CHECK POINT

Check Point CHECKMATES

CPX 2024 Recap

Highlights from our recent CPX 2024 Events

YOU DESERVE THE BEST SECURITY

Check Point 2024:

The Platform Company

AI-Powered

Cloud-Delivered

Comprehensive | Consolidated | Collaborative

CHECK POINT

Check Point Infinity Platform

AI-Powered, Cloud-Delivered

Quantum
Secure the Network

CloudGuard
Secure the Cloud

Harmony
Secure the Workspace

Infinity Core Services

2024 New Product Announcements

AI-Powered. Cloud-Delivered

Quantum

AI Copilot for Quantum
Quantum Force: 10 New Appliances, 2X Threat Prevention
Quantum OS R82, with 95 New Features
Spark New OS, with SD-WAN and IOT
Spark Gateways - 5Gbps Threat Prevention

CloudGuard

CloudGuard WAF as-a-Service
CloudGuard Network Azure vWAN Hub
New Effective Risk Management
CDR - Cloud Detection and Response

Harmony

Game-Changing SASE
SaaS Security
Endpoint Posture
Unified Phishing View
DMARC management

Infinity Core Services

ThreatCloud New AI Engines, 99.8% Prevention Rate of Zero+1 Day Malware
Infinity Playblocks
Infinity XDR/XPR 20 Connectors for 3rd Party Products
AI Copilot for XDR/XPR
New Infinity Data Centres in UAE and China
Infinity for MSSP with Pay-as-you-Go

What’s new in Quantum

Infinity AI Copilot

Your Most Powerful Security Teammate

Powerful, Generative AI engine

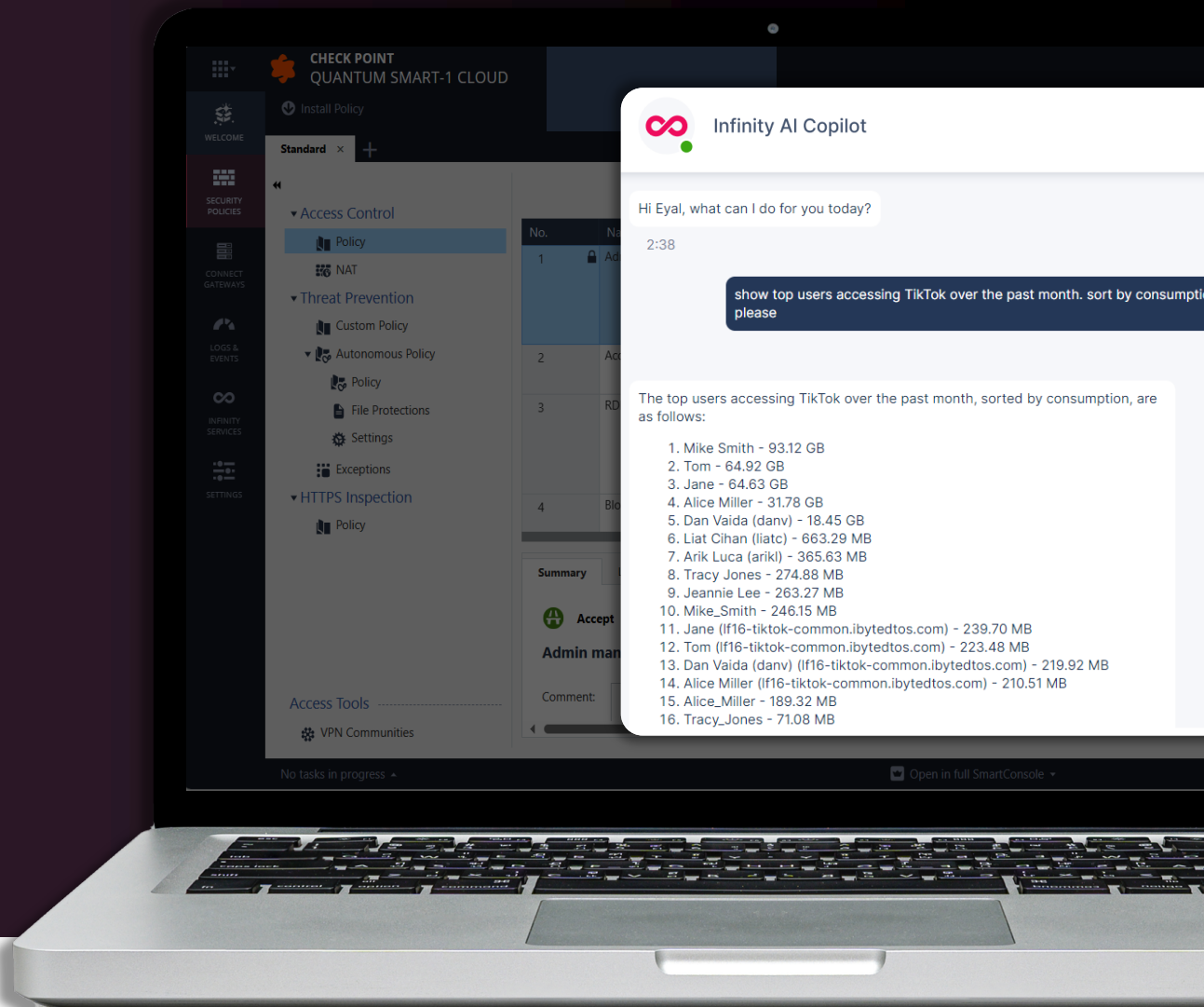
Embedded in the Infinity Platform

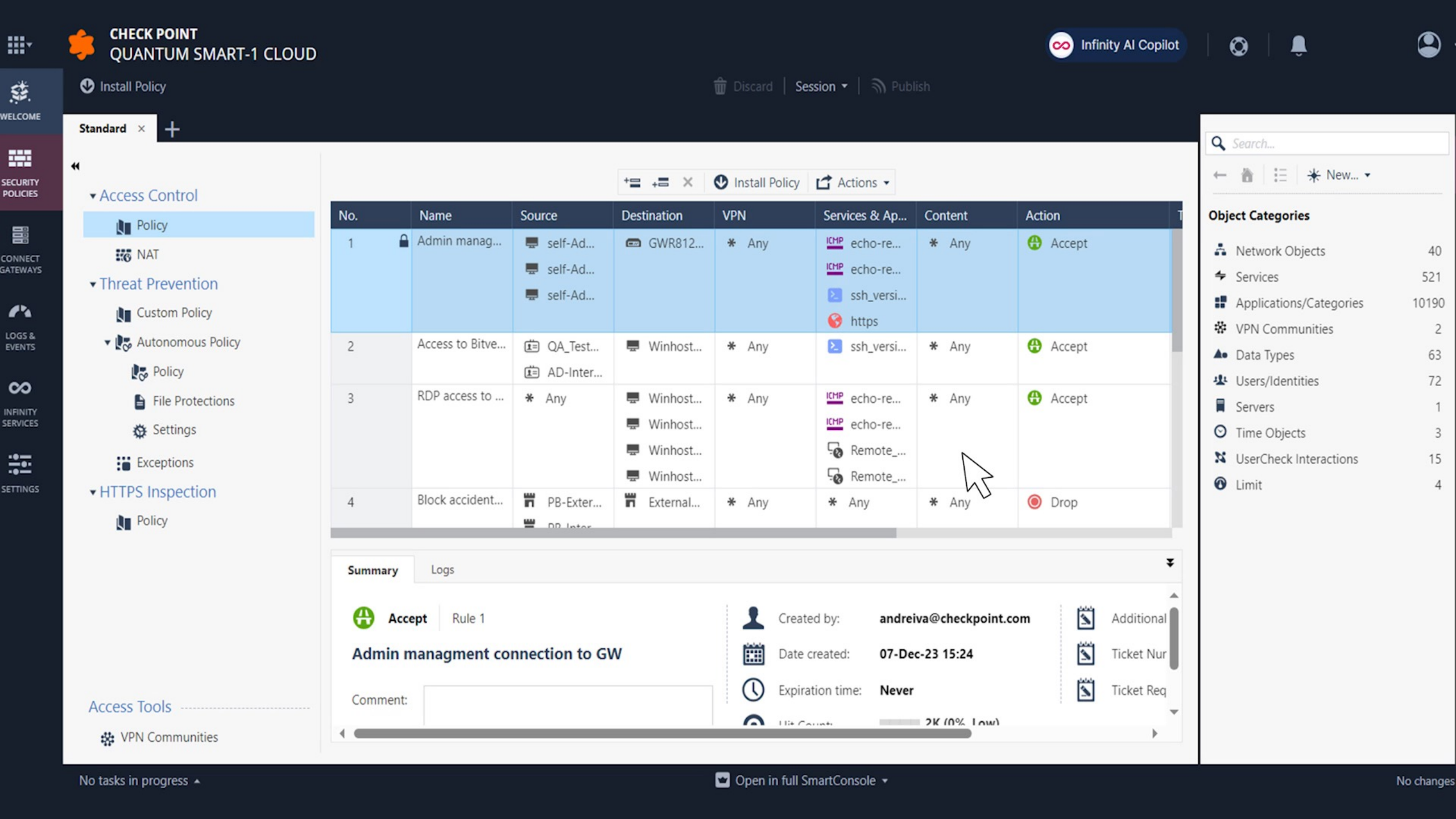
NEW

Security Admin Copilot

NEW

Security Analyst Copilot




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 40
Services 521
Applications/Categories 10190
VPN Communities 2
Data Types 63
Users/Identities 72
Servers 1
Time Objects 3
UserCheck Interactions 15
Limit 4
No tasks in progress
Open in full SmartConsole
No changes

Am I protected against MOVEit Transfer attacks?

Infinity
AI Copilot

Hi Eyal, what can I do for you today?

00:10

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?

