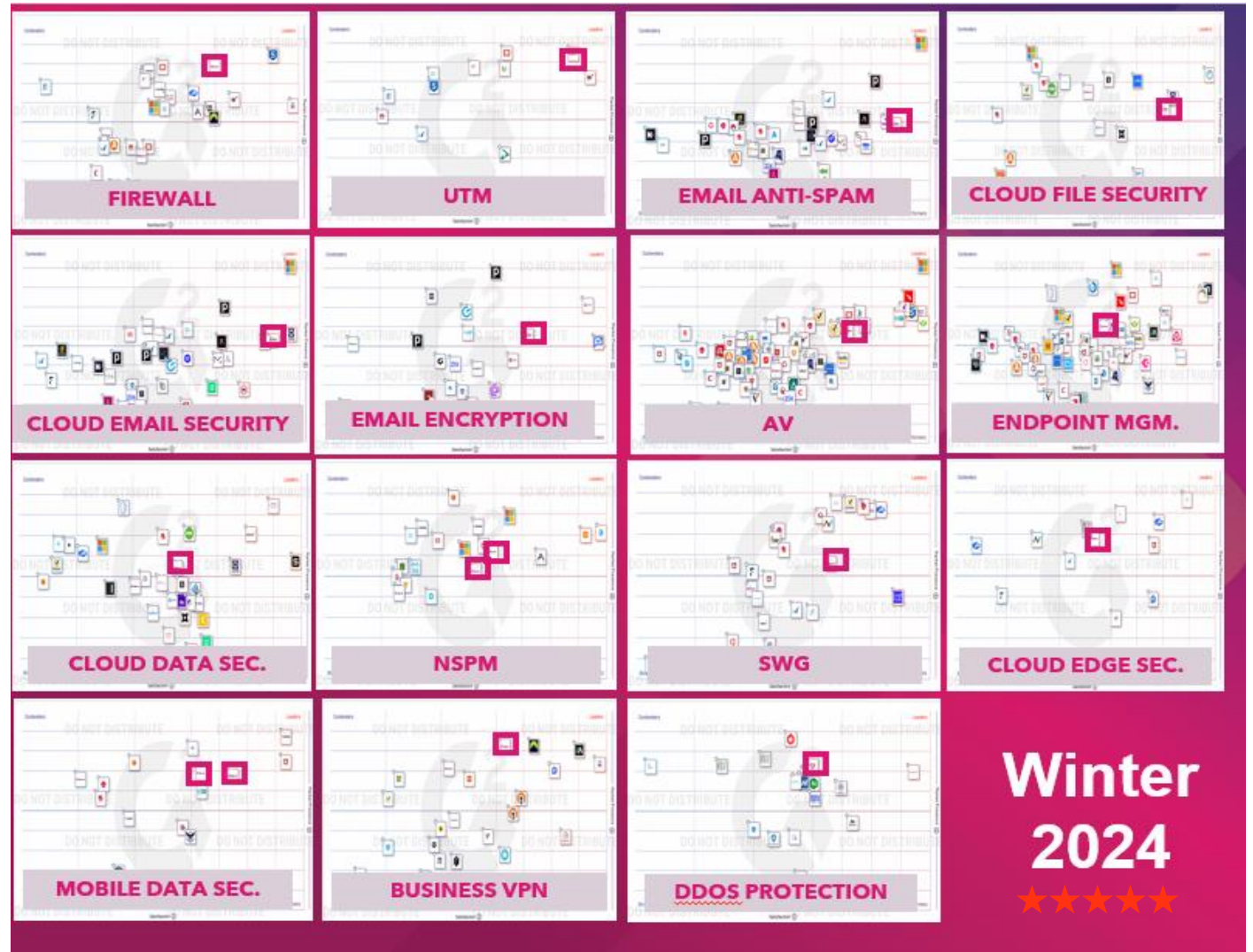
By Forbes,
#1 Cyber Security Vendor



Mais de 1,900 Customer Reviews Leader em 15 Categories!



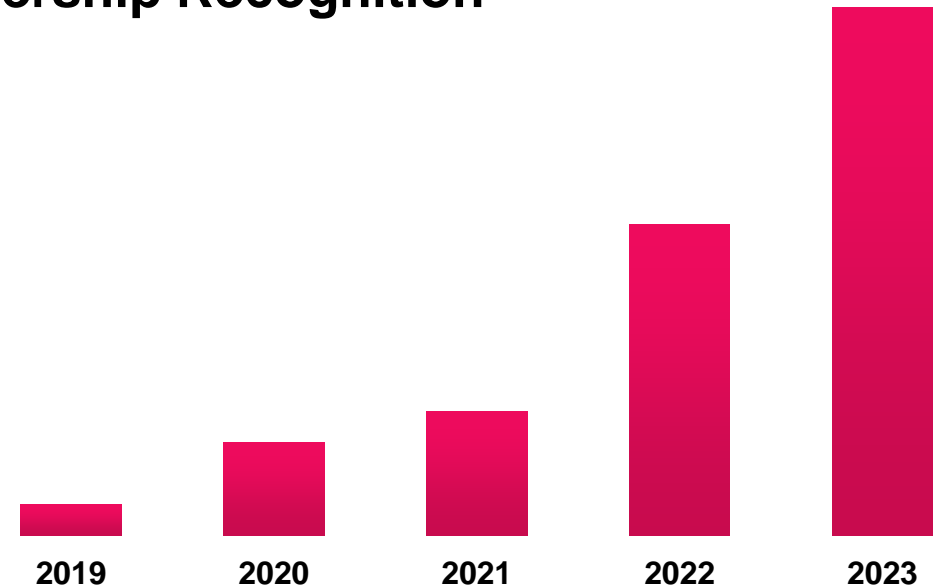
An Achievement
Second to None.



Reconhecimento de Liderança por Analistas do Setor

- Endpoint Security
- Next Gen Firewall
- Zero Trust Platforms
- Cloud Network Security
- Enterprise Email Security
- Cloud Workload Protection
- Cloud Posture Management
- Secure Access Service Edge
- Extended Detection and Response (XDR)

