CHECK POINT

Cloud, On-Prem, Chaos?

Hybrid Mesh bringt Ordnung in die Sicherheit

Dirk Berger, Check Point Software Technologies
Solutions Architect

17.09.2025, Congress Park Hanau

Distributed components

across

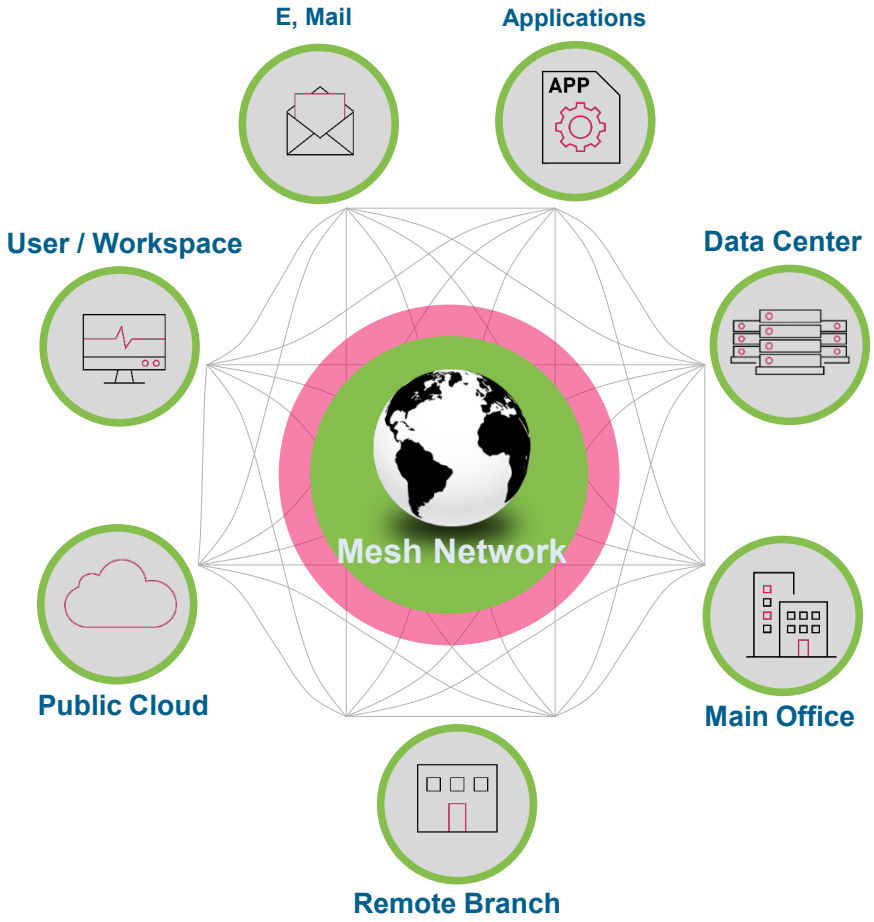
Multiple locations

where

Everyone must talk to Everyone

Everything is

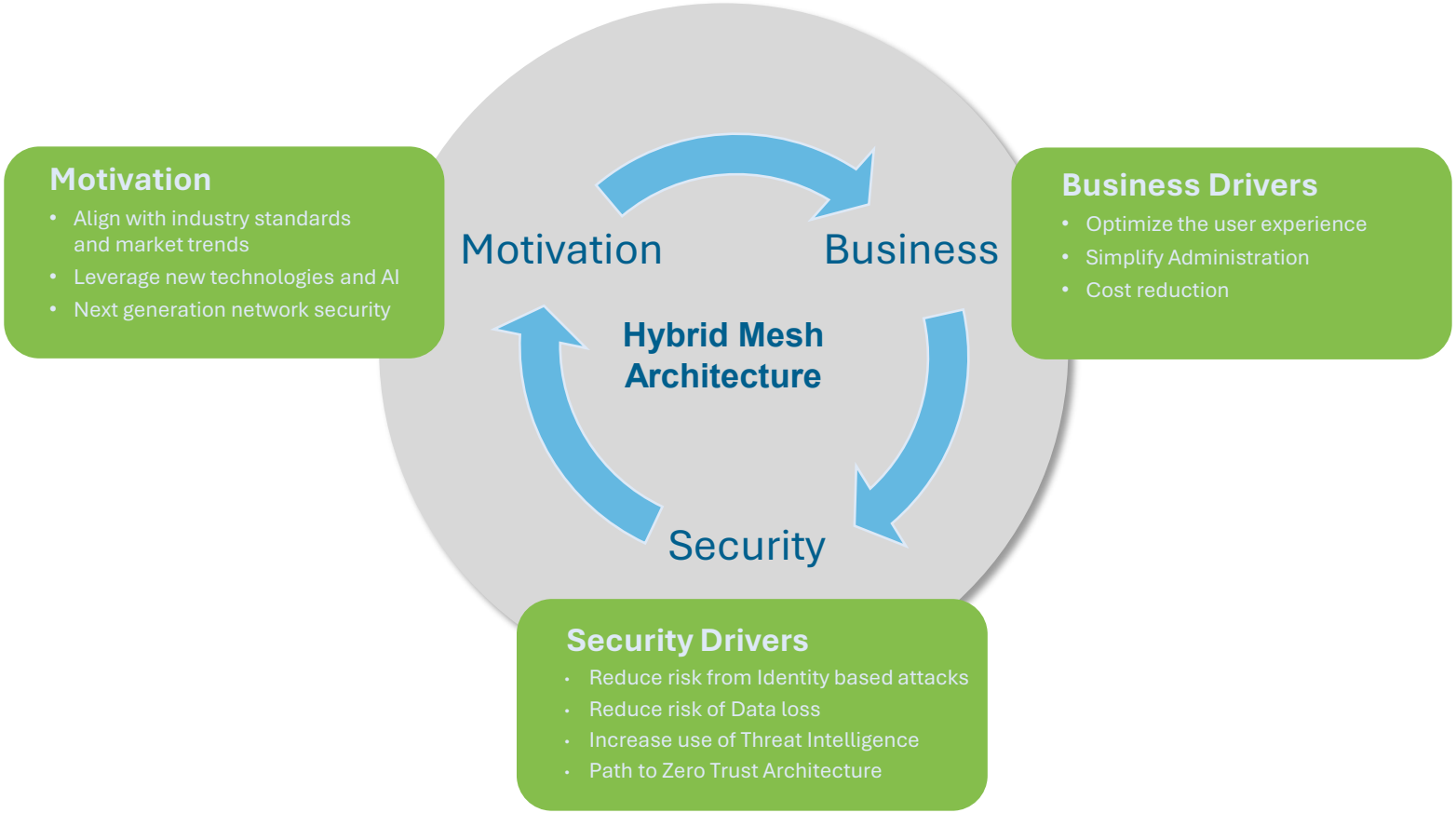
Fast, Dynamic & Interconnected



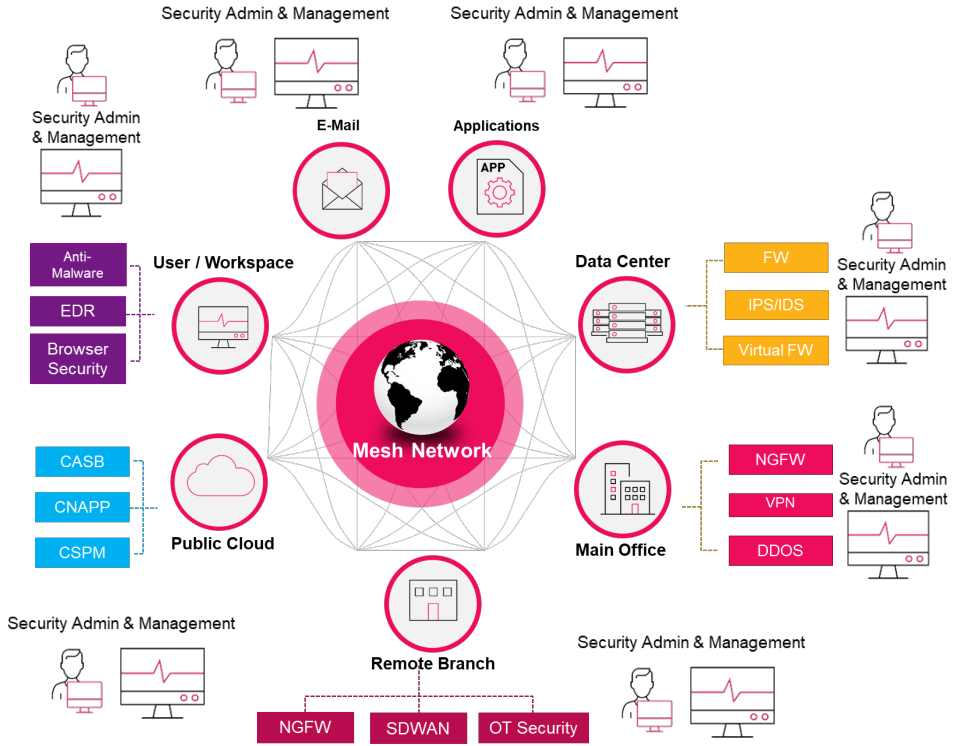
Challenge: How to …?

