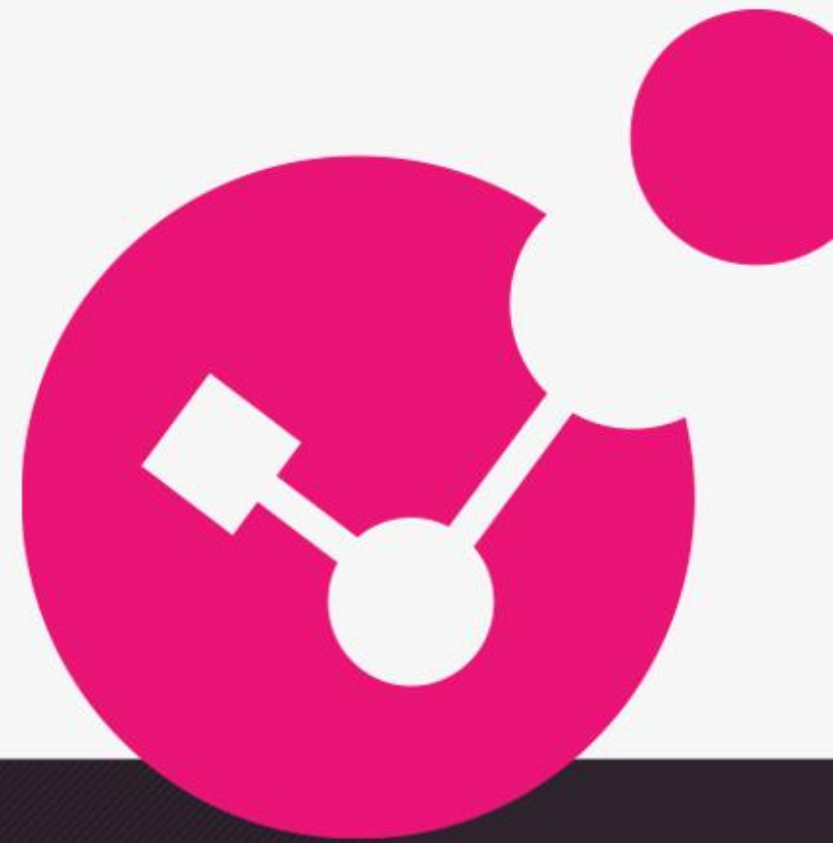




Harmony SASE roadmap

Product Management

Q1 2025



YOU DESERVE THE BEST SECURITY

New released features – past year or so

- **EU data residency**
- **Enhanced Networking**
 - Additional availability zones: NYC, London
 - Redundant tunnels with single IP
 - Hybrid SASE by default – smart split tunnel
 - HTTP-base detection of trusted networks
- **Enhanced Protections**
 - Integrated Check Point URL Filtering
 - Wildcards in URL filtering
 - Malware protection for Linux
- **Agentless RDP enhancements**
 - Native RDP
 - Dynamic RDP - per user
- **Harmony Browse integration**
- **MSP support in Infinity Portal**
- **Infinity Copilot integration**
- **FQDN-based split tunnel for Linux**

