cisco Connect

GO BEYOND

#CiscoConnect

Hybrid Mesh Firewall

The Next Era of Firewalling

Martin Briand
Security Solution Engineer

Agenda

- Introduction
- Cisco Secure Firewall
- Hybrid Mesh Firewall Strategy and Innovations
- Conclusion

Securing modern applications is… “challenging”

Highly distributed

- Spanning data center, cloud
- Containers
- Automated deployments

Nothing can be trusted

- Need deep threat inspection and major trust boundaries AND
- Analyze every flow to limit lateral movement

Patching is hard

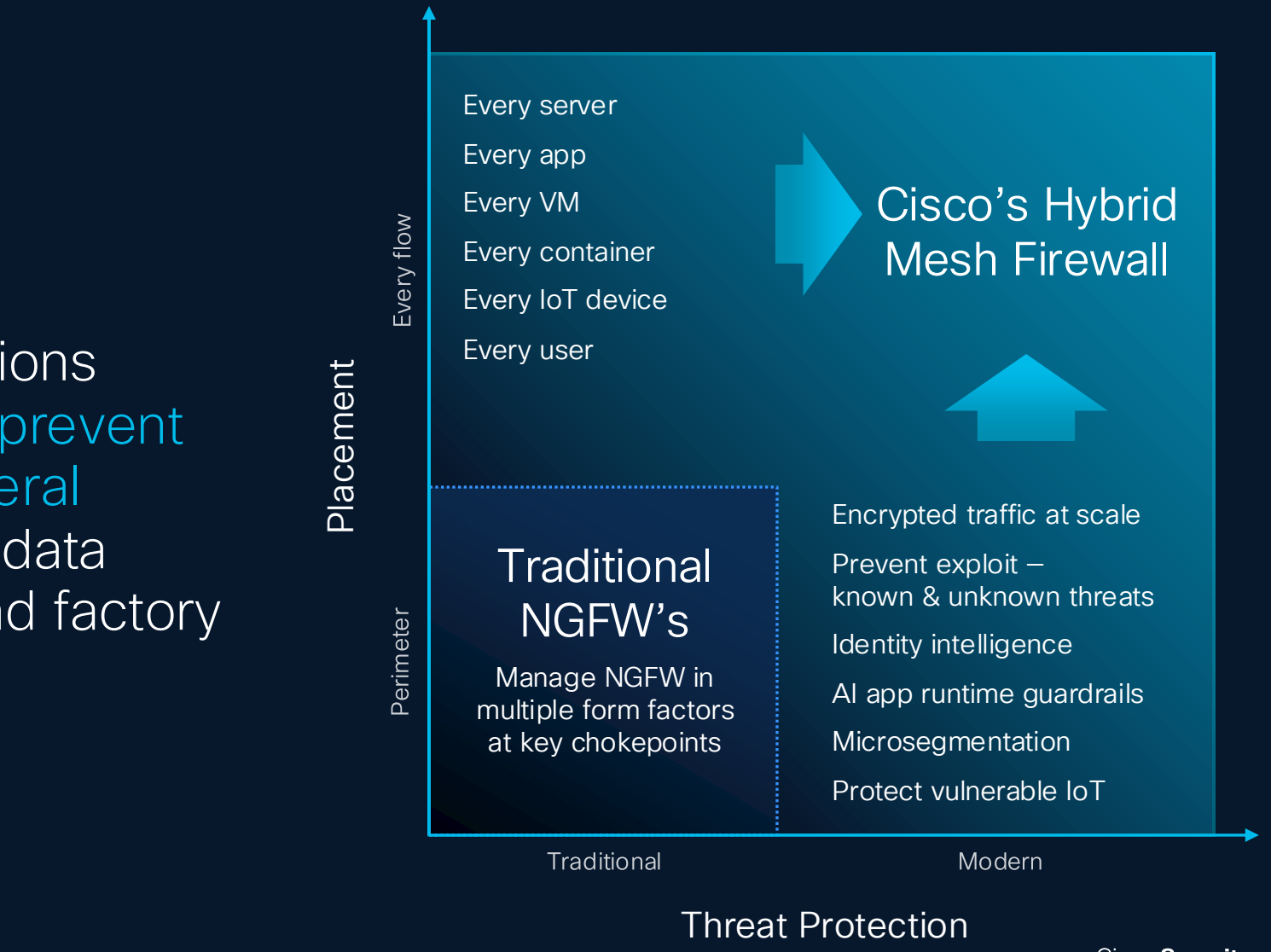
- High vulnerability rate
- Mitigation is too slow
- New exploits of AI models

