

# Securing The Network: A look at Hybrid Mesh Firewall

Adding Security, No Matter The Location

Matt Hendrickson  
Solutions Engineer - Security

Ben Criag  
Solutions Engineer - SD-WAN



# Introductions – Matt Hendrickson



- Nearly 12-years at Cisco
  - Focusing on Security
  - 28+ years in Security
- Robotics Coach – 2 teams
- Specializations in Identity Services Engine, Secure Access, Secure Firewall, and SNA.

# Introductions – Ben Craig



- 4 years at Cisco
- Focusing on SD-WAN

# Agenda

- ✓ **What is Hybrid Mesh Firewall?**
- ✓ **Security Cloud Control**
- ✓ **Hybrid Mesh Firewall Components**
- ✓ **Cisco SD-WAN & SASE**

# What Is Hybrid Mesh Firewall

# Firewalling needs to evolve to meet today's challenges

	Stateful Firewall 1990-2007	Next Generation Firewall 2008-2024	Hybrid Mesh Firewall 2025-
Drivers	Growing internet access Basic attacks Need perimeter control	Rise of SaaS/cloud apps Mobile users App layer threats	Increasingly distributed apps Rise of AI Zero trust imperative
Needs	Tracks connection state Filters by IP/port Basic traffic control	App & user aware Integrated threat prevention SSL/TLS decrypt	Hyper-distribution Integrated AI protection AI-powered management

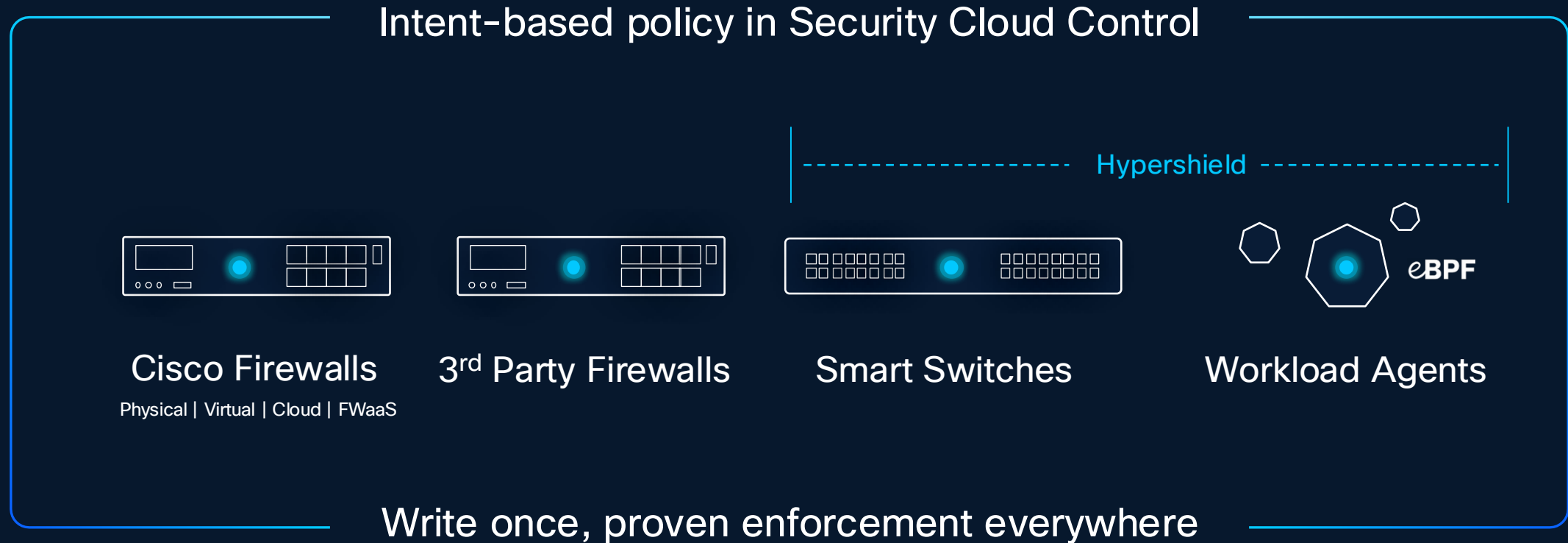
# Key challenges we're solving

Fragmented  
segmentation  
policy can't keep  
up with change

Visibility and  
security gaps  
for modern cloud  
and AI apps

Attackers  
move faster  
than patching  
cycles

# Hybrid Mesh Firewall: Security at the speed of change



Single intent-based policy drives multi-domain segmentation

Modern AI app security: deep visibility and AI guardrails

Shrink exposure window with runtime shielding

# Near-limitless scale for AI readiness



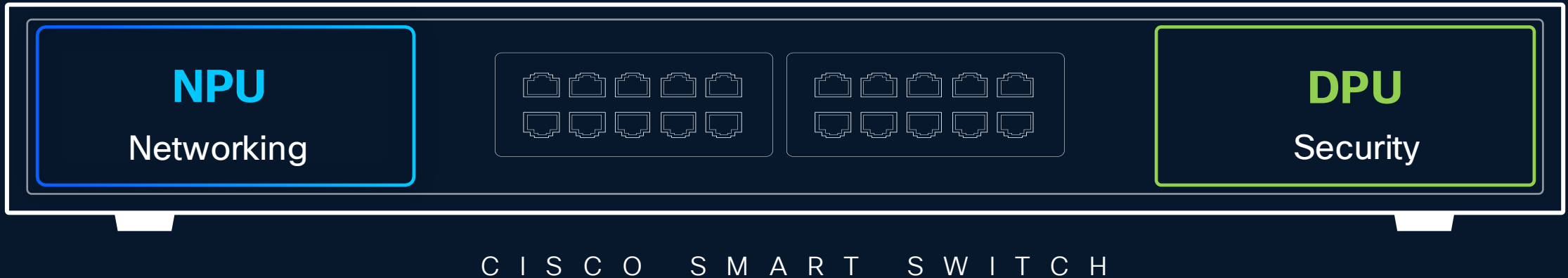
## Cisco Secure Firewall 6100 Series

Scales linearly to 8Tbps of L7,  
applD, threat inspection

Changes math per protected  
Gbps: 80% less space, 60%  
less power, 1/3 the cost

No-compromise security:  
encrypted traffic performance,  
zero-day protection

# Fusing security in

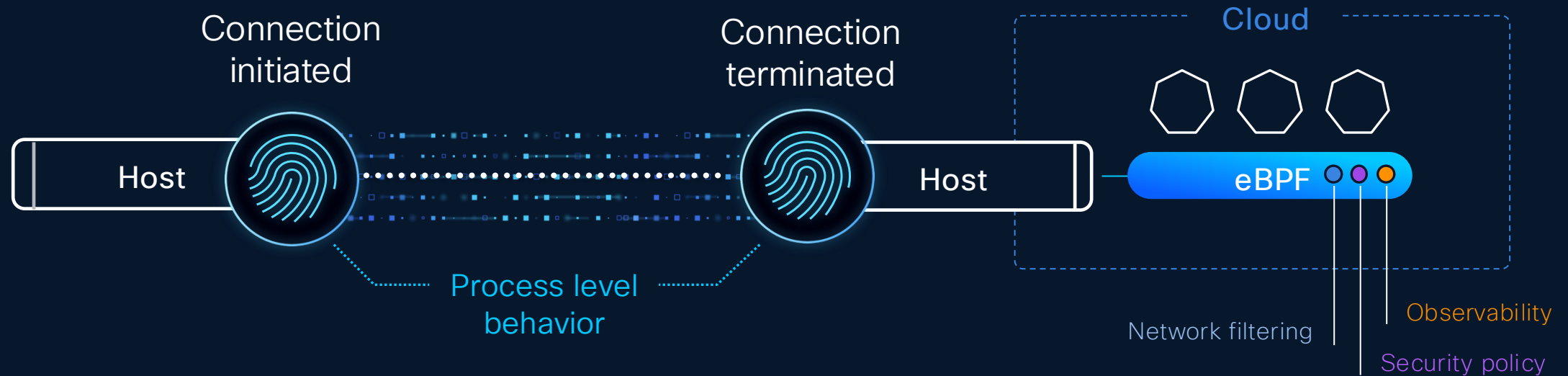


Single appliance,  
dual personality

Greater visibility, fewer  
dropped packets

More easily scale security  
as traffic increases

# Process-level visibility for cloud and containers



See and control the inner workings of modern apps

Segment effectively as apps change

Shield vulnerabilities while you patch

# Secure Firewall embedded in the Secure Router



## Next Generation Firewall



## SASE Ecosystem



# Secure Cloud Control

# Security Cloud Control

Define policy once and enforce anywhere

Cisco Firewalling

AI Defense

3rd Party Firewalls

Secure Firewall

Secure Workload

Hypershield

Secure Access (FW as a service)