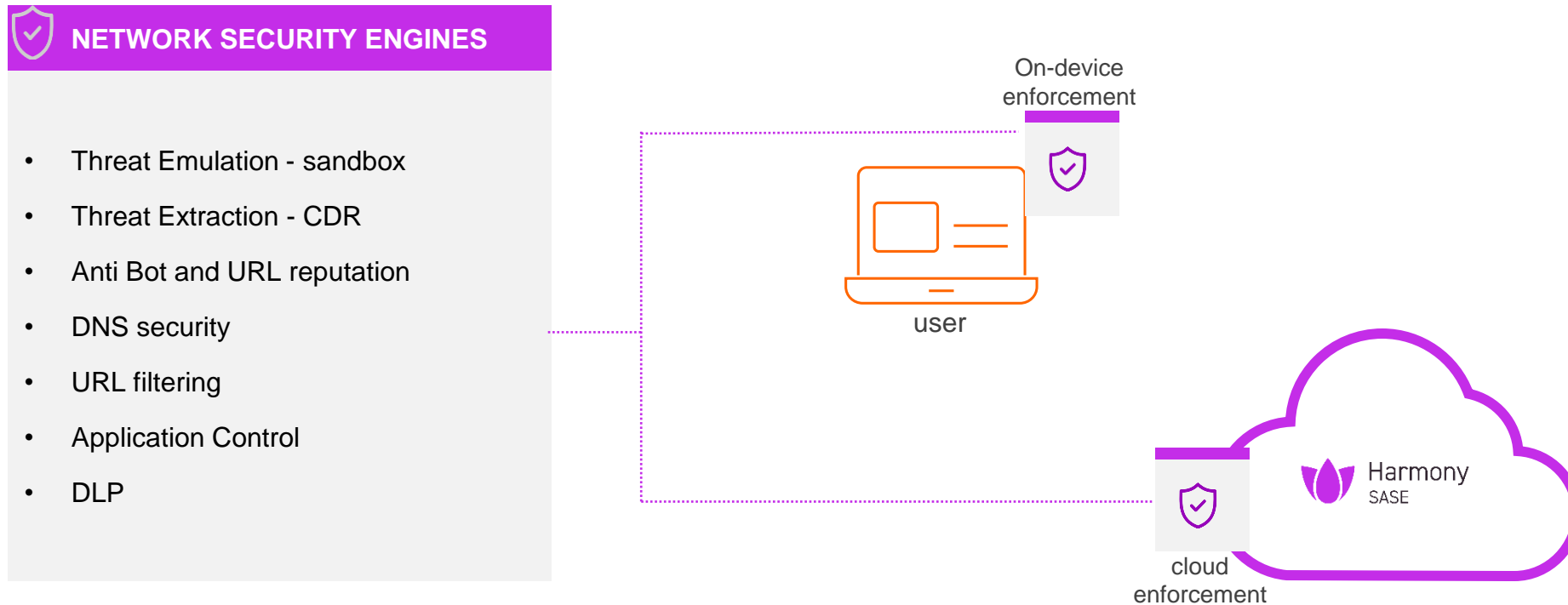
Harmony SASE roadmap – as of Feb 2025

This roadmap reflects Check Point feature release plan for Harmony SASE, as of February 2025.

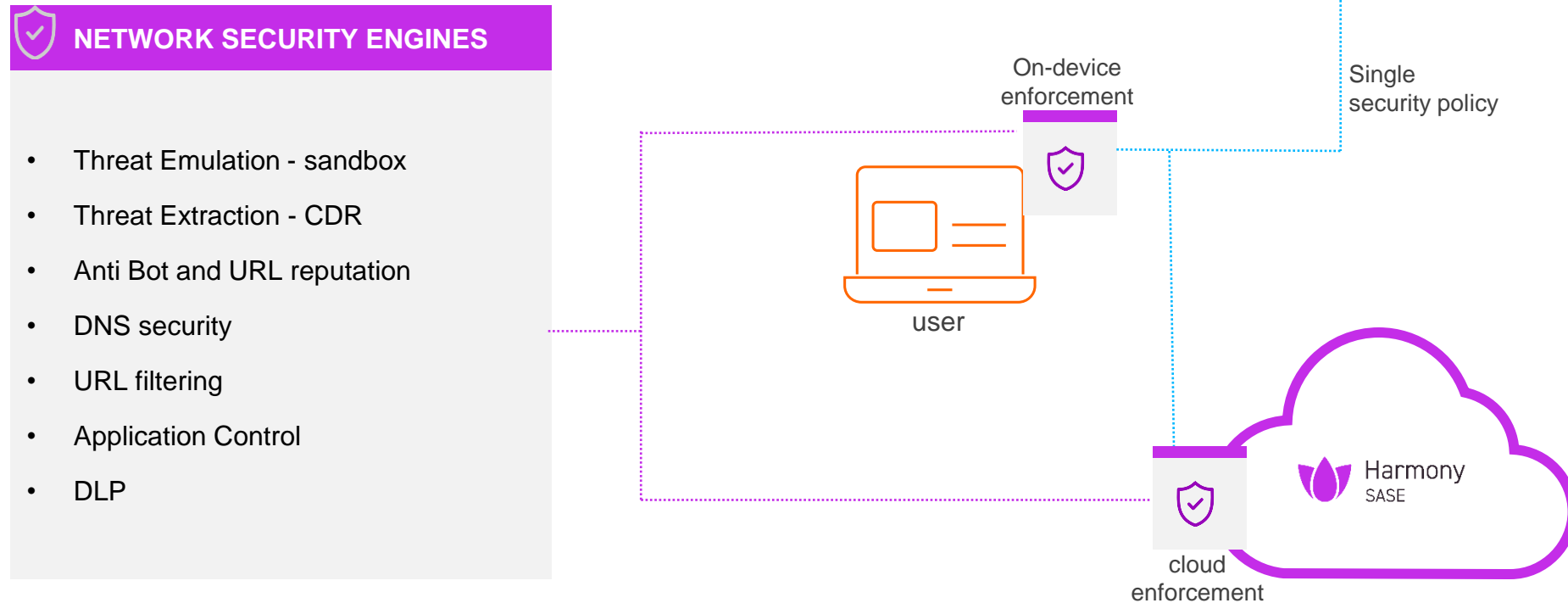
The timelines and content may change and should **not** be considered as a commitment.

