CHECK POINT™

YOU DESERVE THE BEST SECURITY

CPX 360 2022 RE-CAP

Dameon, Shay, and Val

Check Point CHECKMATES

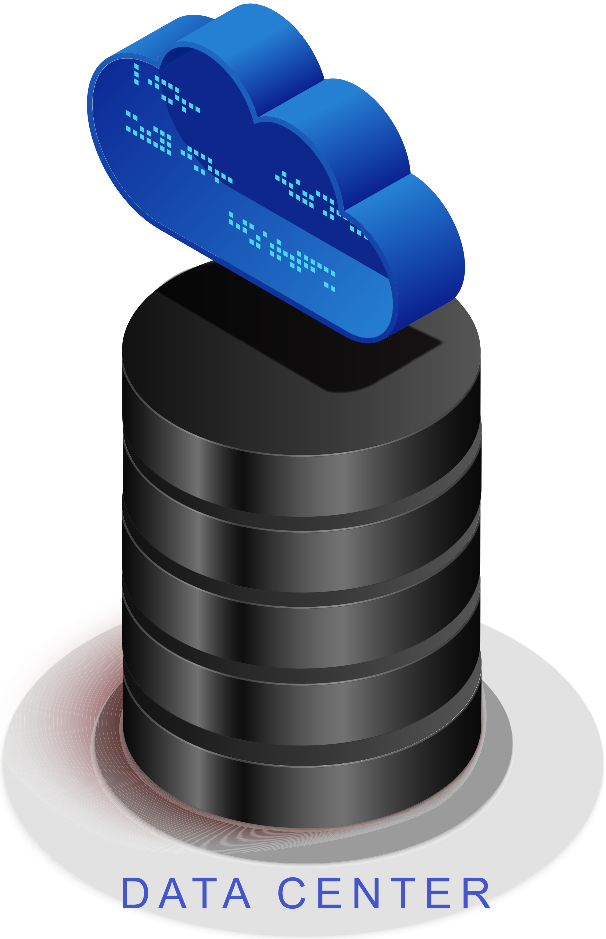
WHAT IS

QUANTUM LIGHTSPEED

Paradigm Shift in Data Center Security

High Performance for Securing East West Traffic

- Deliver better security throughput price performance
- Scale security for 2x network growth every 3 years
- Achieve Ultra Low Latency



Redefining Firewall Security at Network Speed

- Hyper-fast firewall security at line-rate speed
  - 250 to 800 Gbps Hyper-Fast throughput
  - Ultra low latency at 3μs (10X faster)
  - Scalability up to 3Tbps with Maestro

- Leverage Nvidia ConnectX NIC
  - Most Secure and Advanced ASIC
  - Accelerate Packet Processing Technology

QUANTUM LIGHTSPEED

- QLS 250
- QLS 450
- QLS 650
- QLS 800
- MLS 200
- MLS 400

Hyper-Fast, Ultra-low Latency, Scalable

Quantum Lightspeed Family with Six models

Best security to fit any line rate firewall use case

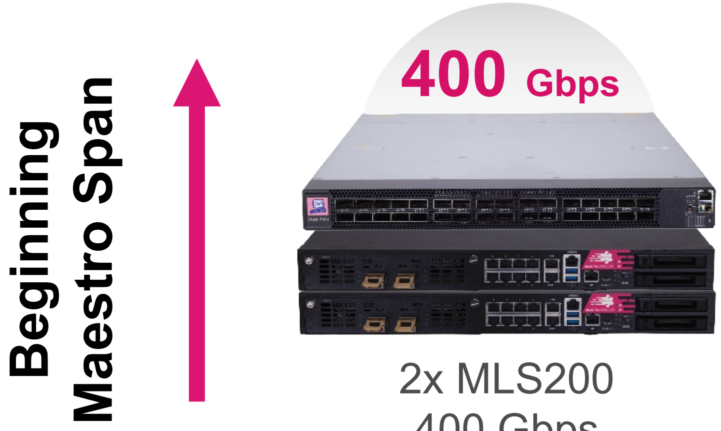
Quantum Lightspeed Model	QLS250	QLS450	QLS650	QLS800
Firewall Throughput	250 Gbps	450 Gbps	650 Gbps	800 Gbps

Maestro Lightspeed Model	MLS200	MLS400
Firewall Throughput	200 Gbps	400 Gbps

250-800 Gbps** faster speeds. **3µs** latency. Scalability of up to **3TBps

Quantum Lightspeed+ Maestro Hyperscale Orchestrator

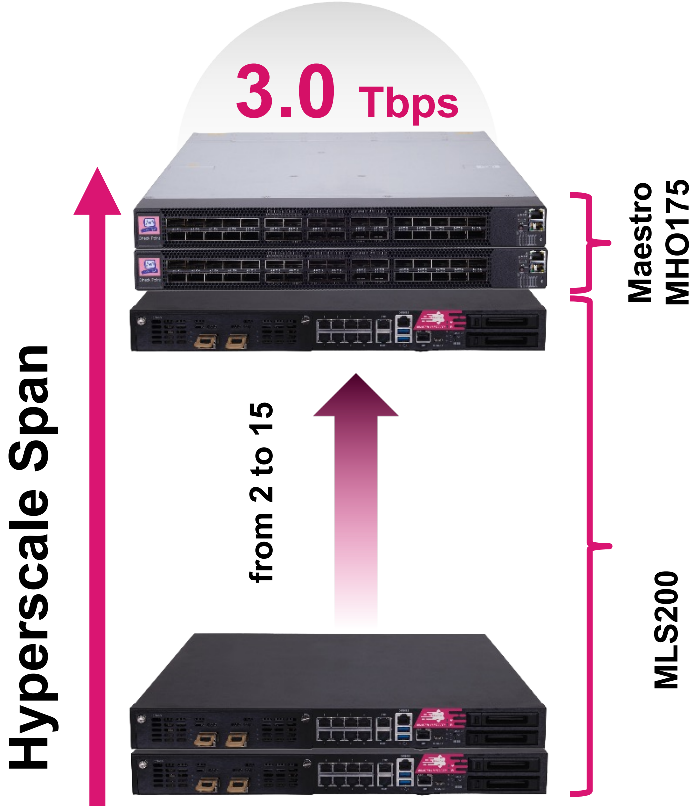
Scale throughput 7.5x to 3 Tbps



Beginning Maestro Span

400 Gbps

2x MLS200
400 Gbps



3.0 Tbps

Hyperscale Span

from 2 to 15

Maestro MHO175

MLS200

2x MLS200
400 Gbps

Maestro Base Configuration

Scale from 400 Gbps to 3 Tbps with Maestro*

* Or achieve the same 3 Tbps with 8x MLS400 + Maestro

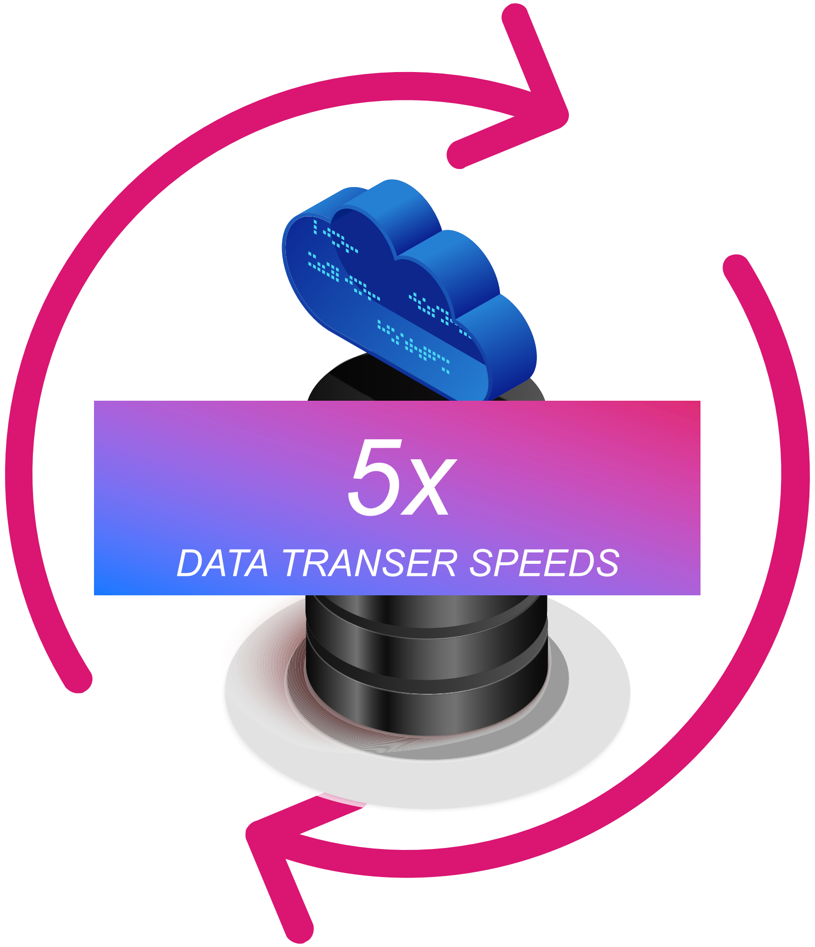
Moving 100 TB of Data Center Backup Across Locations

Quantum
Security Gateway

1.5
hours

145 Gbps

28000



5x
DATA TRANSER SPEEDS

Quantum Lightspeed
Firewall moves backups 5x faster

* 1 x 28000 vs 1 x QLS800

QUANTUM LIGHTSPEED

17
minutes

800 Gbps

QLS 800

CHECK POINT

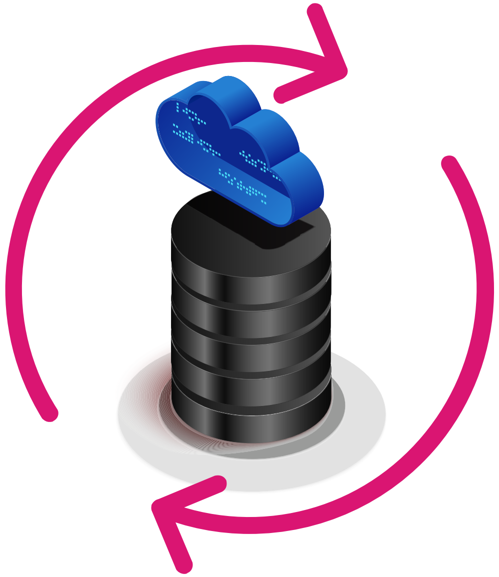
Fastest Access Control for Users across DC with Maestro

Quantum
Security Gateway

145 Gbps

2x 28000 1 + 1 Cluster

20 x FASTER ACCESS



Maestro MHO175

QUANTUM LIGHTSPEED

3.0 Tbps

8x MLS400 + Maestro- N + 1

Quantum Lightspeed Security Throughput Scales higher with Maestro

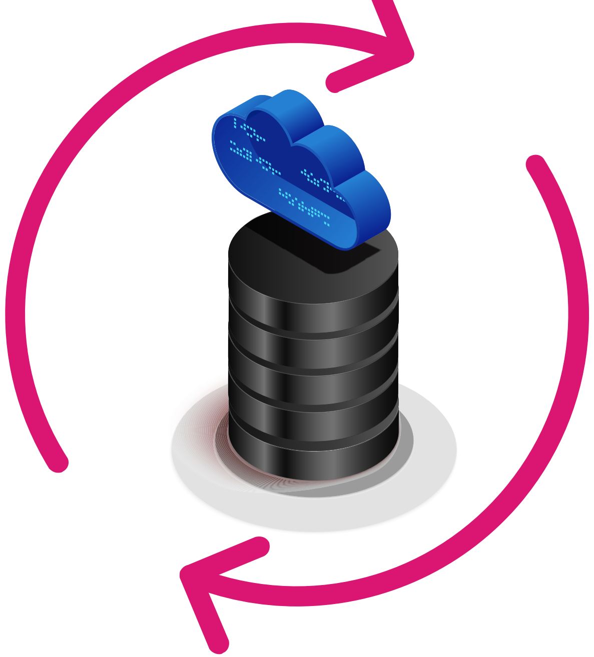
Secure Financial Transactions with Microsecond Latency

Quantum
Security Gateway

LEGACY
30
microseconds

28000

10x
QUICKER TRADES



QUANTUM LIGHTSPEED

3
microseconds

QLS 800

Use cases include High Frequency Trading

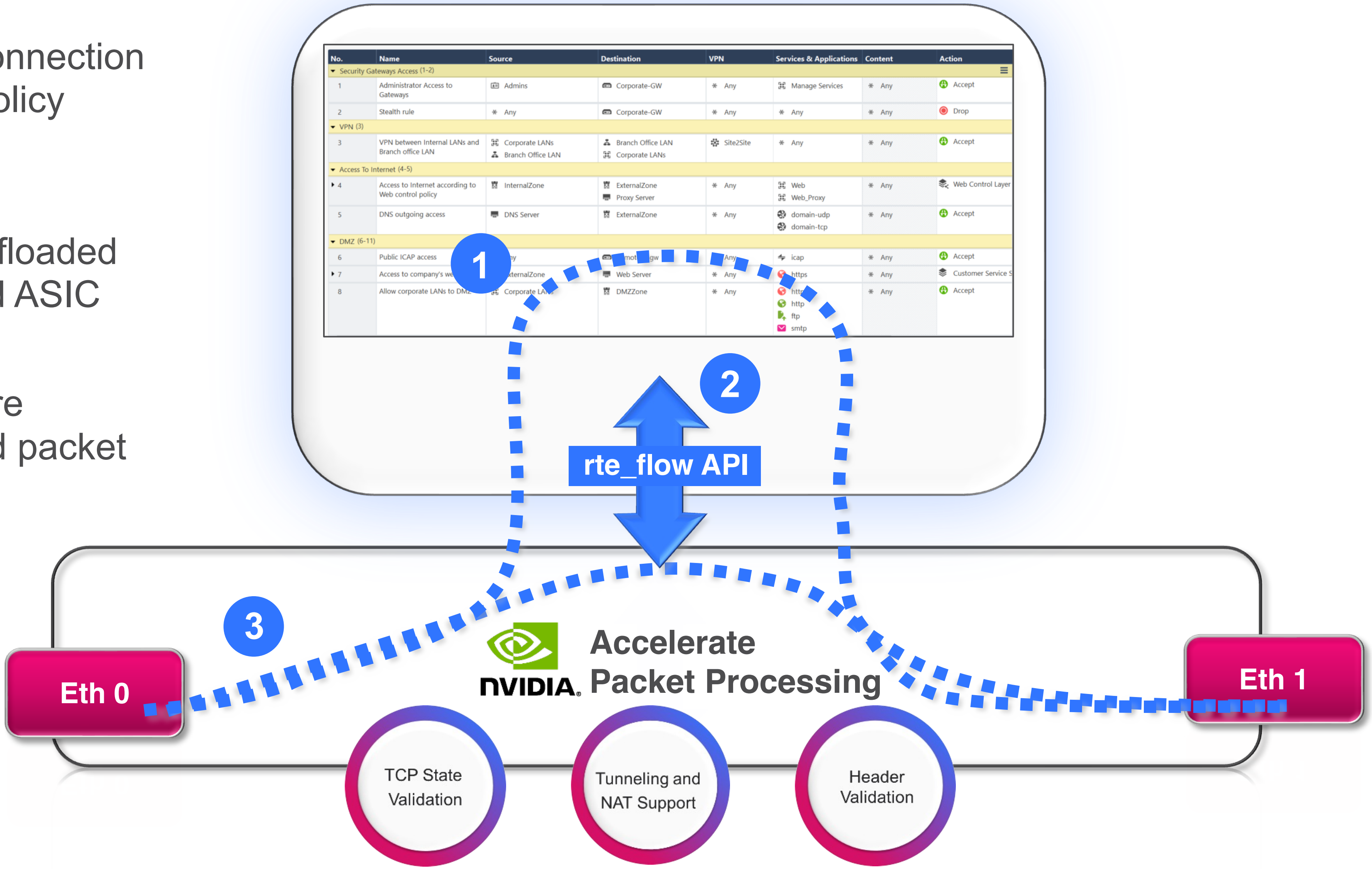
HOW DOES IT WORK?

How does it work?

1. First packet in every connection validated by security policy

2. Approved traffic flow offloaded to Quantum Lightspeed ASIC

3. Subsequent packets are secured by accelerated packet processing ASIC



No.	Name	Source	Destination	VPN	Services & Applications	Content	Action
Security Gateways Access (1-2)							
1	Administrator Access to Gateways	Admins	Corporate-GW	Any	Manage Services	Any	Accept
2	Stealth rule	Any	Corporate-GW	Any	Any	Any	Drop
VPN (3)							
3	VPN between Internal LANs and Branch office LAN	Corporate LANs Branch Office LAN	Branch Office LAN Corporate LANs	Site2Site	Any	Any	Accept
Access To Internet (4-5)							
4	Access to Internet according to Web control policy	InternalZone	ExternalZone Proxy Server	Any	Web Web_Proxy	Any	Web Control Layer
5	DNS outgoing access	DNS Server	ExternalZone	Any	domain-udp domain-tcp	Any	Accept
DMZ (6-11)							
6	Public ICAP access	Any	mot gw	Any	icap	Any	Accept
7	Access to company's we	ExternalZone	Web Server	Any	https	Any	Customer Service S
8	Allow corporate LANs to DMZ	Corporate LANs	DMZZone	Any	http http ftp smtp	Any	Accept

WHAT’S NEXT

Check Point CHECKMATES

Inline Encryption Hardware Engines

SSL Inspection

200Gbps rate for SSL encryption and Decryption for Threat Prevention

IPSEC VPN

Remote Access

Site-2-Site

More info sk176466

HYPERFLOW –

USING DYNAMIC LOAD BALANCING TO SECURE ELEPHANT FLOWS

Check Point
SOFTWARE TECHNOLOGIES LTD

HYPERFLOW

In Quantum Security Gateways

CPX 360

We all know that network throughput

HyperFlow - More Information on CheckMates

- Community Discussion
- EA Info & Contact Details

SNEAK PEEK:
CHECK POINT SD-WAN

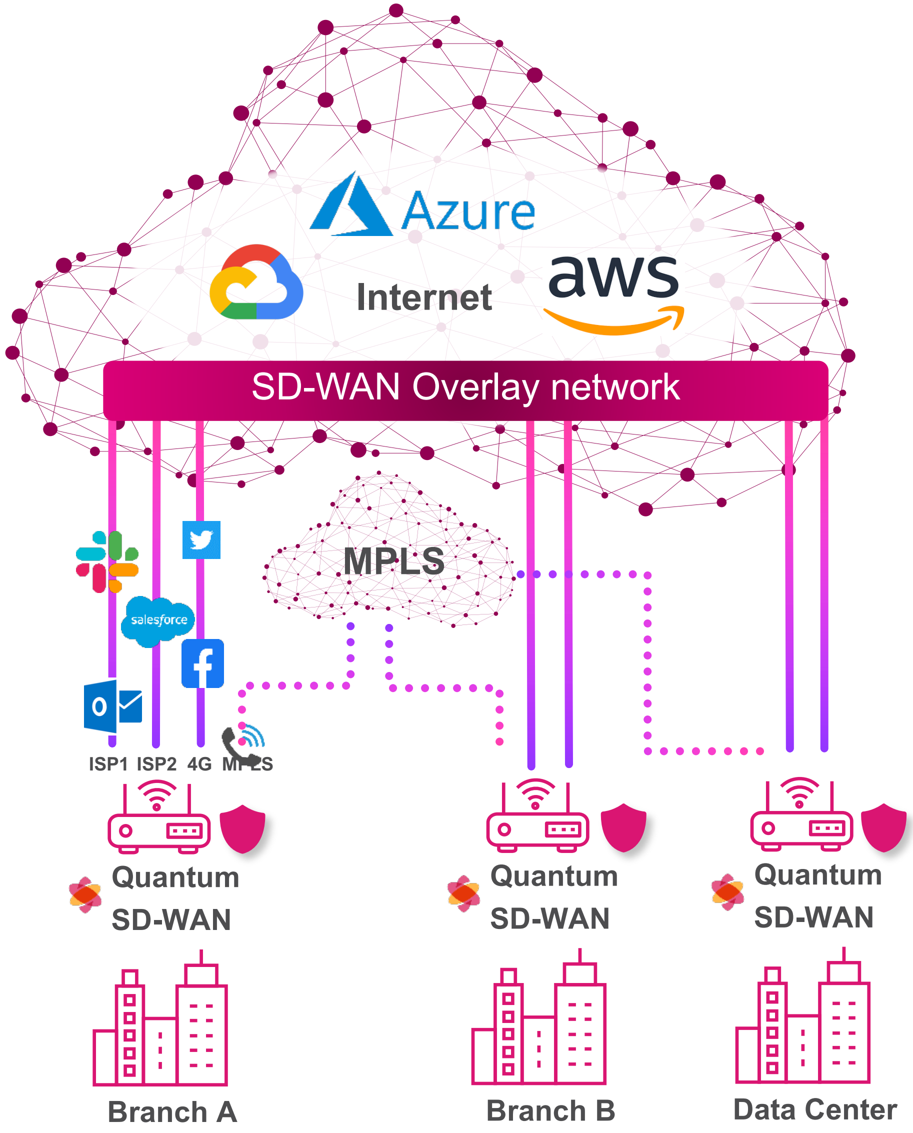
TYPICAL CUSTOMER REQUIREMENTS

Connect Multiple Branches
Connectivity between
branches and data center

Enhanced Connectivity
Use multiple links, utilize more
bandwidth for Internet and Data Center

