CHECK POINT

Cybersecurity trifft GenAI

KI denkt schnell, wir denken sicher. Kontrolle statt Chaos!

Ulrike Scharf | Solutions Architect

18.November 2025

YOU DESERVE THE BEST SECURITY

AI Security report

01 Wie können wir KI einsetzen

02 Wie können wir KI und die Ergebnisse schützen

01

Wie können wir KI einsetzen

Industry Leading Cyber Security Portfolio

On-Premises Security — Quantum

Maestro
Hyperscale Data Center

VPN
Virtual Private Remote Access

Force
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

Cloud Security — CloudGuard

Network
Cloud Firewall

WAF
Web Application Firewall

API Security
Securing API

Secure AI
Securing LLMs

Workspace Security — Harmony

Endpoint
Protection & Posture Management

Email & Collaboration
Cloud Productivity Suite Security

Mobile
Mobile Threat Defense

SASE
Internet Access Private Access

SaaS
Threat Prevention SaaS & GenAI Apps

Web Browser
Threat Prevention for Web Browsers

SECURITY OPERATIONS AND SERVICES — Infinity Platform Services

SECURITY OPERATIONS

XDR/XPR
Extended Prevention and Response

Playblocks
Orchestration and Automation

Events
complete event unification & visibility

External Risk Management
Manage & Mitigate External Risks

AI TOOLS

ThreatCloud AI
AI-Powered Threat Intelligence

AI Copilot
Automating Security with AI

AI Cloud Protect
Securing AI Infrastructure

GenAI Protect
Securing GenAI apps

GLOBAL SERVICES

Assessment and Risks
Threat & Risk Assessment

Professional Services
Design & Deploy

Managed Security
Let Us Do It For You

Training Programs
Educate Your Team

Incident Response
Detection & Digital Forensics

THREATCLOUD AI

The Brain Behind Check Point Security

THREATCLOUD AI
55
AI Powered Engines

