CISCO Connect

# Agents, Mythos, and Mayhem

## Need for Distributed Firewalling

William Hansch
Sr. Manager, Security Business Group



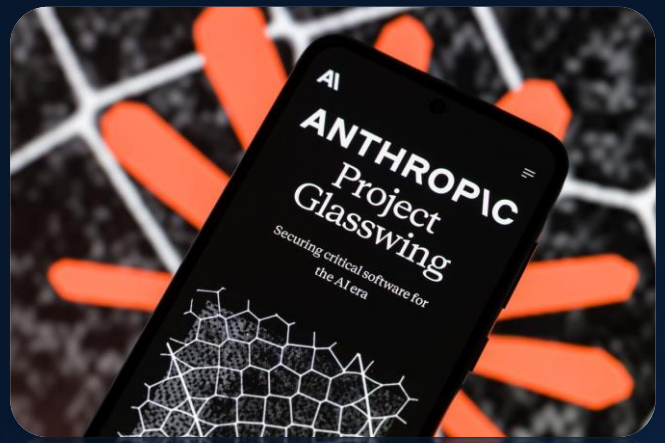

September 23, 2026




© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

# Reality security teams face today

The Mythos moment




Distributed security

Agents accelerating



Security for agents

Exponential complexity



Unified AgenticOps

© 2026 Cisco and/or its affiliates. All rights reserved.

# Firewalling needs to evolve to meet today’s challenges

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

© 2026 Cisco and/or its affiliates. All rights reserved.

…from firewalls to **“firewalling”**…

© 2026 Cisco and/or its affiliates. All rights reserved.

# Hybrid Mesh Firewall: Distributed Defense for the AI Era

## Cisco Cloud Control

- **Perimeter defense**
- **Distributed Segmentation**
- **Workload runtime protection**
- **AI model and agent security**

### Firewall

High-performance threat awareness & protection

- Detect threats in encryption
- Detect zero-day threats

### DC Smart Switch

Highly-distributed L3/L4 segmentation

- Network Visibility
- Network Segmentation

### Workload Agent

eBPF-powered network & runtime security

- Network & Runtime Visibility
- Network Segmentation & Runtime Enforcement

Preventing AI-powered attacks require seamless visibility, enforcement & identity across firewall, network switches & workload

© 2026 Cisco and/or its affiliates. All rights reserved.

# We third-party tested our firewall built for AI-scale. The test tools hit their limit first.

NetSecOPEN independently validates

Cisco Secure Firewall 6160



Our firewall hit the test tools' CPU limits and could've kept going

**100%**

block rate for all tested threats

- Public & private CVEs
- Malware
- Evasions

**5X**

new benchmark for inspected throughput



Cisco Firewall continues to deliver best price-for-inspected-Gbps across all form factors and environments

Source: https://blogs.cisco.com/security/we-third-party-tested-our-firewall-built-for-ai-scale-the-test-tools-hit-their-limit-first

© 2026 Cisco and/or its affiliates. All rights reserved.

# Price-performance leader

## Top to bottom

Branch | Campus | Data center | Cloud

NEW



### 200 Series

2 Models

Up to 3 Gbps



### 1200 Series

6 Models

Up to 18 Gbps



### 3100 Series

5 Models

Up to 45 Gbps



### 4200 Series

3 Models

Up to 140 Gbps

NEW



### 6100 Series

4 Models

Up to 600 Gbps



### Public/Private

20+ cloud variants

No-compromise advanced protection while handling encrypted traffic, powered by AI/ML-driven Encrypted Visibility Engine (EVE) and SnortML

© 2026 Cisco and/or its affiliates. All rights reserved.

Throughputs are calculated based on the operations of Firewalling + Application Visibility Control (AVC) + Intrusion Prevention (IPS) capabilities