Autonomous Steering
Choose best link for each application,
adapt according to burnouts and failures

Secure Connectivity
Secure both incoming and
outgoing branch connectivity



STRATEGIC OPTIONS THAT FITS YOUR BUSINESS

Harmony Connect

Quantum Edge

Protect 3rd party SD-WAN with Check Point Security

Maximum flexibility

Ideal for existing SD-WAN deployment

velocloud™ Now part of VMware

CITRIX®

CISCO

aryaka

aruba a Hewlett Packard Enterprise company

ORACLE® Talari

silver peak®

VERSA NETWORKS

Quantum SD-WAN

New 2022

Activate SDWAN on your Quantum Appliances

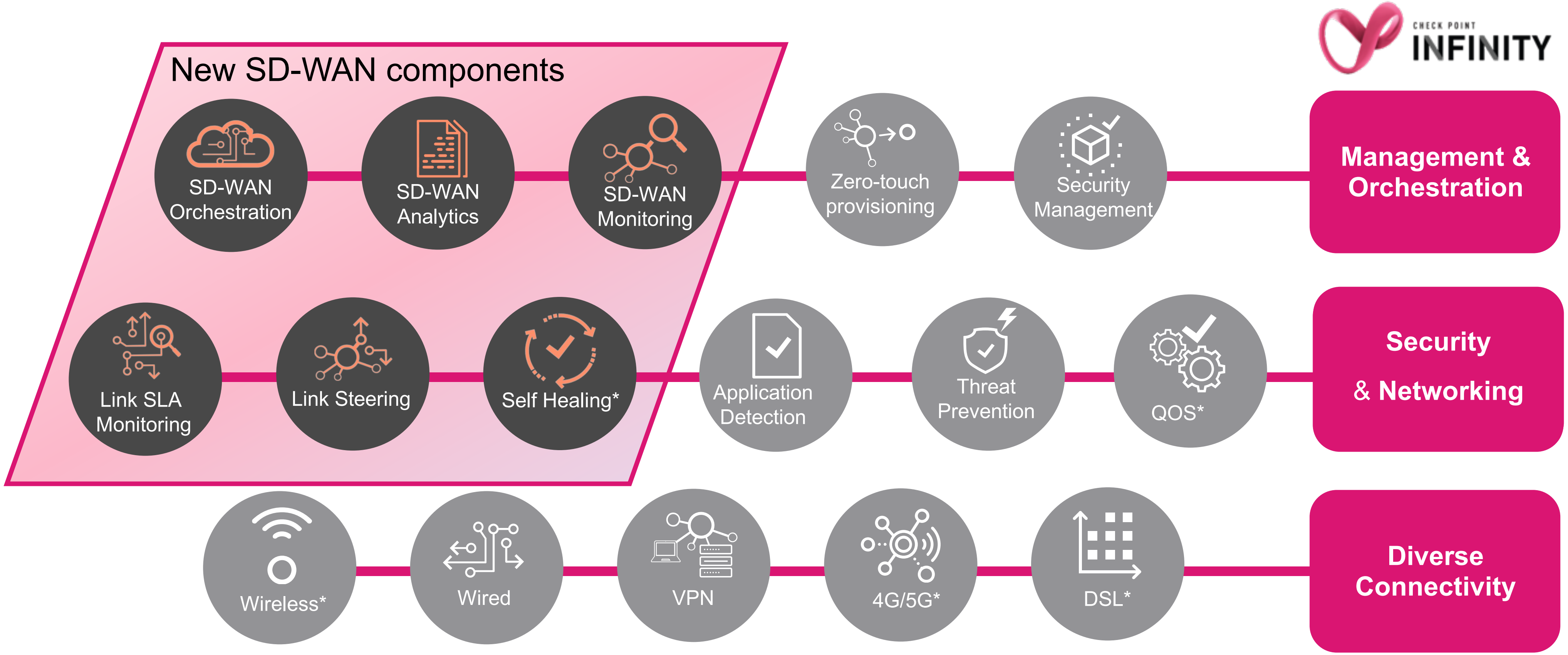
Reduce rollout time and cost

Enhancing Quantum GWs capabilities

CHECK POINT™

QUANTUM SD-WAN ARCHITECTURE

SD-WAN and Security Converged



Based on R81.10

*Roadmap

RICH SD-WAN CAPABILITIES

APPLICATION CENTRIC

Highest number of preconfigured apps

salesforce W

8,600+

IDENTITY AWARE

Identity based steering for best user experience

OPTIMIZE APP CONNECTIVITY

Multiple WAN links support for cost efficiency

Internet | MPLS | 4G/LTE/5G

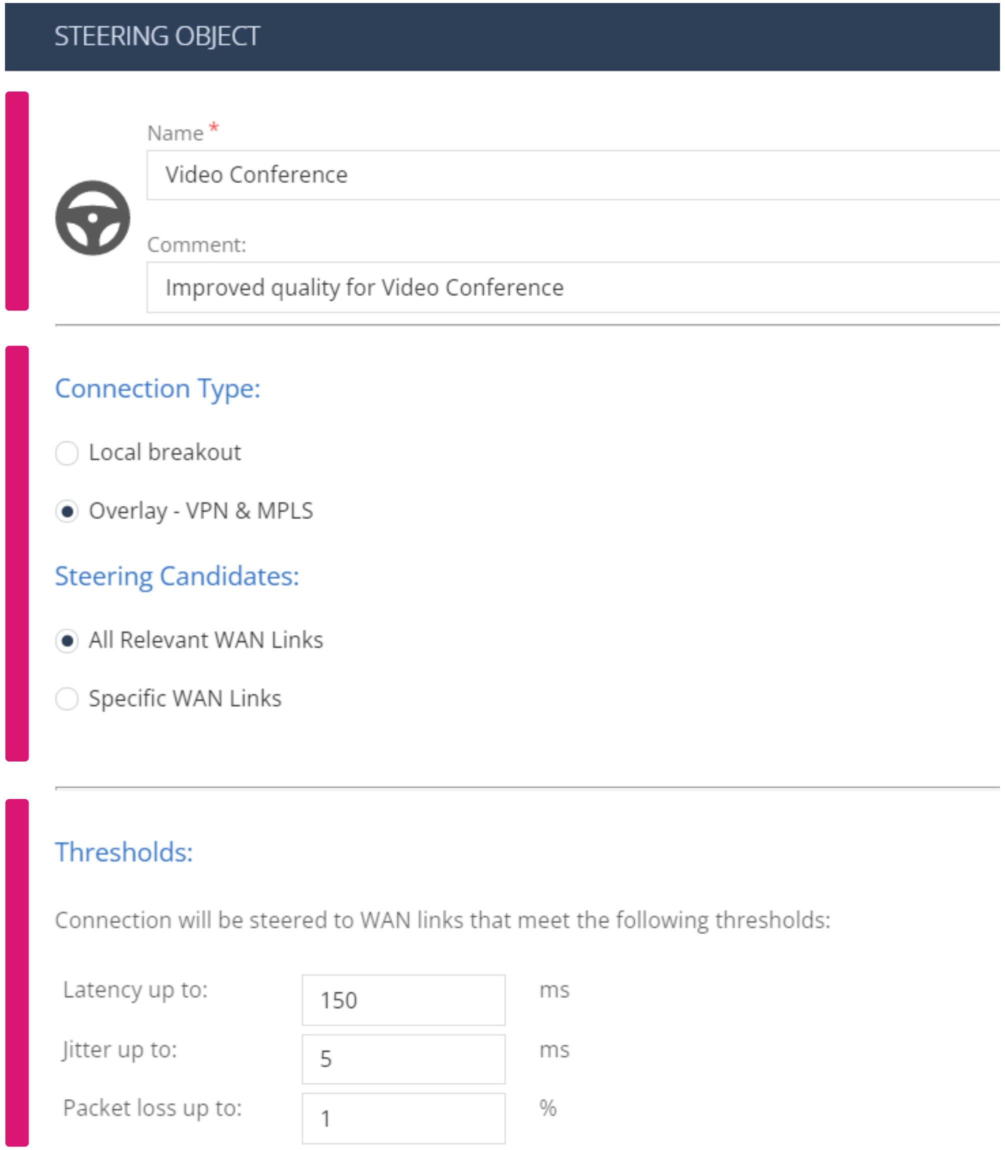
RICH SD-WAN CAPABILITIES

AUTONOMOUS TRAFFIC STEERING

Easy configuration with built-in traffic steering policy

Seamless sub-second failover between service providers (Overlay)

Best path selection based on Latency, Jitter, Packet-Loss



STEERING OBJECT

Name *

Video Conference

Comment:

Improved quality for Video Conference

Connection Type:

○ Local breakout

● Overlay - VPN & MPLS

Steering Candidates:

● All Relevant WAN Links

○ Specific WAN Links

Thresholds:

Connection will be steered to WAN links that meet the following thresholds:

Latency up to:	150	ms
Jitter up to:	5	ms
Packet loss up to:	1	%

UNCOMPROMISING SECURITY

Best Threat Prevention

Prevention First

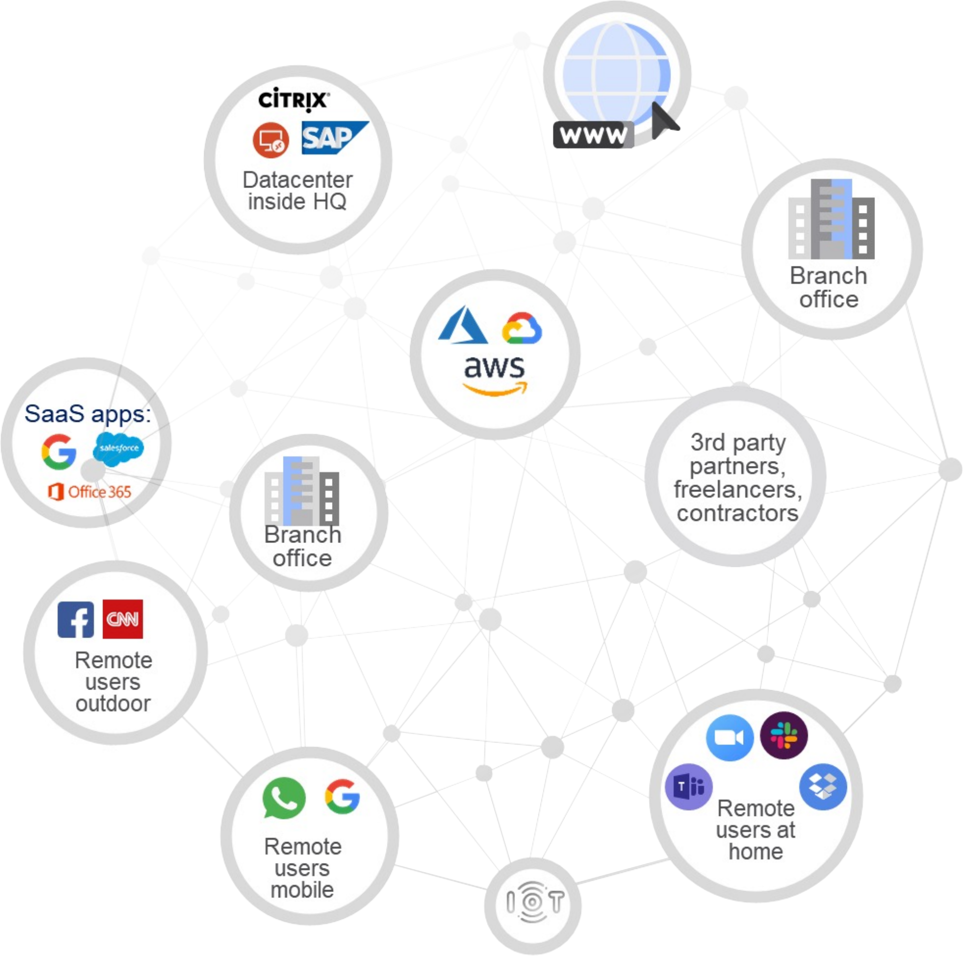
Block attacks faster than anyone else

Best Catch Rate

Of known & unknown threats; big data threat intel and AI engines

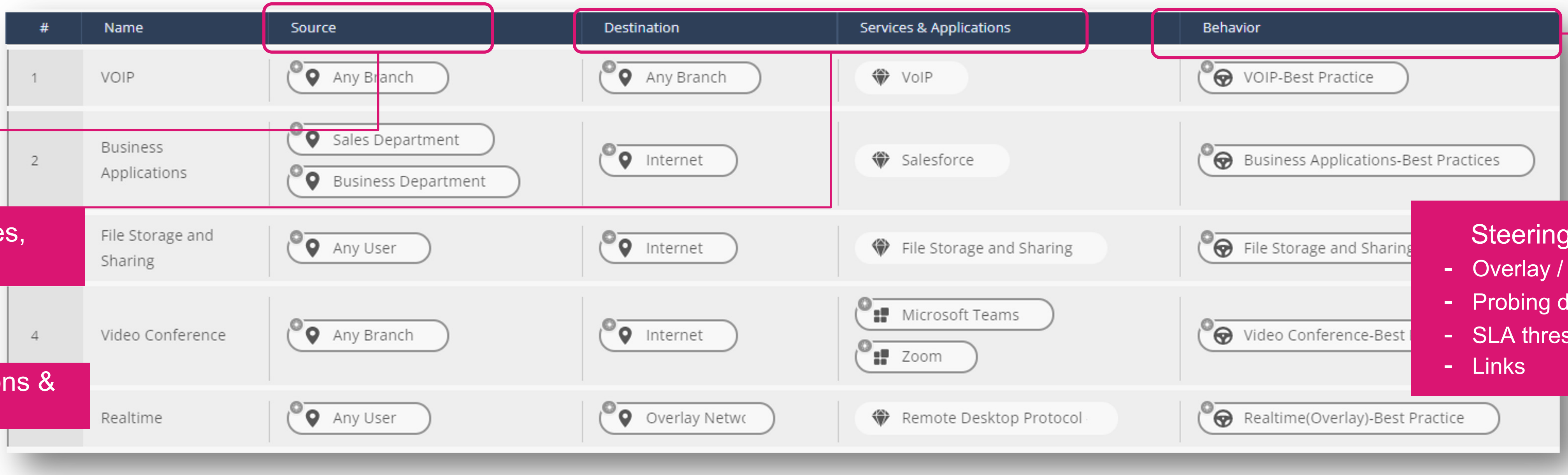
Accurate Prevention

Deep Learning supported signature matching, fewer alerts/tickets



UNMATCHED SIMPLICITY AND MANAGEMENT

Leverage Existing Deployment
Reduce Cost & Rollout Time from Months to Minutes



#	Name	Source	Destination	Services & Applications	Behavior
1	VOIP	Any Branch	Any Branch	VoIP	VOIP-Best Practice
2	Business Applications	Sales Department Business Department	Internet	Salesforce	Business Applications-Best Practices
	File Storage and Sharing	Any User	Internet	File Storage and Sharing	File Storage and Sharing
4	Video Conference	Any Branch	Internet	Microsoft Teams Zoom	Video Conference-Best
	Realtime	Any User	Overlay Netwc	Remote Desktop Protocol	Realtime(Overlay)-Best Practice

Users, devices, Network

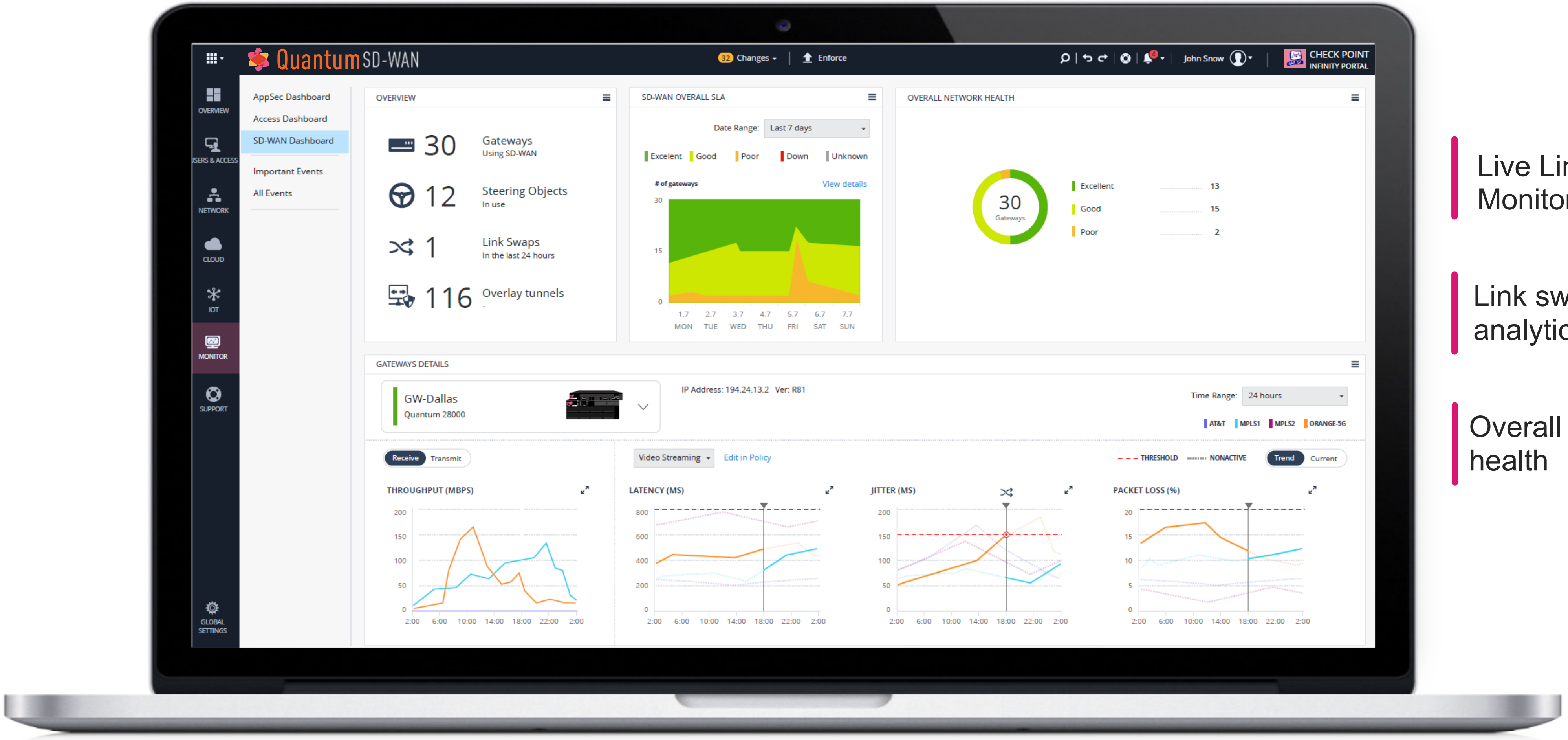
8K+ applications & services

Steering configuration:
- Overlay / Local breakout
- Probing destination
- SLA thresholds
- Links