	Q1-2025	Q2-2025	Q3-2025	Q4-2025
Network Security	On-device protection: <ul style="list-style-type: none"> Threat Emulation Anti-bot Application Control 	In-cloud – site protection: <ul style="list-style-type: none"> URL Filtering Malware Protection Anti Bot 	<ul style="list-style-type: none"> Threat Prevention exceptions management On-device protection: <ul style="list-style-type: none"> DLP Tenant restriction 	<ul style="list-style-type: none"> Granular threat prevention policy
Browser Security	<ul style="list-style-type: none"> GenAI “Ask” action GenAI protection for MacOS 	<ul style="list-style-type: none"> Secure Browser for BYOD access 		<ul style="list-style-type: none"> Browser extension integrated with SASE agent and management GenAI- reports
SaaS out-of-band Security, via API	<ul style="list-style-type: none"> SaaS security integrated in SASE management 	<ul style="list-style-type: none"> Data oversharing protection Enhanced SSPM for MS365 	<ul style="list-style-type: none"> DLP via SaaS APIs 	<ul style="list-style-type: none"> Data security dashboard and enhancements
Networking, Connectivity & Scale		<ul style="list-style-type: none"> Single IP per region 	<ul style="list-style-type: none"> Split tunneling for dynamic services - using updateable objects 	<ul style="list-style-type: none"> Bandwidth enforcement 60K users per tenant China premium connectivity
Cloud PoPs & Data Residencies	<ul style="list-style-type: none"> New PoPs: Belgium, Austria 	<ul style="list-style-type: none"> New PoPs: Switzerland, Taiwan New Residencies: Australia, India 	<ul style="list-style-type: none"> New PoP: Hong Kong 	<ul style="list-style-type: none"> New PoPs: China x 2, New Zealand, Quebec, Turkey
PC Agent & Mobile App	<ul style="list-style-type: none"> Unified mobile app with Harmony Mobile 	<ul style="list-style-type: none"> Improved anti-tampering Transparent install for IA 		<ul style="list-style-type: none"> Agent localization
Quantum & Smart-1 Integration			Phase 1: <ul style="list-style-type: none"> Unified IA policy Identity sharing Streamlined tunnel setup 	
Logging, Monitoring & Automation	<ul style="list-style-type: none"> Threat prevention logs in Infinity Events Playbooks integration, predefined playbooks 		<ul style="list-style-type: none"> Tunnel status monitoring 	<ul style="list-style-type: none"> All logs in Infinity Events

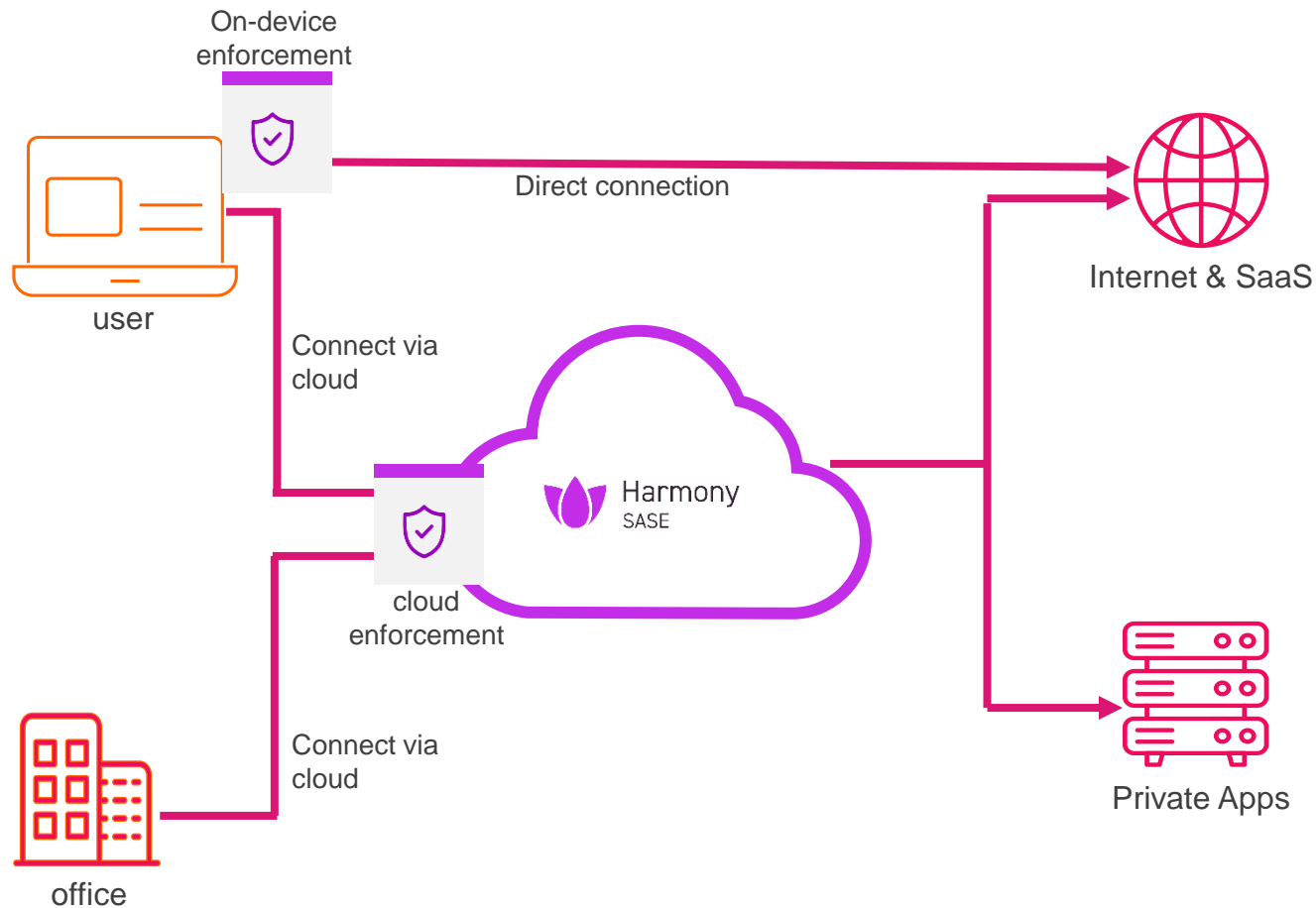
Incorporating Check Point's network security



