CISCO Connect

Segmentation Untangled: Streamlining Hybrid Data Center Security

Buford Peek – Atlanta Select Security SE

October 30, 2025

Streamlining Hybrid Data Center Security

1. Hybrid Mesh Firewall
2. Secure Firewall
3. HyperShield & Isovalent
4. Multicloud Defense
5. AI Defense
6. SASE
7. Security Cloud Control

CISCO Connect

Hybrid Mesh Firewall

From Firewall to Firewalling

	Stateful Firewall	Next generation Firewall	Hybrid Mesh Firewall
	1990-2007	2008-2024	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

Firewalling needs to evolve to meet today's challenges

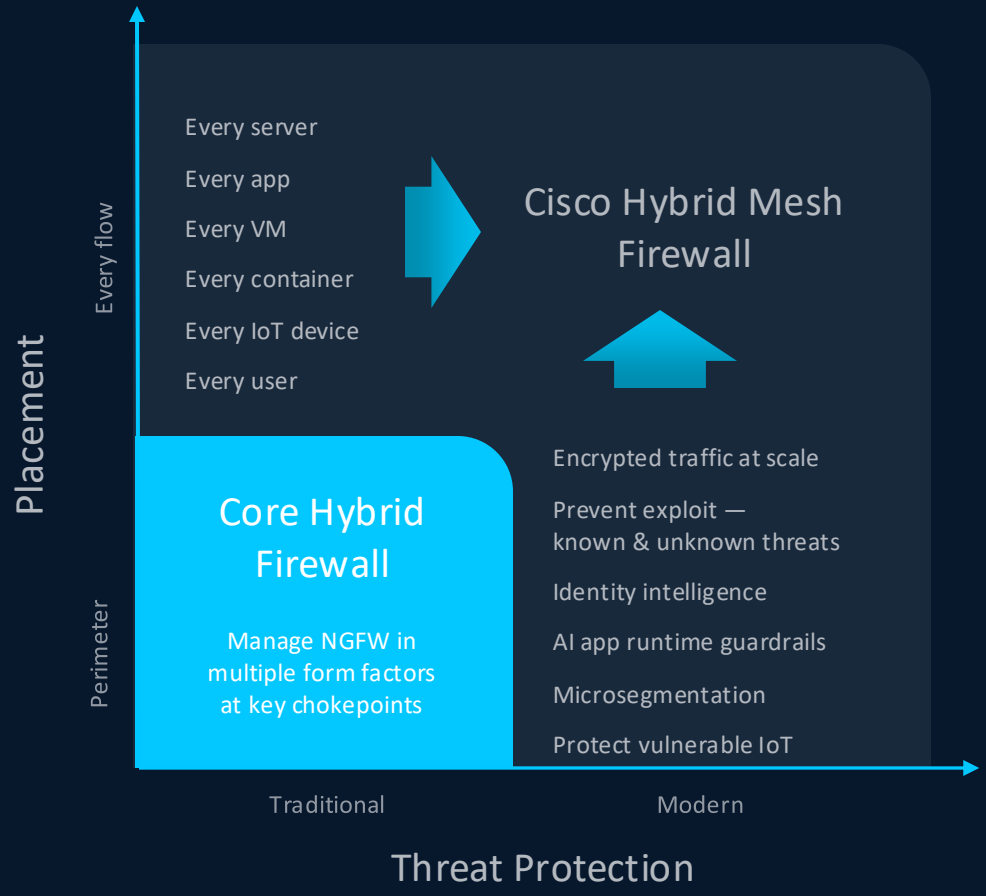
Highly distributed applications	Nothing can be trusted	More vulnerabilities, exploited faster

Our North Star

Make it easy for organizations to

- **Reduce** attack surface
- **Prevent** compromise
- **Stop** lateral movement

in the modern data center, cloud, campus, and factory



Hybrid Mesh Firewall (Segmentation as a Platform)

