CISCO Connect

Every Packet. Every Process. Every Workload

Cisco Hybrid Mesh Firewall

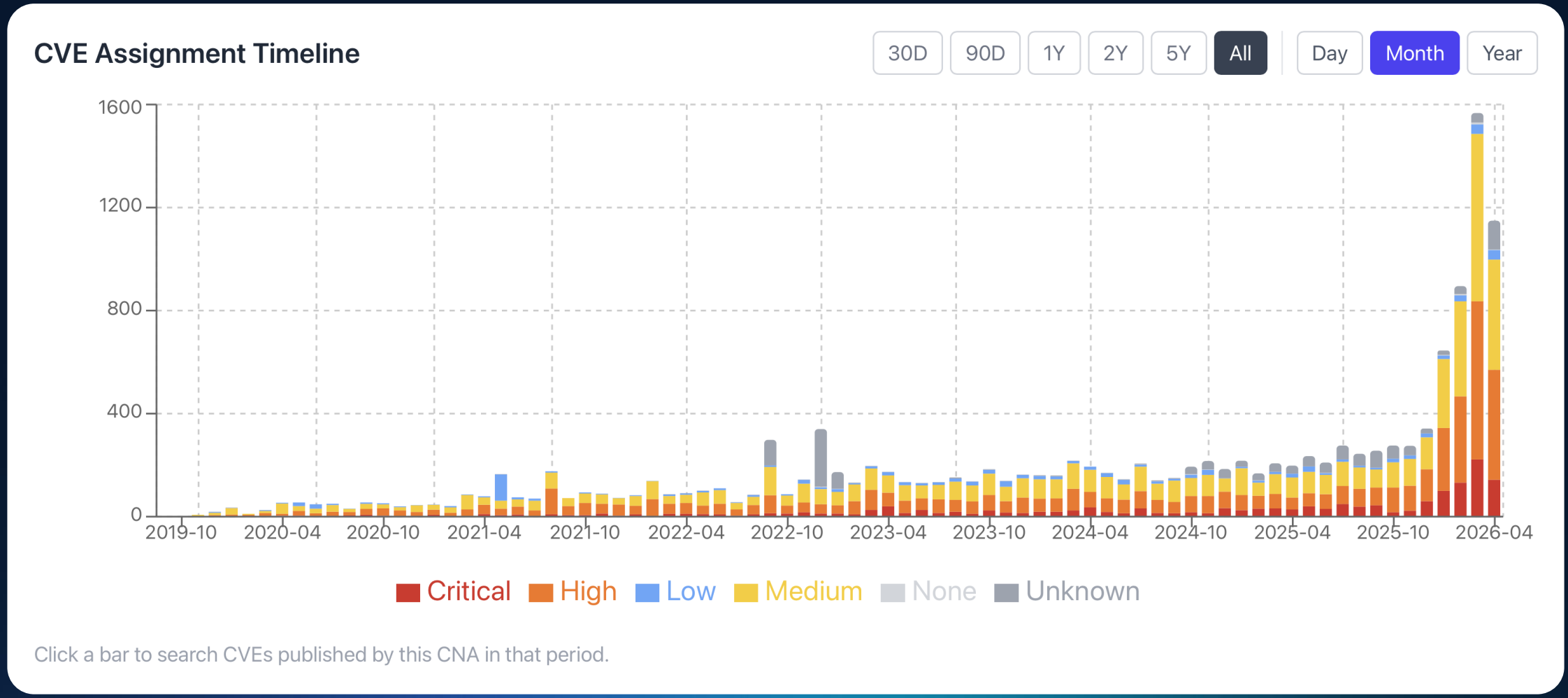


Nadir Lakhani, Technical Solutions Architect - Global

Anwar Adil, Technical Solutions Architect

October 21, 2026

Vulnerability Reports are Spiking



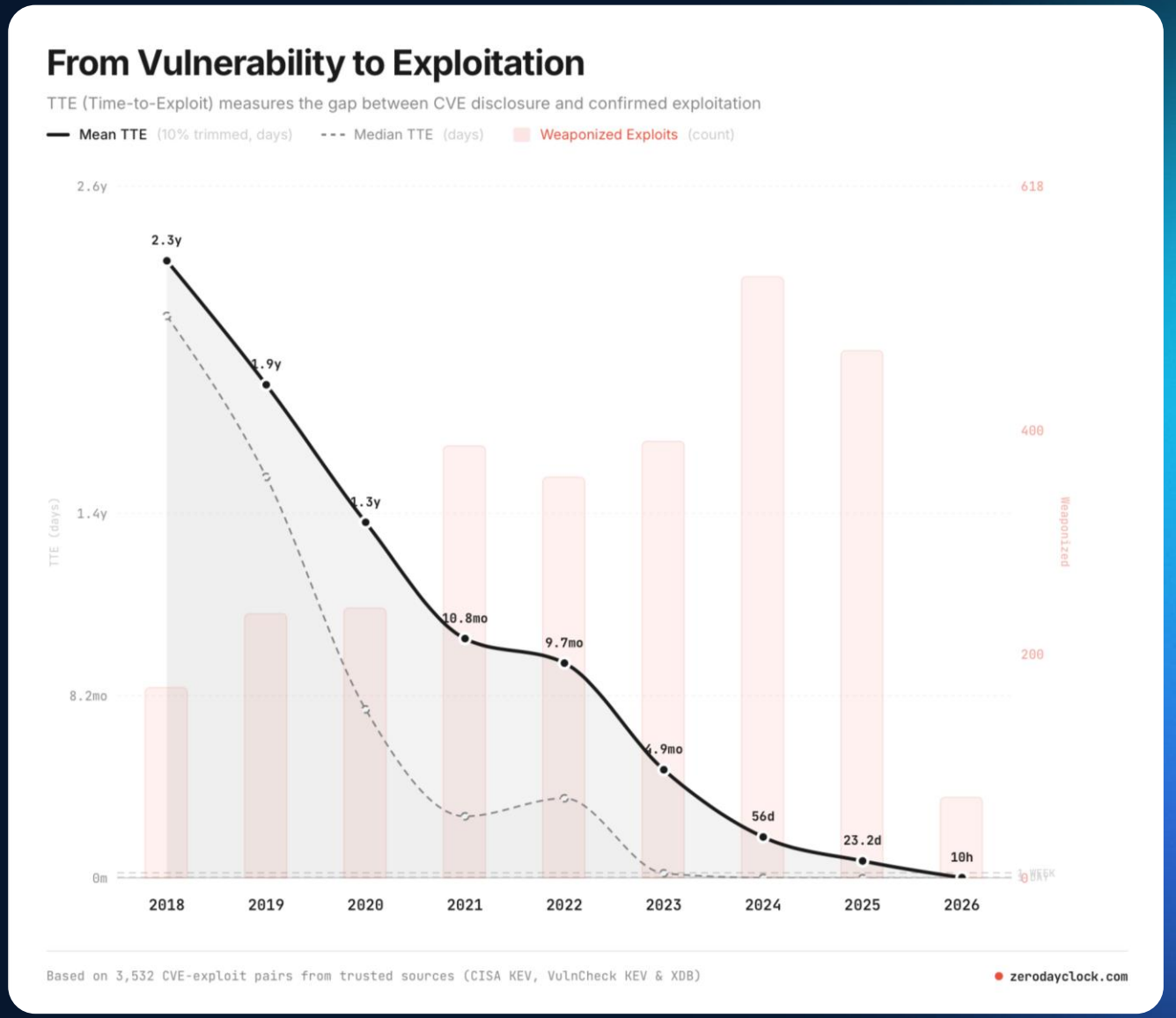