# Cisco Smart Switches

## Fusing security in



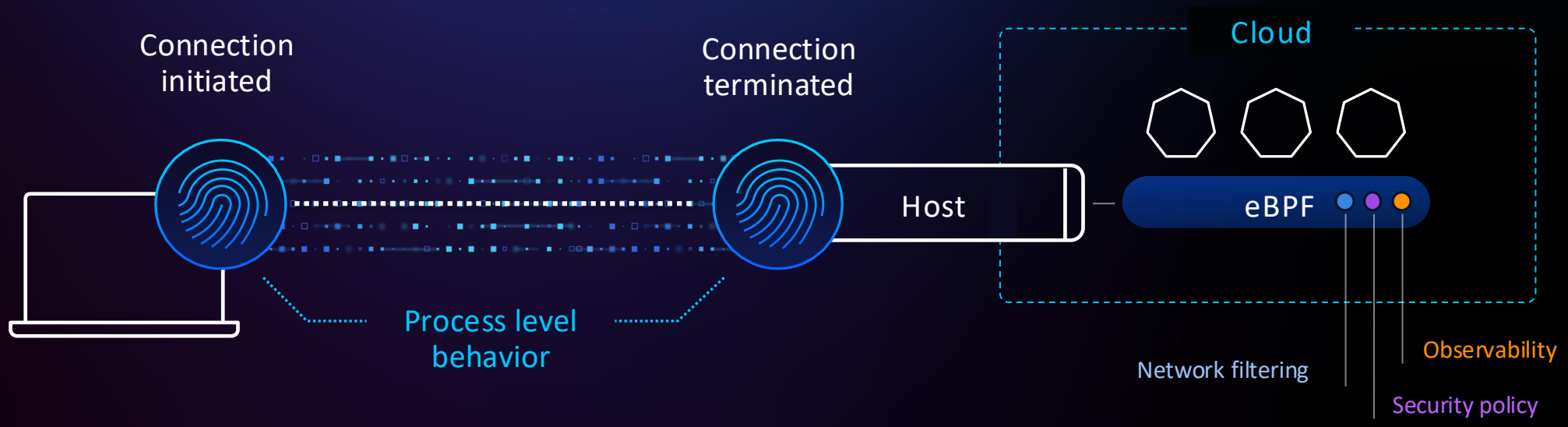

Single appliance, dual personality

Greater visibility, fewer dropped packets

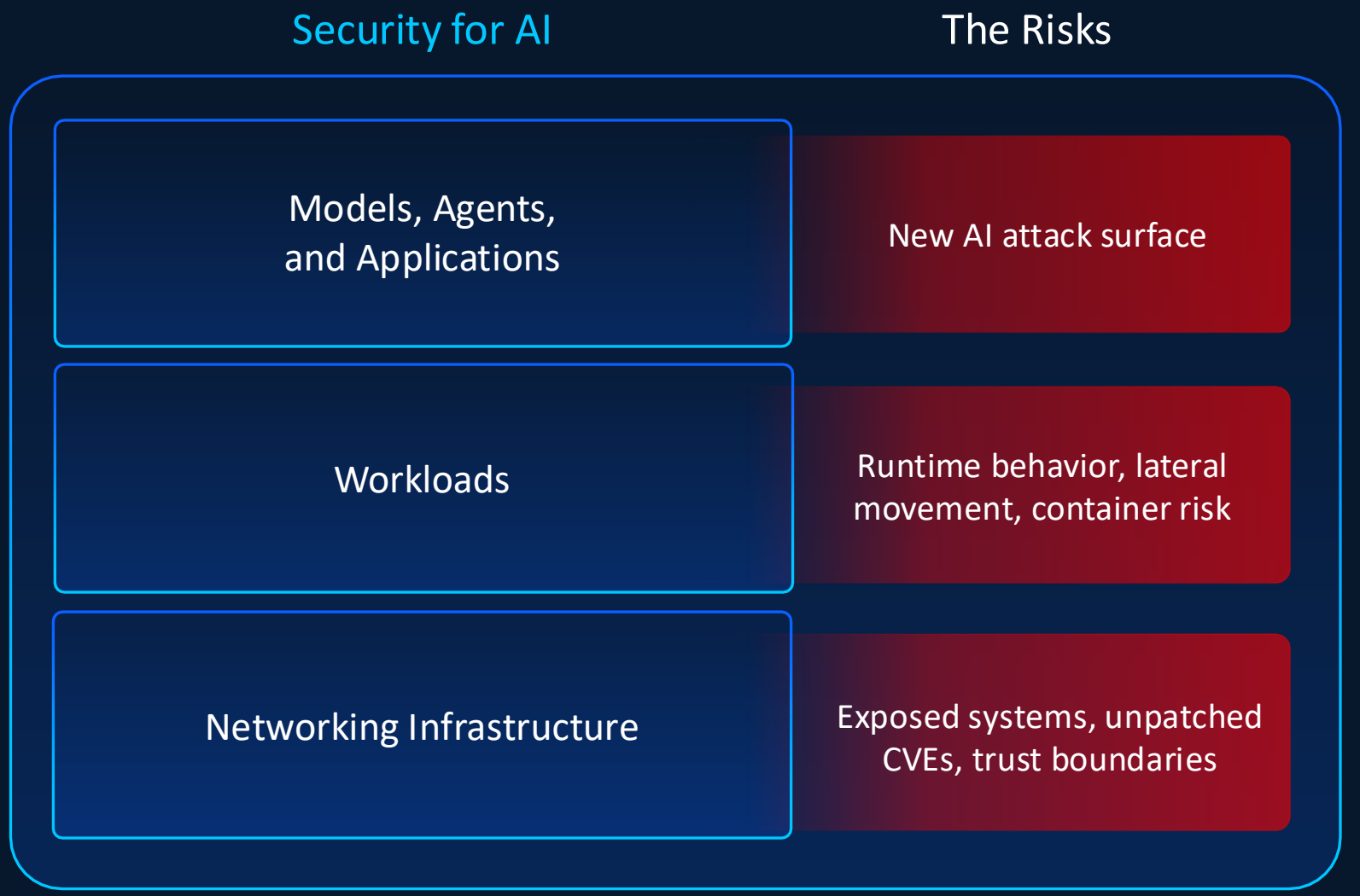
Easily scale security as traffic volume increases

# Modern workload security

Down to the inner workings



# Secure the AI era: new stack, faster attackers




© 2026 Cisco and/or its affiliates. All rights reserved.

# Security-first architecture enables safe Enterprise AI

**Security at all layers of the stack**

**Securing the Model**

**Cisco AI Defense:** Testing and runtime security of LLMs and GenAI applications, integrated with NVIDIA AI.

**Securing the Workloads and Infrastructure**

**Cisco Hybrid Mesh Firewall:** Unified management, consistent, pervasive policies.

**Cisco Isovalent:** Enhanced visibility into cloud native interactions, consistent policy definition and enforcement.

**Cisco Hypershield:** Protection against lateral movement, proactive vulnerability mitigation.

**Cisco Secure Firewall:** Threat protection at scale without compromising performance.

**Security Operations**

**Splunk Enterprise Security:** Real-time threat detection, investigation, and response through analytics, automation, insights.

© 2026 Cisco and/or its affiliates. All rights reserved.