How to design secure hybrid environments, leverage best practices, select proper technologies and solutions?

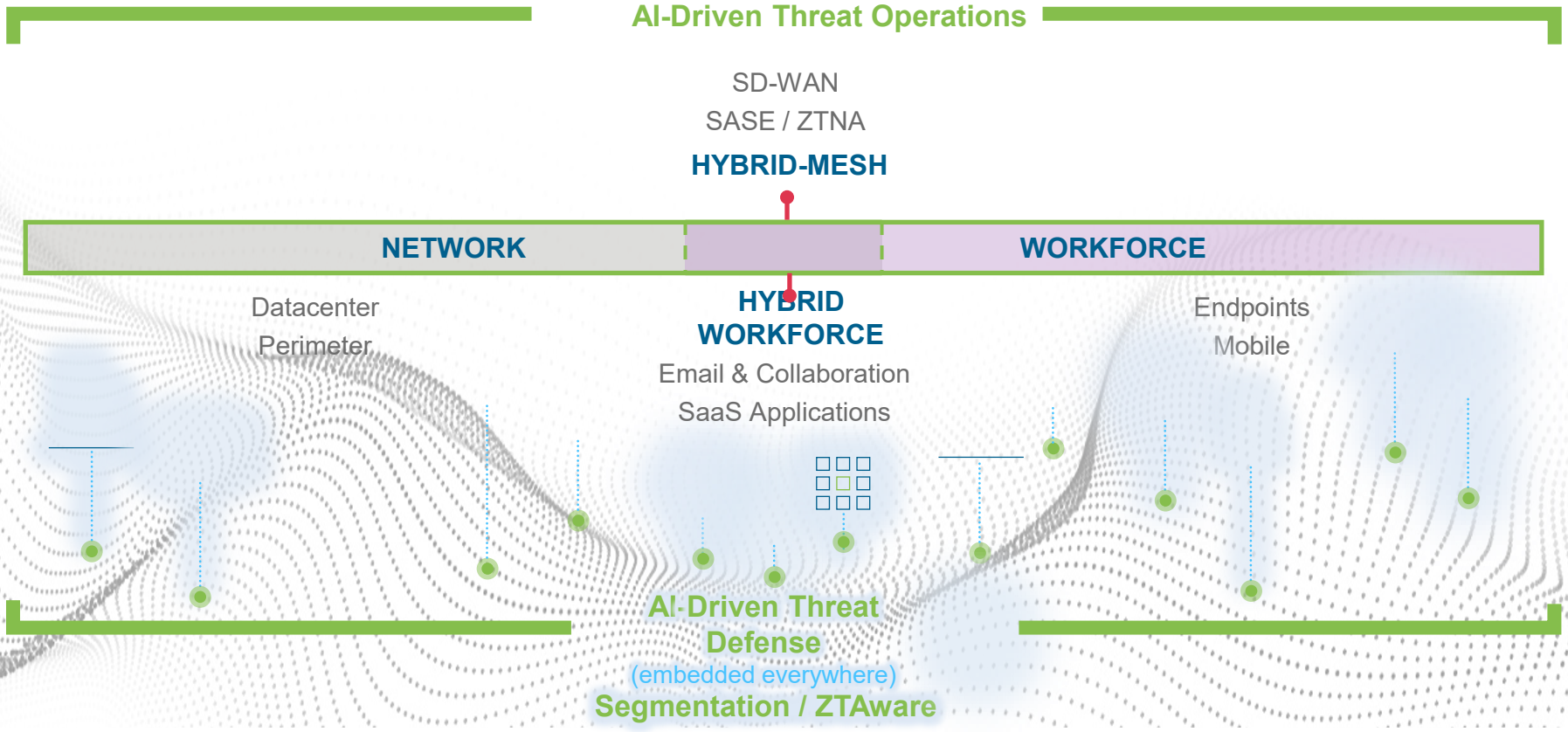
The Road to Hybrid Mesh Architecture



- Fragmented networks often have a higher cost
- Fragmented dashboards often lead to complex ops and prone to human error
- Lack of visibility across entire cyber security ecosystem
- Limited Threat Intelligence Sharing
- AI and innovation challenges due to lack of integration
- Higher MTTD and MTTR



Abstract of Challenge and Solution



Organisational Challenges

Multiple Vendors

High TCO
Creates Gaps

Training

Multiple technologies
Longer resolution
Adds risk

Security

Less threat sharing
Gaps in security
Easier for attackers

Problem Solving

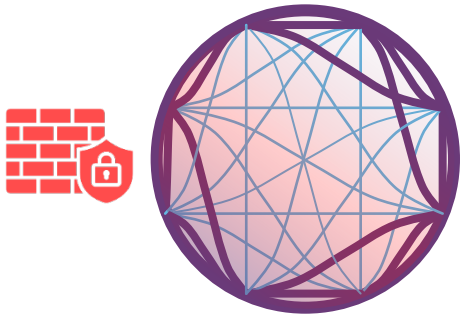
Multiple contact points
Longer resolution

Legal

Varying T&Cs
No consistency
Costs more – time/money

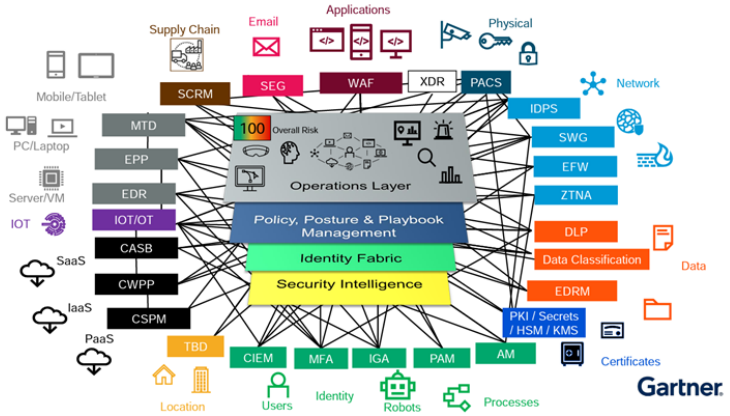
What Gartner says

HMF (Hybrid Mesh Firewall)



A hybrid mesh firewall (HMF) platform is a multi, deployment firewall including hardware and virtual appliance, cloud, based, and as, a, service models with a unified cloud, based management plane.

CSMA (Cyber Mesh)



Mitigate the risks of vendor lock, in and over consolidation by using cyber security mesh architecture as a guide to optimize the mix of platforms and point solutions.