00:11

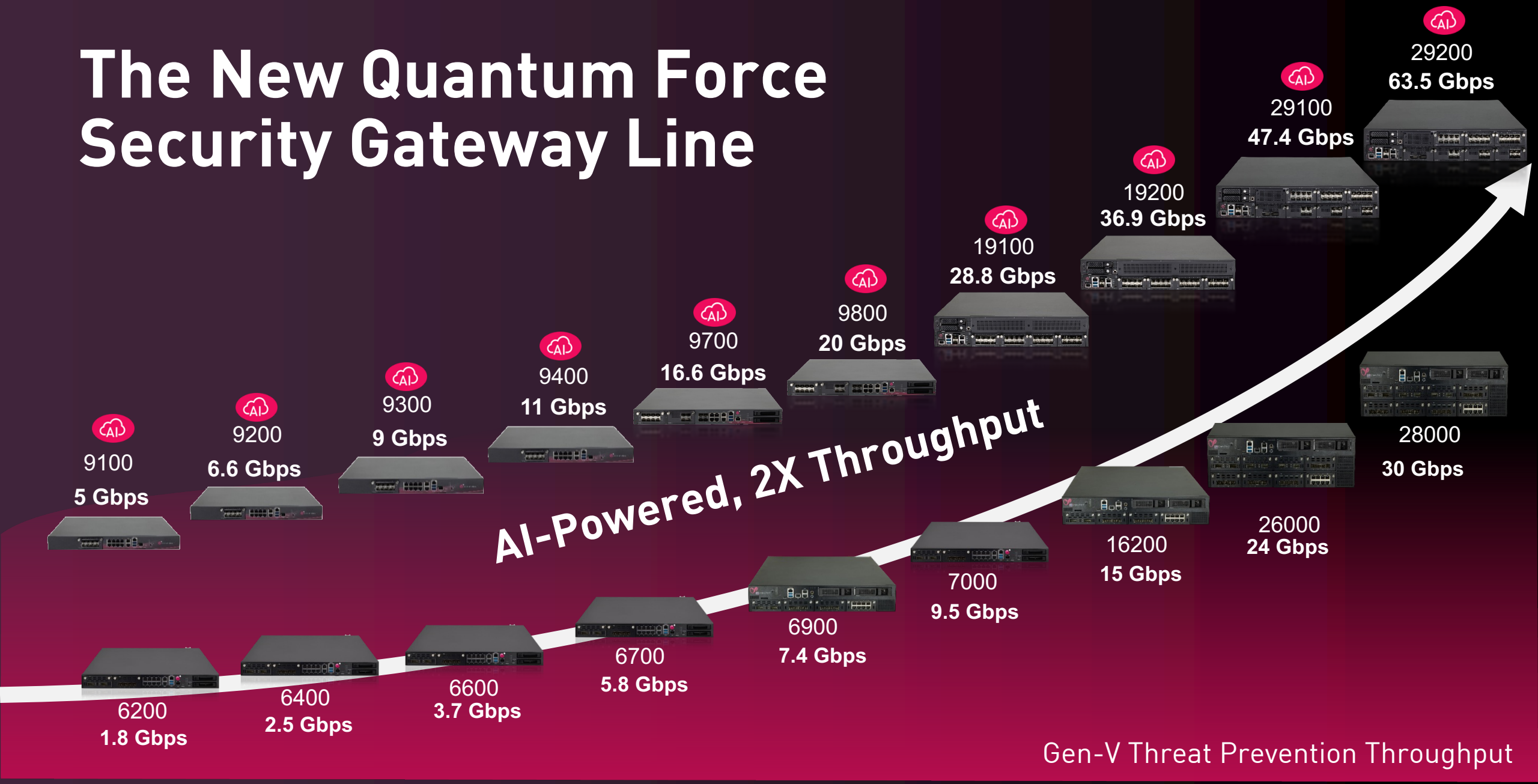
Yes. There were 16 attempts to exploit this attack in the last 30 days. The last attempt was on 2024-01-03 at 13:59:41.

Just now

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

Yes (Notify) No

The New Quantum Force Security Gateway Line

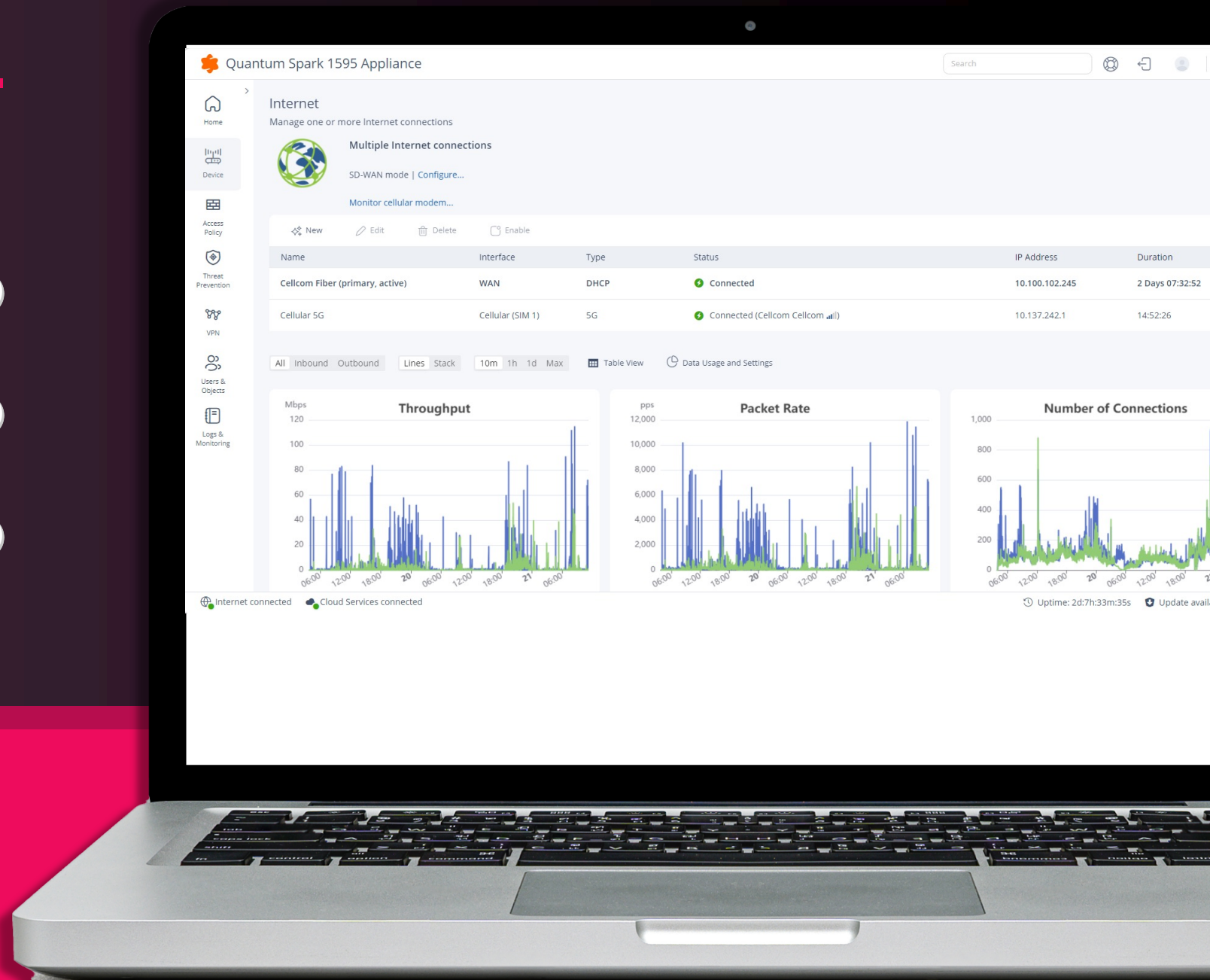


Quantum Spark for Small and Medium-Size Organizations

New Local Management UI NEW

Integrated SD-WAN NEW

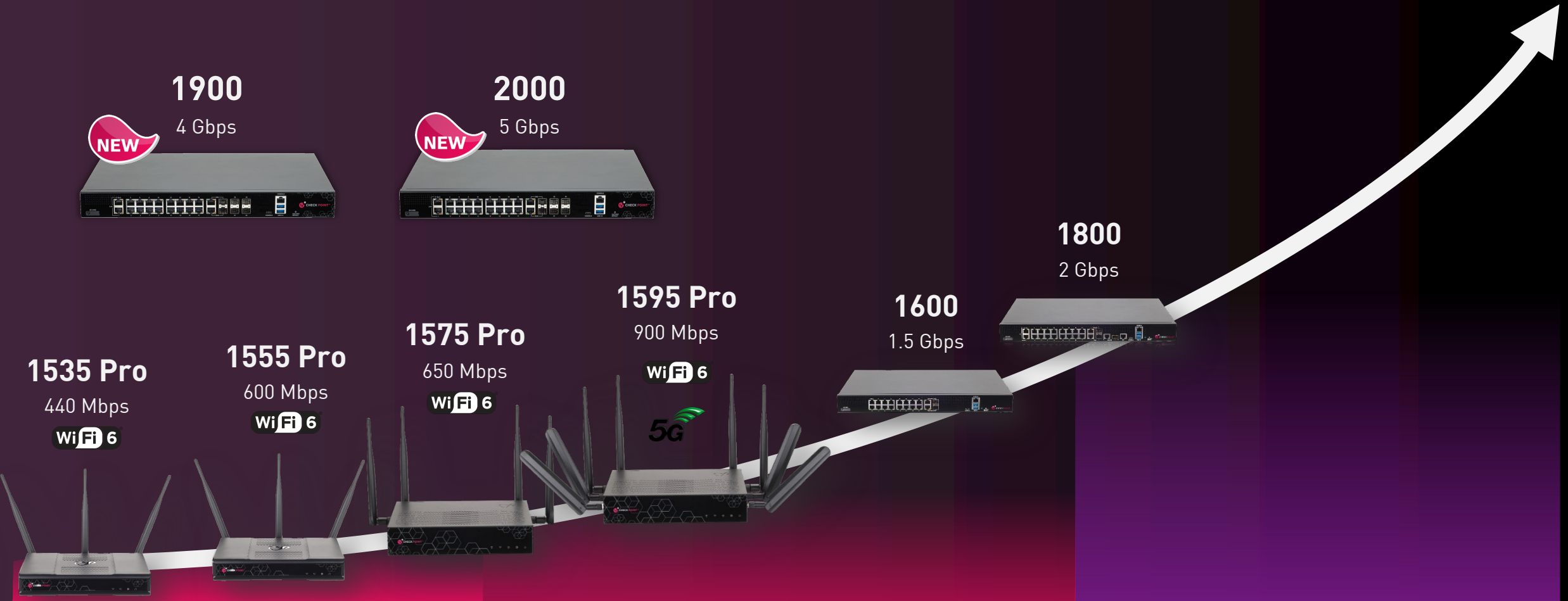
Autonomous IOT Security NEW



CHECK POINT

Extending Quantum Spark to 'Small Enterprises'

Up to 1,000 users. 2X Performance. Affordable Price



Small Organization (1-50 Users)

Midsized Organization (50-500 Users)

Small Enterprise (500-1000 Users)

COMPREHENSIVE

New intuitive user-friendly UI

Quantum Spark 1595 Appliance

Search

CHECK POINT

Home
Device
Access Policy
Threat Prevention
VPN
Users & Objects
Logs & Monitoring

- Overview
  - System
  - Security Dashboard
  - Security Management
  - Cloud Services
  - License
  - Site Map
- Monitoring
  - Notifications
  - Assets
  - Monitoring
  - Reports
- Troubleshooting
  - Dr. Spark
  - Tools
  - Support

AviG-home

WatchTower mobile app

Model	Version	MAC address	Management
1595 Appliance	R81.10.10 (996002508)	00:1C:7F:B5:8C:CB	Locally managed

Internet 2 — Internet connections

Cellcom Fiber (primary)	DHCP	WAN	10.100.102.245
Cellular 5G	Cellular	Cellular	10.156.198.31

WiFi — WiFi networks

Wireless radio (2.4GHz, 802.11b/g/n/ax) is turned off

Wireless radio (5GHz, 802.11a/n/ac/ax (5GHz)) is turned off

Assets 30 — Manage assets

No infected assets

Monitoring

Throughput | Packet Rate

Notifications 50

- A connection of type Web was initiated by administrator avi to WebUI. 17:24:16 27 Dec 2023
- A connection of type Web was initiated by administrator avi to WebUI. 17:07:15 27 Dec 2023
- A connection of type Web was initiated by administrator avi to WebUI. 16:47:45 27 Dec 2023

COMPREHENSIVE

New Quantum Spark Software Blades

Next Generation Firewall

Firewall
VPN
Application-Control
IPS

Next Generation Threat Prevention

Next Generation Firewall +

Anti Virus
Anti Bot
URL Filtering
Anti Spam
Advanced DNS

Sandblast - Gen V Threat Prevention

Next Generation Threat Prevention +

Threat Emulation

Quantum IoT

IoT discovery
IoT threat prevention

R81.10.10

Quantum SD-WAN

Application prioritization
Connectivity monitoring
Automated link failover
Bandwidth aggregation

R81.10.10

10 Blades – Best Security

IoT

SD-WAN

Quantum Cyber Security Platform

More Security. Simpler Operations.

