CISCO Connect

Agents, Mythos, and Mayhem

Need for Distributed Firewalling

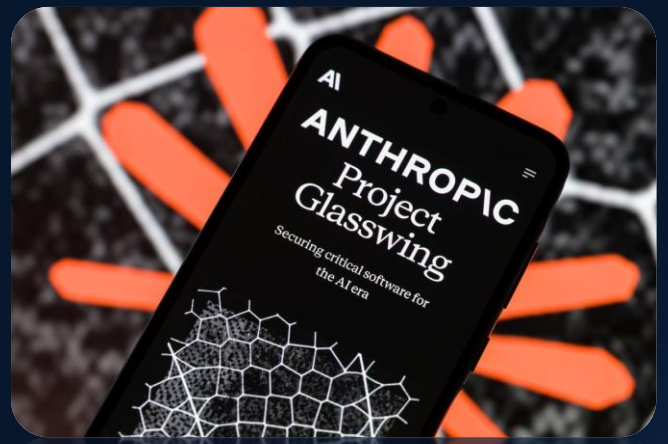
Nick Zeigler, CISSP
Sr Solutions Architect – Forward Deployed Engineering
Cisco Cloud Control and Cisco IQ



September 30th, 2026

Reality security teams face today

The Mythos moment



Distributed security

Agents accelerating



Security for agents

Exponential complexity



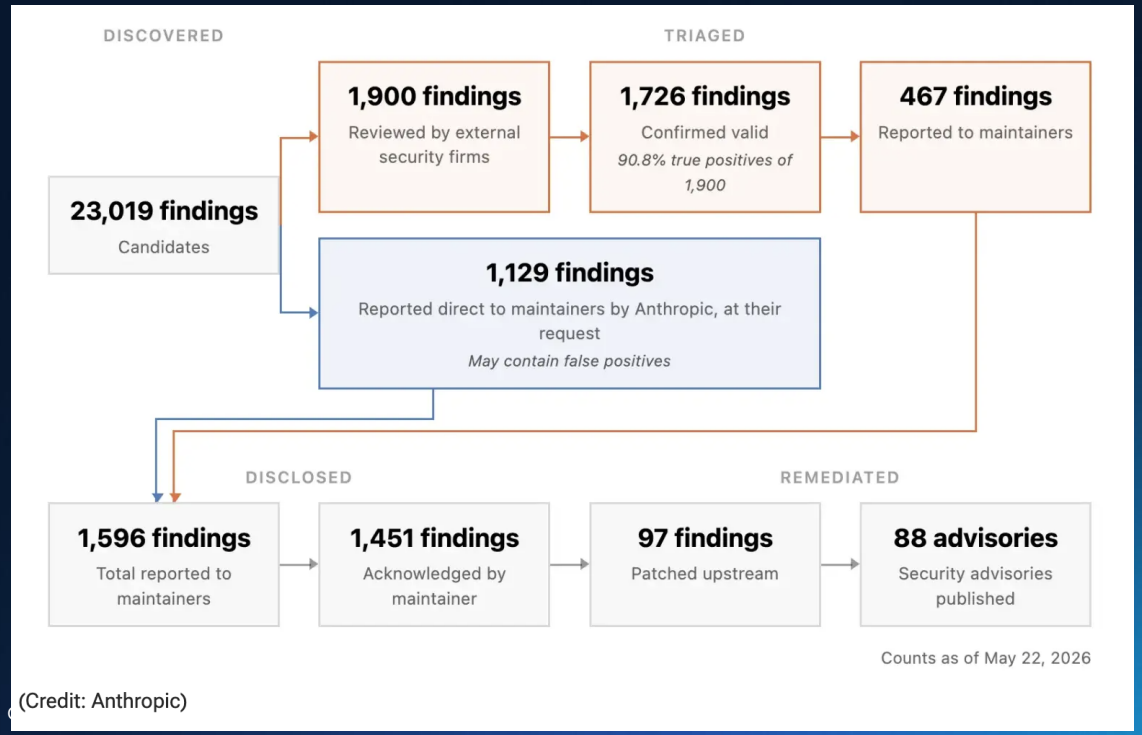
Unified AgenticOps

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

cisco

What is Mythos?

Claude Mythos Preview is a general-purpose, unreleased frontier model that reveals a stark fact: AI models have reached a level of coding capability where they can surpass all but the most skilled humans at finding and exploiting software vulnerabilities.



(Credit: Anthropic)

Project Glasswing:

Last week:

Rogue OpenAI agent 'infiltrated' Australian government website in world first

August 2026:

OpenAI agents hacked Hugging Face in 700-strong swarm, tried to cover tracks, investigations find

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

...from firewalls to **“firewalling”**...

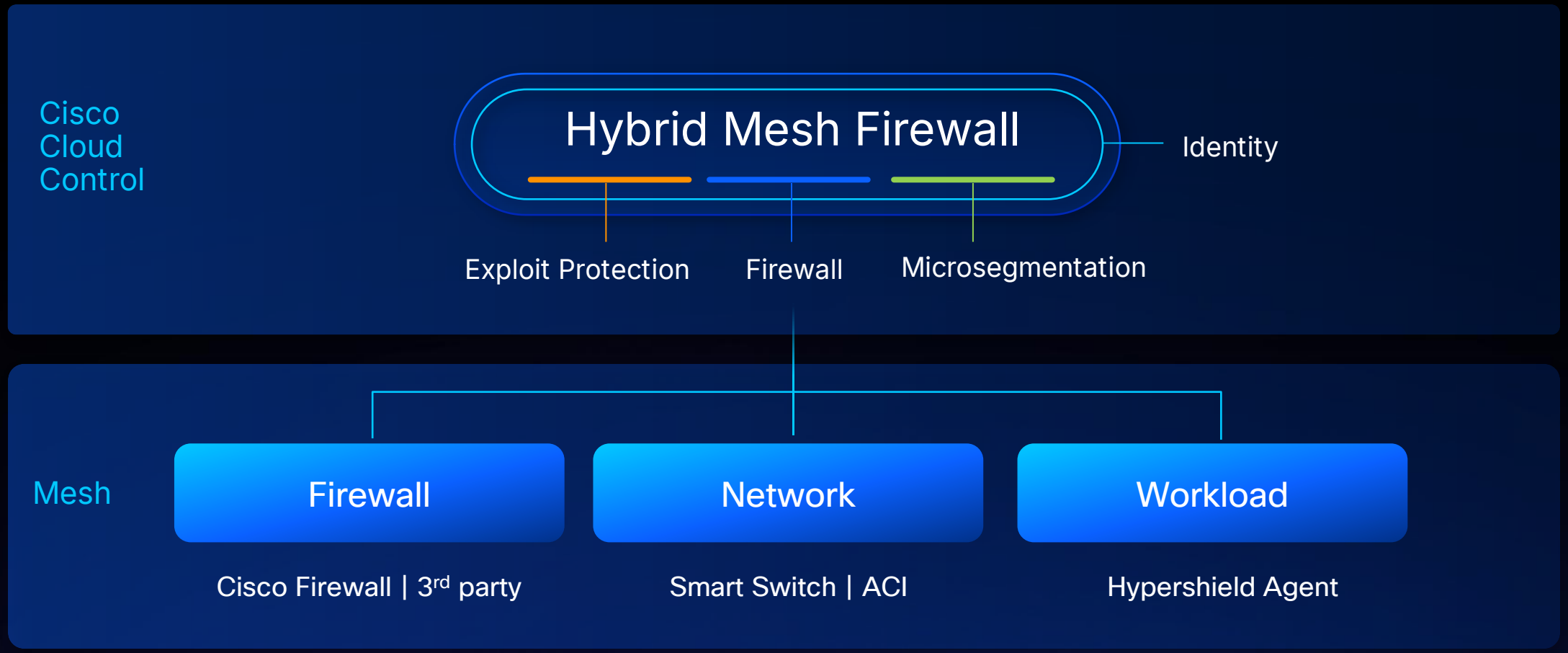
© 2026 Cisco and/or its affiliates. All rights reserved.