AI increasing attack surface and attacker sophistication

Firewalling needs to evolve to meet today's challenges

Our North Star

Make it easy for organizations to reduce attack surface, prevent compromise, and stop lateral movement in the modern data center, cloud, campus, and factory



Cloud Protection Suite

Hybrid Mesh Firewall

Cloud Management (Security Cloud Control)

Major trust boundaries		Everywhere	
L7 Threat Protection	AI Model Protection*	Segmentation	Distributed Exploit Protection

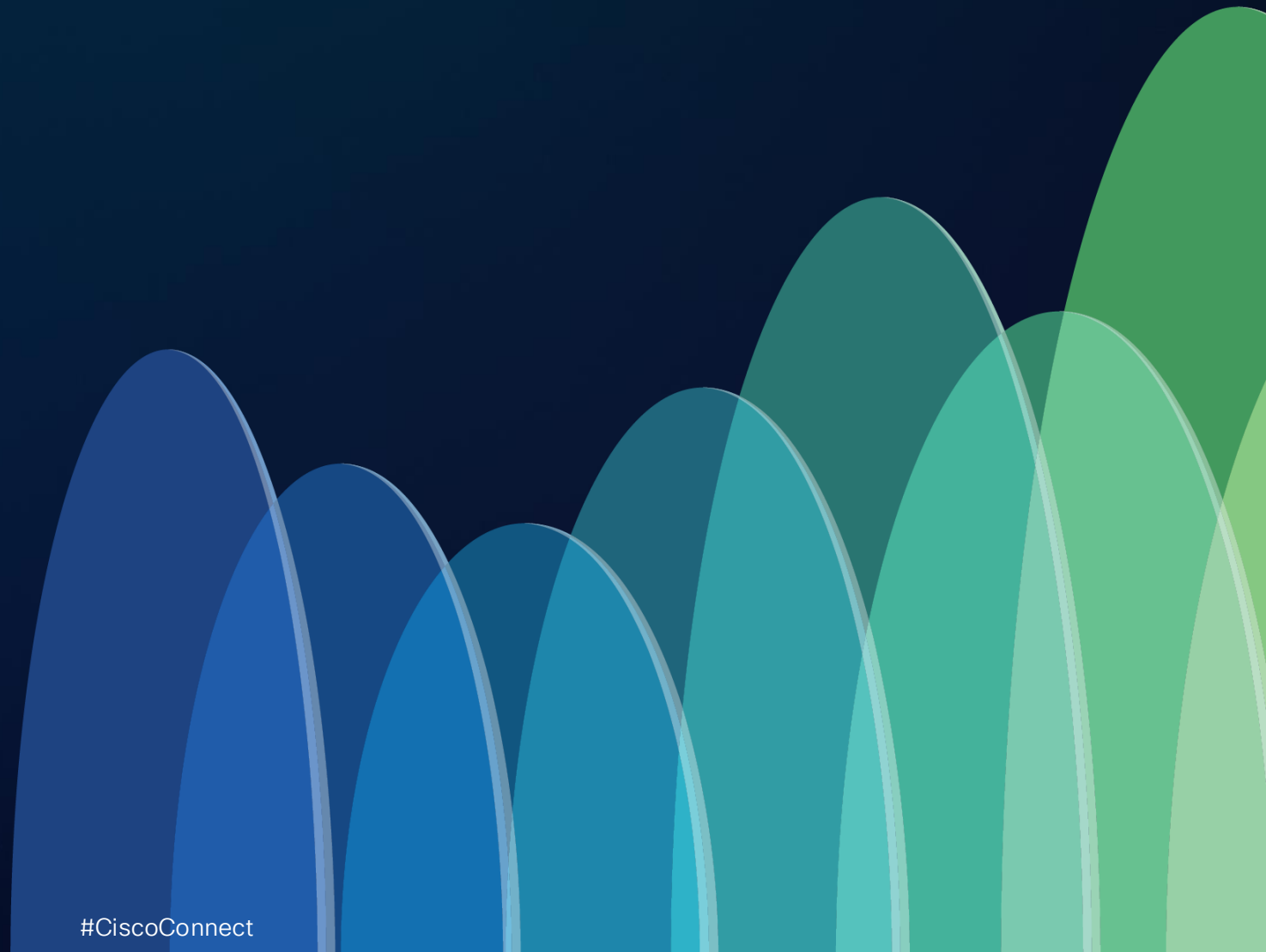
Secure Firewall	Multicloud Defense	Secure Access (FWaaS)*	3rd Party Firewall**	Hypershield (Smart Switch)	Hypershield (agent)	Secure Workload
						

Flexibility to swap components

*AI Defense and Secure Access are add-ons to Cloud Protection Suite
**Future

Some capabilities are planned but not yet available or guaranteed.