# Firewalls are the first line of defense



**Early detection** of threats in encryption

Cisco Encrypted Visibility Engine



**Detect inline zero-day threats**

Threat Intelligence



**Intelligent segmentation**

Native Integration

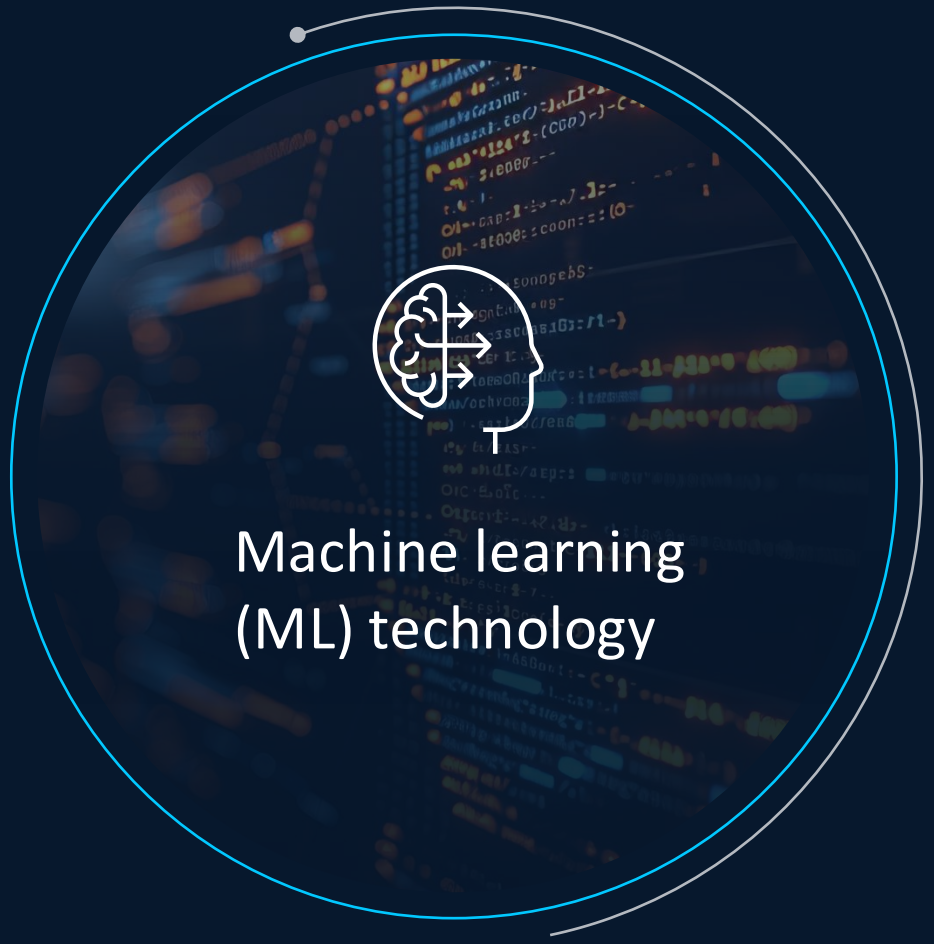
© 2026 Cisco and/or its affiliates. All rights reserved.

# Encrypted Visibility Engine

Visibility for malicious flows in encrypted traffic

**1B+TLS**

fingerprints,
**10K+** malware
samples daily



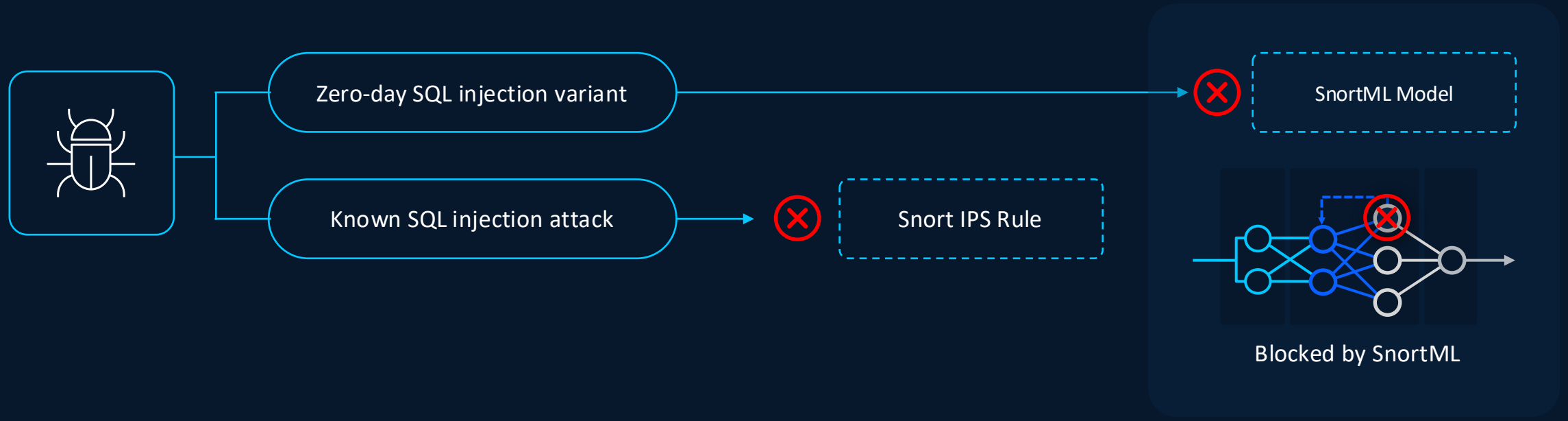
Machine learning
(ML) technology

**10x**

performance
with selective
decryption

© 2026 Cisco and/or its affiliates. All rights reserved.

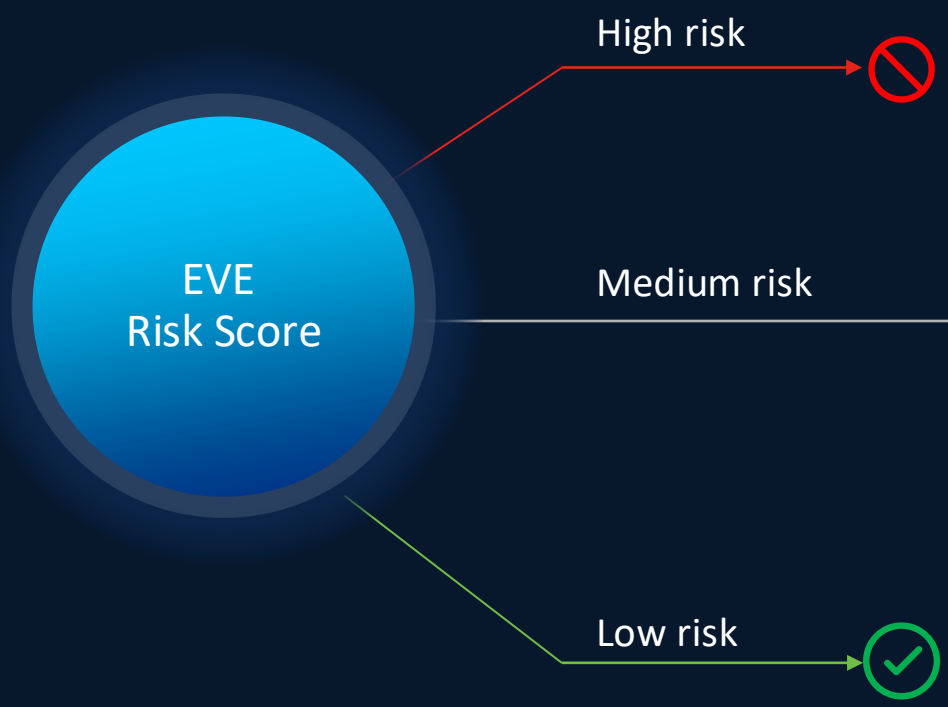
# Stop known and unknown attacks




© 2026 Cisco and/or its affiliates. All rights reserved.