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

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

Protecting your infrastructure and apps, including AI



Secure Firewall 6100: Near-limitless scale for AI readiness



Cisco Secure Firewall
6100 series

Scales linearly to 8Tbps of L7, appID, 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

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

cisco

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



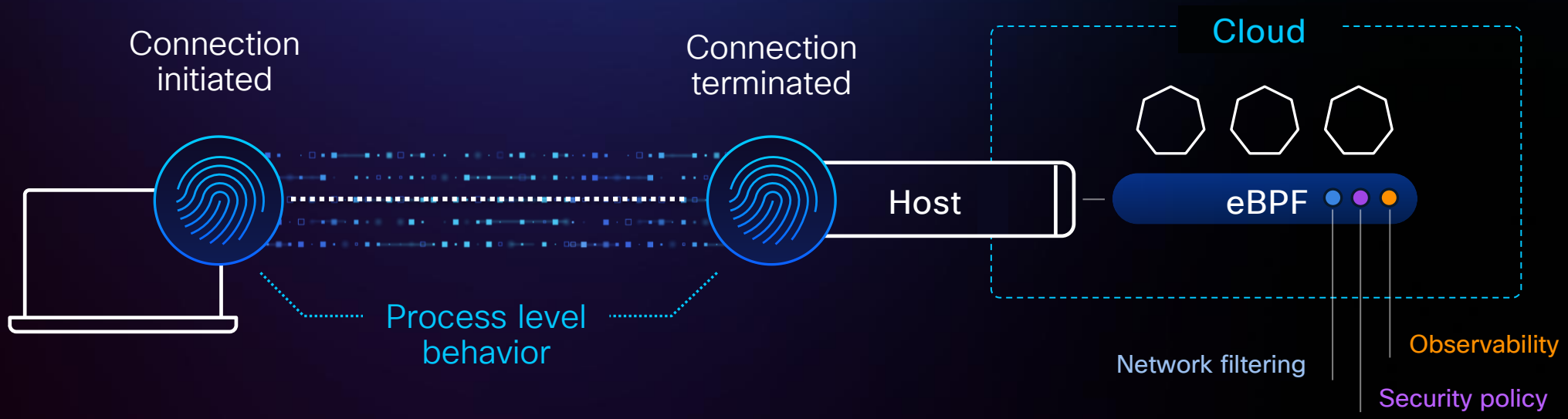
Single appliance, dual personality

Greater visibility, fewer dropped packets

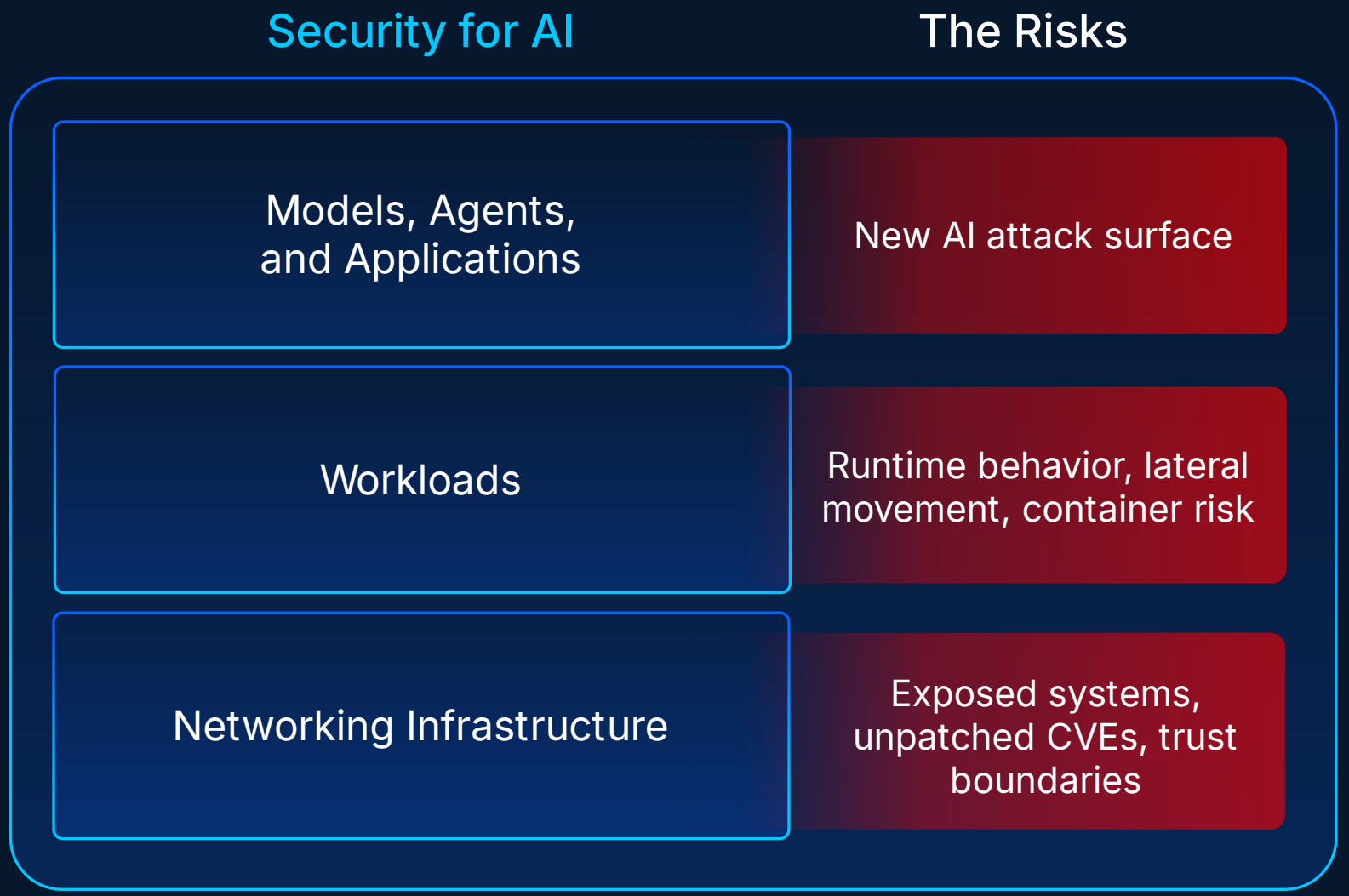
Easily scale security as traffic volume increases

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.

