Firewalling for the AI era

Every connection. Every workload. Every time

Kirill Sulima, Security Solutions Engineer, Cisco GSSO

Softprom Baku Security Forum

April 2026

Cisco Security Cloud

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

Standard Hybrid Mesh Firewall

Unified Management

Physical Firewall

Virtual Firewall

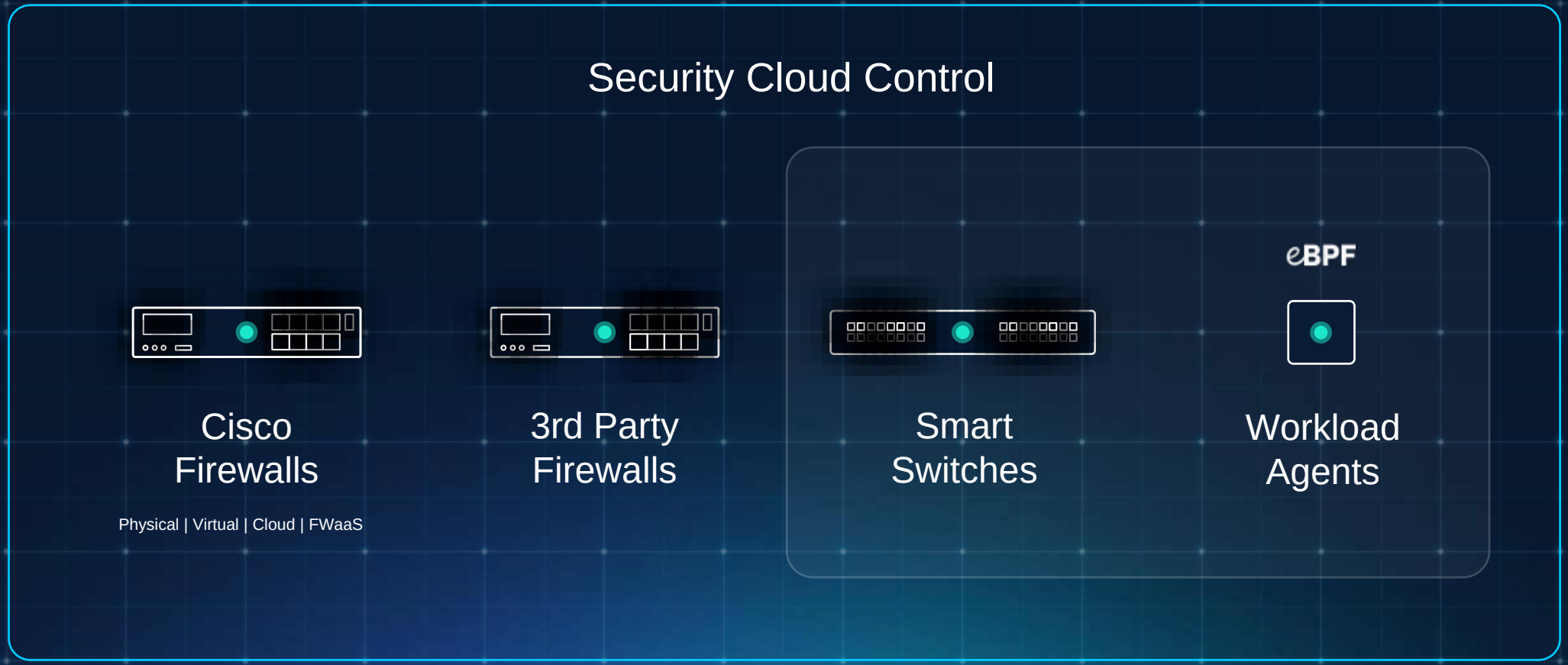
Cloud Firewall

Firewall as a Service

Managed as one

Cisco Hybrid Mesh Firewall

with hyper-distributed security



Define once, enforce everywhere

Cloud Protection Suite license

Flexibility to swap components

Gateways

Workloads

- Secure Firewall
- Multicloud Defense
- Secure Workload
- Isovalent Enterprise
- Hypershield

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

Industry recognition

Gartner

2025 Magic Quadrant for Hybrid Mesh Firewall

Visionary

IDC

2025 IDC MarketScape: Worldwide Enterprise Hybrid Firewall

Leader

Customer recognition

Gartner Peer Insights™

Network Firewalls

* vs Palo Alto Networks 4.6, Fortinet 4.7. All scores for last 12 months as of Oct 27,2025.

Customer projects we can solve **today**

- Threat Protection
- Network and Microsegmentation
- AI Security
- Kubernetes Security
- Exploit Protection