# Next-Generation Traffic Inspection and Defense

**Visibility to malicious flows in encrypted traffic without decryption**

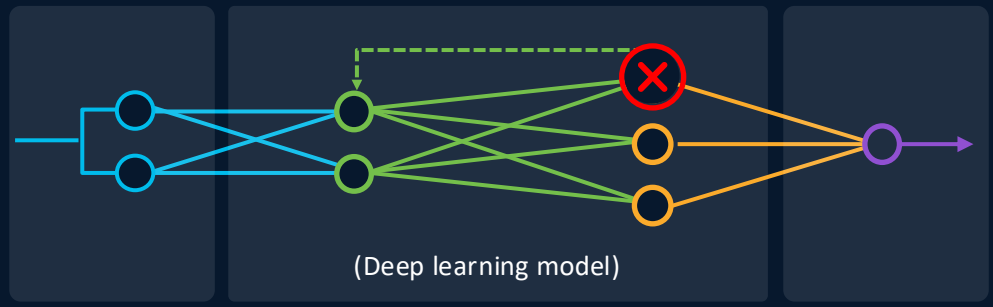



Cisco Encrypted Visibility Engine (EVE)

**Extends IDPS protection to unknown variants of common attacks**

Snort IPS Rule
Known attacks

Snort ML Rule
Zero-day variant




Powered by TALOS Intelligence

© 2026 Cisco and/or its affiliates. All rights reserved.

# Securing AI apps & agents

**Secure third-party agentic components**



AI Supply Chain

**Vulnerability Identification**



Red Teaming

**Guardrails**

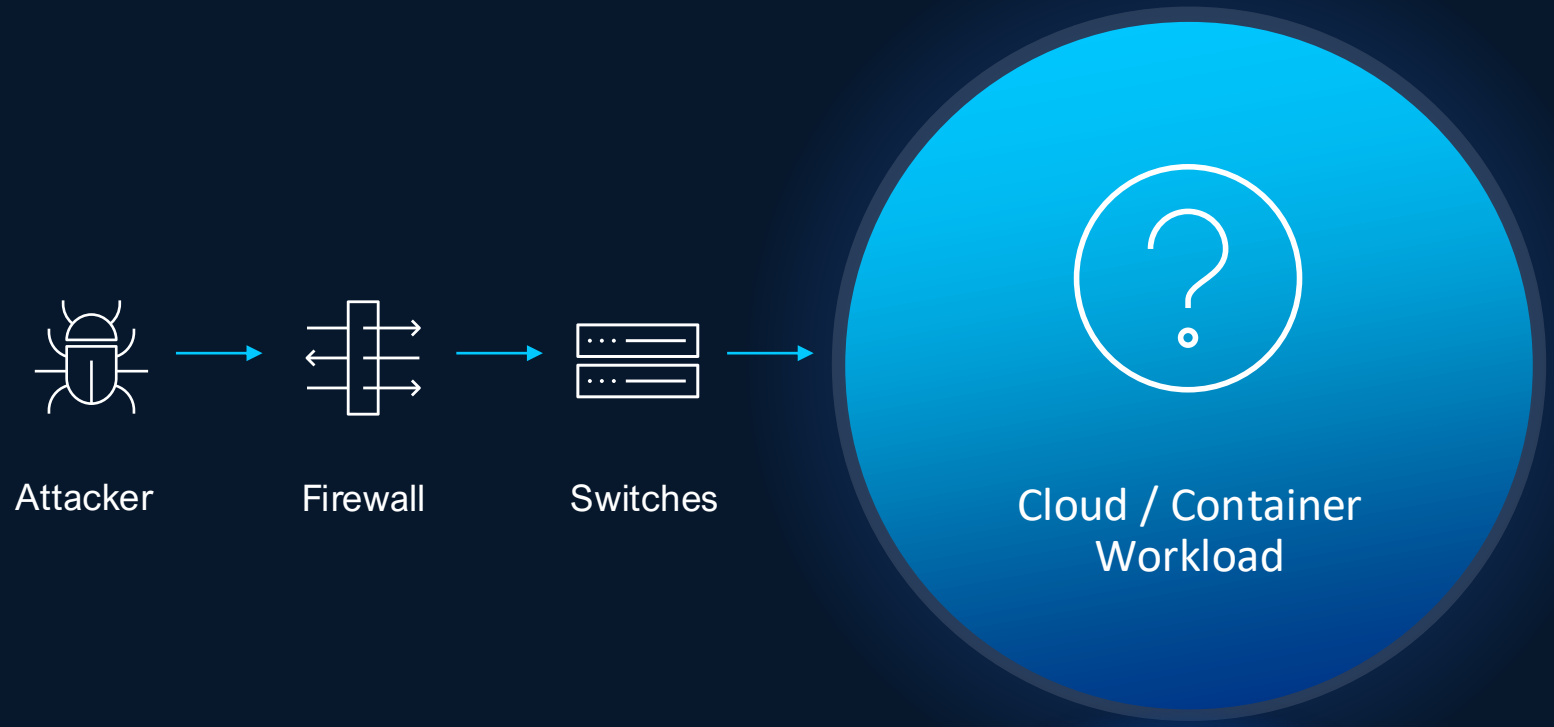


Runtime Protection

© 2026 Cisco and/or its affiliates. All rights reserved.