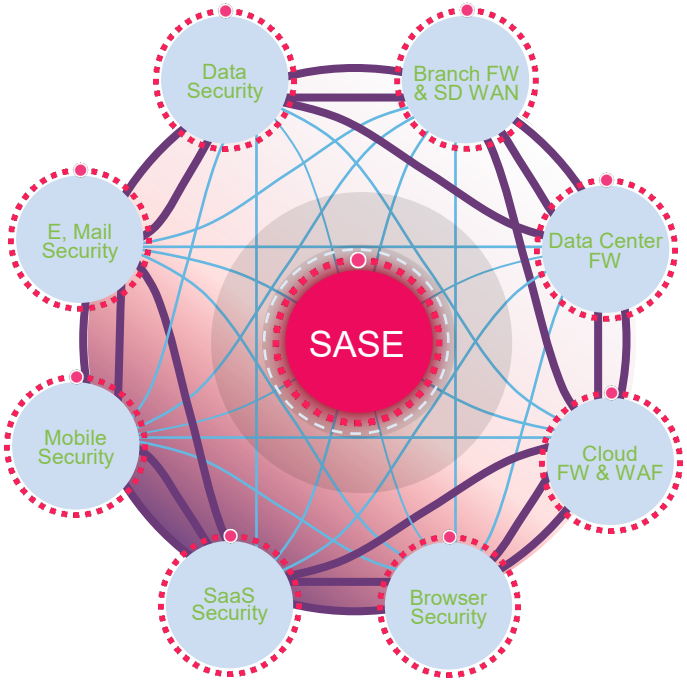
Gartner

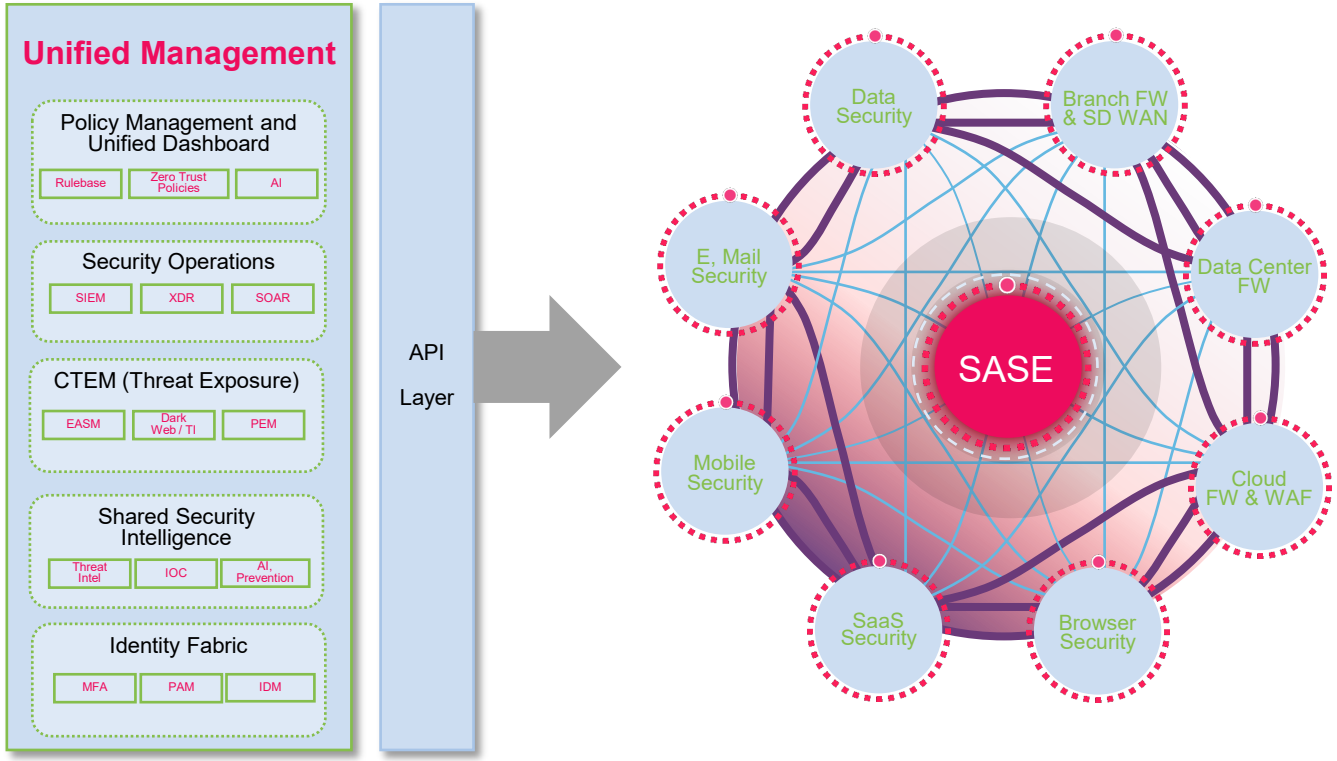
Consistent Security

With Optimized Connectivity
Everywhere

Providing
Business Agility

Under One
Unified and Collaborative Security Architecture





Control access and threat prevention across all enforcement solutions

Unified Management

Policy Management and Unified Dashboard
- Rulebase
- Zero Trust Policies
- AI

Security Operations
- SIEM
- XDR
- SOAR

CTEM (Threat Exposure)
- EASM
- Dark Web / TI
- PEM

Shared Security Intelligence and AI
- Threat Intel
- IOC
- AI-Prevention

Identity Fabric
- MFA
- PAM
- IDM

API Layer

Source & Identity		Policies: Access, Data	Policies: Threat Prevention	Destination	
User	Employee Developer / Admin Contractors Internet users	1. Firewall 2. SD-WAN 3. VPN 4. URL Filter 5. Application Control 6. DLP 7. APIs Security 8. User Identity 9. Cloud Identity 10. IoT Identity	1. IPS 2. Anti Phishing 3. Malware 4. Anti-Bot 5. DDoS 6. DNS Security 7. Anti-Virus 8. WAF 9. GenAI Prompt Security 10. Credential leak	Internet / LLMs	
Workload & AppS	VM / Container SaaS / PsaaS			Workload & AppS	VM / Container SaaS / PsaaS
Devices	PC / Mobile IoT / OT				
Environment	Office Datacenter Cloud			Environment	Office Datacenter Cloud

- Quantum — On-Premises Security
- CloudGuard — Cloud Security
- Harmony SASE — Workspace security
- aws — 3rd party FW

Visibility and Fast Response

Unified Management

Policy Management and Unified Dashboard
- Rulebase
- Zero Trust Policies
- AI

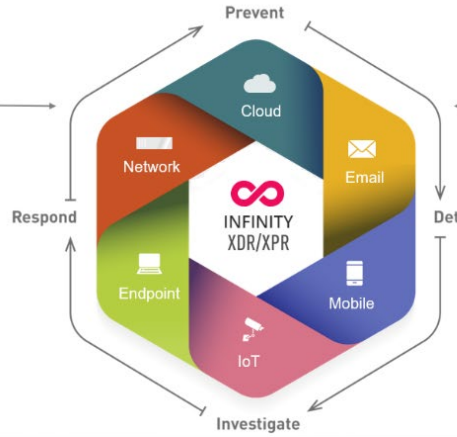
Security Operations
- SIEM
- XDR
- SOAR

CTEM (Threat Exposure)
- EASM
- Dark Web / TI
- PEM

Shared Security Intelligence and AI
- Threat Intel
- IOC
- AI-Prevention

Identity Fabric
- MFA
- PAM
- IDM

API Layer



QUANTUM
Secure the Network

CLOUDGUARD
Secure the Cloud

HARMONY
Secure the Workspace

Open Garden

Microsoft Entra ID
SentinelOne
CrowdStrike
cisco
Palo Alto Networks
TrendMicro
Google Cloud
Azure Active Directory
okta
Office 365
Jira
Microsoft Defender
Google Workspace
Dropbox
aws
Azure
FortiGate Firewall
slack
servicenow
Active Directory

Proactively Identify Threats and Validate Mitigation

Unified Management

Policy Management and Unified Dashboard
- Rulebase
- Zero Trust Policies
- AI

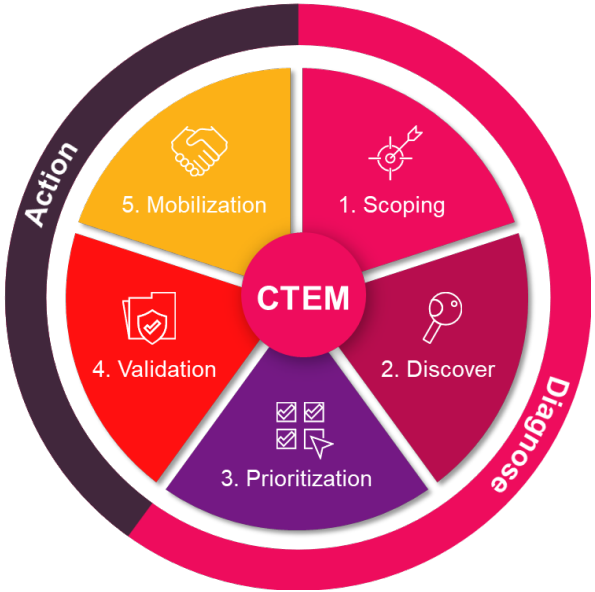
Security Operations
- SIEM
- XDR
- SOAR

CTEM (Threat Exposure)
- EASM
- Dark Web / TI
- PEM

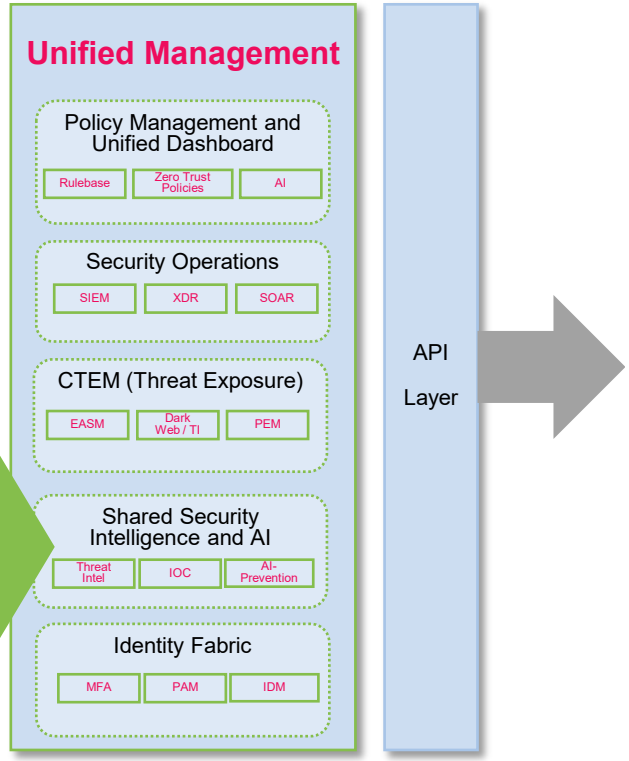
Shared Security Intelligence and AI
- Threat Intel
- IOC
- AI-Prevention

Identity Fabric
- MFA
- PAM
- IDM

API Layer



Ensure Threat Intel is being shared across relevant controls to enforce prevention