Big data threat intelligence

3,700,000,000
Websites and files inspected

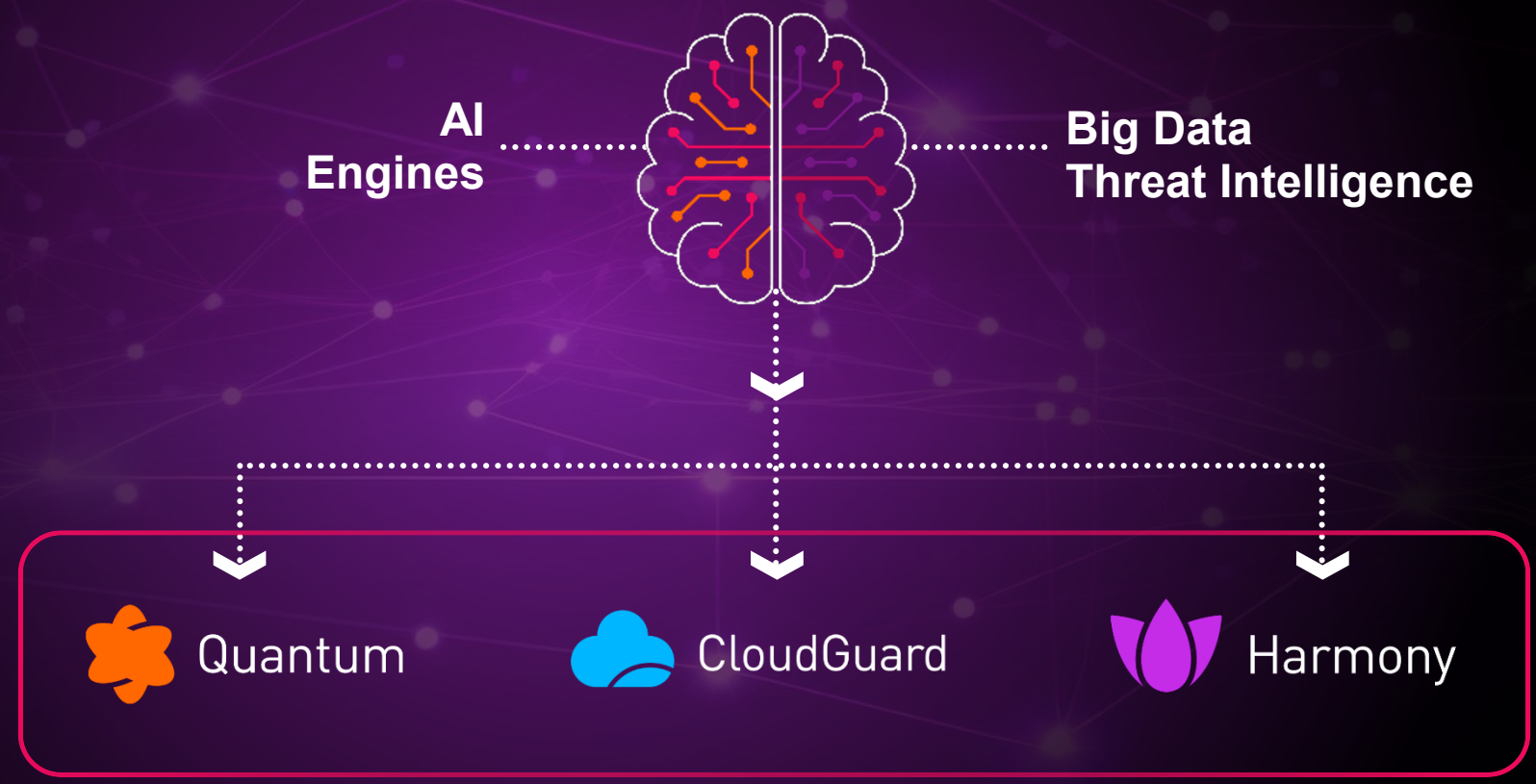
250,000,000
Full content emails

86,000,000
File emulations

3,700,000
Online web forms

1,800,000
Newly installed mobile apps

Counted **DAILY!**



Management Blades

SmartEvent

Manage, report, and analyze events

Compliance

Meet regulations through best practices

Infinity Playblocks

UPGRADED

Collaborative threat prevention

Infinity AI Copilot

UPGRADED

AI-Based security assistant

Infinity Identity

NEW

Authenticated access to sensitive resources

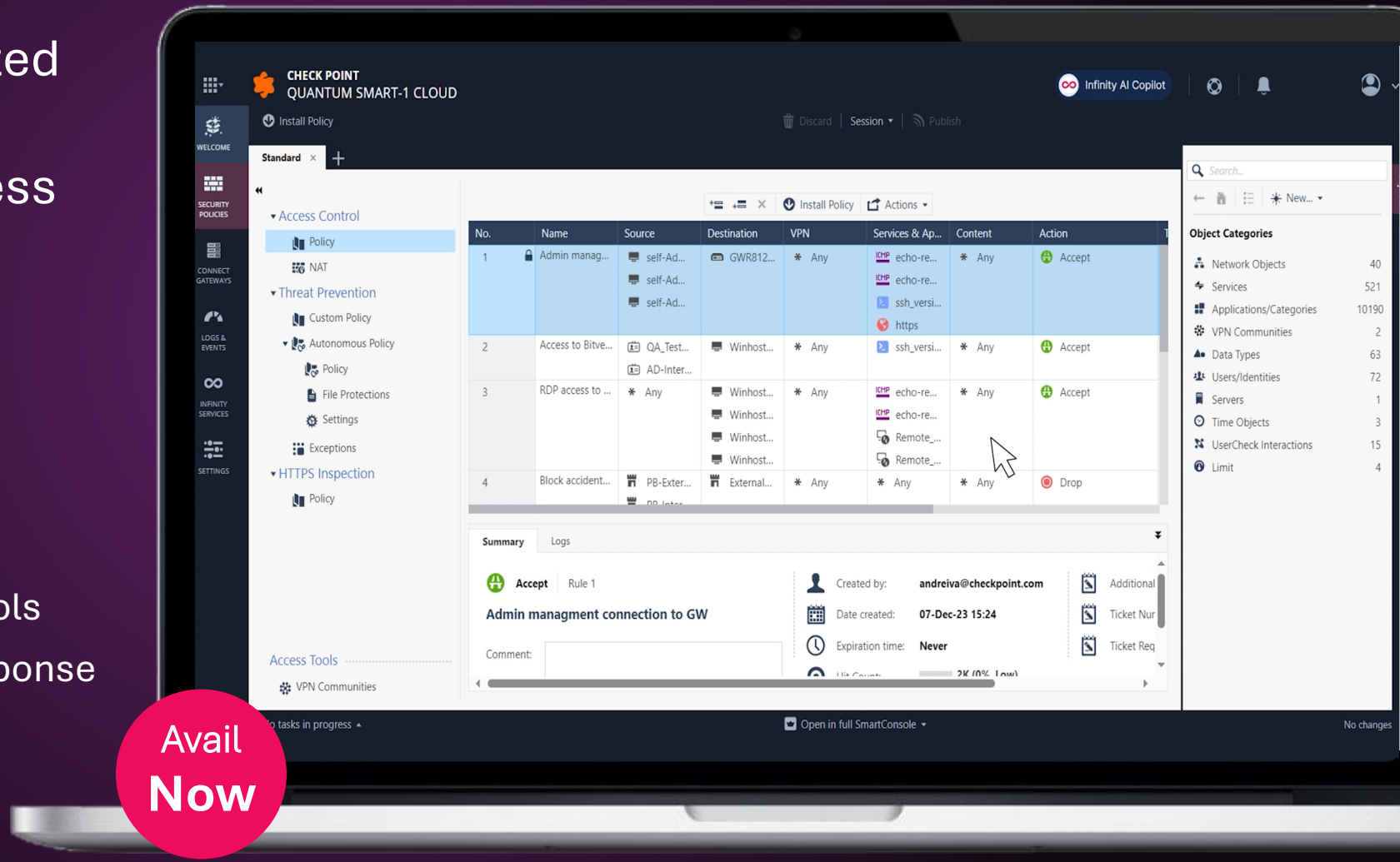
Infinity Copilot

Your Personal GenAI Security Assistant

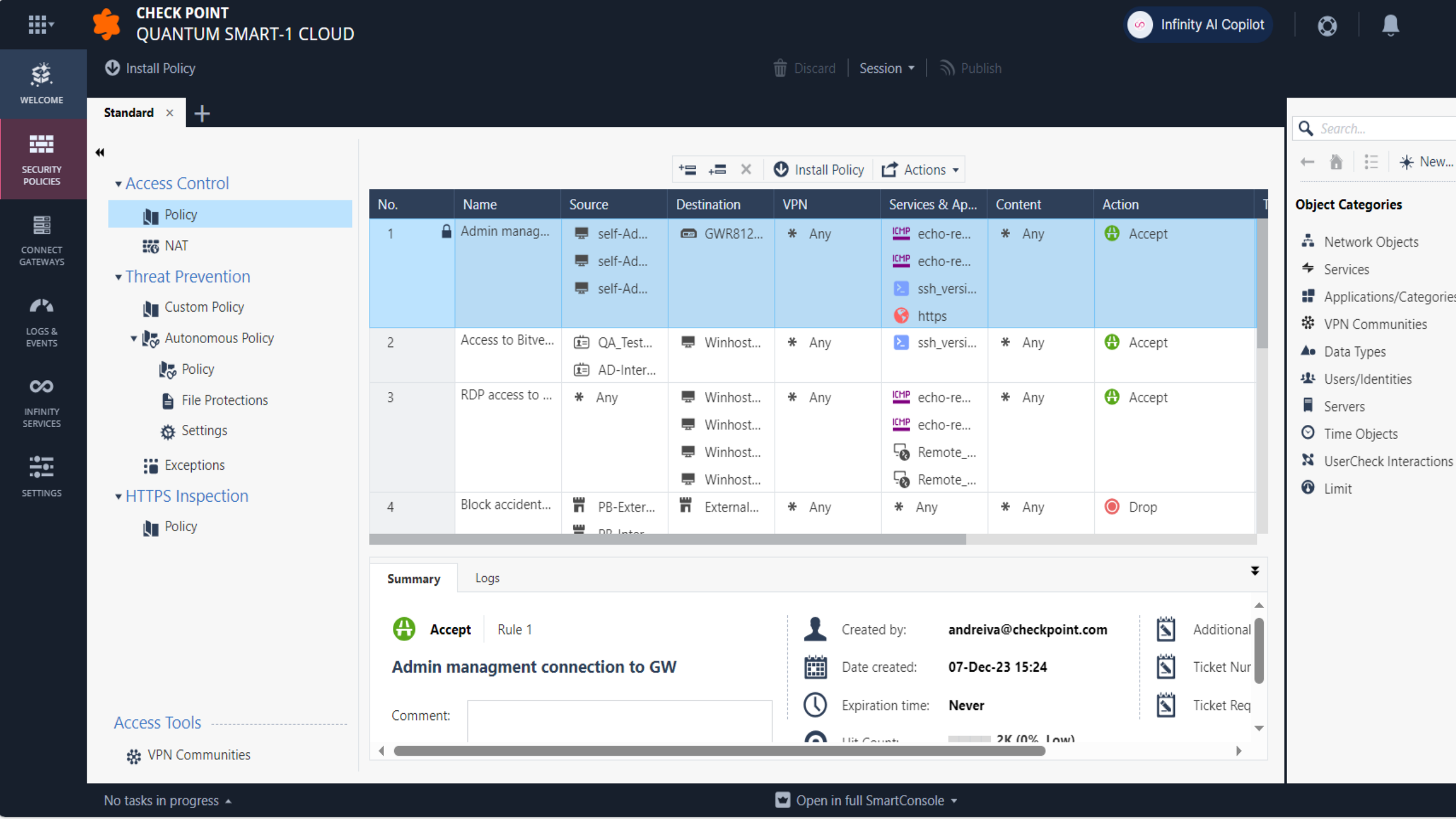
Level 1: AI Assisted

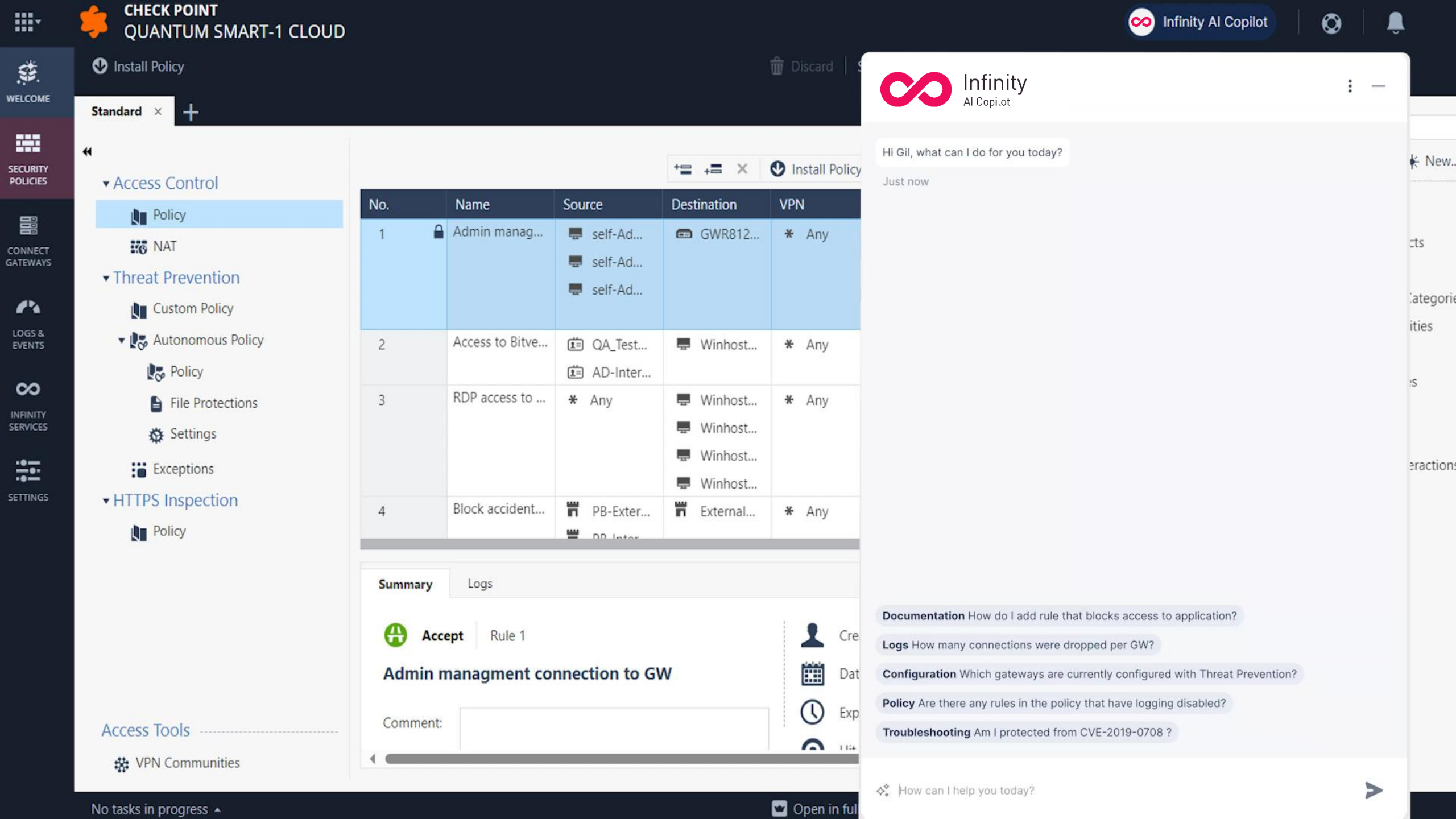
Complete and contextualized answers and actions as it understands policies, access rules, objects, and logs

- AI-elevated administration
- Increase effectiveness of current tools
- Improve incident mitigation and response
- Multilingual Support



Avail **Now**


CHECK POINT
QUANTUM SMART-1 CLOUD
Infinity AI Copilot
Install Policy
Discard
Session
Publish
WELCOME
SECURITY POLICIES
CONNECT GATEWAYS
LOGS & EVENTS
INFINITY SERVICES
SETTINGS
Standard
Access Control
Policy
NAT
Threat Prevention
Custom Policy
Autonomous Policy
Policy
File Protections
Settings
Exceptions
HTTPS Inspection
Policy
Access Tools
VPN Communities
Install Policy
Actions
No. Name Source Destination VPN Services & Ap... Content Action
1 Admin manag... self-Ad... self-Ad... self-Ad... GWR812... Any echo-re... echo-re... ssh_versi... https Any Accept
2 Access to Bitve... QA_Test... AD-Inter... Winhost... Any ssh_versi... Any Accept