cisco

# How are your workloads protected?




SEGMENTATION

**Threat containment**

**Limiting blast radius**

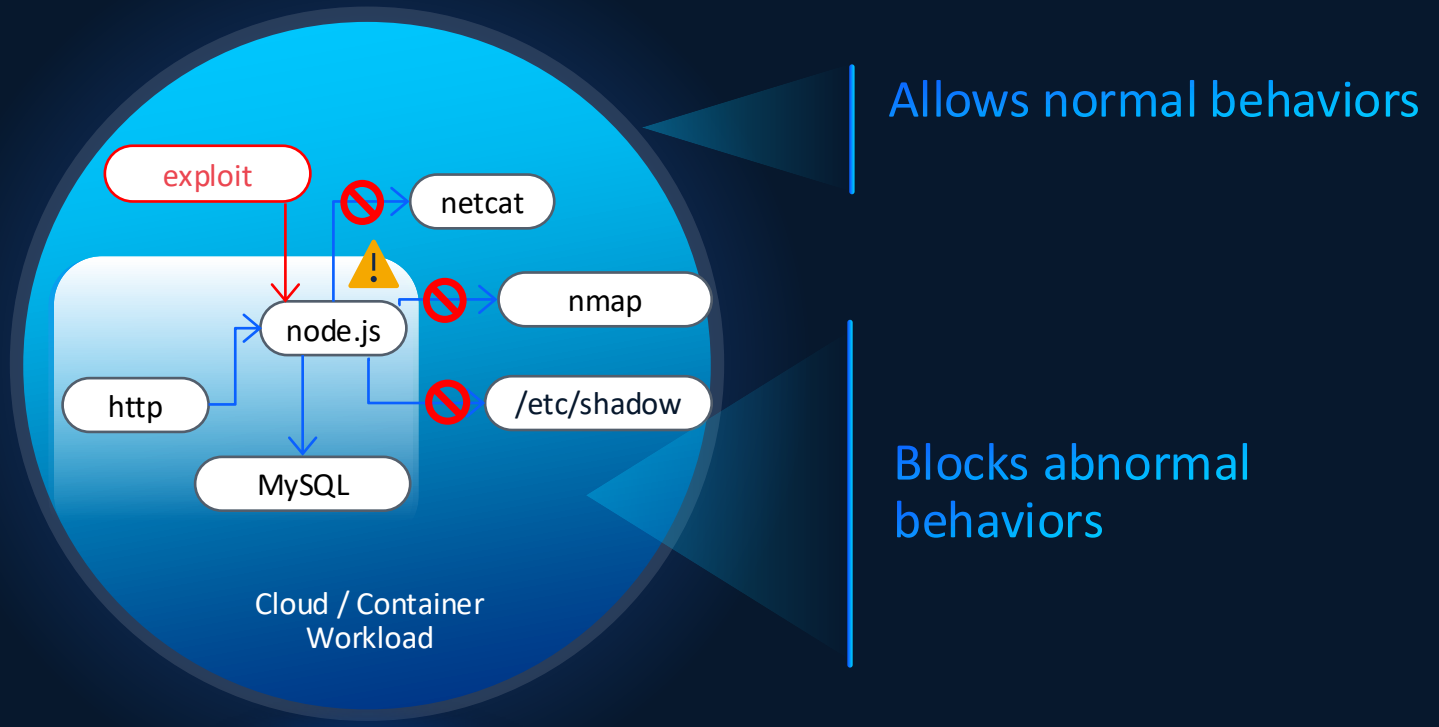
**Identity-driven**

© 2026 Cisco and/or its affiliates. All rights reserved.

# Inspect behaviors instead of data

eBPF provides deep visibility and enforcement within workloads

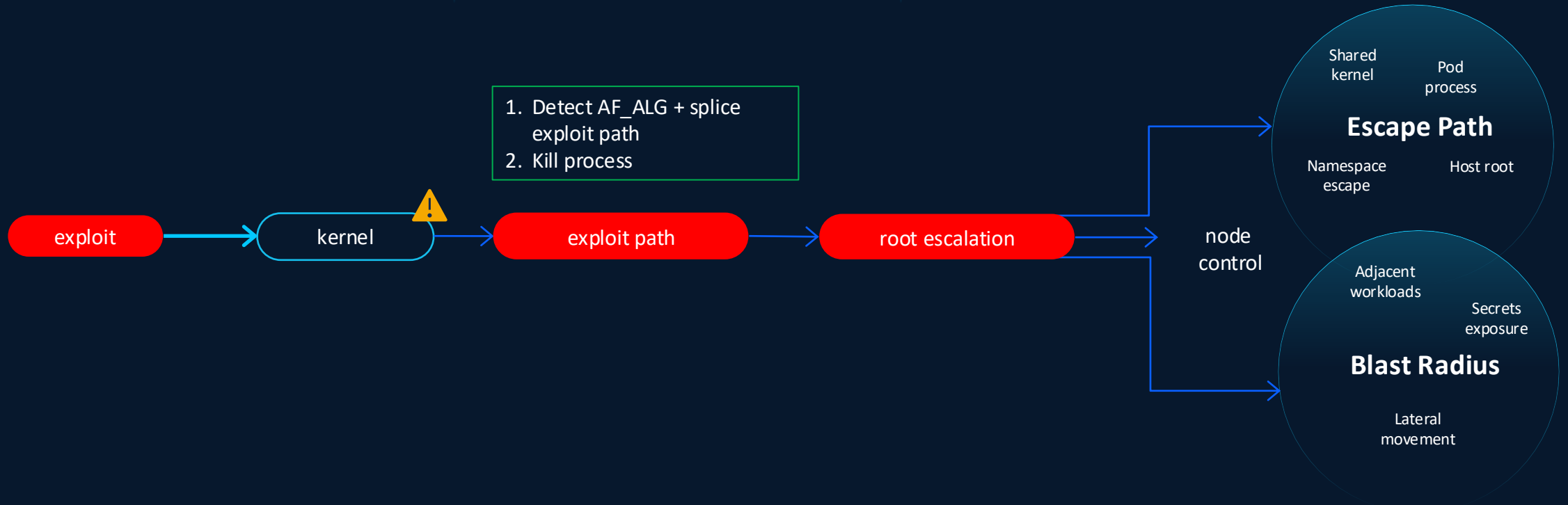
- Network
- File read/write
- Directory




© 2026 Cisco and/or its affiliates. All rights reserved.