Write policy once, enforce across the mesh

CISCO Connect

Secure Firewall

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

NEW

6100 Series

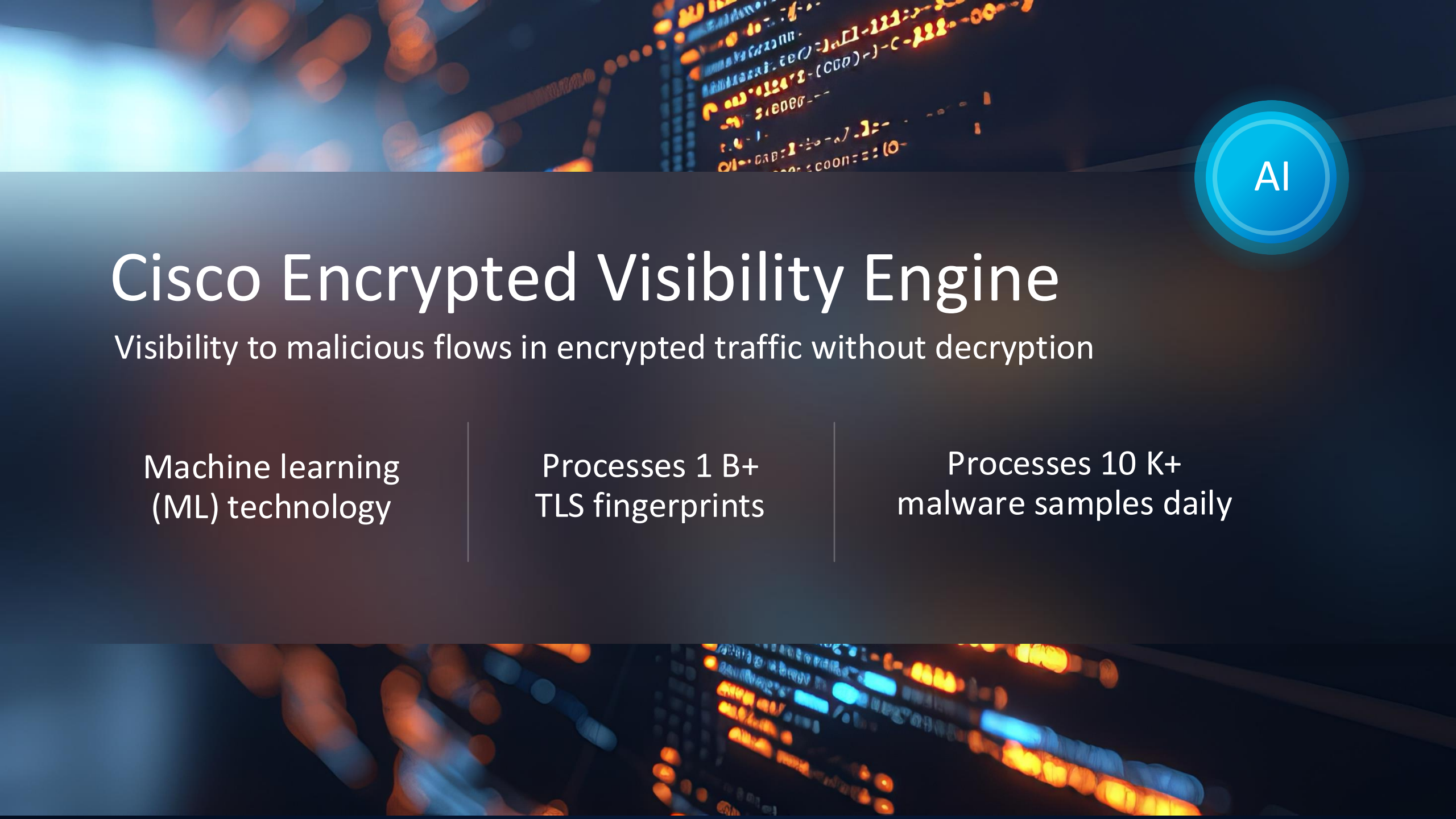
2 Models

Firewalling + IPS

Up to 400 Gbps

Public/Private

20+ cloud variants



Cisco Encrypted Visibility Engine

Visibility to malicious flows in encrypted traffic without decryption

Machine learning (ML) technology

Processes 1 B+ TLS fingerprints

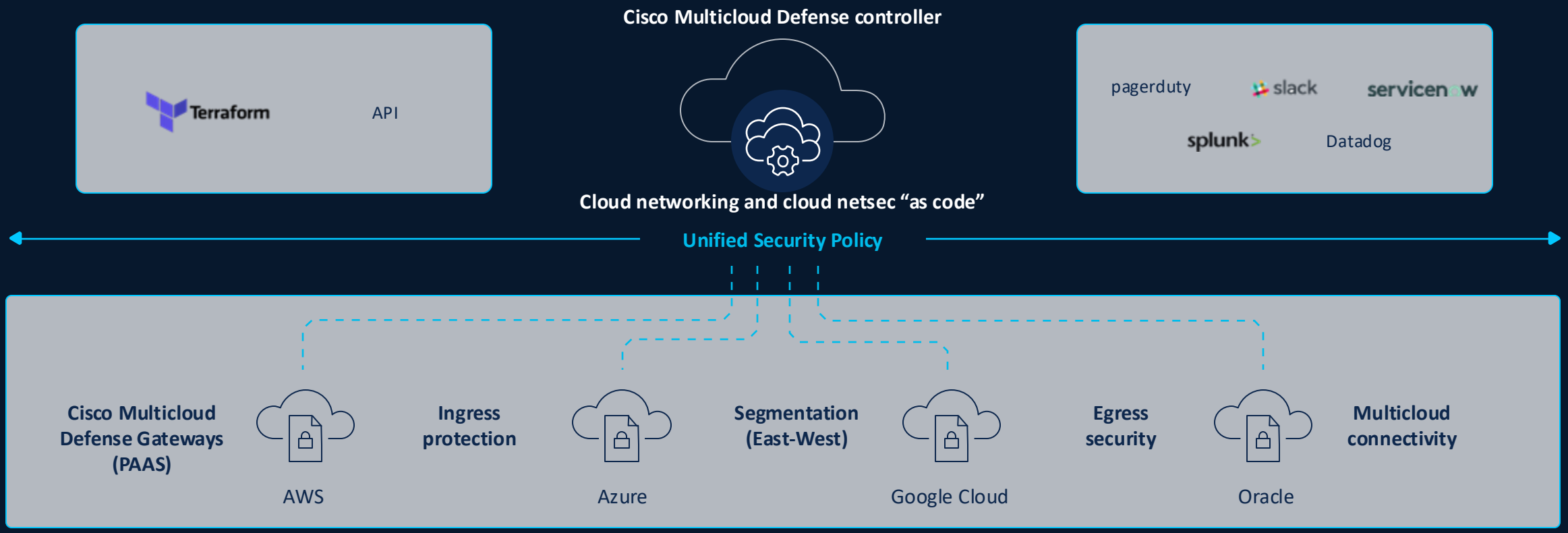
Processes 10 K+ malware samples daily

CISCO Connect

Multicloud Defense

Cisco Multicloud Defense

Combining multicloud networking, automation, and cloud-native network security controls