3 RDP access to ... Any Winhost... Winhost... Winhost... Winhost... Any echo-re... echo-re... Remote_... Remote_... Any Accept
4 Block accident... PB-Exter... External... Any Any Any Drop
Summary
Logs
Accept
Rule 1
Admin managment connection to GW
Comment:
Created by: andreiva@checkpoint.com
Date created: 07-Dec-23 15:24
Expiration time: Never
Additional
Ticket Nur
Ticket Req
Search...
New...
Object Categories
Network Objects
Services
Applications/Categories
VPN Communities
Data Types
Users/Identities
Servers
Time Objects
UserCheck Interactions
Limit
No tasks in progress
Open in full SmartConsole


CHECK POINT
QUANTUM SMART-1 CLOUD
Infinity AI Copilot
Install Policy
Discard
WELCOME
SECURITY POLICIES
CONNECT GATEWAYS
LOGS & EVENTS
INFINITY SERVICES
SETTINGS
Standard
Access Control
Policy
NAT
Threat Prevention
Custom Policy
Autonomous Policy
Policy
File Protections
Settings
Exceptions
HTTPS Inspection
Policy
Access Tools
VPN Communities
Install Policy
No. Name Source Destination VPN
1 Admin manag... self-Ad... self-Ad... self-Ad... GWR812... Any
2 Access to Bitve... QA_Test... AD-Inter... Winhost... Any
3 RDP access to ... Any Winhost... Winhost... Winhost... Winhost... Any
4 Block accident... PB-Exter... External... Any
Summary
Logs
Accept
Rule 1
Admin managment connection to GW
Comment:
No tasks in progress
Open in ful
Infinity
AI Copilot
Hi Gil, what can I do for you today?
Just now
Documentation How do I add rule that blocks access to application?
Logs How many connections were dropped per GW?
Configuration Which gateways are currently configured with Threat Prevention?
Policy Are there any rules in the policy that have logging disabled?
Troubleshooting Am I protected from CVE-2019-0708 ?
How can I help you today?