Firewalls are the first line of defense



Early detection of threats in encryption

Cisco Encrypted Visibility Engine



Detect inline zero-day threats

Threat Intelligence



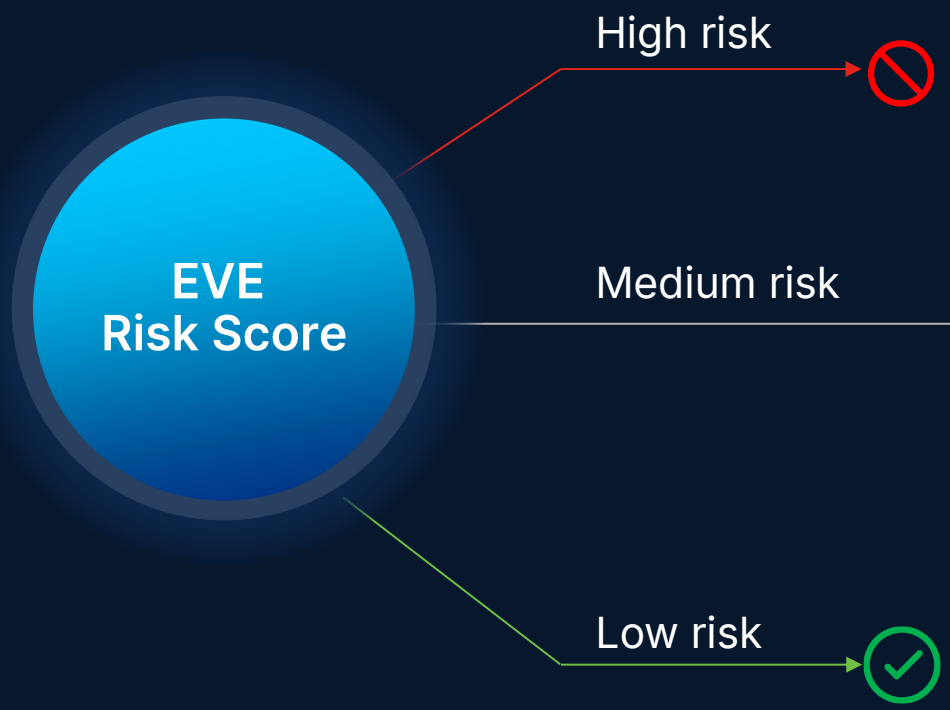
Intelligent segmentation

Native Integration

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

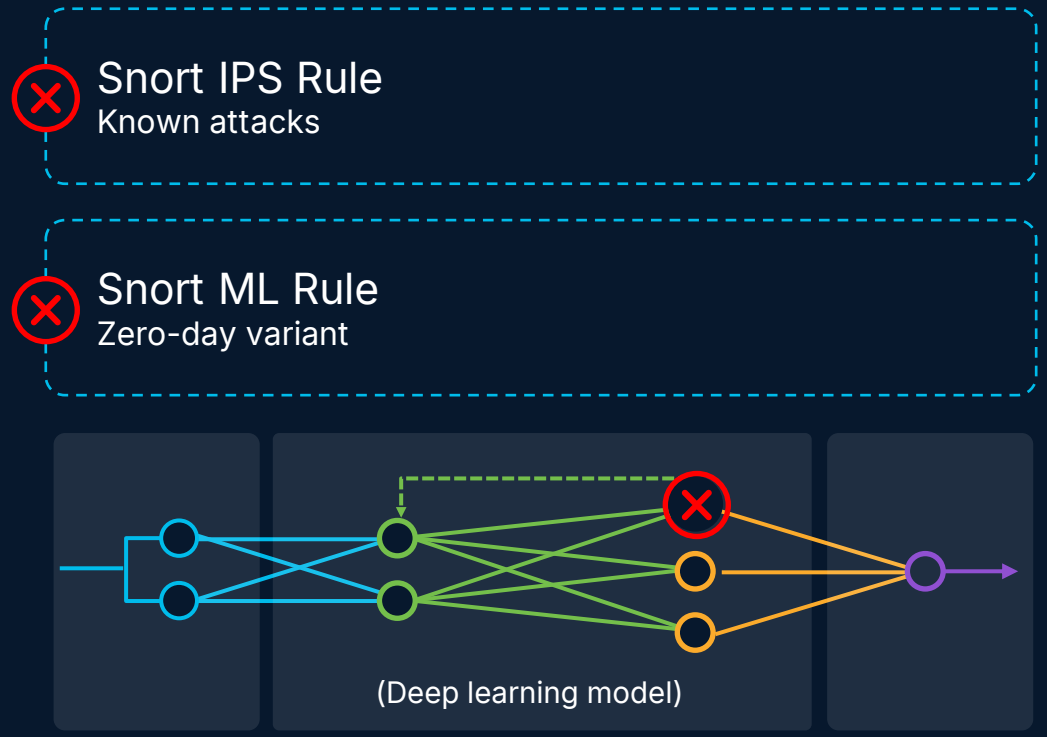
Next-Generation Traffic Inspection and Defense

Visibility to malicious flows in encrypted traffic without decryption



Cisco Encrypted Visibility Engine (EVE)

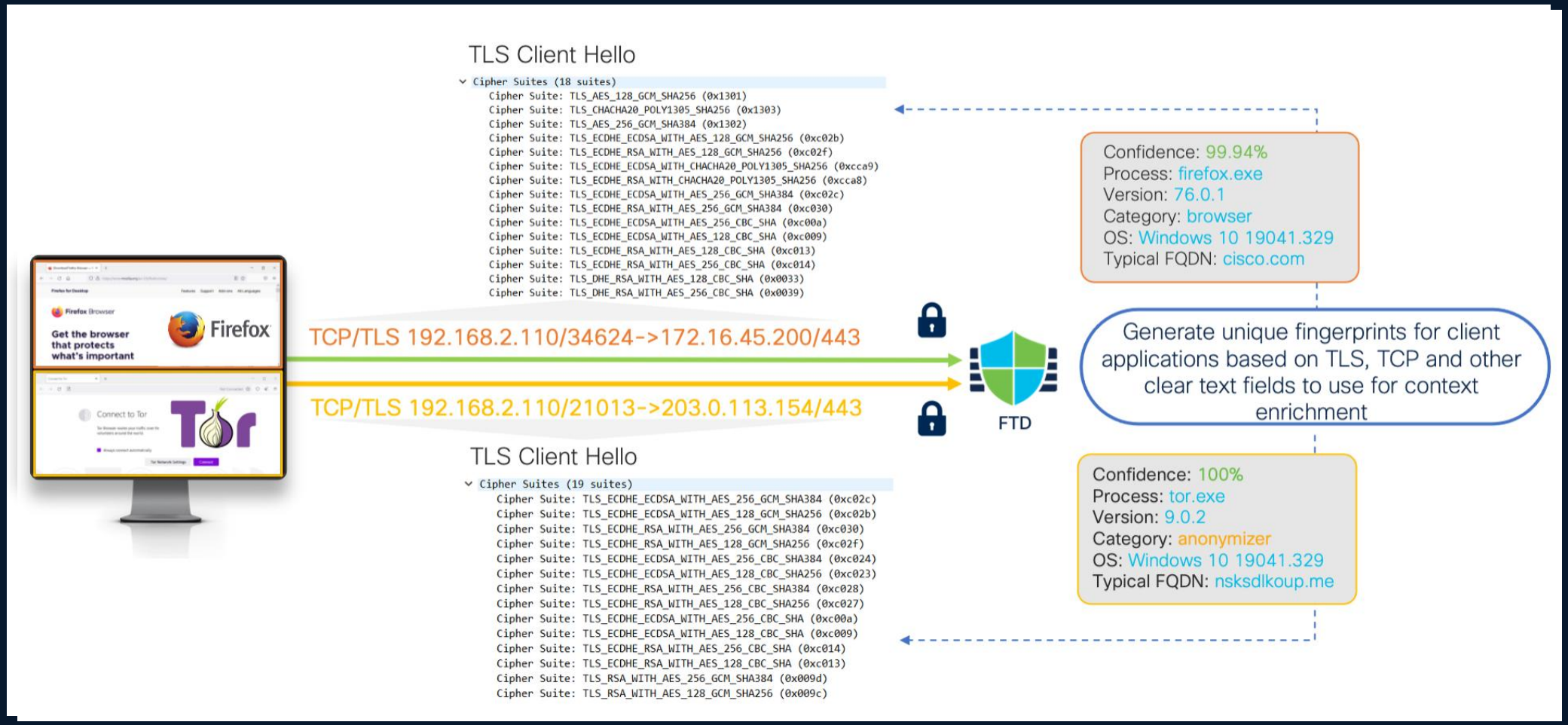
Extends IDPS protection to unknown variants of common attacks



