CHECK POINT

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

6,500+
Employees Worldwide, Top Talent

Cutting-Edge Technologies
Over 30 Years Of Expertise,
Industry's Most Visionary Player

Traded on Nasdaq
1996 I CHKP

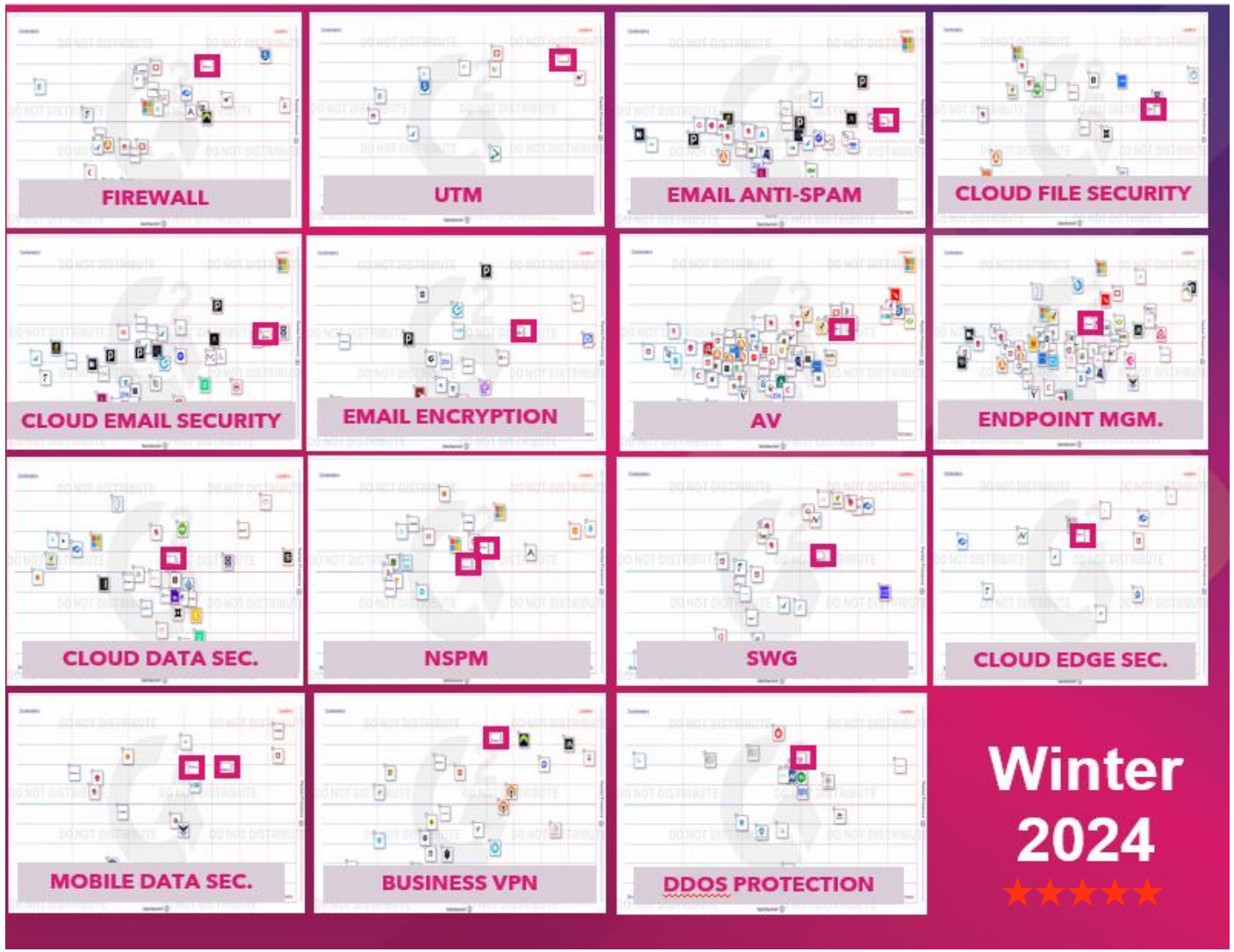
Innovation Leadership
Highest Number Of AI Real-time Prevention Techniques

World's Best Employer
By Forbes,
#1 Cyber Security Vendor

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

Leader
WINTER
2024

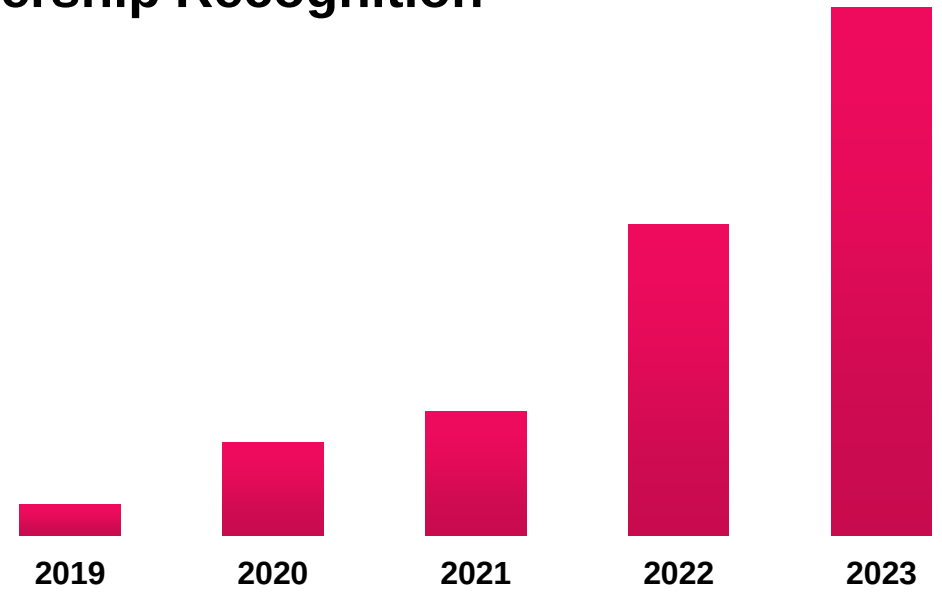
An Achievement Second to None.