Secure Router NGFW



Unified AI Assistant:  
Simplify policy administration **by up to 70%**

NEW

# Security Cloud Control

Industry's first multi-vendor intent-based policy



Absorb and optimize  
existing rules

Change enforcement  
points, not policy

No rip and  
replace

# Secure Firewall Physical Platforms

## Cisco Secure Firewall 200 Series

### Advanced on-box threat inspection for branch

1.5 Gbps encrypted threat protection

Up to 3x price-performance

Integrated SD-WAN

AVAILABLE JAN 2026



## Cisco Secure Firewall 6100 Series

### Highest performance density for AI data centers

285 Gbps per rack unit

Line rate advanced threat protection

Modular scalability

AVAILABLE JAN 2026



# Firewall price-performance leader

Top to bottom

Branch

Campus

Data center

Cloud

NEW



## 200 Series

1 Model  
Firewalling + IPS

Up to 1.5 Gbps



## 1200 Series

6 Models  
Firewalling + IPS

Up to 18 Gbps



## 3100 Series

5 Models  
Firewalling + IPS

Up to 45 Gbps



## 4200 Series

3 Models  
Firewalling + IPS

Up to 140 Gbps



## 6100 Series

2 Models  
Firewalling + IPS

Up to 570 Gbps

NEW



## Public/Private

20+ cloud variants



HyperFlex

NUTANIX



openstack



Microsoft Azure



alkira

rackspace  
Technology

EQUINIX

Alibaba Cloud

ORACLE  
CLOUD INFRASTRUCTURE

# Firewalling at scale across multicloud environments

Secure Firewall is now cloud-native



Cloud agnostic automation  
and orchestration

Automated Deployment  
Auto-scaling  
Self-healing

Deep visibility into  
cloud environments

A blue circular logo with the letters 'AI' in white, centered in the top right corner of the slide.

AI

# Cisco Encrypted Visibility Engine

Visibility to malicious flows in encrypted traffic without decryption

Machine learning  
(ML) technology

Processes 1 B+  
TLS fingerprints daily

Processes 10 K+  
malware samples daily

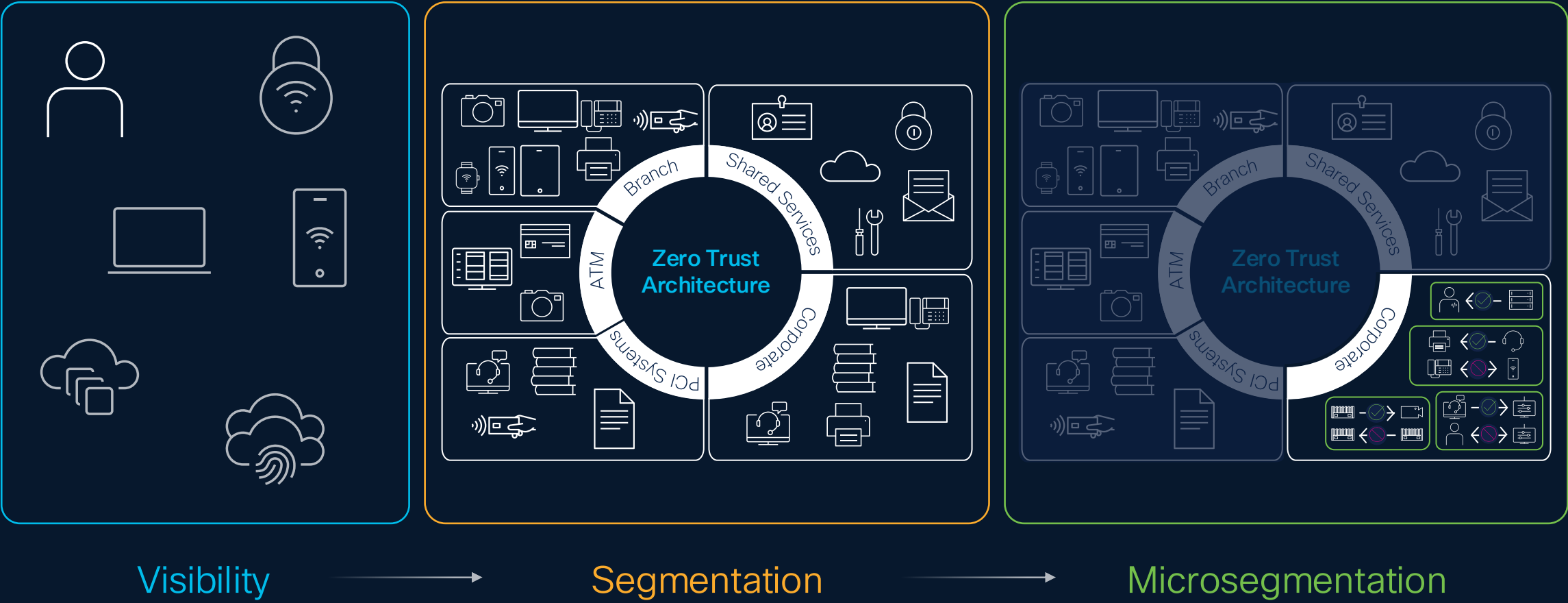
# EVE changes the game on decryption

Risk-based intelligent decryption, powered by Cisco Encrypted Visibility Engine (EVE)



# Cisco Secure Workload

# Compliance and reduction of attack surface with Microsegmentation



# Top Segmentation Use Cases

Prevent and block  
**lateral movement**

Increase  
operational  
efficiency by  
converting NGFWs  
to **SGT-based  
SGFWs**

# Big Picture

Agent

Consistent microsegmentation from on-premises to the cloud

Agentless

Anywhere

Windows Desktop

Windows Server

IBM AIX

Oracle Solaris

Oracle Linux

Centos, Rocky,  
Alma Linux

Ubuntu, Debian

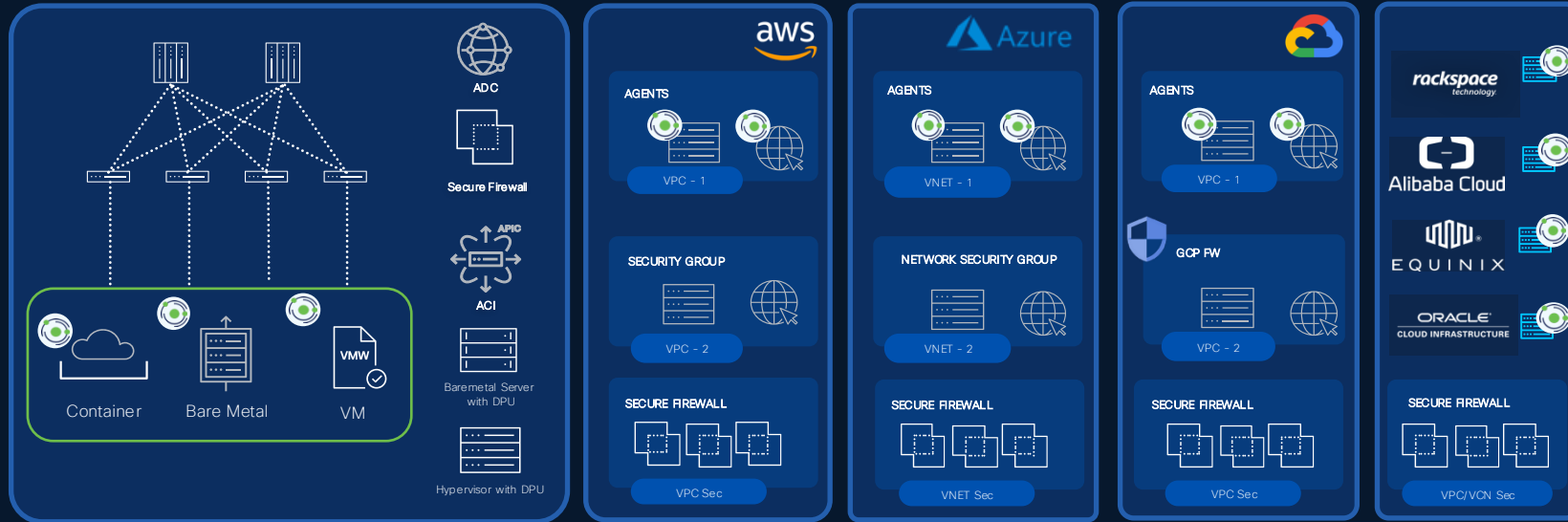
SUSE Linux

RedHat Linux

Amazon Linux

OpenShift

Kubernetes



On Premise

Public Cloud



Bare Metal Servers



Virtual Machines



Containers

User Identity

Tags and Labels

Vulnerability

Threat Feed

Application Encryption

Domain/FQDN

Cisco Security Risk Score

On-Prem

Loadbalancer (ADC)

Firewalls

Data Center Fabric (SDN)

NVIDIA Smart NIC (DPU)