Powered by TALOS Intelligence

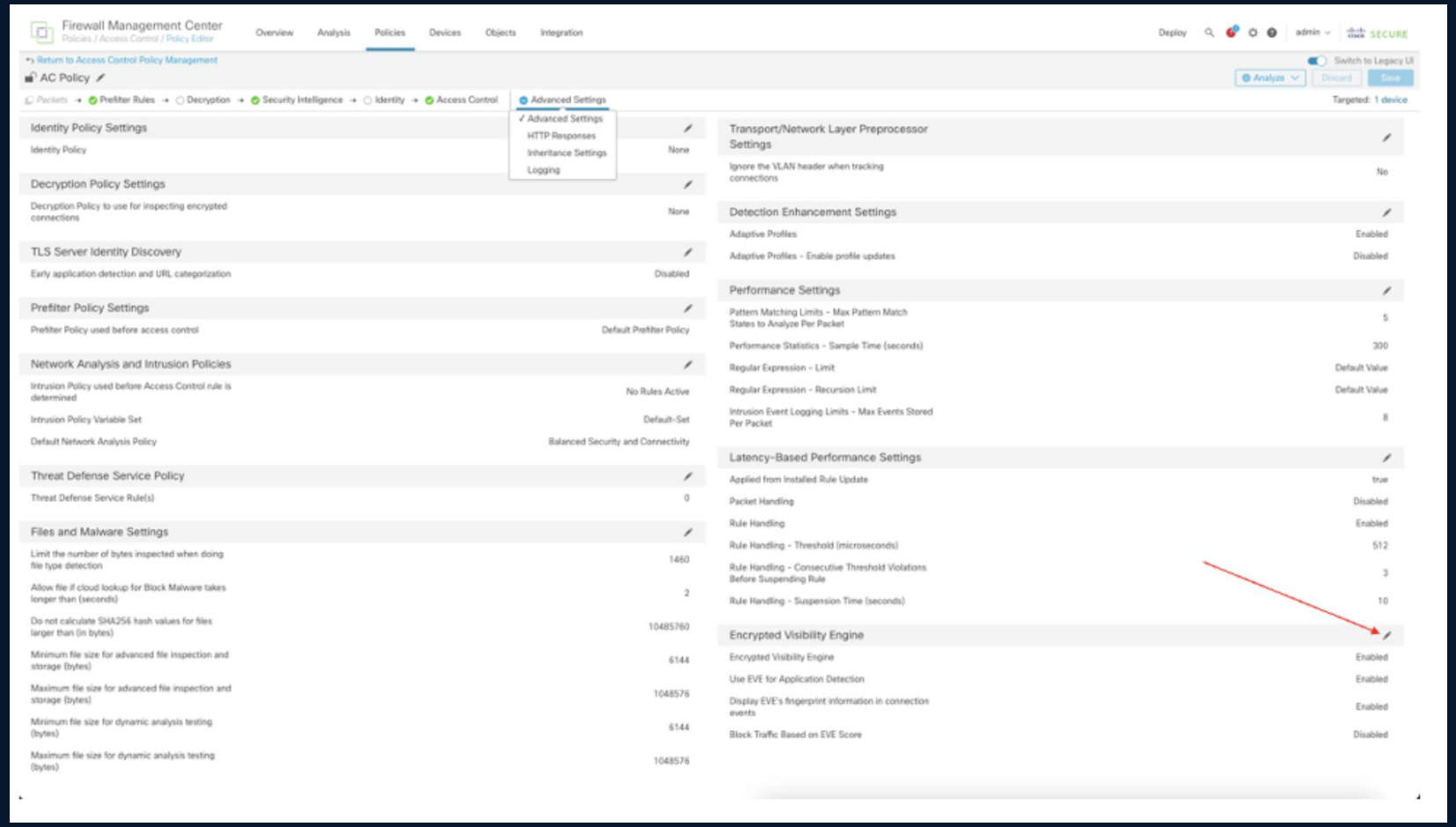
© 2026 Cisco and/or its affiliates. All rights reserved.