Increasing Our Leadership Recognition



FORRESTER

OMDIA

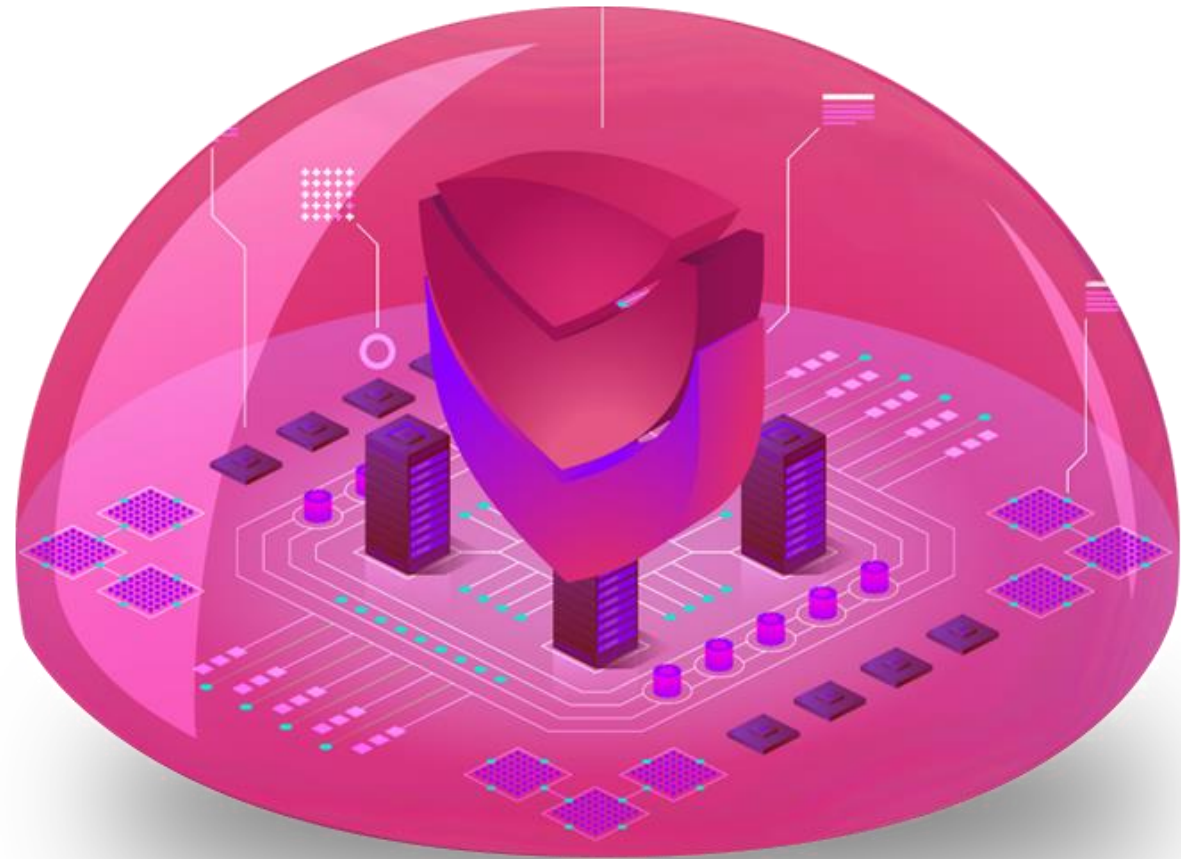
FROST & SULLIVAN

GIGAOM

The Check Point Ethos

Prevention Not Detection

Uma vez que o malware está dentro, já é tarde demais!



Check Point 2024

The Platform Company



AI-Powered

Cloud-Delivered

Comprehensive

Consolidated

Collaborative

Real-Time Threat Prevention



90+

Engines de
Segurança

50+

são AI-Powered

3B

Ataques Prevenidos
por ano

<2 Sec

Sincronizado globalmente
para todos os pontos de
aplicação de políticas



Segurança Colaborativa - ThreatCloud AI

IA é sobre dados!



Big data threat intelligence:

2,800,000,000
Websites and files inspected

146,000,000
Full content emails

53,000,000
File emulations

20,000,000
Potential IoT devices

2,600,000
Malicious indicators

1,500,000
Newly installed mobile apps

1,200,000
Online web forms

Counted
DAILY!

AI-Powered Platform

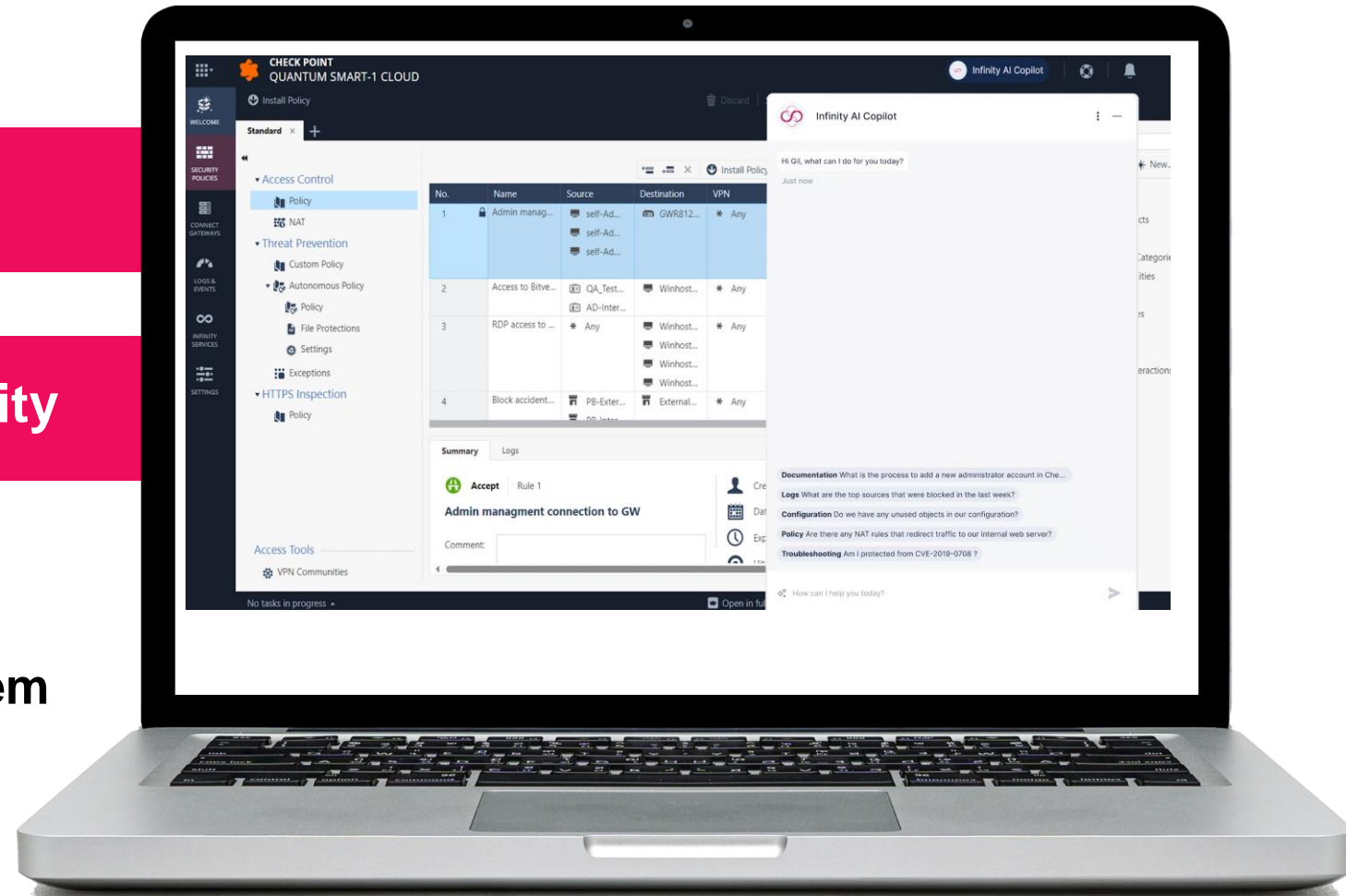
Gerenciamento de Segurança 10X mais efetivo



Powerful, Generative-AI tool

Embarcado na Plataforma Infinity

Gerenciamento de política,
troubleshooting e recomendações **em segundos.**



Check Point Infinity Platform

Level-up Your Security With 3cs of the Best Security



Comprehensive

Prevenção em todos os vetores de ataque

- Da codificação à nuvem, redes, usuários, e-mail e IoT

Consolidated

- Gerenciamento Unificado
- Operações de segurança unificadas para todo o seu conjunto de segurança

Collaborative

Melhores motores de segurança facilmente aplicados a qualquer vetor de ataque

- Inteligência de ameaças compartilhada em tempo real

Api-based, integrado com terceiros

Check Point Infinity Platform



AI-Powered. Cloud-Delivered.



Check Point

Quantum

Secure the Network



Check Point

CloudGuard

Secure the Cloud



Check Point

Harmony

Secure the Workspace




Infinity Core Services

Collaborative Security Operations & Services

SECURE THE ENTERPRISE

AI-Powered. Cloud-Delivered.




SECURE THE NETWORK




Quantum

SECURE THE CLOUD



CloudGuard

SECURE THE WORKSPACE



Harmony



Infinity Core Services
Collaborative Security Operations & Services

Security Operations and AI		Global Services	
• XDR/XPR	• ThreatCloud AI	• Managed Services	• Professional Services
• Playblocks	• AI Copilot	• MDR/Incident Response	• Security Architecture
• Events			• Training

SECURE THE ENTERPRISE

AI-Powered. Cloud-Delivered.