NEW
R82

Unique to Check Point

Effortless
TLS Inspection

Complete Protection
for HTTP/3 over **QUIC**

API-Based
Dynamic Policy Layer

50+
New, Innovative Features

CHECK POINT

Unified Clustering Experience

ElasticXL

New Active-Active
Orchestrator-less Cluster

Unified cluster UX for all platforms

Central configuration & monitoring and Image cloning

Improved MGMT: Single Management Object, same API as regular GW

Description	ClusterXL	Maestro	ElasticXL
Single management object	-	+	+
Applying changes from single member to all members	-	+	+
Add new cluster member in single command	-	+	+
Installable on VM/KVM***	-	-	+

* Still under discussion

Virtualization and Simplicity

VSNext

New VSX Architecture

VSX as a native solution in every Security Cluster running Gaia

User-experience unification with Security Gateway (MgmtAPI, GaiaAPI)

Operational performance improvements, Full WebUI support

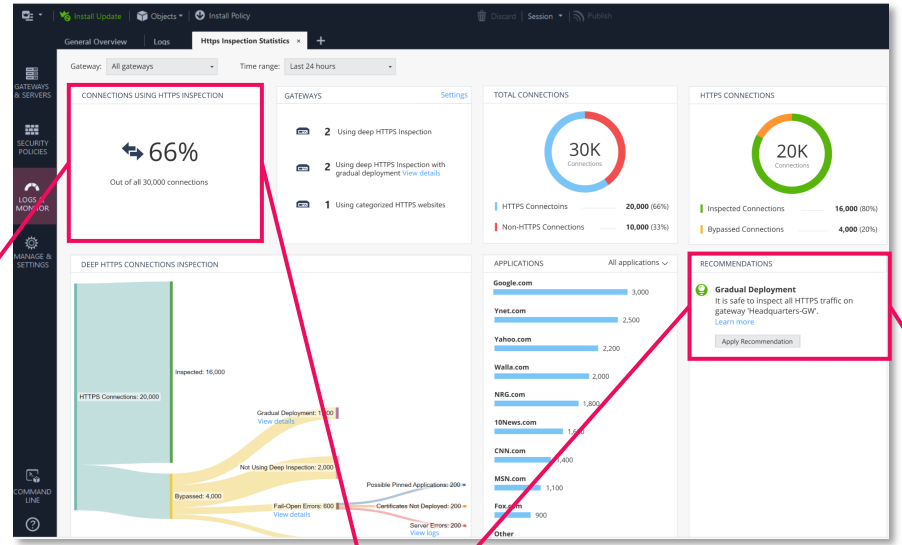
	VSNext	VSX
Provisioning API	GaiaAPI, WebUI, Clish	SmartConsole only
Upgrade tools	As regular gateway	Unique tools
Management representation	VSs can be in different SMC	All VSs in the same SMC

Non-disruptive TLS inspection

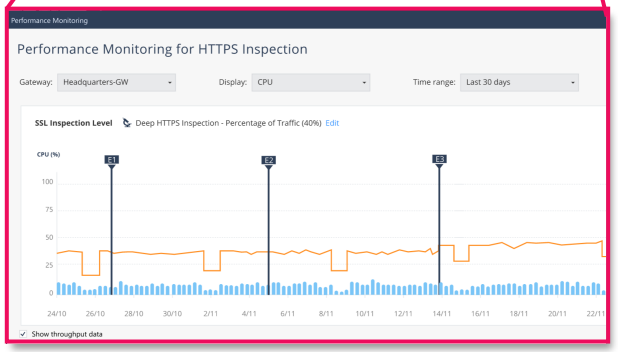
Zero-connectivity issues

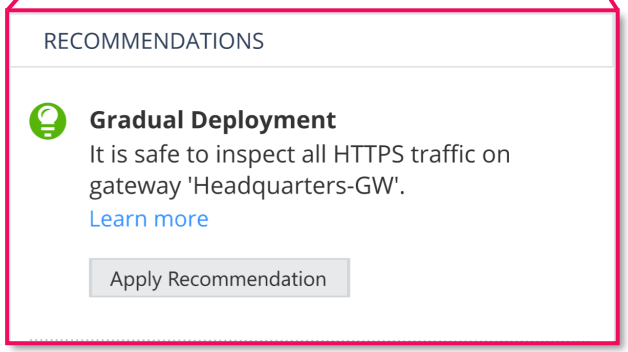
- Automated updates for **trusted sites** and **pinned** applications

NOW



- Support HTTP/3 protocol over **QUIC transport**
- **Gradual** deployment process
- Full **Fail-open-mode**
- **Bypass** under load



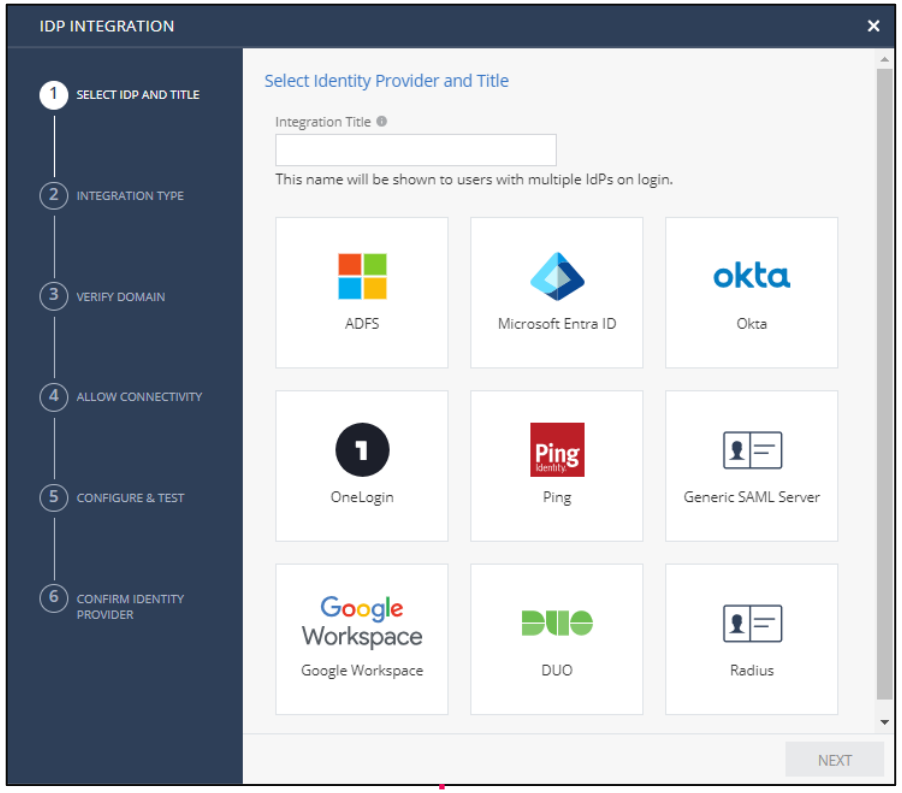


Identity Management

Centrally manage Identity providers to all Check Point products from the **Infinity Portal**

Enhance identity sharing resiliency using **Cache Mode** in case of connectivity issues to PDP

Scalability Boost with New mode - **“PDP-Only”** mode in learning & sharing identities



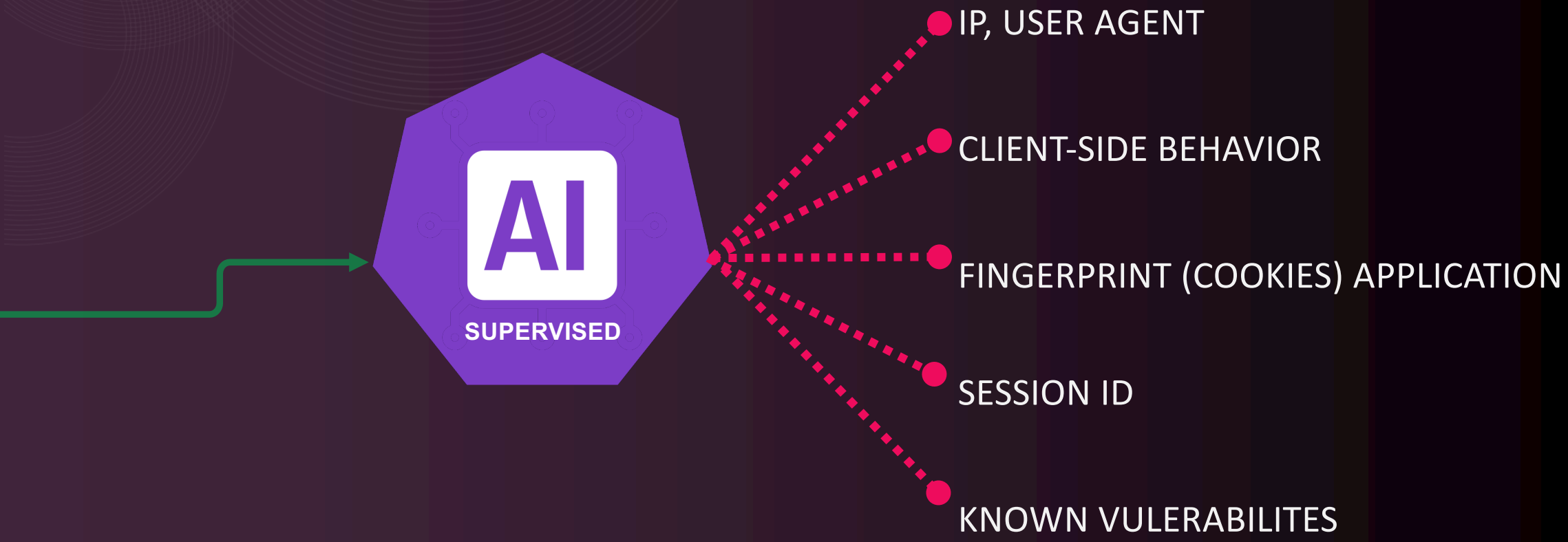
Over 50 More Capabilities…

- **Management scale:**
  Managing 500 gateways from Management Server, Domain or Smart-1 Cloud
- **Multi-Domain Enhancements:**
  Improving upgrade time by 50%, adding the option to clone domain
- **HyperFlow Multi-Core Processing:**
  Supporting CIFS and UDP traffic
- **Site-to-Site VPN resiliency with public cloud:**
  Automatically adjust to changes on AWS, GCP & Azure to ensure connectivity
- **Additional upgrades use cases from SmartConsole:**
  Upgrade of 2nd management, log server and more