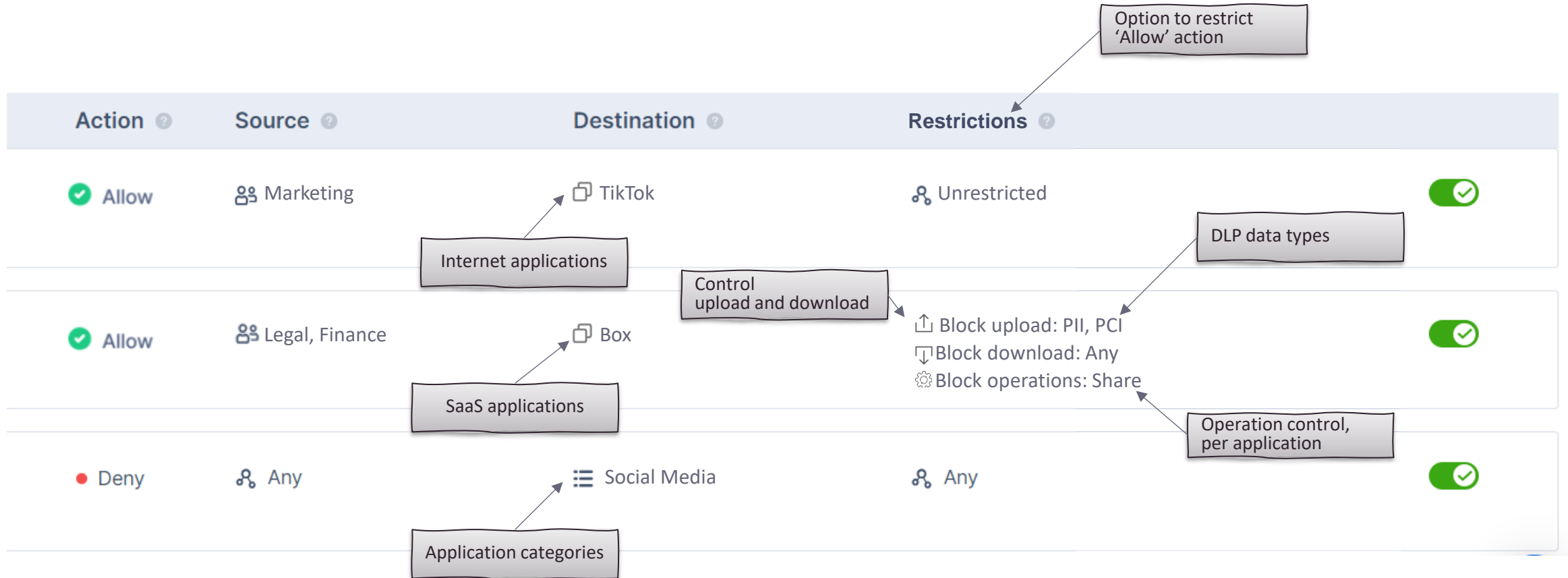
Incorporating Check Point's network security