NEW

SECURE THE NETWORK



Maestro
Hyperscale Data Center

VPN
Virtual Private Remote Access

Gateways
Enterprise Firewalls

SD-WAN
Optimized Connectivity

Spark
SMB Suite

Rugged
ICS Security

DDoS Protector
Block DDoS Attacks

IoT Protect
IoT Security

Smart-1 Cloud
Security Management

SECURE THE CLOUD



Network
Cloud Access Control and Prevention

WAF
Web Application Firewall

Cloud Native Application Protection (CNAPP)
Unified Security from Code to Cloud

Cloud Detection and Response
Contextual and Actionable Intelligence

SECURE THE WORKSPACE



SASE
Internet Access Private Access

Email
Cloud Email and Collaboration Suite Security

SaaS
Threat Prevention for SaaS Applications

Endpoint
Protection & Posture Management

Mobile
Mobile Threat Defense

Web Browser
Prevent Internet Threats and Data Loss

COLLABORATIVE SECURITY OPERATIONS & SERVICES



Security Operations and AI

XDR/XPR
Extended Prevention and Response

Playbooks
Orchestration and Automation

Events
Unified Events

ThreatCloud AI
AI-Powered Threat Intelligence

AI Copilot
Automating Security with AI

MDR/MPR
Managed Prevention and Response

Incident Response
Keep Your Business Running

Consulting & Training
Leverage security architecture design experts

Global Services



Secure the Cloud

AI-Powered. Cloud-Delivered.



Web Application Firewall

Network security

CNAPP

CHECK POINT É CLOUD SECURITY

PROTEGENDO MAIS QUE 4,000 CLIENTES COM CLOUDGUARD

MAIS QUE
500
cloud experts

1 em 4
Dos globais
Fortune 500

1 em 3
dos maiores
bancos do
mundo

1 em 5
Das empresas top
de varejo

TRUSTED BY



LÍDER EM CLOUD SECURITY



Detection & Smart Protection



Continuous Code to Cloud Security & Policies



Enterprise Risk Management

LEADER IN CLOUD NETWORK
SECURITY

Gartner GIGAOM

LEADER IN CLOUD NATIVE
APPLICATION PROTECTION

Gartner FROST & SULLIVAN

LEADER IN WEB APPLICATION & API
PROTECTION

GIGAOM

LEADER IN CLOUD WORKLOAD
PROTECTION

FORRESTER FROST & SULLIVAN

LEADER IN CLOUD SECURITY
POSTURE MANAGEMENT

GIGAOM

LÍDER EM CLOUD SECURITY



Detection & Smart Protection



Continuous Code to Cloud Security & Policies



Enterprise Risk Management

CLOUD RUNTIME PROTECTION



Cloud Network Security (CNS)

LEADER: GigaOm Radar

FIRST: Gartner Critical Capabilities NGFW
Public Cloud Security



Web Application & API Protection (WAAP)

LEADER: GigaOm Radar Report



Cloud Workload Protection Platform (CWPP)

LEADER: Frost & Sullivan Radar

LEADER: Forrester Wave



Cloud Detection and Response (CDR)

CLOUD INFRASTRUCTURE SECURITY



Cloud Native Application Protection
Platform (CNAPP)

RECOGNIZED: Gartner Market Guide

LEADER: Frost & Sullivan Radar Report



Cloud Security Posture Management (CSPM)

LEADER: GigaOm Radar



Cloud Infrastructure & Entitlement
Management (CIEM)



Data Security Posture Management
(DSPM)

CODE SECURITY



Infrastructure as Code Scanning
(IAC)



Software Composition Analysis
(SCA)



Code Scanning

CNAPP

Gartner's Cloud Native Application Protection Platform

Conjunto Integrado de Capacidades de Segurança e Conformidade projetado para ajudar a **proteger e garantir a segurança de aplicações nativas de nuvem** durante o desenvolvimento e a produção.

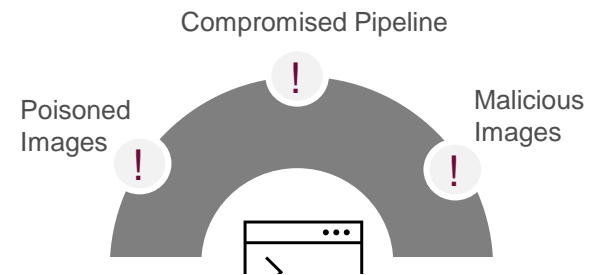
CNAPPs consolidam várias capacidades anteriormente isoladas, incluindo:

- Varredura de contêineres
- Gerenciamento de postura de segurança em nuvem (CSPM)
- Varredura de infraestrutura como código
- Gerenciamento de privilégios de infraestrutura em nuvem
- Plataformas de proteção de carga de trabalho em nuvem em tempo de execução

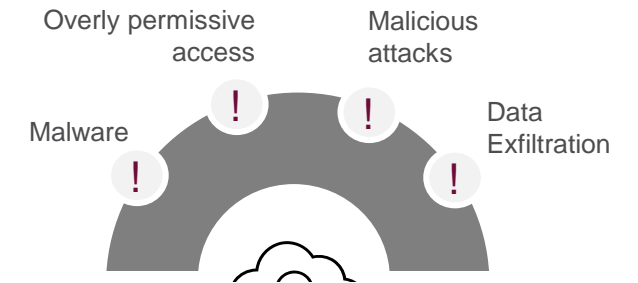
Gartner[®]

Gartner's Cloud Native Application Protection Platform

Deploy



Run



MAPPING OF CLOUDGUARD CNAPP CAPABILITIES AGAINST REQUIREMENTS OF 2023 GARTNER MARKET GUIDE FOR CLOUD-NATIVE APPLICATION PROTECTION PLATFORMS

CNAPP Core Capabilities


- Runtime visibility into virtual machines (VM) and container workloads
- Cloud security posture management, including all leading hyperscale providers and their managed Kubernetes offerings (Kubernetes security posture management [KSPM])
- Infrastructure as code (IaC) scanning, including for major IaC scripting languages and YAML/Helm for Kubernetes
- Cloud infrastructure entitlement management
- Network connectivity mapping
- Scanning of containers and container registries for risk: configuration, vulnerabilities, secrets, attack path analysis
- Software composition analysis, including software bill of materials (SBOM) creation

CNAPP Recommend Capabilities


- Real-time workload visibility from the inside for critical VMs and containers including workload detection/response
- API discovery and scanning for correct configuration in development
- API discovery in development and monitoring at runtime
- Scanning of unstructured IaaS data repositories for risk sensitive data in structured data repositories and malware scanning:
- Network monitoring capabilities
- Workload detection and response
- Expanded cloud detection and response (CDR) capabilities beyond just workload monitoring (for example, looking at event logs, network logs and DNS lookups)
- Drift detection from expected state
- Support for other common clouds - Oracle, IBM, Alibaba Cloud, Tencent
- Scanning of other application artifacts for risk*
 - VMs
 - Serverless functions

CNAPP Optional Capabilities

- Application runtime self-protection (RASP)
- Serverless function instrumentation and monitoring
- Application layer observability/monitoring
- Support for VMware-based infrastructure (on-premises and public-cloud-based)
- Support for other cloud and container environments such as Red Hat OpenShift and SUSE's Rancher
- Support for policy-as-code scanning
- Support for Open Policy Agent
- MicroWAF/web application and API protection (WAAP) at runtime
- Scanning of IaaS structured data repositories for risk: sensitive data in unstructured data repositories and custom code for unknown vulnerabilities
 - Traditional static analysis of custom code for unknown vulnerabilities
 - Traditional dynamic scanning for unknown vulnerabilities
- API scanning for unknown vulnerabilities
- Development pipeline/software supply chain security beyond SCA
- Development pipeline hardening

 CloudGuard Capability

 CloudGuard Roadmap

 Text – not supported



O que é um CSPM?

CSPM

Cloud Security Posture Management (CSPM), conforme definido pelo Gartner, é “um processo contínuo de melhoria e adaptação da segurança em nuvem para reduzir a probabilidade de um ataque bem-sucedido”.