Out of the box steering policy - enhanced connectivity **from day 1**

UNMATCHED SIMPLICITY AND MANAGEMENT

INTUITIVE CLOUD-BASED MONITORING DASHBOARD



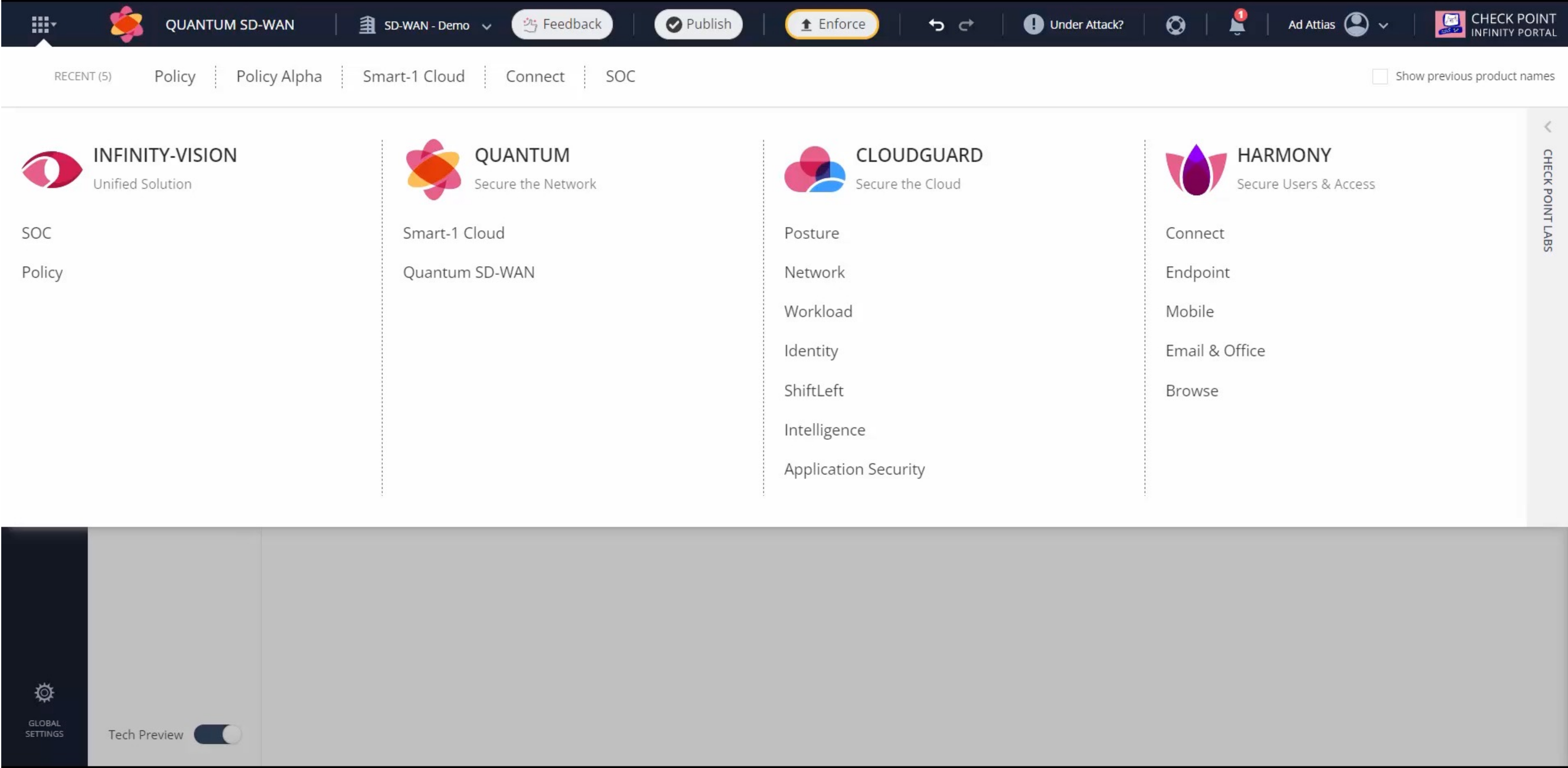
Live Link SLA Monitoring

Link swap analytics

Overall network health

Respond faster to connectivity burnouts and failures

CHECK POINT


QUANTUM SD-WAN
SD-WAN - Demo
Feedback
Publish
Enforce
Under Attack?
1
Ad Attias
CHECK POINT
INFINITY PORTAL
RECENT (5)
Policy
Policy Alpha
Smart-1 Cloud
Connect
SOC
Show previous product names
INFINITY-VISION
Unified Solution
SOC
Policy
QUANTUM
Secure the Network
Smart-1 Cloud
Quantum SD-WAN
CLOUDGUARD
Secure the Cloud
Posture
Network
Workload
Identity
ShiftLeft
Intelligence
Application Security
HARMONY
Secure Users & Access
Connect
Endpoint
Mobile
Email & Office
Browse
CHECK POINT LABS
GLOBAL SETTINGS
Tech Preview

QUANTUM SD-WAN RELEASE + ROADMAP

GA Mid '22 R81.10

Multiple WAN link support

Application & Identity based routing

Multi Path Orchestration

Hub and Spoke Overlay (+MEP)

Autonomous traffic steering

Bandwidth aggregation

High Availability

SD-WAN Monitoring, Logging & Analytics

Full Threat Prevention Capabilities

*Estimated

ROADMAP

Quantum Spark

Self-healing WAN

Full Mesh Overlay

Harmony Connect (SASE)

QOS

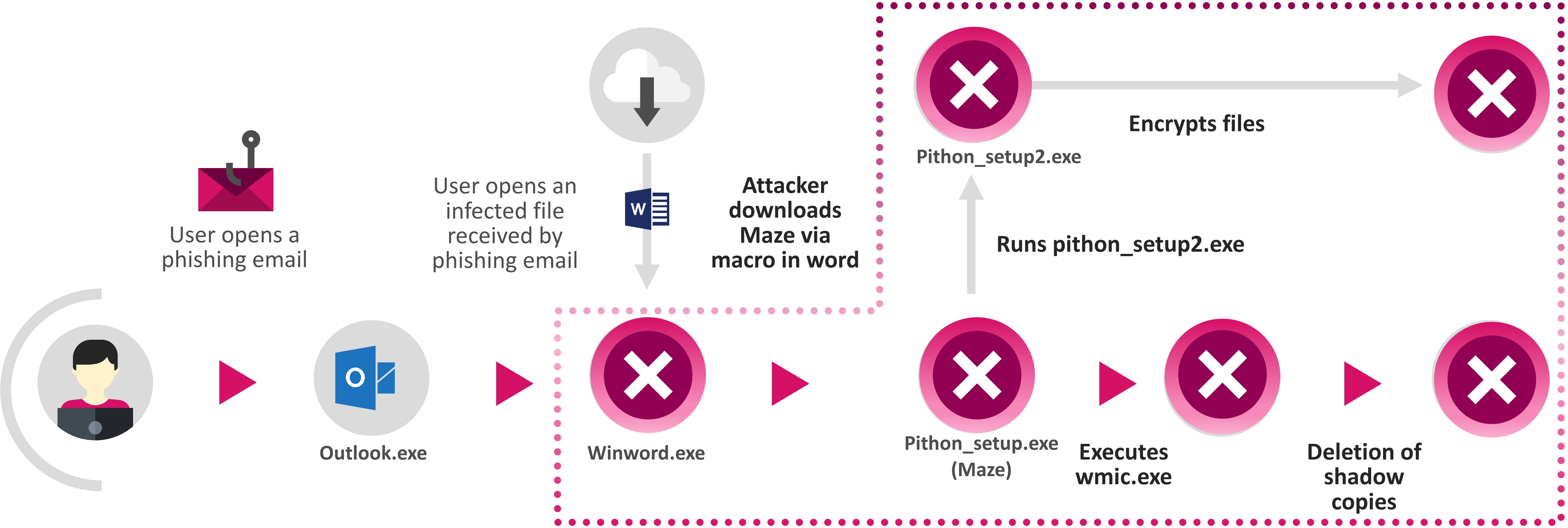
Additional platforms

Large scale management

Join EA Program

pages.checkpoint.com/get-notified-check-point-sd-wan-ea-program.html

AUTOMATED STERILIZATION
ENSURING BUSINESS CONTINUITY



User opens a phishing email
User opens an infected file received by phishing email
Attacker downloads Maze via macro in word
Pithon_setup2.exe
Encrypts files
Runs pithon_setup2.exe
Outlook.exe
Winword.exe
Pithon_setup.exe (Maze)
Executes wmic.exe
Deletion of shadow copies

Harmony Endpoint

CLEANS THE ENTIRE ATTACK

5
Granted patents

HARMONY – UNIFED SECURITY FOR USERS & ACCESS

Harmony Endpoint

Harmony Mobile

Harmony Browse

Harmony Connect

Harmony Email (Avanan) NEW!

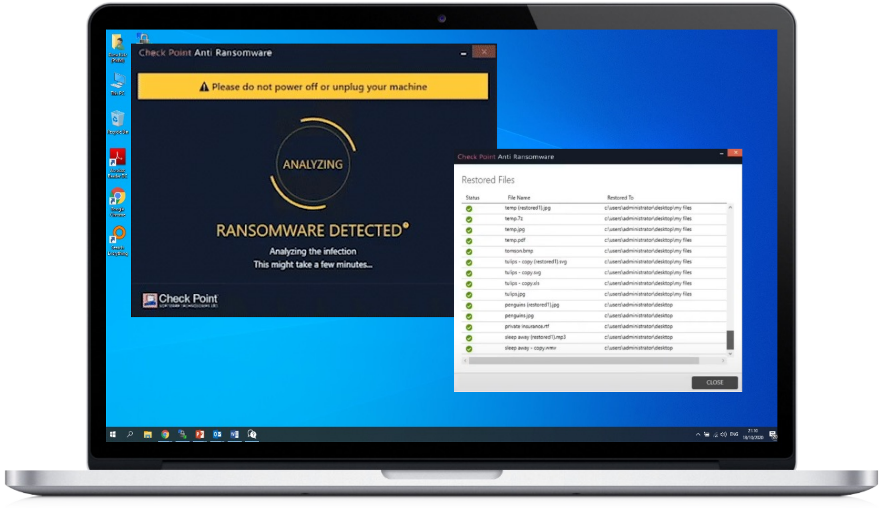
Prevent Ransomware

Prevent Phishing NEW!

Prevent Malware

Prevent Password Loss

FULL ATTACK ANALYSIS & REMEDIATION



Check Point Anti Ransomware

⚠ Please do not power off or unplug your machine

ANALYZING

RANSOMWARE DETECTED

Analyzing the infection
This might take a few minutes...

Check Point

Check Point Anti Ransomware

Restored Files

Status	File Name	Restored To
✓	temp (restored1).jpg	c:\users\administrator\desktop\my files
✓	temp.7z	c:\users\administrator\desktop\my files
✓	temp.jpg	c:\users\administrator\desktop\my files
✓	temp.pdf	c:\users\administrator\desktop\my files
✓	tomson.bmp	c:\users\administrator\desktop\my files
✓	tulips - copy (restored1).svg	c:\users\administrator\desktop\my files
✓	tulips - copy.svg	c:\users\administrator\desktop\my files
✓	tulips - copy.xls	c:\users\administrator\desktop\my files
✓	tulips.jpg	c:\users\administrator\desktop\my files
✓	penguins (restored1).jpg	c:\users\administrator\desktop
✓	penguins.jpg	c:\users\administrator\desktop
✓	private insurance.rtf	c:\users\administrator\desktop
✓	sleep away (restored1).mp3	c:\users\administrator\desktop
✓	sleep away - copy.wmv	c:\users\administrator\desktop

AUTOMATED RECOVERY
Safely restores ransomware-encrypted files

ON-DEVICE ATTACK DETECTION AND REMEDIATION
even in an offline mode

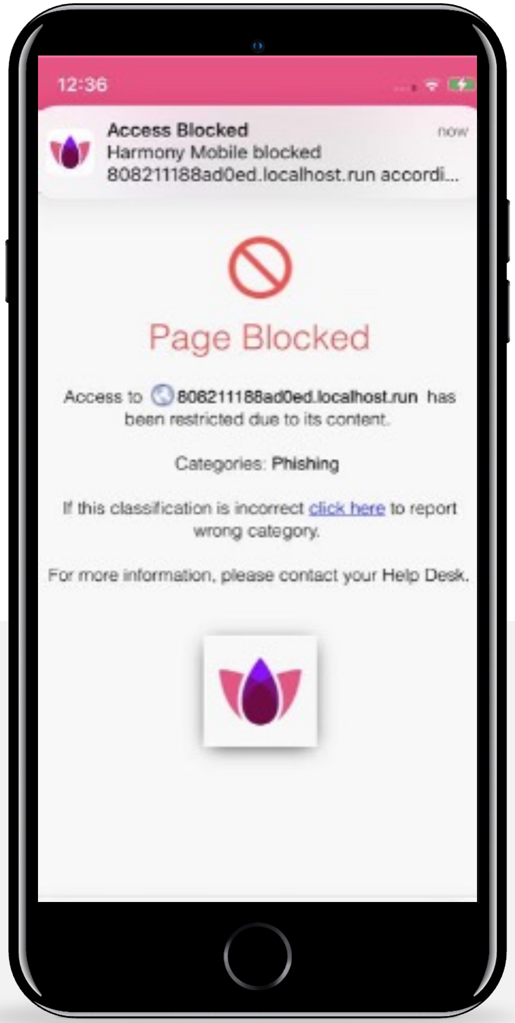
Automated

- Monitors and collects all the events
- Detects attacks
- Quarantines what’s malicious
- **Cleans the entire attack kill chain**
- **File restoration & rollback**
- **Forensics report**

Secured Internet Browsing & Phishing Prevention

User receives a message with a link

URL identified as malicious phishing and blocked



12:36

Access Blocked
Harmony Mobile blocked
808211188ad0ed.localhost.run accordi...

now

Page Blocked

Access to 808211188ad0ed.localhost.run has been restricted due to its content.

Categories: Phishing

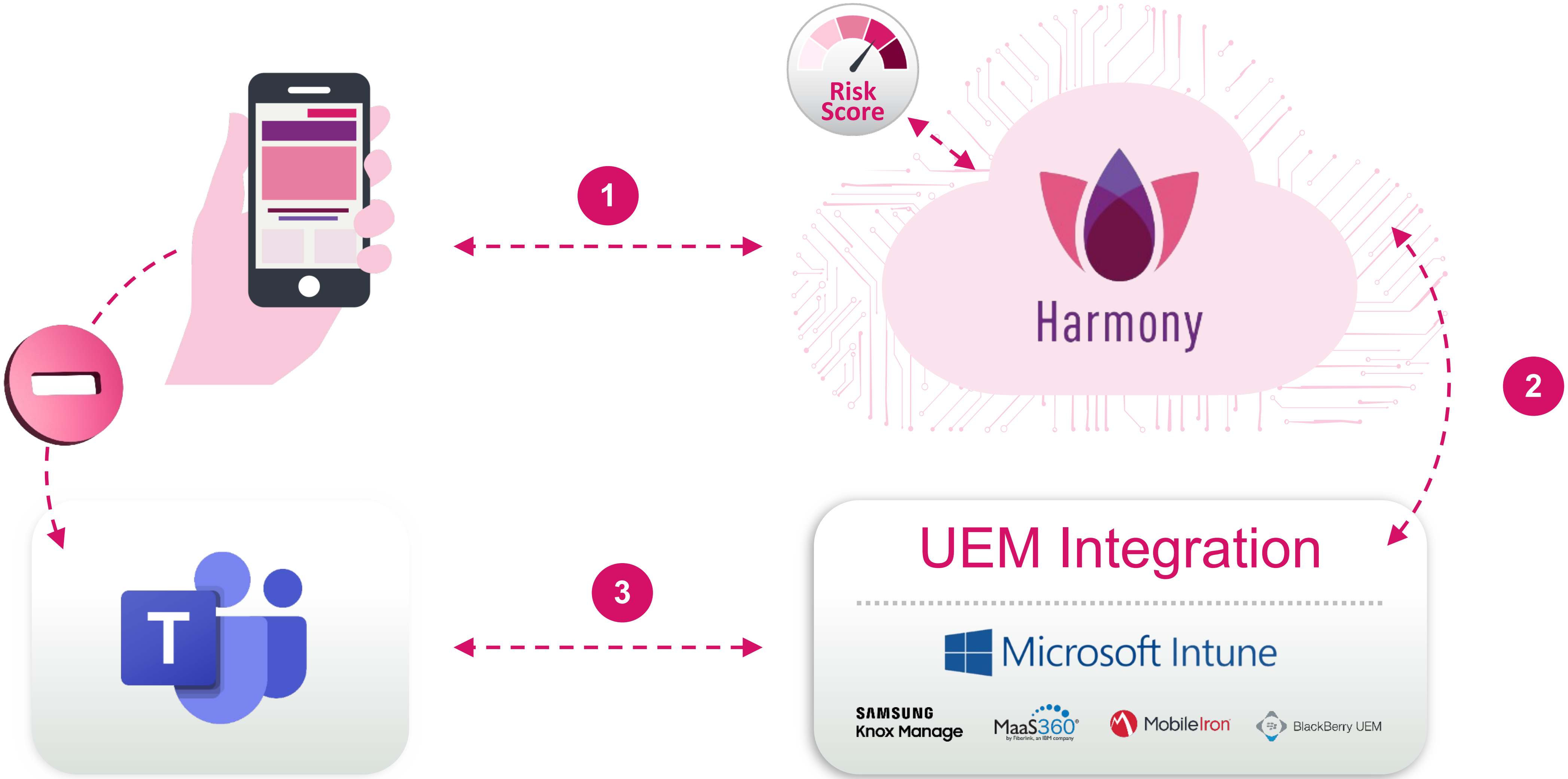
If this classification is incorrect click here to report wrong category.

For more information, please contact your Help Desk.

THREATCLOUD

- Anti-phishing engine instantly inspects the link
- Unknown sites analyzed in real-time with Zero-phishing

Risk-Based Conditional Access



RANSOMWARE PROTECTION WITH HARMONY ENDPOINT AND MOBILE

Harmony Connect Remote Access

The easiest way to secure corporate access

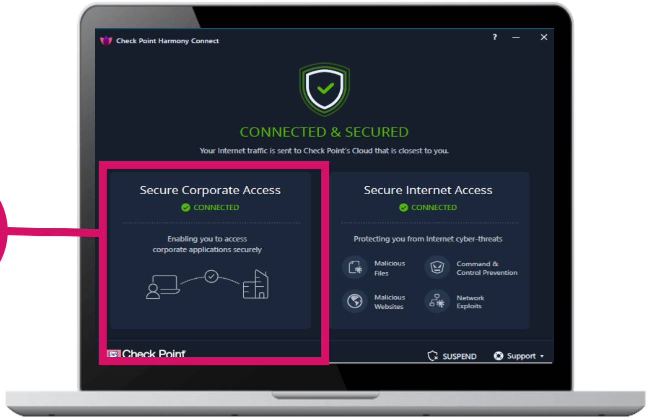
Remote desktop

SharePoint

SAP

Cloud Service

Company-managed devices



Check Point Harmony Connect

CONNECTED & SECURED

Your Internet traffic is sent to Check Point's Cloud that is closest to you.