R82

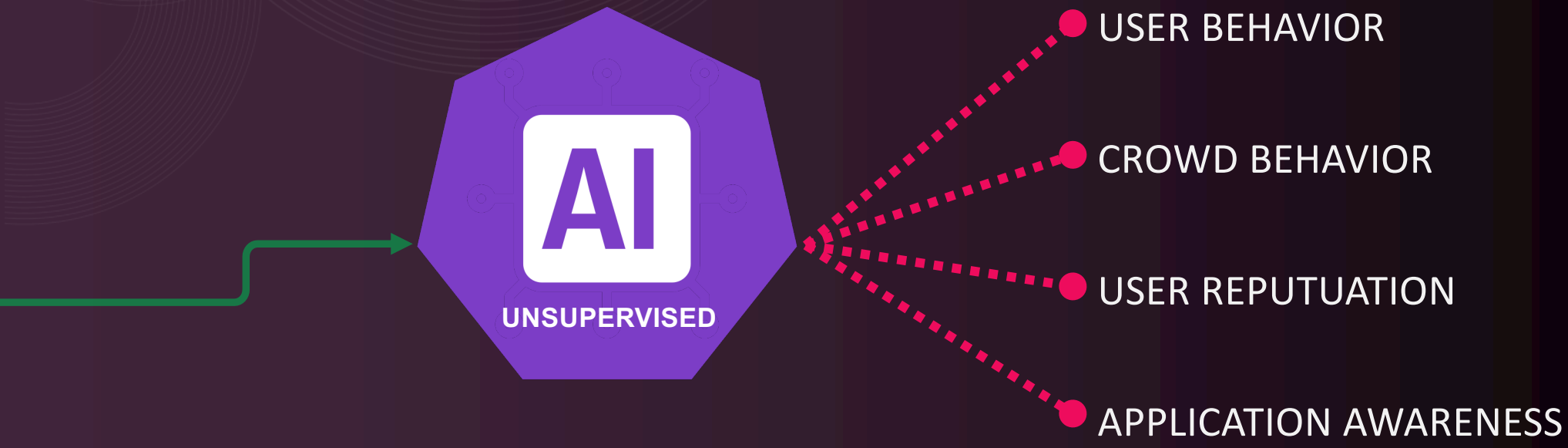
What’s new in CloudGuard

STAGE 1: ATTACK INDICATORS ENGINE



OLD SCHOOL WAFS STOP HERE

STAGE 2: ADVANCED ANALYSIS ENGINE

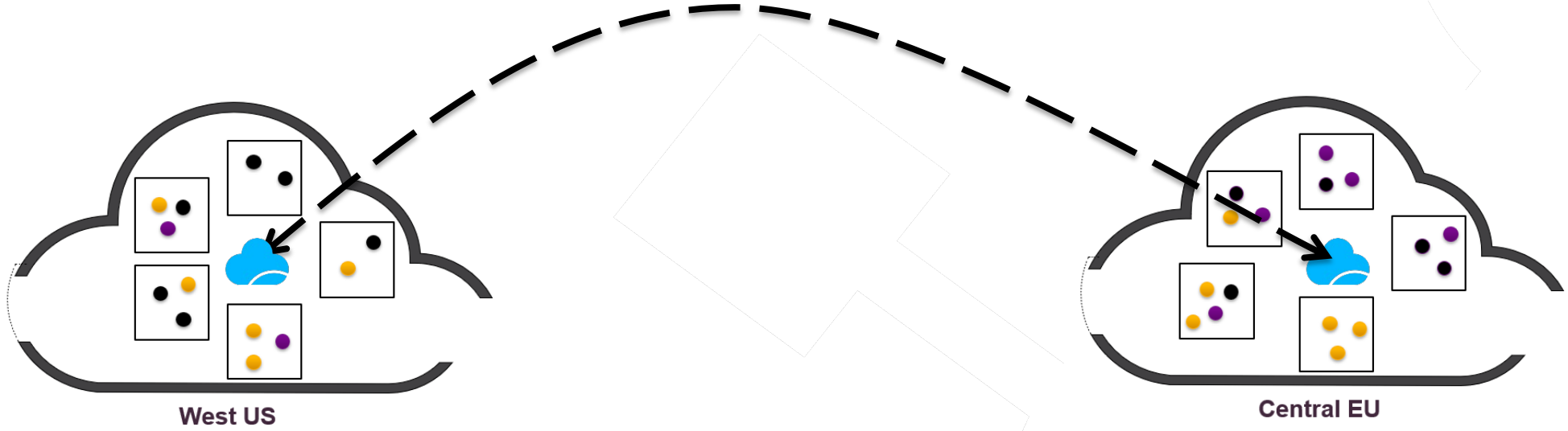


API Discovery

Schema Validation

CloudGuard
Network

Cloud-Native with Azure vWAN



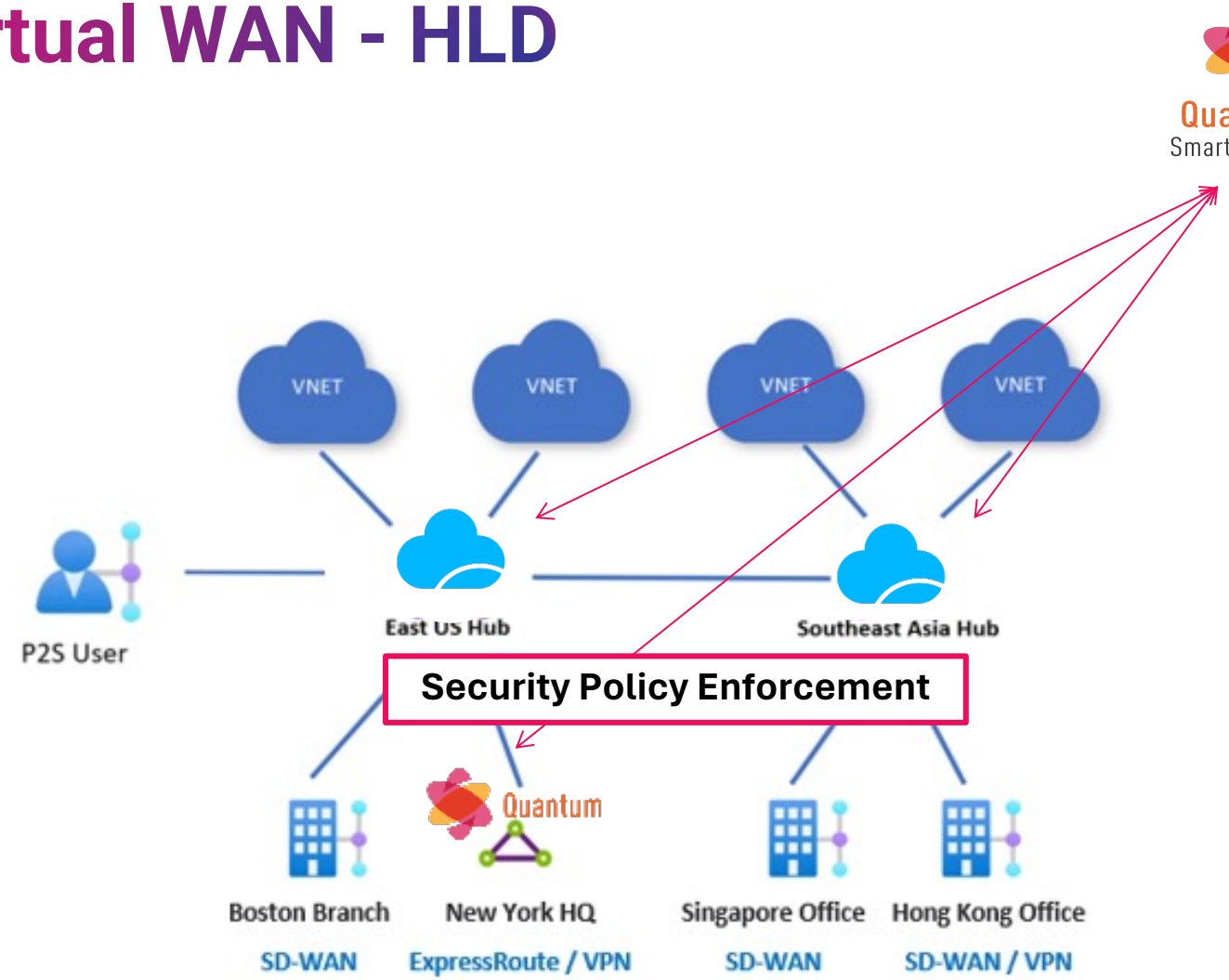
Integrate Check Point Network Security natively into Azure networking infrastructure

Azure Virtual WAN – What is New

- ✓ **Built-in availability and resiliency**
  - ✓ Availability Zone aware and configured to be highly available automatically
- ✓ **Reduced networking complexity**
  - ✓ Simplified Connectivity
  - ✓ Easy configuration of ExpressRoute, SD-WAN branches, and VPN connections
- ✓ **Zero hassle provisioning of CloudGuard Network Security**
  - ✓ Deploy from the Azure Marketplace
  - ✓ Easily apply world-class security between all of your spoke connections

Azure

Azure Virtual WAN - HLD



- Security Policy Configuration
- Logging
- Event Alerting and Reporting
- Compliance
- The benefits of being 100% SaaS (no maintenance or monitoring, always running the latest code)

Azure

CloudGuard

INTRODUCING A NEW PARADIGM IN CLOUD SECURITY

CNAPP

Cloud Native Application Protection

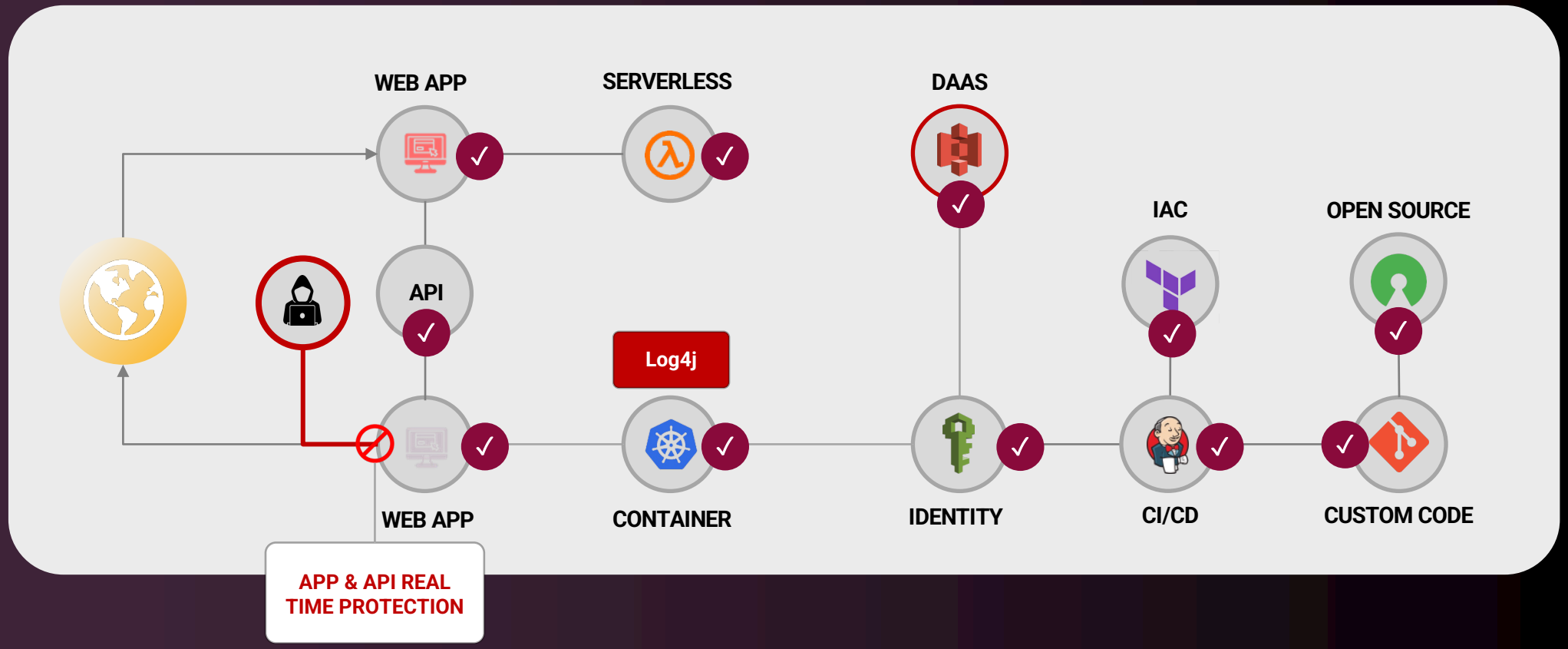
+ Prevention Platform

CLOUDGUARD'S PROPRIETARY AI AUTOMATICALLY PROTECTS AGAINST DEVASTATING ZERO DAY ATTACKS

Cloud Native Application Protection Platform (CNAPP)