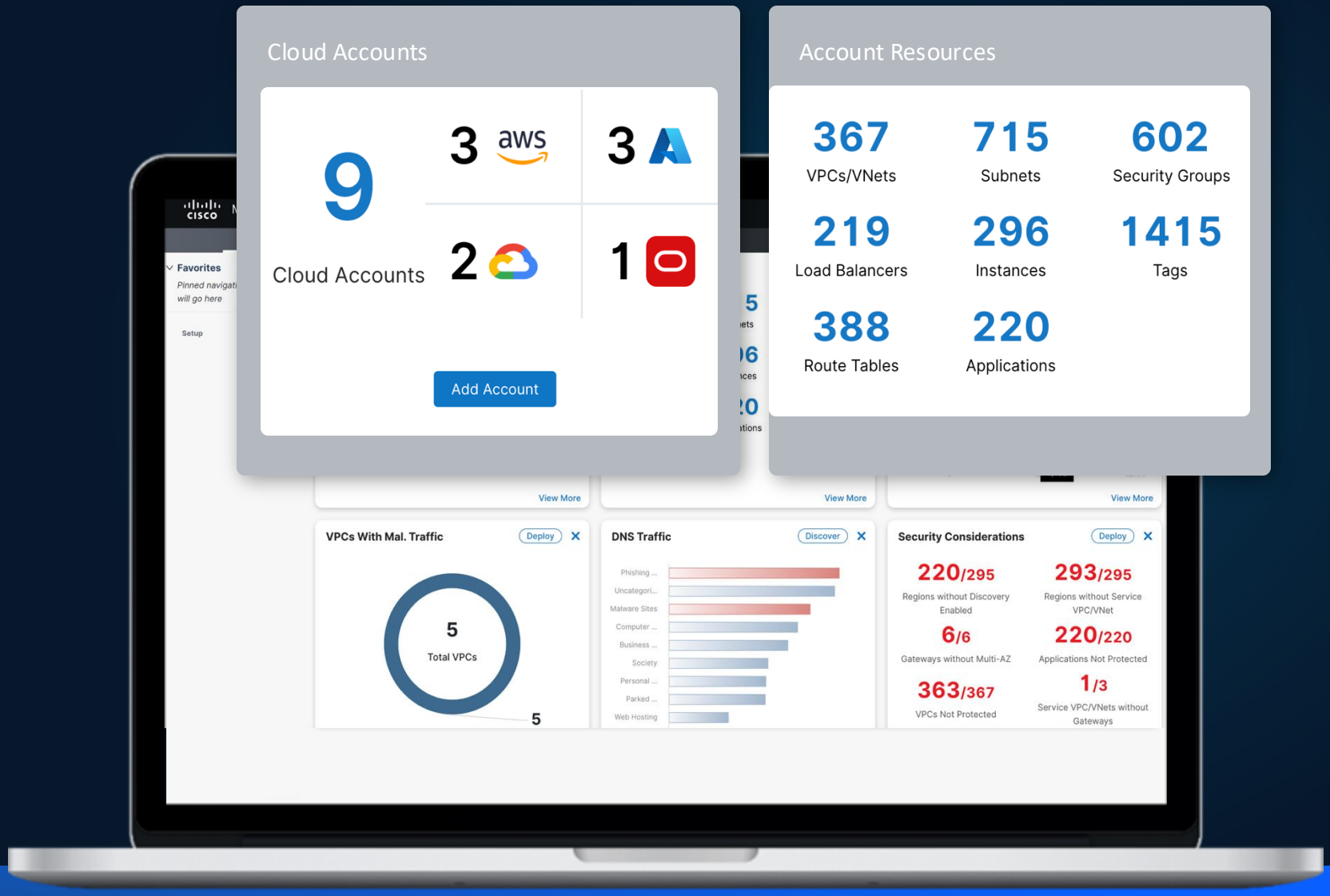


Complete visibility across clouds

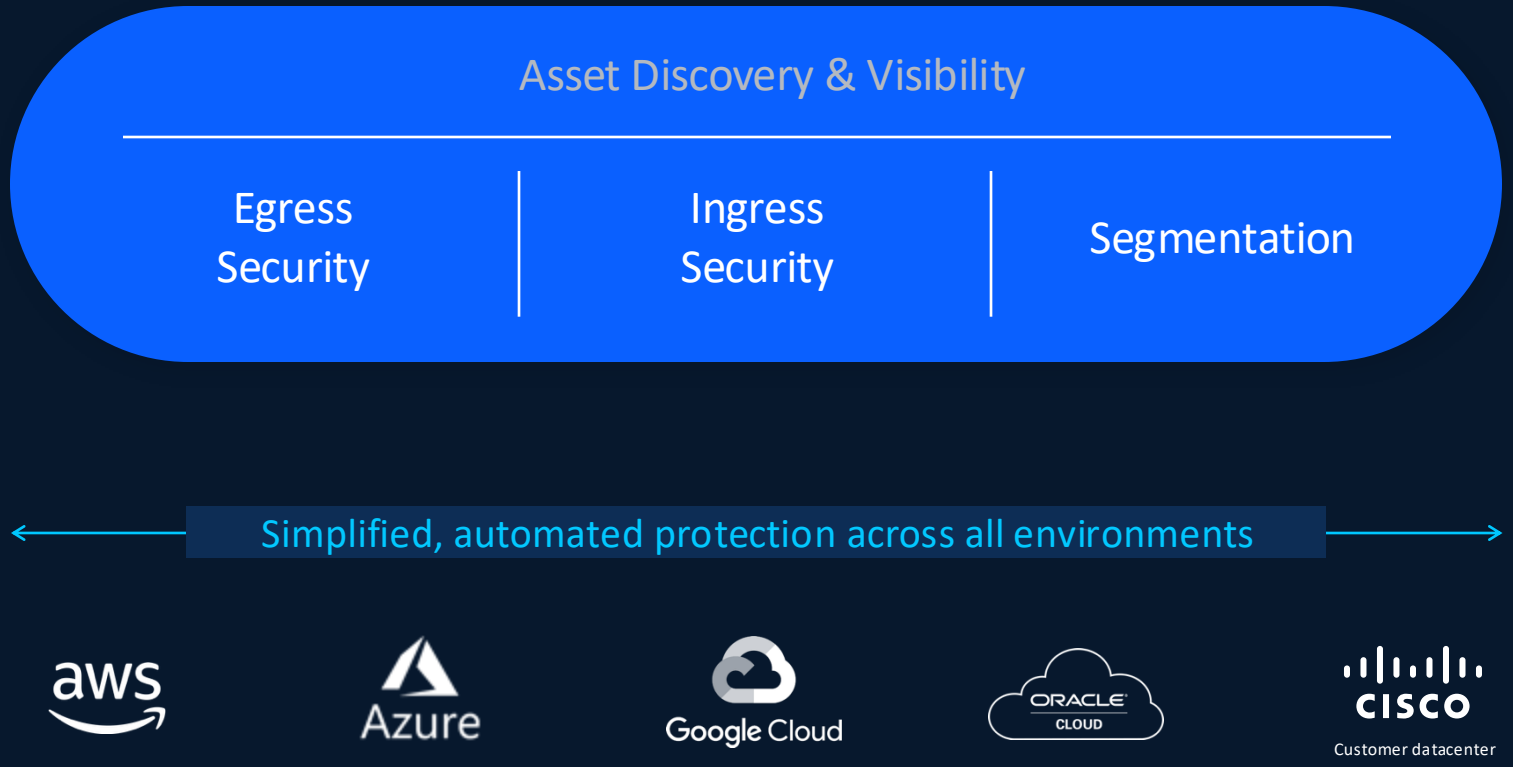
Quickly onboard new cloud accounts with automation

View all cloud assets and accounts in one place

Confidently place security controls where needed



Cisco Multicloud Defense



Unmatched Agility

Cloud-native design; built-in automation and orchestration

Reduced Risk

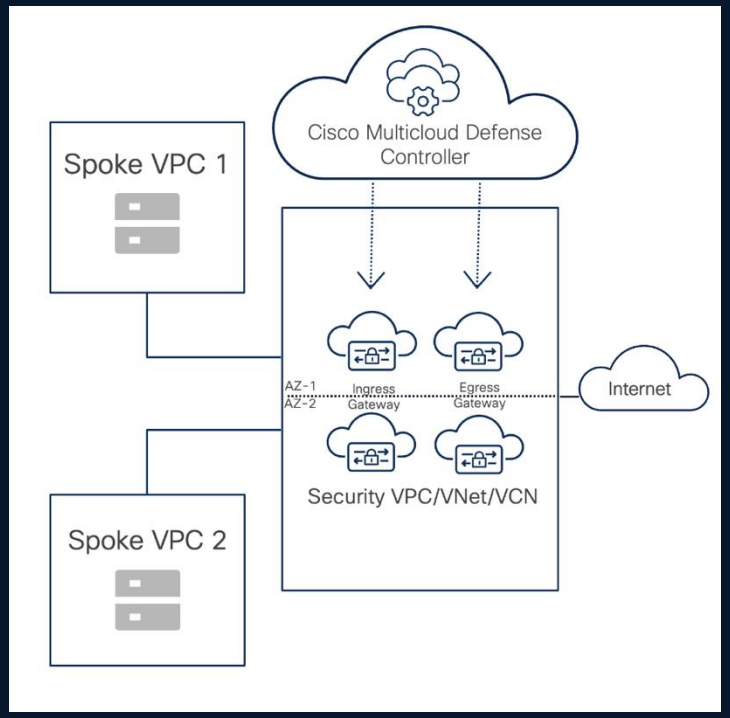
Unified security controls across clouds managed in one place

Lower Cost

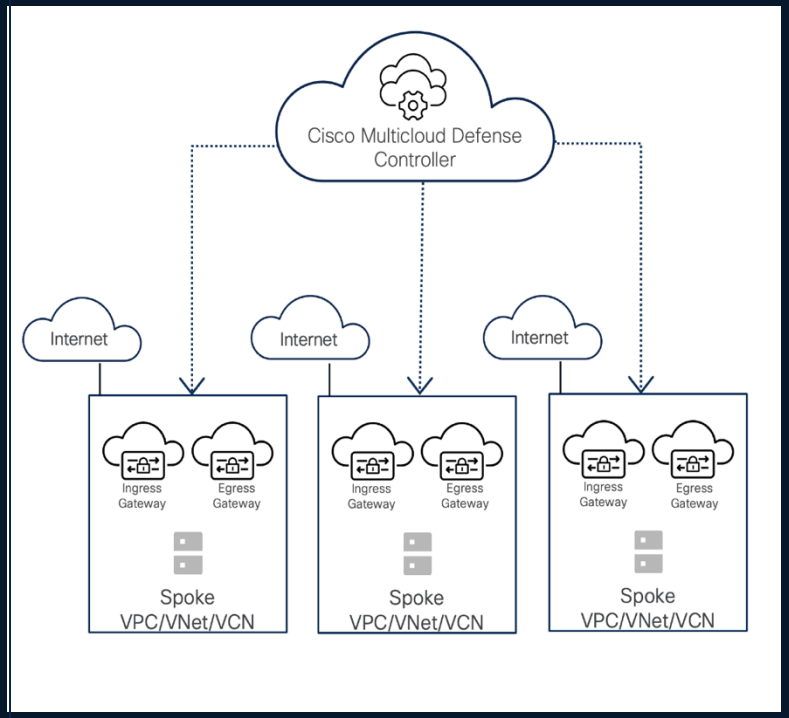
Replace multiple redundant tools; protect faster, train less