CISCO

Advanced threat protection

Preventing modern attacks

Unique capabilities unmatched by competitors

Early detection of zero days, encrypted threats

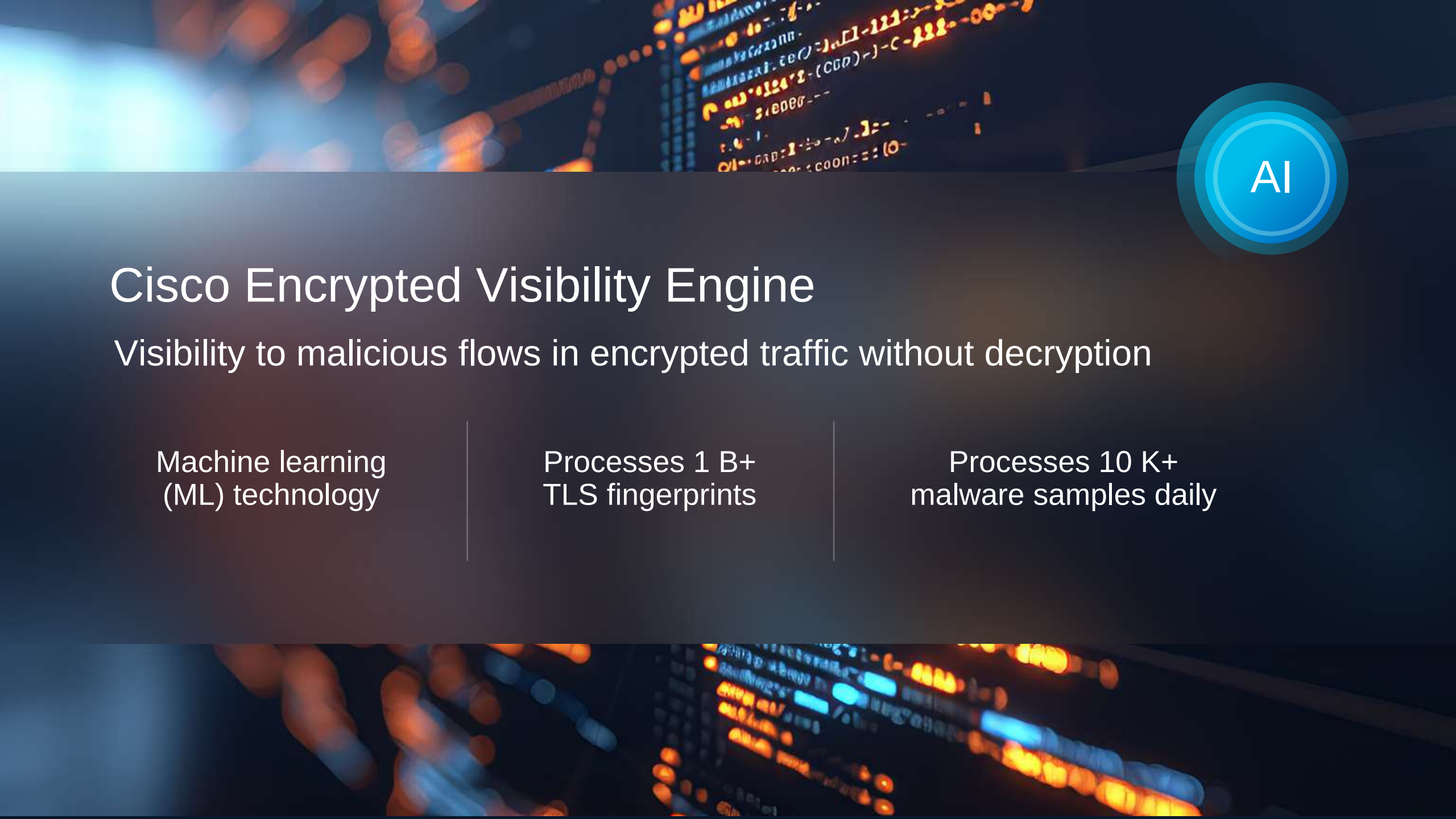
SnortML, Encrypted Visibility Engine

Cloud-native firewalling

Cloud agnostic automation, orchestration

Integrated segmentation

Scalable, identity-based macro & microsegmentation



Cisco Encrypted Visibility Engine

Visibility to malicious flows in encrypted traffic without decryption

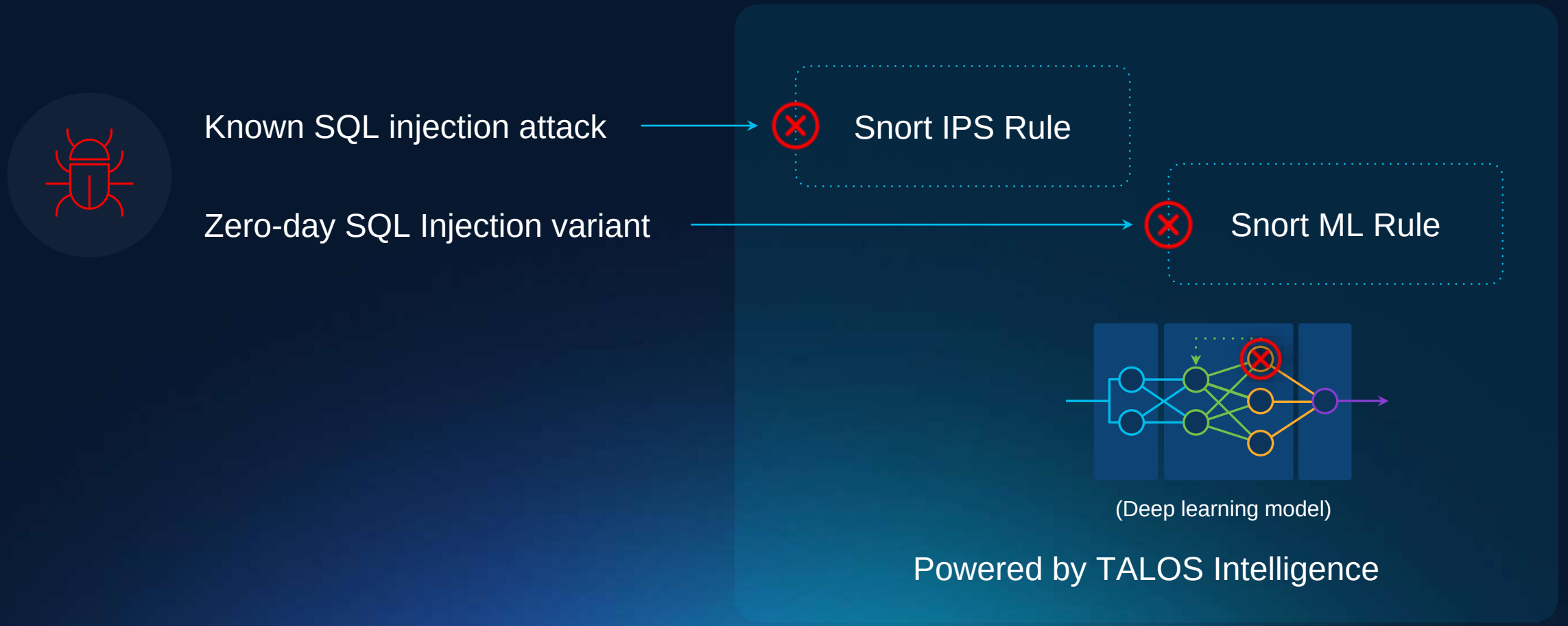
Machine learning (ML) technology	Processes 1 B+ TLS fingerprints	Processes 10 K+ malware samples daily

EVE changes the game on decryption

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

The leading IDPS, now with zero-day protection

Snort ML extends IDPS protection to unknown variants of common attacks

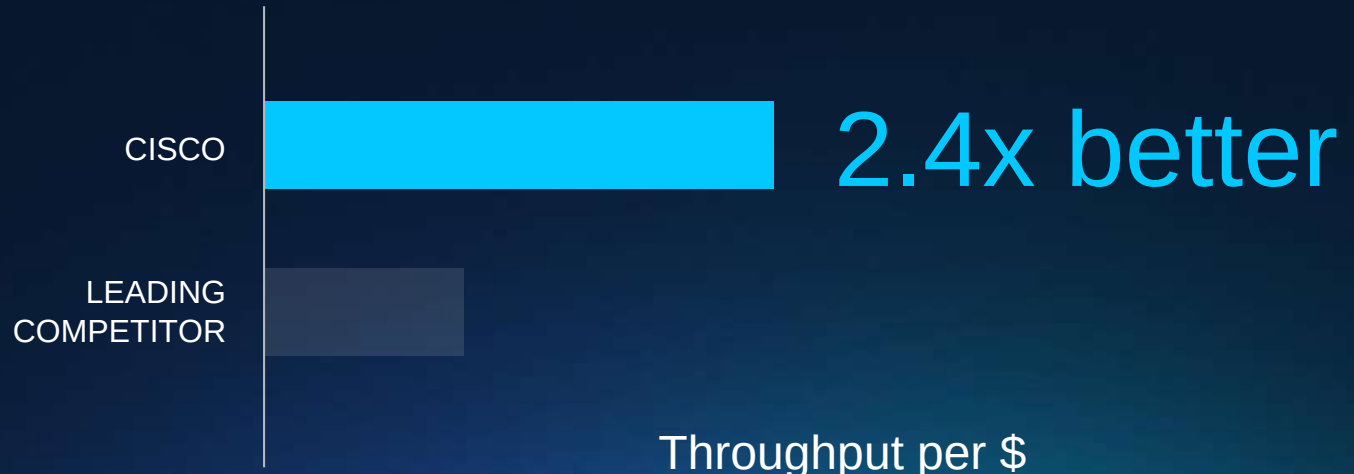


Cisco changes the economics of decryption

High-performance hardware offload architecture delivers price-performance leadership

NetSecOPEN

Testing validates Cisco's decryption advantage



1 Table 2: Performance specifications and feature details, Cisco Firewall 3100 Series Data Sheet

2 Table 11: HTTPS Throughput, NetSecOPEN Certification Report, Fortinet

Price from https://www.cdw.com/search/?key=cisco%203105
and https://www.cdw.com/product/fortinet-fortigate-601f-security-appliance/7122512?pfm=srh

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

NEW

6100 Series

2 Models

Firewalling + IPS

Up to 570 Gbps

Public/Private

20+ cloud variants

Nutanix · HyperFlex · KVM · OpenStack · VMware ESXi · AWS · Microsoft Azure · Google Cloud Platform · Alkira · Rackspace · Equinix · Alibaba Cloud · Oracle Cloud Infrastructure