Source: https://zerodayclock.com/

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

Cisco Confidential

The Weaponization Window has Collapsed

Industry-wide Impacting All Vendors



Source: https://vulntools.net/cnas/GitHub_M

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

Adversaries are using AI-speed discovery

48%
of network assets worldwide are now aging or obsolete

40%
of the top 100 targeted vulnerabilities impacted end-of-life systems

32%
directly impacted are at least 10 years old

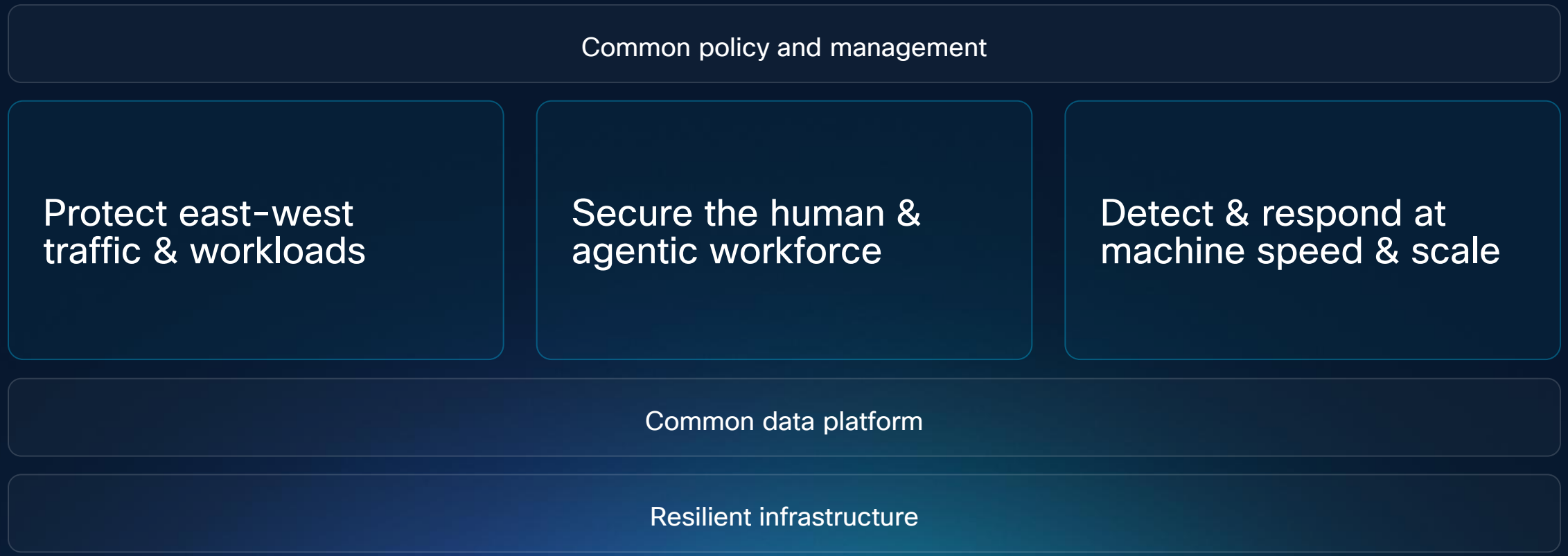
23%
directly impacted network infrastructure devices