Secure Corporate Access

CONNECTED

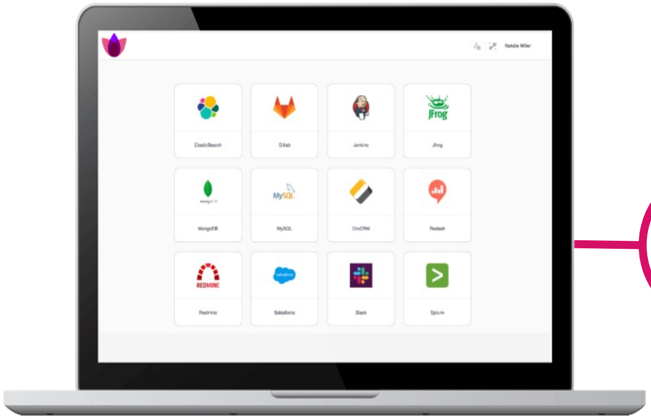
Enabling you to access corporate applications securely

Secure Internet Access

CONNECTED

Protecting you from Internet cyber-threats

Personal laptops & mobiles



Cloud Service

WEB

RDP

SSH

VPN-as-a-service

Client-based

Network-level access

Layer 3 VPN access

Device posture check

ZTNA-as-a-service

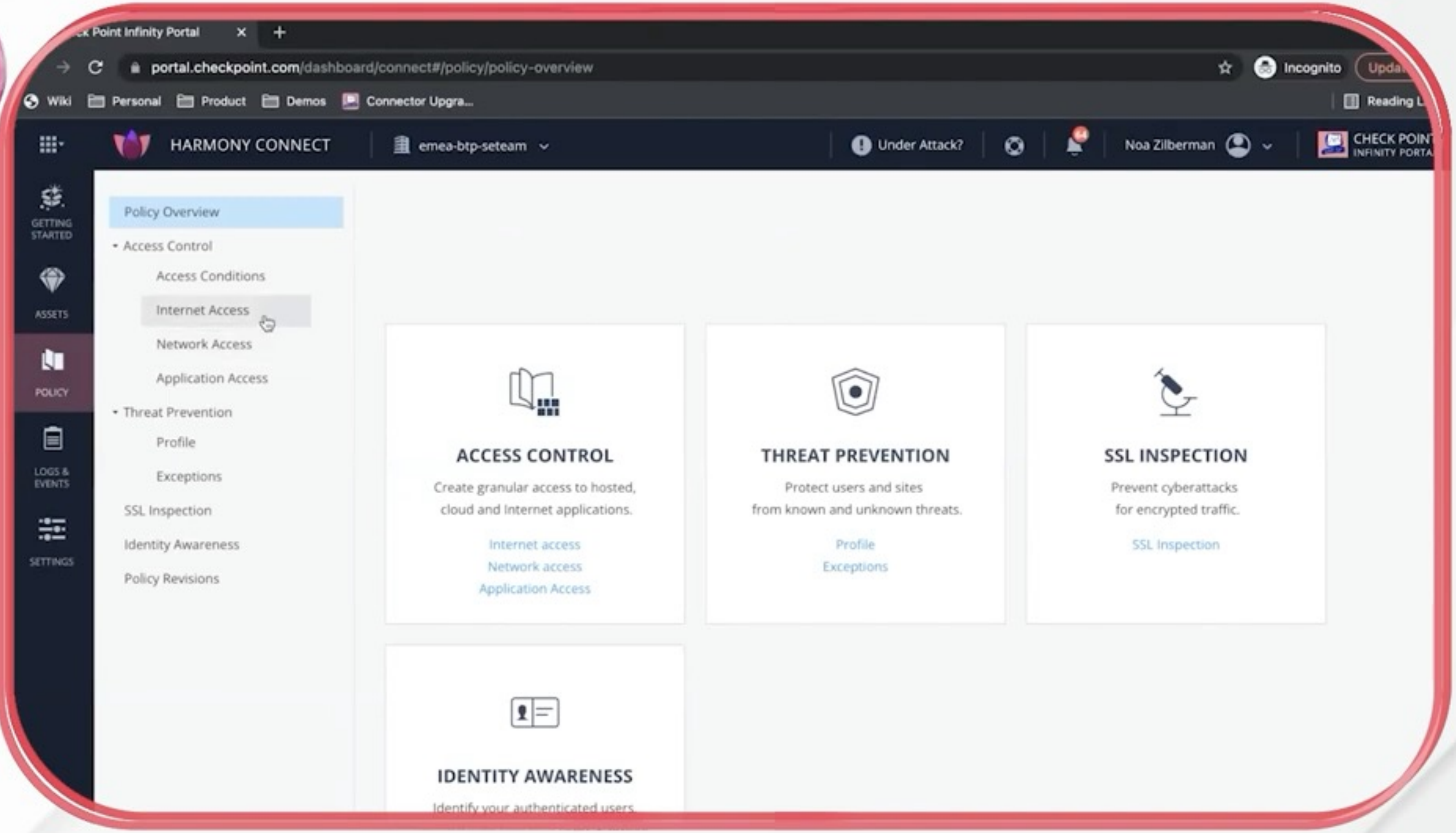
Clientless, no agent required

Application-level access

Friendly web-based UI

Single sign-on (SSO)

CPX 360



k Point Infinity Portal

portal.checkpoint.com/dashboard/connect#/policy/policy-overview

Incognito

Wiki Personal Product Demos Connector Upgra... Reading L

HARMONY CONNECT emea-btp-seteam Under Attack? Noa Zilberman CHECK POINT INFINITY PORTA

GETTING STARTED
ASSETS
POLICY
LOGS & EVENTS
SETTINGS

- Policy Overview
- Access Control
  - Access Conditions
  - Internet Access
  - Network Access
  - Application Access
- Threat Prevention
  - Profile
  - Exceptions
- SSL Inspection
- Identity Awareness
- Policy Revisions

ACCESS CONTROL

Create granular access to hosted, cloud and Internet applications.

Internet access
Network access
Application Access

THREAT PREVENTION

Protect users and sites from known and unknown threats.

Profile
Exceptions

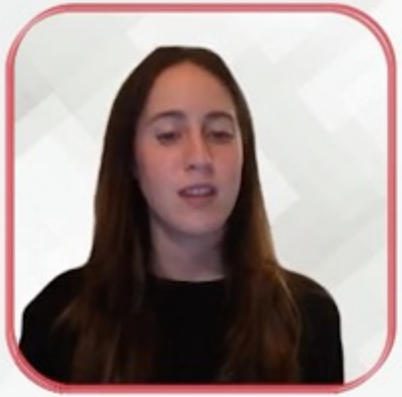
SSL INSPECTION

Prevent cyberattacks for encrypted traffic.

SSL Inspection

IDENTITY AWARENESS

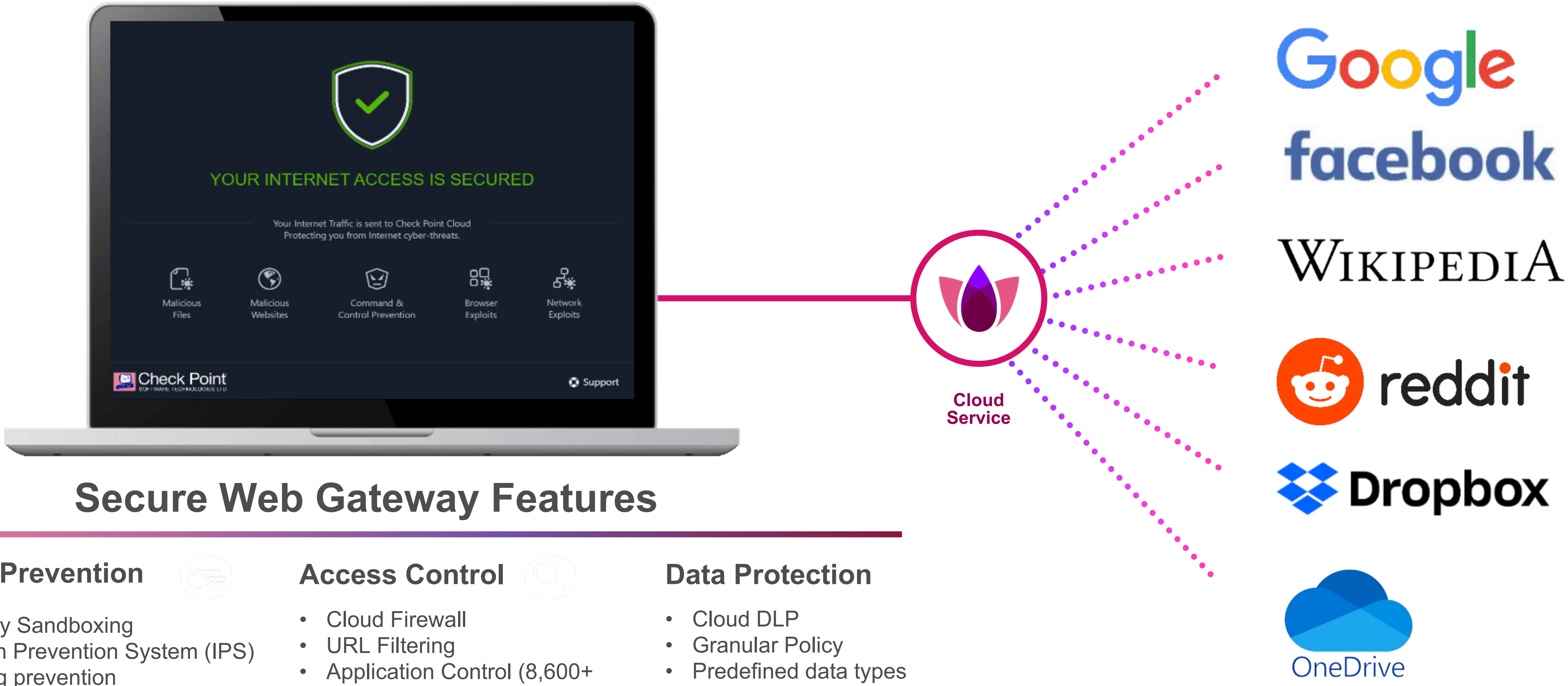
Identify your authenticated users



HARMONY CONNECT: ZTNA AND SASE

SECURE INTERNET ACCESS

HARMONY CONNECT INTERNET ACCESS



YOUR INTERNET ACCESS IS SECURED

Your Internet Traffic is sent to Check Point Cloud
Protecting you from Internet cyber-threats.

Secure Web Gateway Features

Threat Prevention

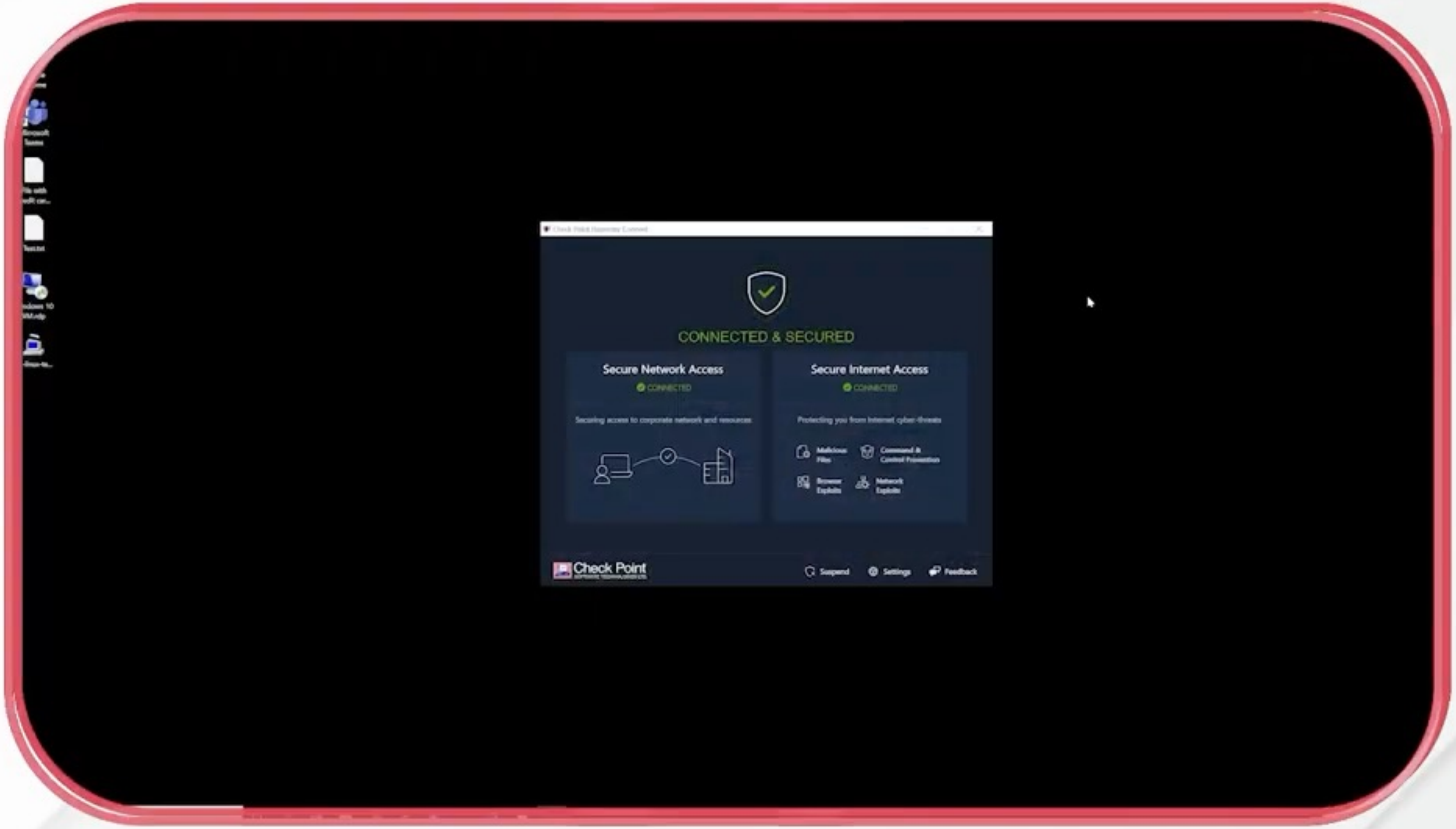
- Zero-day Sandboxing
- Intrusion Prevention System (IPS)
- Phishing prevention
- Malware and C2 bot prevention
- Full SSL Visibility

Access Control

- Cloud Firewall
- URL Filtering
- Application Control (8,600+ Apps)

Data Protection

- Cloud DLP
- Granular Policy
- Predefined data types



Check Point Harmony Connect

CONNECTED & SECURED

Secure Network Access

CONNECTED

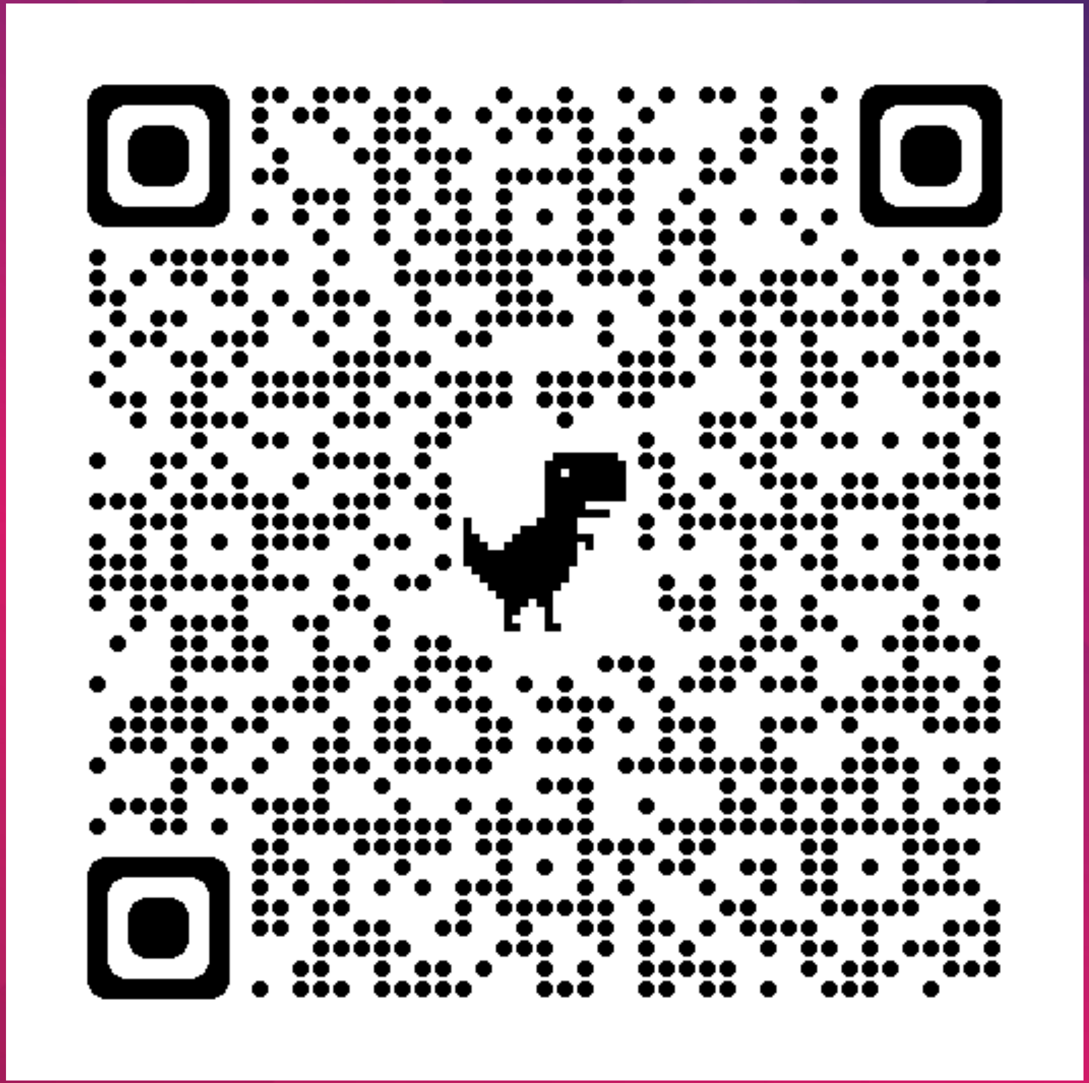
Securing access to corporate network and resources

Secure Internet Access

CONNECTED

Protecting you from Internet cyber-threats

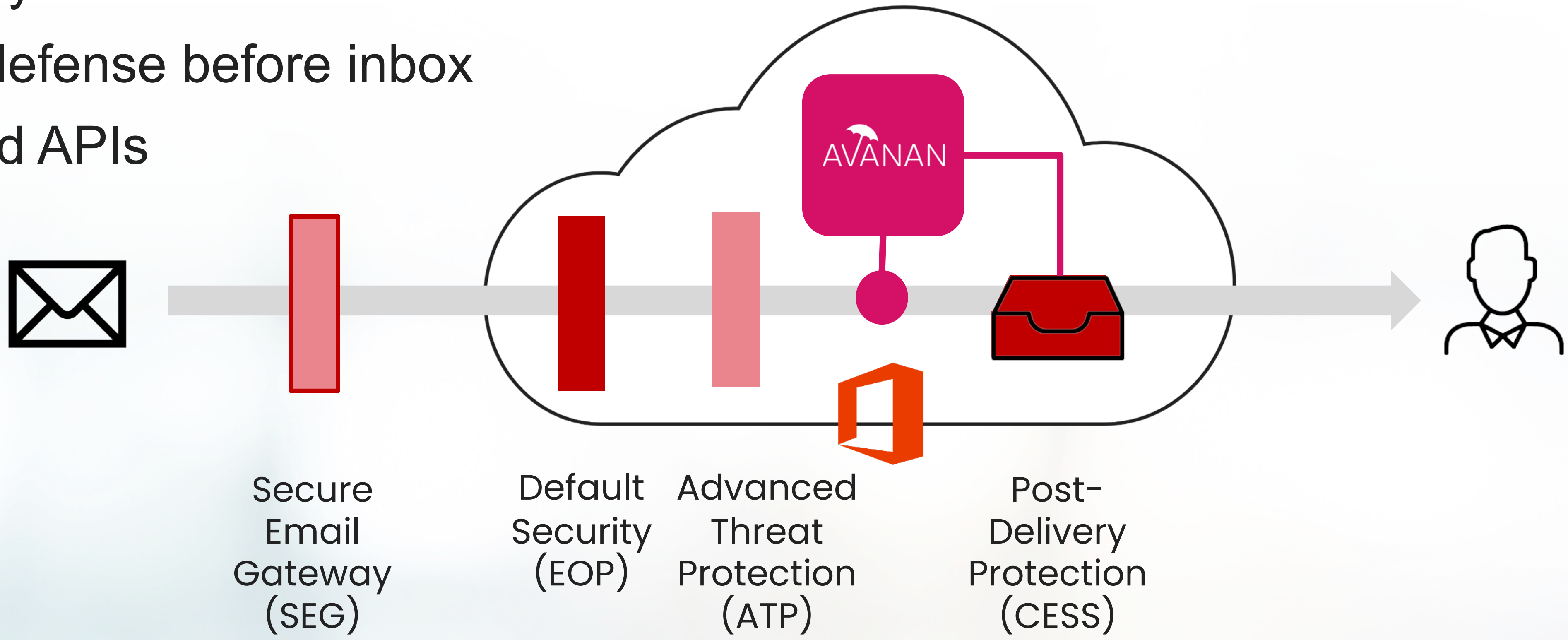
HARMONY CONNECT: SECURE INTERNET ACCESS

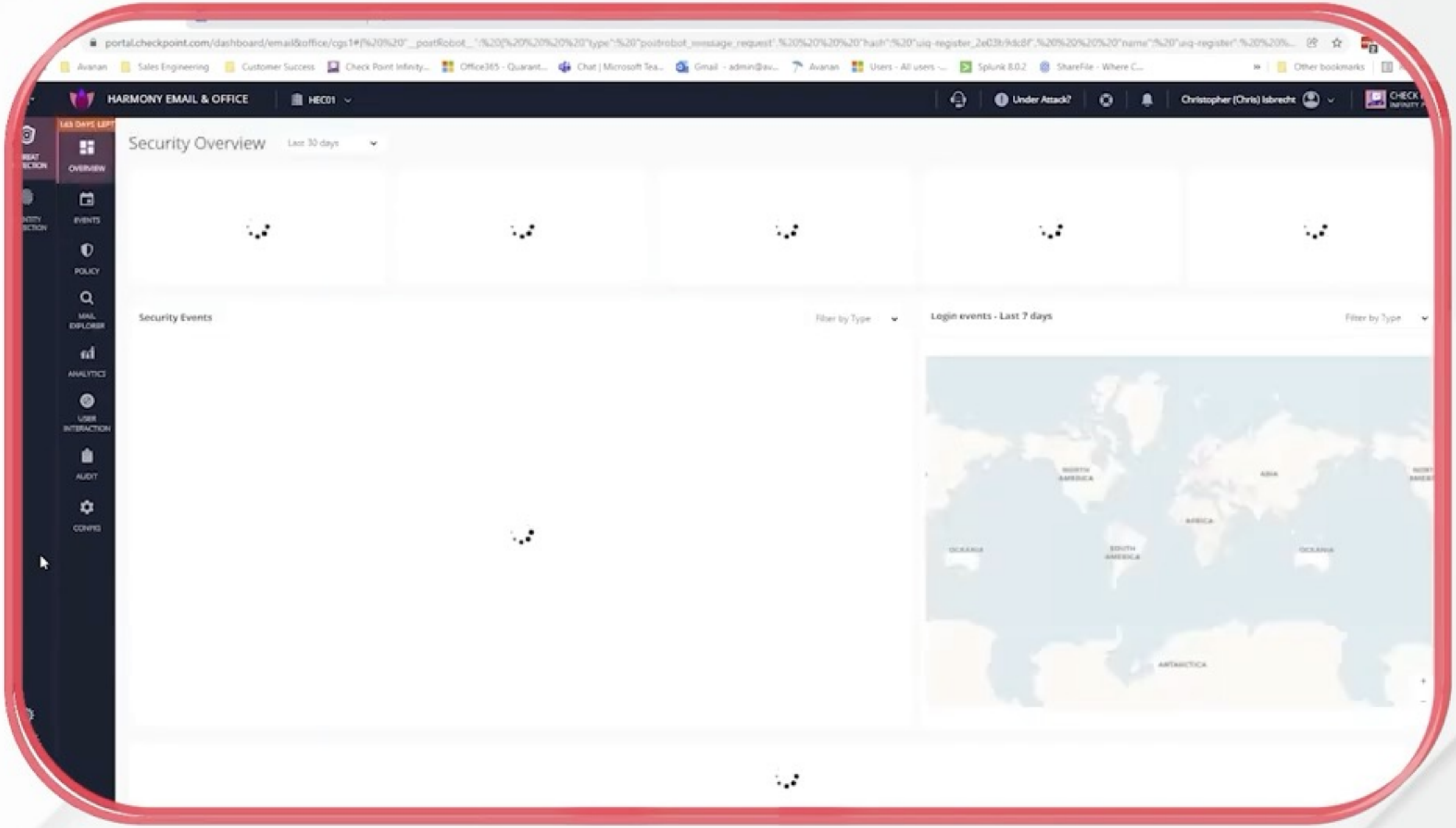


The Check Point Harmony Email & Collaboration Security Architecture

Avanan's Architecture

- Embedded Embedded within O365 as a layer
- Last line of defense before inbox
- Built on cloud APIs