Cisco Secure Firewall



Who took 3rd place in the last World Cup in 2022?

Who is the 3rd largest cell phone maker in the world?

Who is the 3rd firewall vendor?

Market Analysts

Firewalls for every use case

ISA 3000 Series

≦0.4 Gbps NGFW

1010 Series

≦0.9 Gbps NGFW

1200 Series

≦18 Gbps NGFW

3100 Series

≦45 Gbps NGFW
16x Clustering

4200 Series

≦145 Gbps NGFW
16x Clustering

9300 Series

≦68 Gbps NGFW
16x Clustering

IOT / Branch / SASE

Campus / Data Center / Service Providers

Private Cloud

NUTANIX

KVM

openstack

vmware ESXi

HyperFlex

Public Cloud

aws

Google Cloud Platform

Microsoft Azure

rackspace technology

ORACLE CLOUD INFRASTRUCTURE

EQUINIX

Alibaba Cloud

alkira

Gov/IC Cloud

aws

Microsoft Azure

Google Cloud Platform

Cisco's Security Competitive Differentiation

0-day protection

Machine Learning from Talos

24x7 threat hunting with flexible engines that enable on-box real-time traffic inspection without relying on static signatures

Simplify Operations

Efficiency with real tasks

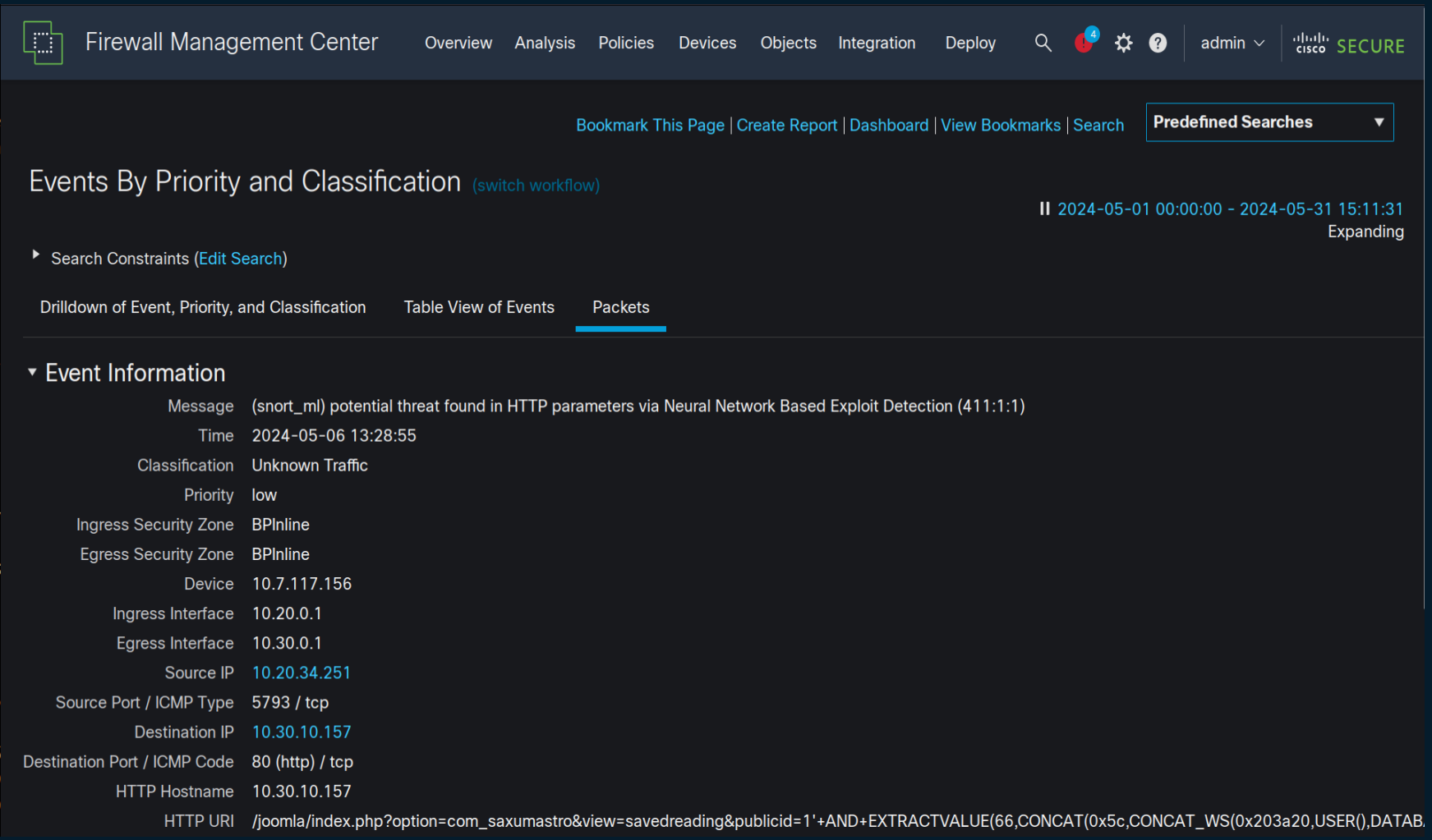
Decide how to deal with encrypted traffic – decrypt, bypass what's considered safe and inspect what's suspicious or can't be identified