# Copy Fail: Kernel-level CVE in the AI Era

Linux kernel privilege escalation | Unprivileged user to root | Container and node escape risk




Kernel-level visibility. Runtime enforcement. Defense-in-depth while patching.

© 2026 Cisco and/or its affiliates. All rights reserved.

# Protecting your infrastructure

From Silicon to Software — Secured at Every Layer

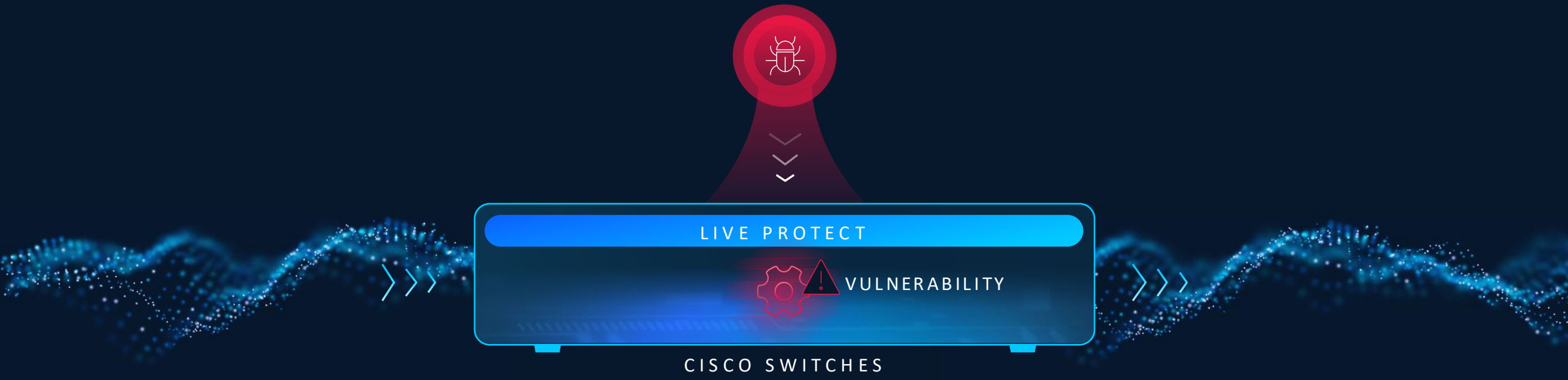



© 2026 Cisco and/or its affiliates. All rights reserved.

# Live Protect

## Vulnerability shielding for Cisco AI networking devices

Stop the attack… but don’t stop the network.




Apply policy to live system

Protect now,
patch in planned window

No downtime or switch reboot

Continuous re-validation

© 2026 Cisco and/or its affiliates. All rights reserved.

# Threat containment at massive scale built into your network



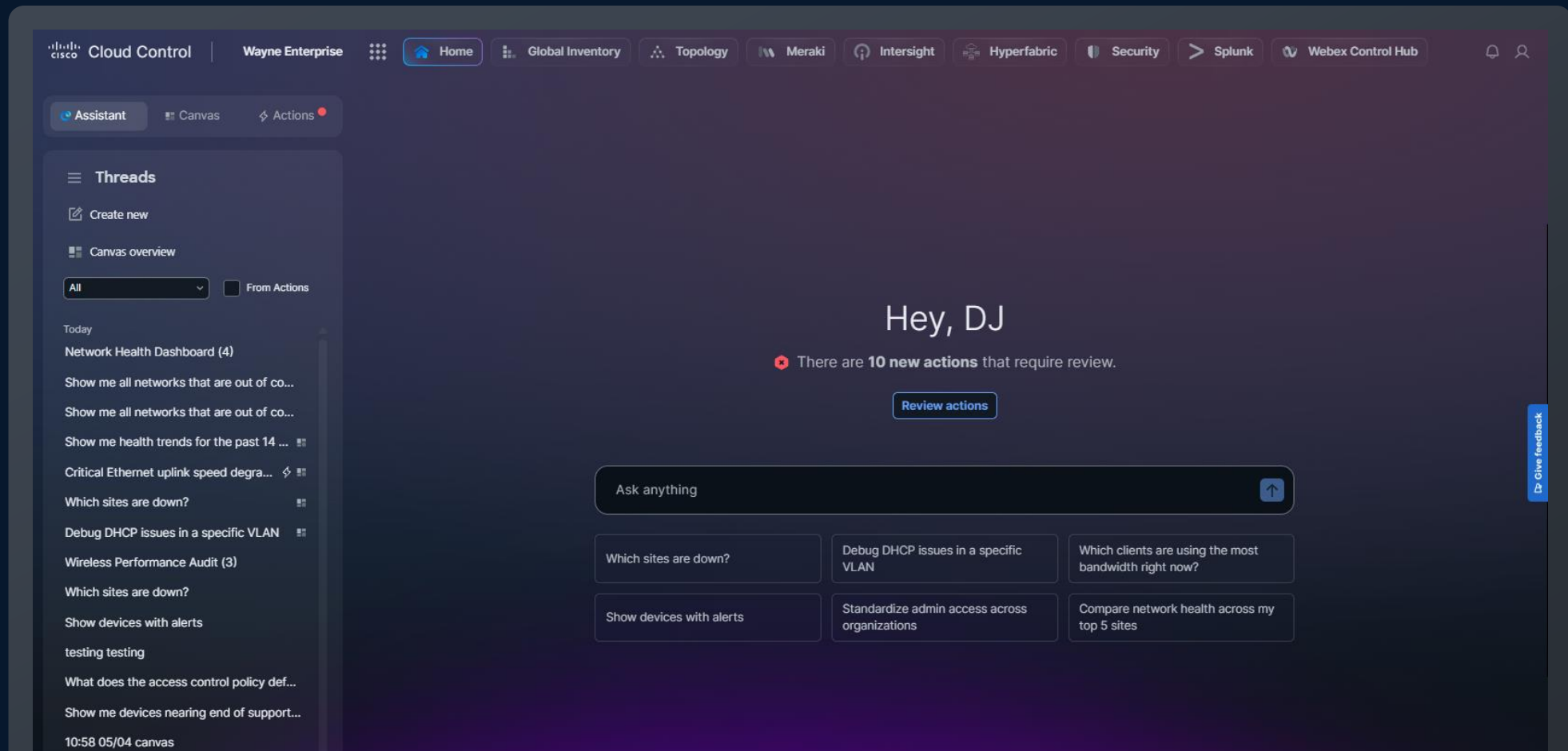

Hardware-accelerated segmentation on every port

© 2026 Cisco and/or its affiliates. All rights reserved.