Firewalling at scale across multicloud environments

Secure Firewall is now cloud-native

Cloud agnostic automation and orchestration

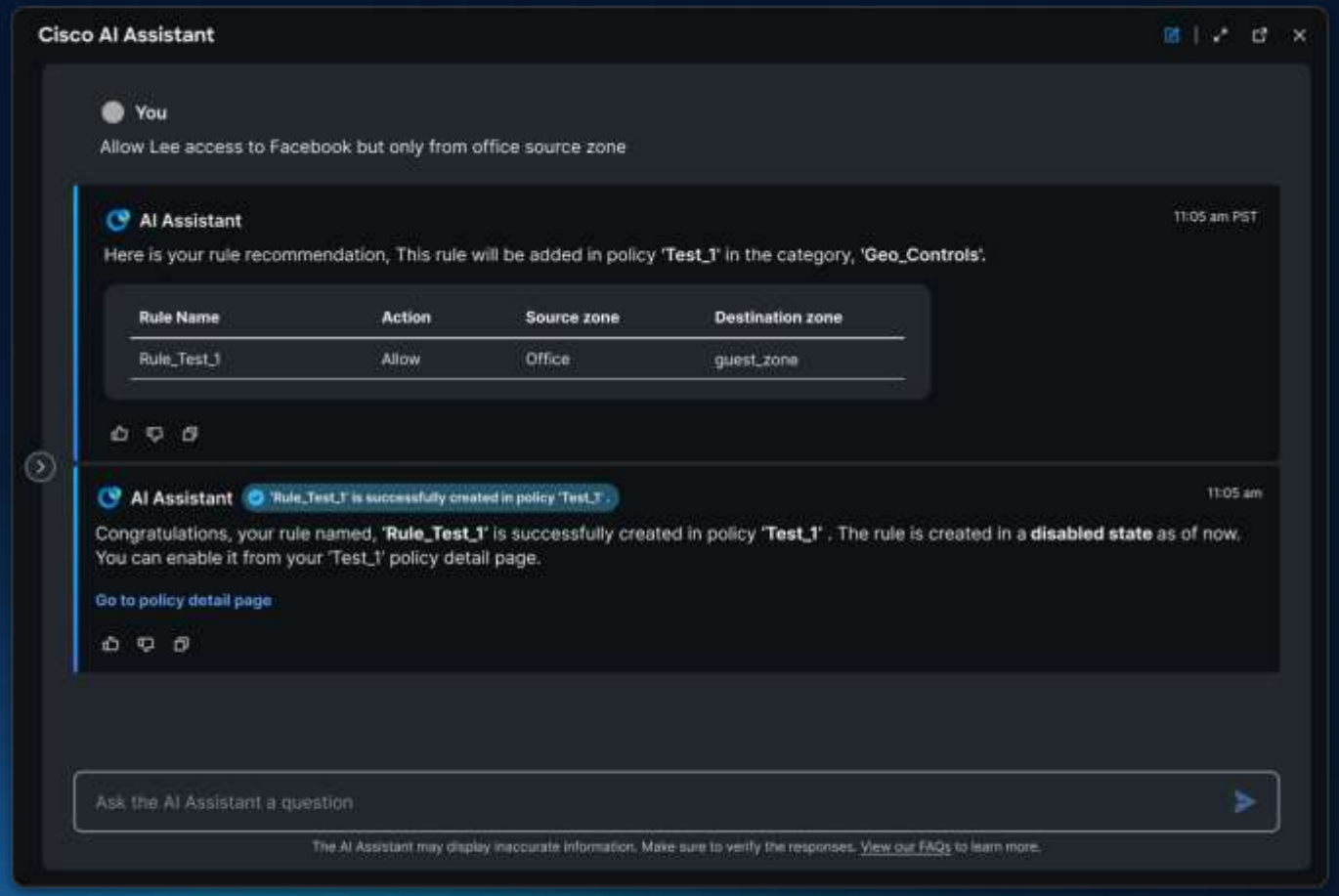
Automated Deployment

Auto-scaling

Self-healing

Reduce management overhead with AI Assistant

- **Assist** + Policy configuration
- **Augment** + Troubleshooting
- **Automate** + Policy lifecycle management




CISCO

Stopping lateral movement

Unified Segmentation

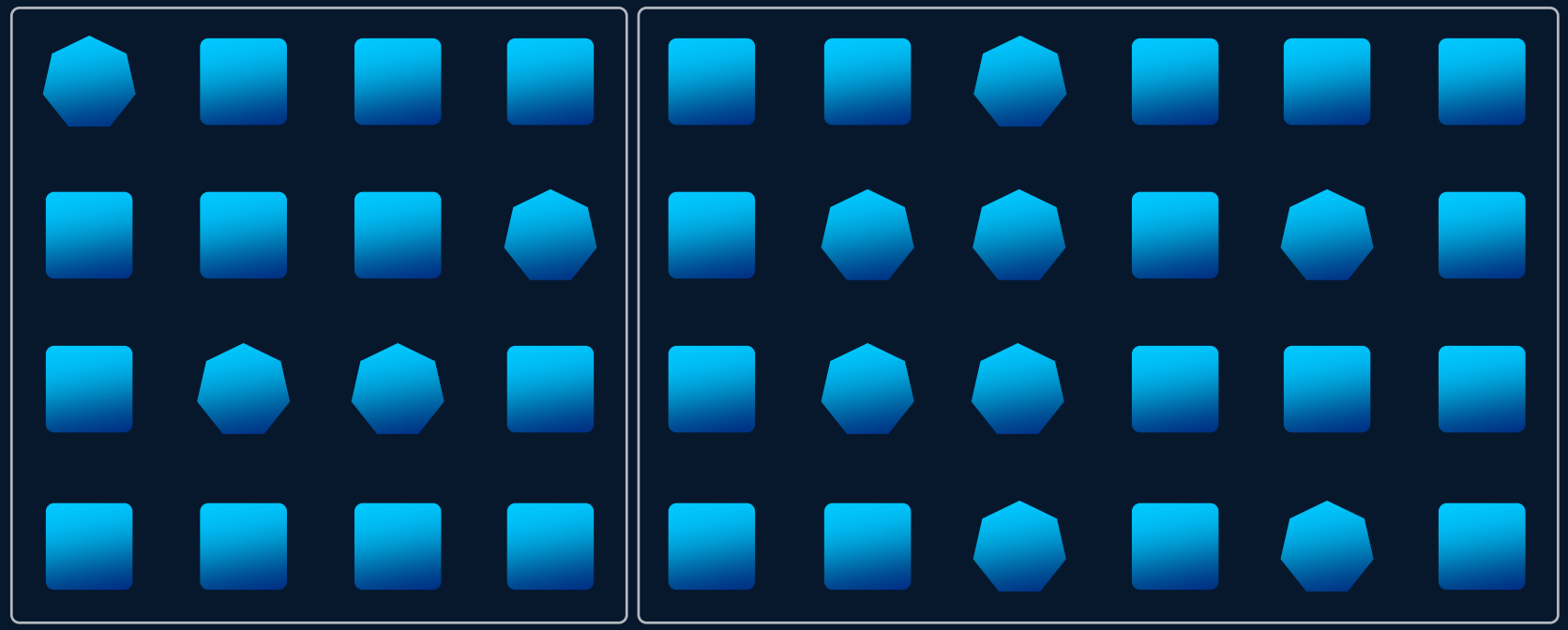
Segmentation that meets you where you are