Boost via cloud

Cloud Platformization

Cloud Assist for AIOps, Zero Touch Provisioning and AI Assistant

SnortML: Zero-day protection

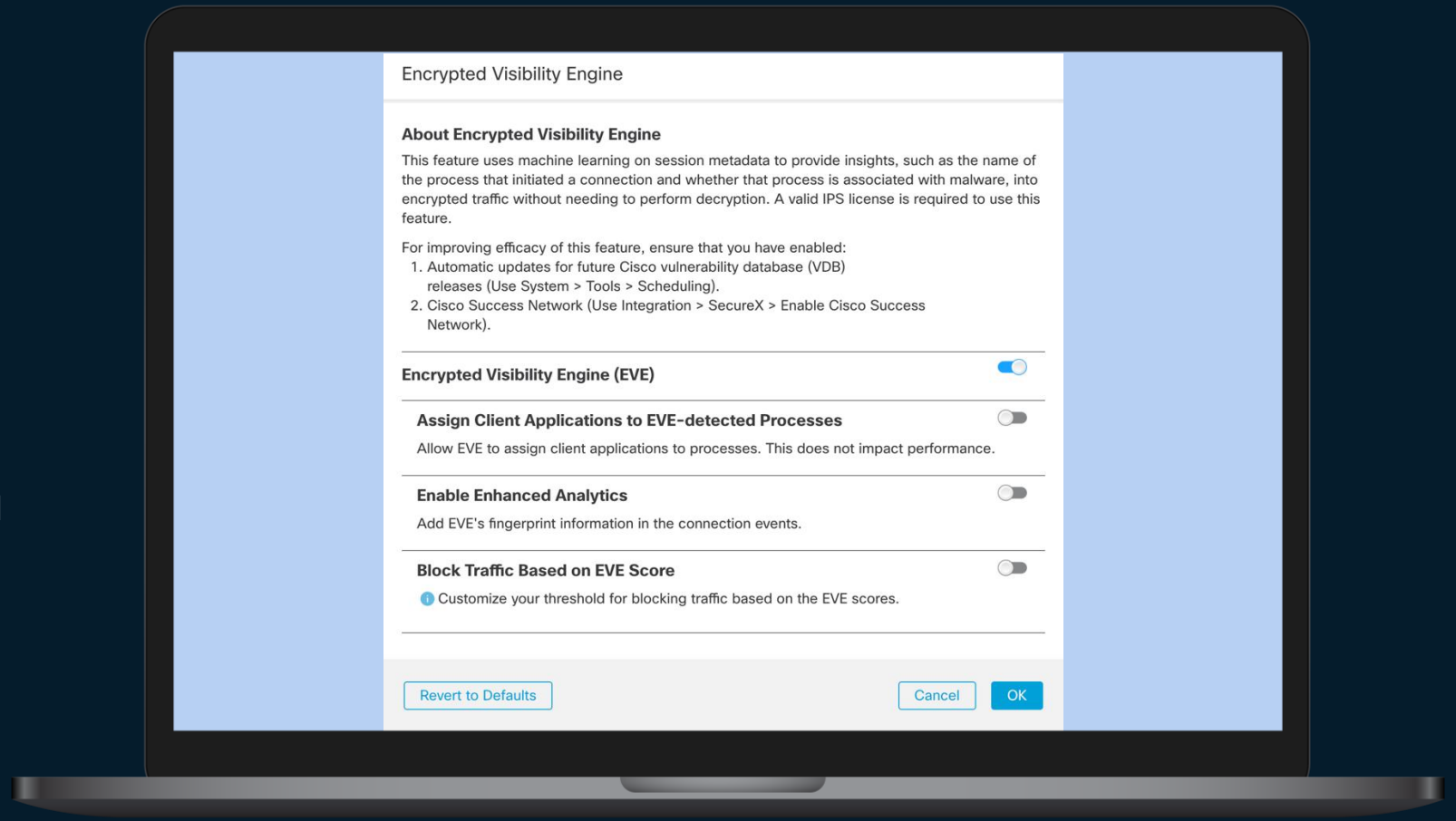


- A machine learning detection engine detecting known vulnerability types
- Proactive blocking of 0-day exploits
- Identifies variations of attacks