Next-Generation Traffic Inspection and Defense



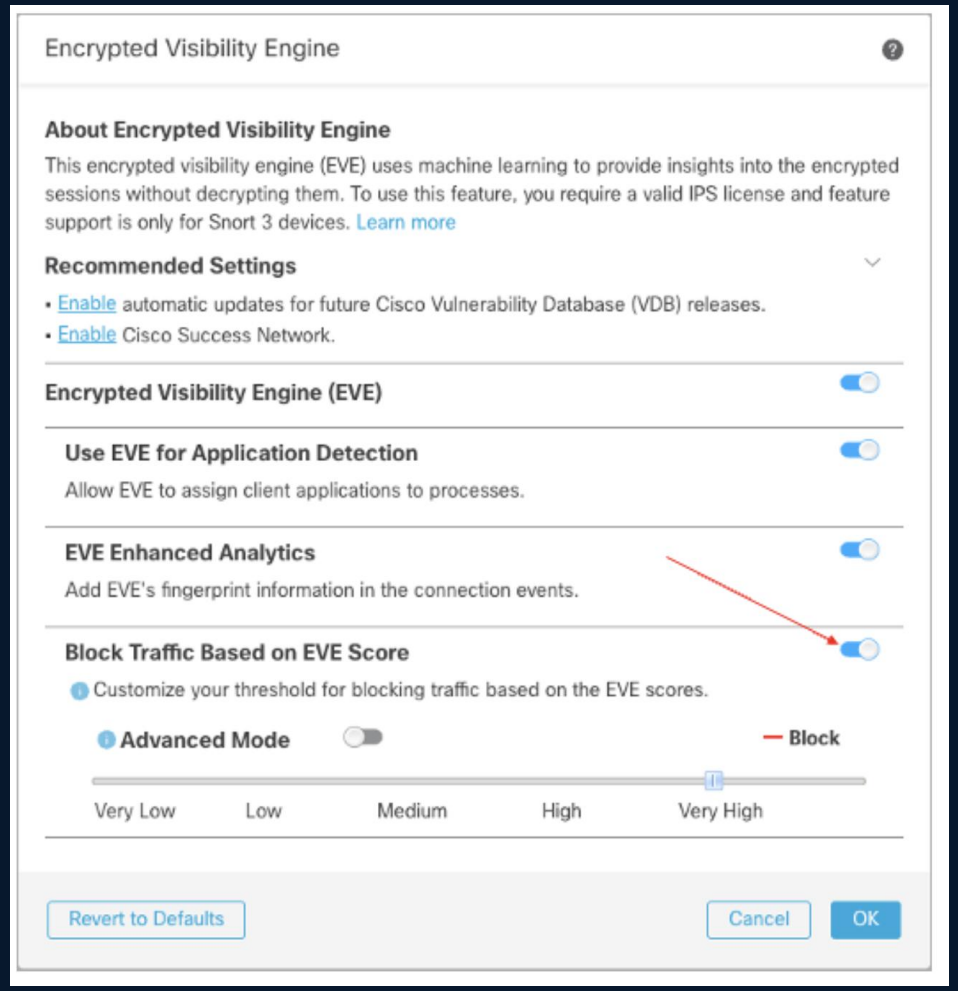
© 2026 Cisco and/or its affiliates. All rights reserved.

Next-Generation Traffic Inspection and Defense



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

Next-Generation Traffic Inspection and Defense



© 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

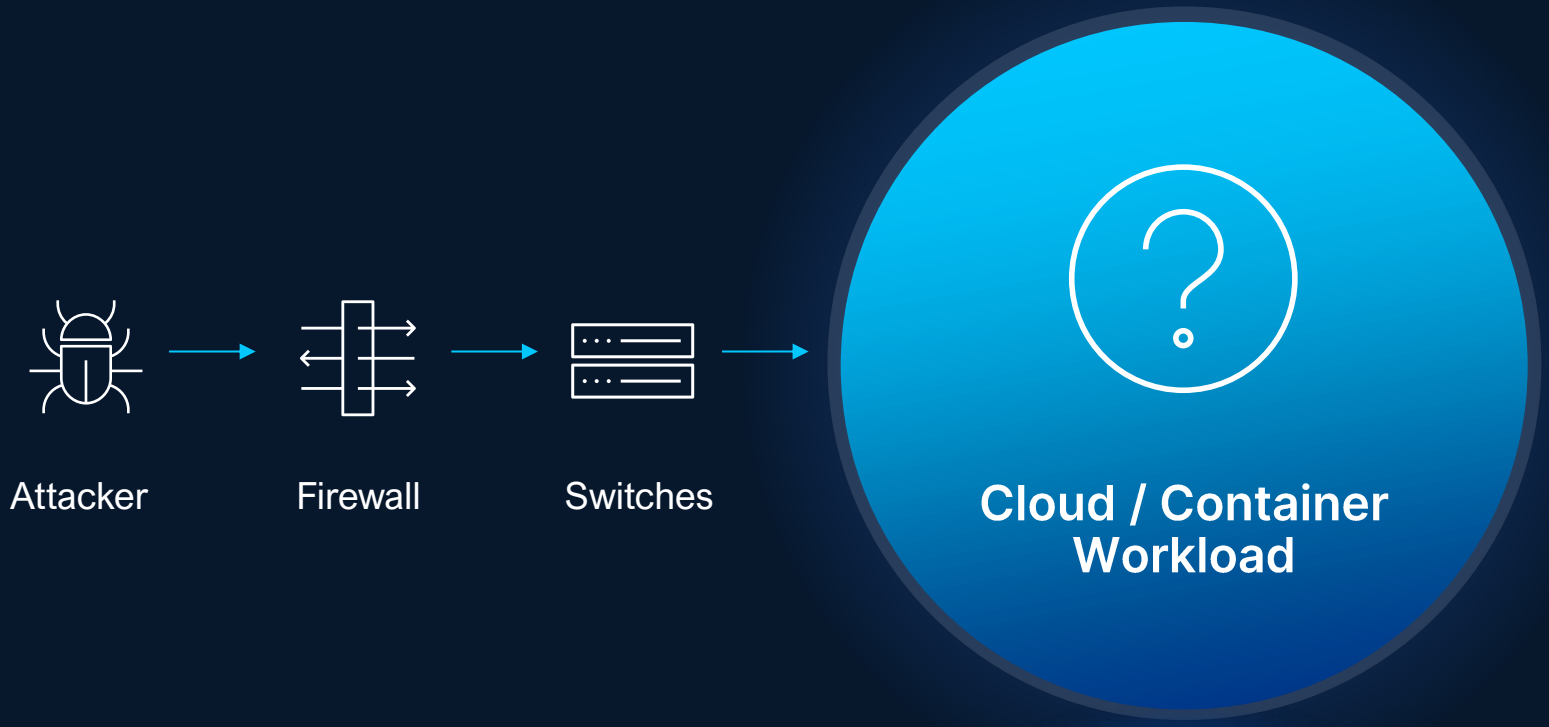
© 2026 Cisco and/or its affiliates. All rights reserved.

Securing AI apps & agents



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

How are your workloads protected?