Security Models

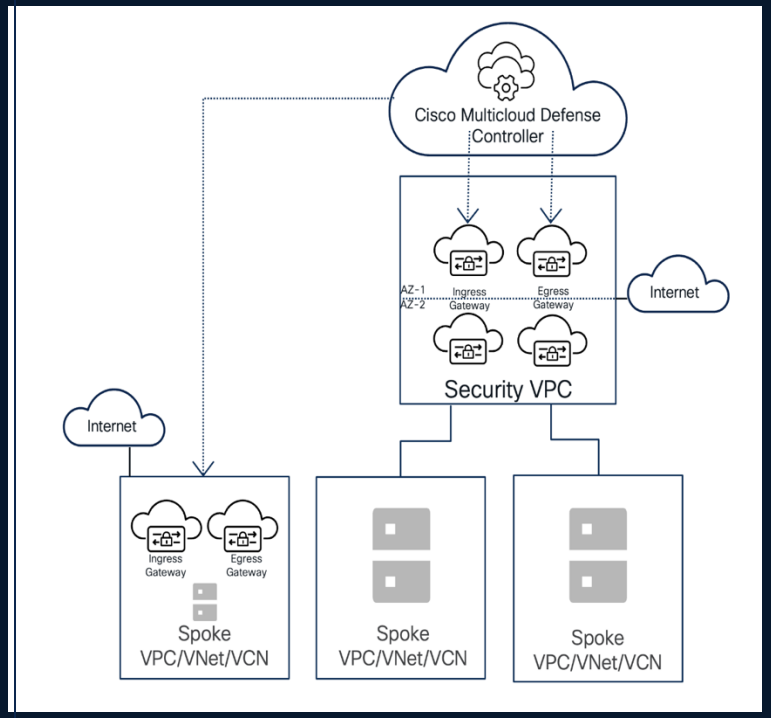
Centralized Security Model



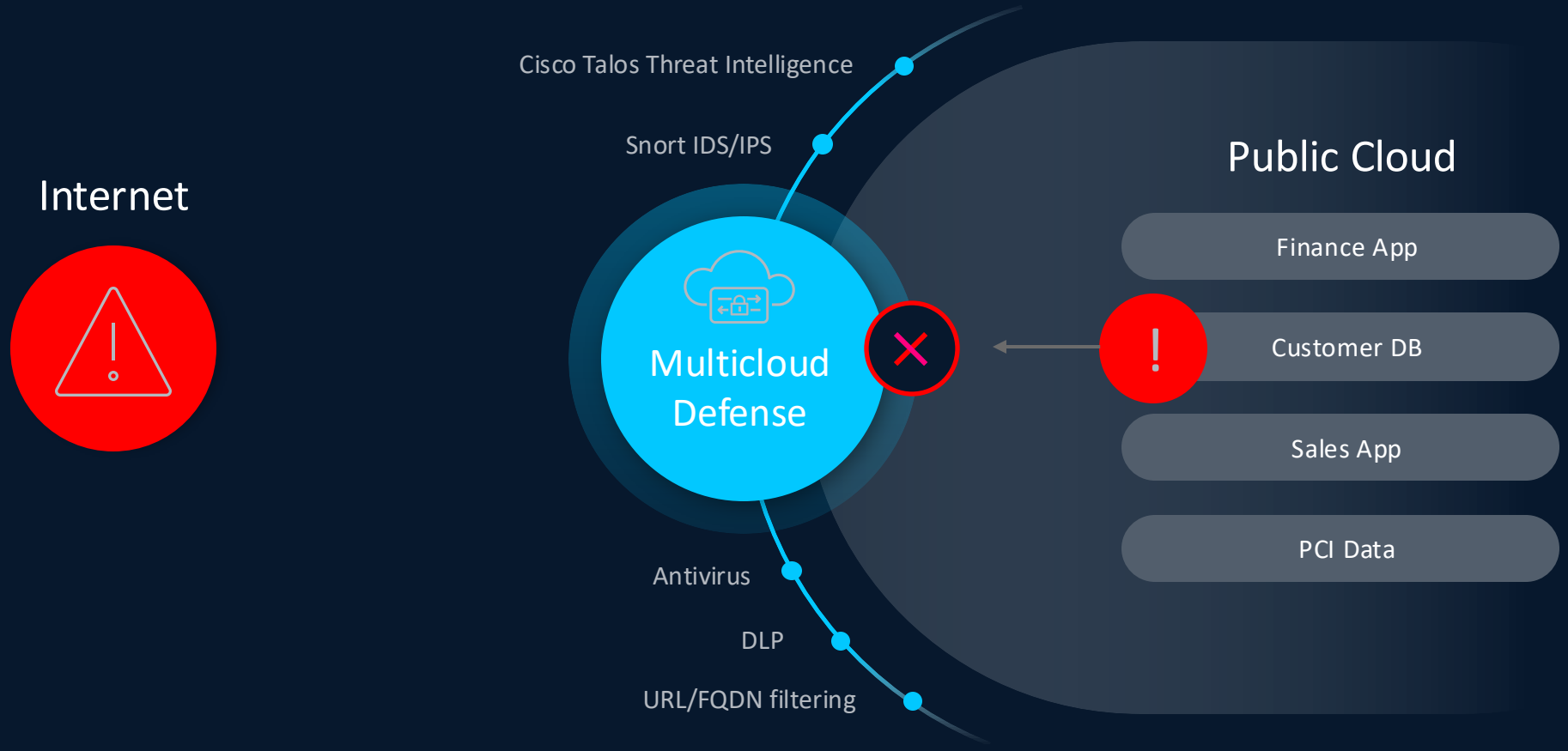
Distributed Security Model



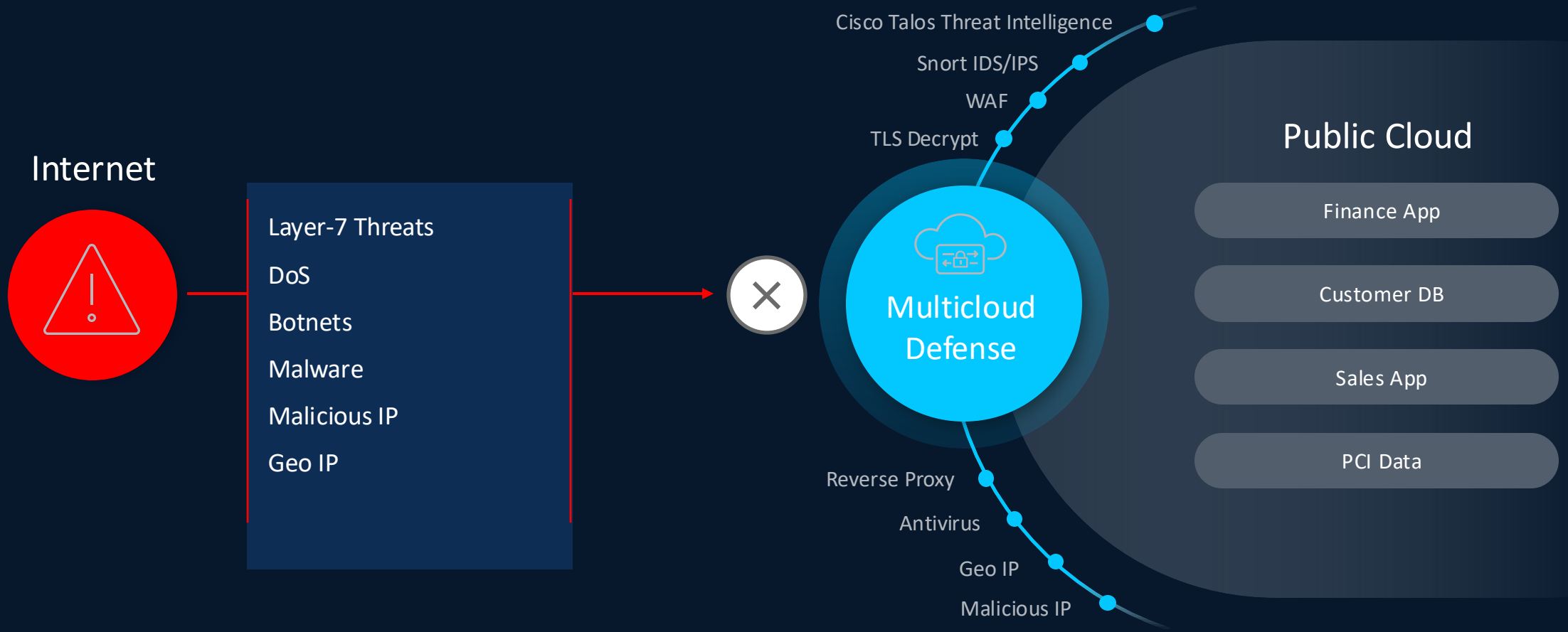
Combined Security Model



Strong and consistent egress security



Ingress security blocks inbound threats



CISCO Connect

HyperShield

Cisco Hypershield

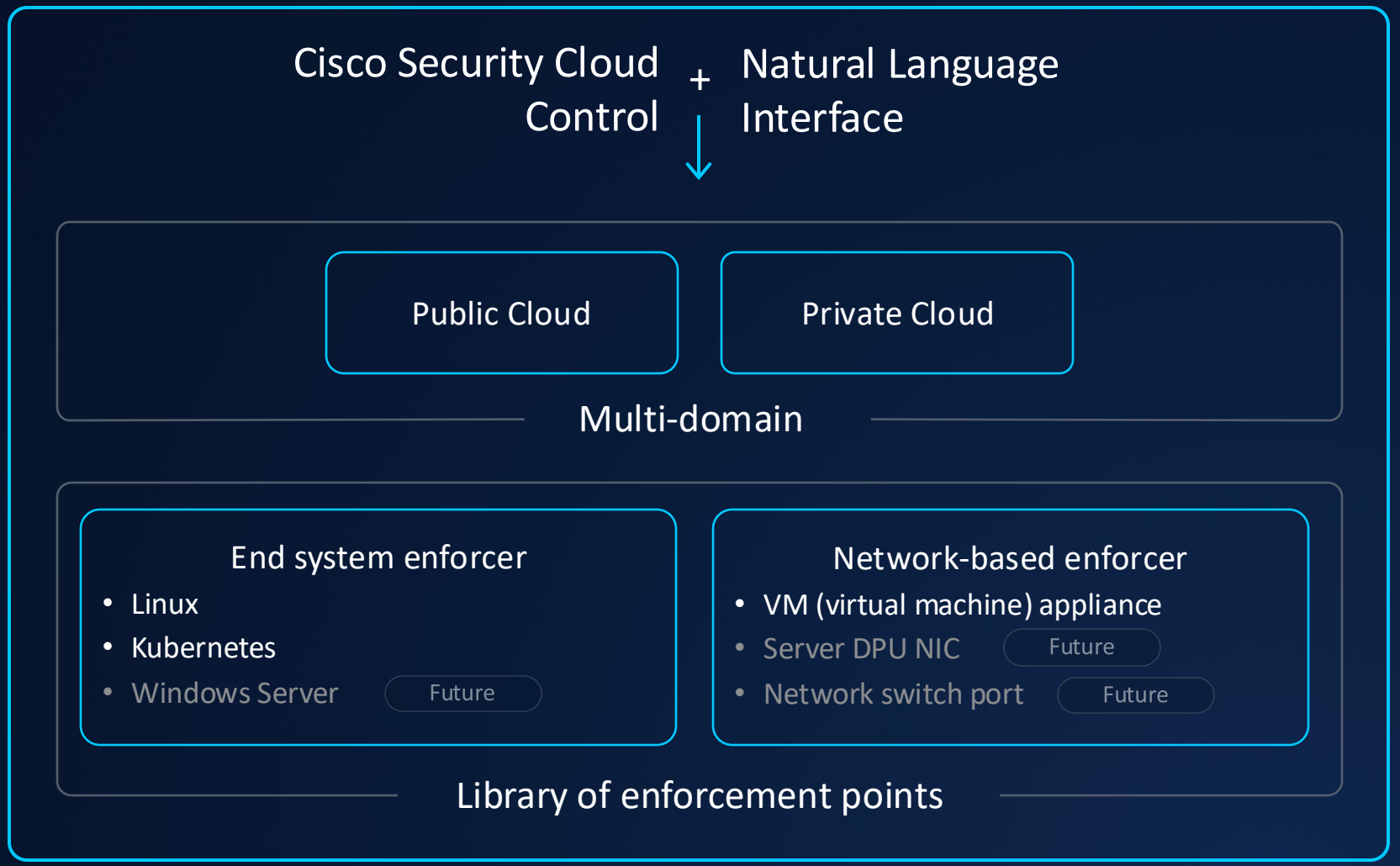