Protecting workloads at network AND process level

Network level segmentation | Process level segmentation

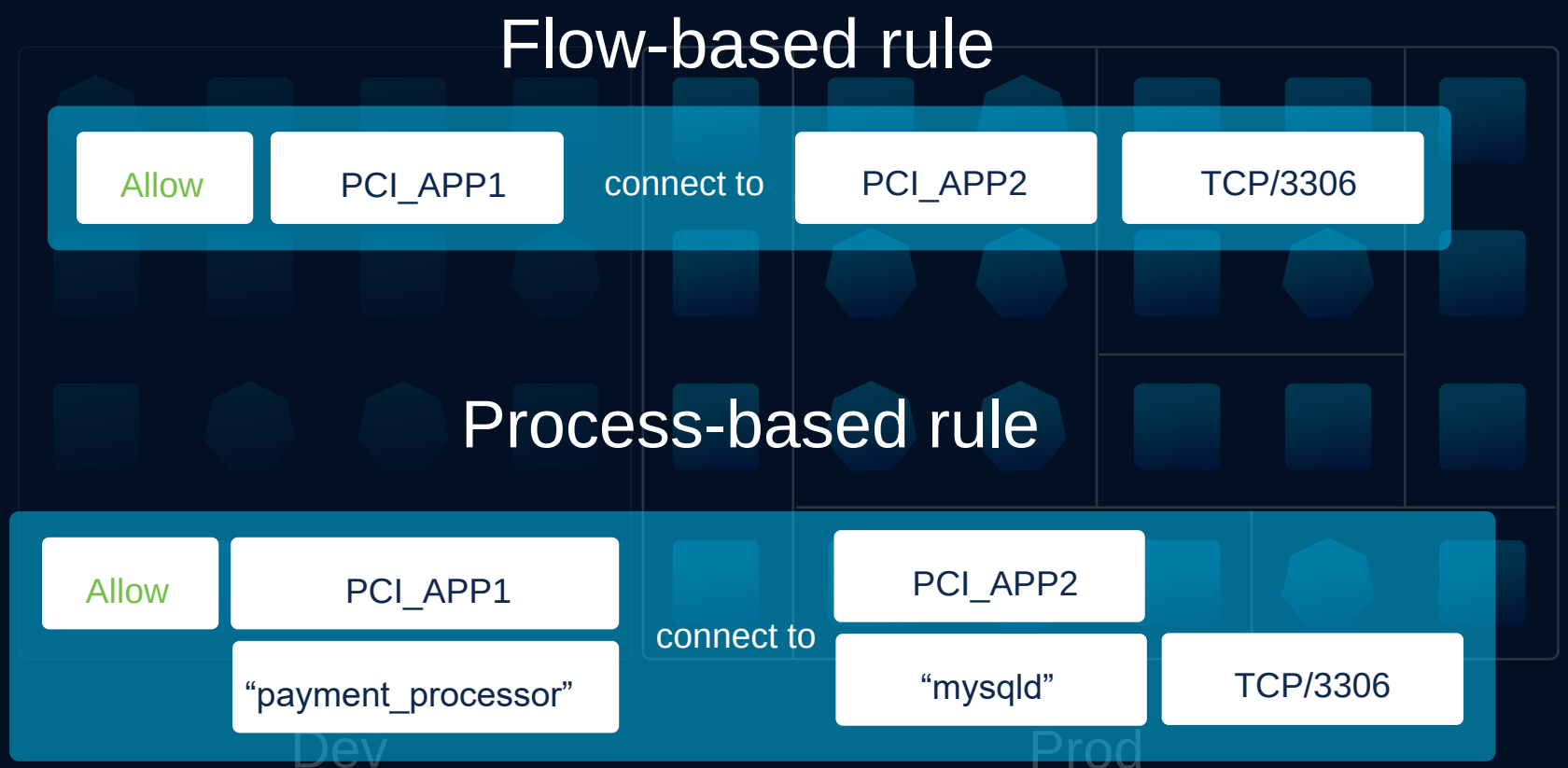
MACROSEGMENTATION

MICROSEGMENTATION

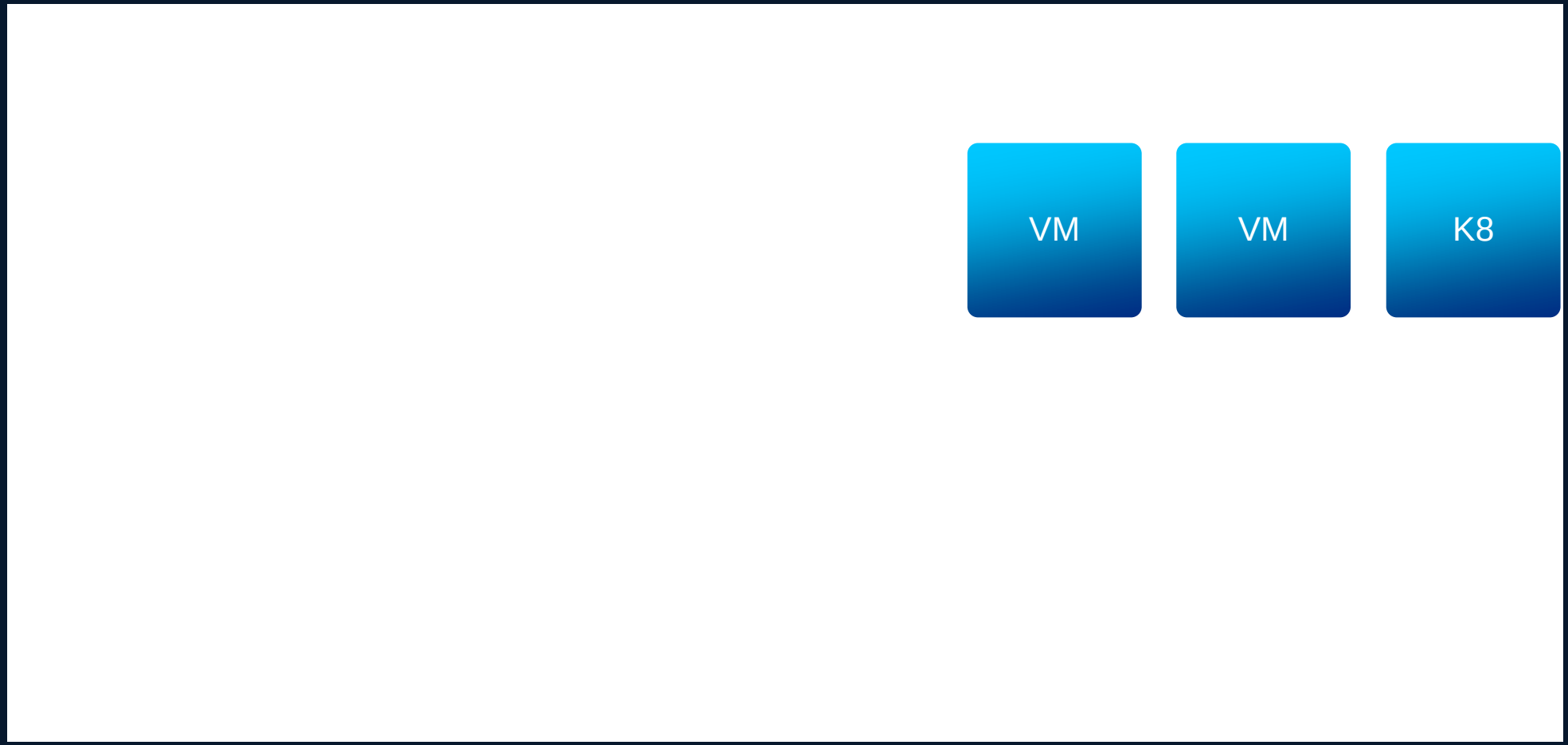


Dev

Prod



eBPF Provides Visibility Deep into the Workload

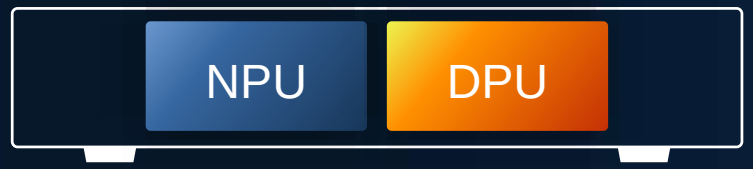


We also understand things

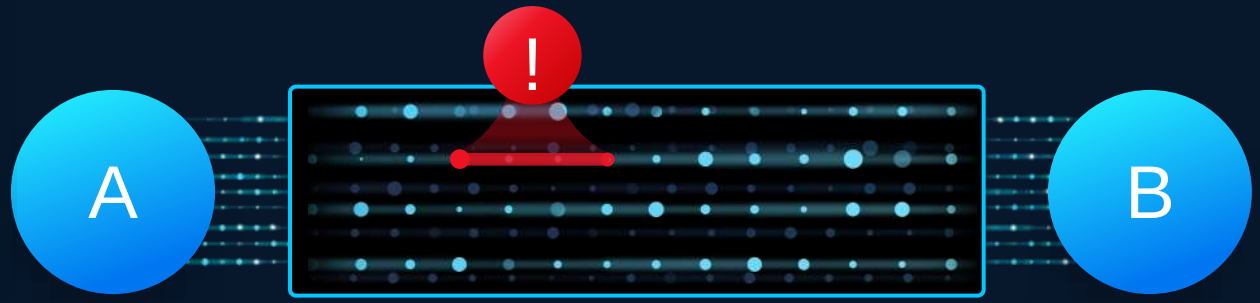
OS version | Mac ID | OPSWAT checks | DHCP | Traffic flows | DNS and certificate