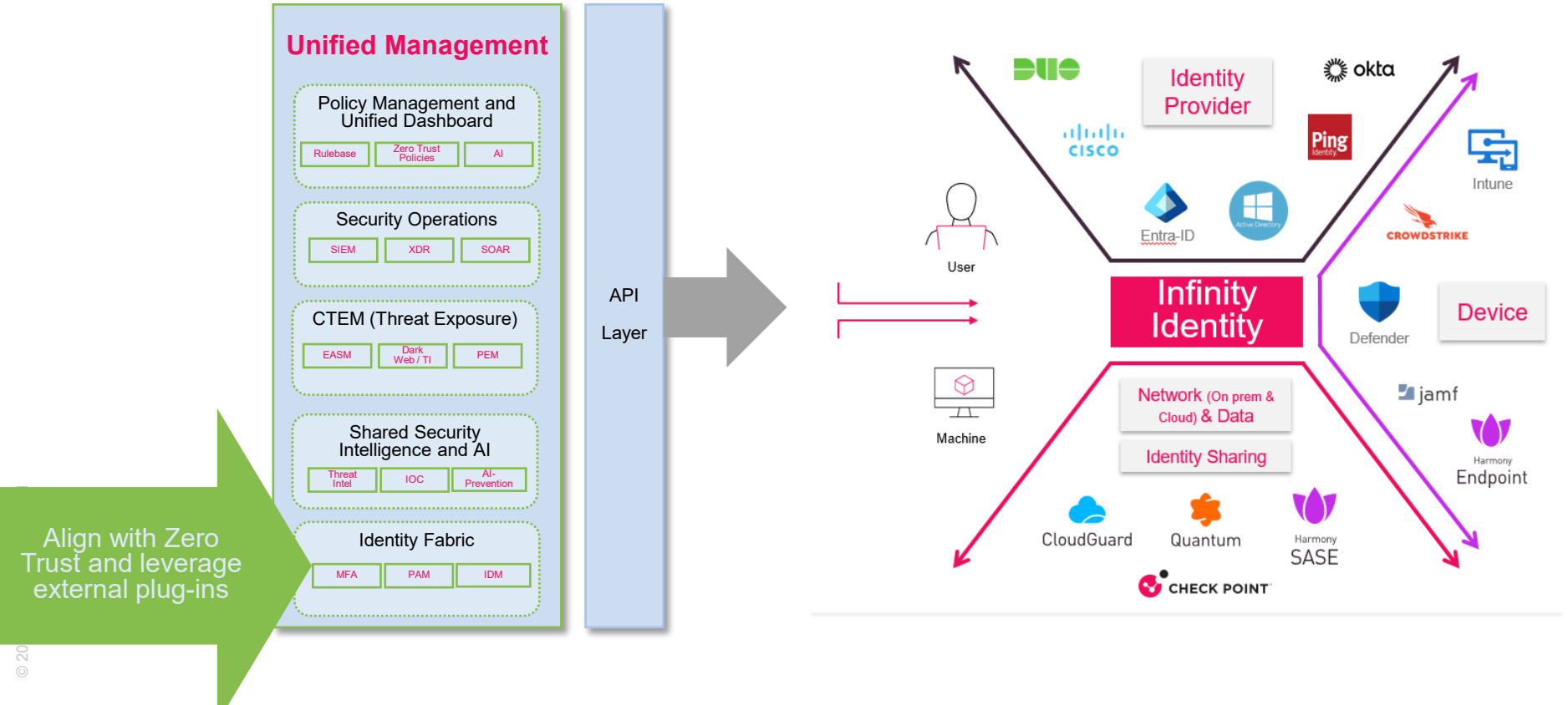


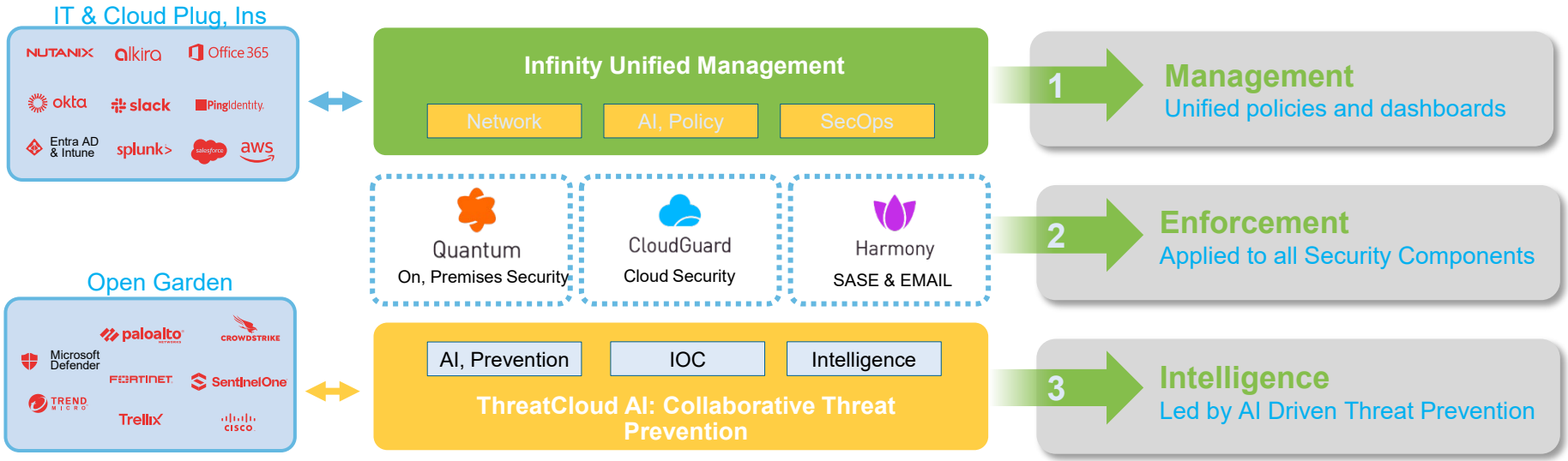
API Layer

AI Technology
55+ AI and GenAI Engines

THREATCLOUD AI

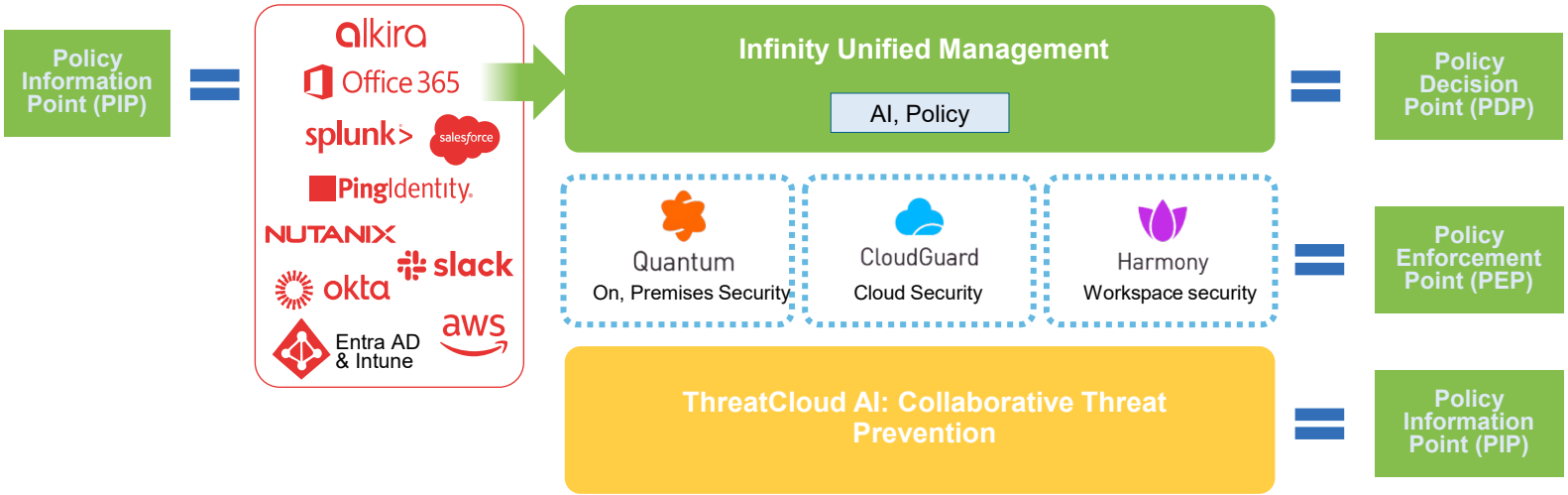
Big Data Threat Intelligence
~4 Billion Attacks Prevented


Unified Management
Policy Management and Unified Dashboard
Rulebase
Zero Trust Policies
AI
Security Operations
SIEM
XDR
SOAR
CTEM (Threat Exposure)
EASM
Dark Web / TI
PEM
Shared Security Intelligence and AI
Threat Intel
IOC
AI-Prevention
Identity Fabric
MFA
PAM
IDM
API Layer
Identity Provider
DUO
okta
cisco
Ping
Intune
Entra-ID
Active Directory
CROWDSTRIKE
User
Infinity Identity
Device
Defender
Machine
Network (On prem & Cloud) & Data
Identity Sharing
jamf
Harmony Endpoint
CloudGuard
Quantum
Harmony SASE
CHECK POINT
Align with Zero Trust and leverage external plug-ins



Value: Context, aware policies via ecosystem integrations

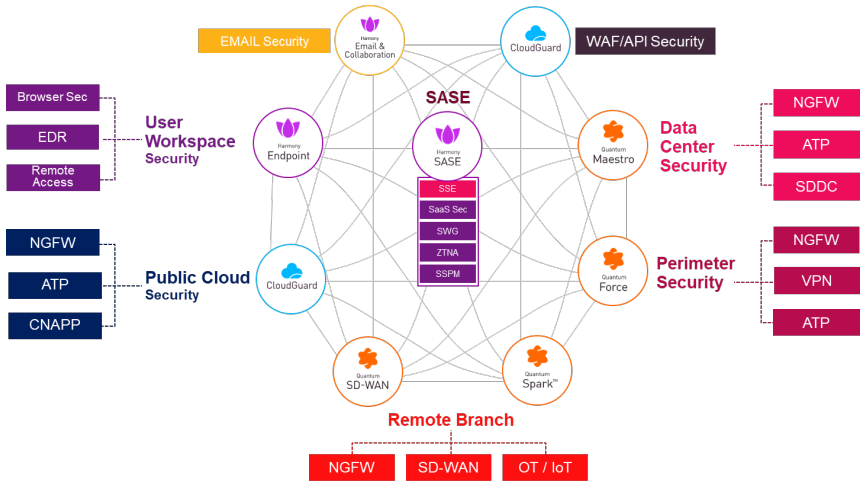
Description: External platforms serve as PIPs, feeding dynamic identity, device, and context data into Infinity's AI, Policy engine to enhance PDP decisions and PEP enforcement.