Sources: Talos Year in Review, Update Critical Cisco Report

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

Cisco Confidential

Security “must-haves” for the agentic era



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

The agentic era demands three security outcomes

01 Protect east-west traffic & workloads

- Stop lateral movement
- Scale beyond traditional perimeters
- Shield workloads

02 Secure the agentic & human workforce

- Know every agent
- Protect every agent
- Authorize every agent action

03 Detect & respond at machine speed & scale

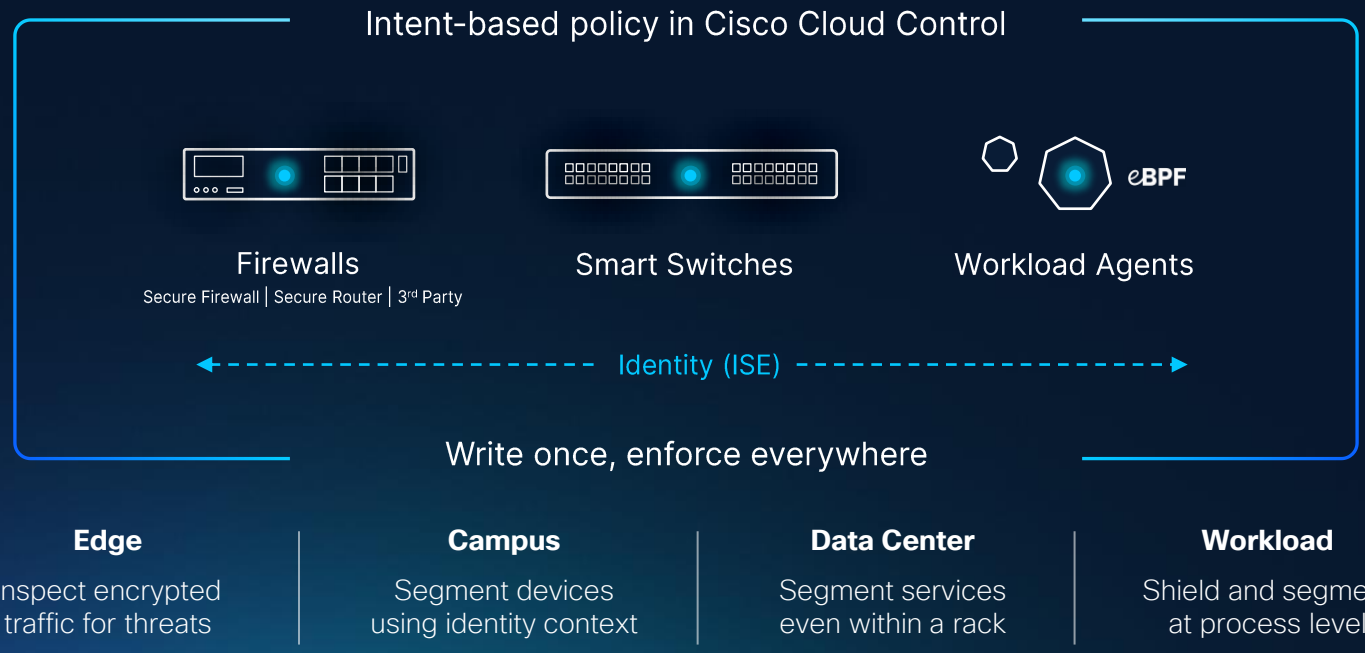
- Leverage machine data at scale
- Detect and respond to threats
- Monitor agent behavior and drift

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

Protect east/west traffic & workloads

Shield workloads and stop lateral movement at the source

Hybrid Mesh Firewall | Security at the speed of change



Edge
Inspect encrypted traffic for threats

Campus
Segment devices using identity context

Data Center
Segment services even within a rack

Workload
Shield and segment at process level

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

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

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

HyperFlex · NUTANIX · KVM · openstack · vmware ESXi · aws · Microsoft Azure · Google Cloud Platform · alkira · rackspace technology · EQUINIX · Alibaba Cloud · ORACLE CLOUD INFRASTRUCTURE