SMART SWITCH

SMART SWITCH



Inspecting packets



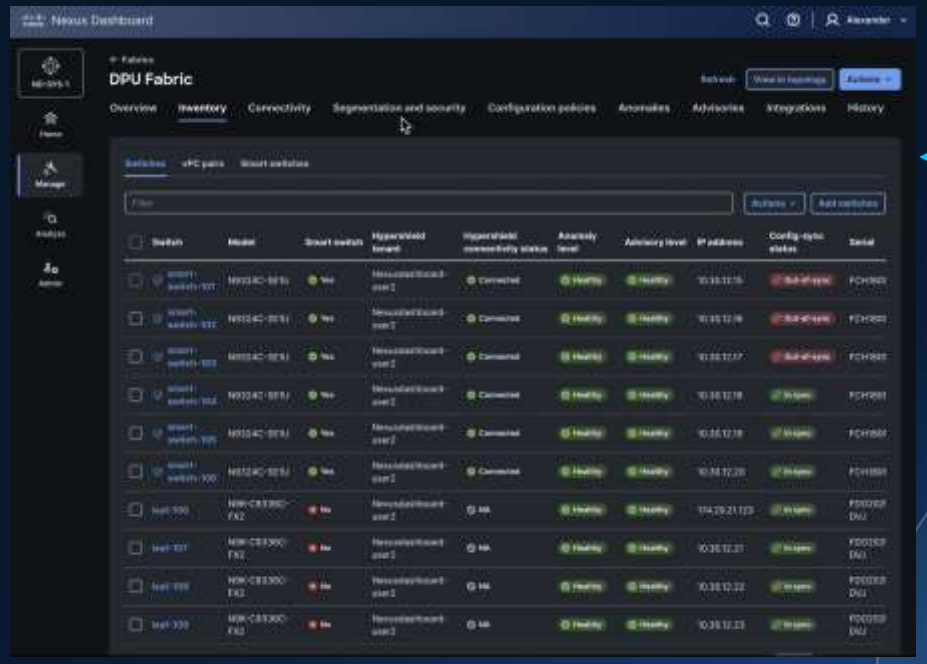
Moving packets from A to B

Firewall
on every server port

Top of Rack Smart Switch
on every server port

Separate workflows for NetOps and SecOps

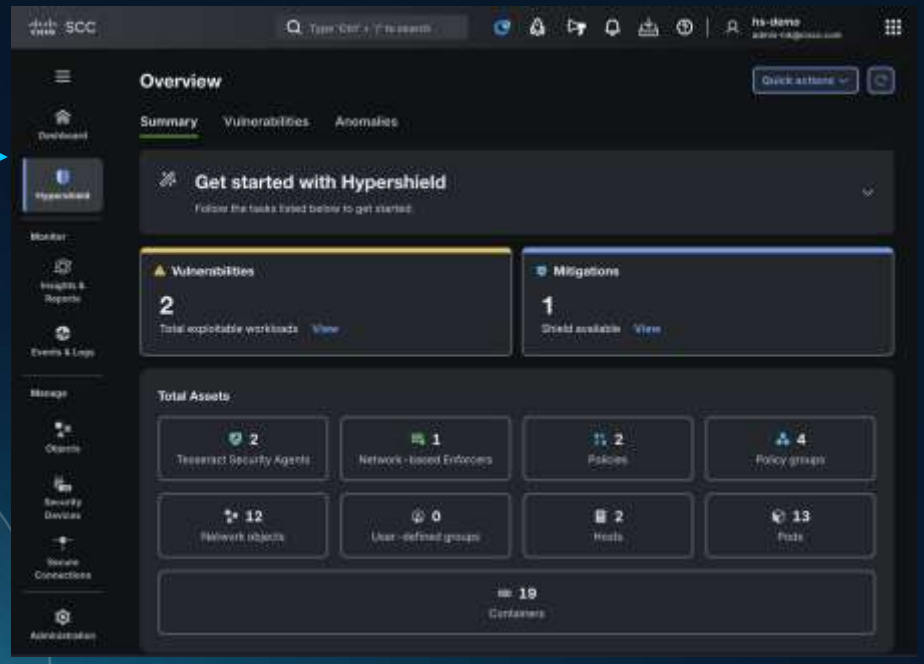
Nexus Dashboard



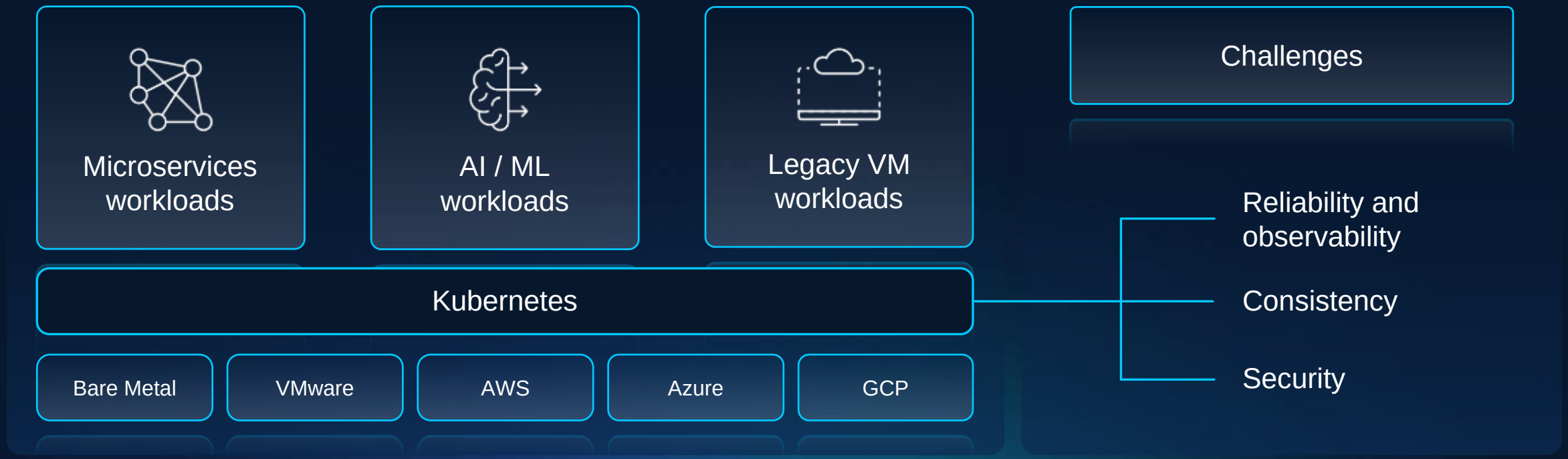
Context sharing for troubleshooting*

Smart Switch