1. User access to the Internet and Corporate resources located in the Data Center and/or in the Public Cloud

2. Remote Branch connectivity to the Internet and DC / Public Cloud

3. Hybrid Cloud Data Center secured networking



USE CASE 1

USE CASE 2

USE CASE 3

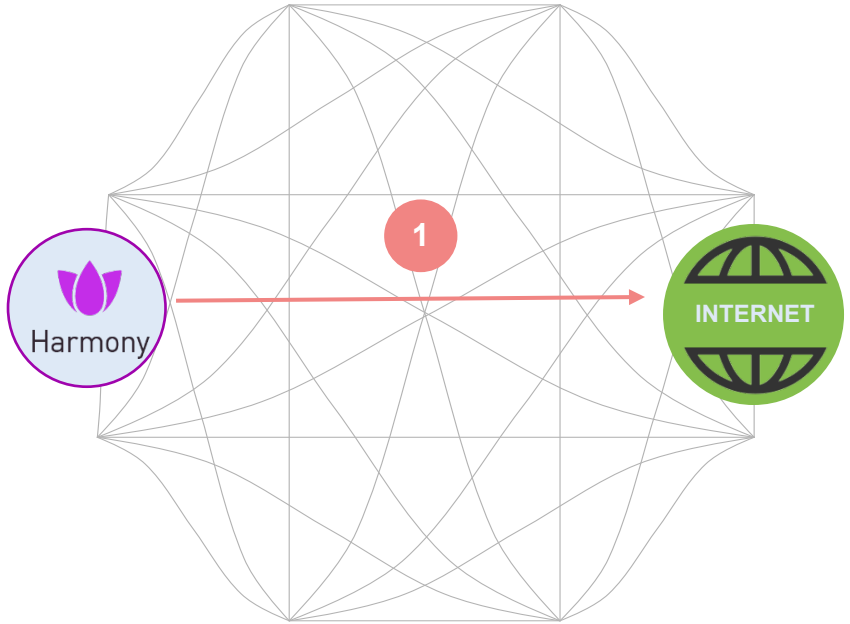
Harmony
SASE

Browser Sec

EDR

Remote Access

User Workspace Security

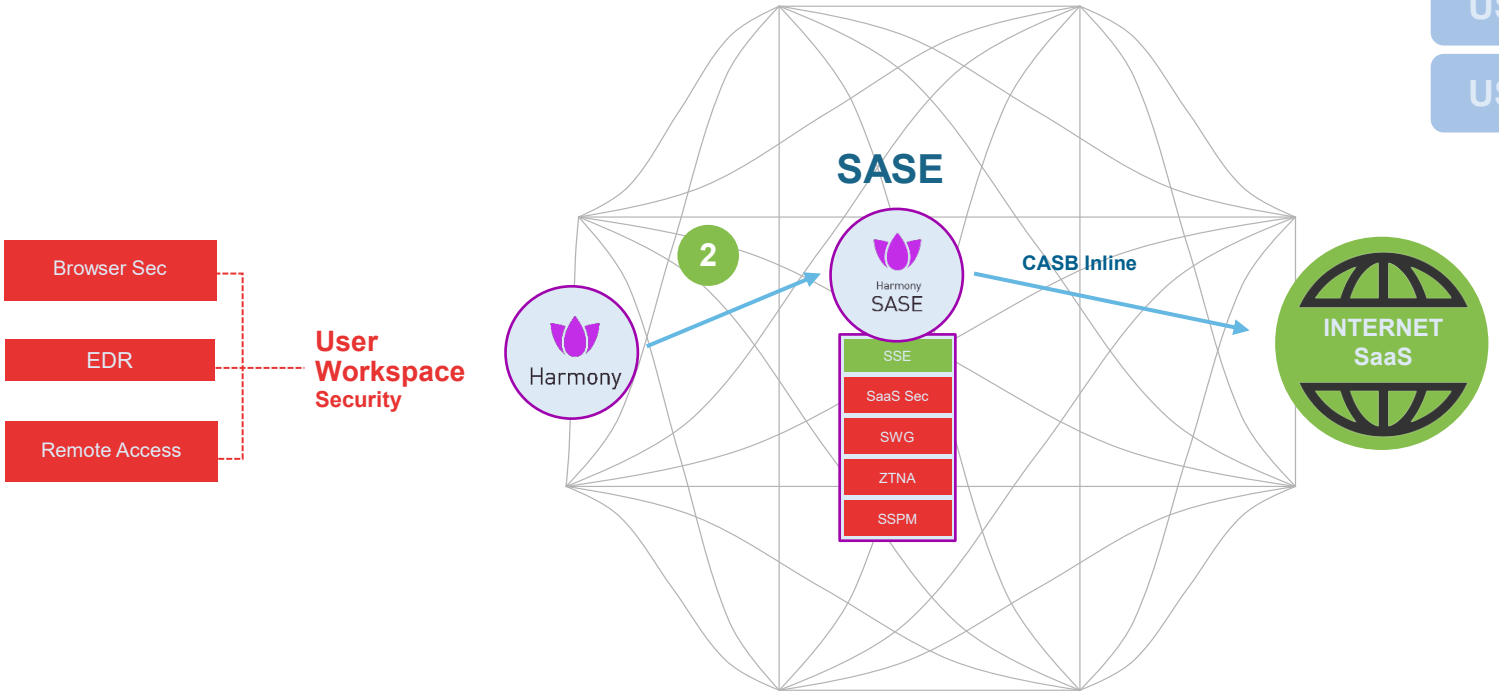


Direct Secure Web Access : Optimized performances for Seamless User Experience

USE CASE 1

USE CASE 2

USE CASE 3