Incorporating Check Point's network security



Internet Access - Unified Policy

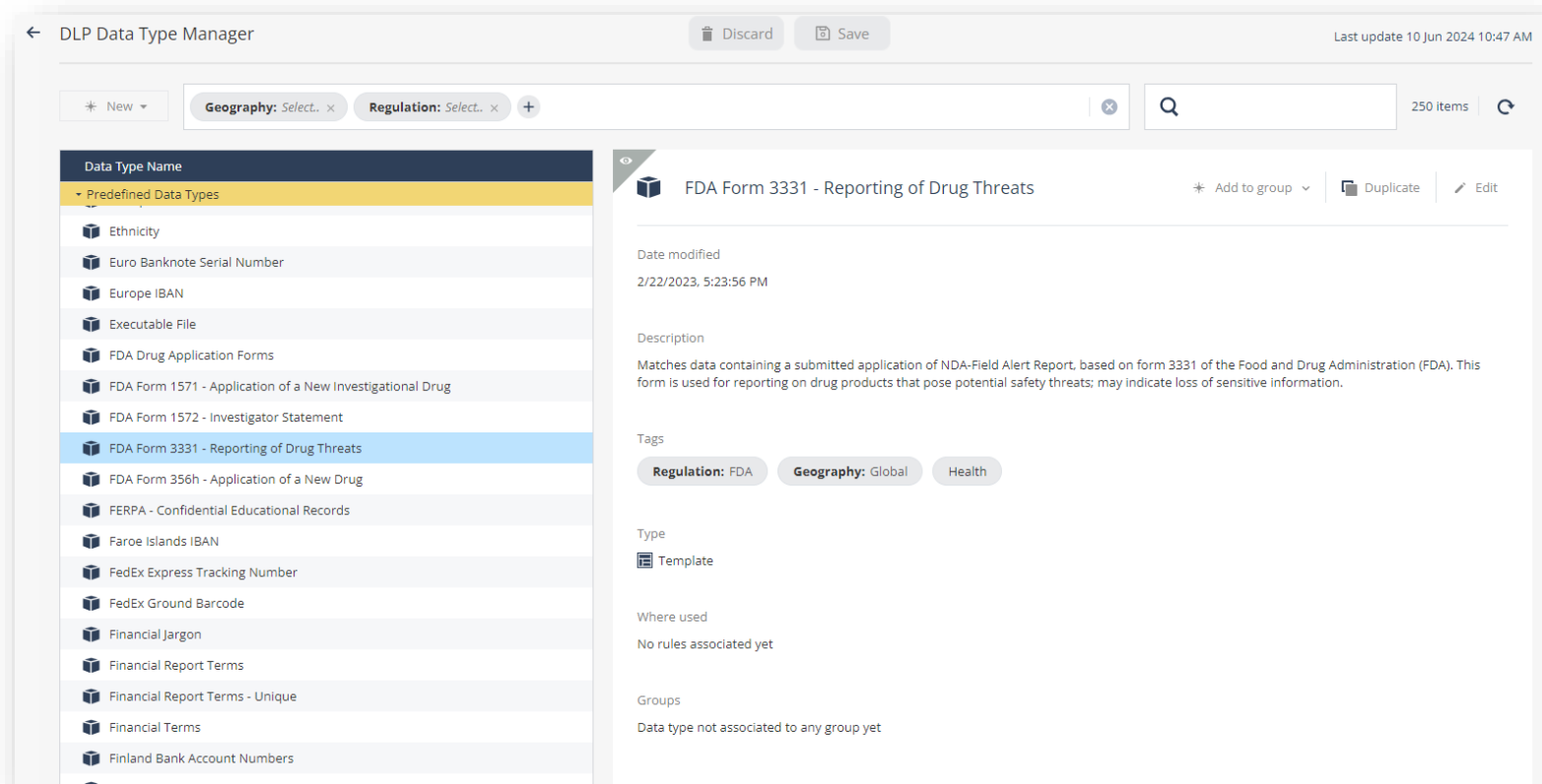


Unified policy for Internet Access and Inline CASB

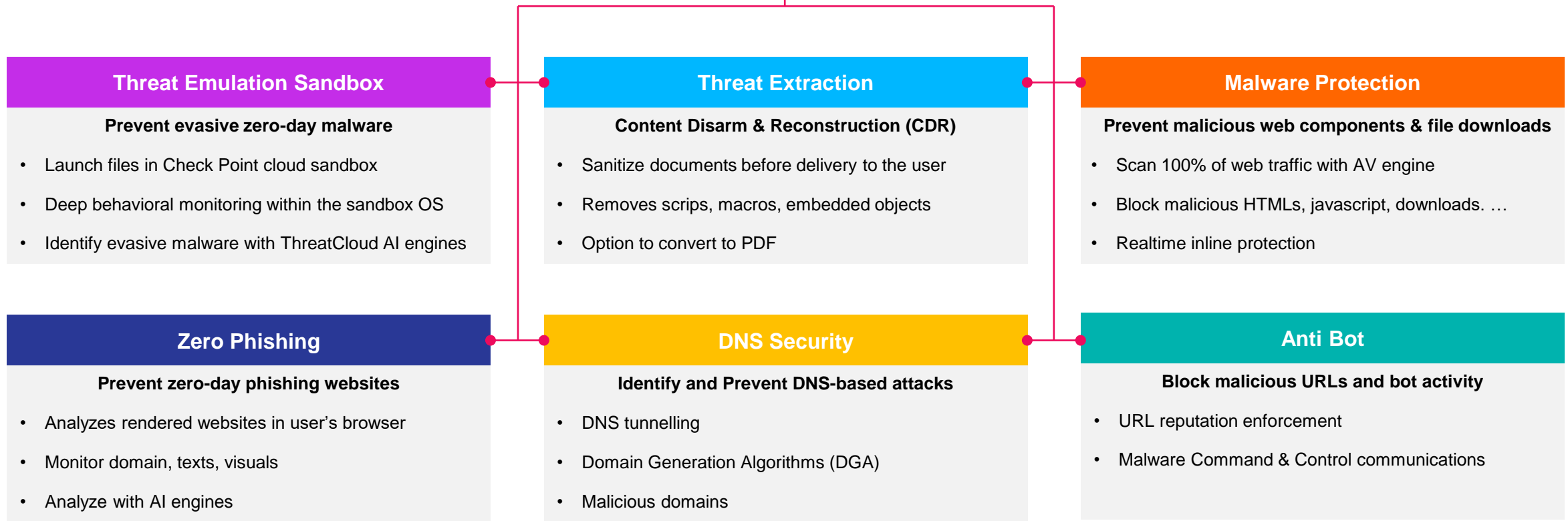
URL Filtering | Application Control | DLP

Integrating Check Point DLP

- Hundreds of predefined data-types
- Versatile data-types:
 - Tags from Microsoft Information Protection
 - Regex
 - Dictionary
 - OCR
 - File attributes
 - Template
 - AI (new)
- Custom data-types



Integrating Advanced Threat Prevention to SASE



Granular Threat Prevention policy

Harmony SASE perimeter 81

SomeName

Ingram Micro Inc. Partner

Overview

Dashboard

Products

Secure Access

Secure Internet

Threat Prevention

Policies

Profiles

Exceptions

Threat Prevention Profiles

Control how data flows between your network resources, members and groups. [Learn more](#)

Create Profile

Default Profiles

Profile Name

Protections

Action

Risk is a function of attack type and the profile configuration

Recommended By: System

Threat Emulation, Threat Extraction +2

Strict By: System

Zero Phishing, Anti-Bot, IPS

Custom Profiles

Profile Name

Practice Type

Test Profile By: Dima Kordun Date: Jan 28, 2024

Threat Emulation

Pre-configured profiles

New Section

Custom Profiles

Out of the box policy optimized for high efficacy and excellent user experience

Threat Prevention Policy

Control how data flows between your network resources, members and groups. [Learn more](#)

Add New Rule

Search by rule name

Add Filter

All Policies (5)

#	Name	Source	Destination	Profile	Enable Logs
1	All Users	Sales Team +4	54.172.60.0 +2	Optimized	<input checked="" type="checkbox"/>
2	Allow Redis	Any	Any	Strict	<input type="checkbox"/>
3	Data Center and US Protection	Internal Tel Aviv +2	192.168.141.0/24 +3	None	<input checked="" type="checkbox"/>
4	Recommended Protections	Design Team +2	External Contractors +8	Optimized	<input checked="" type="checkbox"/>
5	Access to CheckPoint	Checkpoint-II +2	internal.perimeter81... +2	Strict	<input type="checkbox"/>

Collaborative Security - ThreatCloud AI

AI is all about your data

THREATCLOUD AI

- 50+ AI engines
- 40+ traditional algorithm engines
- Dozens of intelligence feeds