CONTEXT-BASED RISK MGMT. | SECURITY POLICY & COMPLIANCE | DETECTION & SMART PROTECTION

Unified Platform — CDR · WAAP · CWPP · CSPM · DSPM · CIEM · IaC Scanning · SCA · Code Scanning



COMBINING TWO SECURITY PHILOSOPHIES:

PREVENTION FIRST

PRIORITIZING & REMEDIATING RISKS BEFORE GETTING TO PRODUCTION

PROTECTING THE REST

RECOGNIZING UNKNOWN THREATS AND AUTOMATICALLY DETECTING THEM & BLOCKING THEM BEFORE CAUSING ANY HARM

CONSOLIDATED & MODULAR PLATFORM

Consisting of Code Scanning, IaC scanning, SCA, CSPM, CIEM, DSPM, CWPP, CNS, CDR, and WAAP

VALUE-BASED RISK MANAGEMENT

Optimize Security Efforts with Context Based Risk Management & Effective Risk Prioritization

CONTINUOUS CLOUD SECURITY

Automate security requirements & internal policies throughout the development lifecycle (code to cloud)

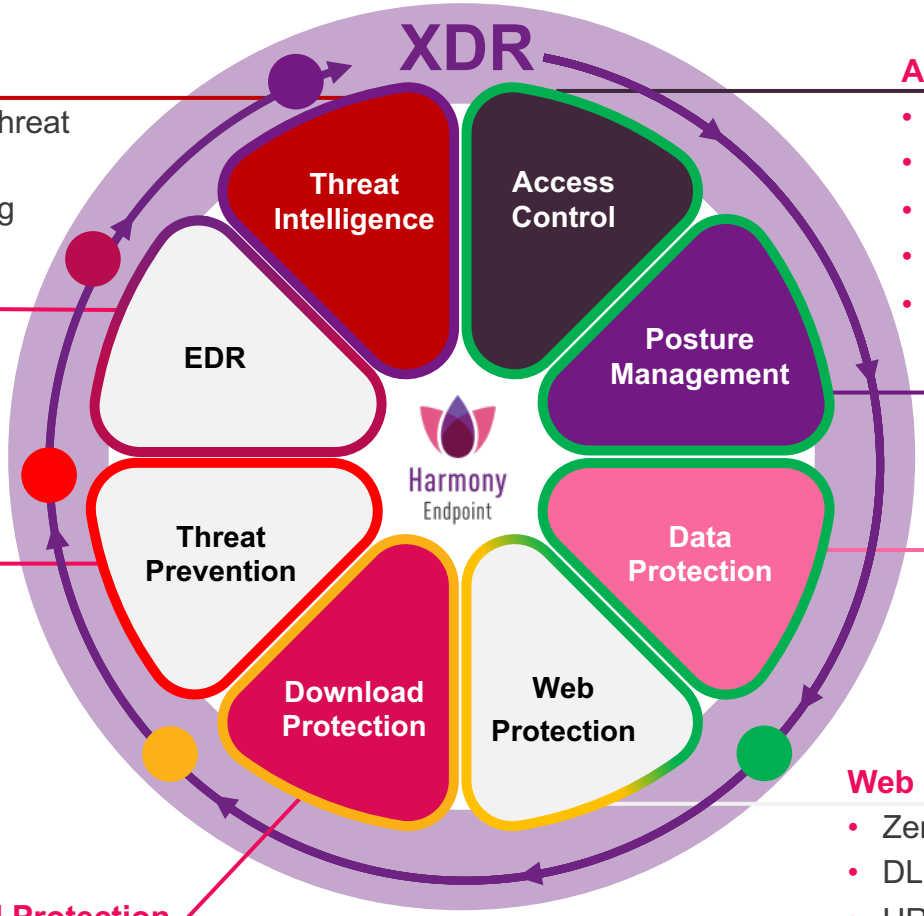
REAL-TIME DETECTION & PROTECTION

Automate Production Protection Against Vulnerabilities that Are Running in Production

What’s new in Harmony

Complete Protection with EPP, EDR & Zero Day Prevention

1. Reduce Attack Surface
2. Prevent Before it Runs
3. Run-Time Protection
4. Contain & Remediate
5. Proactive Analysis & Orchestration



ThreatCloud
- AI Powered Threat Analytics
- Threat Hunting

Detection & Response
- Incident Management
- Research Intelligence
- Automated Reaction
- Triage Tools

Next Gen AV
- Anti-Ransomware
- Anti-Bot
- Anti-Malware
- ML based NGAV
- Anti-Exploit
- Behavioral Guard
- Threat Emulation

Download Protection
- Threat Emulation
- Threat Extraction

Access Control
- Remote Access VPN
- Host Firewall
- Compliance
- Port Protection
- APP Control

Posture Management
- Zero Trust Posture Management
- Vulnerability & Patch Management

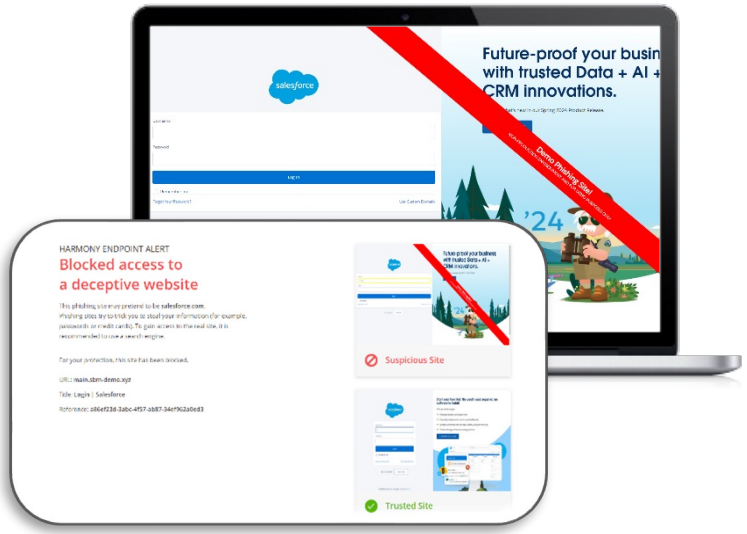
Data Protection
- Media Encryption
- Full Disk Encryption

Web Protection
- Zero-day Phishing
- DLP (Data Loss Protection)
- URL Filtering
- Corporate Password Reuse Protection
- Safe Search