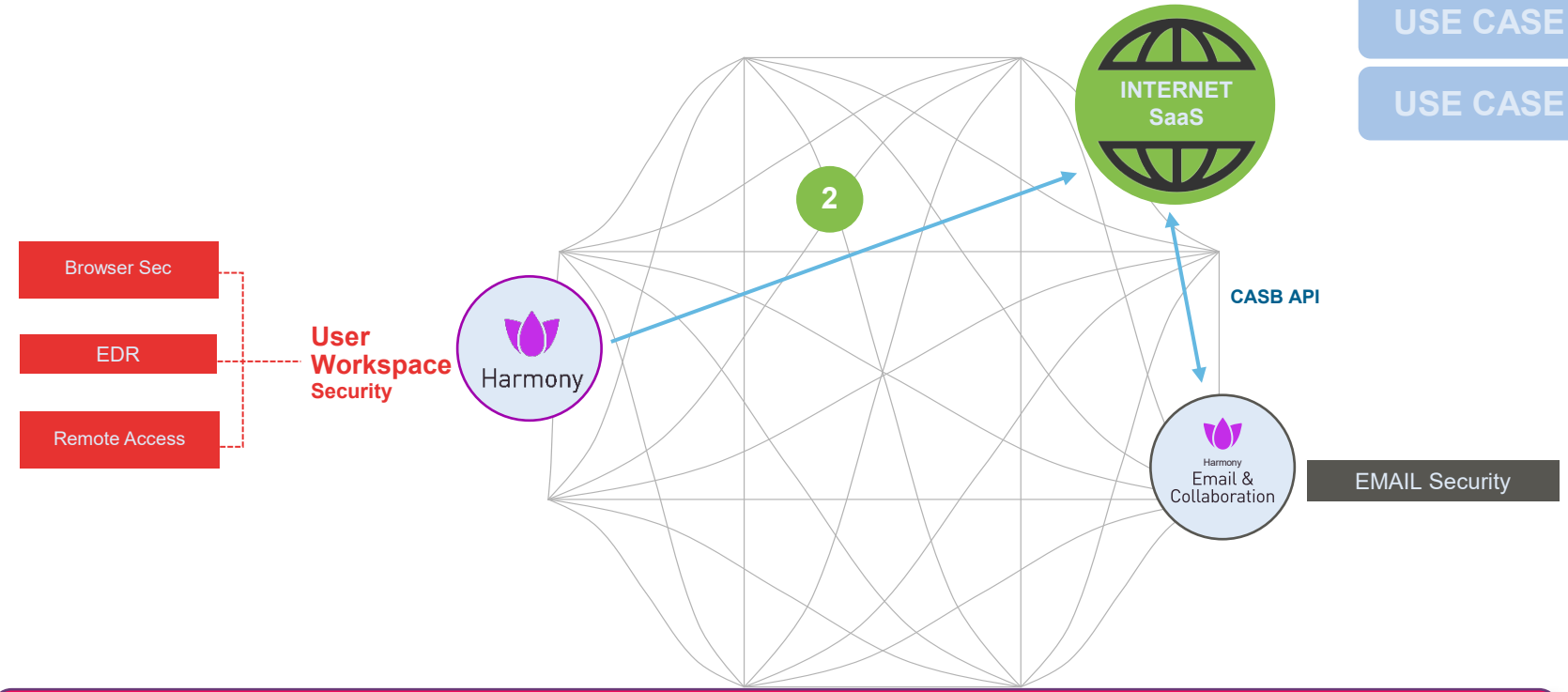


SASE providing Secure Access to SaaS Application

USE CASE 1

USE CASE 2

USE CASE 3

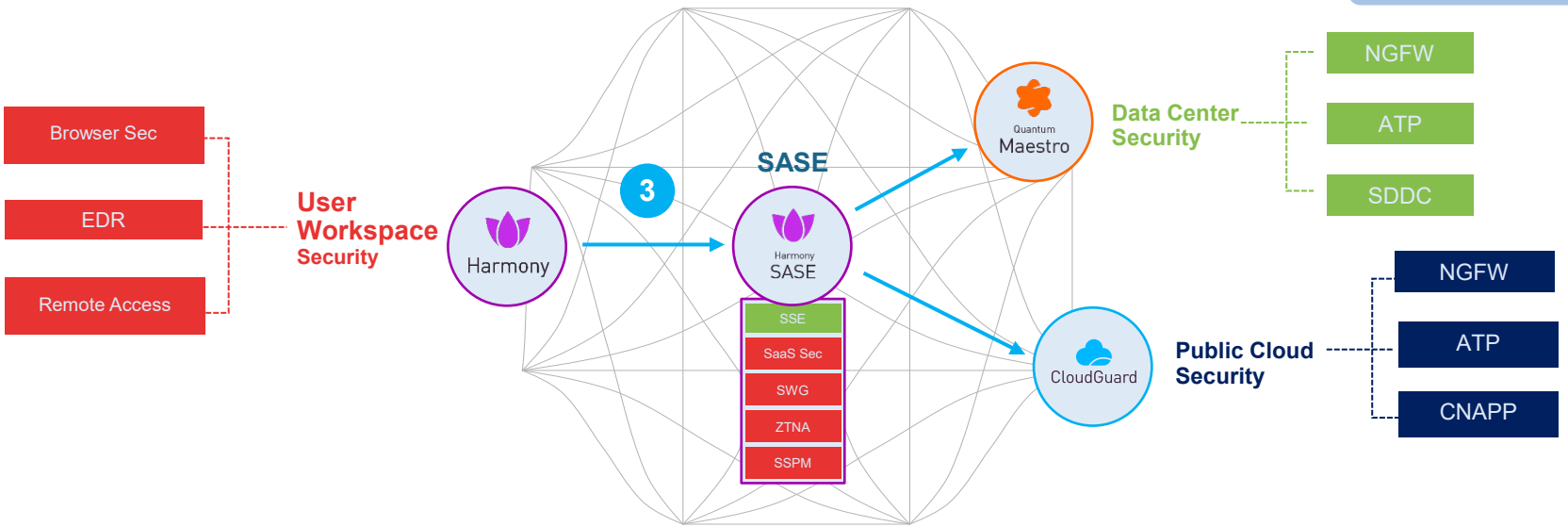


Optimized User experience with Advanced Security for emails

USE CASE 1

USE CASE 2

USE CASE 3

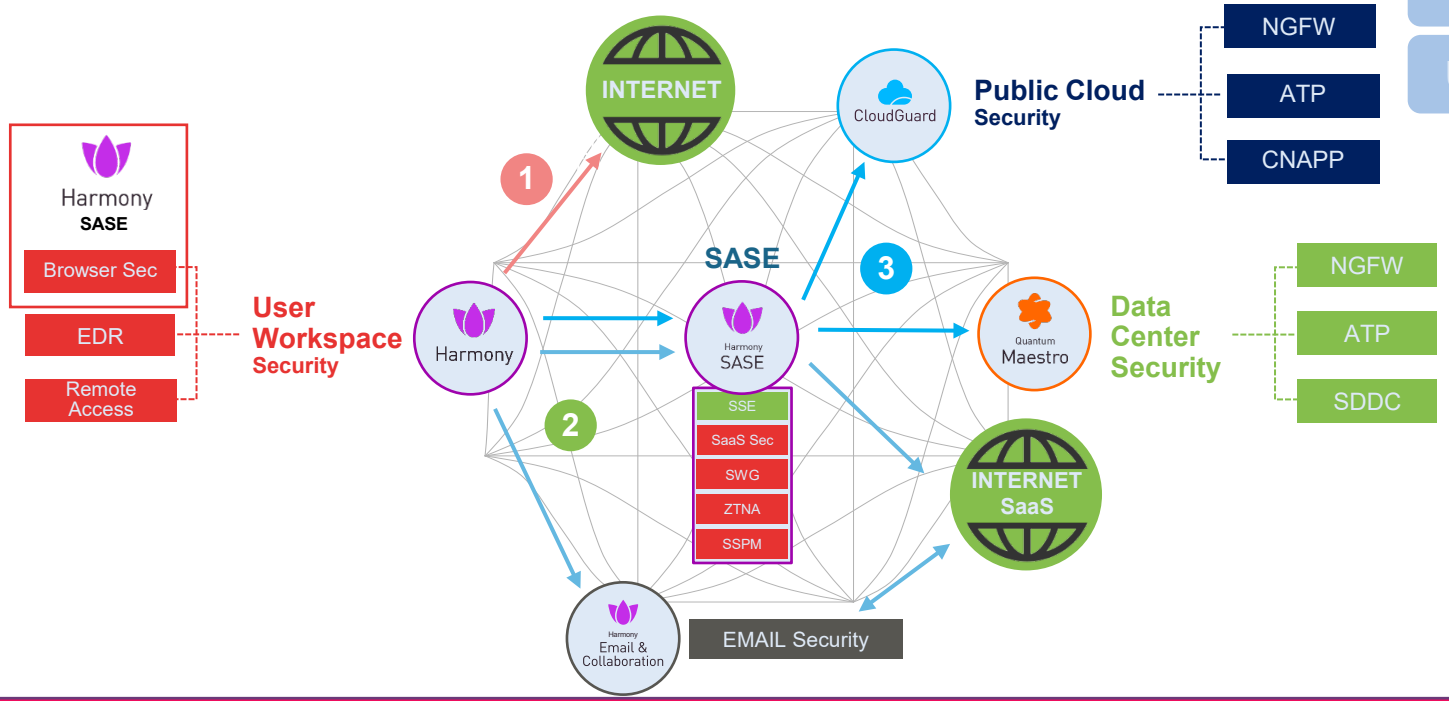


SASE providing seamless Secured Access to all sensitive Resources

USE CASE 1

USE CASE 2

USE CASE 3



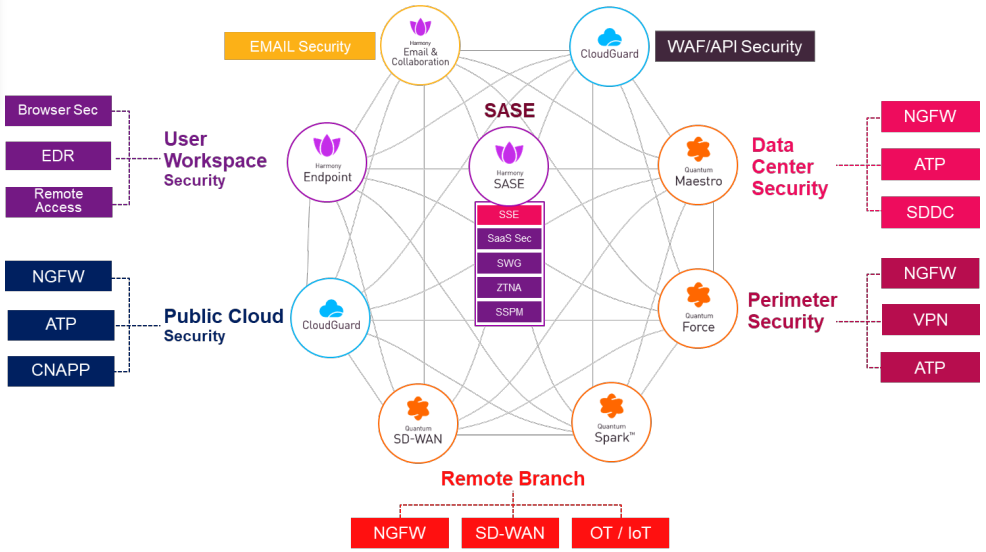
User benefit from seamless experience
While Zero Trust Principles are enforced with optimized Security Controls