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

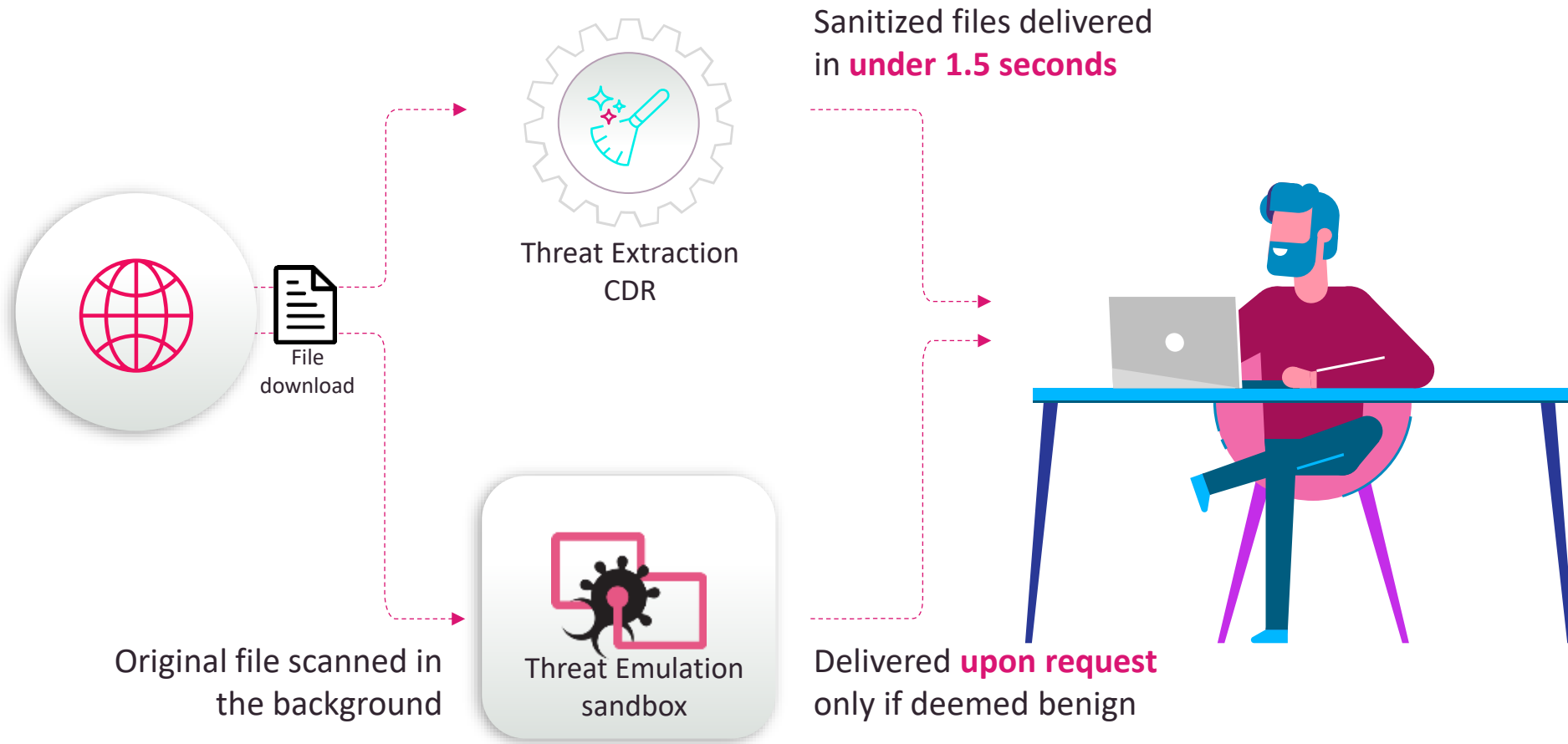
2,600,000
Malicious indicators

1,500,000
Newly installed mobile apps

1,200,000
Online web forms

Counted
DAILY!