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

Fusing security in

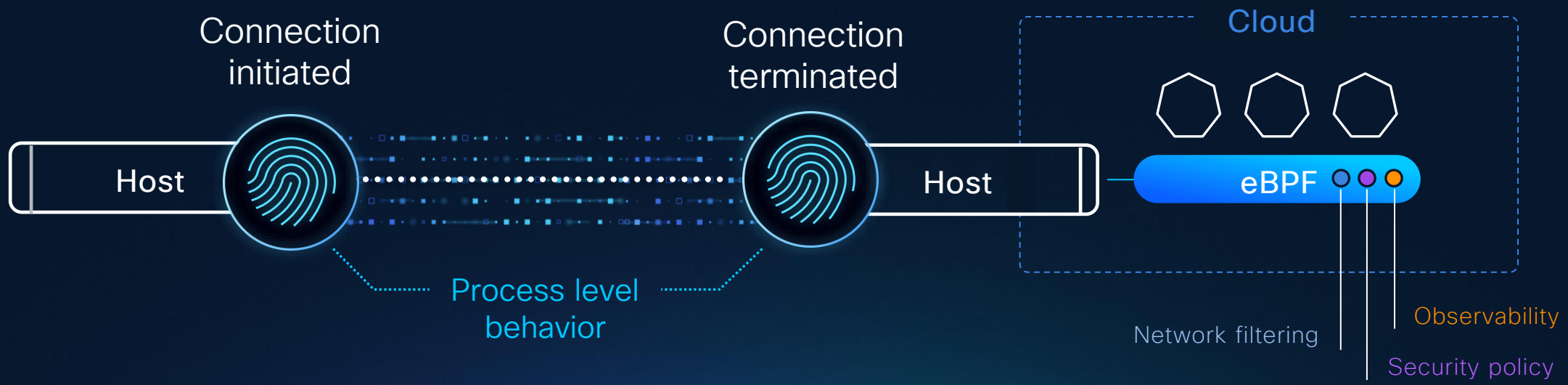


Single appliance, dual personality

Greater visibility, fewer dropped packets

More easily scale security as traffic increases

Process-level visibility for any application



See and control the inner workings of modern apps