AWS, GCP, Azure

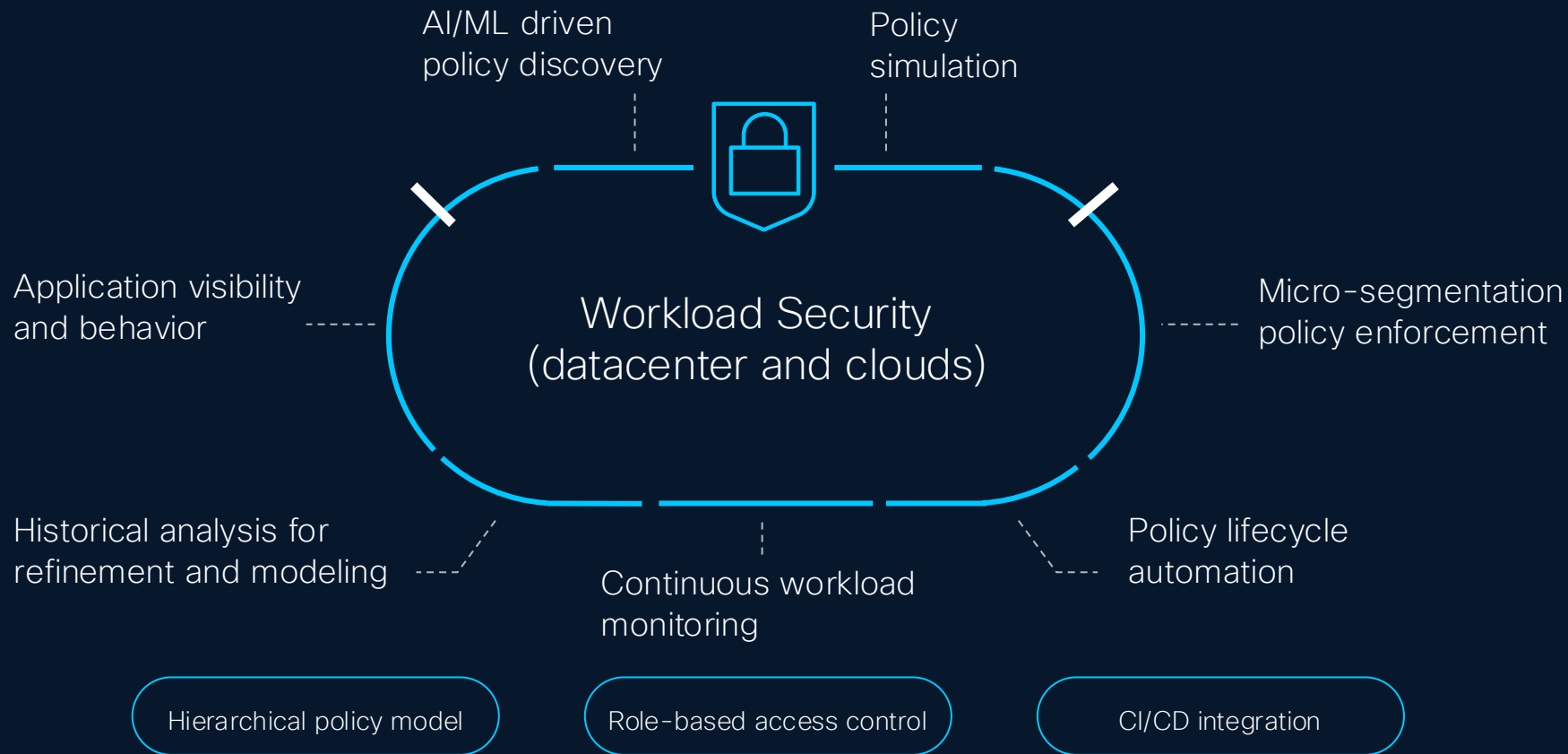
Security Group

Network Security Group

Cloud Network Firewall

Multicloud Defense\*

# Secure Workload

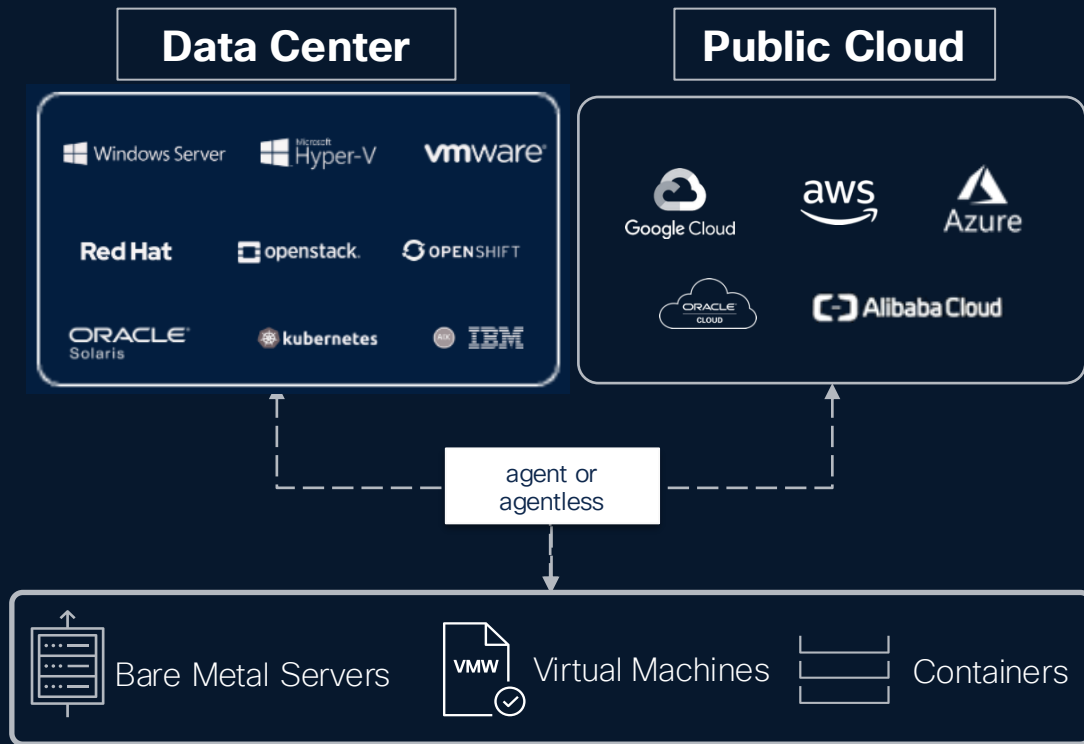


**Stop lateral movement**  
Zero trust microsegmentation protects application workloads across the data center and clouds from one solution

**Quickly improve security posture**  
Understand application behavior and enact best-practice hardening policies such as blocking insecure app to app communications

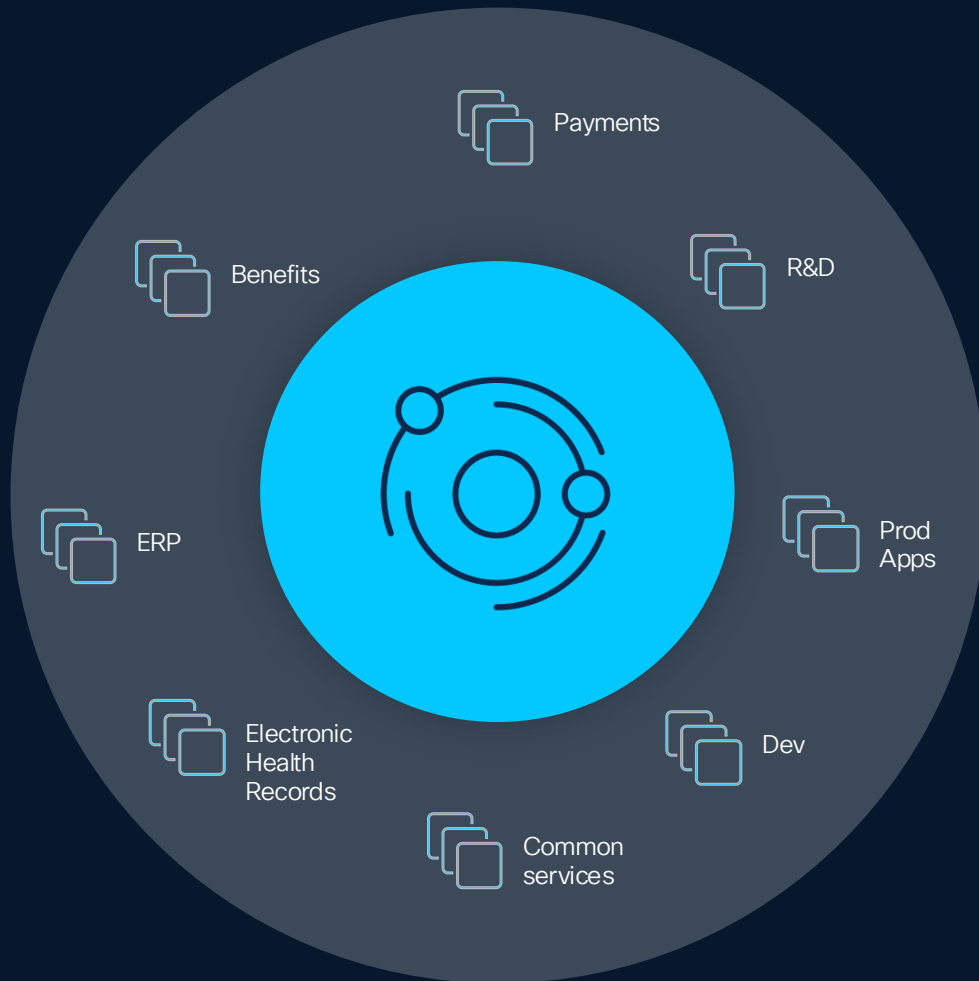
**AI/ML tackles tasks that are beyond human scale**  
Powerful AI/ML driven policy discovery recommends policies tailored to the unique environment and automation ensures consistency and accuracy