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

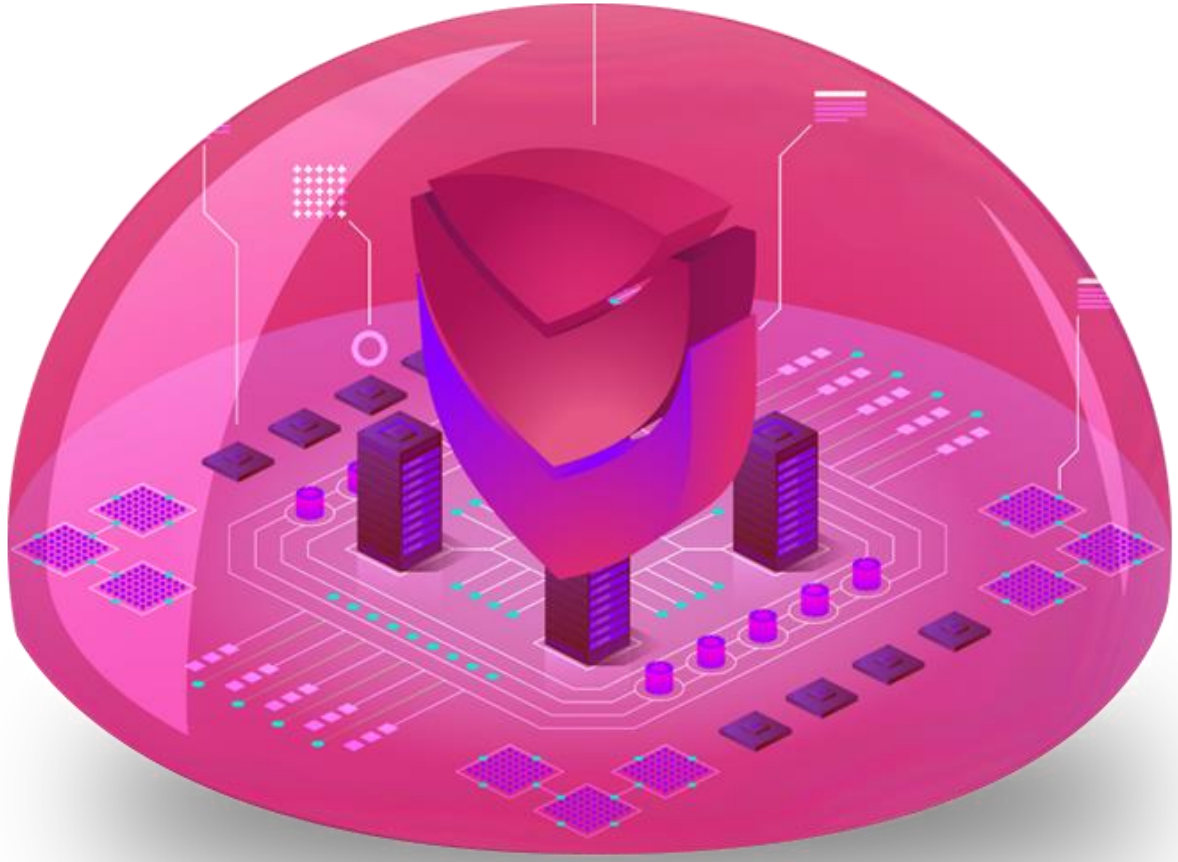


FORRESTER | OMDIA | FROST & SULLIVAN | GIGAOM

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

THREATCLOUD AI

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

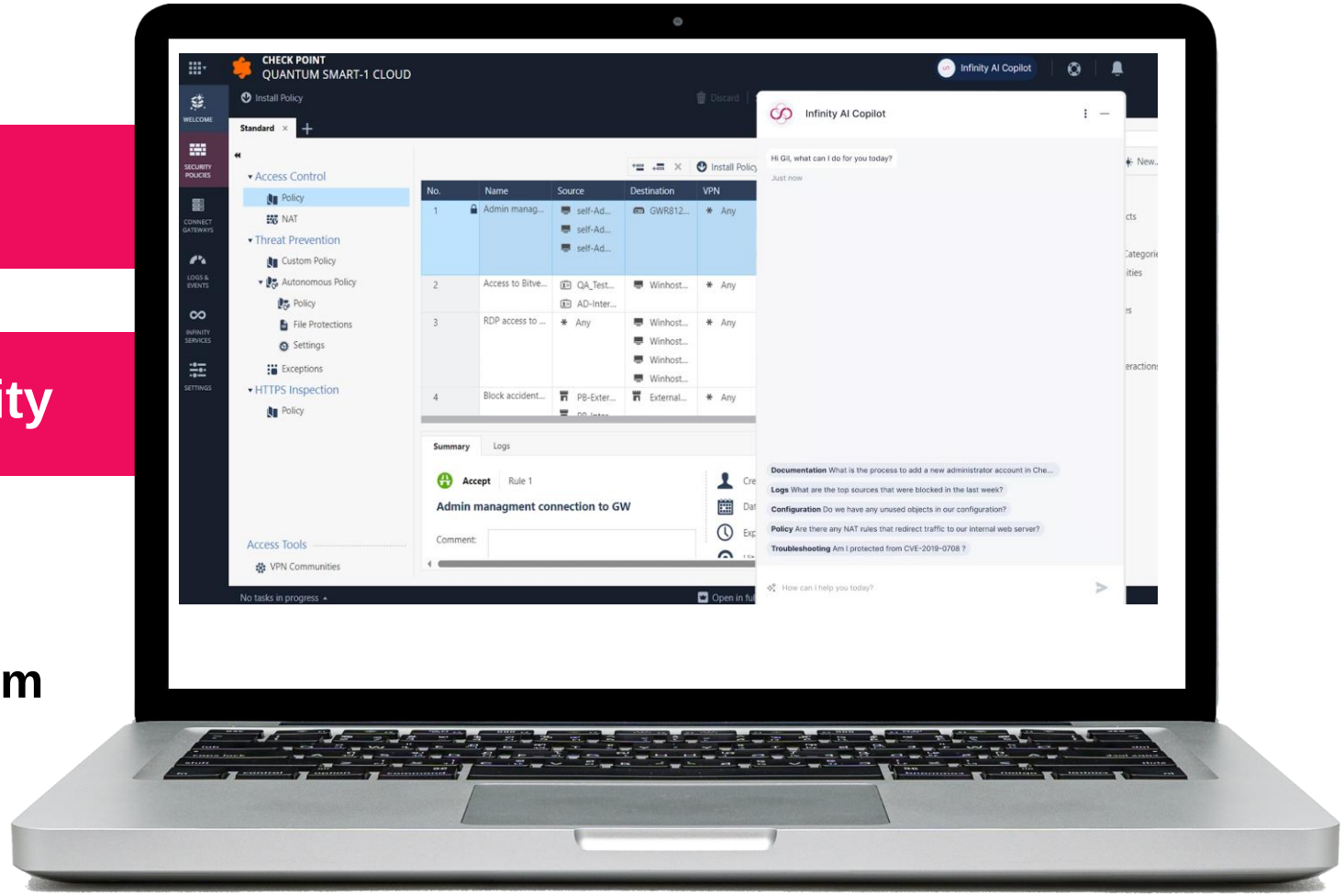
Gerenciamento de Segurança 10X mais efetivo

Infinity AI Copilot

Powerful, Generative-AI tool

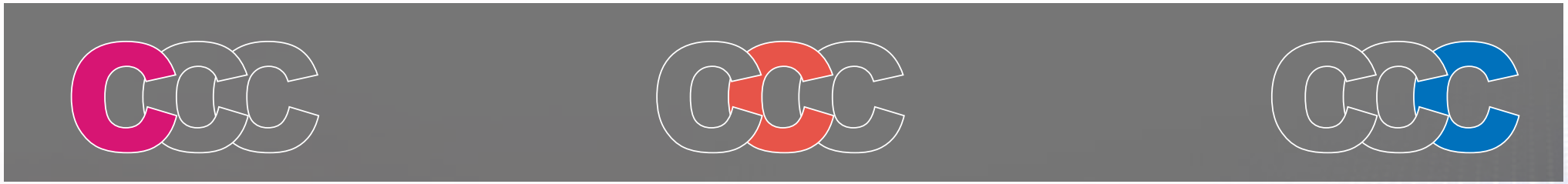
Embarcado na Plataforma Infinity

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

Infinity Platform

AI-Powered. Cloud-Delivered.

SECURE THE **ENTERPRISE**

AI-Powered. Cloud-Delivered.

Infinity Platform

SECURE THE **NETWORK**

Quantum

SECURE THE **CLOUD**

CloudGuard

SECURE THE **WORKSPACE**

Harmony

Infinity Core Services

Collaborative Security Operations & Services

Security Operations and AI

- XDR/XPR
- Playblocks
- Events
- ThreatCloud AI
- AI Copilot

Global Services

- Managed Services
- MDR/Incident Response
- Professional Services
- Security Architecture
- Training

SECURE THE **ENTERPRISE**

AI-Powered. Cloud-Delivered.

Infinity Platform

NEW

SECURE THE **NETWORK**

Quantum

- **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**

CloudGuard

- **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**

Harmony

- **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**

Infinity Core Services

Security Operations and AI

- **XDR/XPR** Extended Prevention and Response
- **Playblocks** Orchestration and Automation
- **Events** Unified Events
- **ThreatCloud AI** AI-Powered Threat Intelligence
- **AI Copilot** Automating Security with AI