Manage globally, enforce locally

Includes

- Unified management
- Single global policy
- Intelligent placement of shields
- Integrations with cloud/app/infra metadata

Environments

- Kubernetes
- Cloud – Private/Public
- On-prem



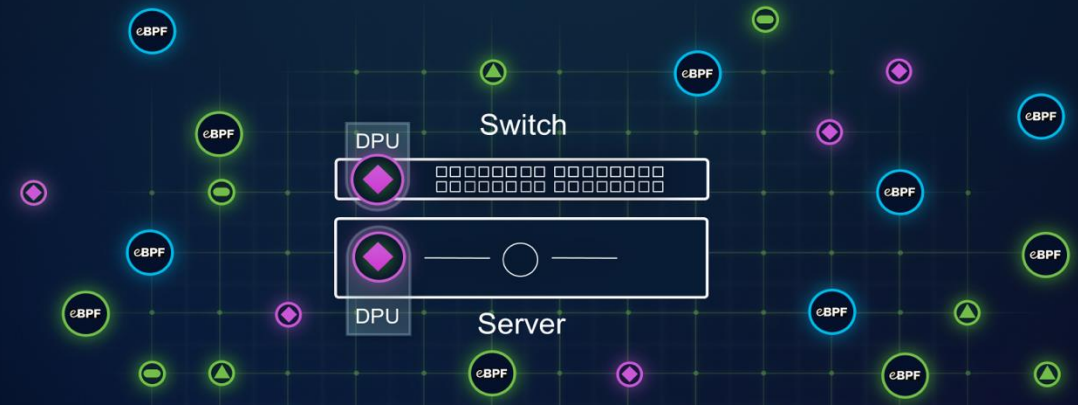
Hypershield Enforcement Points

They can be used separately or can augment each other
Managed from Cisco Cloud Management (Security Cloud Control)