No cerne do CSPM está a **detecção de vulnerabilidades de configuração incorreta** em nuvem que podem levar a violações de conformidade e violações de dados.

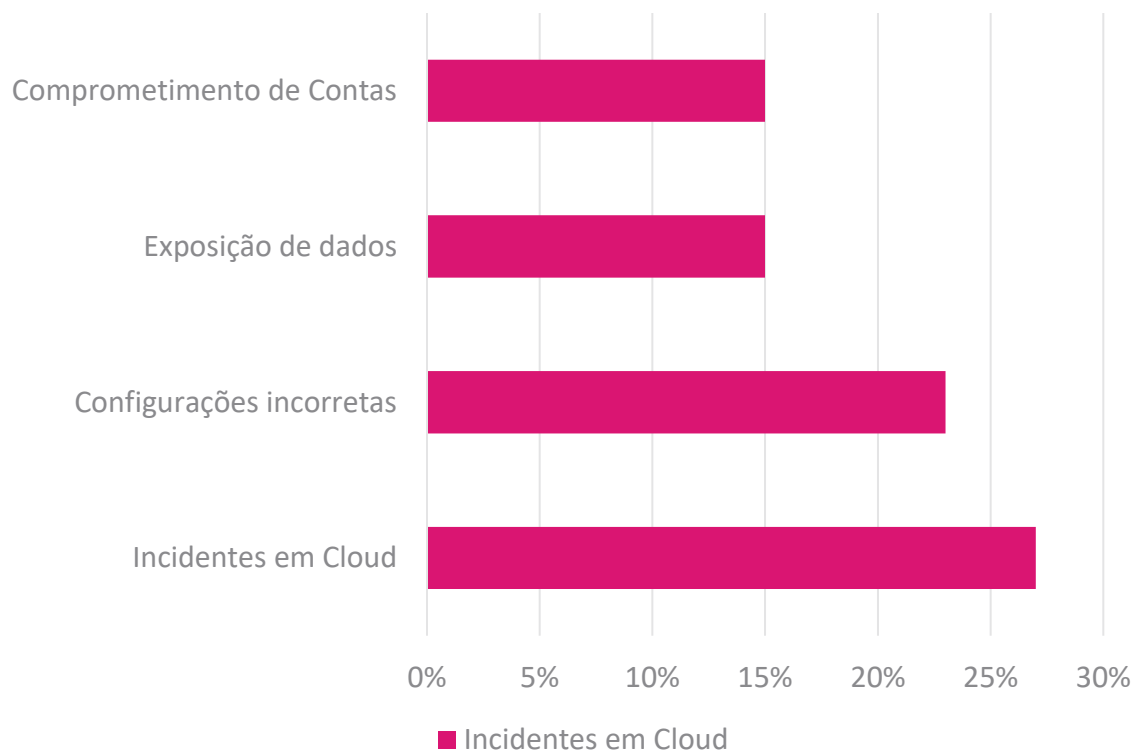
- **Visibilidade contínua** de ambientes multi-nuvem para identificar vulnerabilidades de configuração incorreta em nuvem.
- Capacidade opcional de **realizar remediação automatizada** de configurações incorretas para garantir conformidade contínua e proteger serviços críticos em nuvem.
- **Utilização de frameworks** do mercado como CIS Foundations Benchmarks, SOC 2, PCI, NIST 800-53 ou HIPAA, para verificar que as configurações estão em conformidade¹

Gartner[®]

De acordo com Gartner

- De fato, a segurança em nuvem é uma responsabilidade compartilhada entre os provedores de nuvem e os clientes. **A citação “Até 2025, mais de 80% das falhas de segurança em nuvem serão culpa do cliente”** destaca a importância de os clientes adotarem práticas de segurança sólidas ao usar serviços em nuvem.

Incidentes de Segurança



Devs urged to rotate secrets after CircleCI suffers security breach

John Leyden 05 January 2023 at 14:38 UTC
Updated: 06 January 2023 at 10:09 UTC

Data Breach Cyber-attacks DevSecOps



DevOps platform advises customers to revoke API tokens



AWS patches bypass bug in CloudTrail API monitoring tool

Charlie Osborne 23 January 2023 at 13:01 UTC

Vulnerabilities Cloud Security API



Threat actors poking around AWS environments and API calls could stay under the radar