Documentation How do I add rule that blocks access to application?

Logs How many connections were dropped per GW?

Configuration Which gateways are currently configured with Threat Prevention?

Policy Are there any rules in the policy that have logging disabled?

Troubleshooting Am I protected from CVE-2019-0708 ?

Am I protected against MOVEit Transfer attacks?

Infinity
AI Copilot

Hi Gil, what can I do for you today?

21:16

Am I protected against MOVEit Transfer attacks?

Just now

Yes. You are protected. Your IPS is set to prevent attempts to exploit this attack. (CVE-2023-34362, CVE-2023-35036, CVE-2023-35708, CVE-2023-36932, CVE-2023-36934, CVE-2023-36933)

Just now

Were there any recent attack attempts?

21:17

Were there any recent attack attempts?

21:17

Yes. There were 16 attempts to exploit this attack in the last 30 days. The last attempt was on 2024-01-03 at 13:59:41.

Just now

Do you want me to notify you upon new CVE's in the future?

Yes (Notify) No

Management Blades

SmartEvent

Manage, report, and analyze events

Compliance

Meet regulations through best practices

Infinity Playblocks

UPGRADED

Collaborative threat prevention

Infinity AI Copilot

UPGRADED

AI-Based security assistant

Infinity Identity

NEW

Authenticated access to sensitive resources

Infinity AIOps

NEW

Preventive infrastructure monitoring

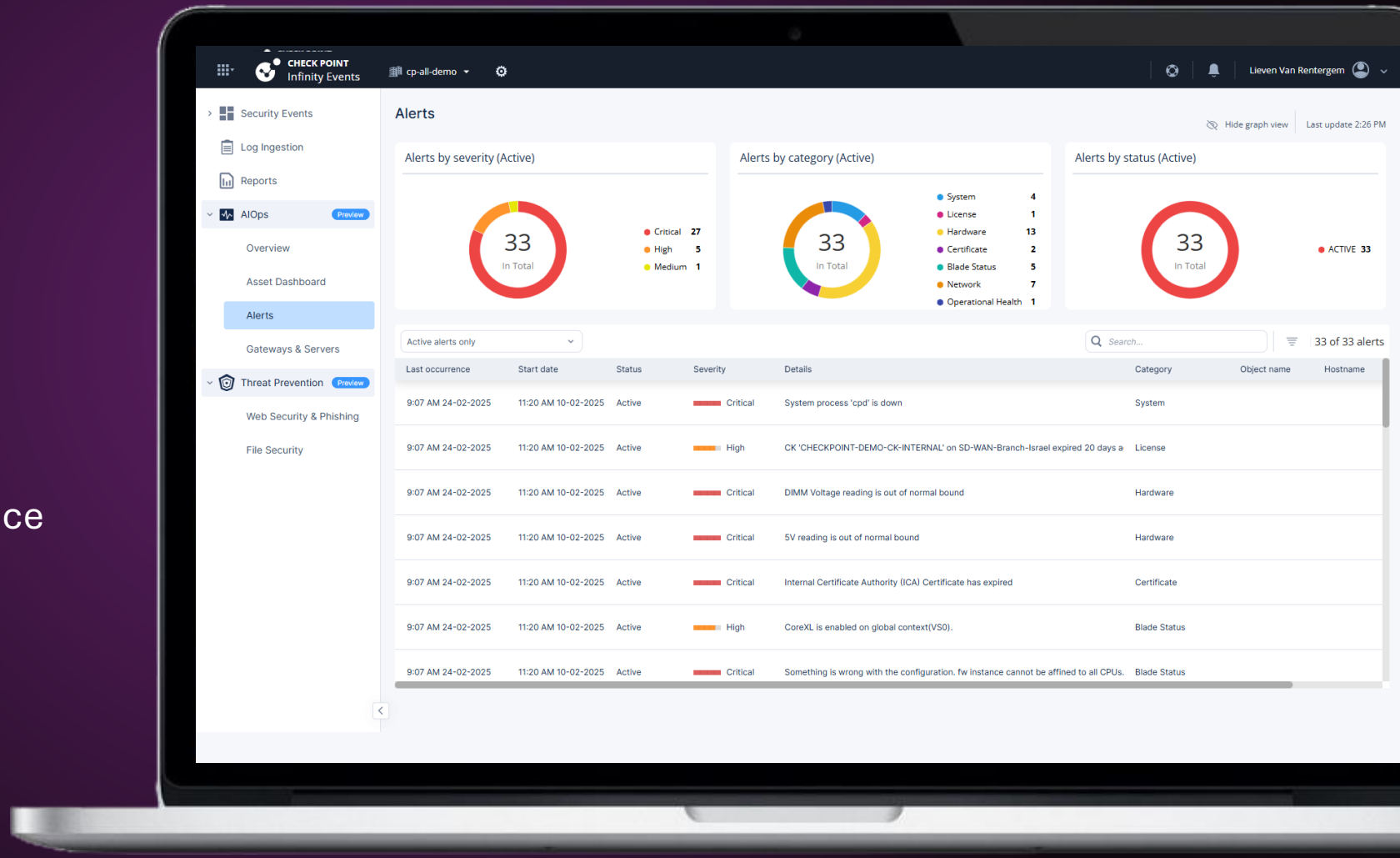
Introducing AIOps

Proactive, actionable monitoring AI Agent

NEW!

Cloud Based Monitoring AI Agent

- Gateway Monitoring as a cloud service
- Live and historical monitoring data
- Real-time alerts
- Health insights and predictions (H2)
- Auto escalation to support (H2)