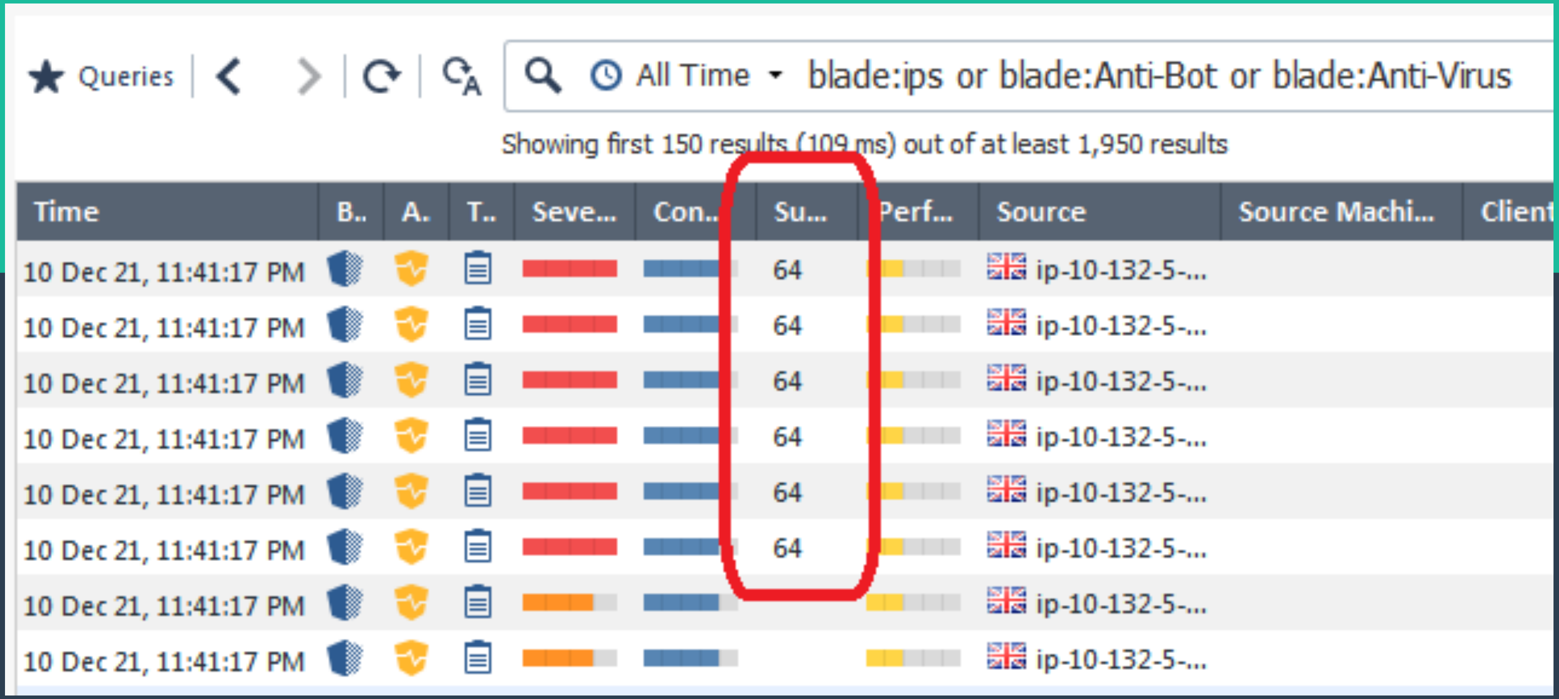

AVANAN
Secure Email Gateway (SEG)
Default Security (EOP)
Advanced Threat Protection (ATP)
Post-Delivery Protection (CESS)


portal.checkpoint.com/dashboard/email&office/cgs1#/{%20%20"__postRobot__":%20{%20%20%20%20"type":%20"postrobot_message_request",%20%20%20%20"hash":%20"uiq-register_2e03b9dc8f",%20%20%20%20"name":%20"uiq-register",%20%20%...
Avanan
Sales Engineering
Customer Success
Check Point Infinity...
Office365 - Quarant...
Chat | Microsoft Tea...
Gmail - admin@av...
Avanan
Users - All users -...
Splunk 8.0.2
ShareFile - Where C...
Other bookmarks
HARMONY EMAIL & OFFICE
HEC01
Under Attack?
Christopher (Chris) Isbrecht
CHECK
INFINITY
143 DAYS LEFT
THREAT DETECTION
OVERVIEW
IDENTITY DETECTION
EVENTS
POLICY
MAIL EXPLORER
ANALYTICS
USER INTERACTION
AUDIT
CONFIG
Security Overview
Last 30 days
Security Events
Filter by Type
Login events - Last 7 days
Filter by Type
NORTH AMERICA
ASIA
AFRICA
SOUTH AMERICA
OCEANIA
OCEANIA
ANTARCTICA

DEEP DIVE INTO THE FUTURE OF EMAIL SECURITY

Threat Prevention Log Suppression Display

- It is extremely easy to miss the Suppressed Logs field if you are not looking for it!
- Note that the Suppressed Logs field value *is* shown in the Results Pane when looking at the list of logs, but it is smashed horizontally by default and difficult to spot, be on the lookout for a non-empty value here which is an important clue!

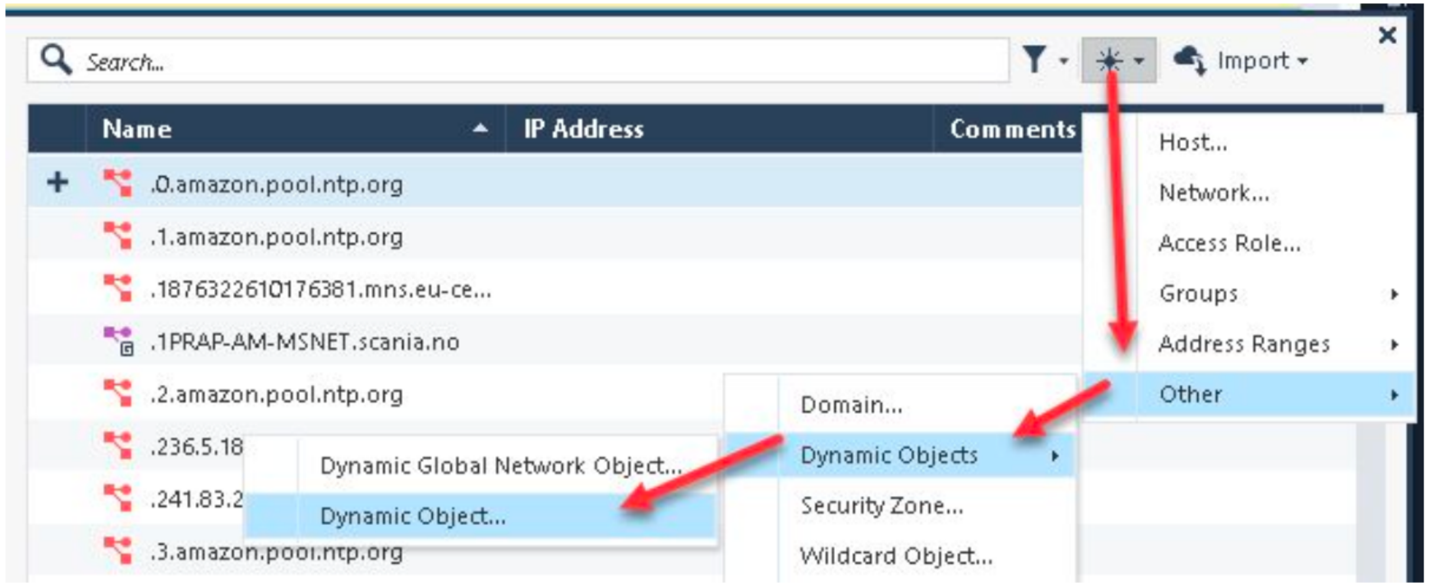


All Time ▾ blade:ips or blade:Anti-Bot or blade:Anti-Virus

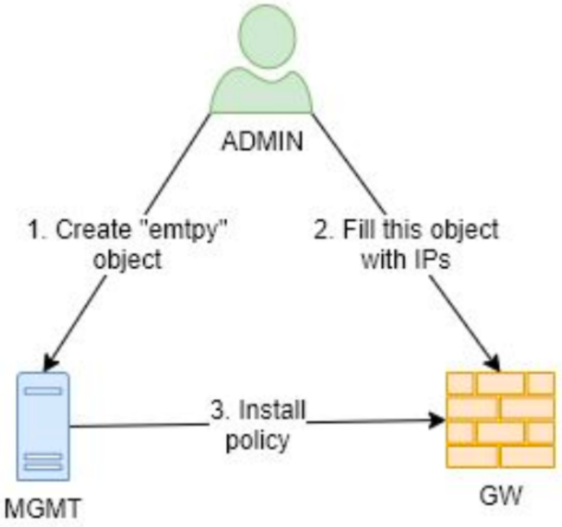
Showing first 150 results (109 ms) out of at least 1,950 results

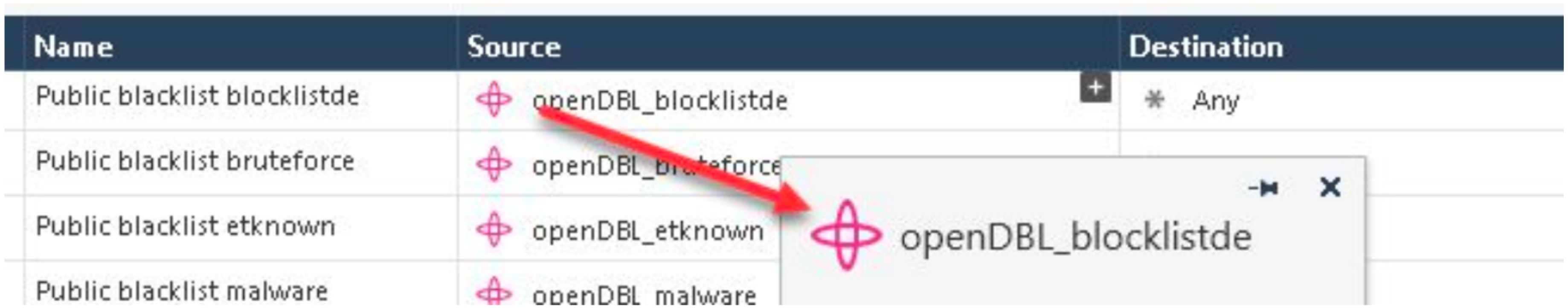
Time	B..	A.	T..	Seve...	Con..	Su...	Perf...	Source	Source Machi...	Client
10 Dec 21, 11:41:17 PM	🛡	🛡	📋	🟥	🟦	64	🟨	ip-10-132-5-...		
10 Dec 21, 11:41:17 PM	🛡	🛡	📋	🟥	🟦	64	🟨	ip-10-132-5-...		
10 Dec 21, 11:41:17 PM	🛡	🛡	📋	🟥	🟦	64	🟨	ip-10-132-5-...		
10 Dec 21, 11:41:17 PM	🛡	🛡	📋	🟥	🟦	64	🟨	ip-10-132-5-...		
10 Dec 21, 11:41:17 PM	🛡	🛡	📋	🟥	🟦	64	🟨	ip-10-132-5-...		
10 Dec 21, 11:41:17 PM	🛡	🛡	📋	🟥	🟦	64	🟨	ip-10-132-5-...		
10 Dec 21, 11:41:17 PM	🛡	🛡	📋	🟧	🟦		🟨	ip-10-132-5-...		
10 Dec 21, 11:41:17 PM	🛡	🛡	📋	🟧	🟦		🟨	ip-10-132-5-...		

Dynamic Objects - Implementation Mgmt



Name	IP Address	Comments
.0.amazon.pool.ntp.org		
.1.amazon.pool.ntp.org		
.187632261O176381.mns.eu-ce...		
.1PRAP-AM-MSNET.scania.no		
.2.amazon.pool.ntp.org		
.236.5.18		
.241.83.2		
.3.amazon.pool.ntp.org		





Name	Source	Destination
Public blacklist blocklistde	openDBL_blocklistde	Any
Public blacklist bruteforce	openDBL_bruteforce	
Public blacklist etknown	openDBL_etknown	
Public blacklist malware	openDBL_malware	

AGENDA

- NETWORK SECURITY AS A SERVICE ON AWS
- KUBERNETES AI MICROSEGMENTATION
- DEVELOPER FIRST SECURITY (SPECTRAL)
- AZURE VWAN

Cloud Network Security as a Service

Network Segmentation Security Made Easy!

Cloud Network Security as a Service – Automated

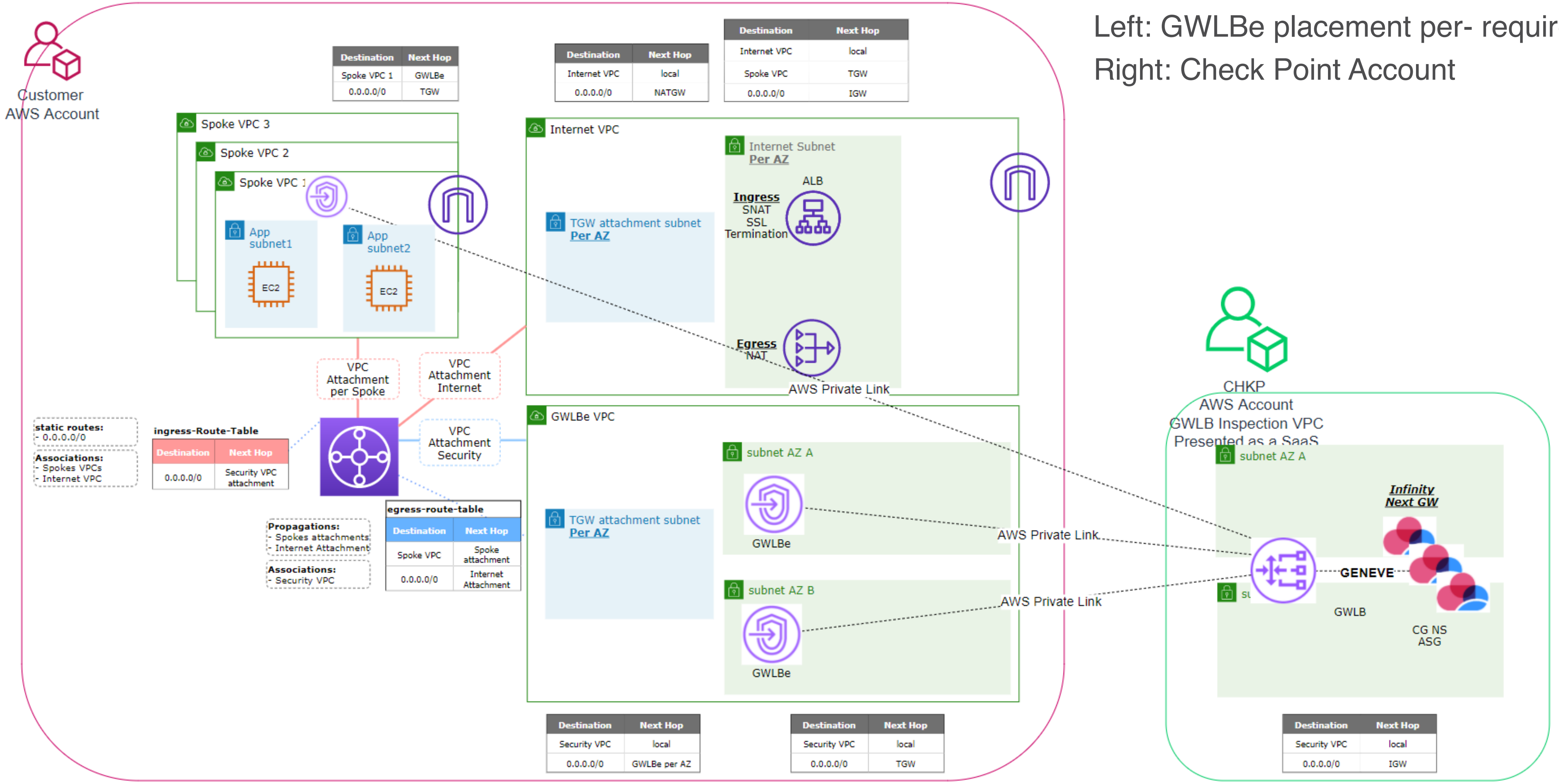
- ✓10 minutes onboarding
- ✓APIs first design
- ✓Web UI manager
- ✓Fully scalable, Highly available
- ✓Policy automation

Check Point
SOFTWARE TECHNOLOGIES LTD
Cloud Network Security as a Service

Customer deployment architecture

Left: GWLBe placement per- requirements

Right: Check Point Account



Destination	Next Hop
Spoke VPC 1	GWLBe
0.0.0.0/0	TGW

Destination	Next Hop
Internet VPC	local
0.0.0.0/0	NATGW

Destination	Next Hop
Internet VPC	local
Spoke VPC	TGW
0.0.0.0/0	IGW

static routes:
- 0.0.0.0/0

Associations:
- Spokes VPCs
- Internet VPC

ingress-Route-Table

Destination	Next Hop
0.0.0.0/0	Security VPC attachment

Propagations:
- Spokes attachments
- Internet Attachment

Associations:
- Security VPC

egress-route-table

Destination	Next Hop
Spoke VPC	Spoke attachment
0.0.0.0/0	Internet Attachment

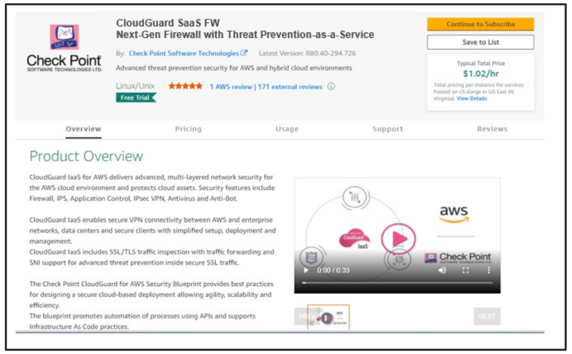
Destination	Next Hop
Security VPC	local
0.0.0.0/0	GWLBe per AZ

Destination	Next Hop
Security VPC	local
0.0.0.0/0	TGW

Destination	Next Hop
Security VPC	local
0.0.0.0/0	IGW

Customer Onboarding

AWS Marketplace page



CloudGuard SaaS FW
Next-Gen Firewall with Threat Prevention-as-a-Service

By: Check Point Software Technologies   Latest Version: R80.40-294.726

Advanced threat prevention security for AWS and hybrid cloud environments

Linux/Unix ★★★★★ 1 AWS review | 171 external reviews

Free Trial

Typical Total Price
$1.02/hr
Total pricing per instance for services hosted on c5.xlarge in US East (N. Virginia). View Details

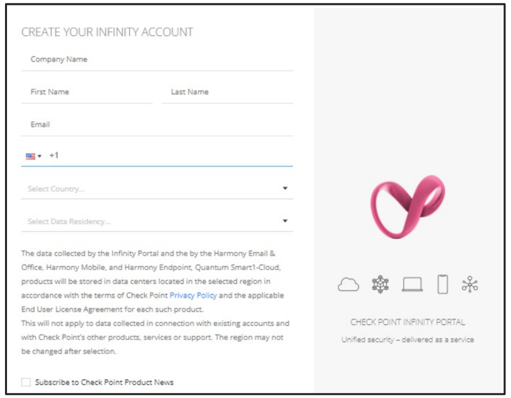
Product Overview

CloudGuard IaaS for AWS delivers advanced, multi-layered network security for the AWS cloud environment and protects cloud assets. Security features include Firewall, IPS, Application Control, IPsec VPN, Antivirus and Anti-Bot.