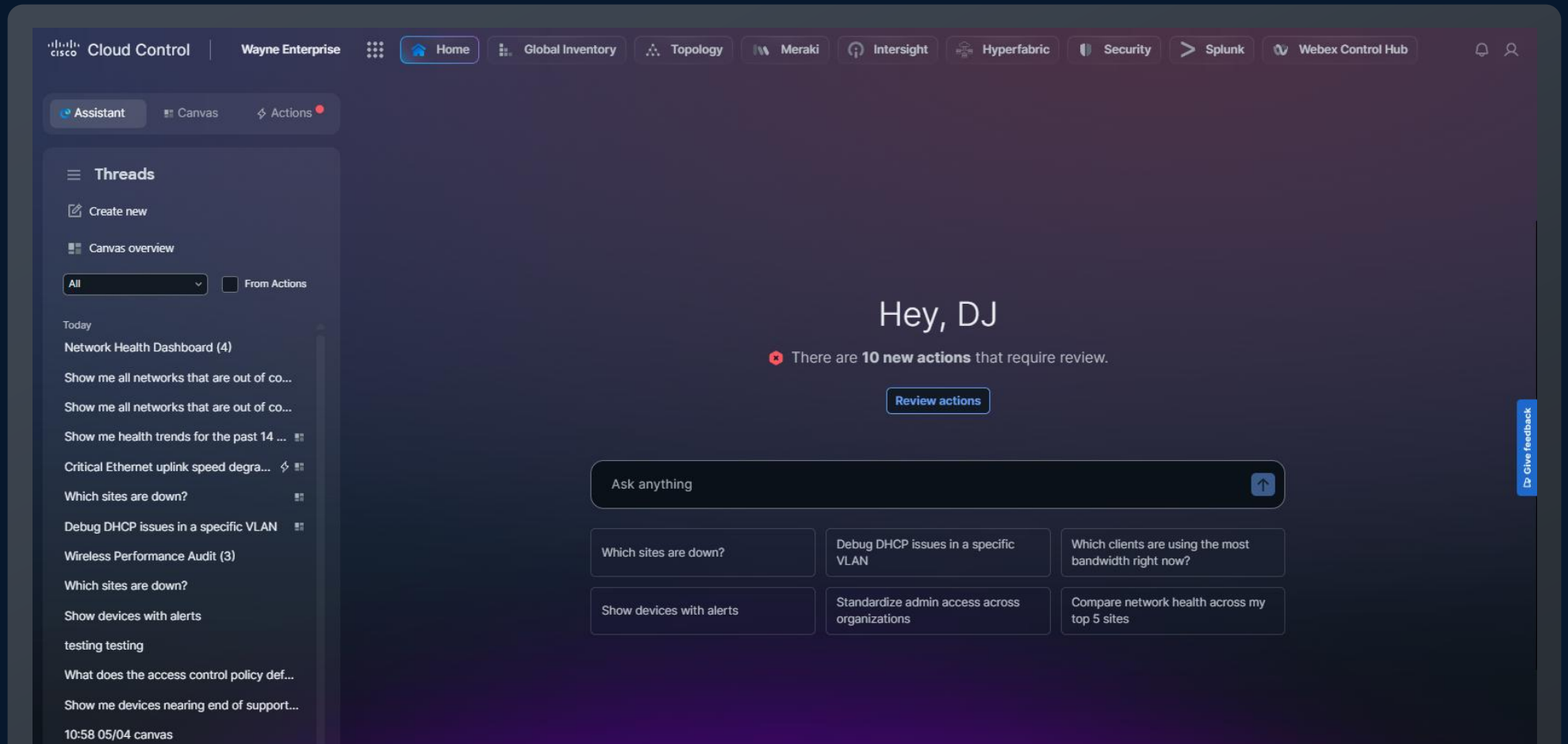
Segment effectively as apps change

Shield vulnerabilities while you patch

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



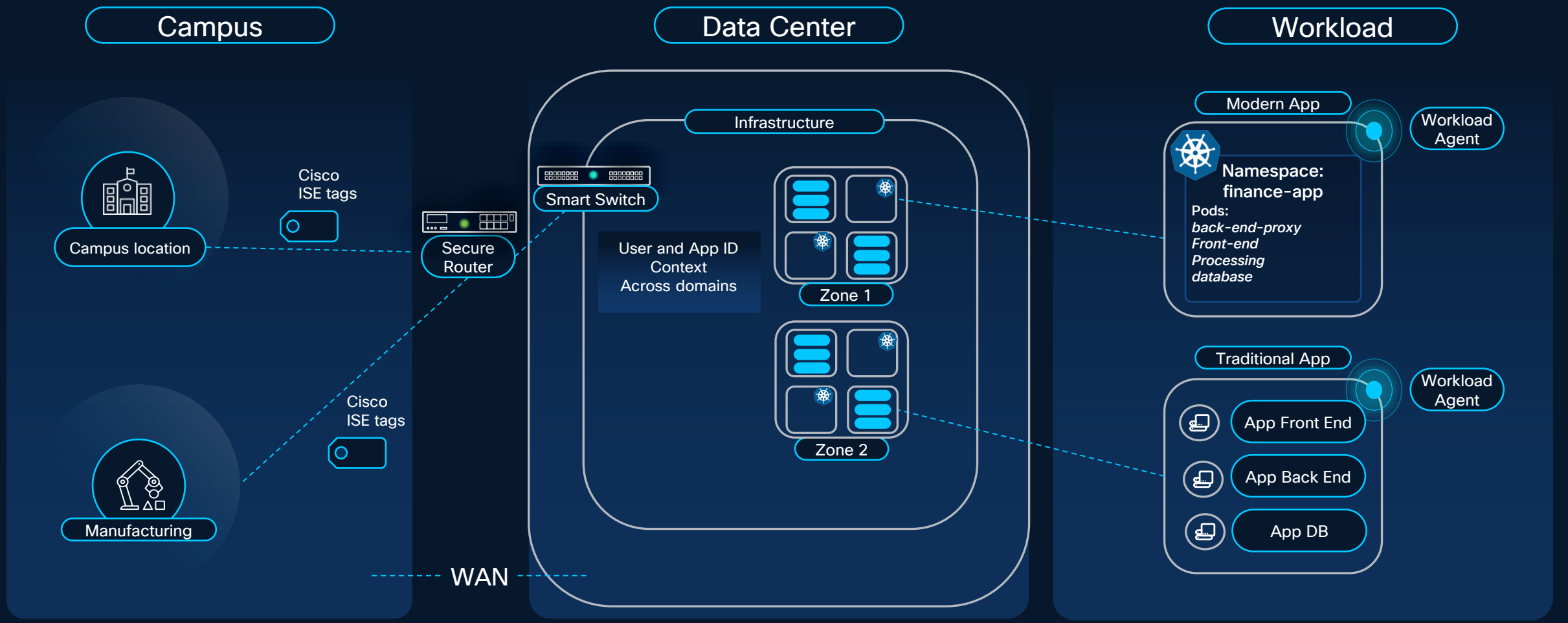
Outcomes we solve for

- Segmentation
- Exploit Protection
- Advanced Threat Protection
- Unified Agentic Operations