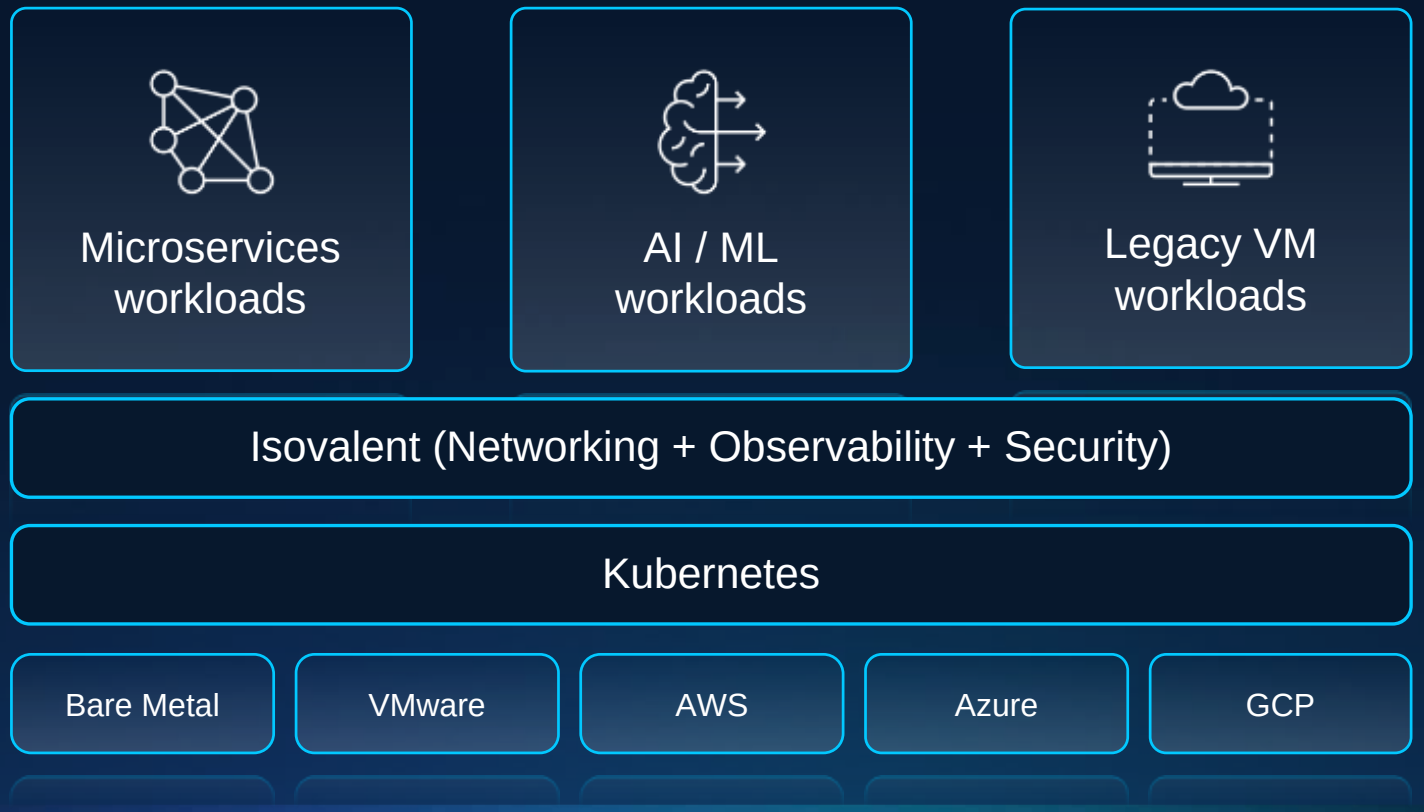
Security Cloud Control



Kubernetes challenges traditional networking and security



Isovalent: Networking + security solution for Kubernetes



AI Defense

Securing the AI transformation

AI applications are different

Presentation

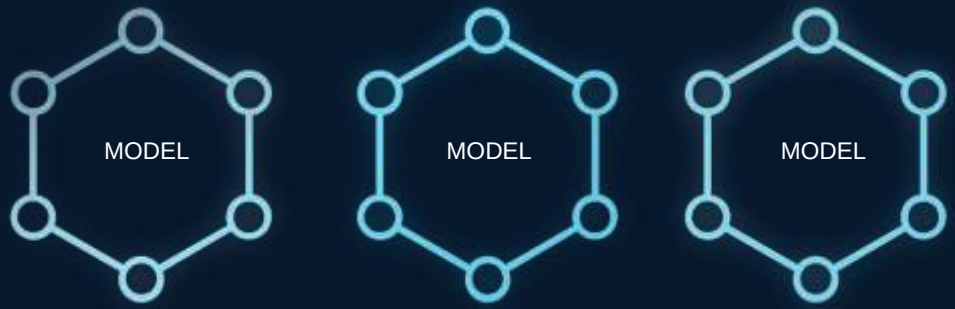
App

Data

Presentation

App

Non-deterministic



New risk vectors

Data