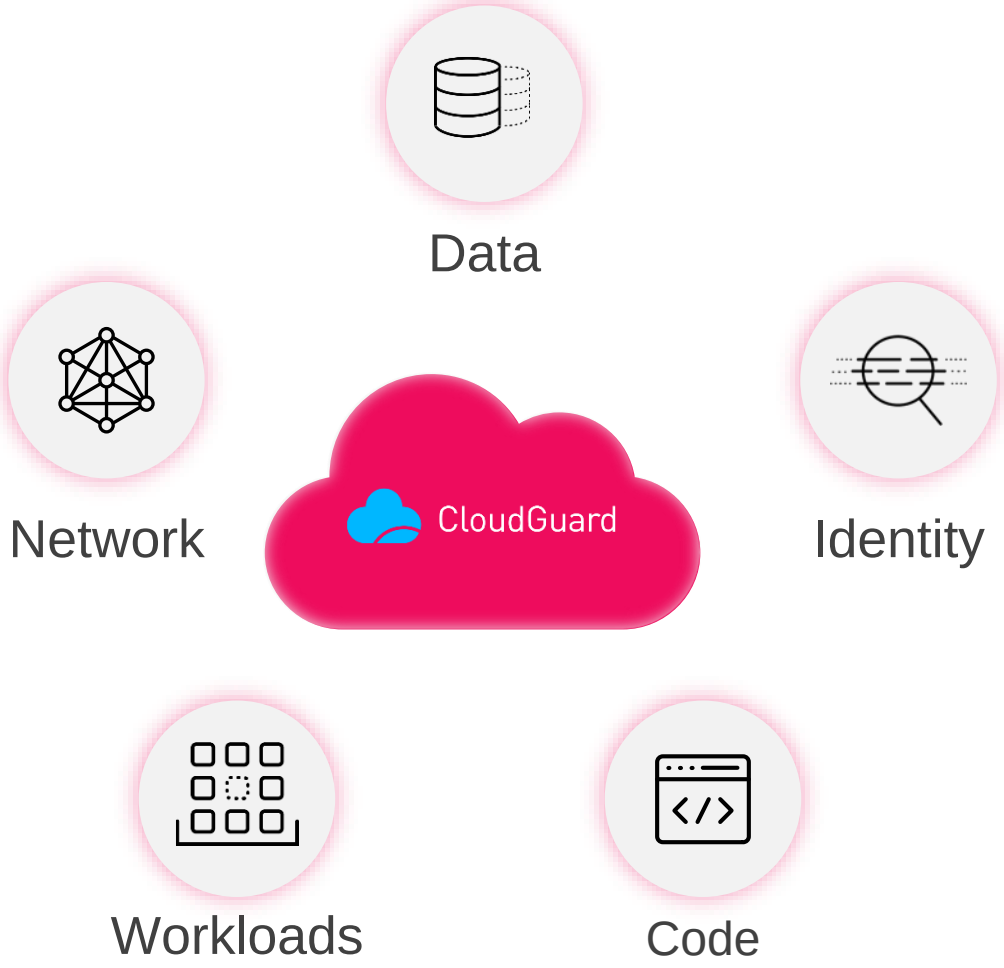
Global Services

- **MDR/MPR** Managed Prevention and Response
- **Incident Response** Keep Your Business Running
- **Consulting & Training** Leverage security architecture design experts

CloudGuard

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 **C**loud **N**ative **A**pplication **P**rotection **P**latform

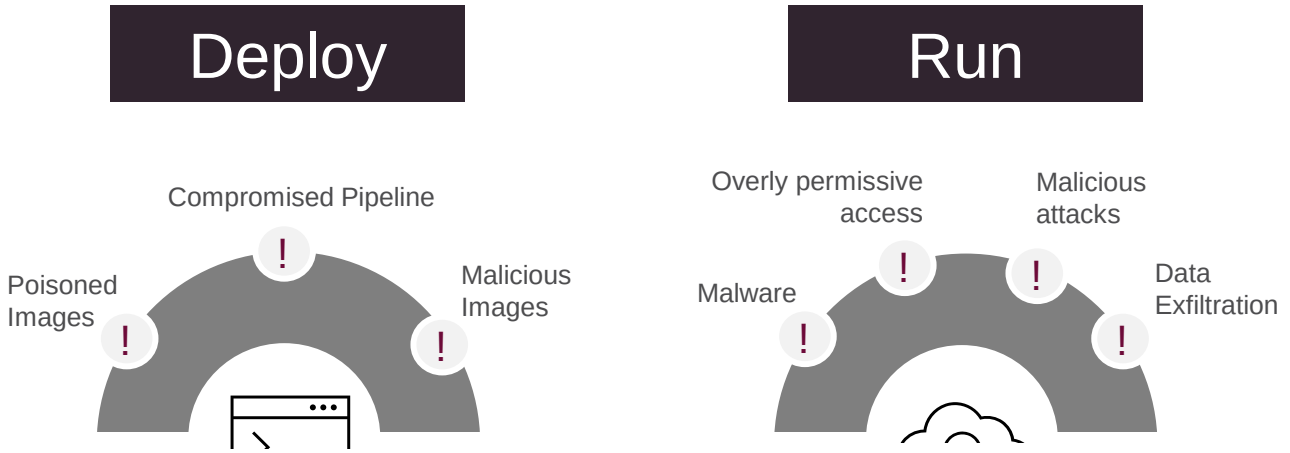
Conjunto Integrado de Capacidades de Segurança e Conformidade projetado para ajudar a **proteger e garantir a segurança de aplicações nativas de nuvem** durante o desenvolvimento e a produção.

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 **C**loud **N**ative **A**pplication **P**rotection **P**latform



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".

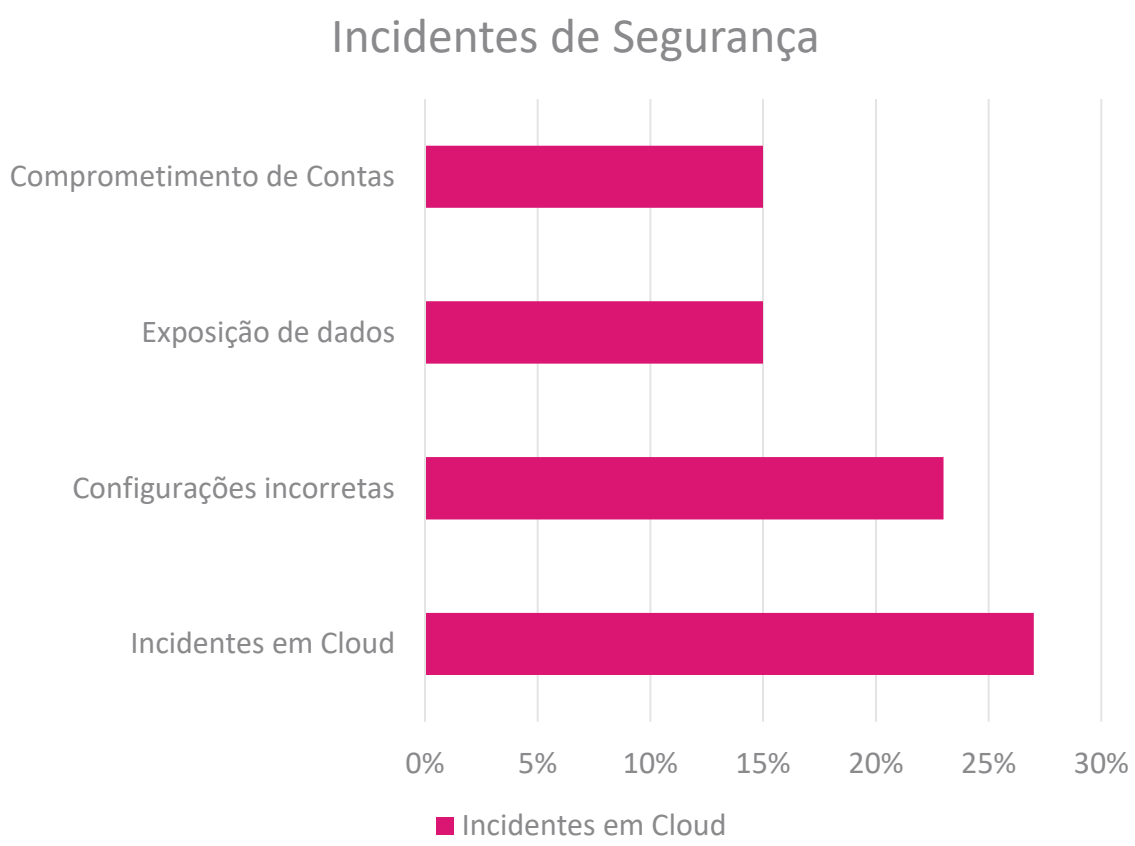
No cerne do CSPM está a detecção de vulnerabilidades de configuração incorreta em nuvem que podem levar a violações de conformidade e violações de dados.