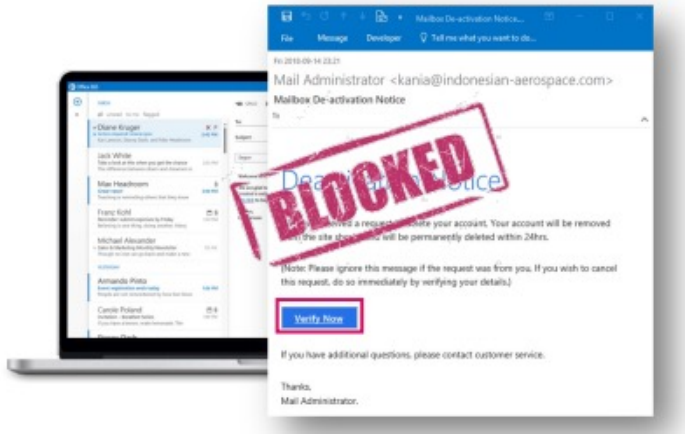
It’s possible to stay protected

With Check Point’s 360° Phishing Protection

Prevent user’s access to phishing sites



Prevent phishing emails from reaching the user’s inbox



Prevent Phishing SMS from reaching the user’s phone

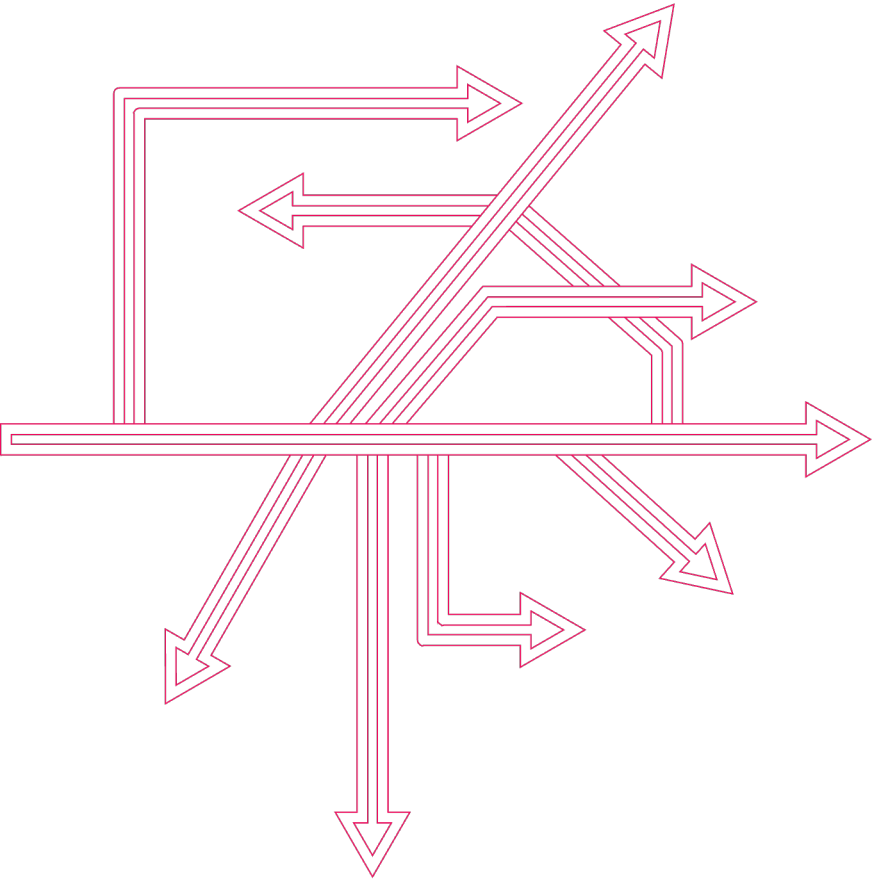
Harmony
SASE

Secure Internet Access

Secure Private Access

Secure SD-WAN

Zero Trust Network Access



Ensure least privilege access to applications

- Based on User Identity
- Based on Device Posture

Connect all users and devices

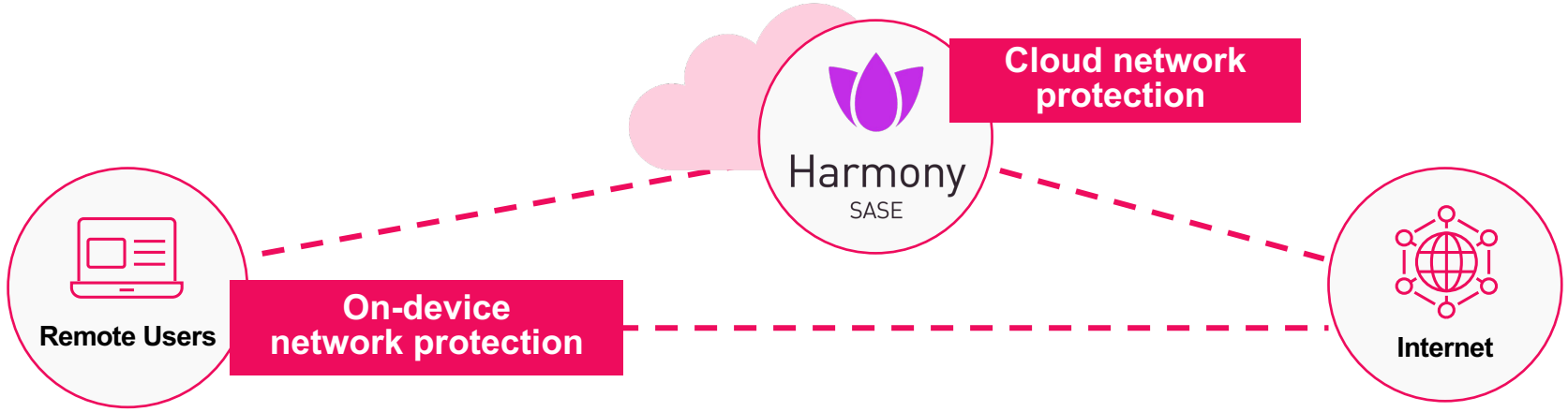
- Lightweight agent for all platforms
- BYOD and contractors – agentless

Minimize the attack surface

- Network segmentation
- Datacenter obfuscation

The Power of Hybrid SASE:

On-Device & Cloud network protections



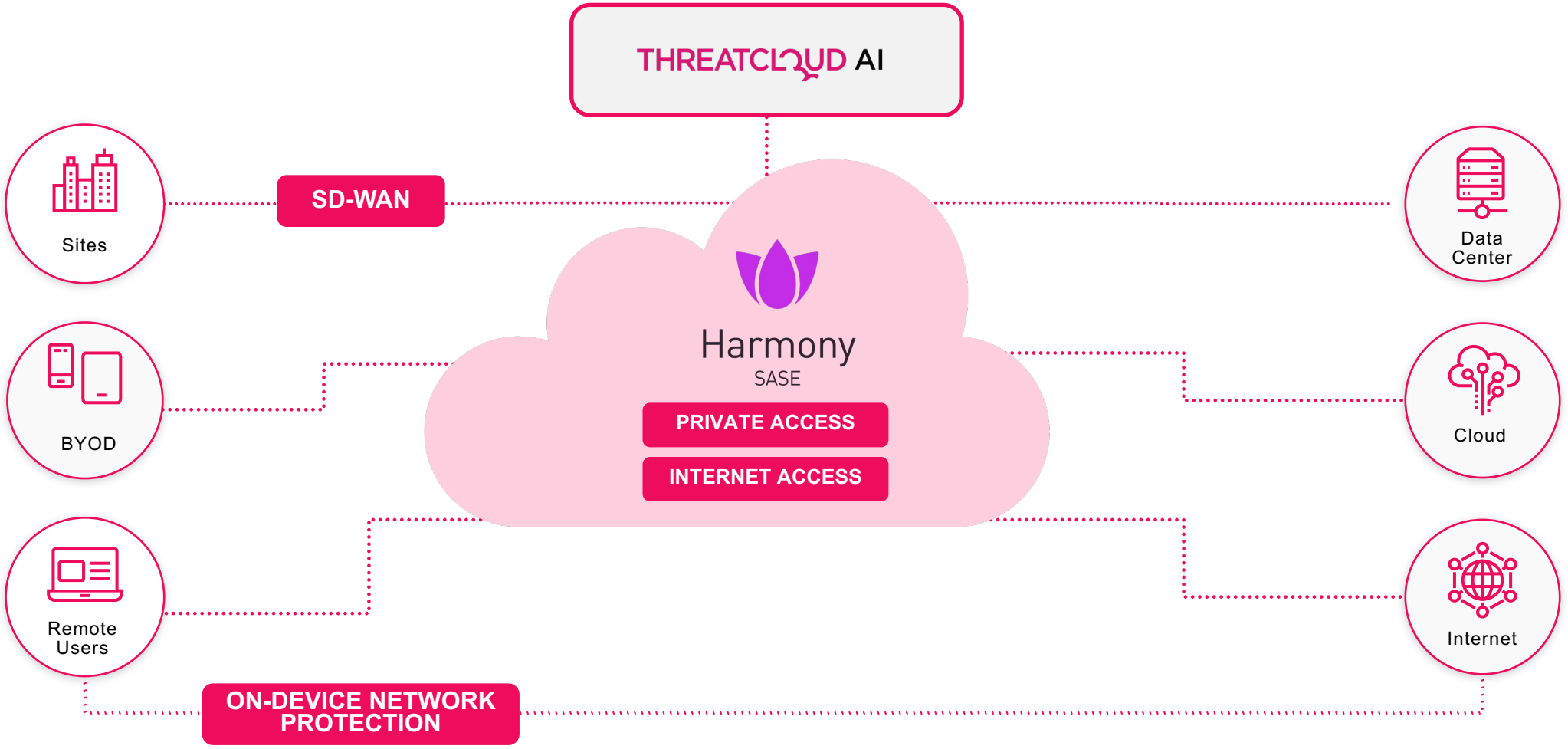
Outstanding user experience & privacy

- On-device network protections
  Avoid routing internet traffic through the cloud
- Avoid cloud latency

Advanced Protections

- Web Filtering
- DNS Security
- Malware Prevention
- Secure Wi-Fi traffic

Single-Vendor SASE with Unified Management and Threat Prevention



Introducing Harmony SaaS

Continually Reduce your Attack Surface

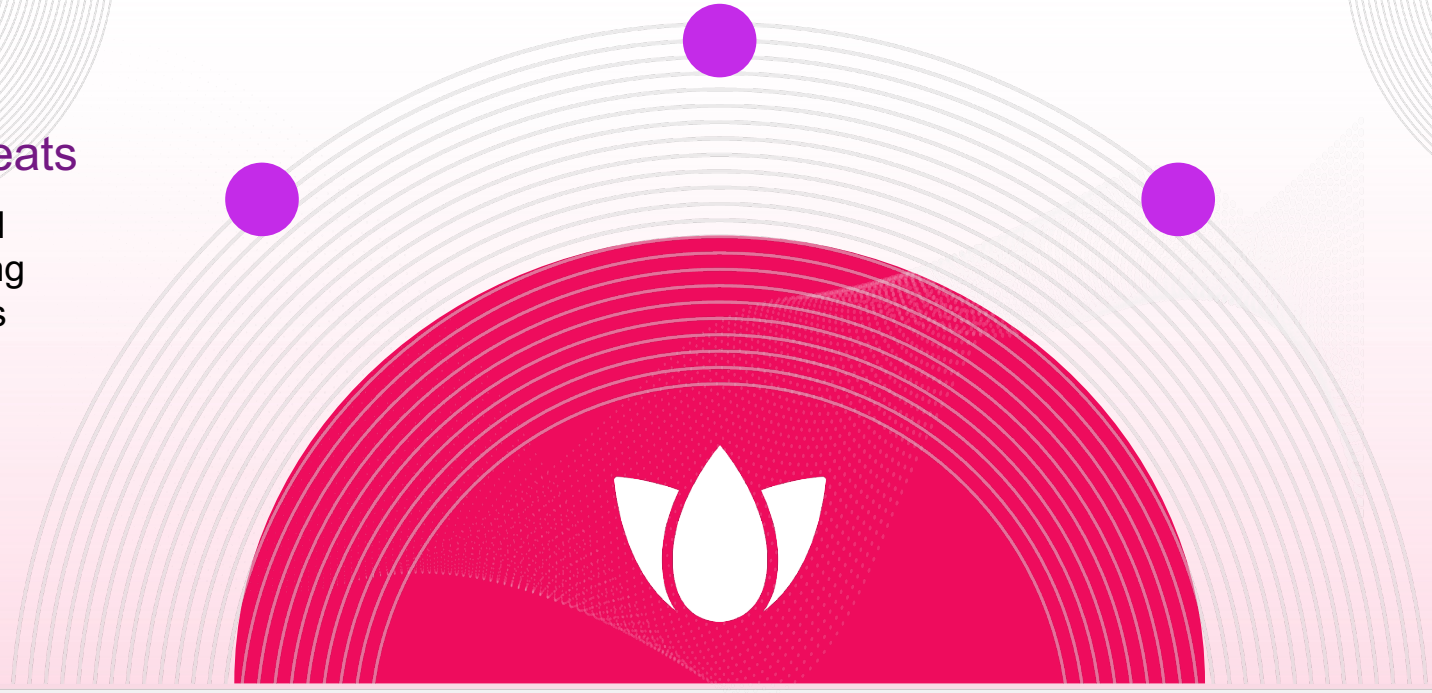
Discover your SaaS ecosystem and remediate security gaps