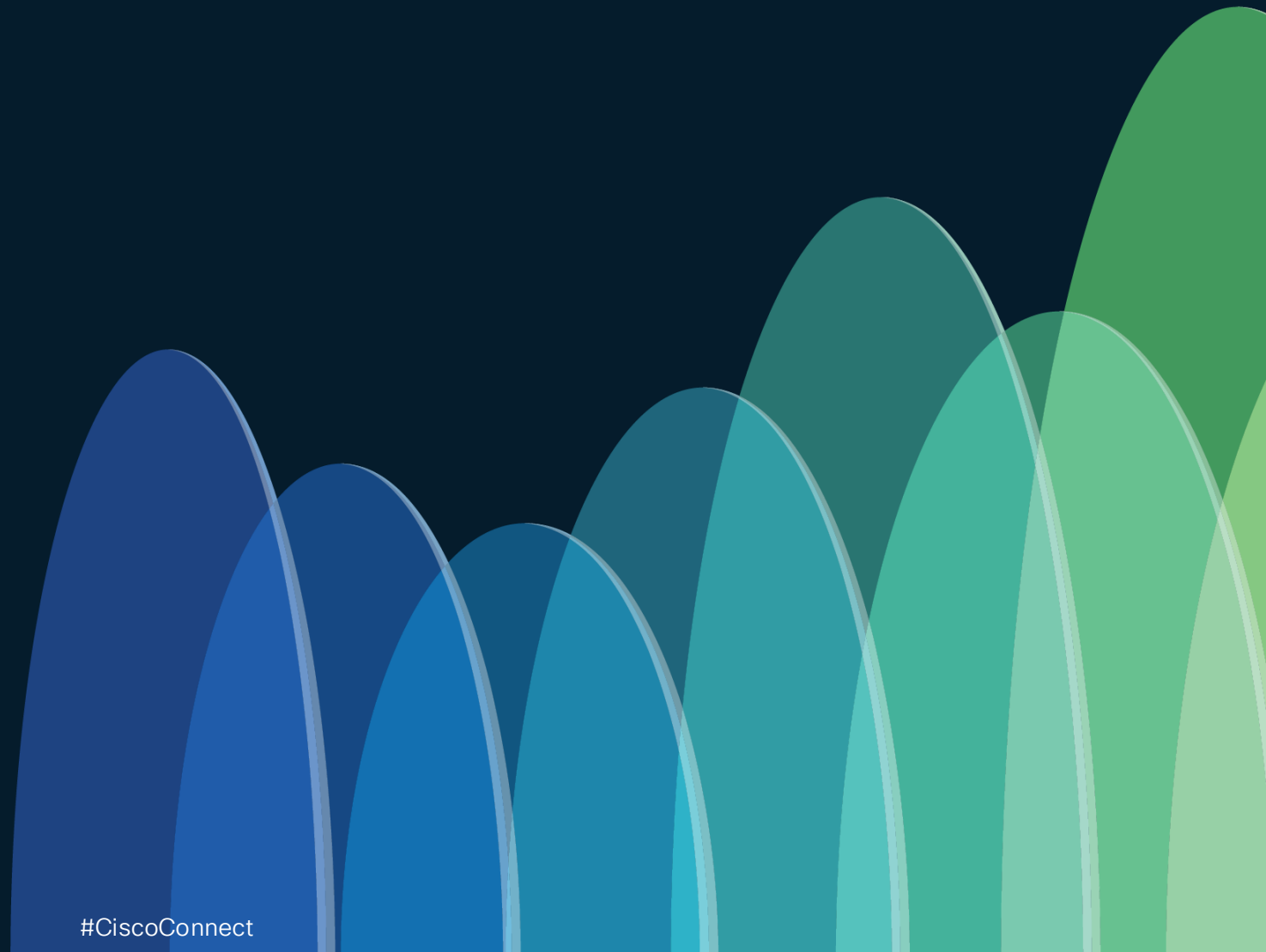
Gain control over encrypted threats

Without decryption, encrypted visibility engine 2.0 uses AI/ML to block encrypted threats for thorough security, simplicity, privacy and performance

- Simplify encrypted traffic inspection
- Preserved privacy and compliance
- Accelerate firewall performance
- Application visibility and control in encrypted streams
- TLS 1.3 and QUIC protocol support



Hybrid Mesh Firewall Innovations



Cloud Protection Suite

Hybrid Mesh Firewall

Cloud Management (Security Cloud Control)

Major trust boundaries		Everywhere	
L7 Threat Protection	AI Model Protection*	Segmentation	Distributed Exploit Protection

Secure Firewall	Multicloud Defense	Secure Access (FWaaS)*	3rd Party Firewall**	Hypershield (Smart Switch)	Hypershield / Isovalent	Secure Workload
						

Flexibility to swap components

*AI Defense and Secure Access are add-ons to Cloud Protection Suite
**Future

Some capabilities are planned but not yet available or guaranteed.

Security Cloud Control

Secure Firewall Threat Defense

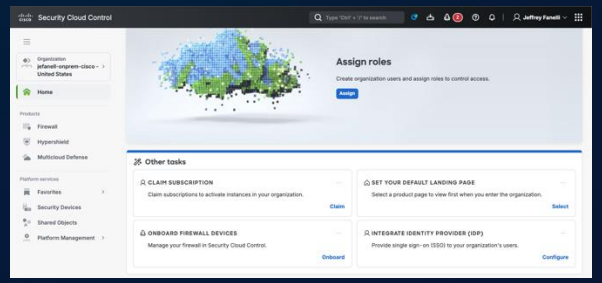
Multicloud Defense

Hypershield

Secure Access

Secure Workload

AI Defense



Integrations

Dynamic Objects

Licensing

Provisioning

Tenancy

User Management