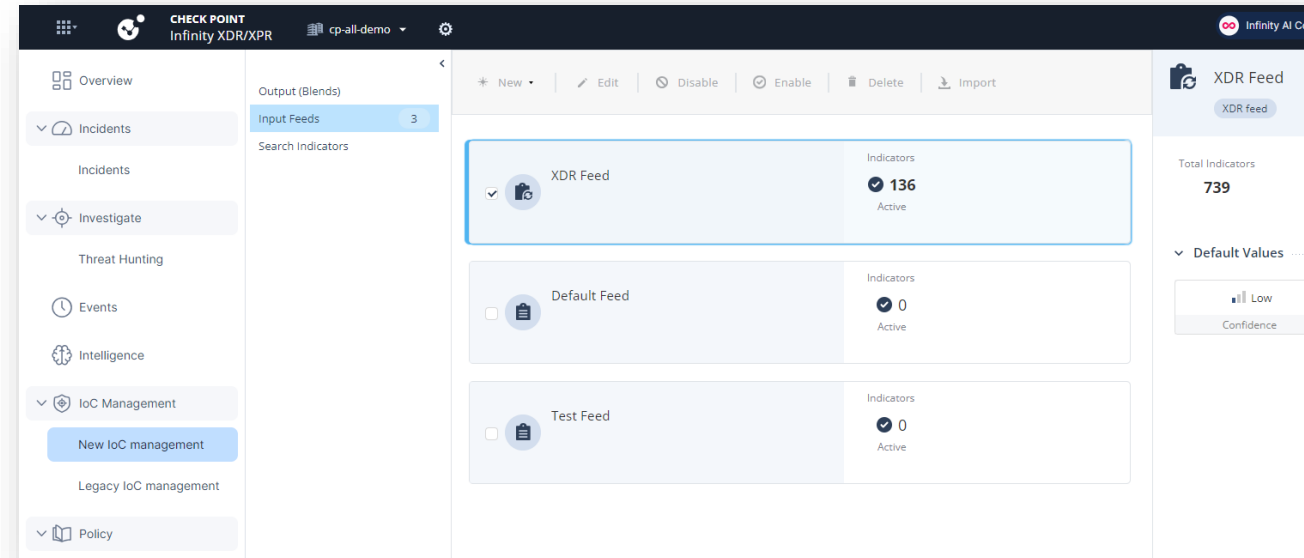
Zero-Day Prevention: Threat Extraction + Threat Emulation



Custom IoCs Enforcement

SASE Integration with Check Point XDR

- Customer's private threat intelligence enforced by SASE threat prevention
- Indicators of Compromise (IoCs) managed in Check Point XDR app
 - IOC types: IP addresses, File hashes, Domains, URLs
 - Incorporate private IOC feeds
 - Applied to all Check Point products, including SASE



Our Vision for Total Network Security

Integrating **Harmony SASE** with **Quantum Gateways**

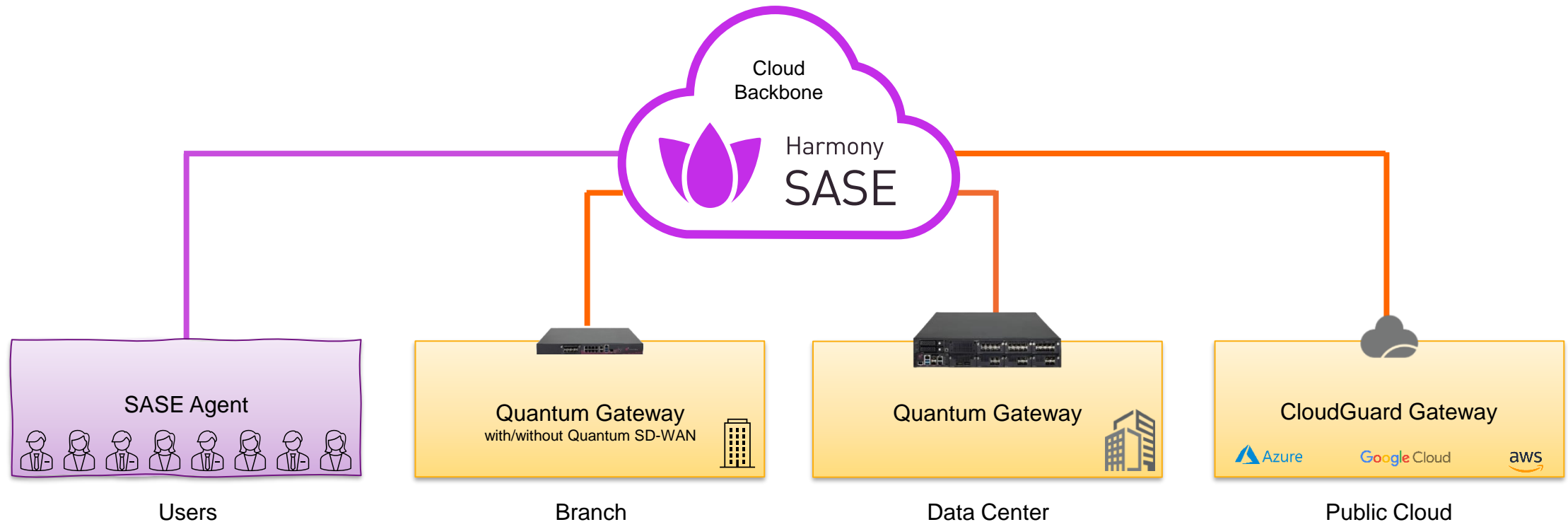


Simple
Set-Up

Unified
Policy

Shared
Identity

Optimized
Connectivity





THANK YOU

YOU DESERVE THE BEST SECURITY