# Visibility



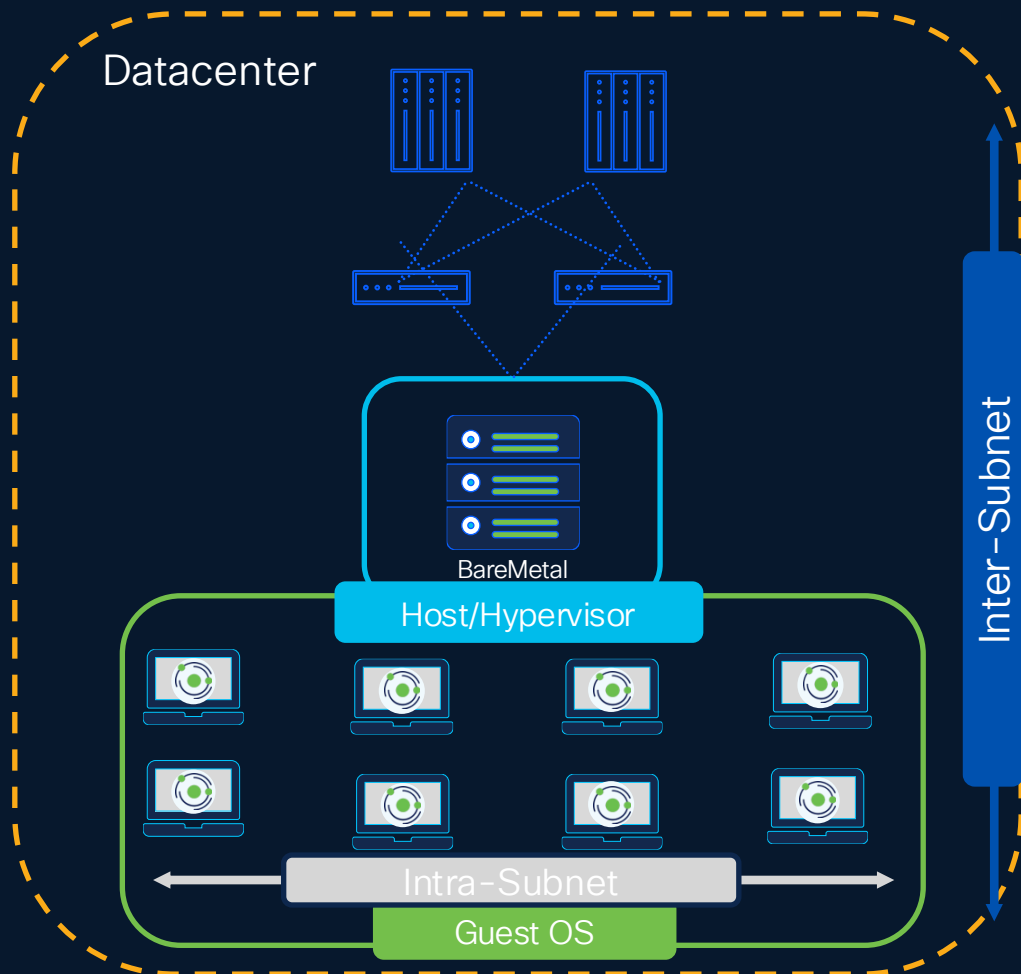
- ✓ Discover applications, identify interactions, and understand vulnerabilities
- ✓ Discover applications across on-prem data center, public and private cloud with agents and/or agentless approach
- ✓ Get process-level visibility into Microsoft Windows, Linux, Solaris, AIX, and Container infrastructure
- ✓ Agentless discovery through pre-built integrations with hypervisors, cloud providers, CMDB, IPAM, IDP, DNS, VMM, etc.

# Application protection



- ✓ Enforce micro-segmentation throughout the network stack: SDN, edge firewall, subnet, application
- ✓ Use vulnerability risk score for access policies to change
- ✓ AI/ML-driven policy review to eliminate stale or overlapping policies
- ✓ Use policy templates to accelerate micro-segmentation aligned with NIST and CISA frameworks

# Virtual Desktop Infrastructure Microsegmentation



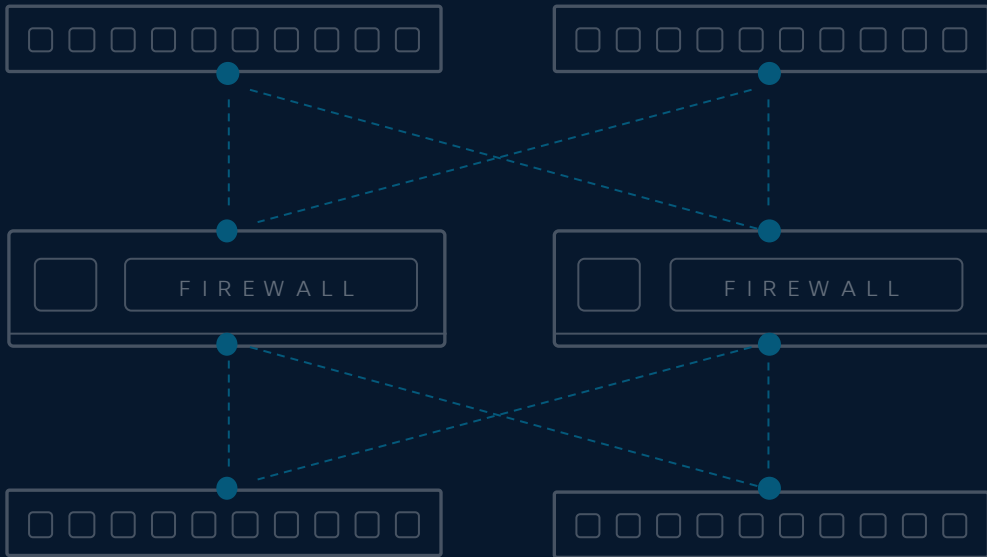
## Host-Based Agent VDI Microsegmentation

- Same agent as for workloads
- Ideal for fine-grained segmentation
  - In-depth endpoint visibility
  - Protection at the VDI user/desktop level
- Suitable for all personas