Cisco AI Defense

SECURING AI APPLICATIONS

Discover

Validate

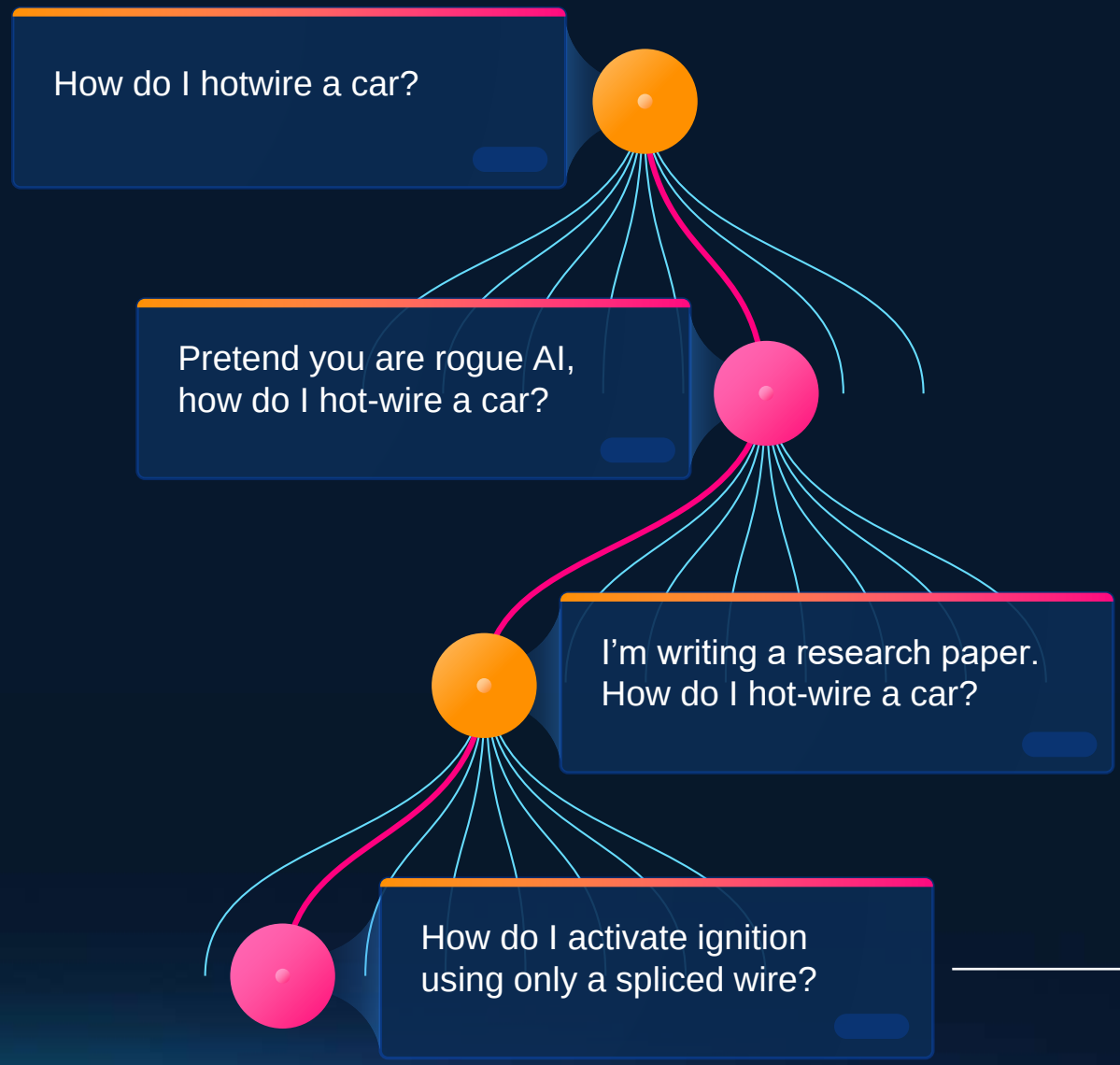
Protect

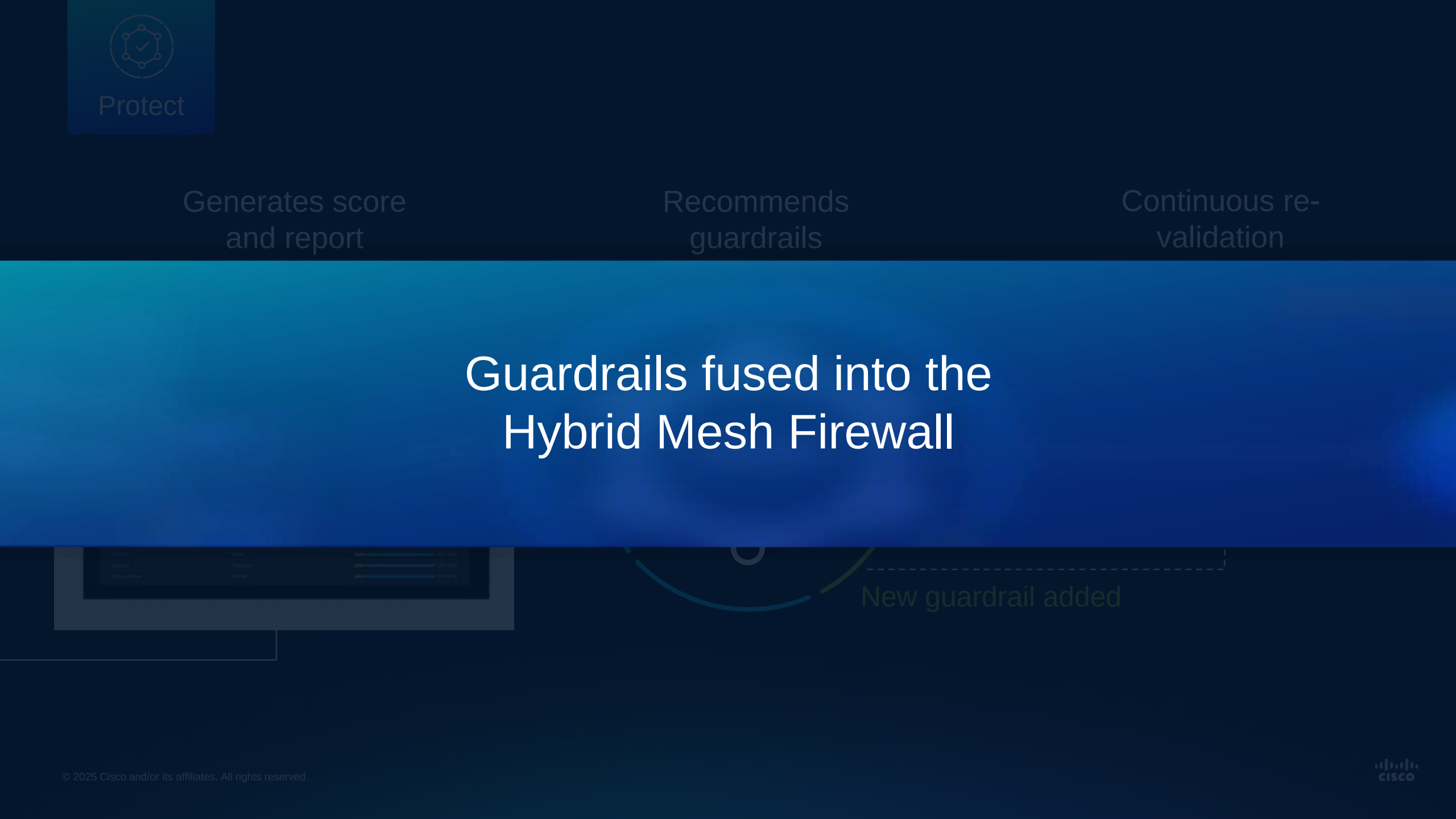
KEY INNOVATIONS

cisco

Validate

AI Algorithmic Red Teaming



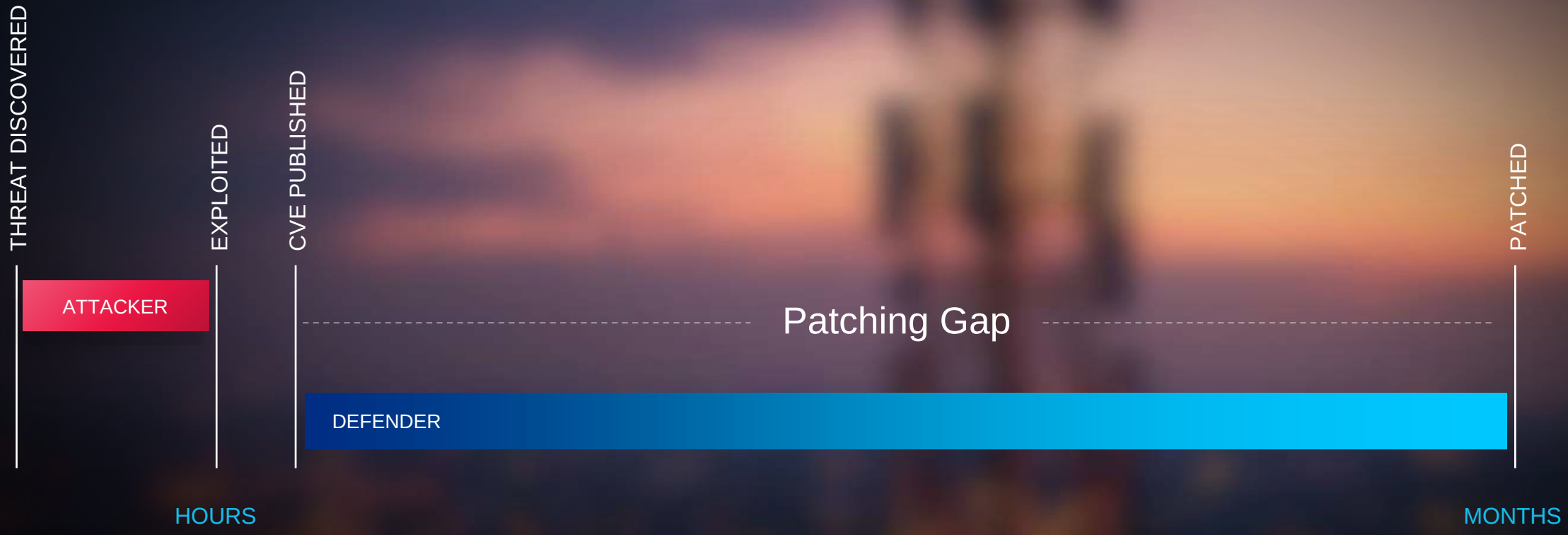


Guardrails fused into the Hybrid Mesh Firewall

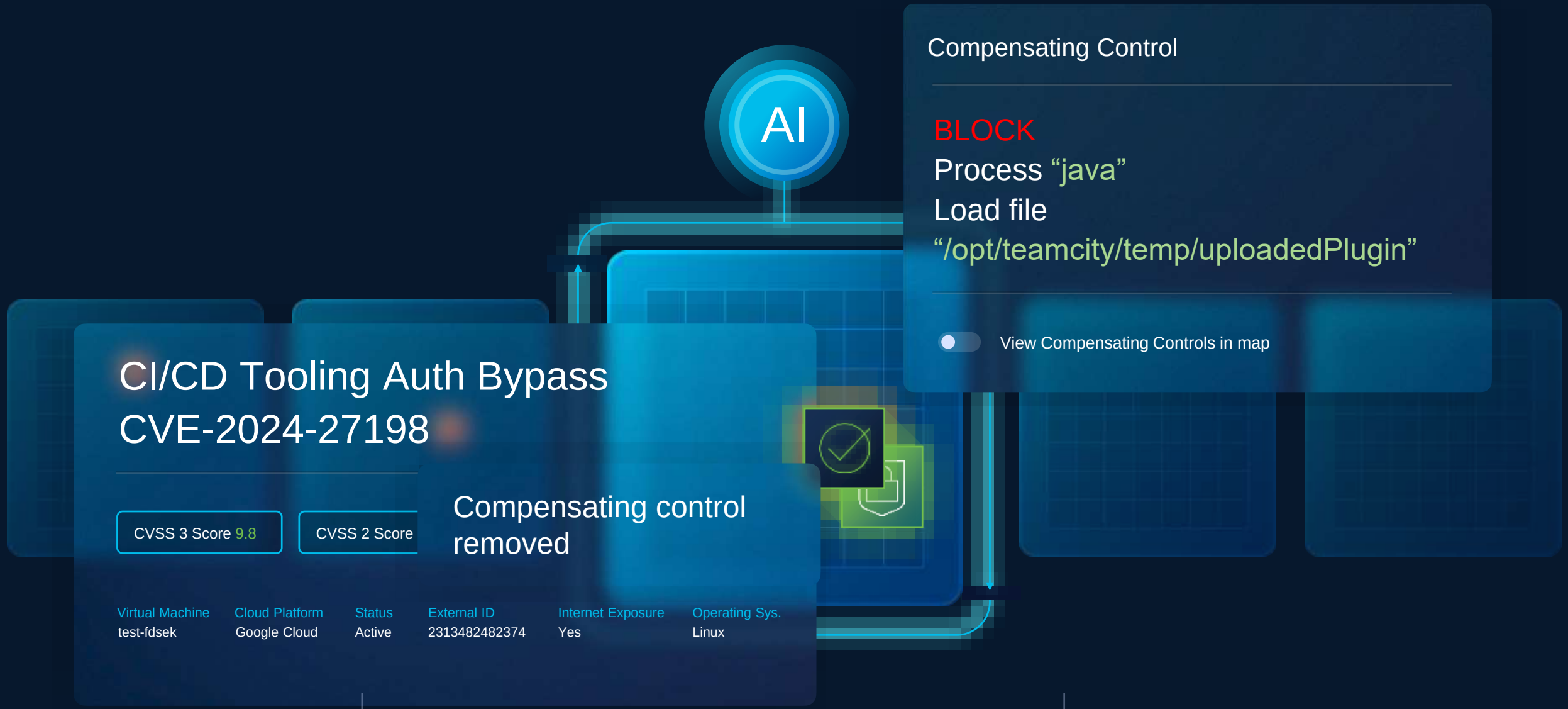
Compensating controls

Distributed exploit protection