Vulnerability in AWS AppSync allowed unauthorized access to cloud resources

Ben Dickson 25 November 2022 at 10:22 UTC
Updated: 25 November 2022 at 11:17 UTC

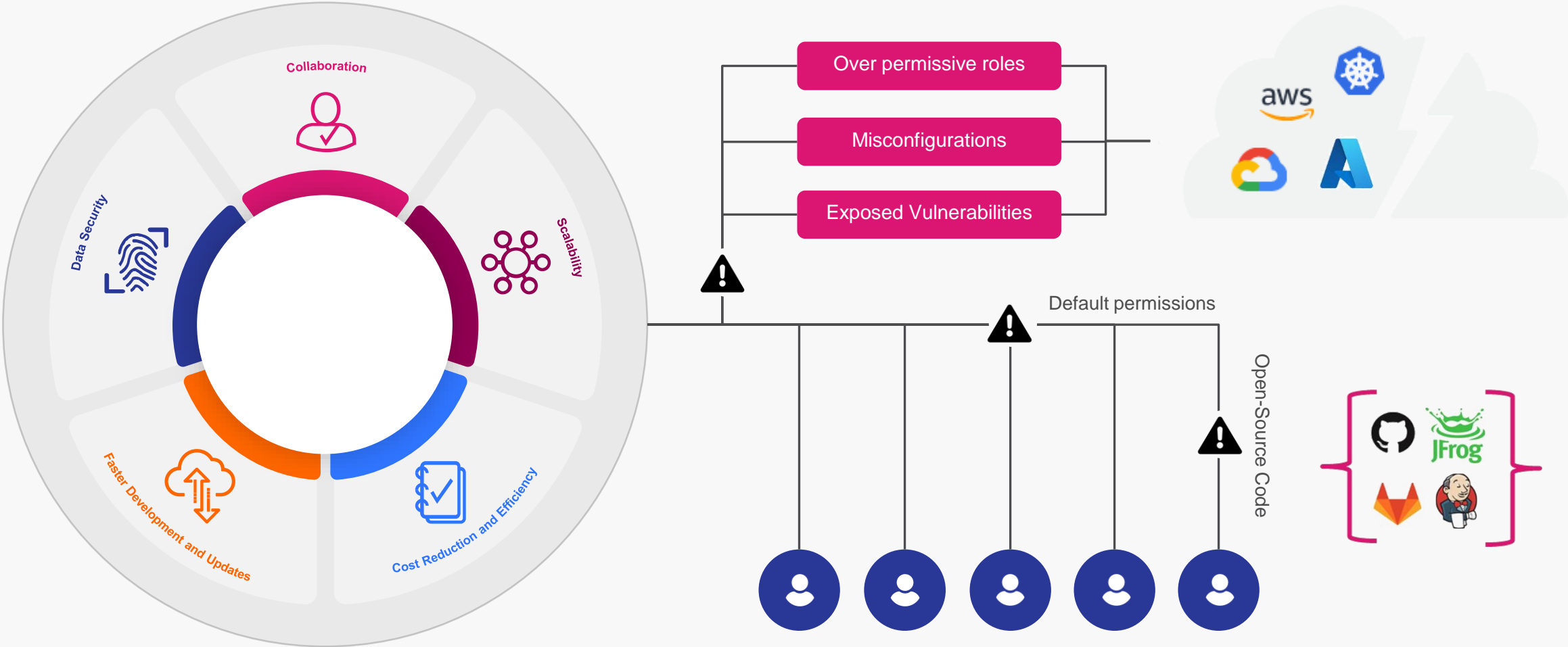
Vulnerabilities Research Cloud Security

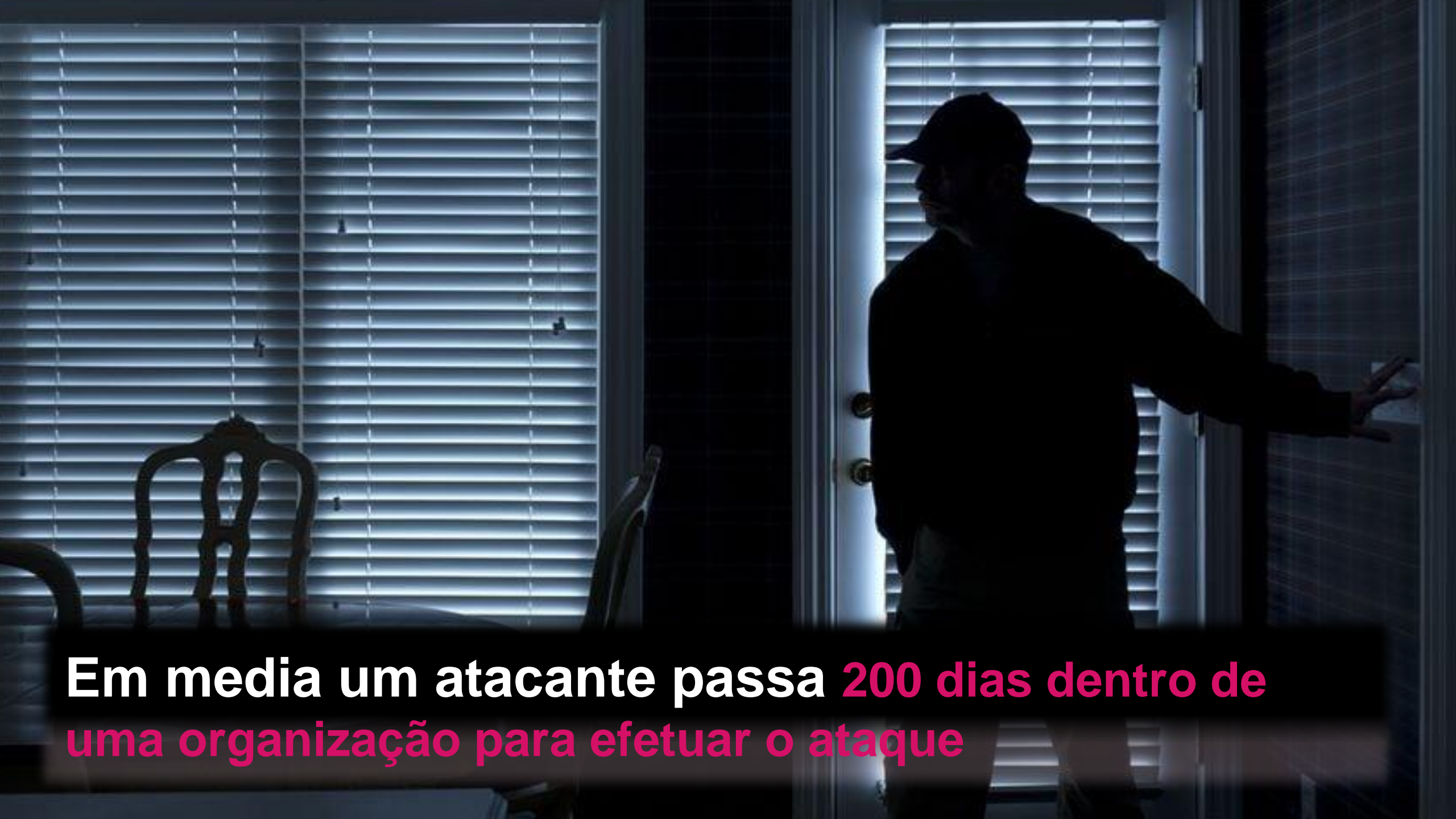


Attackers could gain full control of a cloud-hosted database



MAIS VELOCIDADE PARA DEV= MAIS RISCOS PARA SEC





Em media um atacante passa 200 dias dentro de uma organização para efetuar o ataque

DEPLOY SEPARATE TOOLS TO FIX ISSUES

Misconfigured Code



IAC Security & Code Scanning

Overly Permissive Users



Cloud Entitlement Management

Compliance & Misconfigurations



Cloud Posture Management

Threat Monitoring



Cloud Detection & Response

Malware & Vulnerabilities



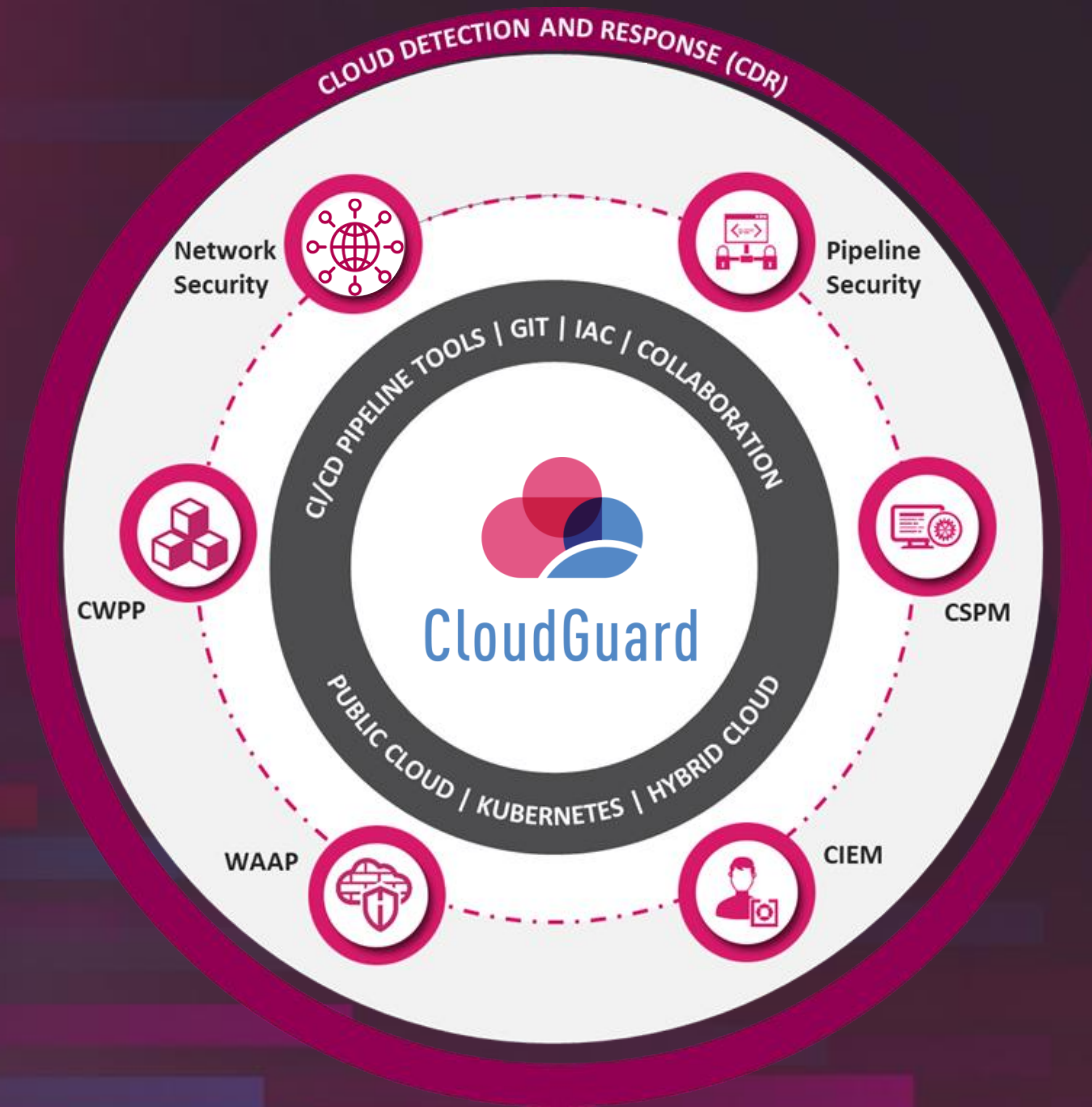
Container & Agentless Scanning

Web, API, & Bot Attacks



WAF, API SecGW & Bot Mitigation

Complicated
Too Many
Security
Alerts
Management





CloudGuard

More **Context** – Actionable **Security** – Smarter **Prevention**

1 Obtenha insights mais profundos e visibilidade ampliada.

Cloud Security Posture Management with Agentless Workload Posture

2 Compreender as permissões e privilégios

Cloud Infrastructure Entitlement Management

3 Identificar problemas de Segurança no pipeline

Shift-Left Pipeline Security powered by Spectral

4 Priorizar riscos em toda a sua infraestrutura de nuvem

Effective Risk Management Engine

PREVENTION-FIRST CNAPP IN ACTION

More **Context** – Actionable **Security** – Smarter **Prevention**



Mais Contexto

O CloudGuard examina todo o ambiente em nuvem para identificar riscos de segurança, compreendendo o caminho do ataque e o impacto da exposição para o negócio, a fim de aplicar medidas de segurança acionáveis - contextualmente.