**Hypershield**

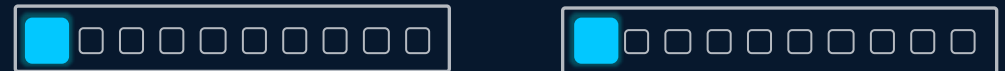
# Unprecedented ROI

6 boxes



2 boxes

Cisco Smart Switch



Power



Software licenses



Optics



Support contracts



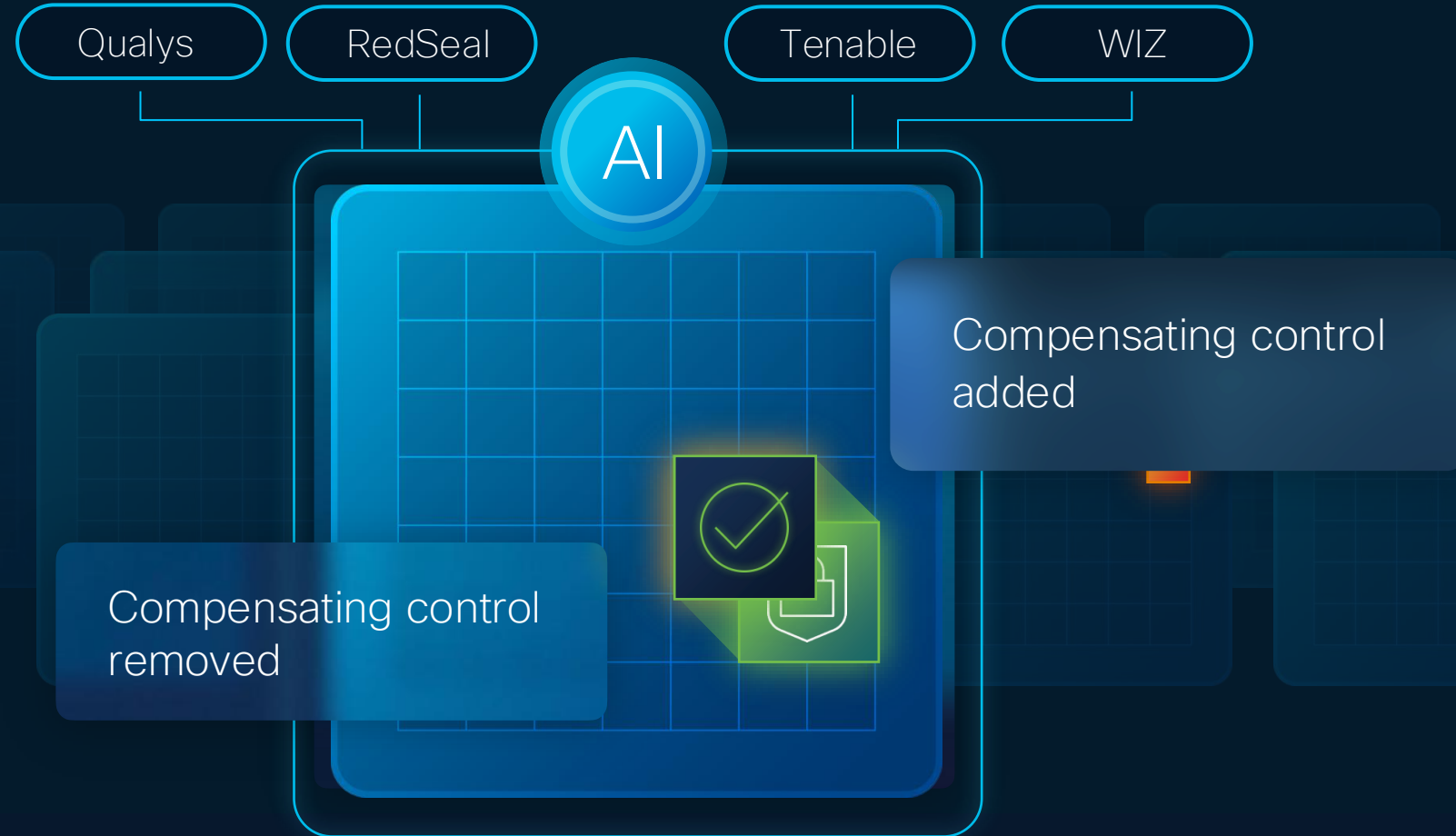
Cables



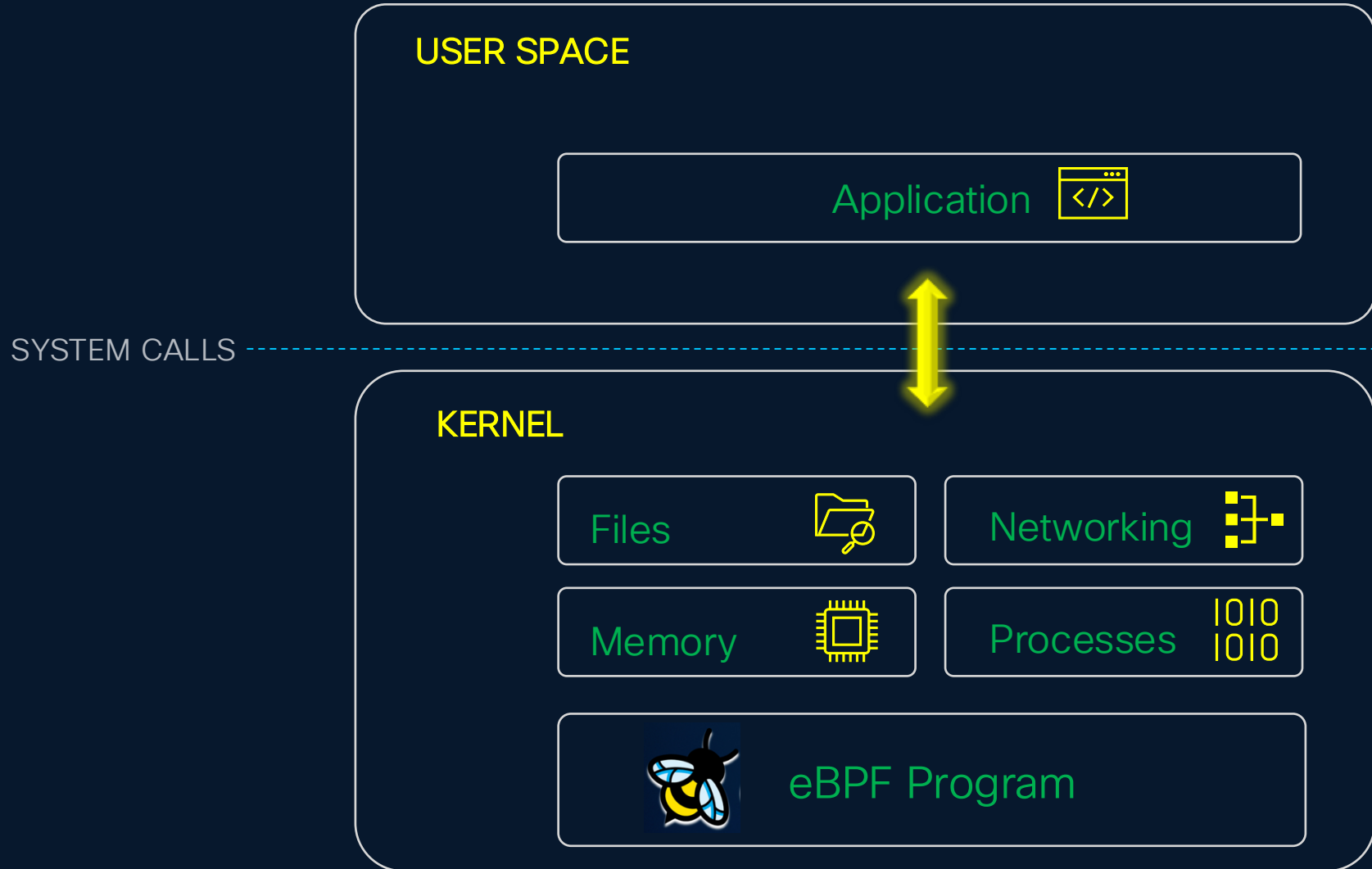
# Patching is hard



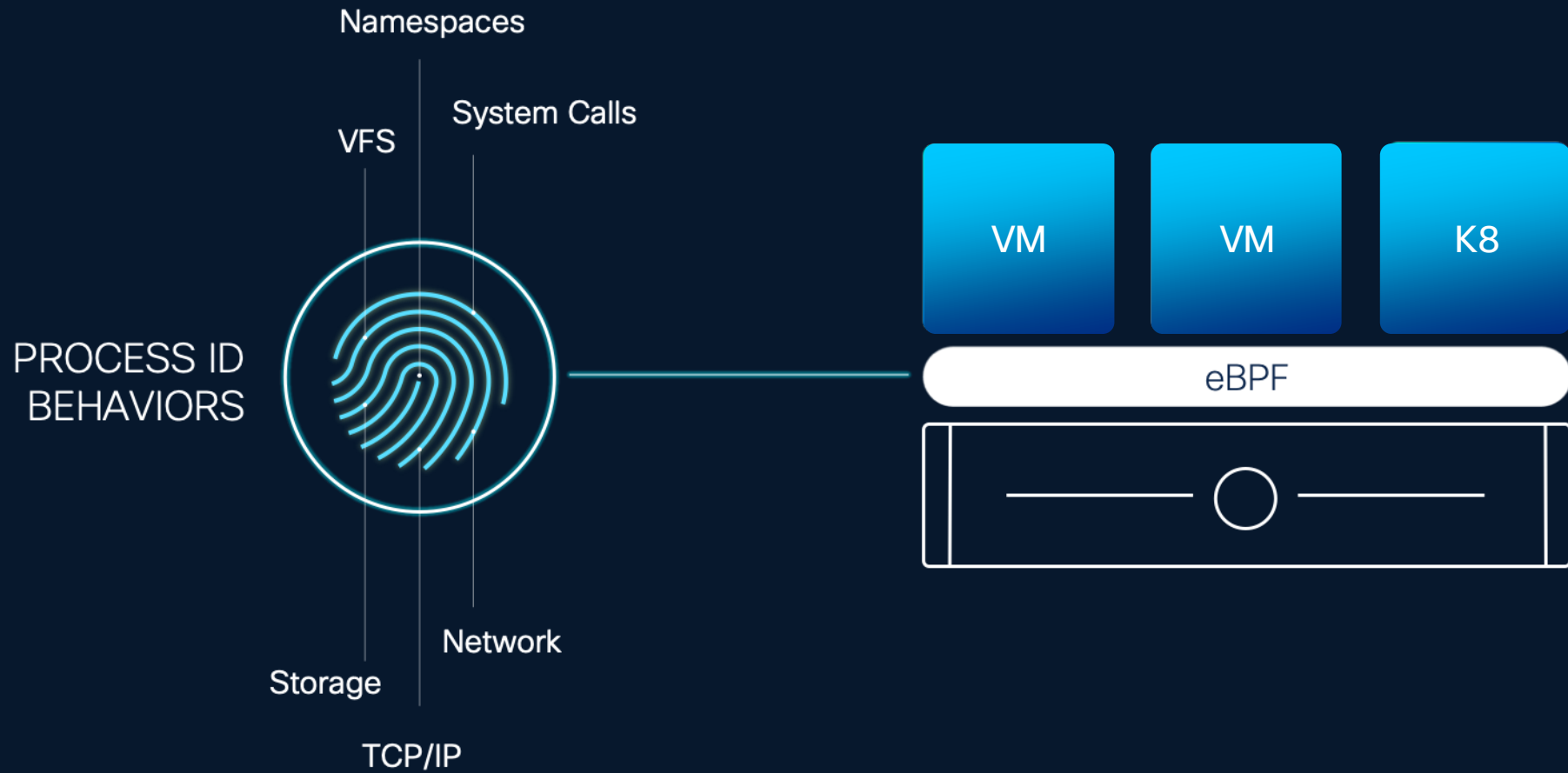
# Distributed Exploit Protection



# Hypershield Building Blocks - eBPF



# eBPF Provides Visibility Deep into the Workload



# We also understand things



OS version | Mac ID | OPSWAT checks | DHCP | Traffic flows | DNS and certificate

**Security fused into the Network**



**Catalyst SD-WAN & SASE**

# Simple Secure WAN

# Journey to simplified Secure WAN portfolio

Market leading  
enterprise routers



ASR / ISR

Continued investment  
in current portfolio



Catalyst 8000



MX

Converged portfolio

NEW



8000 Series  
Secure Router

More throughput to support increased traffic to data center

Advanced embedded NGFW for secure branch connectivity

Post-quantum secure

DevOps style Branch-as-code for rapid deployment

# Introducing Secure Routers for the AI-powered unified branch



## Cisco 8000 Secure Routers

# Cisco 8000 Series Secure Routers for every size location



## Small Branch: 8100

4 Variants

IPsec:  
Up to 1.5 Gbps

SD-WAN:  
Up to 1 Gbps

Threat Protection:  
Up to 1 Gbps



## Medium Branch: 8200

2 Variants