CloudGuard IaaS enables secure VPN connectivity between AWS and enterprise networks, data centers and secure clients with simplified setup, deployment and management.
CloudGuard IaaS includes SSL/TLS traffic inspection with traffic forwarding and SNI support for advanced threat prevention inside secure SSL traffic.

The Check Point CloudGuard for AWS Security Blueprint provides best practices for designing a secure cloud-based deployment allowing agility, scalability and efficiency.
The blueprint promotes automation of processes using APIs and supports Infrastructure As Code practices.

Cloud Infra Account Creation



CREATE YOUR INFINITY ACCOUNT

Company Name

First Name   Last Name

Email

+1

Select Country...

Select Data Residency...

The data collected by the Infinity Portal and the by the Harmony Email & Office, Harmony Mobile, and Harmony Endpoint, Quantum Smart1-Cloud, products will be stored in data centers located in the selected region in accordance with the terms of Check Point Privacy Policy and the applicable End User License Agreement for each such product.
This will not apply to data collected in connection with existing accounts and with Check Point's other products, services or support. The region may not be changed after selection.

☐ Subscribe to Check Point Product News

CHECK POINT INFINITY PORTAL
Unified security – delivered as a service

Cloud Infra App Selection

CloudGuard
Firewall-as-a-Service

Cross Account

- AWS <> CP cross account handshake

Service setup

- Cross account role creation
- GWLB / Endpoint association

Security Policy Setup

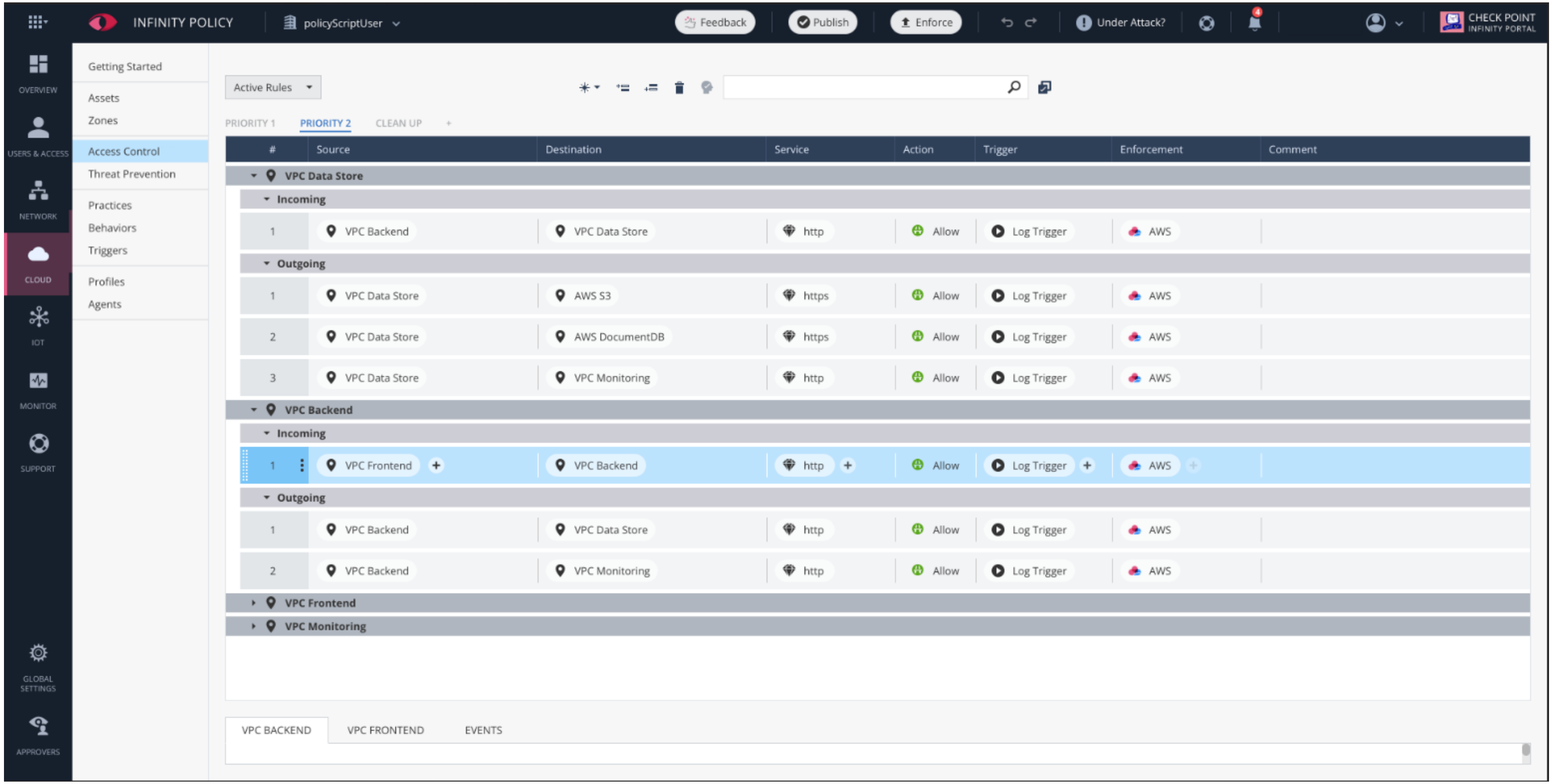
- Practices selection
- Setting triggers – logs
- Policy rules creation

Situational visibility

- Monitor status
- Logs visibility

CHECK POINT

Check Point Infinity Management Portal



#	Source	Destination	Service	Action	Trigger	Enforcement	Comment
VPC Data Store							
Incoming							
1	VPC Backend	VPC Data Store	http	Allow	Log Trigger	AWS	
Outgoing							
1	VPC Data Store	AWS S3	https	Allow	Log Trigger	AWS	
2	VPC Data Store	AWS DocumentDB	https	Allow	Log Trigger	AWS	
3	VPC Data Store	VPC Monitoring	http	Allow	Log Trigger	AWS	
VPC Backend							
Incoming							
1	VPC Frontend	VPC Backend	http	Allow	Log Trigger	AWS	
Outgoing							
1	VPC Backend	VPC Data Store	http	Allow	Log Trigger	AWS	
2	VPC Backend	VPC Monitoring	http	Allow	Log Trigger	AWS	
VPC Frontend							
VPC Monitoring							

Registration for EA is now open

www.checkpoint.com/nsaas

CHECK POINT™

CLOUDGUARD K8S MICROSEGMENTATION

Add container-level access control to your K8s clusters in a modern, automated & easy way

CPX 360

Why Microsegmentation in K8s?

K8s Microsegmentation is a **critical security layer:**

- Background: In K8s different Pods need to communicate with:
  - other pods/services (complex microservice architectures)
  - Internet (in- or outbound)
- Challenge: No default restrictions for pod-2-pod communication
- Risk: **If pod is breached -> high risk of lateral movement!**
- Solution: **Microsegmentation on pod/container-level for Zero Trust Network Security in K8s clusters**

CloudGuard K8s Microsegmentation Components

- **Nano Attachment:** lightweight library, added automatically to running containers. Monitors and enforces in- & outbound traffic to container.
  Asks the Nano Agent for policy decisions and caches results.
- **Nano Agent:** Holds the policy, receives 5-tuples from Nano Attachments for policy decisions, communicates with „Infinity Policy“ Mgmt, 1 agent/worker node
- **Attachment Deployment Agent:** Deploys Nano Attachments to each pod when started.
- **Discovery Agent:** Collects detailed info about the assets in the K8s cluster (pods, services, labels, ...) and provides it to the Mgmt

How is K8s Microsegmentation managed?

- **Infinity Policy:** SaaS Mgmt, integrated in „Infinity Portal“, manages

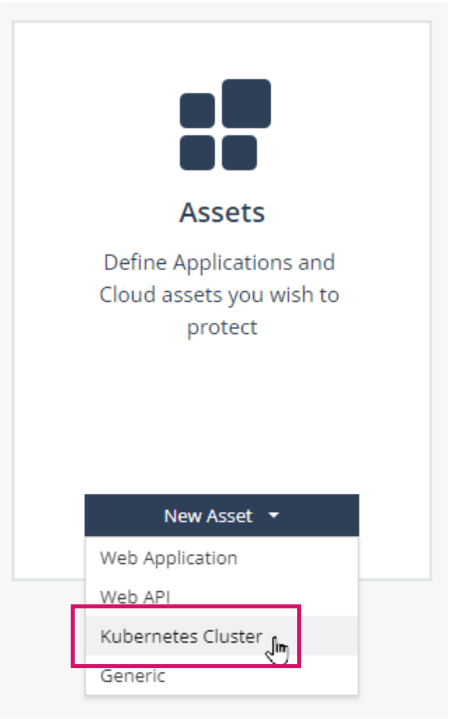
  Manages Access Control policies, Zones, Agent Deployment Profiles, Learning
  Provides Logs, Reporting, Learning, Visualization

- **Infinity Portal:** SaaS Mgmt for all Check Point products
- **API support** (GraphQL)
- **Infinity Policy provides unified next-gen mgmt** also for other solutions: CloudGuard AppSec, NSaaS for AWS as well as Quantum IOT Protect

Get started here: https://portal.checkpoint.com

Deployment

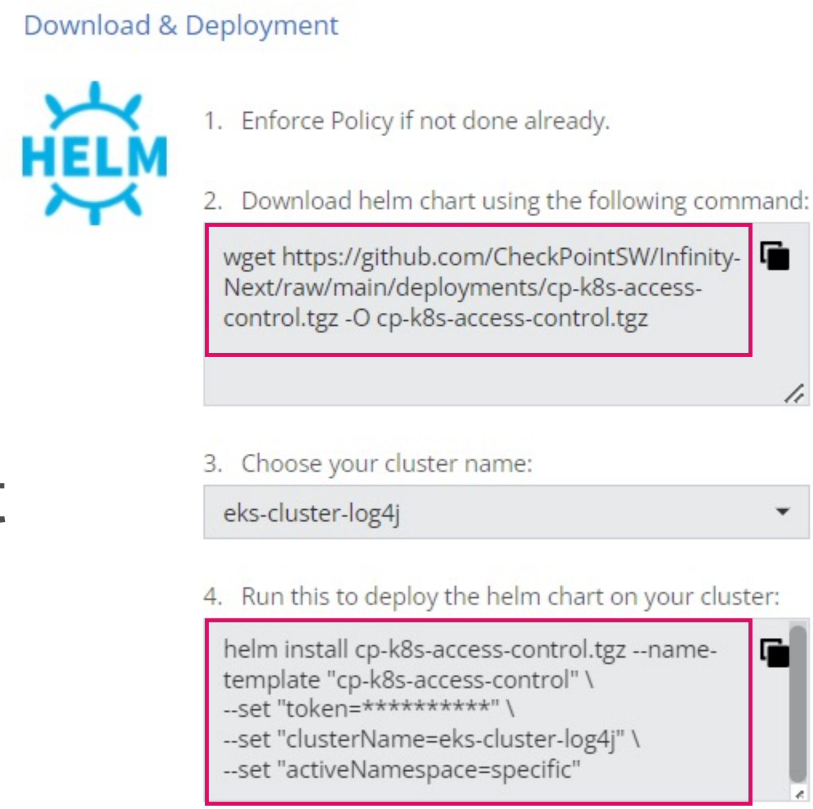
- **Create new K8s cluster** asset in Infinity Policy, this will generate also an agent deployment profile:



Assets

Define Applications and Cloud assets you wish to protect

- **Download** and install the **helm chart** as shown in the agent deployment profile:



Download & Deployment

1. Enforce Policy if not done already.
2. Download helm chart using the following command:

```
wget https://github.com/CheckPointSW/Infinity-Next/raw/main/deployments/cp-k8s-access-control.tgz -O cp-k8s-access-control.tgz
```

3. Choose your cluster name:

eks-cluster-log4j

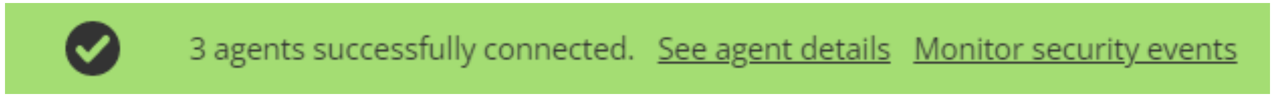
4. Run this to deploy the helm chart on your cluster:

```
helm install cp-k8s-access-control.tgz --name-template "cp-k8s-access-control" \
--set "token=**********" \
--set "clusterName=eks-cluster-log4j" \
--set "activeNamespace=specific"
```

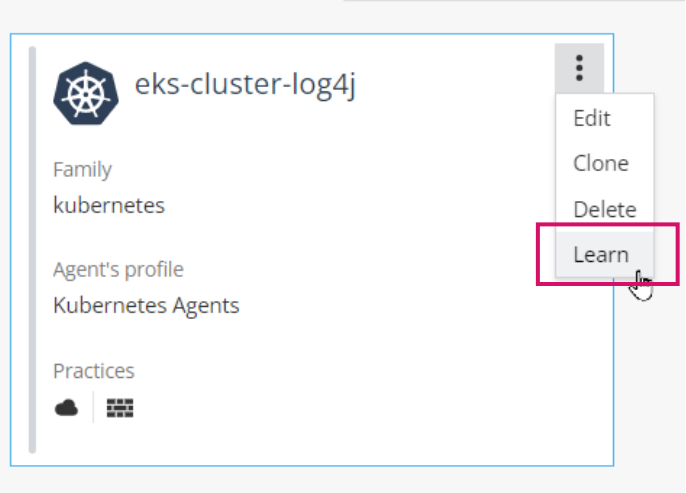
- Restart all pods eventually running during deployment once so they also get the Nano attachment added.

ML-based Learning

- Once deployed agents connect back to the mgmt:



✓ 3 agents successfully connected. See agent details Monitor security events



eks-cluster-log4j

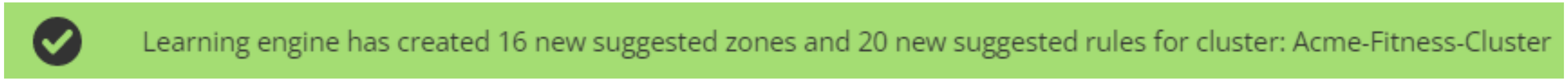
Family
kubernetes

Agent's profile
Kubernetes Agents

Practices

- Now system starts logging traffic in K8s cluster. Once typical traffic patterns have been observed, activate the „Learning“:

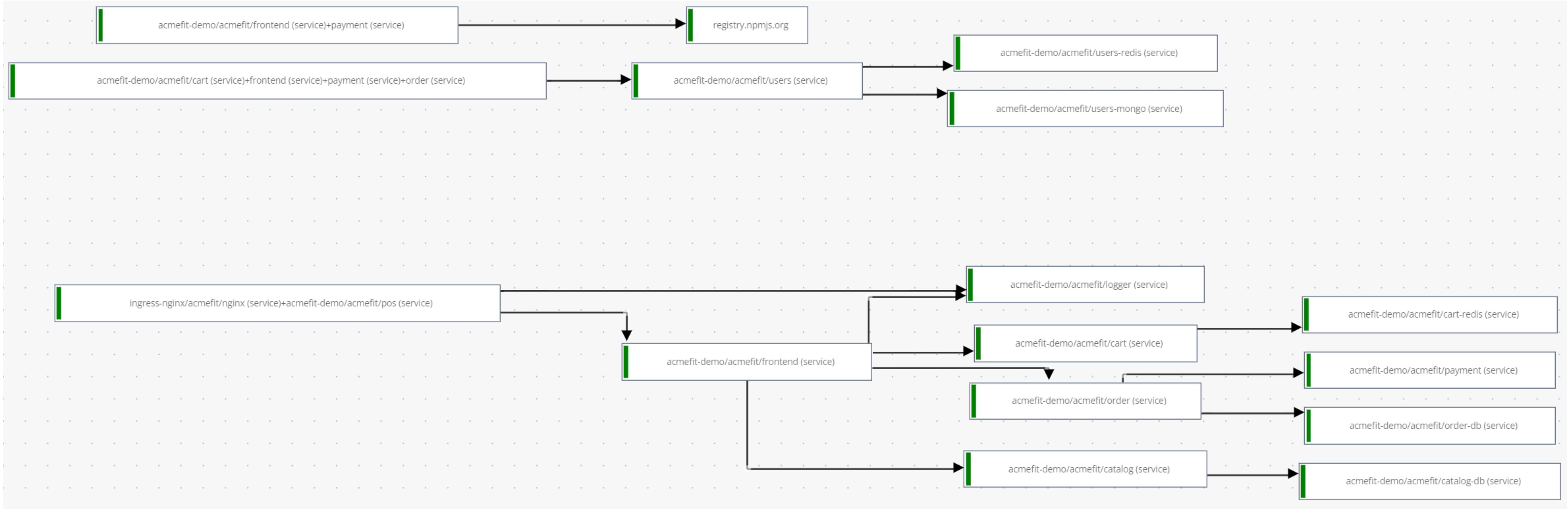
- ML-engine then performs automatic learning on traffic observed so far. Sends notification when done:



✓ Learning engine has created 16 new suggested zones and 20 new suggested rules for cluster: Acme-Fitness-Cluster

Automatic Visualization

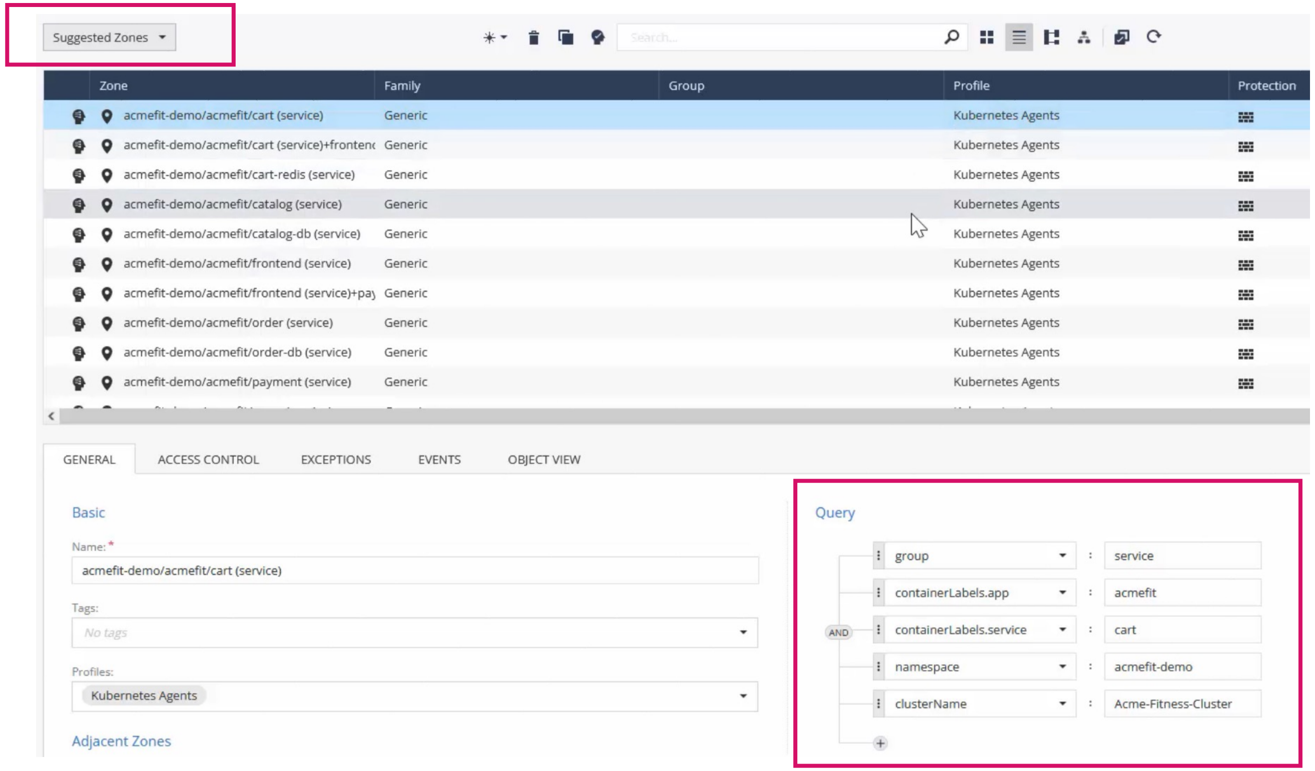
- Learning Engine automatically suggest „**Zones**“ (dyn. objects for K8s asset grouping), „**Rules**“ (based on Zones) and visualizes them:


acmefit-demo/acmefit/frontend (service)+payment (service)
registry.npmjs.org
acmefit-demo/acmefit/users-redis (service)
acmefit-demo/acmefit/cart (service)+frontend (service)+payment (service)+order (service)
acmefit-demo/acmefit/users (service)
acmefit-demo/acmefit/users-mongo (service)
acmefit-demo/acmefit/logger (service)
ingress-nginx/acmefit/nginx (service)+acmefit-demo/acmefit/pos (service)
acmefit-demo/acmefit/cart-redis (service)
acmefit-demo/acmefit/cart (service)
acmefit-demo/acmefit/frontend (service)
acmefit-demo/acmefit/payment (service)
acmefit-demo/acmefit/order (service)
acmefit-demo/acmefit/order-db (service)
acmefit-demo/acmefit/catalog (service)
acmefit-demo/acmefit/catalog-db (service)

CHECK POINT

Suggested Zones

- Suggested Zones can be reviewed, adjusted if needed and turned active.
- They are based on dyn. queries matching e.g.:
  - namespace,
  - labels,
  - clusterName, ...