Automatically Prevent SaaS Threats

The most advanced solution for preventing SaaS-based threats

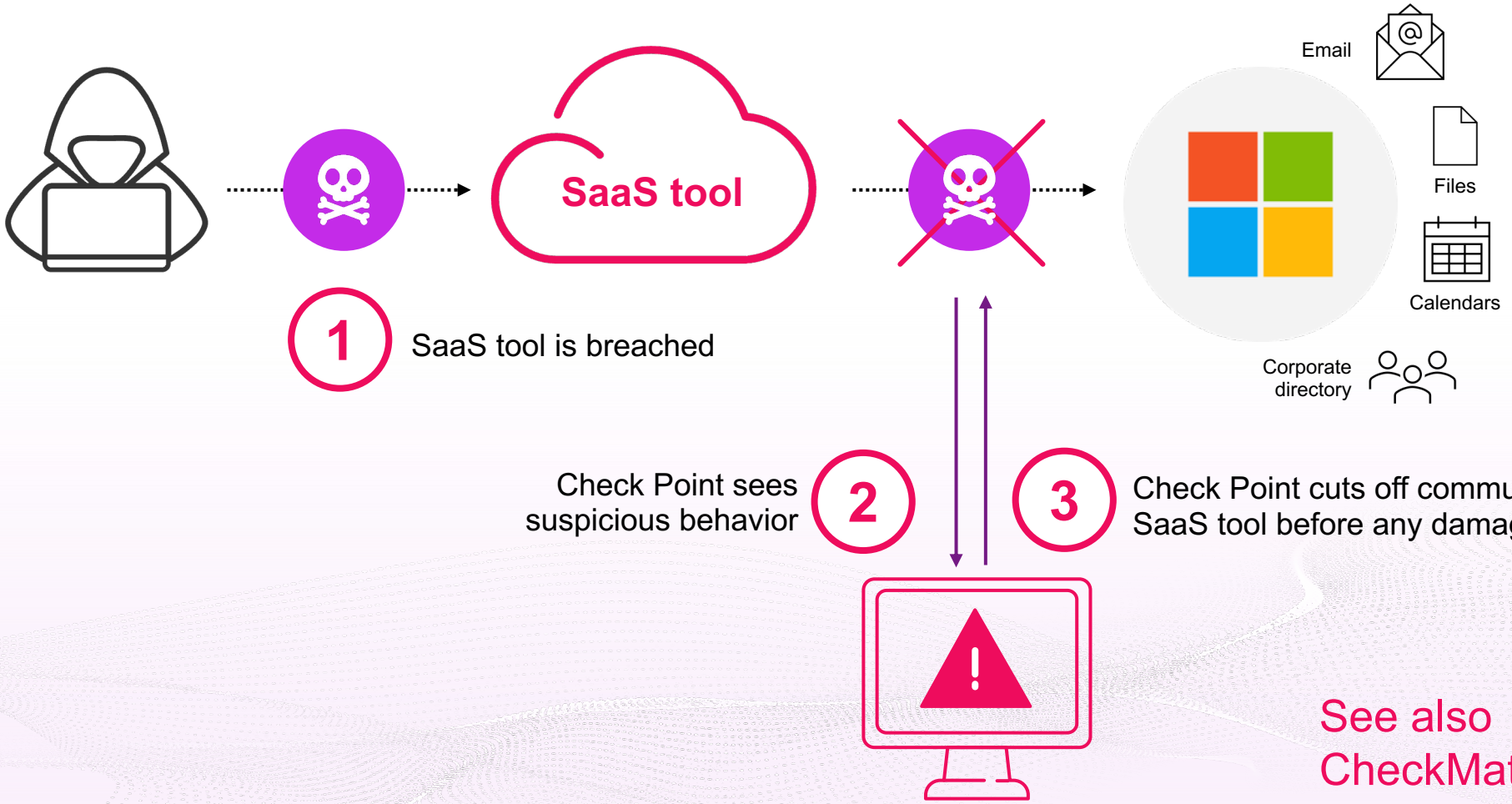
Best time-to-value

Install with a few clicks and get started in minutes



Automated SaaS Threat Prevention

Leverages ML to Identify Anomalous Behavior



See also CheckMates TechTalk

Check Point Harmony Email and Collaboration Security

- First API-based Email Security solution (2016)
- 23,000 paying customers
- Fastest Growing Email Security vendor
- Ranked as a Leader by all major analysts
- Top ranked by review sites: Gartner Peer Insights, G2, Info-Tech, and more

FORRESTER®

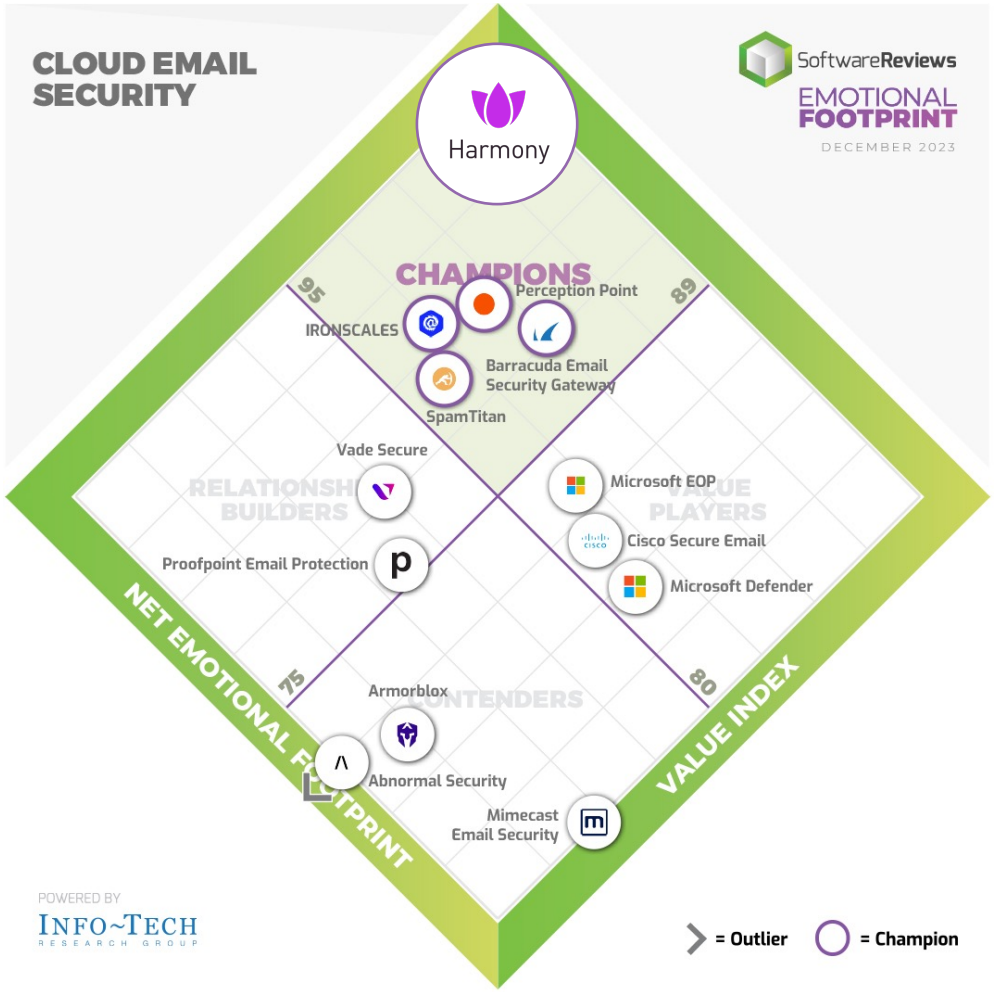
Leader WINTER 2024

OMDIA

GIGAOM

INFO~TECH RESEARCH GROUP

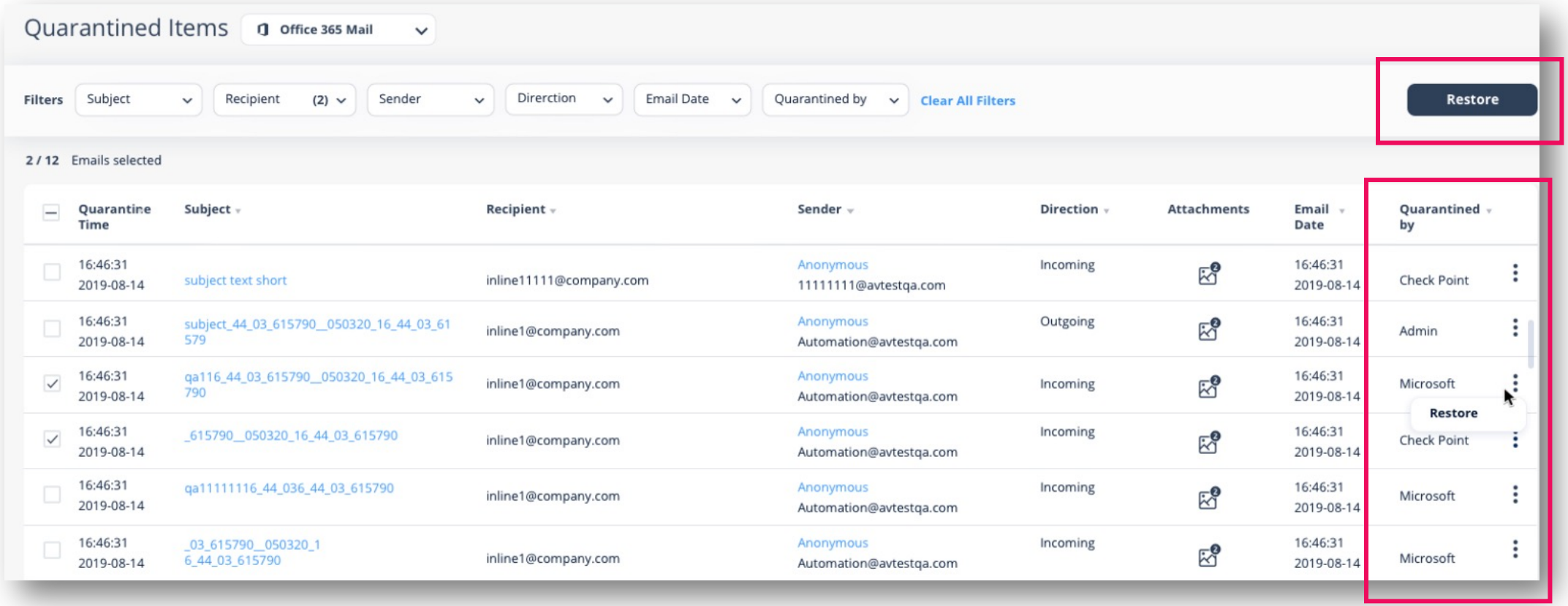
Gartner Peer Insights™



Unified Admin Quarantine View

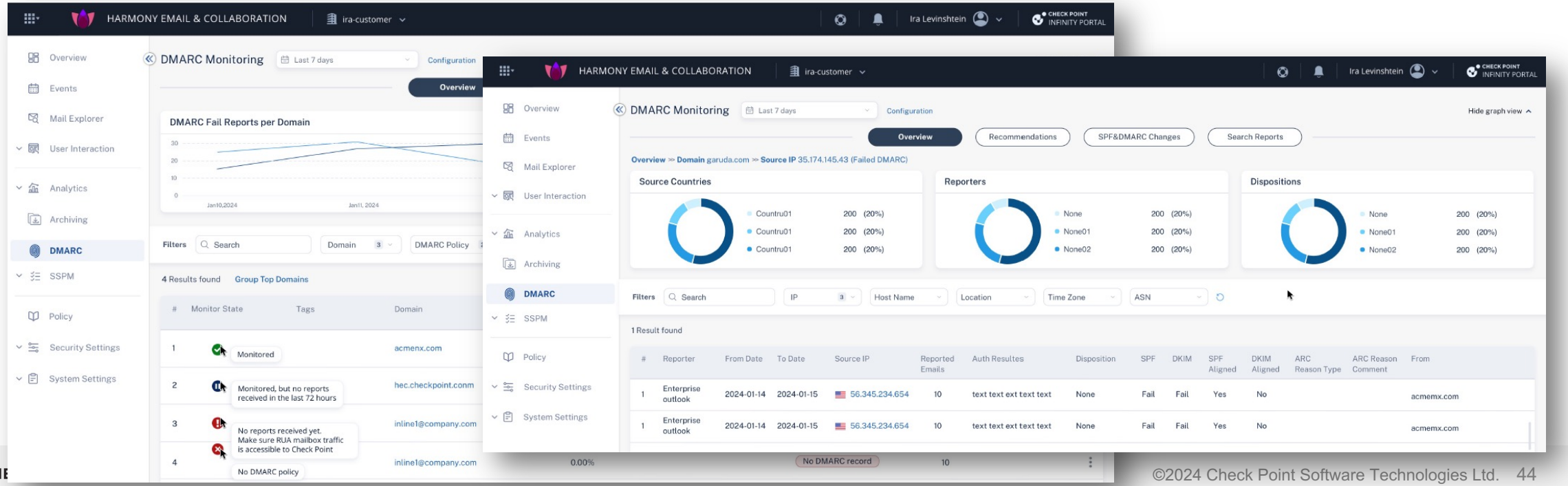
Patent pending

Viewing ***and restoring*** emails quarantine either by Microsoft or Check Point



DMARC Management

- Ensure safe transition to a restrictive DMARC policy
- Visibility to all the services sending emails on your behalf
- Search engine into all DMARC failures of emails sent on your behalf
- Actionable DMARC record change recommendations