IPsec:  
Up to 5 Gbps

SD-WAN:  
Up to 4 Gbps

Threat Protection:  
Up to 2.5 Gbps



## Large Branch: 8300

2 Variants

IPsec:  
Up to 20 Gbps

SD-WAN:  
Up to 15 Gbps

Threat Protection:  
Up to 7 Gbps



## Campus: 8400

3 Variants

IPsec:  
Up to 45 Gbps

SD-WAN:  
Up to 23 Gbps

Threat Protection:  
Up to 11 Gbps



## Data Center: 8500

2 Variants

IPSec:  
Up to 45 Gbps

SD-WAN:  
Up to 23 Gbps

Route Scale up to 8M

# Secure WAN Portfolio Transition

## Branch

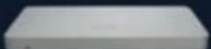
### Small



8100 Secure Router



ISR1000

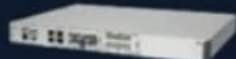


MX 67/68/75

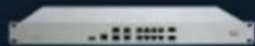
### Medium



8200 Secure Router



Catalyst 8200



MX 85/95/105

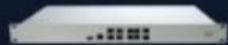
### Large



8300 Secure Router

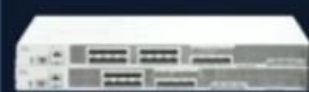


Catalyst 8300

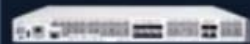


MX 250/450

## Campus / Datacenter



8400 Secure Router



Catalyst 8500L



Net-New MX  
Scale



8500 Secure Router



Catalyst 8500

## Cloud



Catalyst 8000V



SRIOV  
Hypervisor/Cloud



## Cellular



CG522



MG41/E  
MG52/E

# Use Cases – Cisco 8000 Series Secure Router



## IP Connectivity

MSPs to offer reliable and sustainable connectivity with simplified management



## Routing VPN

Future-proof your data center & branch with high-performance, secure connectivity