Management Blades

SmartEvent

Manage, report, and analyze events

Compliance

Meet regulations through best practices

Infinity Playblocks

UPGRADED

Collaborative threat prevention

Infinity AI Copilot

UPGRADED

AI-Based security assistant

Infinity Identity

NEW

Authenticated access to sensitive resources

Infinity AIOps

NEW

Preventive infrastructure monitoring

Quantum Policy Insights

NEW

Optimize policy & ensure zero trust

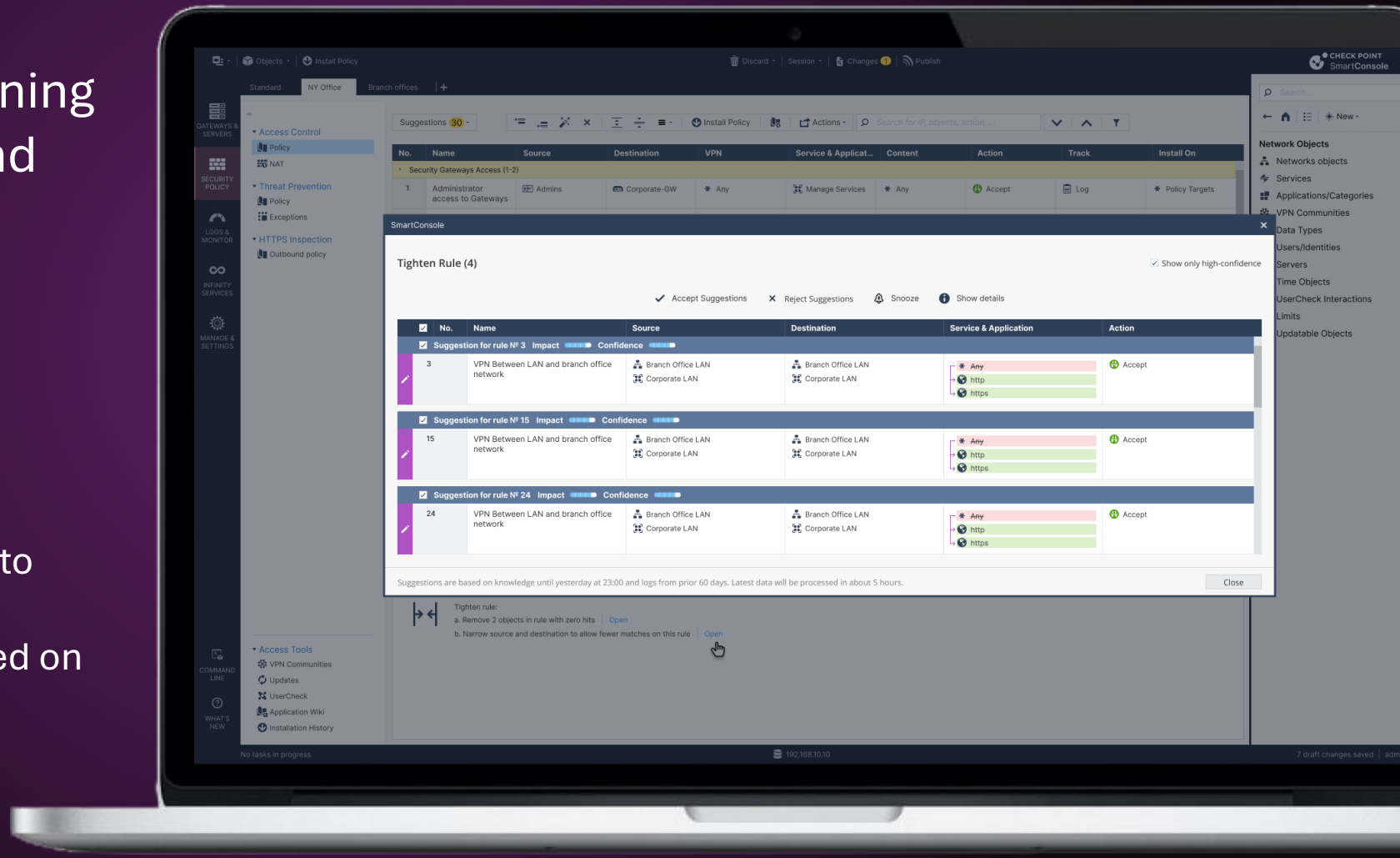
COMING SOON

Policy Insights

AI-powered Policy Hardening, Driving to Zero Trust

Level 2: AI Augmented

Continuous Security hardening based on network traffic and policy analysis



- Optimize users and network groups to least privileges
- Optimize over-permissive rules based on actual flows
- Remove unused objects in policies