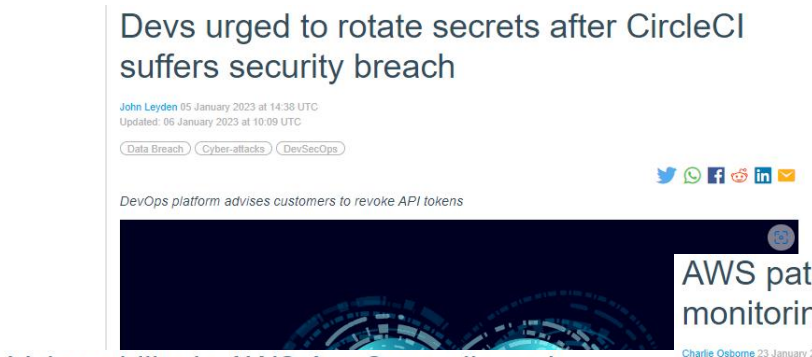
- **Visibilidade contínua de ambientes multi-nuvem para identificar vulnerabilidades de configuração incorreta em nuvem.**
- **Capacidade opcional de realizar remediação automatizada de configurações incorretas para garantir conformidade contínua e proteger serviços críticos em nuvem.**
- **Utilização 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®

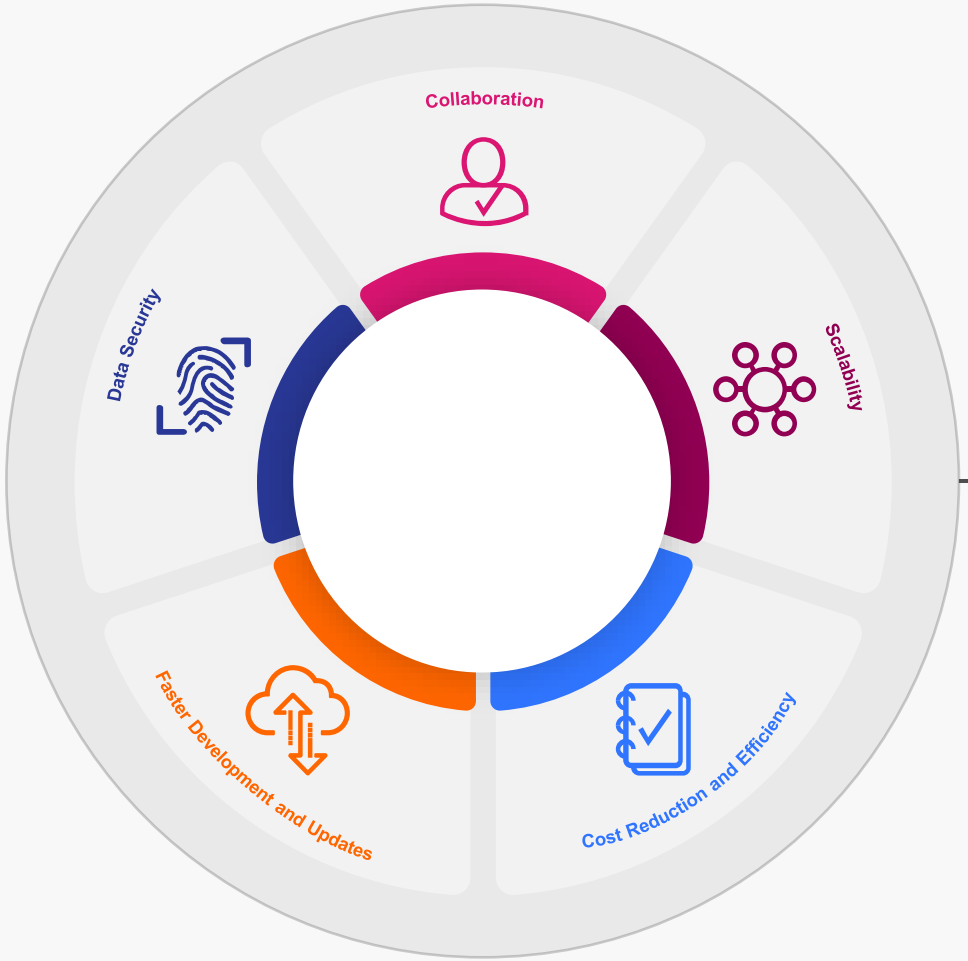
De acordo com Gartner

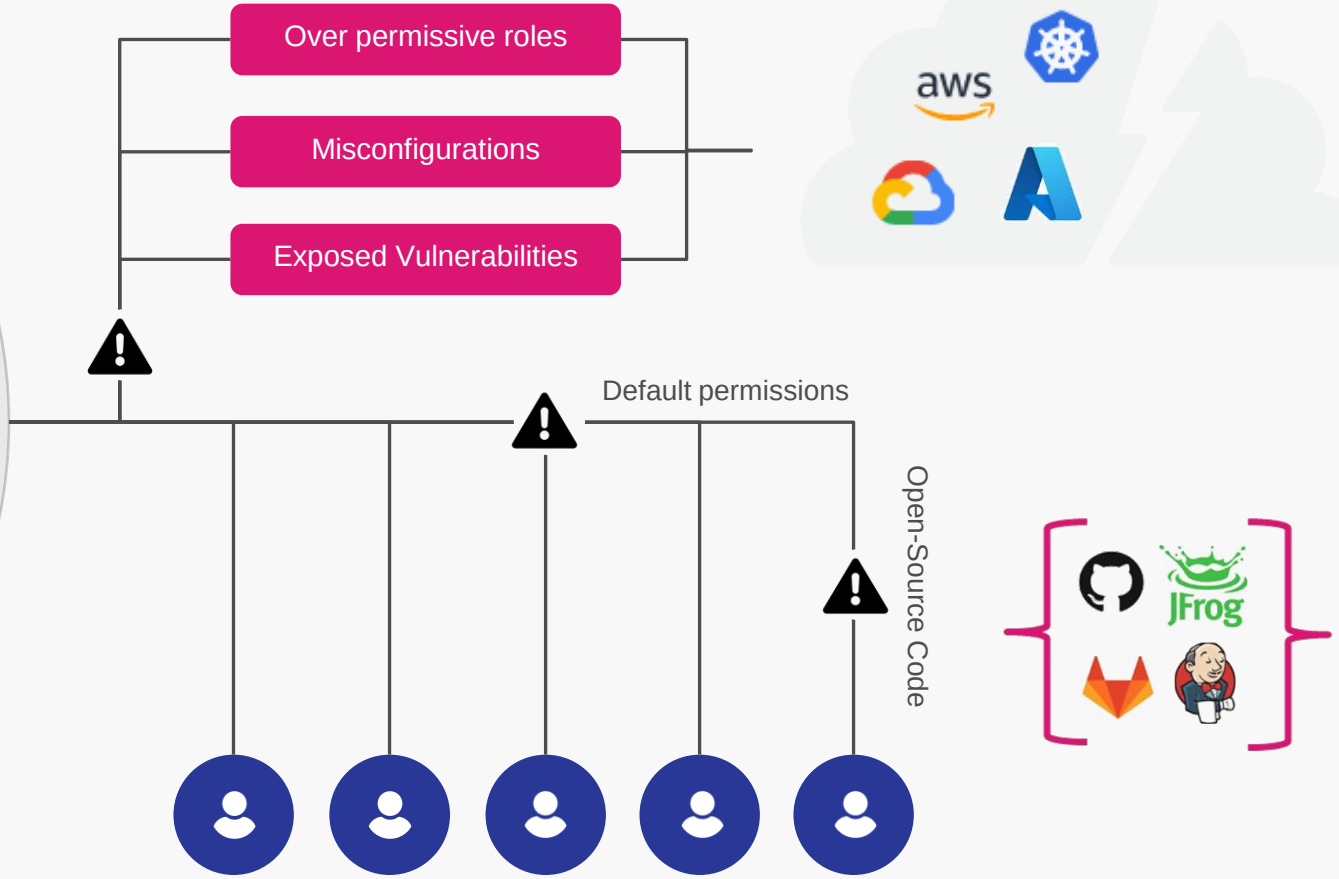
- De fato, a segurança em nuvem é uma responsabilidade compartilhada entre os provedores de nuvem e os clientes. **A citação "Até 2025, mais de 80% das falhas de segurança em nuvem serão culpa do cliente"** destaca a importância de os clientes adotarem práticas de segurança sólidas ao usar serviços em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