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

End-to-end segmentation with Cisco

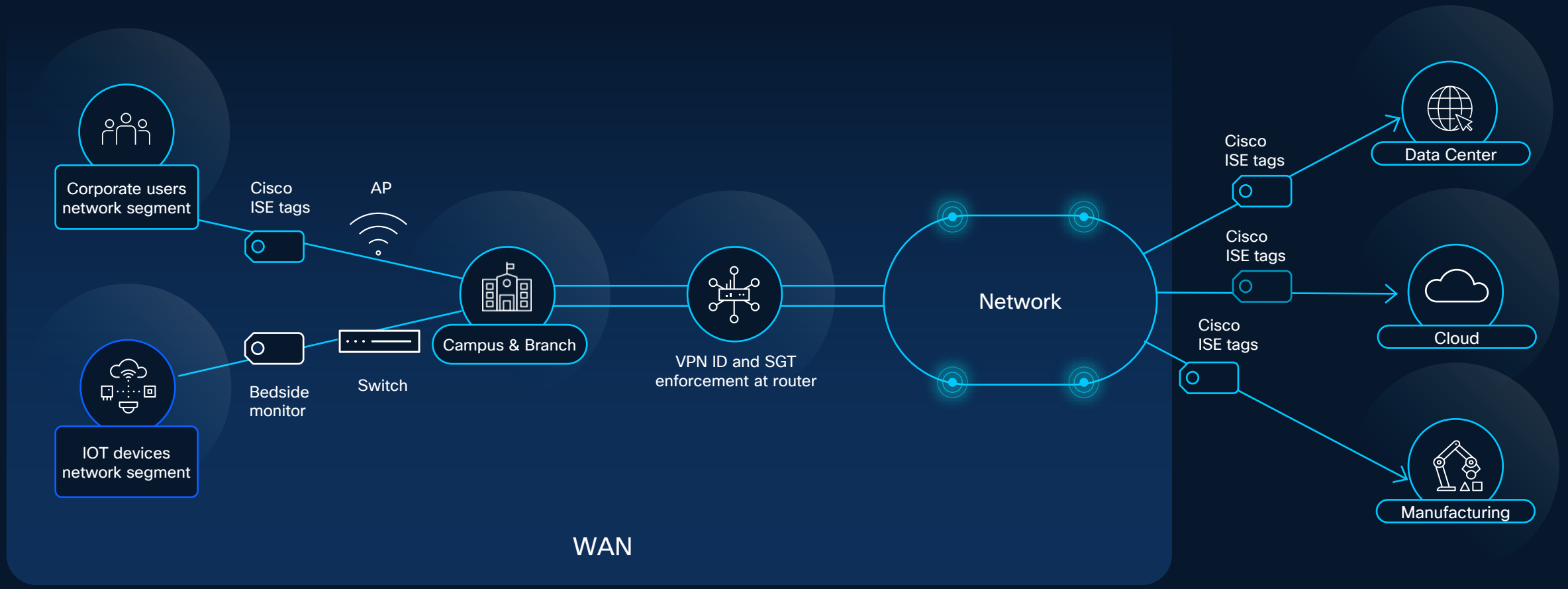
Complete segmentation solution for campus, data center, top of rack, as well as traditional and modern workloads



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

ISE tags can be pushed across the WAN to data center

Security Group Tags (SGTs) push policy across campus through WAN to firewalls at data center, cloud, and manufacturing



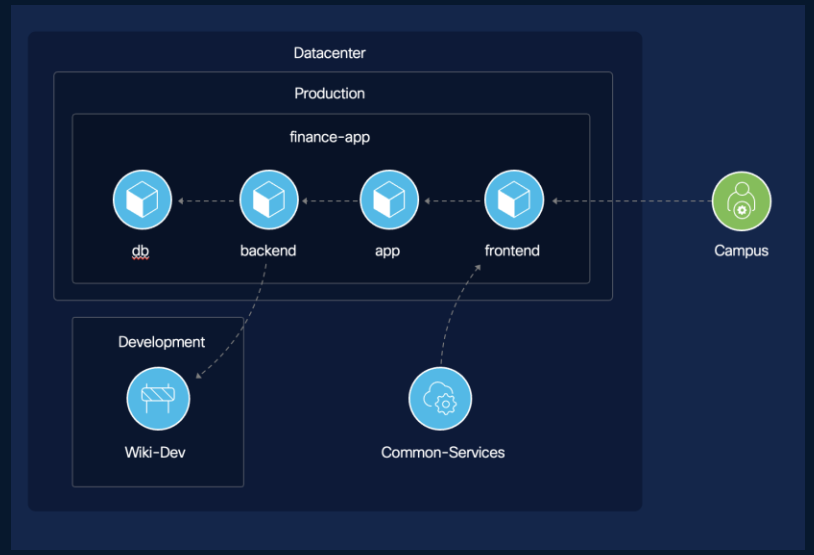
© 2026 Cisco and/or its affiliates. All rights reserved.