RBAC

API Gateway

Unified AI Assistant

Common UI Experience

Extending Firewalling to the cloud, *natively*

NEW

- Cloud-agnostic automation and orchestration
- Comprehensive visibility of clouds, assets, and their risks
- Automatically deploy, scale, and heal, from Security Cloud Control
- Hourly price; unlike other offers based on size and bandwidth

Cisco AI Defense

AI Security Journey

EARLY ACCESS

Safely enable generative AI across your organization

Discovery

Uncover shadow AI workloads, apps, models, and data.

Detection

Test for AI risk, vulnerabilities, and adversarial attacks

Protection

Place guardrails and access policies to secure data and defend against runtime threats.

AI Defense

EARLY ACCESS

Recommended Actions

Protect applications (67)

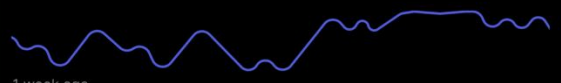
Secures sensitive data, prevents unauthorized access, and protects proprietary algorithms from theft or misuse.

Hide View →

Review increased app usage 3 days ago

Review sudden spikes in blocked events to avoid security risks.

ExternalChatBot Application
45MB +7%



1 week ago

Hide View →

Review third party apps (67) 3 days ago

Safeguards user privacy, prevents data breaches, and ensures compliance with security and regulatory standards.