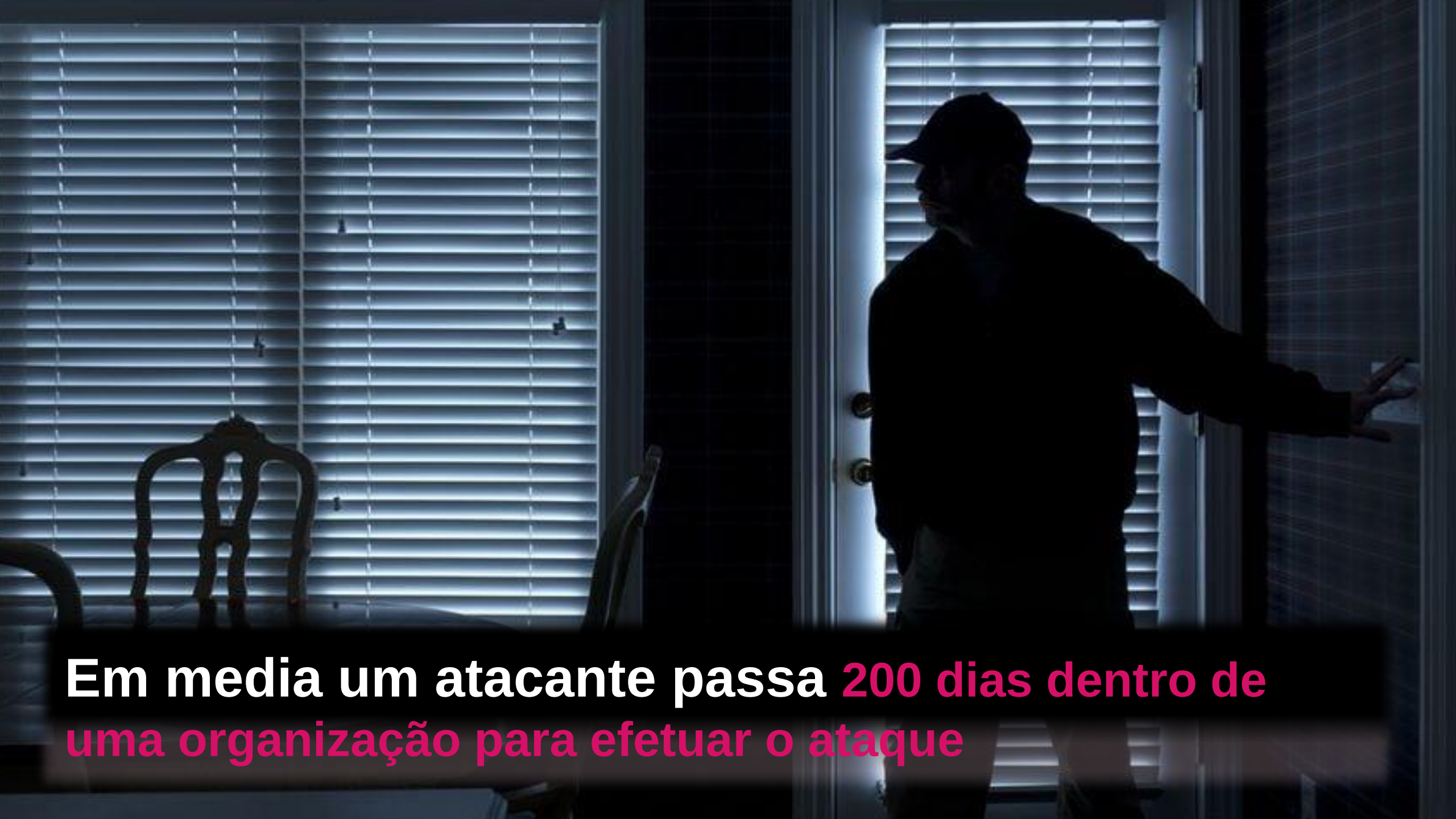




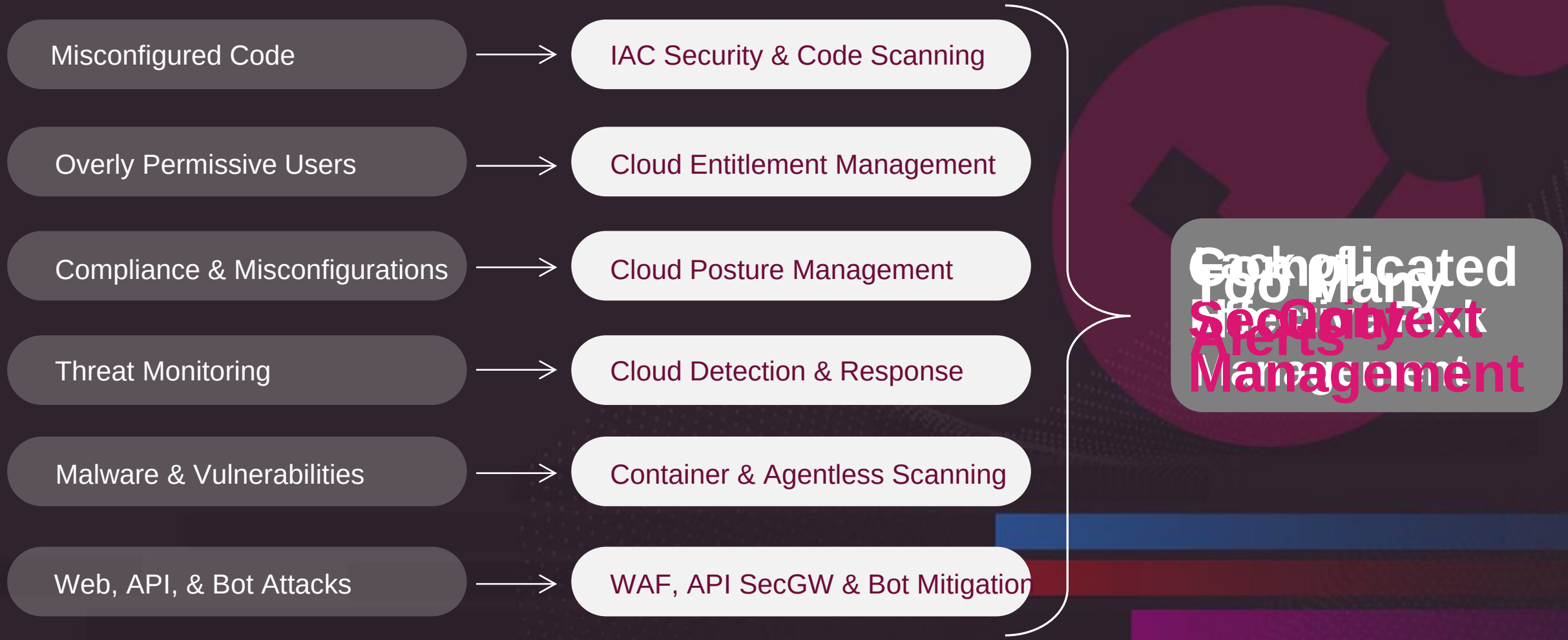
MAIS VELOCIDADE PARA DEV= MAIS RISCOS PARA SEC