Agent Enforcement Point

Autonomous segmentation | Distributed exploit protection

Network Enforcement Point



Security fused into the network
Hypershield service on Cisco Smart Switches

Transform Your Network Security using Cisco Smart Switches integrated with Cisco Hypershield

N9324C-SE1U

24-port 100G

- Cloud Edge, Zone-Based segmentation, DCI, Top-of-Rack
- 2.4T switch throughput, 800G services throughput
- Silicon One E100 ASIC + AMD DPUs
- Shipping now, Hypershield Target Initial Product Readiness: end of July'25

NEW

N9348Y2C6D-SE1U

48-port 25G, 6-port 400G, 2-port 100G

- DC Top-of-Rack
- 3.8T switch throughput, 800G services throughput
- Silicon One E100 + AMD DPUs
- Target Limited Orderability: July ‘25*

NEW

Cisco C9350

48/24 ports 10G/mGig, network-modules, 90W UPoE

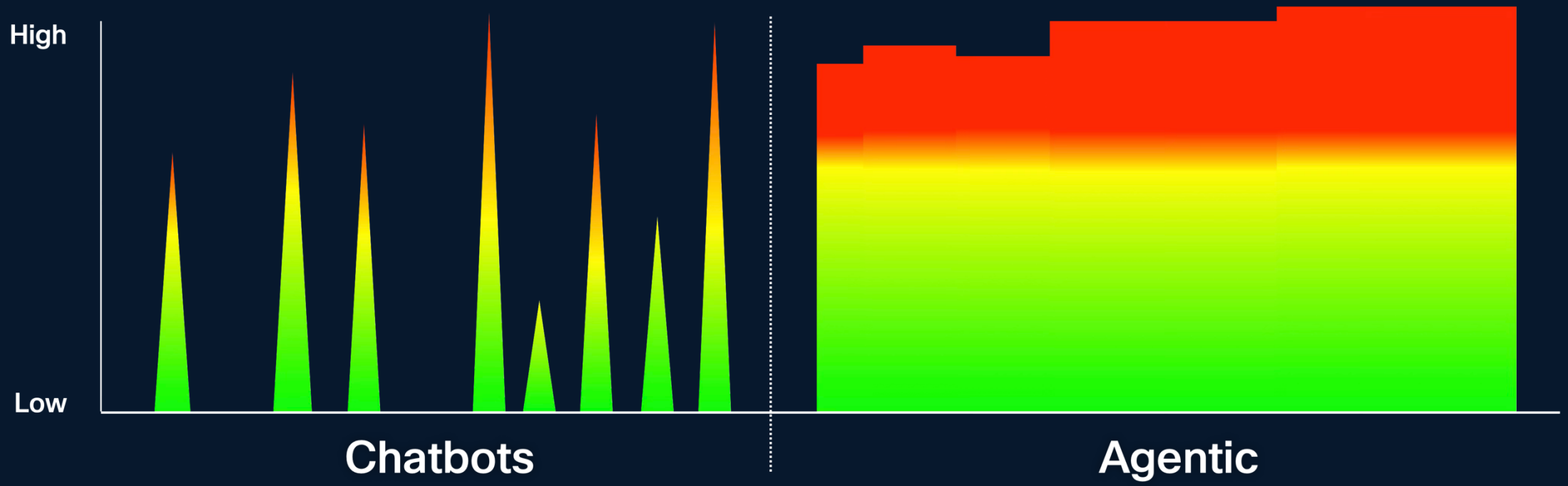
- Campus
- 1.3T (800G stacking, 500G for switch) throughput
- Silicon One E100 + Security co-processor
- Target Orderability: June ’25*

© 2025 Cisco and/or its affiliates. All rights reserved.

* Hypershield capabilities are with appropriate licensing and planned for delivery over time

Inferencing demand

Power I Compute I Networking



CISCO Connect

Isovalent

From Open-Source to Enterprise Platform

Open-Source Leadership

- **Creators and maintainers of Cilium**, the leading cloud-native networking project.
- **Creators of Tetragon**, the eBPF-based runtime security and observability engine.
- **Key contributors to the eBPF ecosystem**
- Powering technologies **trusted by hyperscalers like AWS, Google, and Microsoft.**
- **Backed by a vibrant open-source community** and CNCF ecosystem.

ISOVALENT
now part of cisco

Enterprise-Ready Platform

- **Hardened** enterprise platform
- **Enterprise features** for production use
- Enterprise-grade **support and SLAs**
- **Built-in capabilities** for compliance, threat detection, and forensics.
- **Trusted by regulated industries** and global enterprises.