Zone	Family	Group	Profile	Protection
acmefit-demo/acmefit/cart (service)	Generic		Kubernetes Agents	▦
acmefit-demo/acmefit/cart (service)+frontenc	Generic		Kubernetes Agents	▦
acmefit-demo/acmefit/cart-redis (service)	Generic		Kubernetes Agents	▦
acmefit-demo/acmefit/catalog (service)	Generic		Kubernetes Agents	▦
acmefit-demo/acmefit/catalog-db (service)	Generic		Kubernetes Agents	▦
acmefit-demo/acmefit/frontend (service)	Generic		Kubernetes Agents	▦
acmefit-demo/acmefit/frontend (service)+pay	Generic		Kubernetes Agents	▦
acmefit-demo/acmefit/order (service)	Generic		Kubernetes Agents	▦
acmefit-demo/acmefit/order-db (service)	Generic		Kubernetes Agents	▦
acmefit-demo/acmefit/payment (service)	Generic		Kubernetes Agents	▦

Basic

Name: *
acmefit-demo/acmefit/cart (service)

Tags:
No tags

Profiles:
Kubernetes Agents

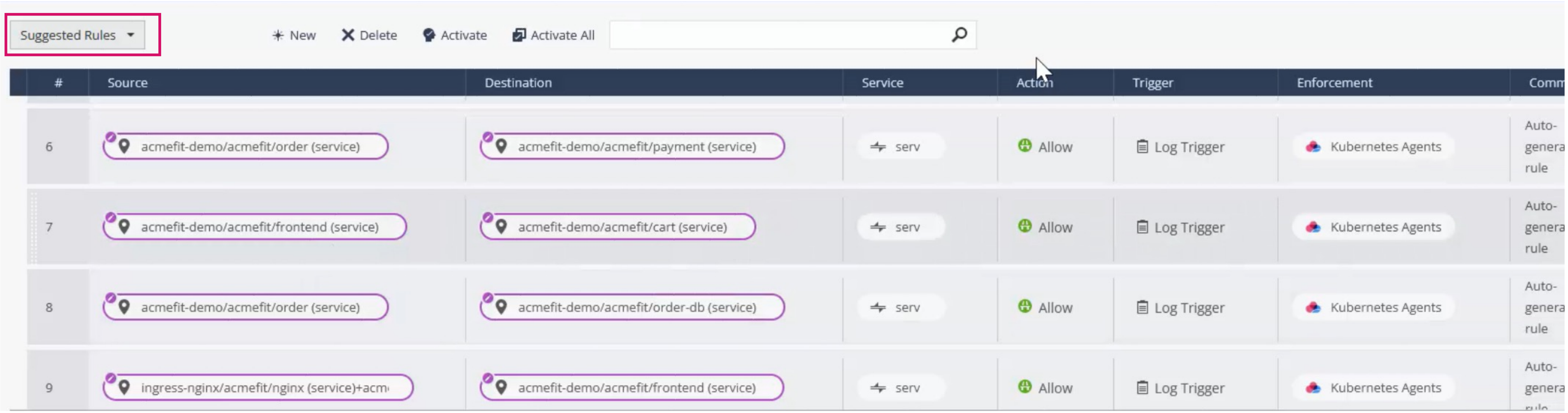
Adjacent Zones

Query

group	service
containerLabels.app	acmefit
containerLabels.service	cart
namespace	acmefit-demo
clusterName	Acme-Fitness-Cluster

Suggested Access Control Policy Rules

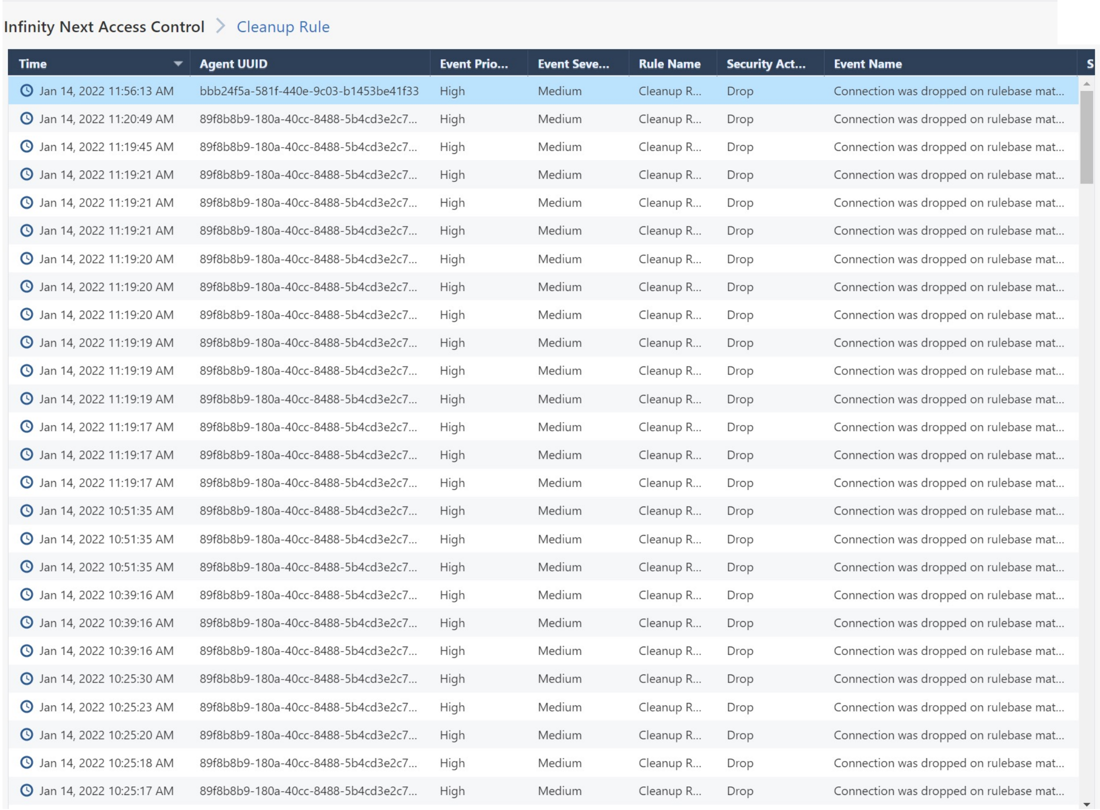
- Suggested Rules can be reviewed, adjusted if needed and activated.
- SRC and DST fields use the dynamic Zones.



#	Source	Destination	Service	Action	Trigger	Enforcement	Comm
6	acmefit-demo/acmefit/order (service)	acmefit-demo/acmefit/payment (service)	serv	Allow	Log Trigger	Kubernetes Agents	Auto- genera rule
7	acmefit-demo/acmefit/frontend (service)	acmefit-demo/acmefit/cart (service)	serv	Allow	Log Trigger	Kubernetes Agents	Auto- genera rule
8	acmefit-demo/acmefit/order (service)	acmefit-demo/acmefit/order-db (service)	serv	Allow	Log Trigger	Kubernetes Agents	Auto- genera rule
9	ingress-nginx/acmefit/nginx (service)+acm	acmefit-demo/acmefit/frontend (service)	serv	Allow	Log Trigger	Kubernetes Agents	Auto- genera rule

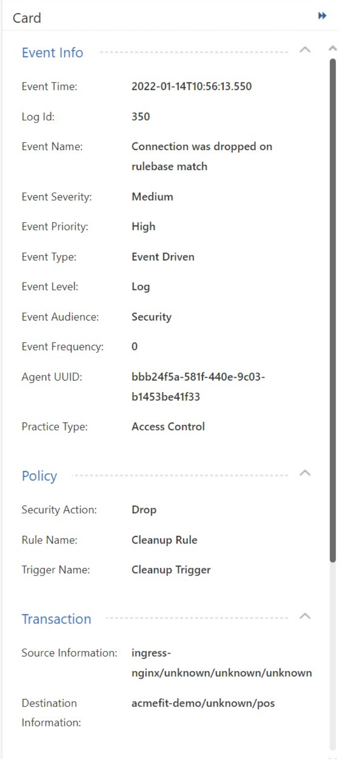
Logging and Reporting

- There‘s detailed Logs/Reports:



Infinity Next Access Control > Cleanup Rule

Time	Agent UUID	Event Prio...	Event Seve...	Rule Name	Security Act...	Event Name	S
Jan 14, 2022 11:56:13 AM	bbb24f5a-581f-440e-9c03-b1453be41f33	High	Medium	Cleanup R...	Drop	Connection was dropped on rulebase mat...	
Jan 14, 2022 11:20:49 AM	89f8b8b9-180a-40cc-8488-5b4cd3e2c7...	High	Medium	Cleanup R...	Drop	Connection was dropped on rulebase mat...	
Jan 14, 2022 11:19:45 AM	89f8b8b9-180a-40cc-8488-5b4cd3e2c7...	High	Medium	Cleanup R...	Drop	Connection was dropped on rulebase mat...	
Jan 14, 2022 11:19:21 AM	89f8b8b9-180a-40cc-8488-5b4cd3e2c7...	High	Medium	Cleanup R...	Drop	Connection was dropped on rulebase mat...	
Jan 14, 2022 11:19:21 AM	89f8b8b9-180a-40cc-8488-5b4cd3e2c7...	High	Medium	Cleanup R...	Drop	Connection was dropped on rulebase mat...	
Jan 14, 2022 11:19:21 AM	89f8b8b9-180a-40cc-8488-5b4cd3e2c7...	High	Medium	Cleanup R...	Drop	Connection was dropped on rulebase mat...	
Jan 14, 2022 11:19:20 AM	89f8b8b9-180a-40cc-8488-5b4cd3e2c7...	High	Medium	Cleanup R...	Drop	Connection was dropped on rulebase mat...	
Jan 14, 2022 11:19:20 AM	89f8b8b9-180a-40cc-8488-5b4cd3e2c7...	High	Medium	Cleanup R...	Drop	Connection was dropped on rulebase mat...	
Jan 14, 2022 11:19:20 AM	89f8b8b9-180a-40cc-8488-5b4cd3e2c7...	High	Medium	Cleanup R...	Drop	Connection was dropped on rulebase mat...	
Jan 14, 2022 11:19:19 AM	89f8b8b9-180a-40cc-8488-5b4cd3e2c7...	High	Medium	Cleanup R...	Drop	Connection was dropped on rulebase mat...	
Jan 14, 2022 11:19:19 AM	89f8b8b9-180a-40cc-8488-5b4cd3e2c7...	High	Medium	Cleanup R...	Drop	Connection was dropped on rulebase mat...	
Jan 14, 2022 11:19:19 AM	89f8b8b9-180a-40cc-8488-5b4cd3e2c7...	High	Medium	Cleanup R...	Drop	Connection was dropped on rulebase mat...	
Jan 14, 2022 11:19:17 AM	89f8b8b9-180a-40cc-8488-5b4cd3e2c7...	High	Medium	Cleanup R...	Drop	Connection was dropped on rulebase mat...	
Jan 14, 2022 11:19:17 AM	89f8b8b9-180a-40cc-8488-5b4cd3e2c7...	High	Medium	Cleanup R...	Drop	Connection was dropped on rulebase mat...	
Jan 14, 2022 11:19:17 AM	89f8b8b9-180a-40cc-8488-5b4cd3e2c7...	High	Medium	Cleanup R...	Drop	Connection was dropped on rulebase mat...	
Jan 14, 2022 10:51:35 AM	89f8b8b9-180a-40cc-8488-5b4cd3e2c7...	High	Medium	Cleanup R...	Drop	Connection was dropped on rulebase mat...	
Jan 14, 2022 10:51:35 AM	89f8b8b9-180a-40cc-8488-5b4cd3e2c7...	High	Medium	Cleanup R...	Drop	Connection was dropped on rulebase mat...	
Jan 14, 2022 10:51:35 AM	89f8b8b9-180a-40cc-8488-5b4cd3e2c7...	High	Medium	Cleanup R...	Drop	Connection was dropped on rulebase mat...	
Jan 14, 2022 10:39:16 AM	89f8b8b9-180a-40cc-8488-5b4cd3e2c7...	High	Medium	Cleanup R...	Drop	Connection was dropped on rulebase mat...	
Jan 14, 2022 10:39:16 AM	89f8b8b9-180a-40cc-8488-5b4cd3e2c7...	High	Medium	Cleanup R...	Drop	Connection was dropped on rulebase mat...	
Jan 14, 2022 10:39:16 AM	89f8b8b9-180a-40cc-8488-5b4cd3e2c7...	High	Medium	Cleanup R...	Drop	Connection was dropped on rulebase mat...	
Jan 14, 2022 10:25:30 AM	89f8b8b9-180a-40cc-8488-5b4cd3e2c7...	High	Medium	Cleanup R...	Drop	Connection was dropped on rulebase mat...	
Jan 14, 2022 10:25:23 AM	89f8b8b9-180a-40cc-8488-5b4cd3e2c7...	High	Medium	Cleanup R...	Drop	Connection was dropped on rulebase mat...	
Jan 14, 2022 10:25:20 AM	89f8b8b9-180a-40cc-8488-5b4cd3e2c7...	High	Medium	Cleanup R...	Drop	Connection was dropped on rulebase mat...	
Jan 14, 2022 10:25:18 AM	89f8b8b9-180a-40cc-8488-5b4cd3e2c7...	High	Medium	Cleanup R...	Drop	Connection was dropped on rulebase mat...	
Jan 14, 2022 10:25:17 AM	89f8b8b9-180a-40cc-8488-5b4cd3e2c7...	High	Medium	Cleanup R...	Drop	Connection was dropped on rulebase mat...	



Card

Event Info

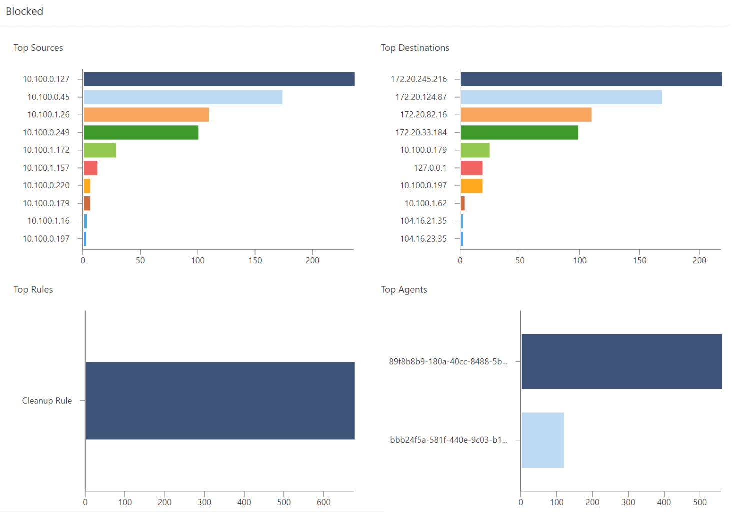
Event Time:	2022-01-14T10:56:13.550
Log Id:	350
Event Name:	Connection was dropped on rulebase match
Event Severity:	Medium
Event Priority:	High
Event Type:	Event Driven
Event Level:	Log
Event Audience:	Security
Event Frequency:	0
Agent UUID:	bbb24f5a-581f-440e-9c03-b1453be41f33
Practice Type:	Access Control

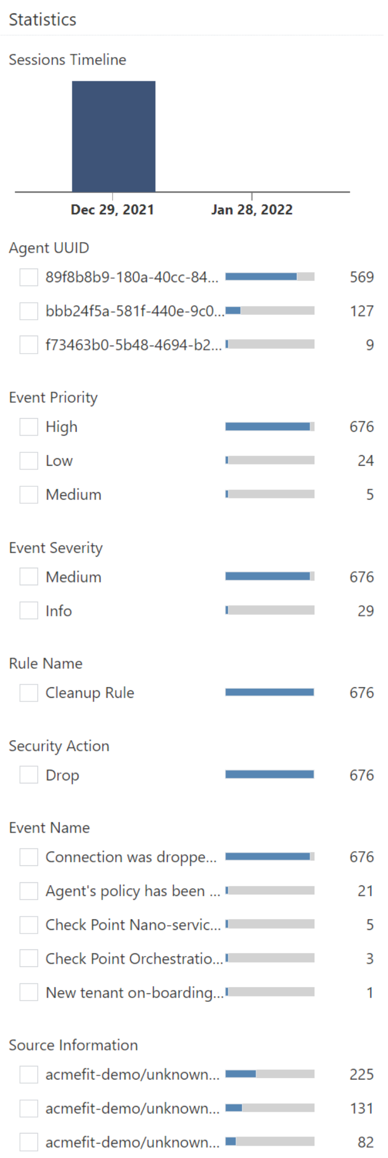
Policy

Security Action:	Drop
Rule Name:	Cleanup Rule
Trigger Name:	Cleanup Trigger

Transaction

Source Information:	ingress-nginx/unknown/unknown/unknown
Destination Information:	acmefit-demo/unknown/pos





Agent UUID

□ 89f8b8b9-180a-40cc-84...	569
□ bbb24f5a-581f-440e-9c0...	127
□ f73463b0-5b48-4694-b2...	9

Event Priority

□ High	676
□ Low	24
□ Medium	5

Event Severity

□ Medium	676
□ Info	29

Rule Name

□ Cleanup Rule	676

Security Action

□ Drop	676

Event Name

□ Connection was droppe...	676
□ Agent's policy has been ...	21
□ Check Point Nano-servic...	5
□ Check Point Orchestratio...	3
□ New tenant on-boarding...	1

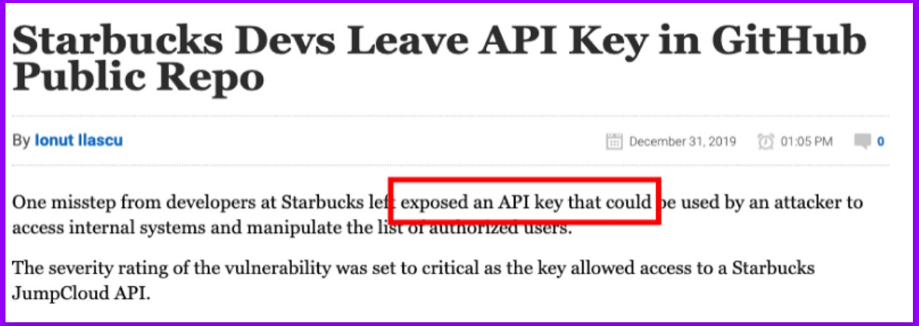
Source Information

□ acmefit-demo/unknown...	225
□ acmefit-demo/unknown...	131
□ acmefit-demo/unknown...	82

CHECK POINT™

DEVELOPER-FIRST CLOUD SECURITY / SPECTRAL

Secrets. Misconfiguration. Data privacy. Oops! 💣

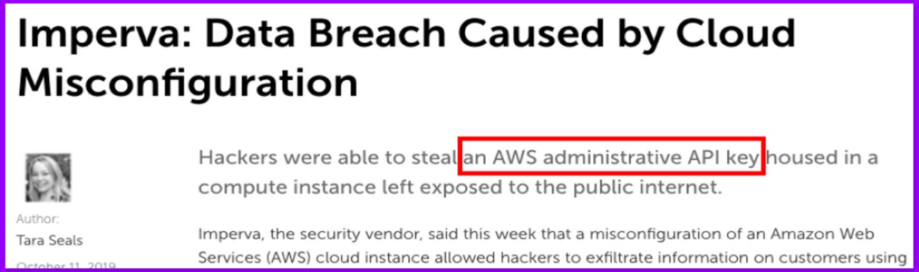


Starbucks Devs Leave API Key in GitHub Public Repo

By Ionut Ilascu December 31, 2019 01:05 PM 0

One misstep from developers at Starbucks left exposed an API key that could be used by an attacker to access internal systems and manipulate the list of authorized users.