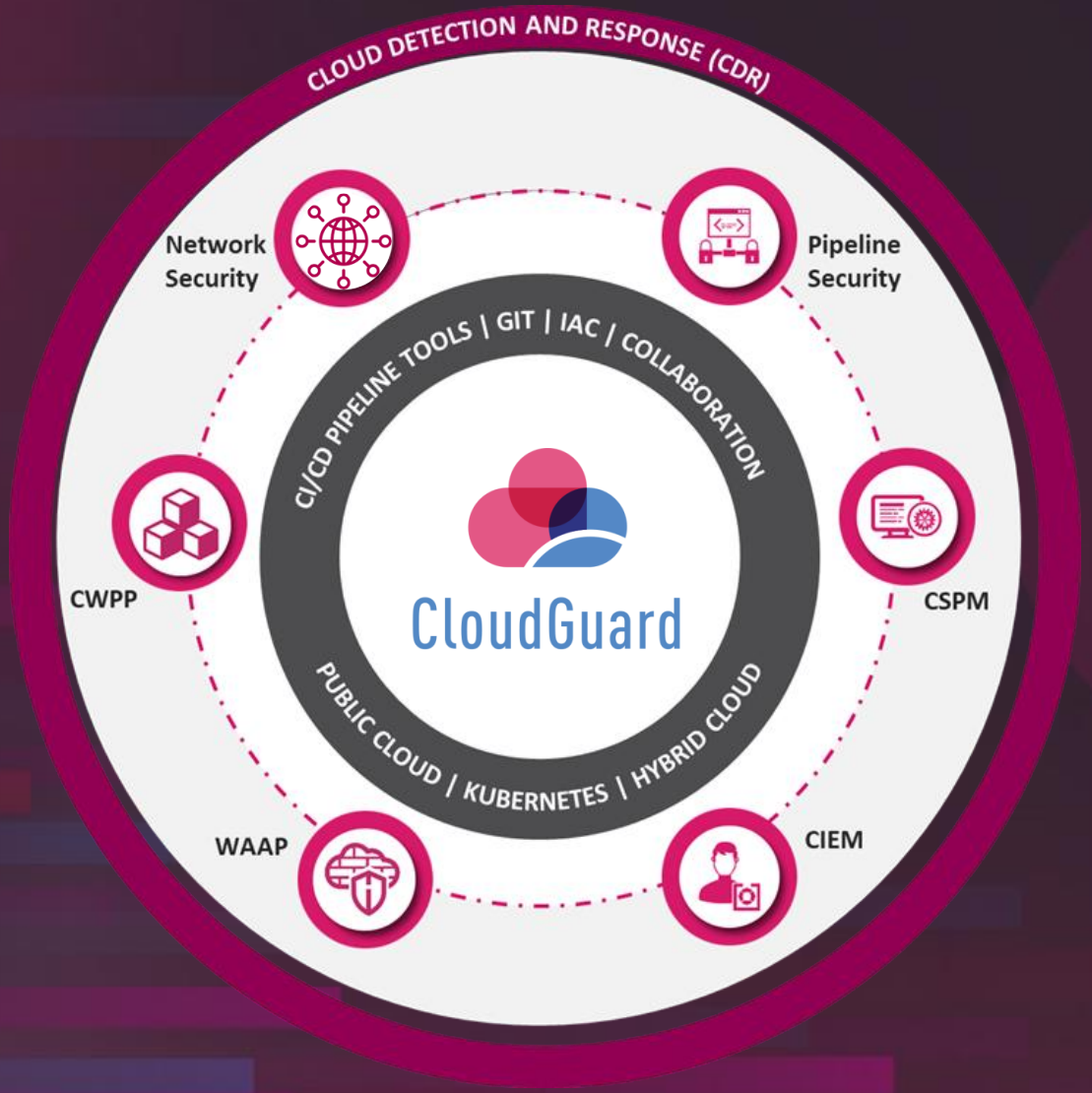





Em media um atacante passa 200 dias dentro de
uma organização para efetuar o ataque

DEPLOY SEPARATE TOOLS TO FIX ISSUES





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.	**9.8 Misconfigured Crown-Jewel Workload**
	9.3 Overly Permissive Role
Segredos encontrados em repositório do GitHub que foi compartilhado	**9.2 Secret in shared repository**
Vulnerabilidade identificada no Código da aplicação	**8.1 Vulnerable Code**
Senha fraca configurada na console de gerenciamento do lab	**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

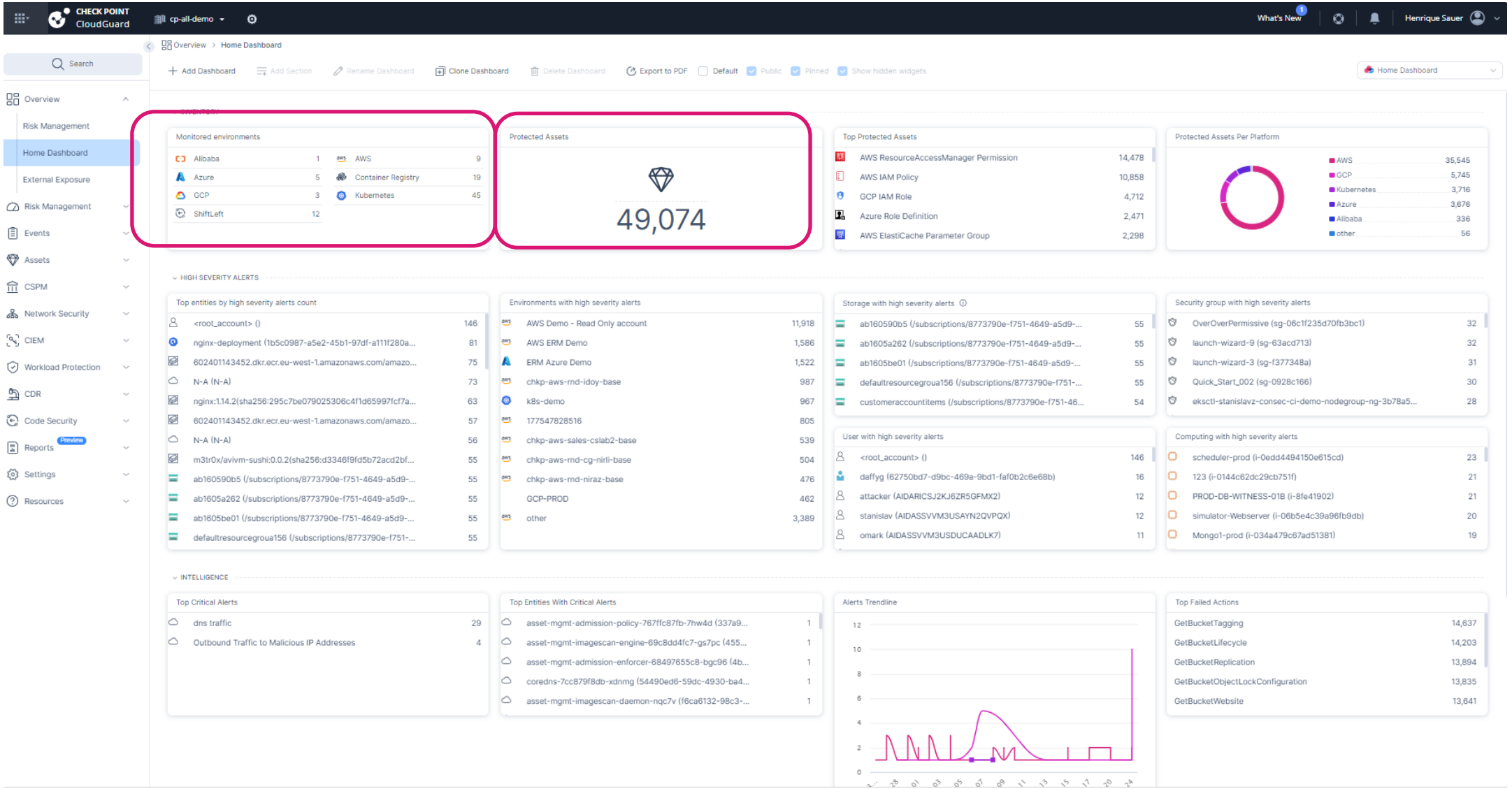
Misconfigured Workload:
Automatic Remediation: CloudGuard automatically turned-on encryption on storage bucket using CloudBots