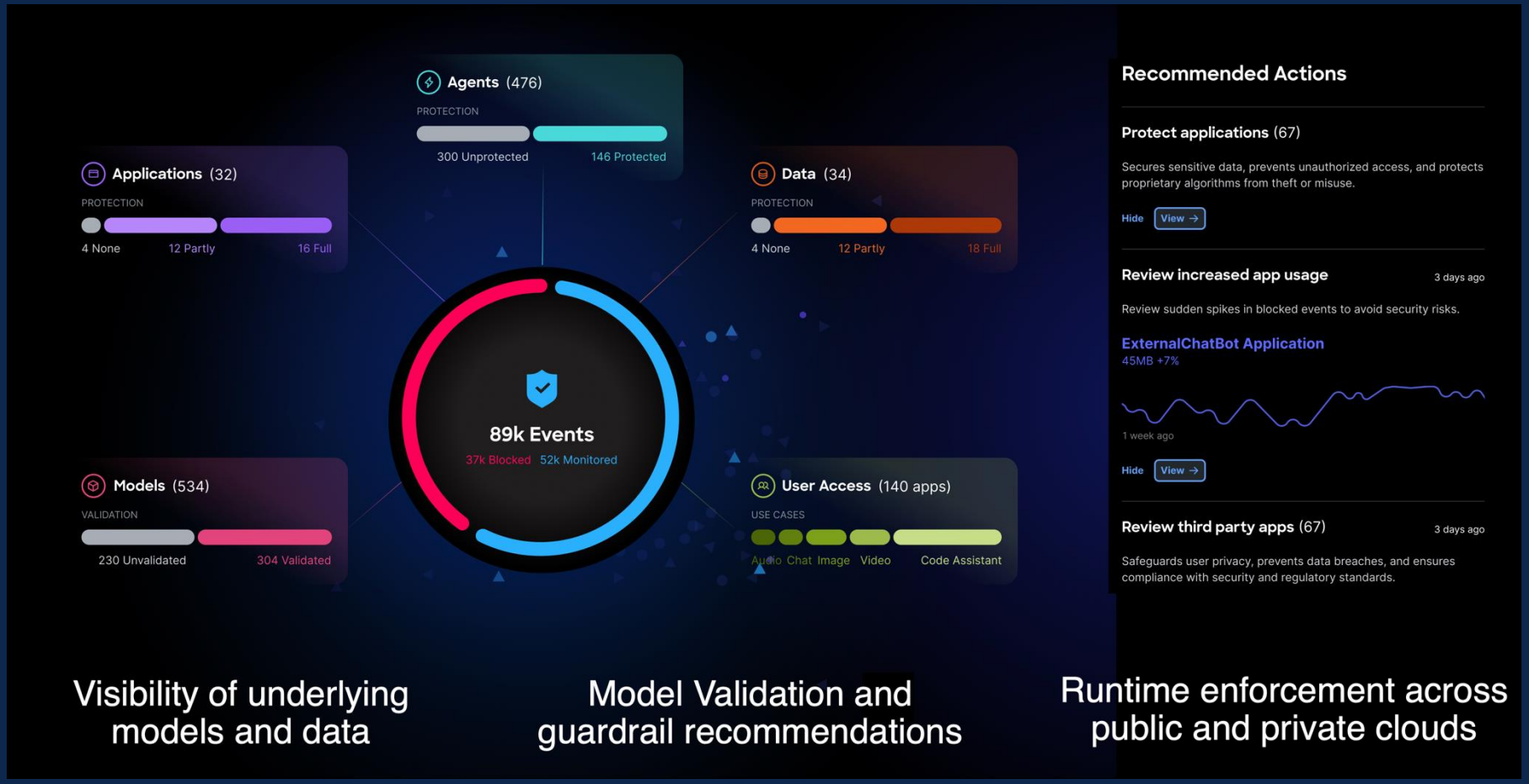
Visibility of underlying models and data

Model Validation and guardrail recommendations

Runtime enforcement across public and private clouds

Delivered via the Hybrid Mesh Firewall

EARLY ACCESS



Visibility of underlying models and data

Model Validation and guardrail recommendations

Runtime enforcement across public and private clouds

Cisco Security Cloud Enforcement Points

- Secure Firewall
- Secure Firewall Cloud
- Hypershield
- Secure Access

ISOVALENT

now part of **CISCO**

Isovalent
Enterprise Platform is the
industry-leading solution for
Kubernetes Networking
and Security

Isovalent is the eBPF-
powered foundation for
Cisco Hypershield
on Kubernetes,
public/private cloud VMs,
and bare-metal servers

Isovalent delivers a
consistent layer of
connectivity and security
that runs everywhere
across both
public & private clouds.