Security Findings

Contextual Inputs

Business Impact

Attack Path

Vulnerability identified in store-front application code in development

Unencrypted storage found, linked to an externally-facing, crown-jewel web-server using default Admin Role policies with no WAF protection

Secrets found in GitHub repository that has been shared

Weak password configured on lab management console

PREVENTION-FIRST CNAPP IN ACTION

More **Context** – Actionable **Security** – Smarter **Prevention**

2. Actionable Security

Em vez de analisar um milhão de descobertas, destaque os riscos e ameaças mais críticos em ambientes de nuvem, cargas de trabalho e código.

Armazenamento não criptografado encontrado, vinculado a um servidor web de joia da coroa voltado para o exterior, usando políticas de função de administrador padrão sem proteção de WAF.

Segredos encontrados em repositório do GitHub que foi compartilhado

Vulnerabilidade identificada no Código da aplicação

Senha fraca configurada na console de gerenciamento do lab

9.8 Misconfigured Crown-Jewel Workload

9.3 Overly Permissive Role

9.2 Secret in shared repository

8.1 Vulnerable Code

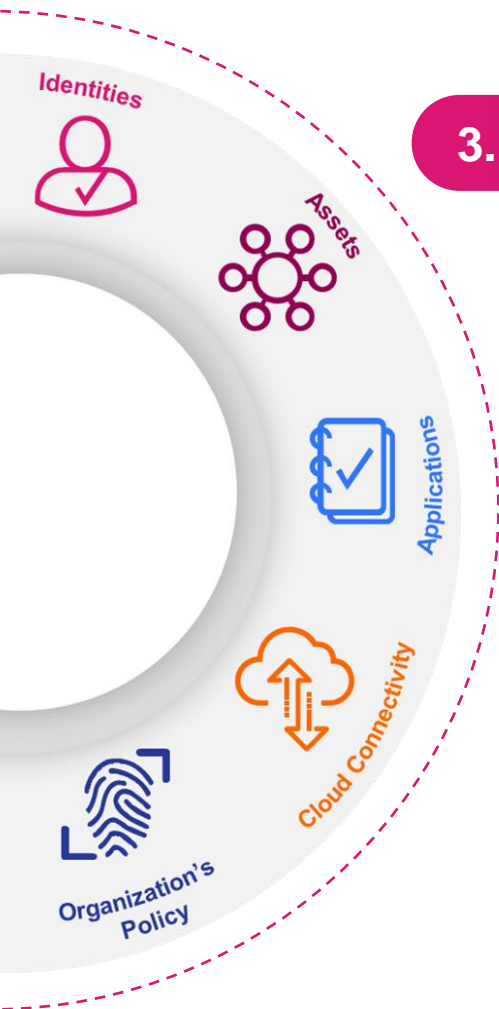
7.1 Weak Passwords in Lab Admin Console

Remediation
Urgency



PREVENTION-FIRST CNAPP IN ACTION

More **Context** – Actionable **Security** – Smarter **Prevention**



3. Smarter Prevention

Prevenção eficaz com o caminho mais rápido para resolver problemas de segurança — combinando prevenção em tempo de execução e orientação inteligente para remediação ao longo de todo o ciclo de vida da aplicação

9.8 Misconfigured Crown-Jewel Workload

9.3 Overly Permissive Role

9.2 Secret in shared repository

Misconfigured Workload:

Automatic Remediation: CloudGuard automatically turned-on encryption on storage bucket using CloudBots

Overly Permissive Role:

Suggested Remediation: CloudGuard recommends a least-permissive model for existing role

Secret Left Behind:

Suggested Remediation: CloudGuard recommends removing secret from code artifact

Unauthorized Access:

Automatic Prevention: CloudGuard automatically blocked an attempt to execute and unauthorized process on serverless functions

DASHBOARD

CHECK POINT CloudGuard cp-all-demo

What's New 1

Henrique Sauer

Overview > Home Dashboard

Search

+ Add Dashboard Add Section Rename Dashboard Clone Dashboard Delete Dashboard Export to PDF Default Public Pinned Show hidden widgets

Home Dashboard

Monitored environments

Alibaba	1	AWS	9
Azure	5	Container Registry	19
GCP	3	Kubernetes	45
ShiftLeft	12		

Protected Assets

49,074

Top Protected Assets

AWS ResourceAccessManager Permission	14,478
AWS IAM Policy	10,858
GCP IAM Role	4,712
Azure Role Definition	2,471
AWS ElastiCache Parameter Group	2,298

Protected Assets Per Platform

AWS	35,545
GCP	5,745
Kubernetes	3,716
Azure	3,676
Alibaba	336
other	56

HIGH SEVERITY ALERTS

Top entities by high severity alerts count

<root_account> ()	146
nginx-deployment (1b5c0987-a5e2-45b1-97df-a111f280a...	81
602401143452.dkr.ecr.eu-west-1.amazonaws.com/amazo...	75
N-A (N-A)	73
nginx:1.14.2(sha256:295c7be079025306c4f1d65997cf7a...	63
602401143452.dkr.ecr.eu-west-1.amazonaws.com/amazo...	57
N-A (N-A)	56
m3tr0x/avivm-sushi:0.0.2(sha256:d3346f9fd5b72acd2bf...	55
ab160590b5 (/subscriptions/8773790e-f751-4649-a5d9-...	55
ab1605a262 (/subscriptions/8773790e-f751-4649-a5d9-...	55
ab1605be01 (/subscriptions/8773790e-f751-4649-a5d9-...	55
defaultresourcegroua156 (/subscriptions/8773790e-f751-...	55

Environments with high severity alerts

AWS Demo - Read Only account	11,918
AWS ERM Demo	1,586
ERM Azure Demo	1,522
chkp-aws-rnd-ldoy-base	987
k8s-demo	967
177547828516	805
chkp-aws-sales-cslab2-base	539
chkp-aws-rnd-cg-nirfi-base	504
chkp-aws-rnd-niraz-base	476
GCP-PROD	462
other	3,389

Storage with high severity alerts

ab160590b5 (/subscriptions/8773790e-f751-4649-a5d9-...	55
ab1605a262 (/subscriptions/8773790e-f751-4649-a5d9-...	55
ab1605be01 (/subscriptions/8773790e-f751-4649-a5d9-...	55
defaultresourcegroua156 (/subscriptions/8773790e-f751-...	55
customeraccountItems (/subscriptions/8773790e-f751-46...	54

Security group with high severity alerts

OverOverPermissive (sg-06c1f235d70fb3bc1)	32
launch-wizard-9 (sg-63acd713)	32
launch-wizard-3 (sg-f377348a)	31
Quick_Start_002 (sg-0928c166)	30
eksctl-stanislavz-consec-ci-demo-nodegroup-ng-3b78a5...	28