cisco

CISCO Connect

AI Defense

Security for AI

Using AI Apps

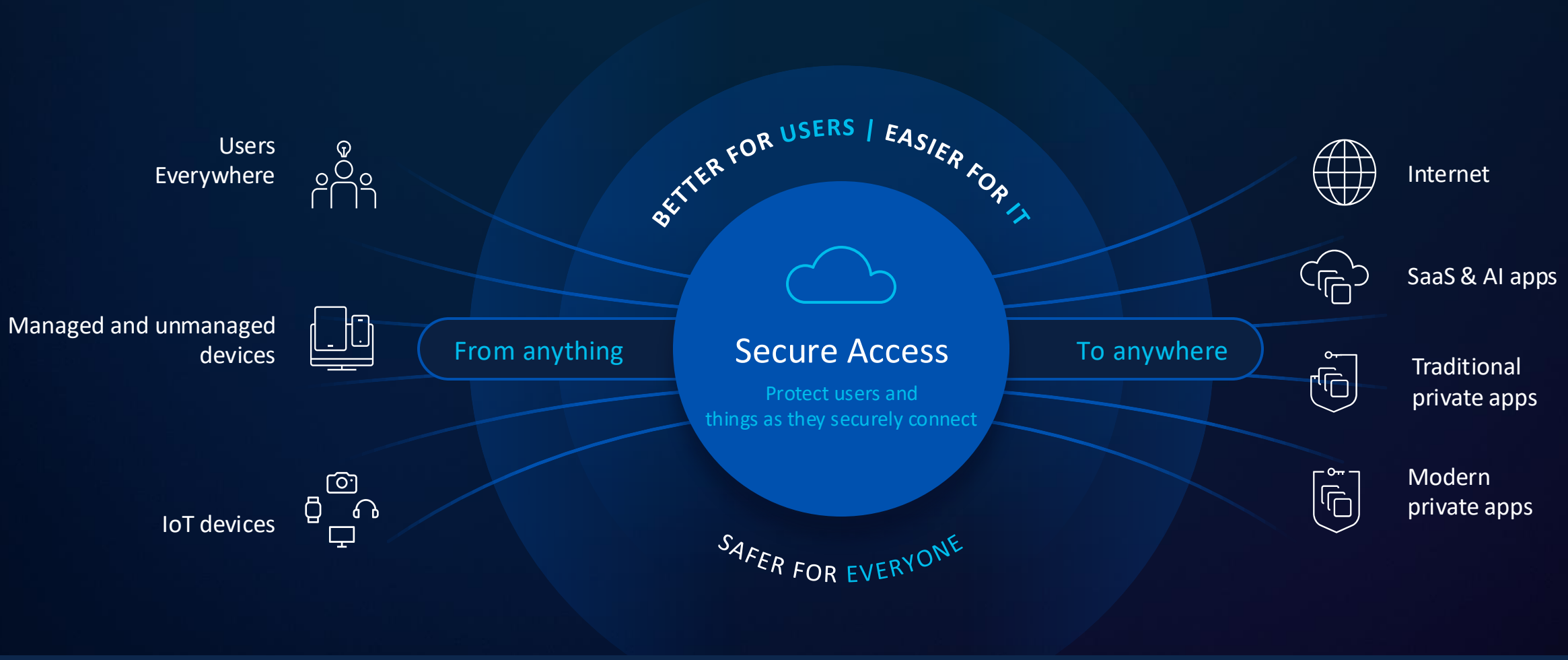
Developing AI Apps

CISCO Connect

SASE – Remote Employee

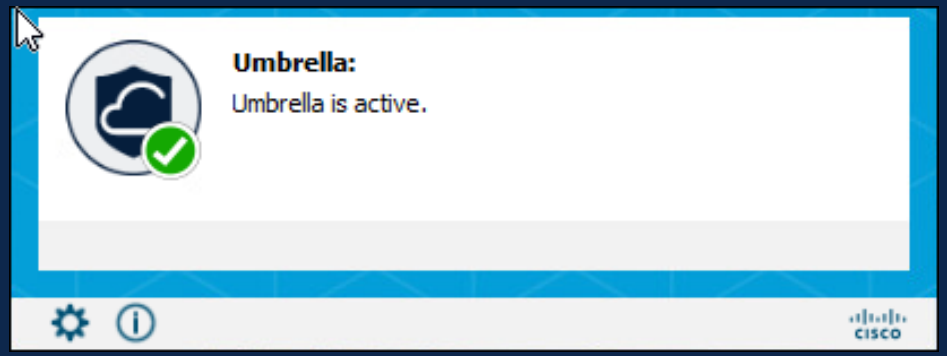
Cisco Secure Access

Converged cloud-native security grounded in zero trust



Remote | Campus | Branch | Airplane | Oil rig | Stadium | Field | •••

Roaming Security Module



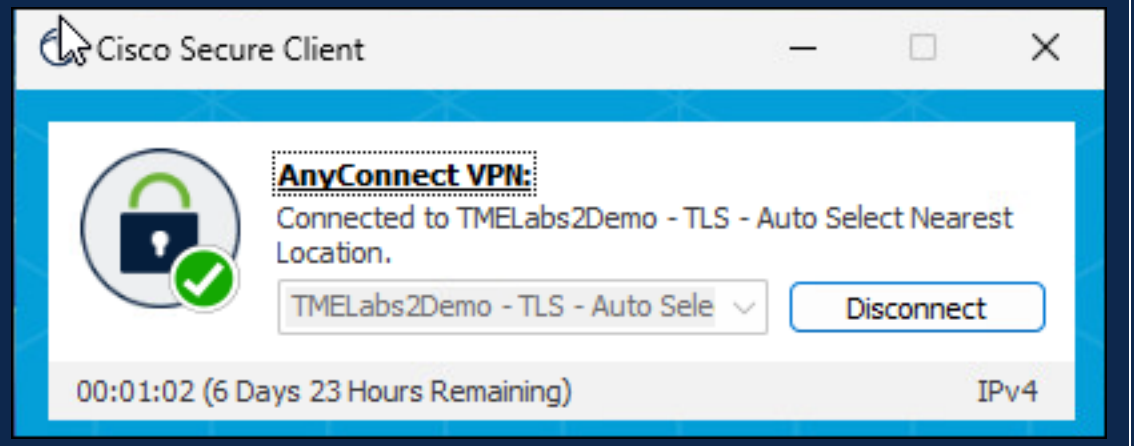
Cisco Secure Client 5.1 (formerly AnyConnect)

- Redirects DNS and HTTP(s)
  - DNS is sent over DNSCrypt
  - HTTP/s is converted to explicit proxy requests
  - HTTP only redirected on TCP 80/443
- Exceptions for destinations added in dashboard
  - Local domain suffix is excluded
  - Same exemptions apply to PAC file deployment
  - Download and deploy OrgInfo file from dashboard
- Dual stack is supported but not native IPv6
- Authentication occurs using UPN of the logged-in user

https://docs.sse.cisco.com/sse-user-guide/docs/roaming-security-module-requirements