# Cisco Cloud Control

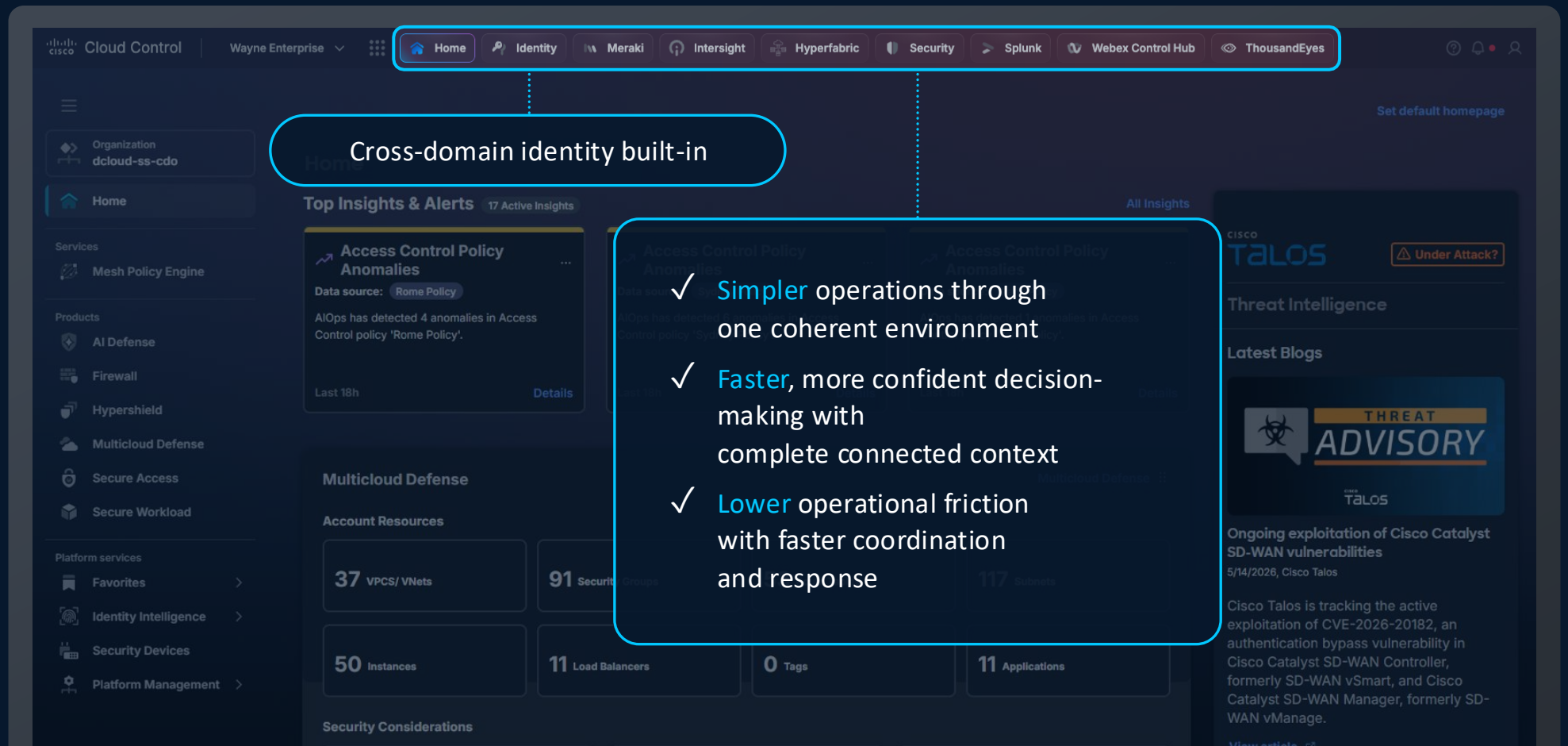
One platform. Every domain. The foundation everything else is built on.

Meraki • ThousandEyes • Security • Splunk • Nexus Dashboard • Catalyst SD-WAN • Intersight • Webex • IQ • and more



# One platform, every domain

## Security in Cloud Control



# Agentic workforce for security built-in

## Turn conversational prompts into action

Security in Cisco Cloud Control with AI Canvas




Example

Allow only doctors to access the electronic health record (EHR) system, deny nurses and all others, log every attempt.



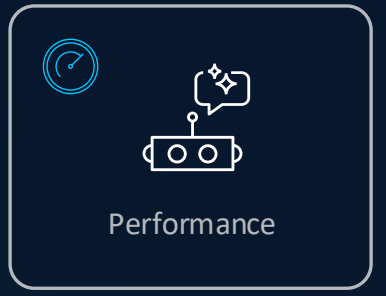

Example

Check the London-to-Frankfurt VPN, identify tunnel issues, explain cause, and recommend safe remediation steps.




Example

Review our zero trust policies for the HR application and identify any users, devices, or locations with overly broad access.




Example

Investigate elephant flow spikes, identify affected traffic, explain likely causes, and recommend safe remediation.

© 2026 Cisco and/or its affiliates. All rights reserved.

# Specialized skills built into security agents




© 2026 Cisco and/or its affiliates. All rights reserved.