USE CASE 1

USE CASE 2

USE CASE 3

2 Remote Branch connectivity to the Internet and DC / Public Cloud

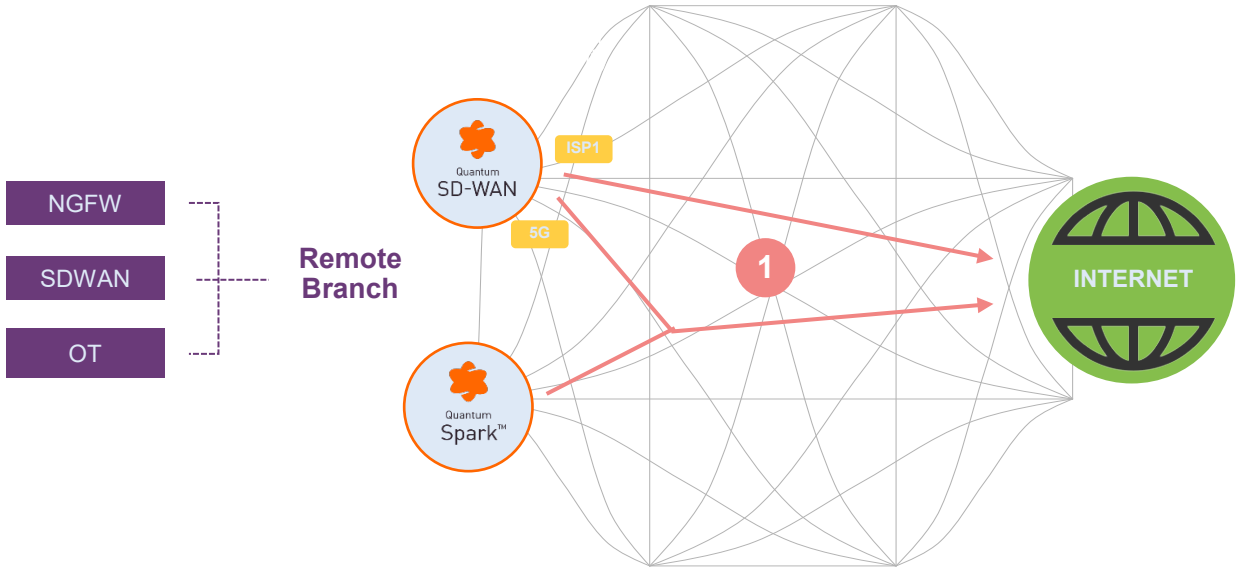


Branch to the Internet

USE CASE 1

USE CASE 2

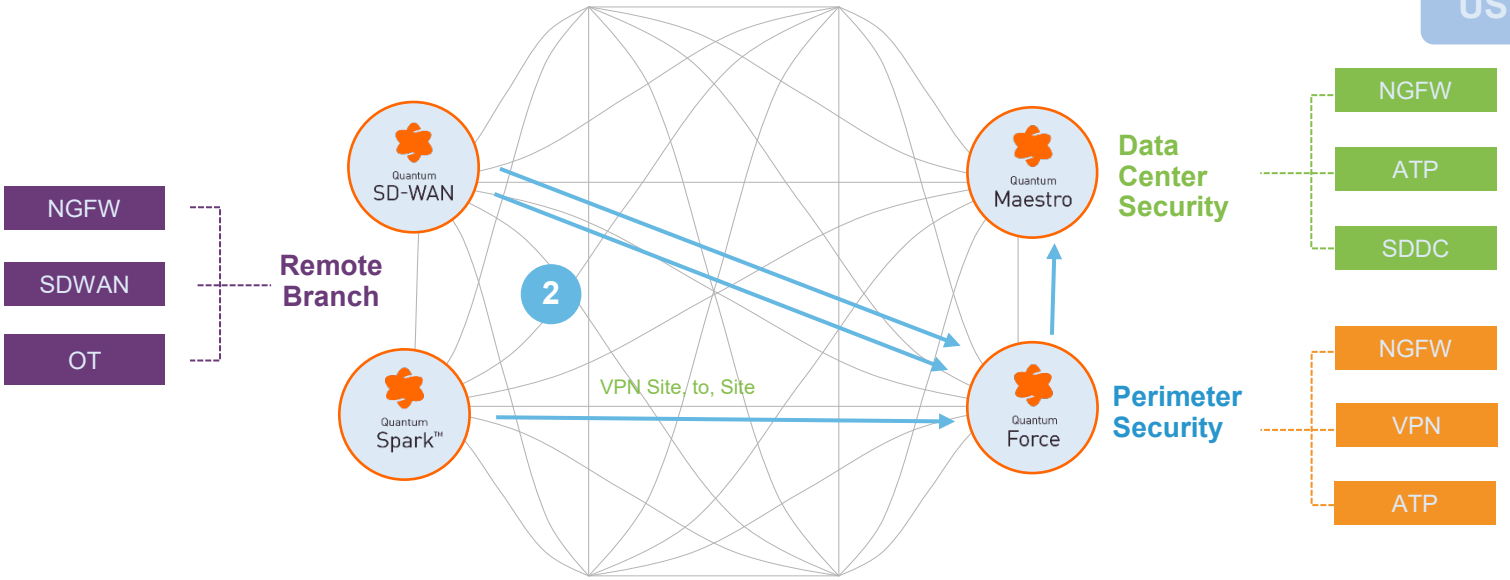
USE CASE 3



Resilience, flexibility & performances, no backhaul required
Secure direct connection with built, in NGFW capabilities

Branch to Internal Resources

USE CASE 1
USE CASE 2
USE CASE 3



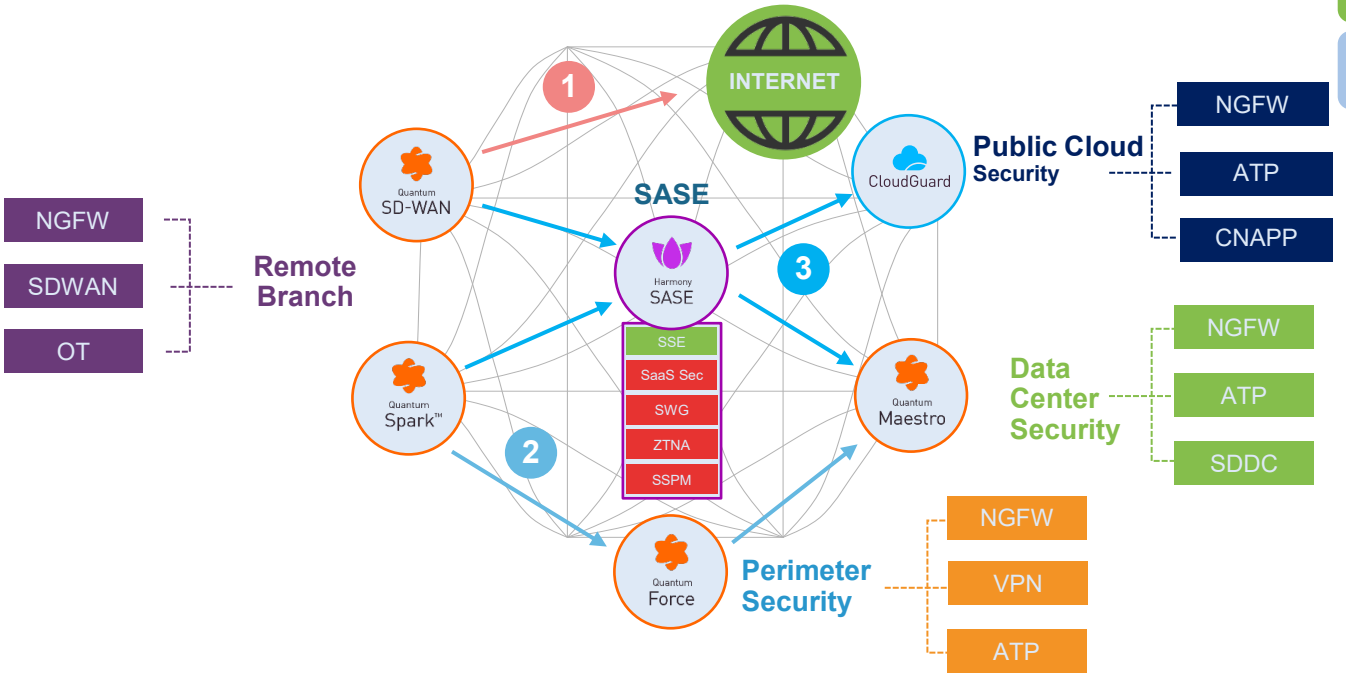
Resilience, flexibility & performances, no backhaul required
Secure direct connection with built, in NGFW capabilities