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

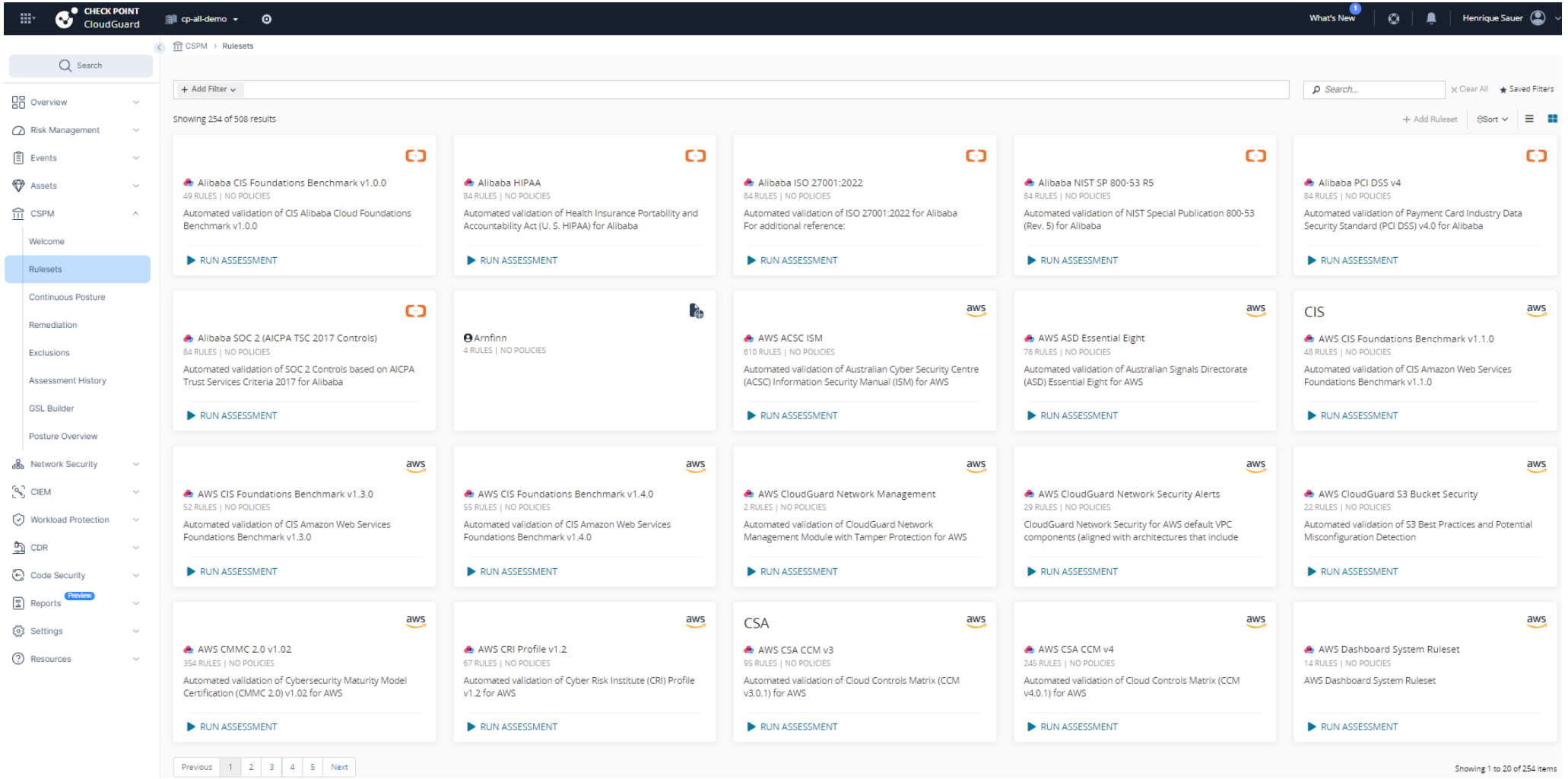
Secret Left Behind:
Suggested Remediation: CloudGuard recommends removing secret from code artifact