Management Blades

SmartEvent

Manage, report, and analyze events

Compliance

Meet regulations through best practices

Infinity Playblocks

UPGRADED

Collaborative threat prevention

Infinity AI Copilot

UPGRADED

AI-Based security assistant

Infinity Identity

NEW

Authenticated access to sensitive resources

Infinity AIOps

NEW

Preventive infrastructure monitoring

Quantum Policy Insights

NEW

Optimize policy & ensure zero trust

COMING SOON

Quantum Policy Auditor

NEW

Assure compliance with security guidelines

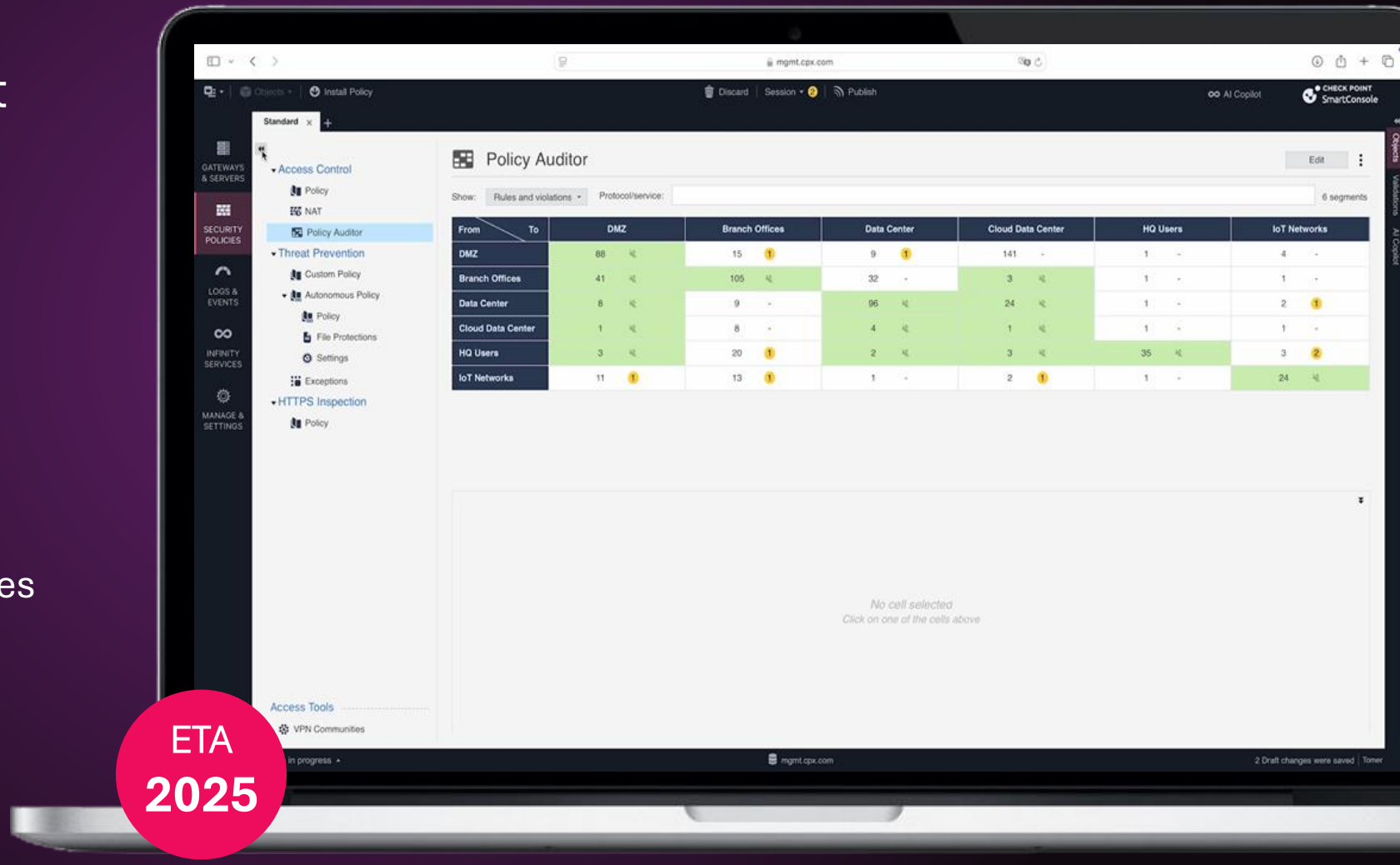
COMING SOON

Policy Auditor

The CISO check-up

Level 2: AI Augmented

High-Level visibility to least privilege access violations



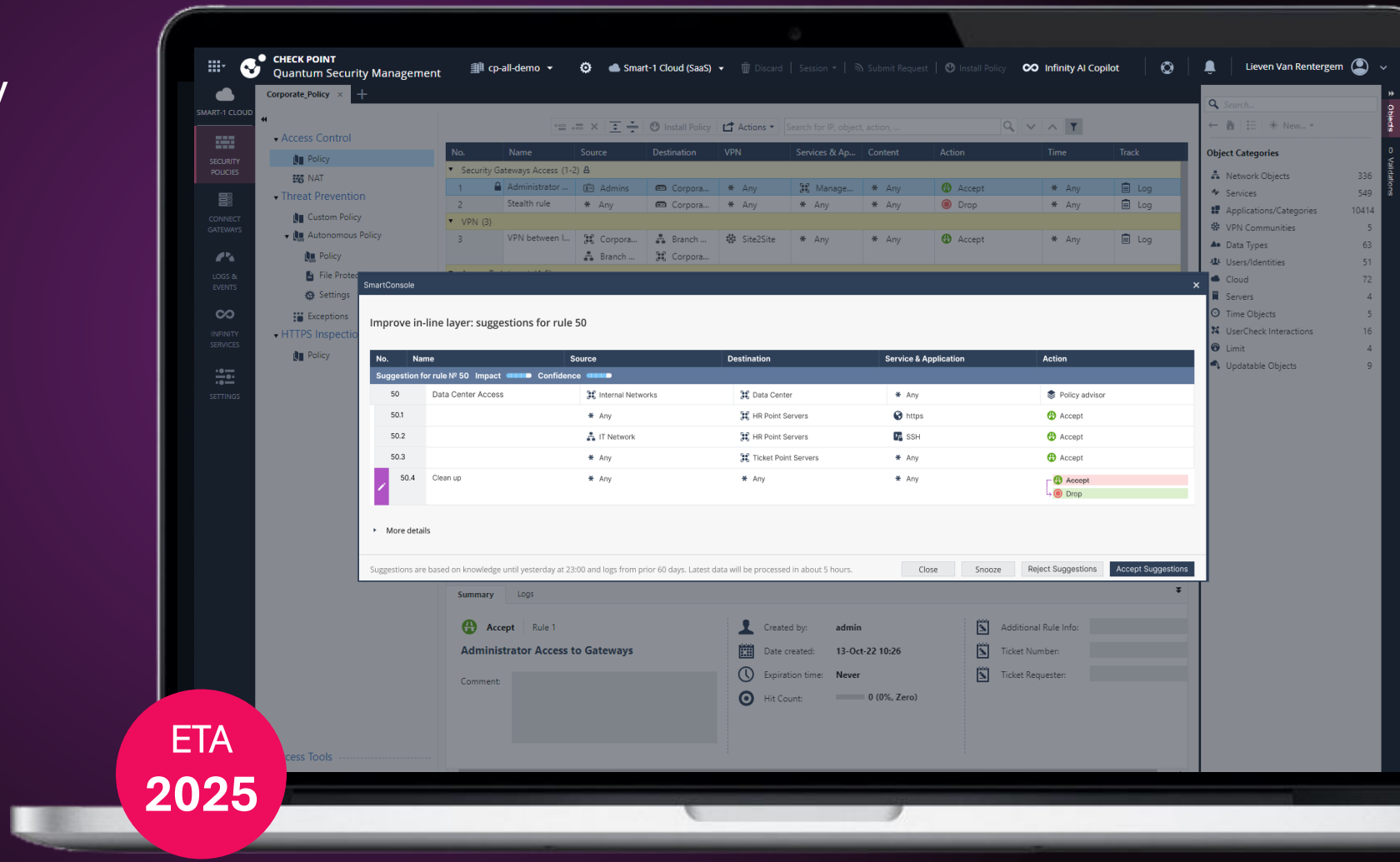
- Align Policies with Security Guidelines
- Highlight violations and drive fast mitigation
- Integrated into R81.20 and above

Autonomous Policy Builder

Taking Security Policy Management to the Next Level

Level 2: AI Augmented

Autonomous Access Policy creation and tuning based

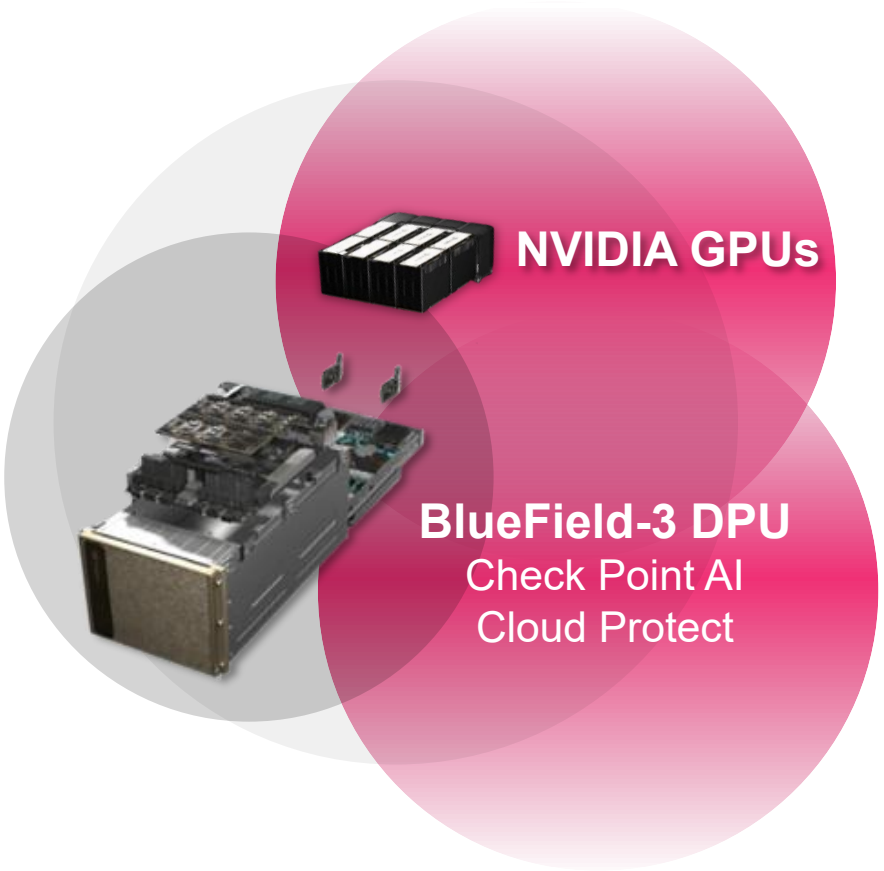


ETA
2025

02

Wie können wir KI und die Ergebnisse schützen

Security for AI



Protect the AI Makers

- Infrastructure level: Protect the NVIDIA® Data Center
- Application level: LLM WAF- prompt injection protection, jailbreaks