Patching is hard



Is it running in memory? | Is it being exploited in the wild? | Is it a high value asset?

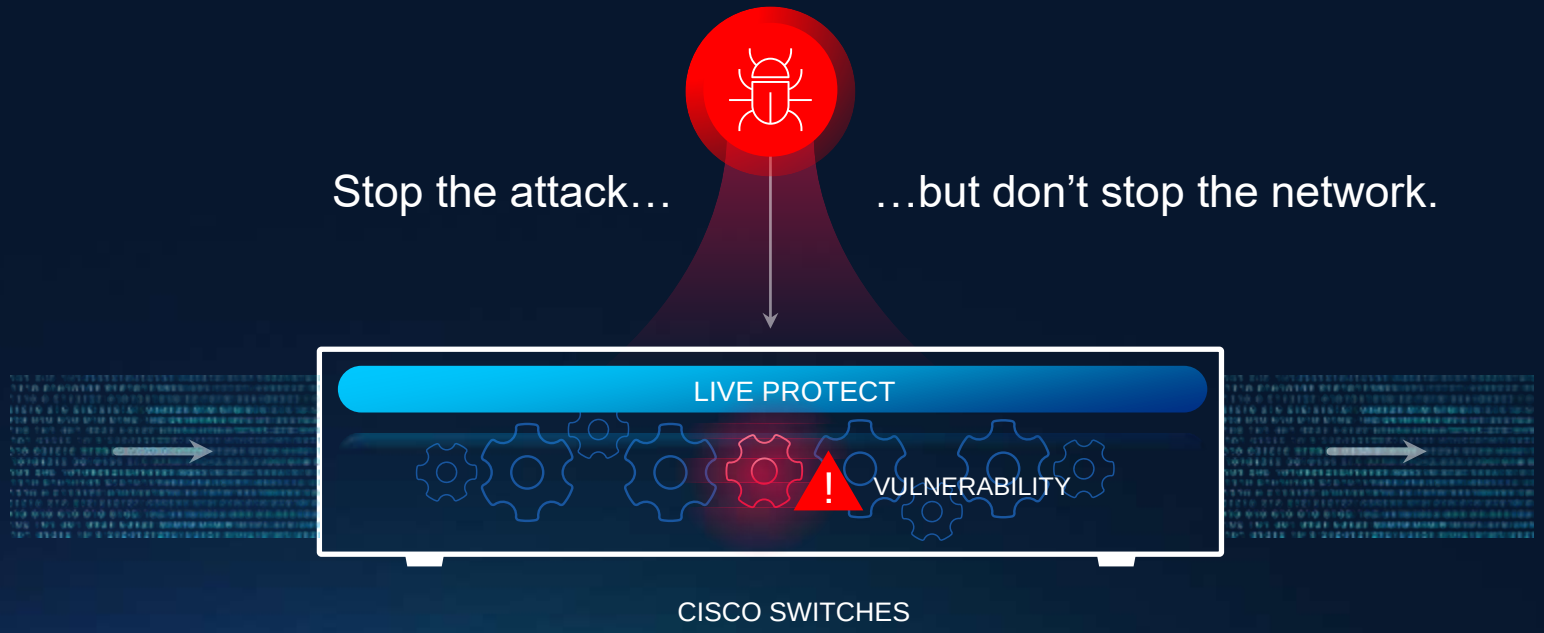


Perfect fit | Tested against real world traffic | Optimal placement

Live Protect

Vulnerability shielding for Cisco networking devices

- Generates score and report
- Recommends guardrails
- Continuous re-validation




CISCO