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

DASHBOARD



COMPLIANCE

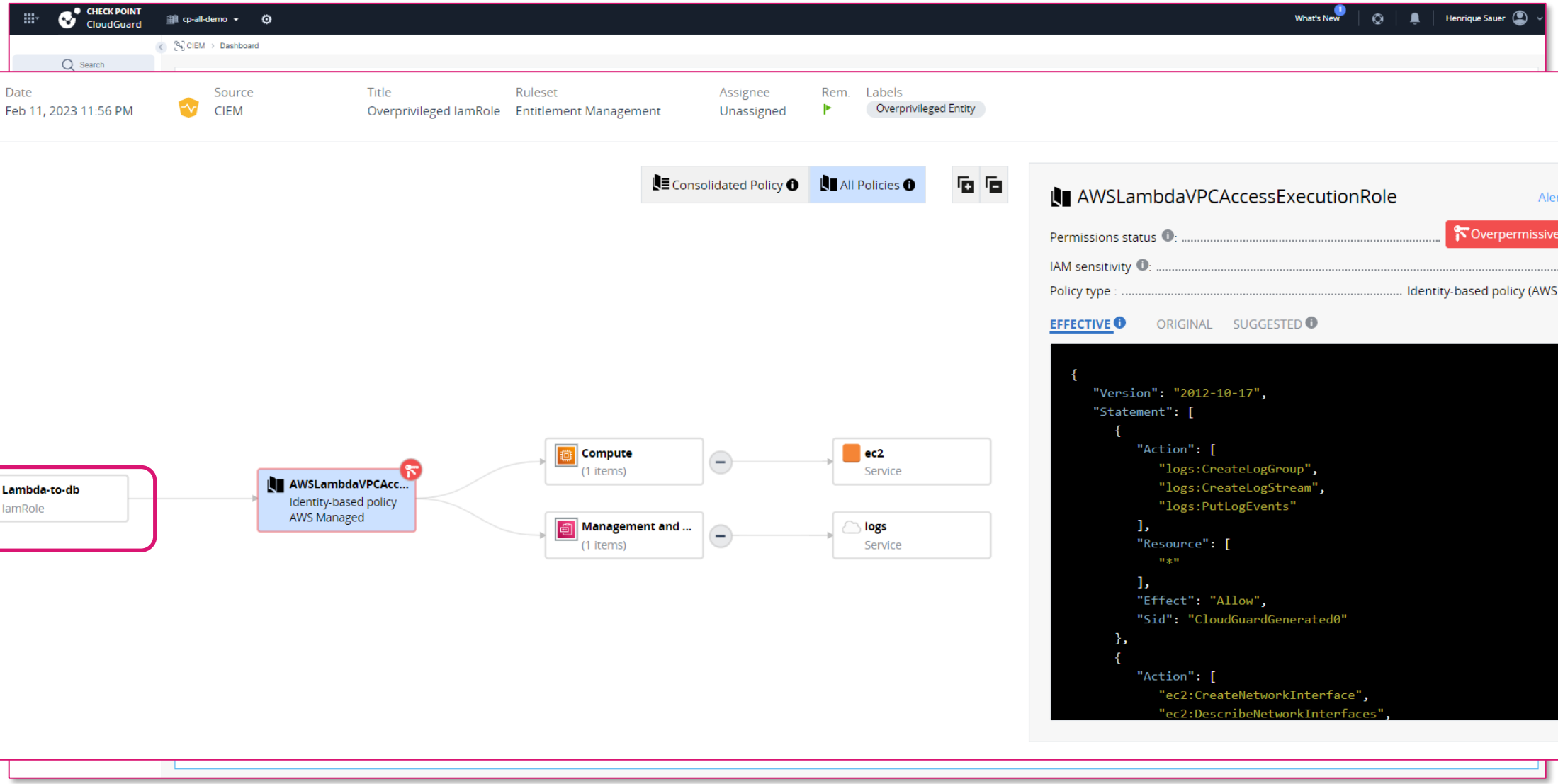


MORE CONTEXT

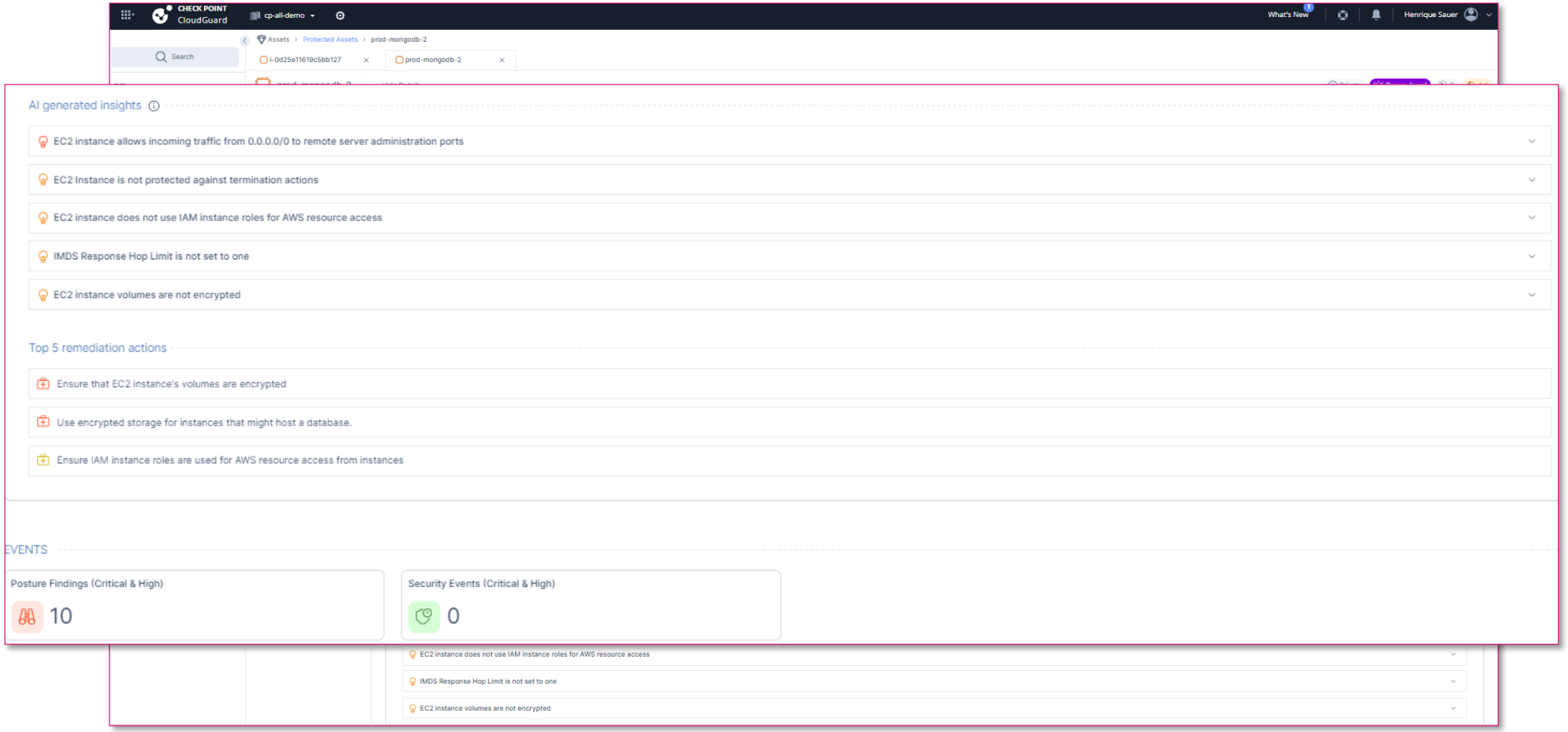
Drag here to set row groups

							Risks							
Risk	Entity	Platform	Type	Environment	Is Ru...	Business Priority	CVEs				Misconfigurations			
9.7	CentOsServrer	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-	Kubernetes	Kubernetes DaemonSet	k8s-demo (bb87ca6e-ddce-42		Undefined	183	597	280	28	0	2	0	1
8.9	aws-node (23539ac7-1f5c-4deb-	Kubernetes	Kubernetes DaemonSet	CPX-2023 (12037699-4019-4b		Undefined	171	461	254	22	0	1	0	0
8.7	cpx-2023-pod (632cd2a9-93ac-4	Kubernetes	Kubernetes Pod	CPX-2023 (12037699-4019-4b		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-0647eeff31e0da1	AWS	AWS EC2 Instance	AWS ERM Demo (2bad14a5-7b	●	High Importance	11	109	91	6	0	1	1	0
8.6	kube-proxy (078c8cb4-c83e-452	Kubernetes	Kubernetes DaemonSet	CPX-2023 (12037699-4019-4b		Undefined	29	46	17	3	0	1	0	0
8.5	central_prod_us (i-08d371669daf	AWS	AWS EC2 Instance	AWS ERM Demo (2bad14a5-7b	●	High Importance	5	113	63	4	0	1	1	0
8.5	nginx-deployment (1b5c0987-a5	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



THREAT INTELLIGENCE

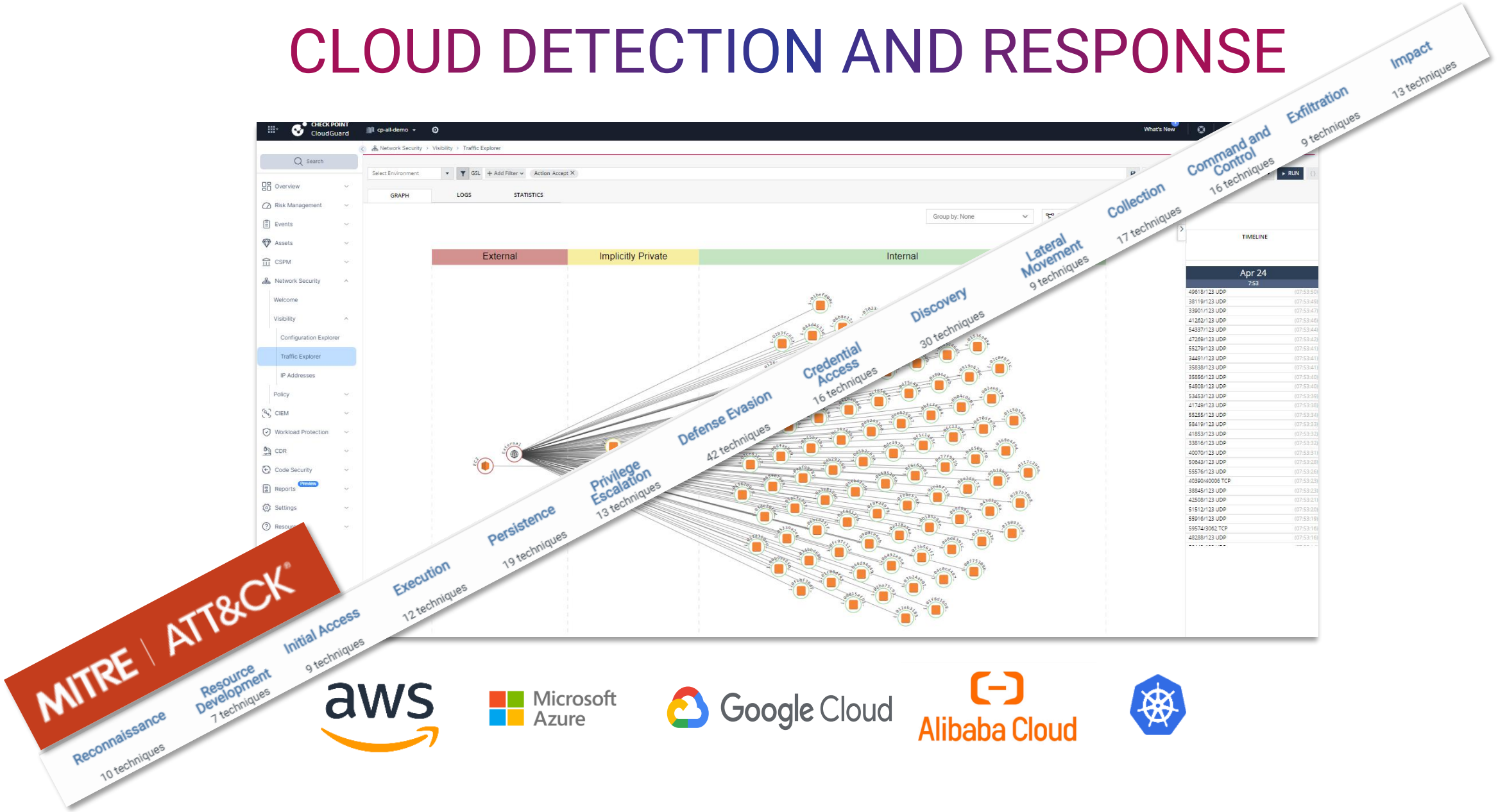


ANALISE OS CAMINHOS DO ATAQUE COM O GRÁFICO DE CONTEXTO

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



CloudGuard

PREVENTION-FIRST CNAPP

More Context ▶ Actionable Security ▶ Smarter Prevention

Demo

CHECK POINT™

Thank You!

YOU DESERVE THE BEST SECURITY