https://docs.sse.cisco.com/sse-user-guide/docs/download-the-orginfo-json

Remote Access VPN

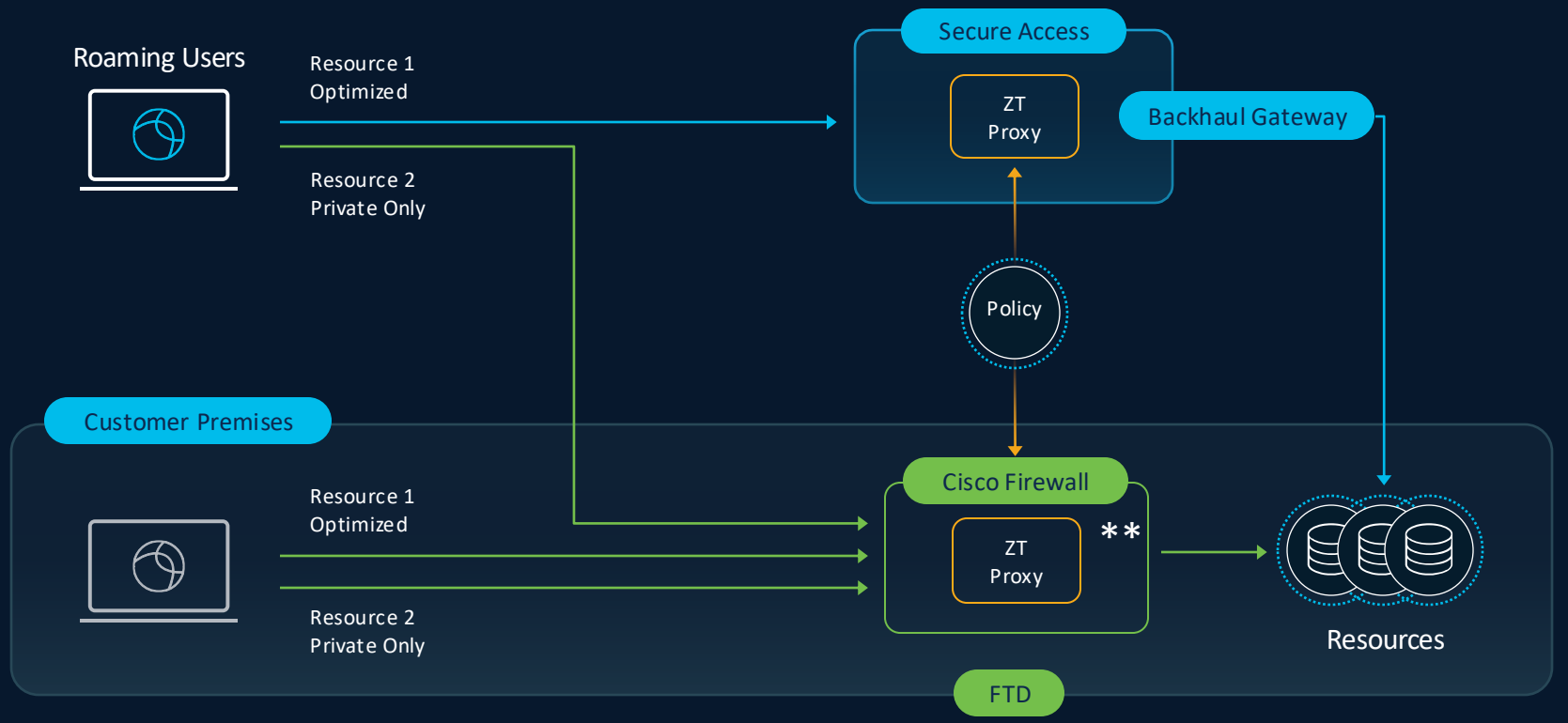


Cisco Secure Client 5.1 (formerly AnyConnect)

- Full or split-tunnel options are available
- Same deployment as the private access use-case
- Web traffic is evaluated by Cloud Firewall and Secure Web Gateway
  - Snort IDP/IPS
  - Layer 3-7 firewall rules
  - Data Loss Prevention
  - Anti-malware
  - Tenant controls
  - CASB
- Non-web traffic is evaluated by Cloud Firewall
  - Snort IDP/IPS
  - Layer 3-7 firewall rules

Hybrid Private Access for flexible enforcement

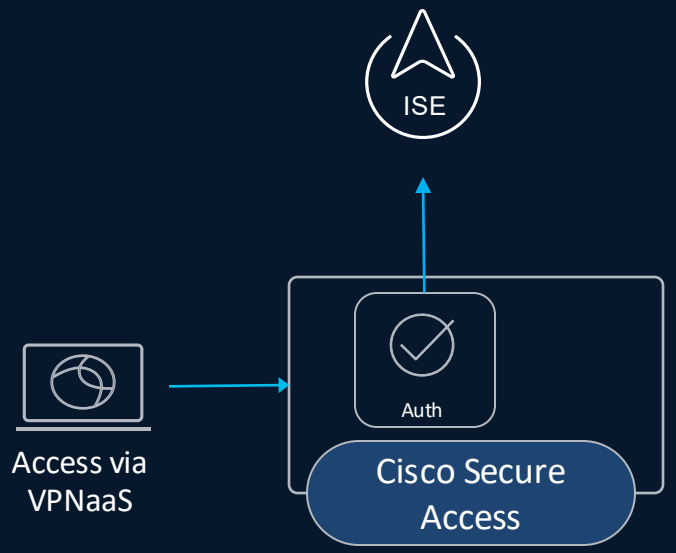
- Single set of ZTNA policies used in cloud and on-premise



** Roadmap: policy enforcement on 8k routers

ISE integration with Secure Access VPNaaS

RADIUS authentication, in addition to SAML authentication



- Cisco Identity Services Engine (ISE) or 3rd Party RADIUS supported
- AAA or authorize only
- Up to 8 servers within a single server group
- ISE posture supported (optional)
- SGT assignment via authorization

CISCO Connect

Security Cloud Control

Firewalling needs to evolve to meet today's challenges

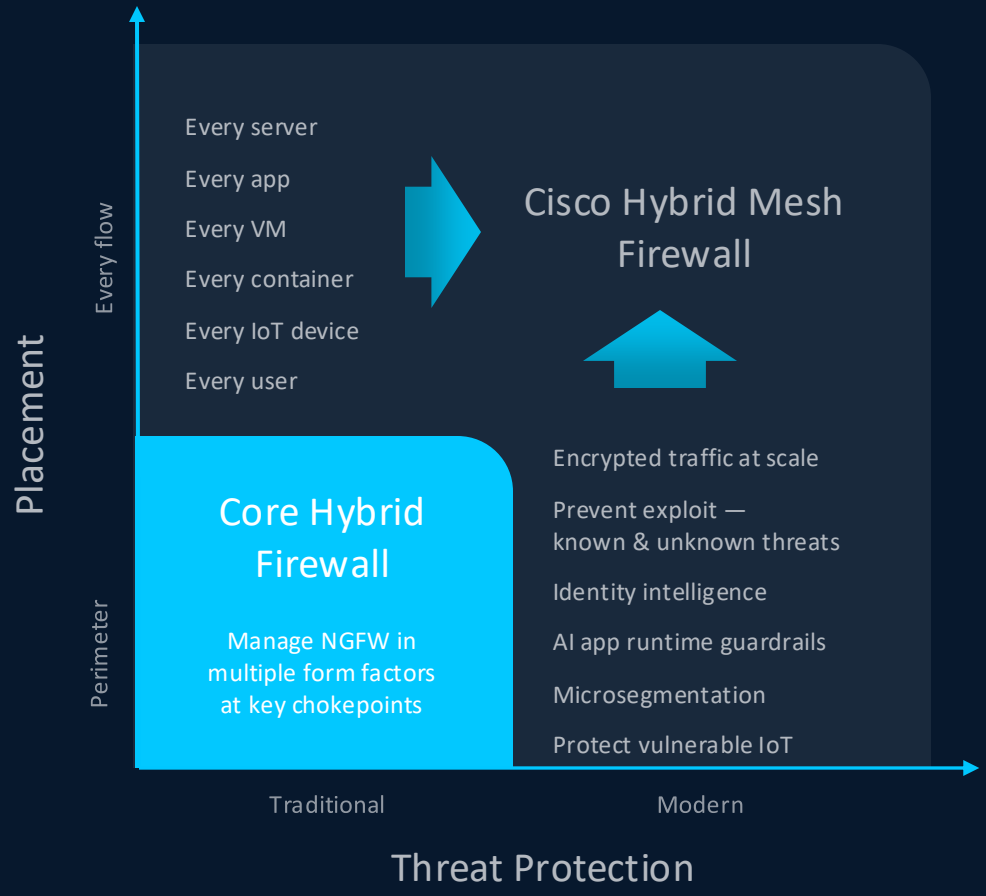
Highly distributed applications	Nothing can be trusted	More vulnerabilities, exploited faster

Our North Star

Make it easy for organizations to

- **Reduce** attack surface
- **Prevent** compromise
- **Stop** lateral movement

in the modern data center, cloud, campus, and factory



Hybrid Mesh Firewall (Segmentation as a Platform)

Write policy once, enforce across the mesh

Outcome focused Security Platforms

AI Powered Cisco Security Cloud: Cisco shines where Security meets the Network

AI-Ready Data Centers

Hybrid Mesh Firewall

Cloud Protection Suite

Future-Proofed Workplaces

Universal Zero Trust Network Access

User Protection Suite

Digital Resilience

Power Security Operations

Breach Protection Suite
Splunk Security

cisco

CISCO Connect

Thank you


CISCO