User with high severity alerts

<root_account> ()	146
daffyg (62750bd7-d9bc-469a-9bd1-faf0b2c6e68b)	16
attacker (AIDARICSJ2KJ6ZRS5GFMX2)	12
stanislav (AIDASSVM3USAYN2QVPQX)	12
omark (AIDASSVVM3USDUCAADL7K)	11

Computing with high severity alerts

scheduler-prod (i-0edd4494150e615cd)	23
123 (i-0144c62dc29cb751f)	21
PROD-DB-WITNESS-01B (i-8fe41902)	21
simulator-Webserver (i-06b5e4c39a96fb9db)	20
Mongo1-prod (i-034a479c67ad51381)	19

INTELLIGENCE

Top Critical Alerts

dns traffic	29
Outbound Traffic to Malicious IP Addresses	4

Top Entities With Critical Alerts

asset-mgmt-admission-policy-767fc87fb-7hw4d (337a9...	1
asset-mgmt-imagescan-engine-69c8dd4fc7-gs7pc (455...	1
asset-mgmt-admission-enforcer-68497855c8-bgc96 (4b...	1
coredns-7cc879f8db-xdnmg (54490ed6-59dc-4930-ba4...	1
asset-mgmt-imagescan-daemon-nqc7v (f6ca6132-98c3-...	1

Alerts Trendline

Top Failed Actions

GetBucketTagging	14,637
GetBucketLifecycle	14,203
GetBucketReplication	13,894
GetBucketObjectLockConfiguration	13,835
GetBucketWebsite	13,641

CHECK POINT

©2023 Check Point Software Technologies Ltd. 37

COMPLIANCE

CHECK POINT CloudGuard cp-all-demo What's New Henrique Sauer

Search

Overview
Risk Management
Events
Assets
CSPM
Welcome
Rulesets
Continuous Posture
Remediation
Exclusions
Assessment History
GSL Builder
Posture Overview
Network Security
CIEM
Workload Protection
CDR
Code Security
Reports
Settings
Resources

Showing 254 of 508 results

Rule Name	Rules	Policies	Provider
Alibaba CIS Foundations Benchmark v1.0.0	49	NO	Alibaba
Alibaba HIPAA	84	NO	Alibaba
Alibaba ISO 27001:2022	84	NO	Alibaba
Alibaba NIST SP 800-53 R5	84	NO	Alibaba
Alibaba PCI DSS v4	84	NO	Alibaba
Alibaba SOC 2 (AICPA TSC 2017 Controls)	84	NO	Alibaba
Arnfinn	4	NO	Arnfinn
AWS ACSC ISM	610	NO	AWS
AWS ASD Essential Eight	76	NO	AWS
CIS	48	NO	AWS
AWS CIS Foundations Benchmark v1.3.0	52	NO	AWS
AWS CIS Foundations Benchmark v1.4.0	55	NO	AWS
AWS CloudGuard Network Management	2	NO	AWS
AWS CloudGuard Network Security Alerts	29	NO	AWS
AWS CloudGuard S3 Bucket Security	22	NO	AWS
AWS CMMC 2.0 v1.02	354	NO	AWS
AWS CRI Profile v1.2	67	NO	AWS
CSA	95	NO	AWS
AWS CSA CCM v3	95	NO	AWS
AWS CSA CCM v4	245	NO	AWS
AWS Dashboard System Ruleset	14	NO	AWS

Previous 1 2 3 4 5 Next

Showing 1 to 20 of 254 items

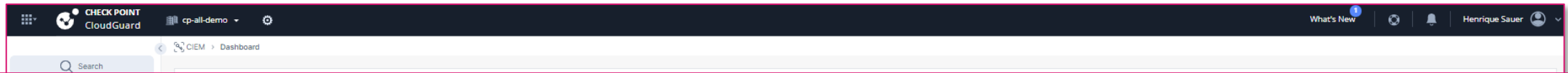
MORE CONTEXT



Drag here to set row groups

Risk	Entity	Platform	Type	Environment	Is Ru...	Business Priority	Risks							
							CVEs				Misconfigurations			
9.7	CentOsServer	Azure	Azure Virtual Machine	AWP-Demo (0ead7794-3f19-4!	●	Crown Jewel	6	26	25	0	0	0	0	0
8.9	aws-node (6939ba36-f51c-455e-i	Kubernetes	Kubernetes DaemonSet	k8s-demo (bb87ca6e-ddce-42!		Undefined	183	597	280	28	0	2	0	1
8.9	aws-node (23539ac7-1f5c-4deb-i	Kubernetes	Kubernetes DaemonSet	CPX-2023 (12037699-4019-4bc		Undefined	171	461	254	22	0	1	0	0
8.7	cpx-2023-pod (632cd2a9-93ac-4	Kubernetes	Kubernetes Pod	CPX-2023 (12037699-4019-4bc		Undefined	43	80	75	13	1	5	0	4
8.7	sushi (3f264afe-7c2e-4d7d-a0b0-	Kubernetes	Kubernetes Deployment	k8s-demo (bb87ca6e-ddce-42!		Undefined	43	76	73	13	0	2	0	2
8.6	central prod (i-0647eef31e0da1e	AWS	AWS EC2 Instance	AWS ERM Demo (2bad14a5-7t	●	High Importance	11	109	91	6	0	1	1	0
8.6	kube-proxy (078c8cb4-c83e-452f	Kubernetes	Kubernetes DaemonSet	CPX-2023 (12037699-4019-4bc		Undefined	29	46	17	3	0	1	0	0
8.5	central_prod_us (i-08d371669daf	AWS	AWS EC2 Instance	AWS ERM Demo (2bad14a5-7t	●	High Importance	5	113	63	4	0	1	1	0
8.5	nginx-deployment (1b5c0987-a5i	Kubernetes	Kubernetes Deployment	k8s-demo (bb87ca6e-ddce-42!		Undefined	14	52	51	1	0	2	0	2
8.5	kube-proxy (899408d4-90a8-465	Kubernetes	Kubernetes DaemonSet	k8s-demo (bb87ca6e-ddce-42!		Undefined	13	35	35	7	0	2	0	1
8.4	asset-mgmt-runtime-daemon (a1	Kubernetes	Kubernetes DaemonSet	k8s-demo-CPX (c46be6b8-148		Undefined	6	8	7	1	0	0	0	1
8.3	alpine4 (88c38f7a-e0b1-4c4e-b1!	Kubernetes	Kubernetes Pod	k8s-demo (bb87ca6e-ddce-42!		Undefined	4	12	3	0	1	6	0	3
8.3	alpine-portscan (ca386bc6-79fb-	Kubernetes	Kubernetes Pod	k8s-demo (bb87ca6e-ddce-42!		Undefined	4	12	3	0	1	6	0	3
8.3	kube-flannel-ds (4b9545c7-e988-	Kubernetes	Kubernetes DaemonSet	registry-scanner-cluster (34e19		Undefined	5	5	2	0	0	1	0	1

SMARTER PREVENTION



Severity	Date	Source	Title	Ruleset	Assignee	Rem.	Labels
Critical	Feb 11, 2023 11:56 PM	CIEM	Overprivileged lamRole	Entitlement Management	Unassigned	▶	Overprivileged Entity

Consolidated Policy | All Policies

AWSLambdaVPCAccessExecutionRole [Alert Details](#)

Permissions status: **Overpermissive - Critical**

IAM sensitivity: **99**

Policy type: Identity-based policy (AWS Managed)