SEGMENTATION

Threat containment

Limiting blast radius

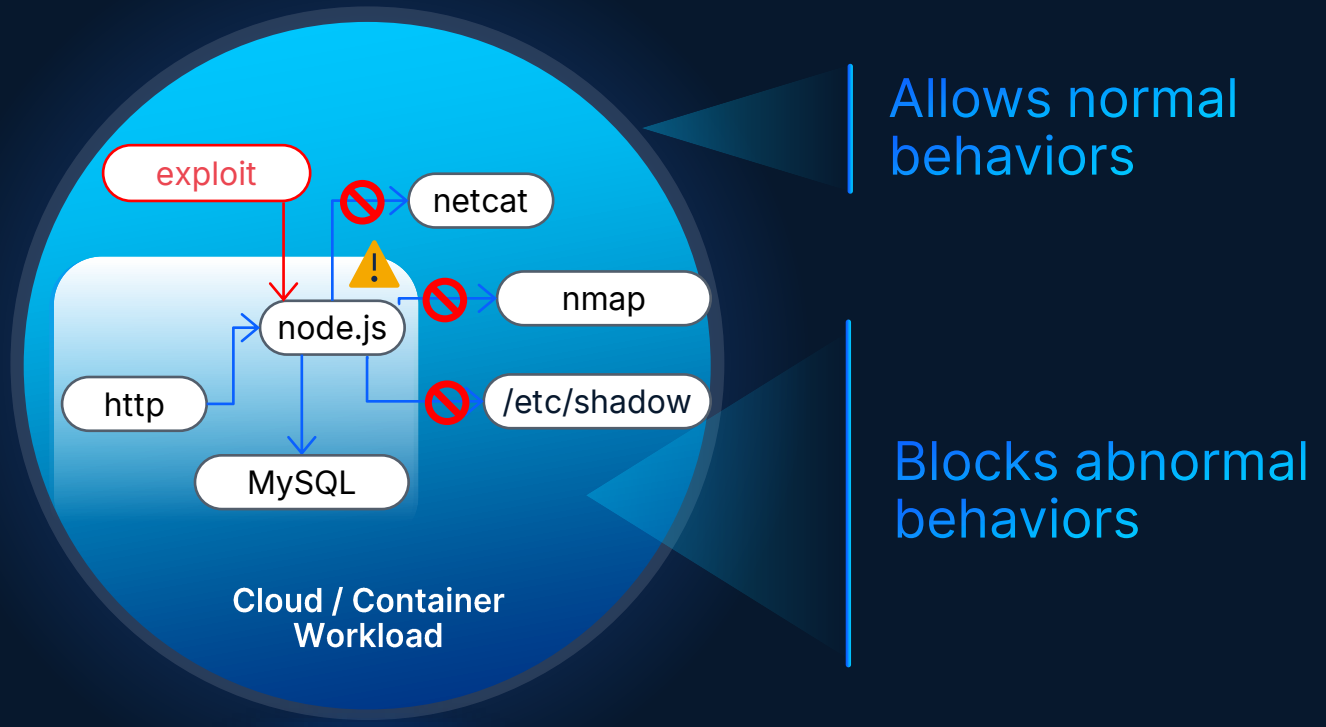
Identity-driven

© 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.

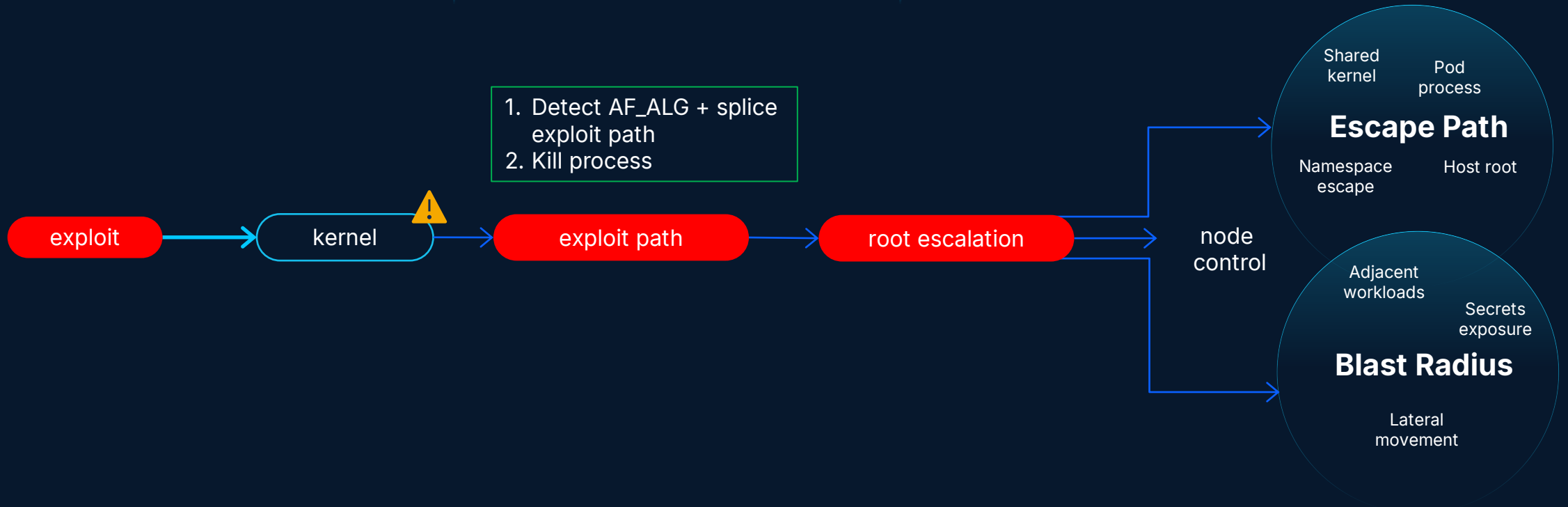
What is eBPF?

- eBPF - extended Berkely Packet Filter
- A way to safely extend the Linux the Linux kernel without recompiling
- Allows us to make real time changes to the way packets are handled at the kernel level -- this includes intra container traffic that may never hit the wire to be seen by a switch with LiveProtect or a firewall

© 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

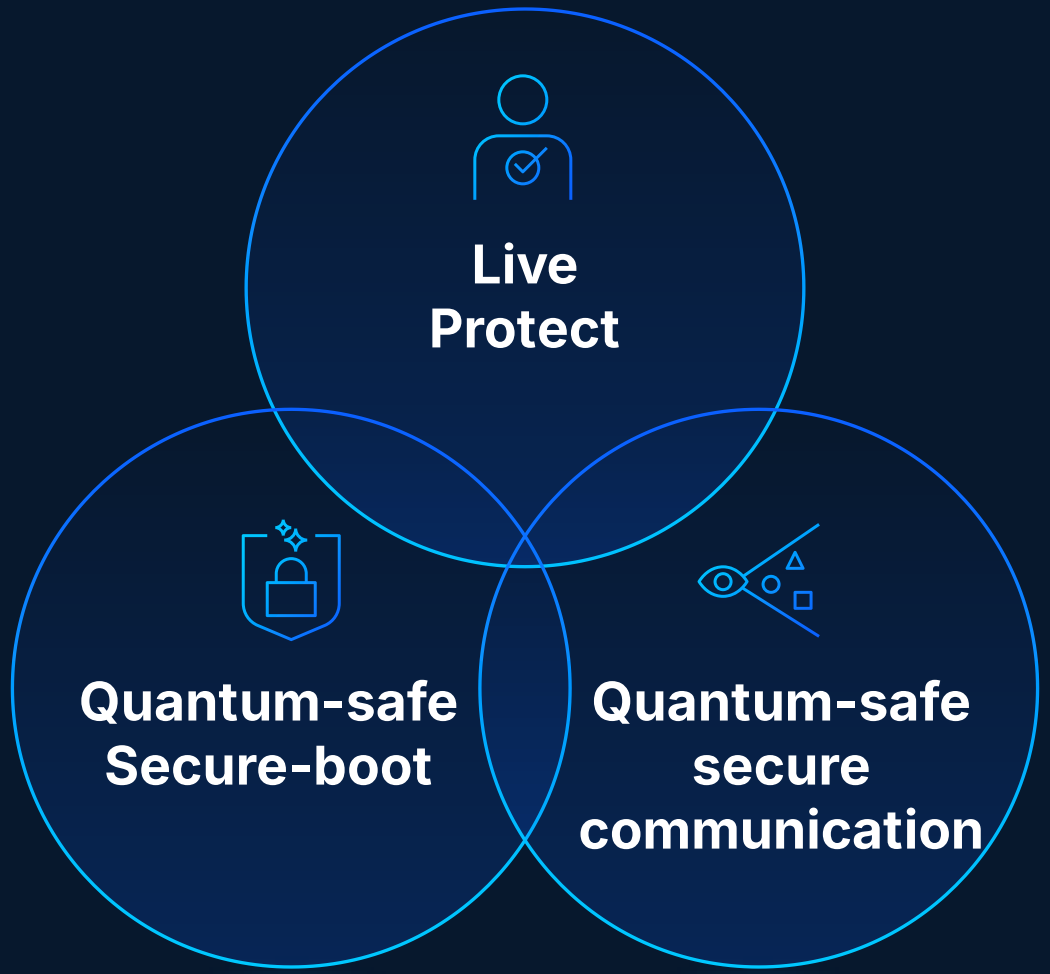


Kernel-level visibility. Runtime enforcement. Defense-in-depth while patching.