Infinity Platform Services

GenAI Tools
Boost Productivity,
But Add Exponential Risk:

New GenAI apps are introduced daily; **not all are trusted**

Increased data loss events due to GenAI usage

New regulations demand **more visibility and control**

Gen AI Protect

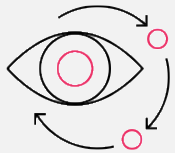
Safely adopt generative AI services in your organization

Discover and Assess Risk of Gen AI Usage

See GenAI tools used in your organization, their purpose, and risk

Prevent Data Loss In Real Time Using AI

Reduce the risk of data leakage with AI-based data classification engine

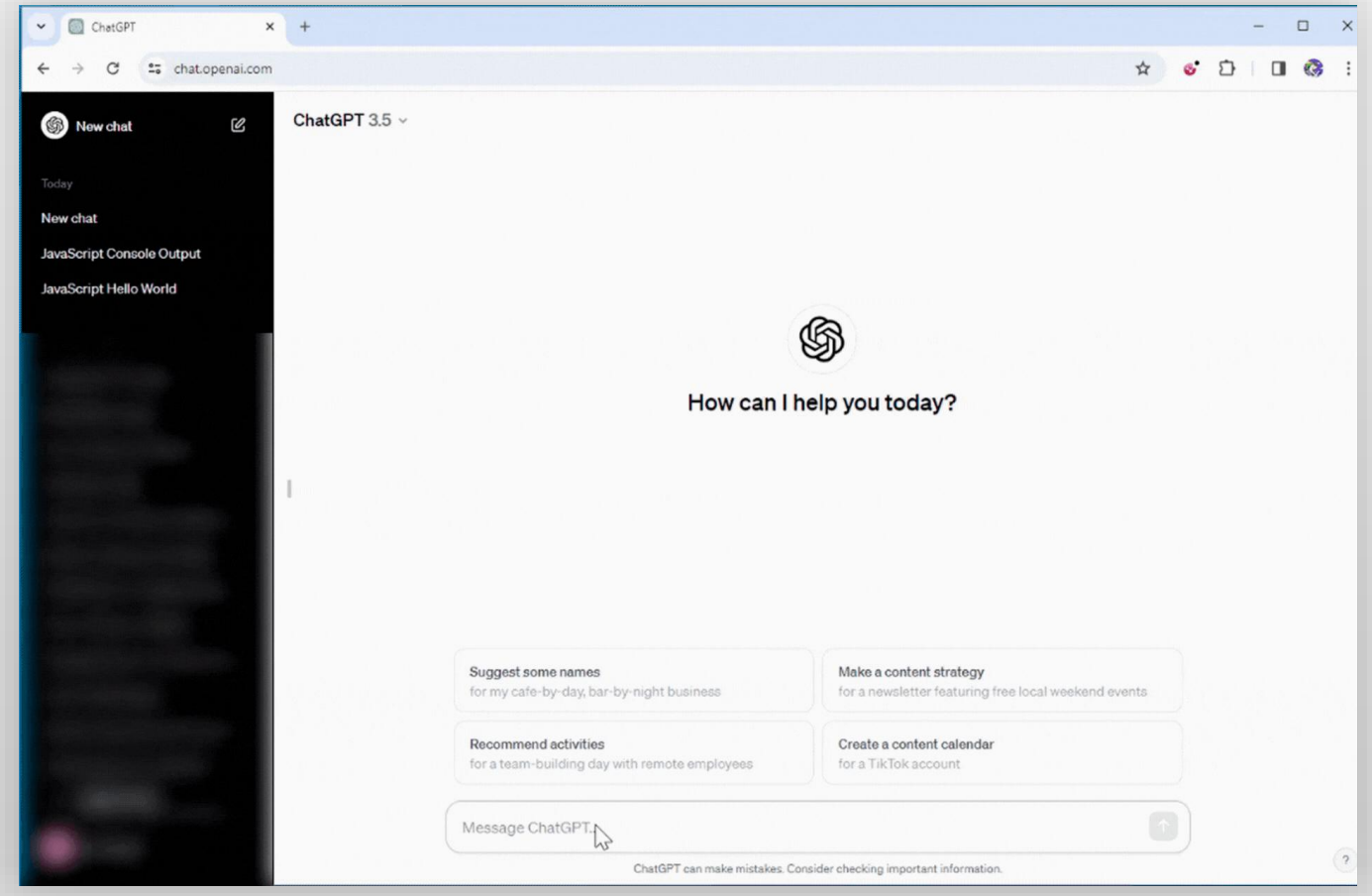


Meet Regulations With Enterprise-Grade Visibility

Get granular monitoring and audit trail to facilitate regulatory compliance

AI-Powered. Cloud Delivered.

Prevent Data Loss Via GenAI Apps



Keeps intellectual property safe

Key features:

- Discover and assess risk of GenAI usage
- AI-powered classification of unstructured data
- Copy/paste restrictions
- Customizable policy
- Meet regulations with enterprise-grade visibility and reporting