Summary: Branch Connectivity

USE CASE 1

USE CASE 2

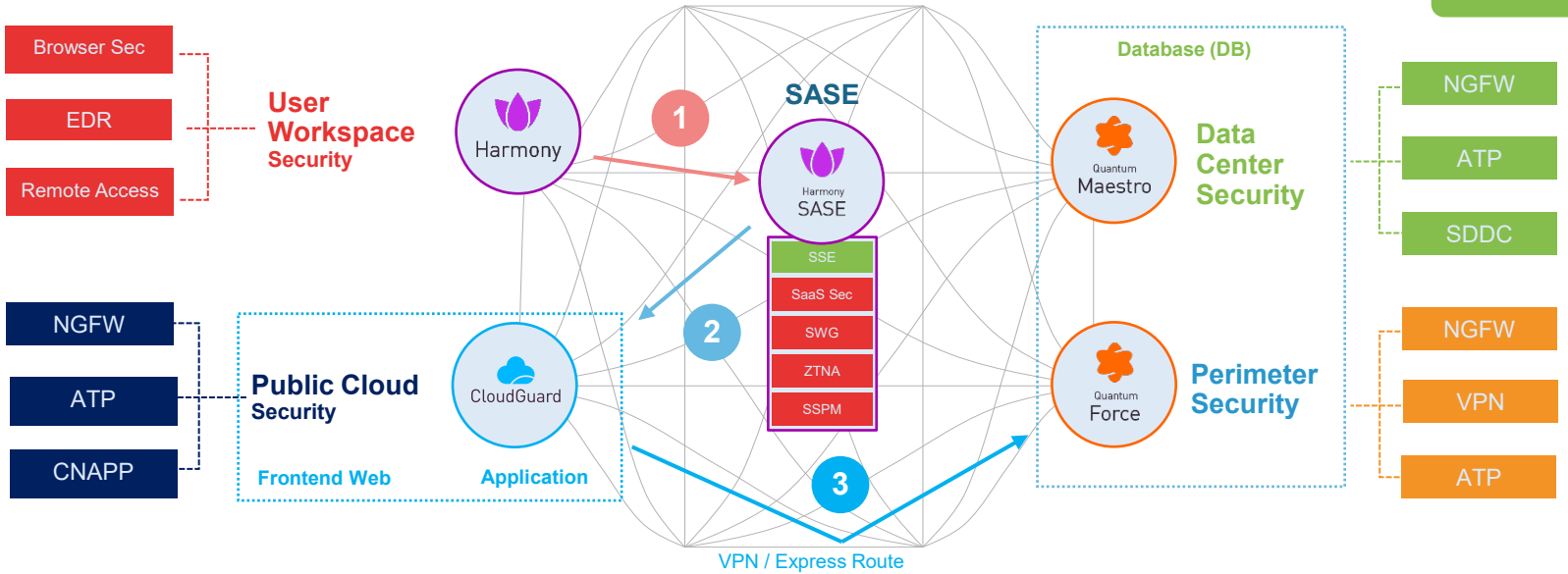
USE CASE 3



Remote branches benefit from flexible connectivity options
that balance performance, security, and cost.

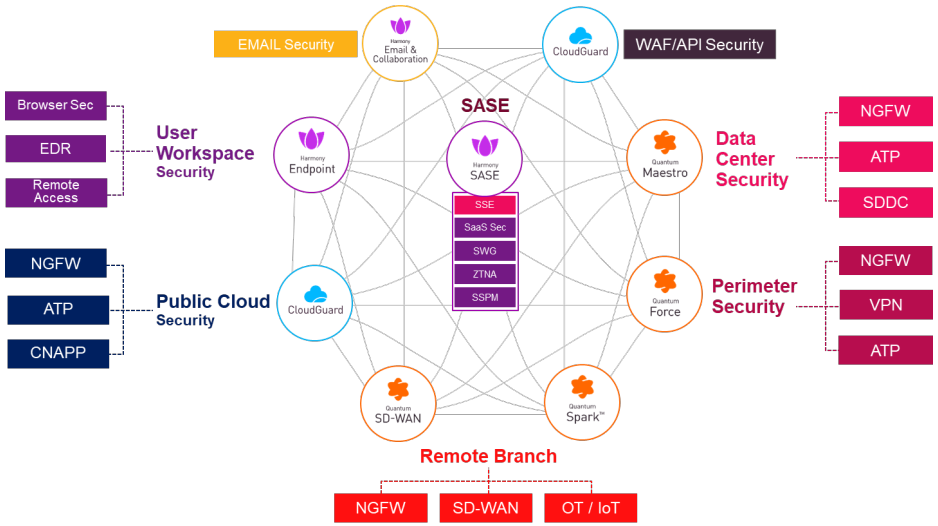
Hybrid Cloud Datacenter Secure Networking

USE CASE 1
USE CASE 2
USE CASE 3

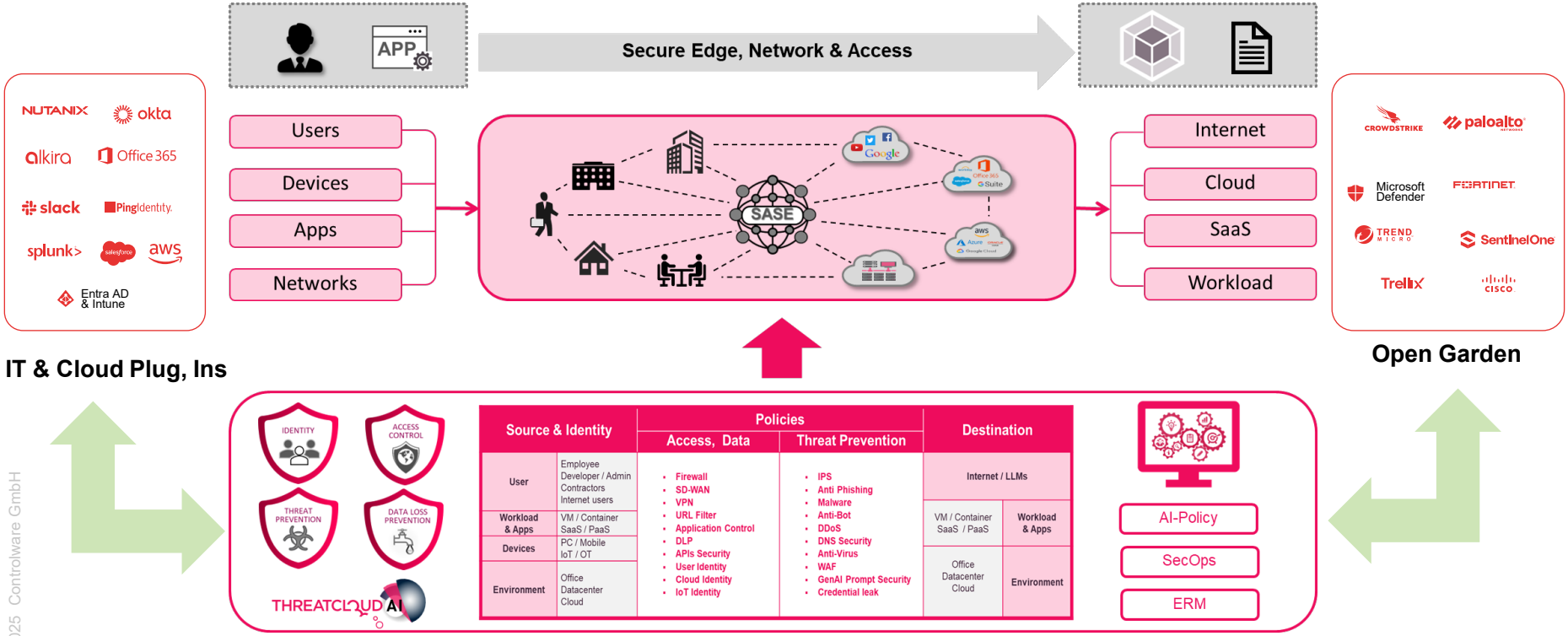


Combines performances and cost, efficiency
By enabling flexible secure connectivity to / between cloud and on, prem resources

- Security should align with business use cases, not force rigid routing
- Check Point Hybrid Mesh protects traffic regardless of path
- Threat Prevention is enforced everywhere
- Not all traffic must go through SASE – options matter
- Use cases show Hybrid Mesh flexibility and security coverage



Infinity Hybrid Mesh Network Security
Unified End, to, End Security & Visibility



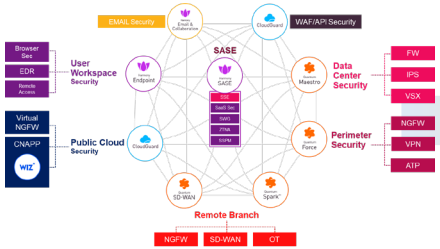
Hybrid Mesh Workshop

Free advisory engagement with experts – Contact Now !

Review current security environment and see how it aligns with Hybrid Mesh concepts

Tailor the Architecture and Use Cases Scenarios

Learn and map Solution and Technology to realize the architecture



Controlware
Security Day

Danke für Ihre Aufmerksamkeit.
Wir freuen uns über Ihr Feedback!

Bitte geben Sie den ausgefüllten Bogen am Empfang ab und erhalten Sie als Dankeschön ein kleines Präsent.