© 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



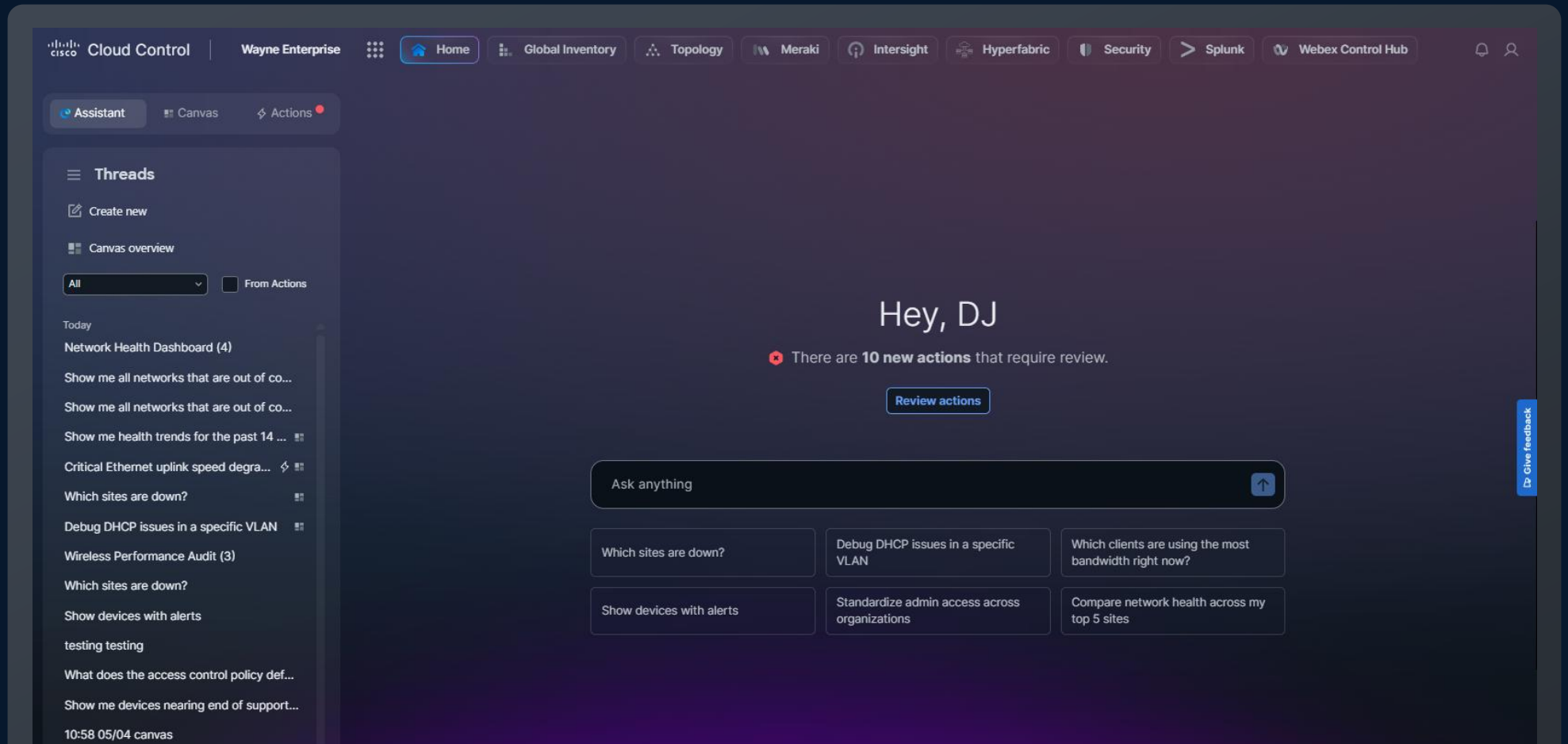
Hardware-accelerated segmentation on every port

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

Cisco Cloud Control

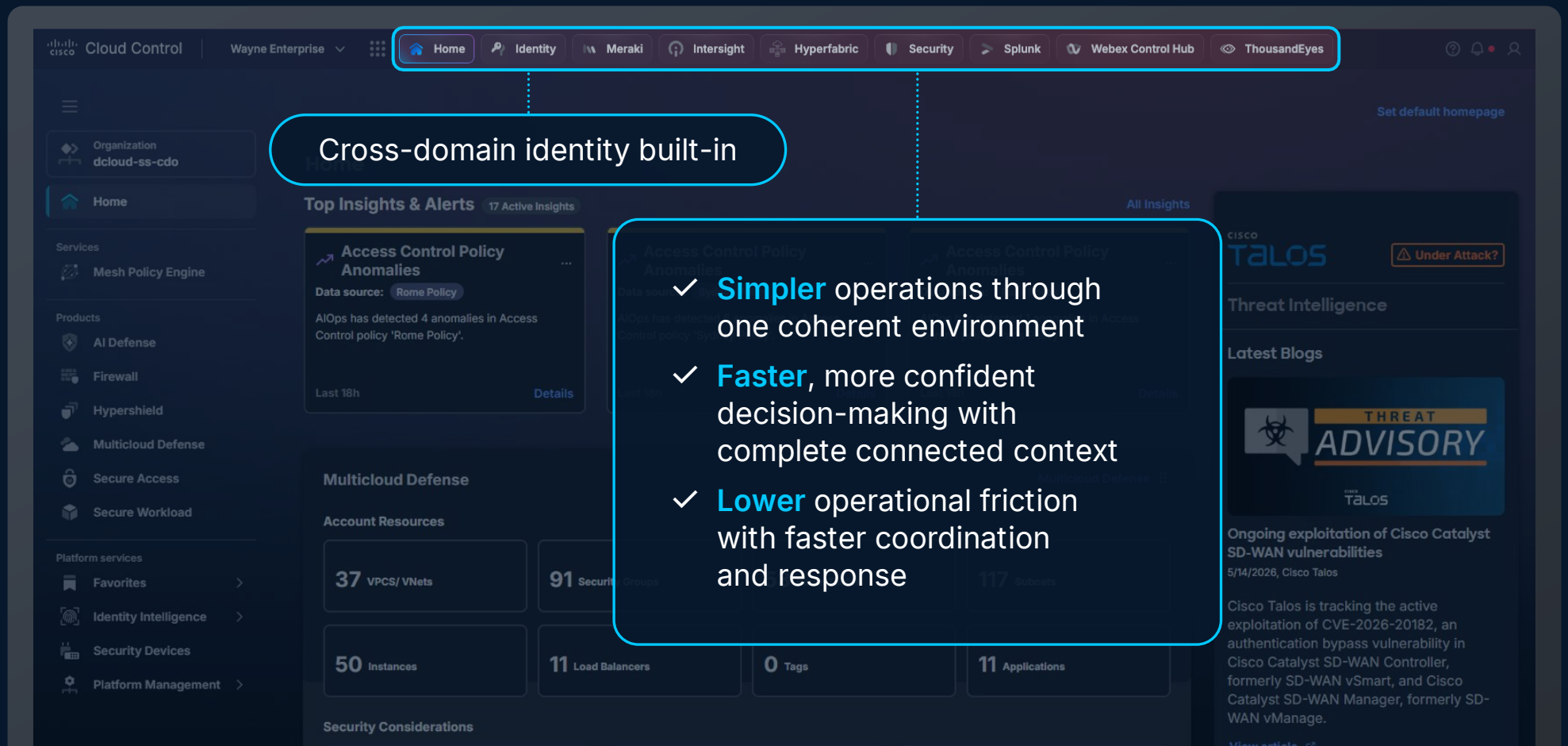
One platform. Every domain. The foundation everything else is built on.