## SD-WAN

Seamless, secure, and scalable connectivity for modern offices



## Secure SD-WAN w/ NGFW

Consistent enforcement of network and security policy by NetOps and SecOps



## SASE

Empower hybrid workers with secure, reliable remote access

Meeting customers where they are

# Flexible management options



## On-Prem or Cloud

---

### Cisco SD-WAN Manager

Use cases require on-prem delivery,  
or advanced configuration



## Cloud

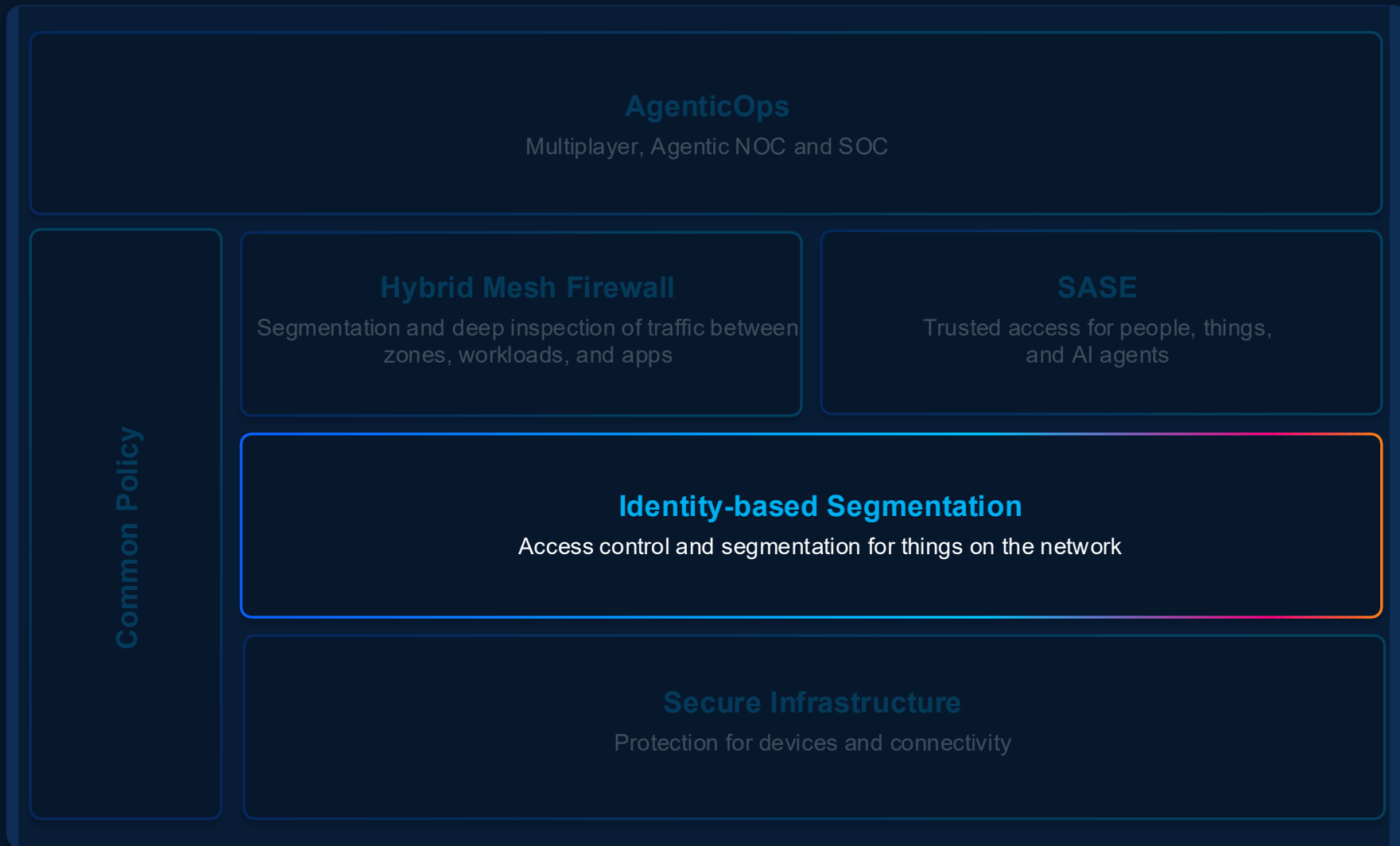
---

### Meraki Dashboard

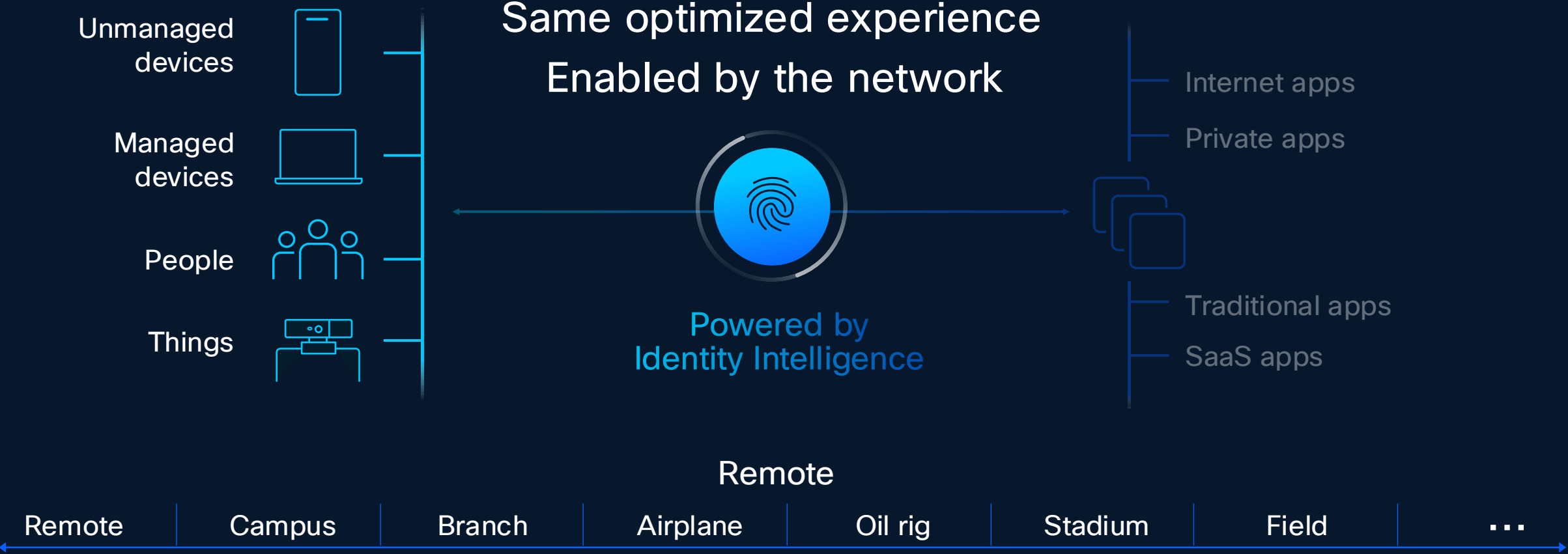
Prefer cloud-enabled delivery for full stack  
with Agentic Ops

Delivering optimized, simplified experiences for all customers.

# Reference design for fusing security into the network

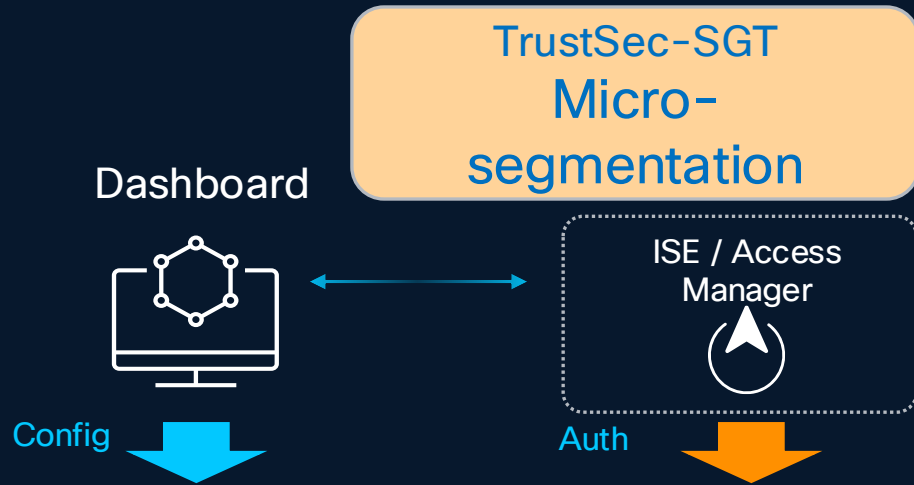


# Securing Users, Device access to Apps with Universal ZTNA from Cisco



# Cisco Zero Trust Segmentation

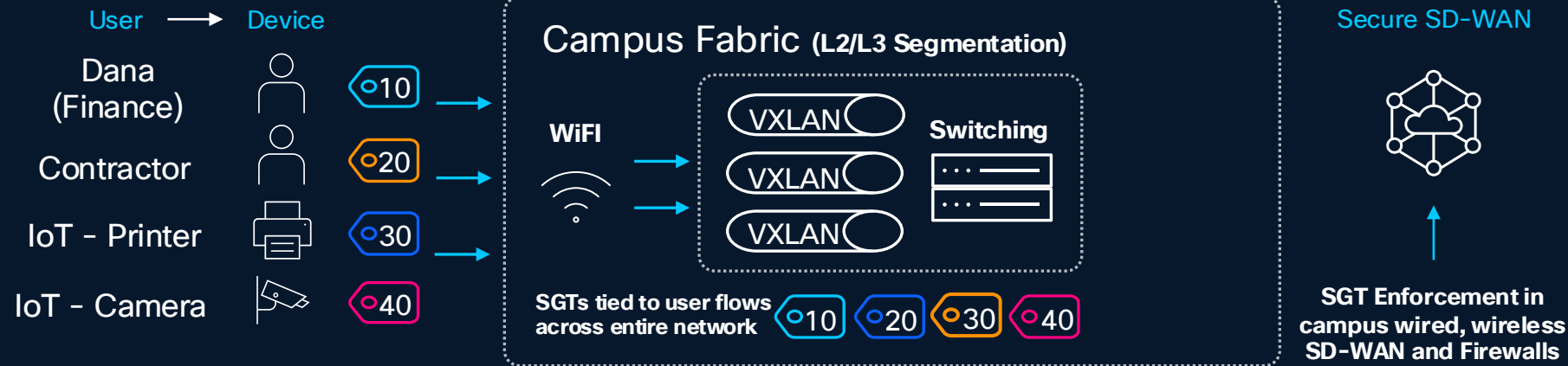
Campus and Unified Branch User to App



## Campus Fabric:

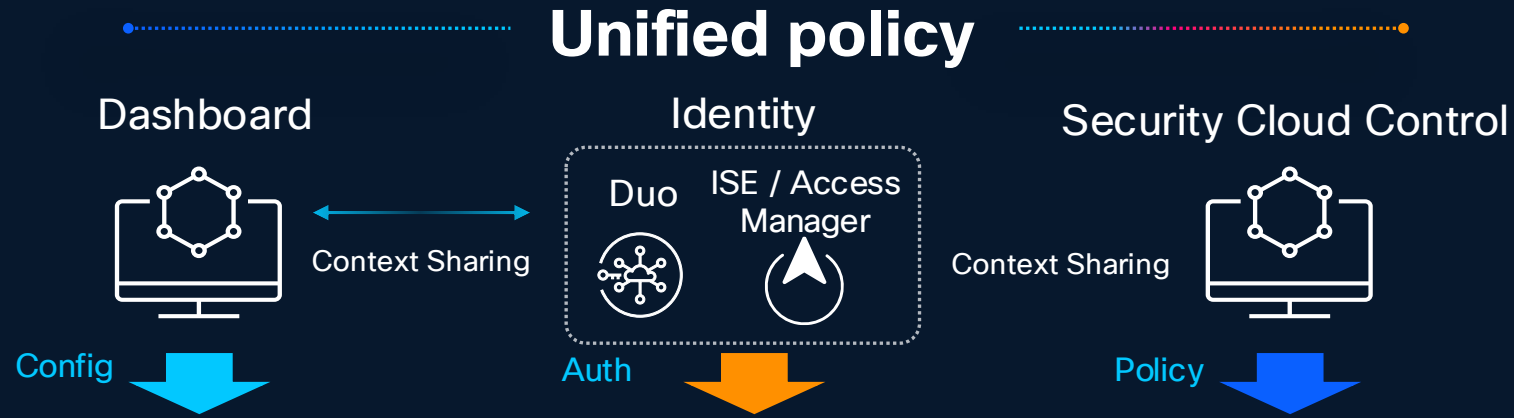
- Macro Segmentation with VRF / VXLAN
- Integrated Wired, Wireless and SD-WAN policies