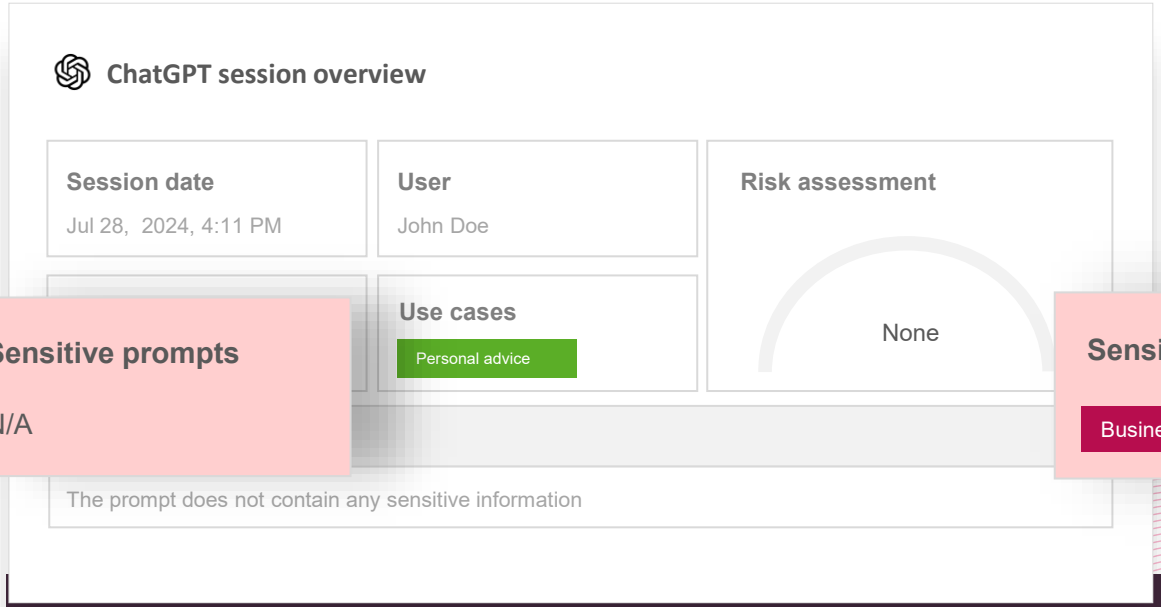
55%

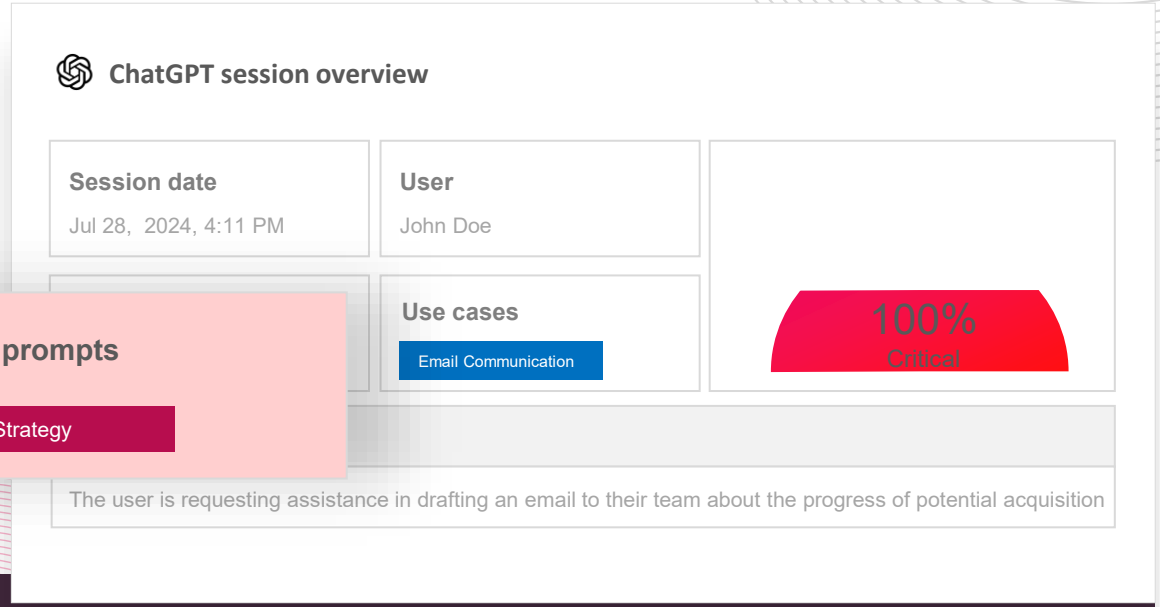
of data loss events are due to GenAI

LLM-based data classification

I am about to **acquire a $300 pair of running shoes**. Build me a personal training plan for the next three months.

We are preparing to **acquire Best.ai for $470M**, to boost our advertising service. Suggest an internal communication email.



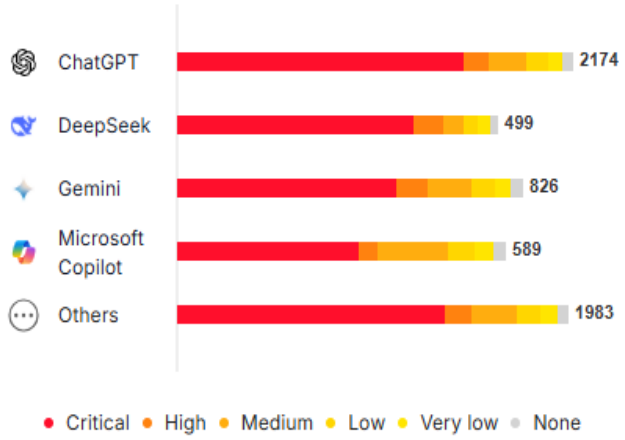


Accurately identify context and data sensitivity in conversational prompts

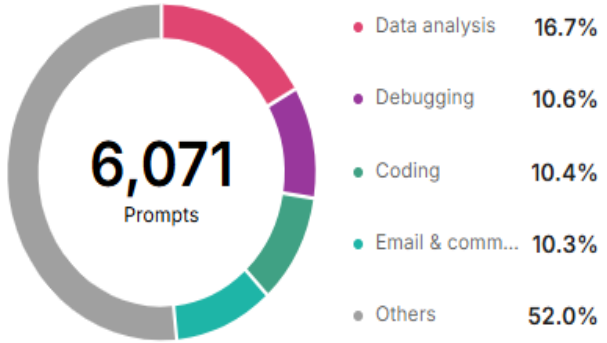
Last 7 days

Dashboard
Compliance
Ecosystem
Insights
Events
GenAI Protect

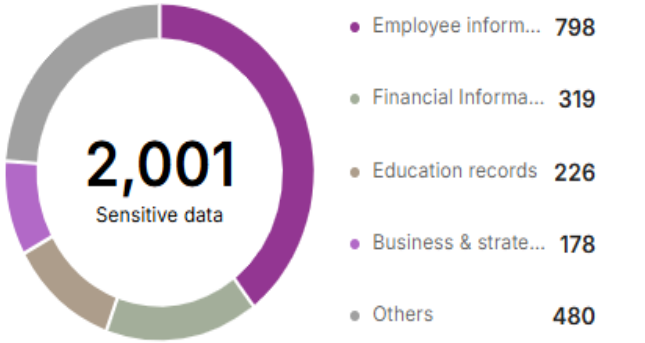
Risky sessions by app



Use cases



Sensitive data types



Total sessions 6,071 | Applications 20 | Sensitive data types 21 | Use cases 22 | Users 425 | Services 5

Preset Filters

Search this table...

1–25 of 6,071

Session risk	Application	Description		Use cases	Sensitive content	Users	Enforcement	Date & Time
Low	Design.ai	The prompt is a ...	More >>	Coding	-	Brian Sanchez		Nov 18, 2025, 3:1...
Medium	Microsoft Copi	The prompt is a ...	More >>	Grammar	-	Esther Torres		Nov 18, 2025, 3:1...
None	DeepSeek	The prompt doe...	More >>	+1	-	Helena Alexander		Nov 18, 2025, 3:1...
Low	Microsoft Copi	The prompt doe...	More >>	Debugging	-	Xerxes Turner		Nov 18, 2025, 3:1...

Summary

- Wo können wir KI einsetzen
- Wie können wir den Gebrauch von KI schützen

CHECK POINT™

Thank You!

YOU DESERVE THE BEST SECURITY