# Multi-vendor intent-based policy

Cloud Control



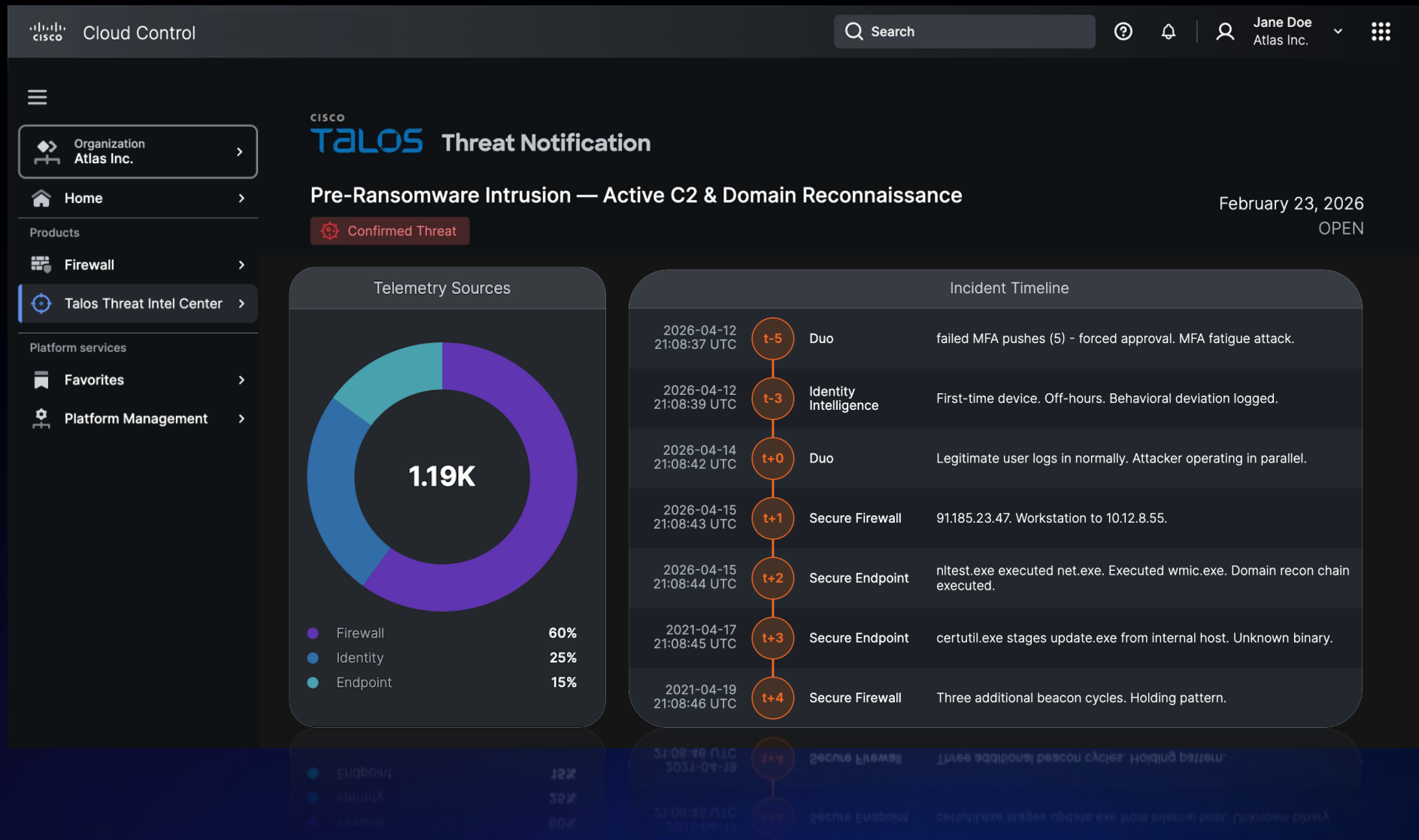

Absorb and optimize existing rules

Change enforcement points, not policy

No rip and replace

# Introducing Cisco Talos Threat Hunting

A helping hand for the Mythos era



# Introducing
# New Firewall Management Center appliance

FTD 10.0+

FMC x800 Series

Based out of UCS M8 Server

Manage up to 1500 FTDs
50% boost over 4700

Improved event retention and event rate
2x vs FMC4700

Extended Lifecyle
Expected Sellable life till CY2030 and beyond



© 2026 Cisco and/or its affiliates. All rights reserved.

# Migration options



## Cloud Integration

**On-premises**
FMC appliance for FTD management

**Cloud**
Subset of Security Cloud Control capabilities

**IDEAL FOR ORGANIZATIONS...**

Looking to improve security posture with existing investments in Cisco Secure Firewall



## Fully Cloud

Management, monitoring, and event logging via Security Cloud Control

**IDEAL FOR ORGANIZATIONS...**

Pursuing a cloud-first strategy to boost OpEx efficiency and avoid the CapEx of on-premises upgrades

© 2026 Cisco and/or its affiliates. All rights reserved.

# Benefits by migration option

| | Cloud Integration | Fully Cloud |
|---|---|---|
| Zero upfront cost | ✓ | |
| Policy analyzer & optimizer | ✓ | ✓ |
| AI assistant | ✓ | ✓ |
| Feature adoption | ✓ | ✓ |
| Best practice recommendation | ✓ | ✓ |
| Secure mgt access from anywhere | | ✓ |
| No on-premises FMC appliance | | ✓ |
| Latest mgt firmware with zero overhead | | ✓ |
| 99.99% uptime SLA without HA | | ✓ |
| Auto backups | | ✓ |
| Elastic scale: add/remove devices | | ✓ |
| Combined visibility of FTD & ASA events | | ✓ |
| Streamlined security management | | ✓ |

© 2026 Cisco and/or its affiliates. All rights reserved.

# From Connect to action: Next steps

Want to know more about Cisco Hybrid Mesh Firewall?

Pick a date and join our Cisco Hybrid Mesh Firewall Design Clinic: https://ciscosecurityworkshop.com/workshop-events/list-all-workshops

Request a demo for Cisco AI Defense: https://www.cisco.com/c/en/us/products/security/ai-defense/request-demo.html

Pick a date and join our workshop to develop effective segmentation strategies:

https://cloudsecurity.cisco.com/streamlining-hybrid-data-center-security

© 2026 Cisco and/or its affiliates. All rights reserved.

CISCO Connect

# Thank you




CISCO