The severity rating of the vulnerability was set to critical as the key allowed access to a Starbucks JumpCloud API.

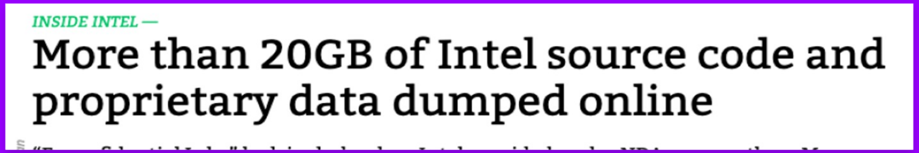


Imperva: Data Breach Caused by Cloud Misconfiguration

Author:
Tara Seals
October 11, 2019

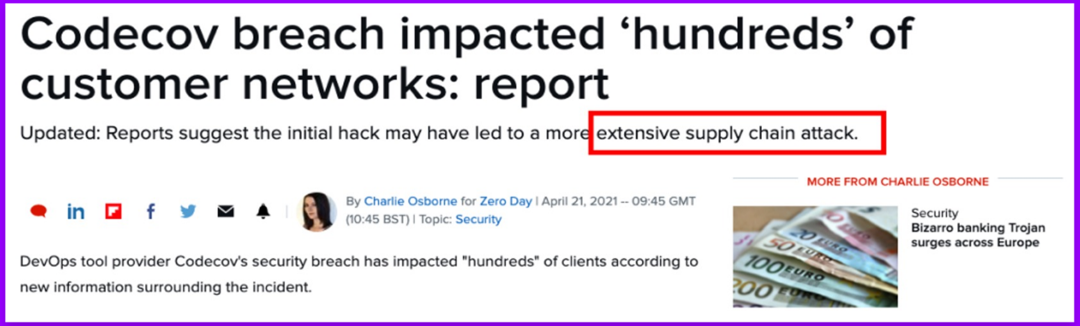
Hackers were able to steal an AWS administrative API key housed in a compute instance left exposed to the public internet.

Imperva, the security vendor, said this week that a misconfiguration of an Amazon Web Services (AWS) cloud instance allowed hackers to exfiltrate information on customers using



INSIDE INTEL —

More than 20GB of Intel source code and proprietary data dumped online



Codecov breach impacted 'hundreds' of customer networks: report

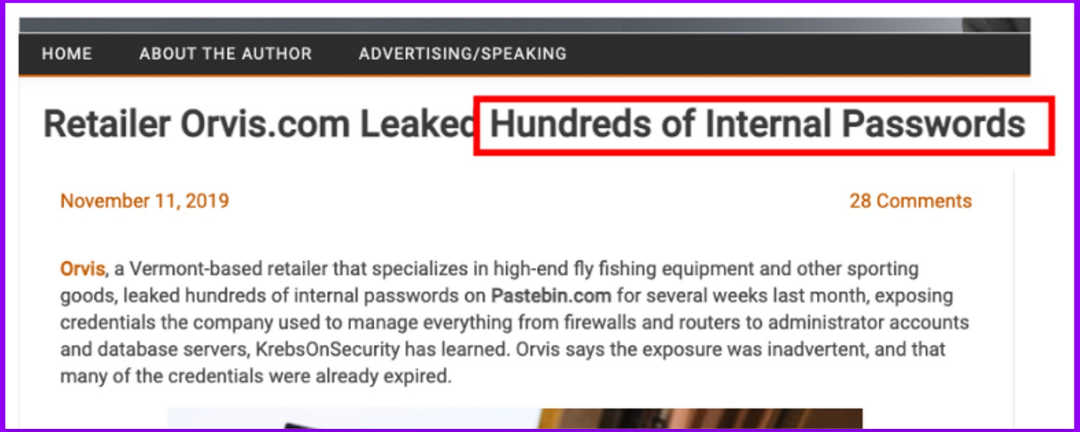
Updated: Reports suggest the initial hack may have led to a more extensive supply chain attack.

By Charlie Osborne for Zero Day | April 21, 2021 -- 09:45 GMT (10:45 BST) | Topic: Security

DevOps tool provider Codecov's security breach has impacted "hundreds" of clients according to new information surrounding the incident.

MORE FROM CHARLIE OSBORNE

Security
Bizarro banking Trojan surges across Europe



Retailer Orvis.com Leaked Hundreds of Internal Passwords

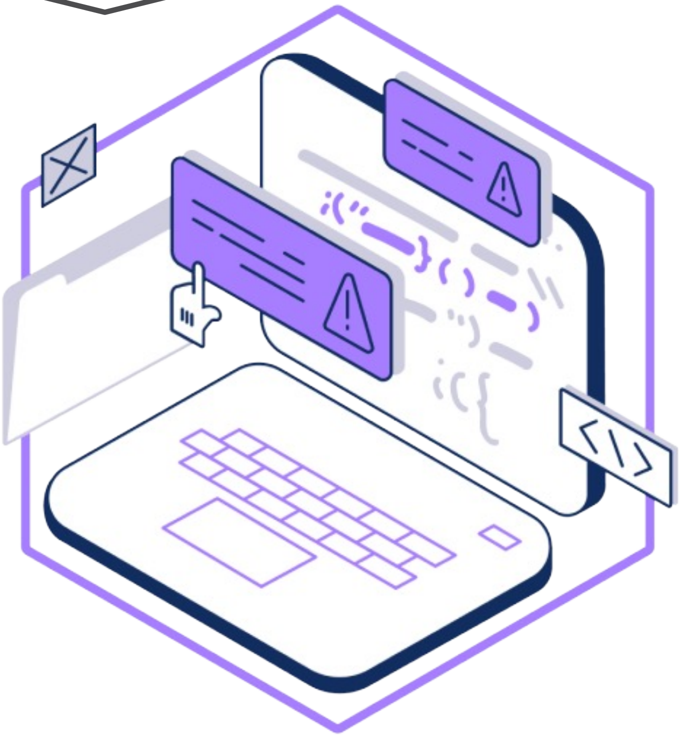
November 11, 2019 28 Comments

Orvis, a Vermont-based retailer that specializes in high-end fly fishing equipment and other sporting goods, leaked hundreds of internal passwords on **Pastebin.com** for several weeks last month, exposing credentials the company used to manage everything from firewalls and routers to administrator accounts and database servers, KrebsOnSecurity has learned. Orvis says the exposure was inadvertent, and that many of the credentials were already expired.

Spectral Value:

Prevent Costly Mistakes in Build Time

What we are solving: Ensure a secure development process for a dev team enforced by CI. Harden CI/CD processes by eliminating common mistakes.



Benefits:

Integrate with your CI

- SpectralOps integrates with all leading CI systems with built-in support for Jenkins, Azure and others.

Detect as early as a pre-commit

- When working with Git, employ our pre-commit, Husky and custom hooks to automate early issue detection.

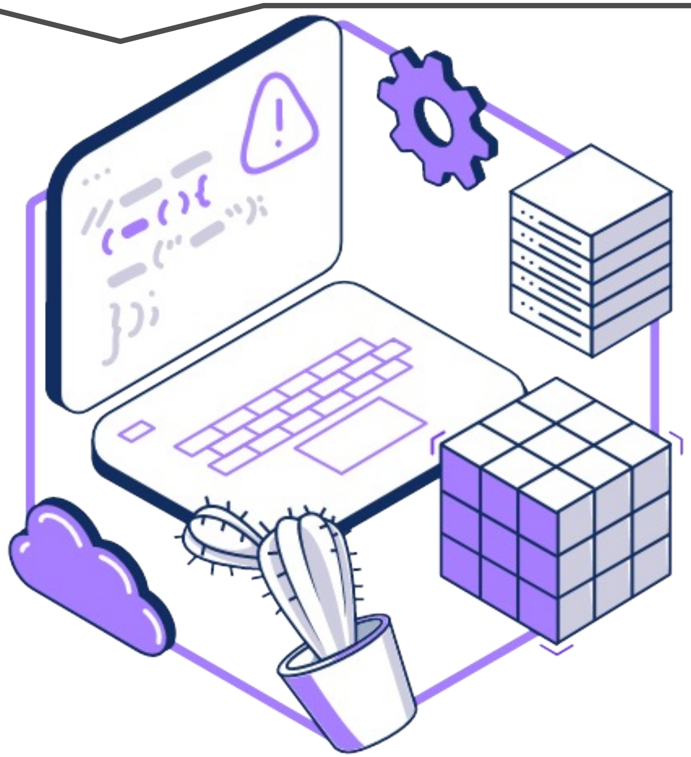
Install your build systems plugin

- Scan during your static builds with native plugins for JAMStack, Webpack, Gatsby, Netlify and more.

Spectral Value:

Developer First

What we are solving: Developer friendly security which can be driven from your command line, is extendable, and customizable.



Benefits:

Scan at record time

- Average sized repo only takes seconds to scan.

Leverage zero-config

- Runs securely by default with no special configuration needed.

Secure by design

- Scan your GitHub, GitLab, Bitbucket, Npm, and more without granting any permissions of any kind.

CHECK POINT

Spectral use cases: Shift-Left done right

Shift-left Infra & Code Scanning

Scan code, configuration, binaries, or any other material in your codebase. Uncover issues that are visible and hidden from plain sight.

Shift-left Source Controls & CI/CD Security

Ensure a secure development process for a dev team enforced by CI. Harden CI/CD processes by eliminating common mistakes.

Shift-left Source Code Leakage Detection

Mitigate secret leaks caused by bad credentials hygiene and human error

Shift-left Code Tampering Prevention

Easy and safe shift-left provenance, verifying runnable scripts and binaries. Plug your own malware/threat detection

Shift-left Hard Coded Secret Detection

Map and monitor hidden sensitive assets such as codebases, logs, and other sensitive intellectual property that belong to your organization, but were left exposed in public facing repositories.

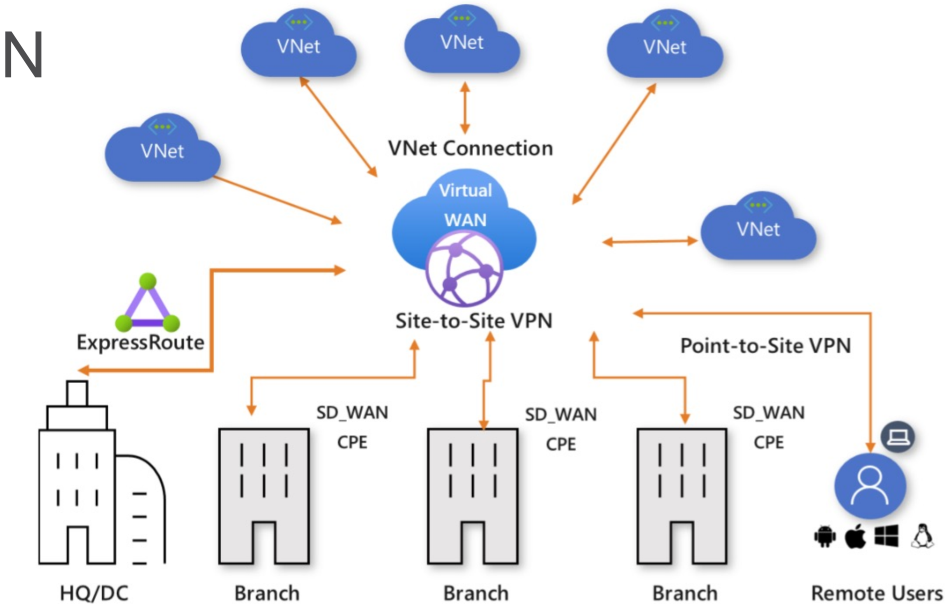
CHECK POINT™

SECURING AZURE VWAN HUB

CPX 360

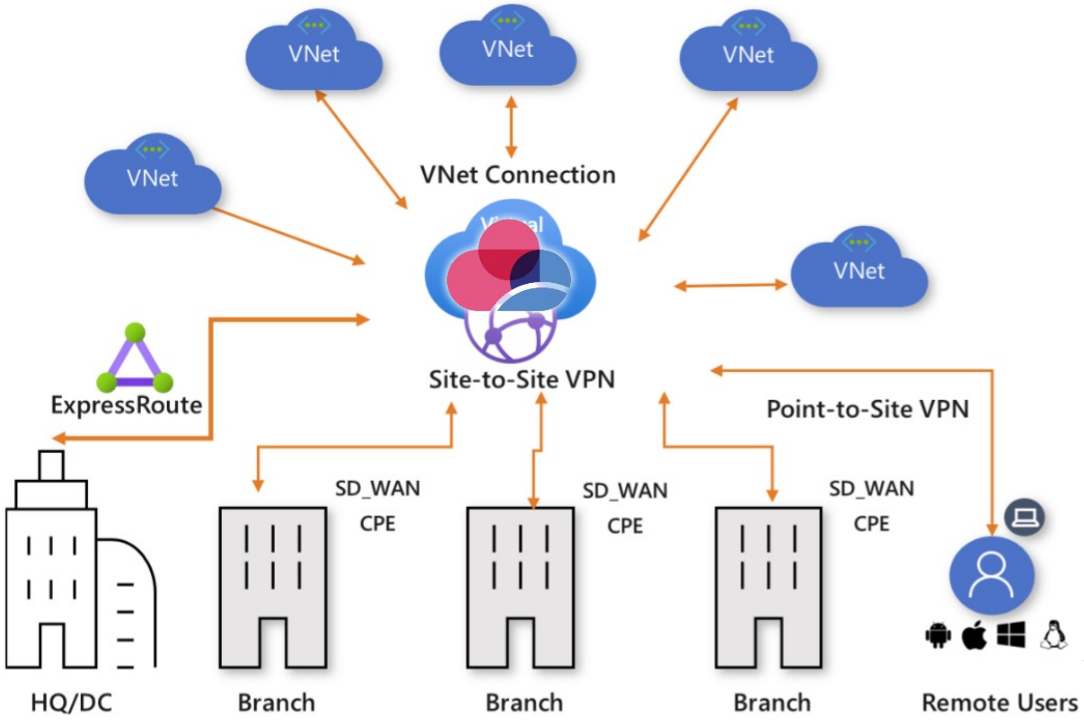
Azure vWAN Overview

- Hub and Spoke architecture
  The Hub managed and hosted by Azure as a service.
- Connectivity to workloads distributed globally in virtual networks:
  - Working at home and mobile users using point-to-site VPN
  - Main campuses and data centers using ExpressRoute
  - Branch offices using site-to-site VPN



Azure vWAN integration

- CloudGuard Gateway integrates into vWAN hub to inspect any-to-any traffic
- The CloudGuard Gateway is deployed into an Azure managed subscription in a high availability mode



Benefits

- Ability to inspect traffic inside Azure vWAN
- Simplified and managed deployment
- No lifecycle management
- Built-in HA
- No routing configuration
- Streamlined joint support

Use Cases

Single Virtual Hub

1. East-West Branch to Branch
   East-West VNet to VNet

2. North-South Branch to VNET
   North-South VNET to Branch

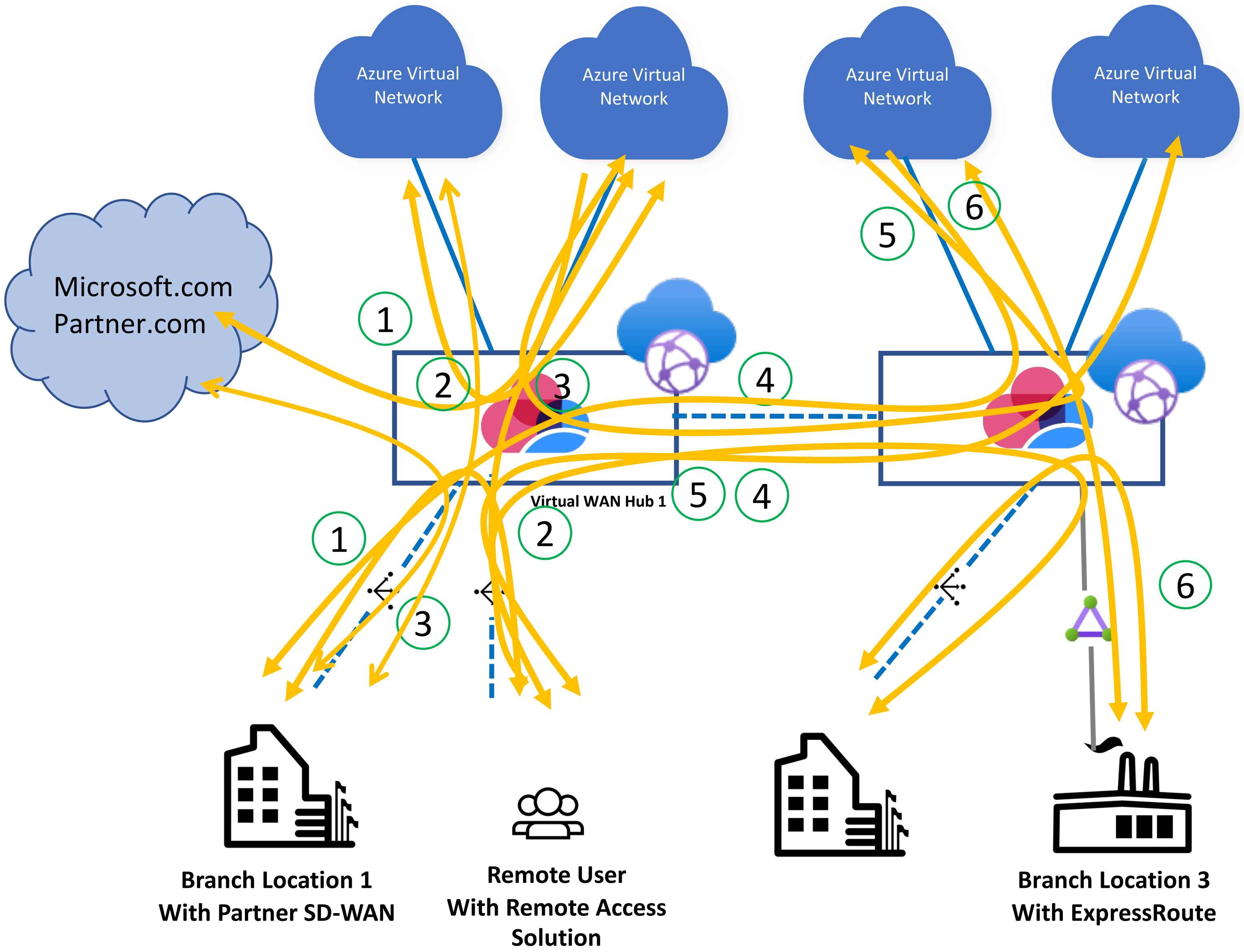
3. North-South Branch to Internet
   North-South VNet to Internet

Inter-hub and Hybrid Scenarios

4. East-West Branch to Branch
   East-West VNet to VNet

5. North-South Branch to VNET
   North-South VNET to Branch

6. Azure ExpressRoute to VNET
   Azure ExpressRoute to SD-WAN



QUESTIONS?

Check Point CHECKMATES

THANK YOU

Valeri (VAL) Loukine

Cyber Security Evangelist | Community Lead

CheckMates Live Virtual Series 2022

Check Point CHECKMATES