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.



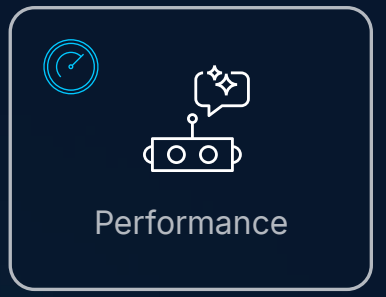
Example

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



CISCO

paloalto NETWORKS

FORTINET

JUNIPER NETWORKS

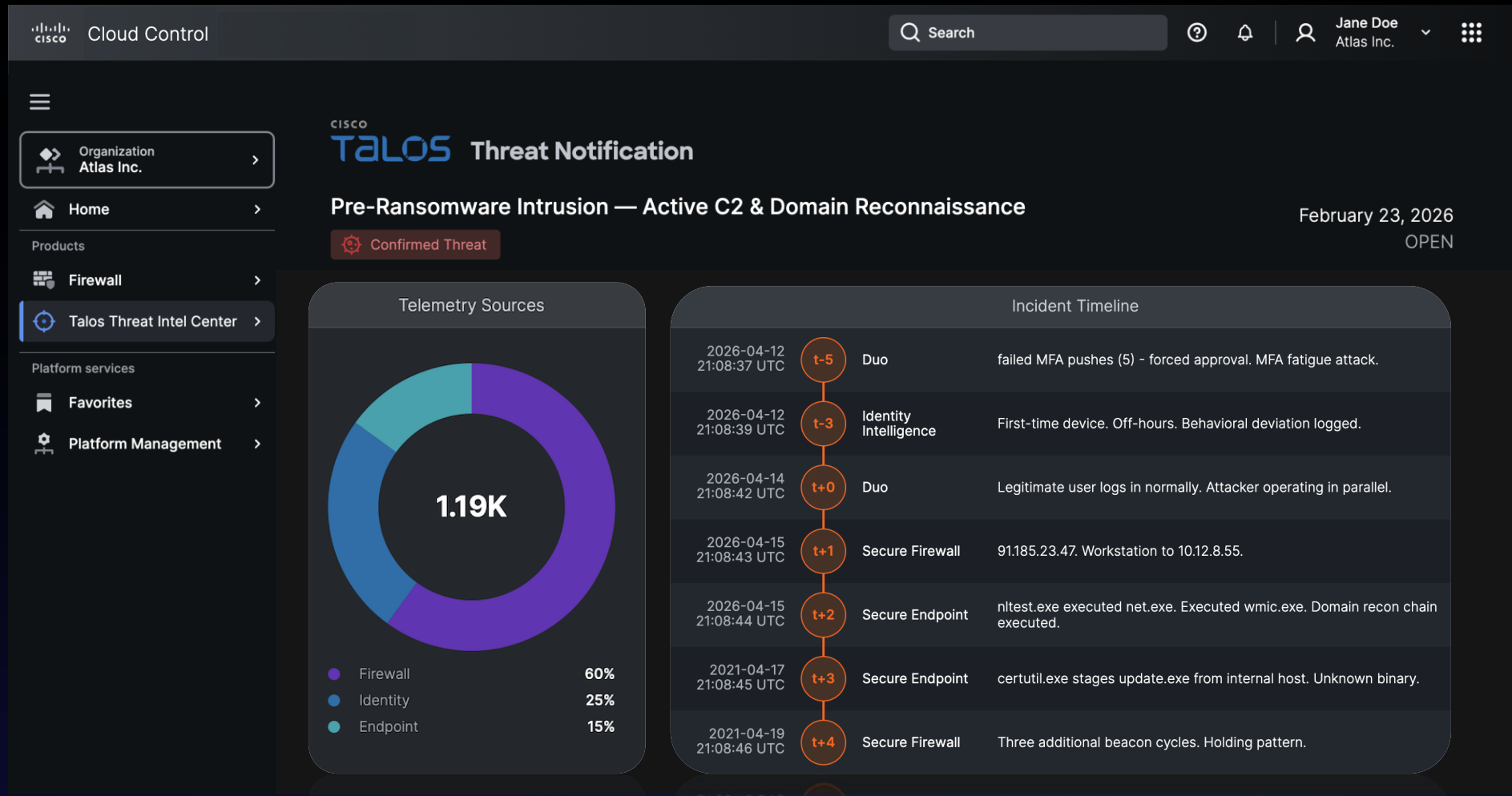
Absorb and optimize existing rules

Change enforcement points, not policy

No rip and replace

Introducing Cisco Talos Threat Hunting

A helping hand for the Mythos era



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.

From Connect to action: Next steps

Free AI Tools - AI Defense Explorer Edition, DefenseClaw, LLM Scorecard

AI Defense: Explorer Edition - A free, self-service tool for your developers and security teams to stress-test AI agents before they hit production. It runs multi-turn adversarial simulations (prompt injection, jailbreaks, unsafe outputs) using the same validation engine behind our Global 2000 deployments and generates exportable compliance reports. Try it for free here: https://explorer.aidefense.cisco.com/

DefenseClaw - An open-source (Apache 2.0) secure agent framework, built on NVIDIA OpenShell. It scans agent skills, MCP servers, agent-to-agent traffic, generated code, and supply chain components before anything executes, then enforces guardrails at runtime with full audit logging into Splunk or any OTLP backend. Blocked skills have permissions revoked and files quarantined in under two seconds, no restart required. The DefenseClaw GitHub link is: https://github.com/cisco-ai-defense/defenseclaw

LLM Security Leaderboard - A public ranking of popular LLMs by their resilience to adversarial attacks, so your teams have an objective signal when choosing which models to trust in production. You can find it here: https://leaderboard.aidefense.cisco.com/rankings

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

From Connect to action: Next steps

Free AI Tools - AI Defense Explorer Edition, DefenseClaw, LLM Scorecard

AI Defense Explorer Edition: https://explorer.aidefense.cisco.com/

DefenseClaw: https://github.com/cisco-ai-defense/defenseclaw

LLM Scorecard Leaderboard: https://leaderboard.aidefense.cisco.com/rankings

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

CISCO Connect

Thank you




CISCO