When Security meets the Network

Cisco Nexus 9000 Services Accelerated Switch (SAS) + Hypershield

EARLY ACCESS

Security
Hypershield

- Intelligent Security Policy placement
- Self-qualifying updates (Dual Dataplane)
- Unified architecture across workload and network enforcement – Public and private clouds

Compelling innovation

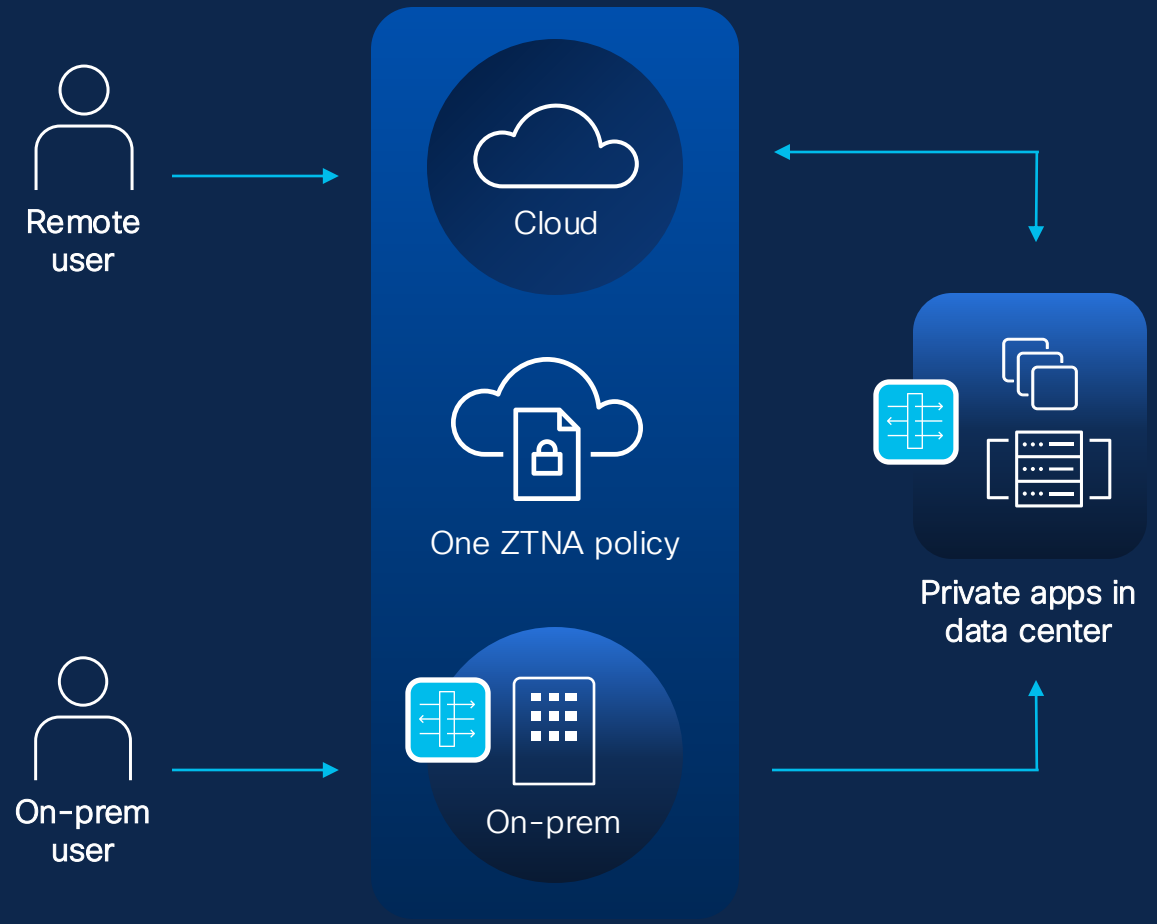
Network
Nexus

Nexus 9000 SAS

- Converge stateful services and network
- Built-in DPU hardware accelerator to scale, extend, or add stateful services
- Use Cases: Cloud Edge, Zone-based segmentation, DCI, and Top of Rack

Hybrid Private Access (UZTNA)

EARLY ACCESS



- Single ZTNA policy created and automatically applied from Security Cloud Control
- Cloud and on-prem firewall enforcement, including on-prem inspection for sensitive apps
- Reduced cost and latency when on-prem users access on-prem apps
- No additional infrastructure or purchase to implement

Hybrid Mesh Firewall - Summary

A security fabric for tomorrow

L7 Threat Protection

Segmentation

AI Model Protection

Distributed Exploit Protection

Only from Cisco

cisco Connect

GO BEYOND

#CiscoConnect