## Campus



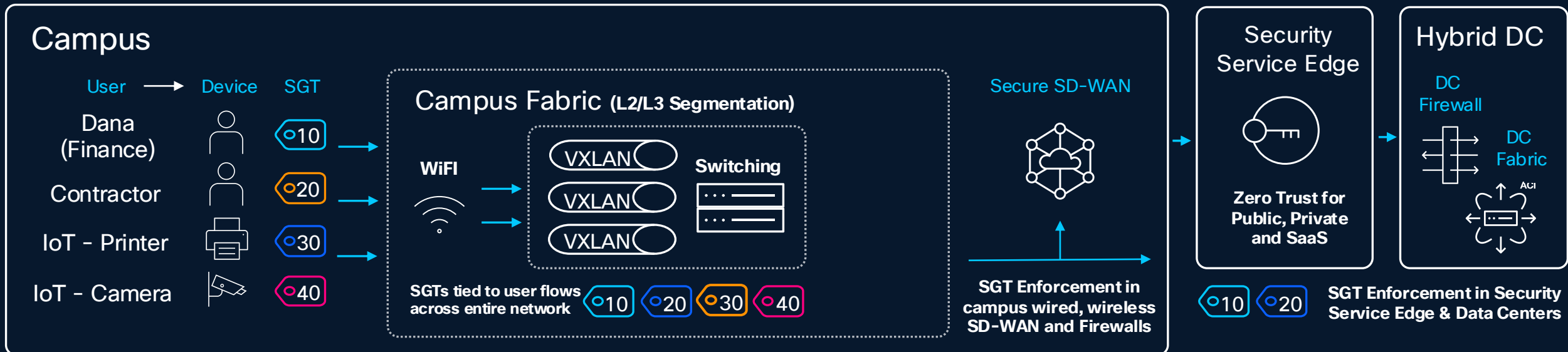
# Cisco Zero Trust Segmentation

Campus and Unified Branch User to App

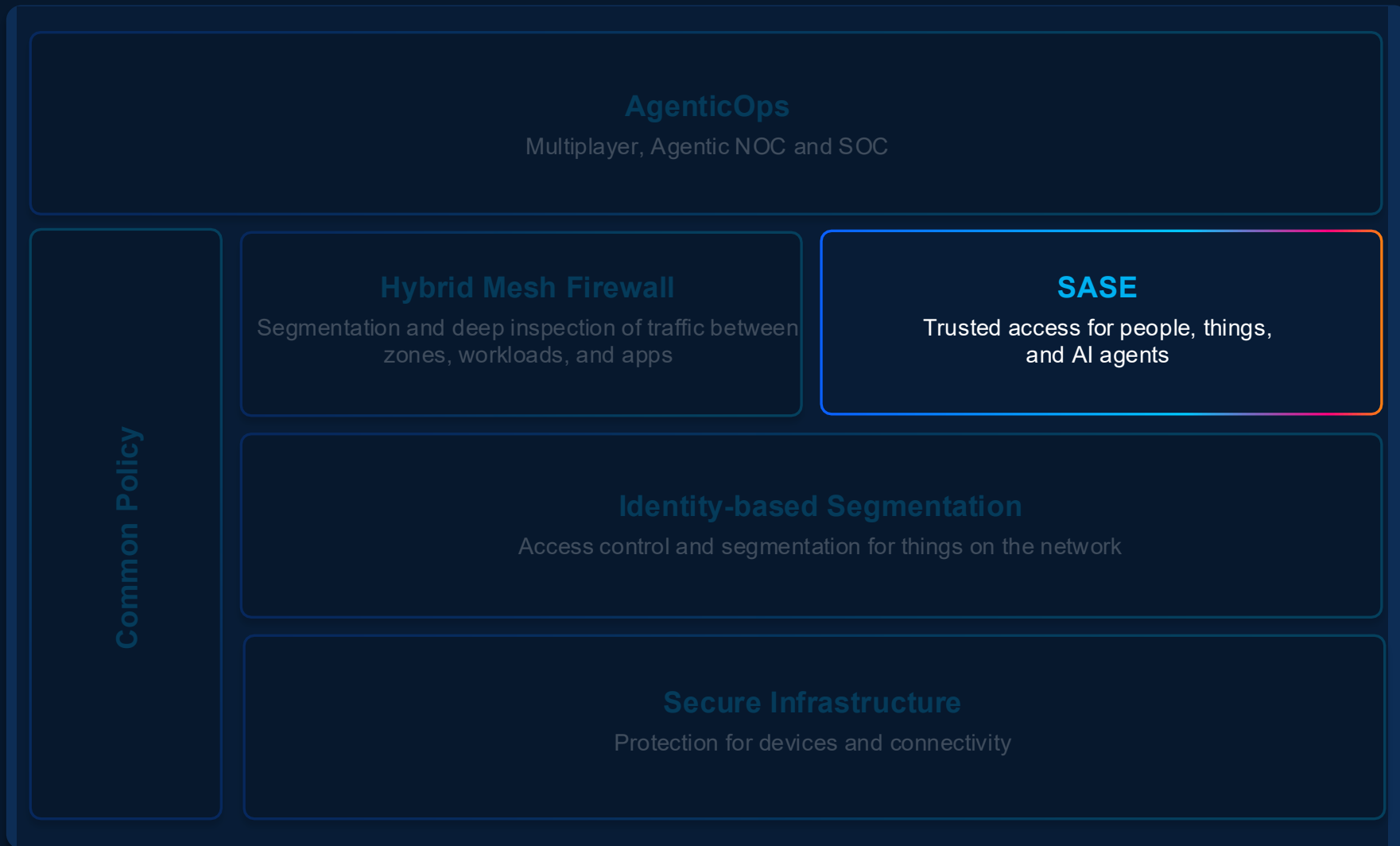


# Security Cloud Control

- Unified policy between network, firewalls, SSE and Hybrid DC fabric
- User identity trust



# Reference design for fusing security into the network



# Securing users, devices and apps with Cisco SASE



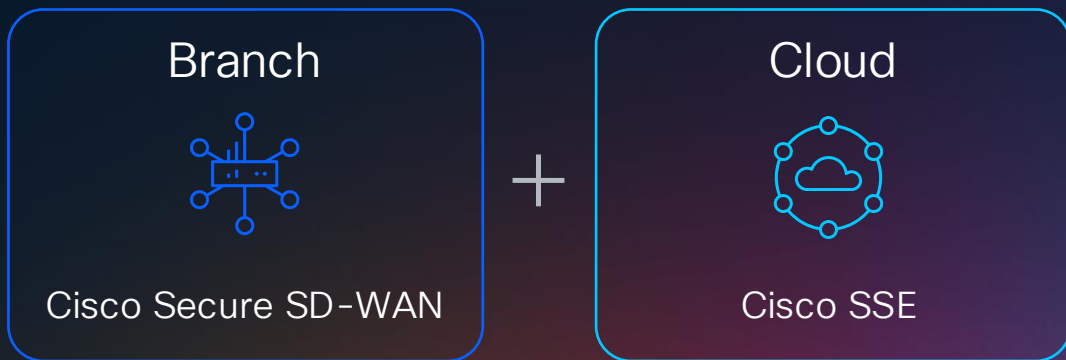
- L3 - L7 FW**  
Manage traffic flow
- IPS/IDPS**  
Protect assets from bad actors
- AMP**  
Protect against malware
- Sandboxing**  
File Analysis using Threat Grid
- URL-F**  
Filter Internet traffic
- TLS Decryption**  
Inspect encrypted traffic
- DNS Security**  
Inspect risky domains

# Cisco SASE

Solutions designed to meet you on your journey to secure connectivity, anywhere

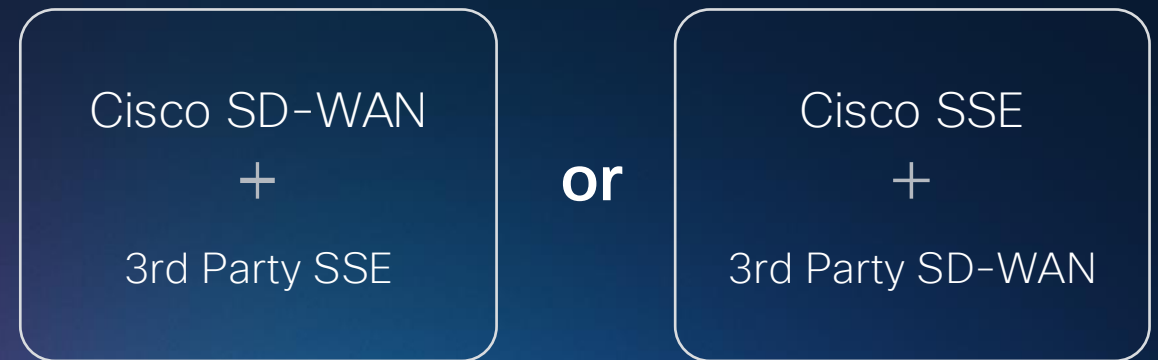
## Cisco SASE

Powerful, flexible, and intelligent



## Open SASE

Open, validated integrations



# Cisco eases your journey to a future proof secure branch



\*when combined this is known as SASE architecture

# Where we're going?

Secure Routers on Dashboard  
Cloud Management

Hardware convergence  
Secure Router Consolidating Portfolio

Unified SASE experience  
Security Cloud Control

AI ops  
Troubleshooting and remediation by agents

Thank you