What’s New in Infinity

THREATCLOUD AI: THE BRAIN
BEHIND CHECK POINT SECURITY

99.8%
Security effectiveness
BEST RESULT IN THE INDUSTRY

AI technology
40+ AI and Machine Learning technologies that identify and block emerging threats that were never seen before

THREATCLOUD AI

Big data threat intelligence
Always acquires the most recent IoCs and protections of latest attacks seen in the wild

Telemetry

ACCURATE PREVENTION
(MALICIOUS/SAFE)

Telemetry

ThreatCloud APIs

Quantum
Secure the Network

CloudGuard
Secure the Cloud

Harmony
Secure the Workspace

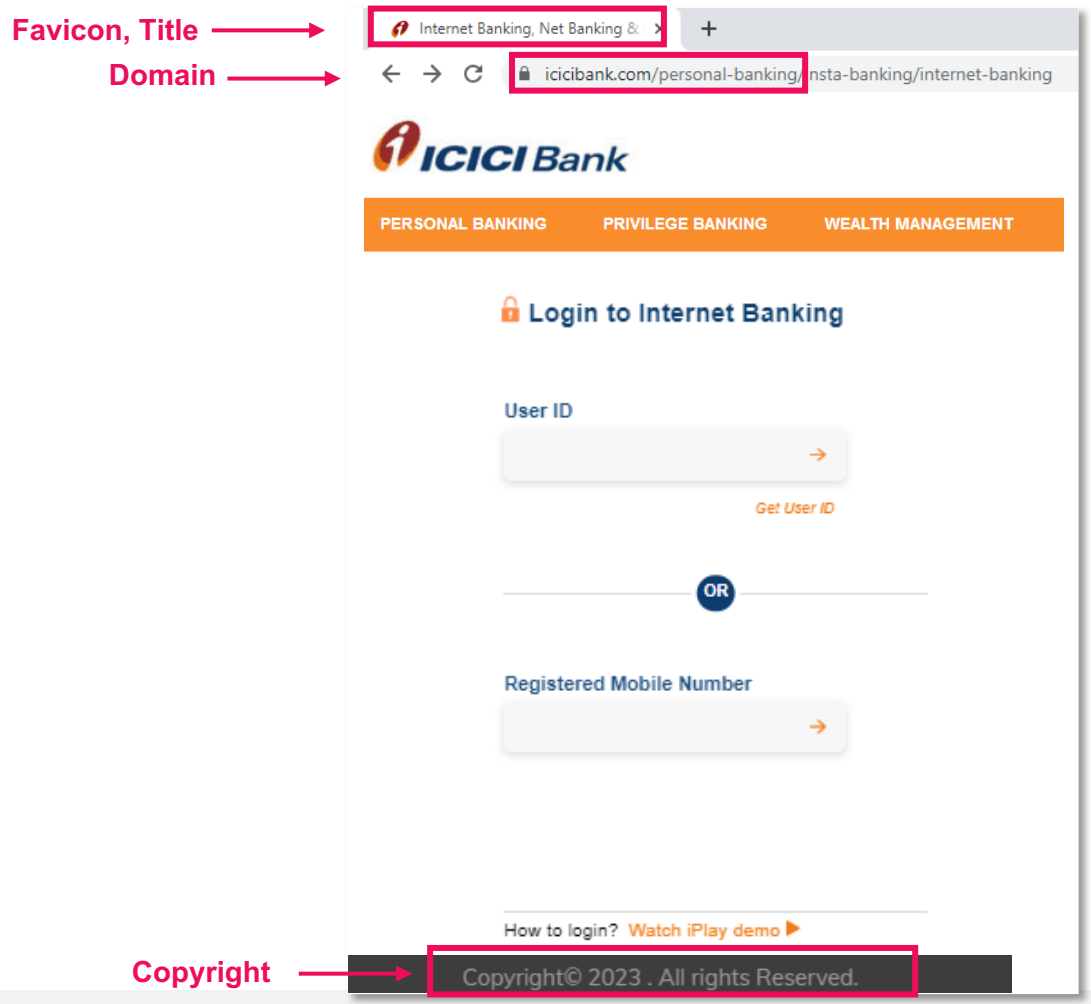
Infinity Core Services

Local Brand Spoofing

Targeted local brands, across languages and countries!

India

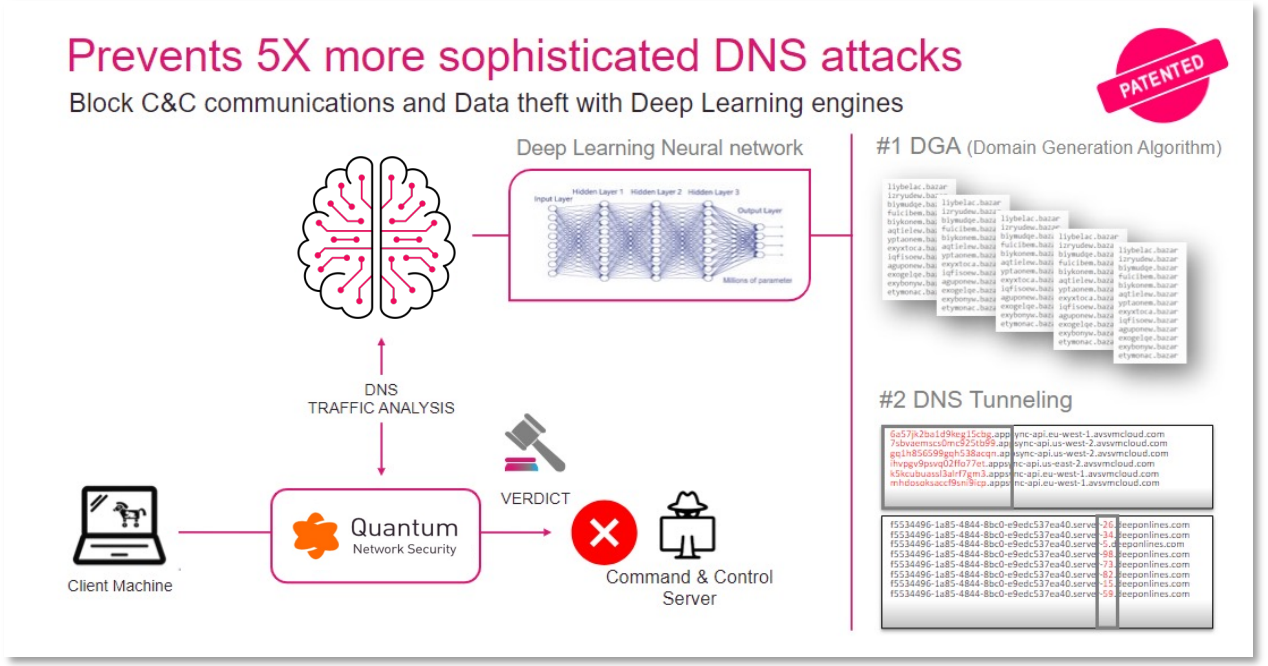
- **AI-enabled engine**
  Innovative AI-powered algorithms leveraging Natural Language Processing (NLP)
- **Prevention first**
  Identify and prevent brand impersonation phishing attacks in real time
- **All Check Point products**
  Serving Harmony, Quantum and CloudGuard product suits



DNS Security

ML/Deep Learning DNS engines:

- Brand impersonation
- DGA
- DNS Tunneling
- Ultra-slow tunneling
- DNS Hijacking ROADMAP



XDR/XPR addresses the cyber complexity with the 3C's of Best Security

Infinity XDR/XPR

COMPREHENSIVE
THREAT PREVENTION

Automatic attack prevention across the entire security estate

INTELLIGENT
CORRELATIONS

Powered by AI and Threat intelligence Correlating Check Point & 3rd Party Events

CONSOLIDATED
ANALYTICS

Improve posture through visibility to attack behavior, context and damage

Collaborative Security In Action

	I. Stop Web Vulnerability Exploits	**II. Prevent Lateral Movement**	**III. Proactive Zero-Trust Policy Assignment**
	Attacker identified on gateway in one geo	Endpoint file detected on Endpoint	New type of IoT device detected in network
Infinity Playblocks	Blocked attacker's IP across all international gateways & alerted admin	Quarantined infected device and blocked Trojan attack	Automatically assigned correct zero-trust policy & informed admin

2024 New Product Announcements

AI-Powered. Cloud-Delivered

Quantum

AI Copilot for Quantum
Quantum Force: 10 New Appliances, 2X Threat Prevention
Quantum OS R82, with 95 New Features
Spark New OS, with SD-WAN and IOT
Spark Gateways - 5Gbps Threat Prevention

CloudGuard

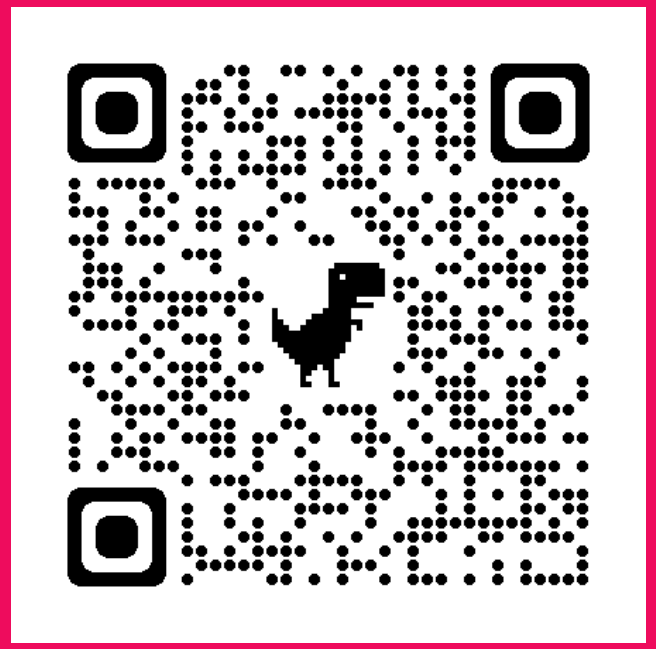
CloudGuard WAF as-a-Service
CloudGuard Network Azure vWAN Hub
New Effective Risk Management
CDR - Cloud Detection and Response

Harmony

Game-Changing SASE
SaaS Security
Endpoint Posture
Unified Phishing View
DMARC management

Infinity Core Services

ThreatCloud New AI Engines, 99.8% Prevention Rate of Zero+1 Day Malware
Infinity Playblocks
Infinity XDR/XPR 20 Connectors for 3rd Party Products
AI Copilot for XDR/XPR
New Infinity Data Centres in UAE and China
Infinity for MSSP with Pay-as-you-Go



See all the CPX 2024 content on CheckMates!

https://community.checkpoint.com/t5/General-Topics/CPX-2024/m-p/208174

CHECK POINT

Check Point CHECKMATES

Thank You!

YOU DESERVE THE BEST SECURITY