EFFECTIVE | ORIGINAL | SUGGESTED

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource": [
        "*"
      ],
      "Effect": "Allow",
      "Sid": "CloudGuardGenerated0"
    },
    {
      "Action": [
        "ec2:CreateNetworkInterface",
        "ec2:DescribeNetworkInterfaces",

```

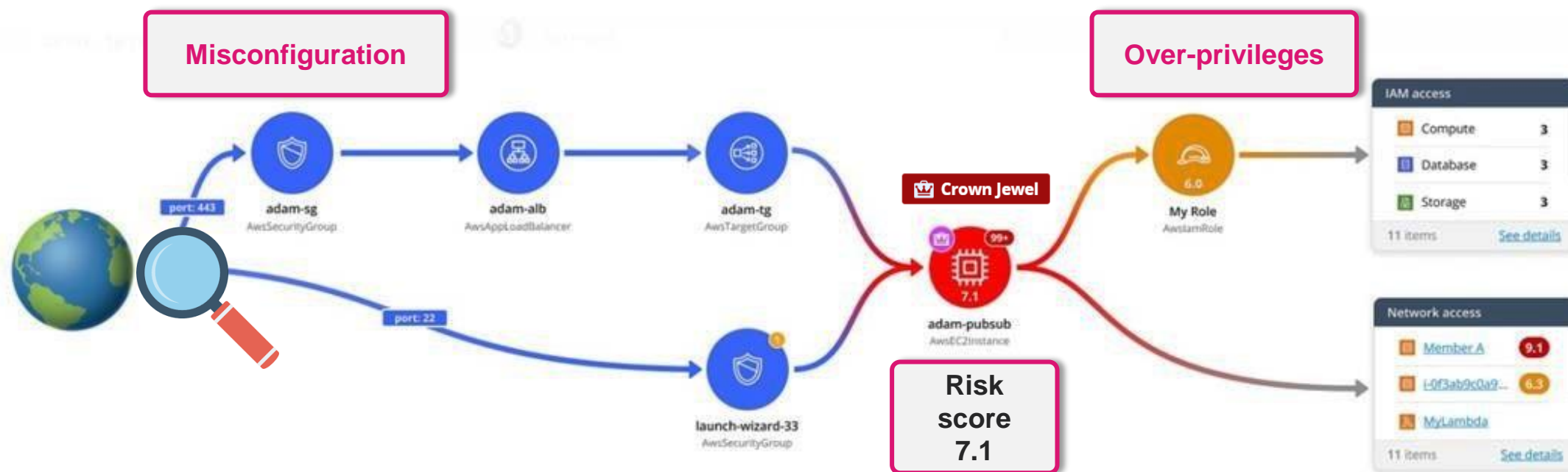
THREAT INTELLIGENCE

The screenshot displays the Check Point CloudGuard interface for a protected asset named 'prod-mongodb-2'. The interface is divided into several sections:

- AI generated insights:** A list of five findings, each with a lightbulb icon and a dropdown arrow:
 - EC2 instance allows incoming traffic from 0.0.0.0/0 to remote server administration ports
 - EC2 Instance is not protected against termination actions
 - EC2 instance does not use IAM instance roles for AWS resource access
 - IMDS Response Hop Limit is not set to one
 - EC2 instance volumes are not encrypted
- Top 5 remediation actions:** A list of three actions, each with a plus icon and a dropdown arrow:
 - Ensure that EC2 instance's volumes are encrypted
 - Use encrypted storage for instances that might host a database.
 - Ensure IAM instance roles are used for AWS resource access from instances
- EVENTS:** Two summary cards:
 - Posture Findings (Critical & High):** 10 findings (indicated by a red icon).
 - Security Events (Critical & High):** 0 events (indicated by a green icon).

At the bottom of the interface, a list of findings is visible, including 'EC2 instance does not use IAM instance roles for AWS resource access', 'IMDS Response Hop Limit is not set to one', and 'EC2 instance volumes are not encrypted'.

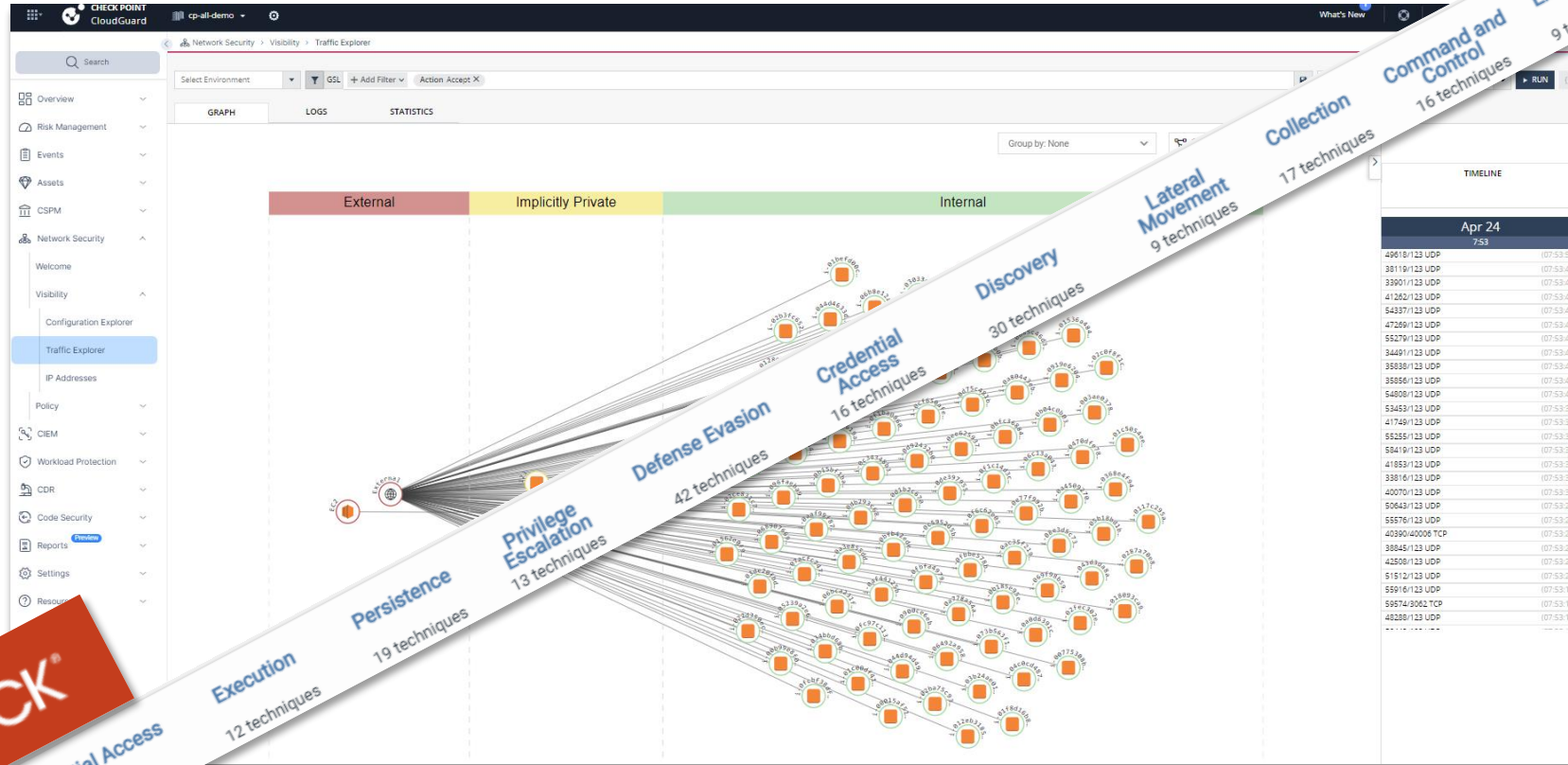
ANALISE OS CAMINHOS DO ATAQUE COM O GRÁFICO DE CONTEXTO



Veja o que está oculto: Avalie a exposição e o impacto dos ativos na nuvem para tomar decisões informadas sobre a mitigação de riscos.

Mitigate risks: Implemente medidas de segurança direcionadas, como ajuste fino de políticas IAM, etc., para fortalecer seu ambiente em nuvem

CLOUD DETECTION AND RESPONSE



MITRE | ATT&CK

Reconnaissance
10 techniques

Resource Development
7 techniques





CloudGuard

PREVENTION-FIRST CNAPP



More Context



Actionable Security



Smarter Prevention

Demo



Thank You!

YOU DESERVE THE BEST SECURITY