Automated Application Policy Discovery

Baseline workload protection posture

- Network communications
- Process behavior
- Labels
- ISE SGT tags

Secure Workload



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

Hypershield for Nexus Smart Switch

Hypershield turns
every port
on the Nexus N9300 Smart Switch
into an enforcement point

Hypershield programs
Smart Switch DPU
to bring distributed
Stateful L3/L4 segmentation

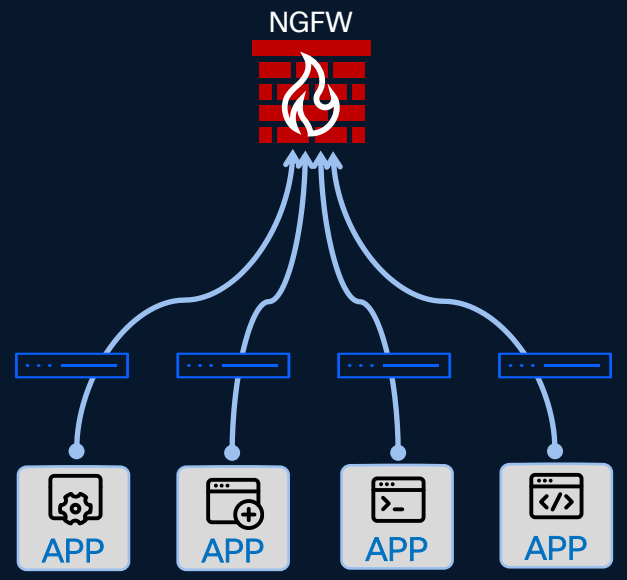


DISTRIBUTED | STATEFUL | SECURE | FUSED INTO THE FABRIC

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

Hyper-distributed security, without the bottlenecks

Traditional
Centralize chokepoint

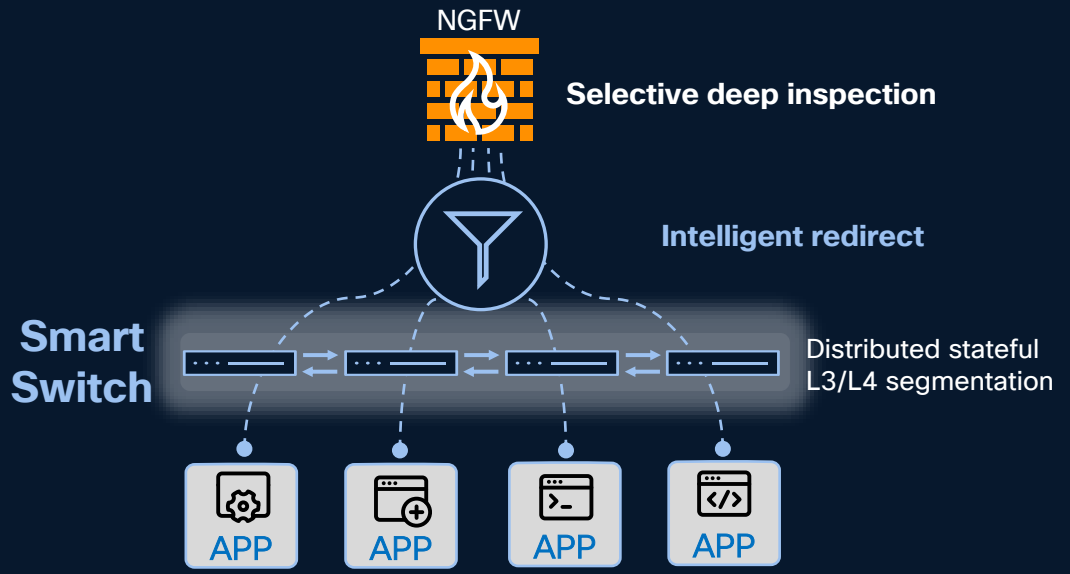


Performance bottlenecks

High cost at scale

High cost at scale

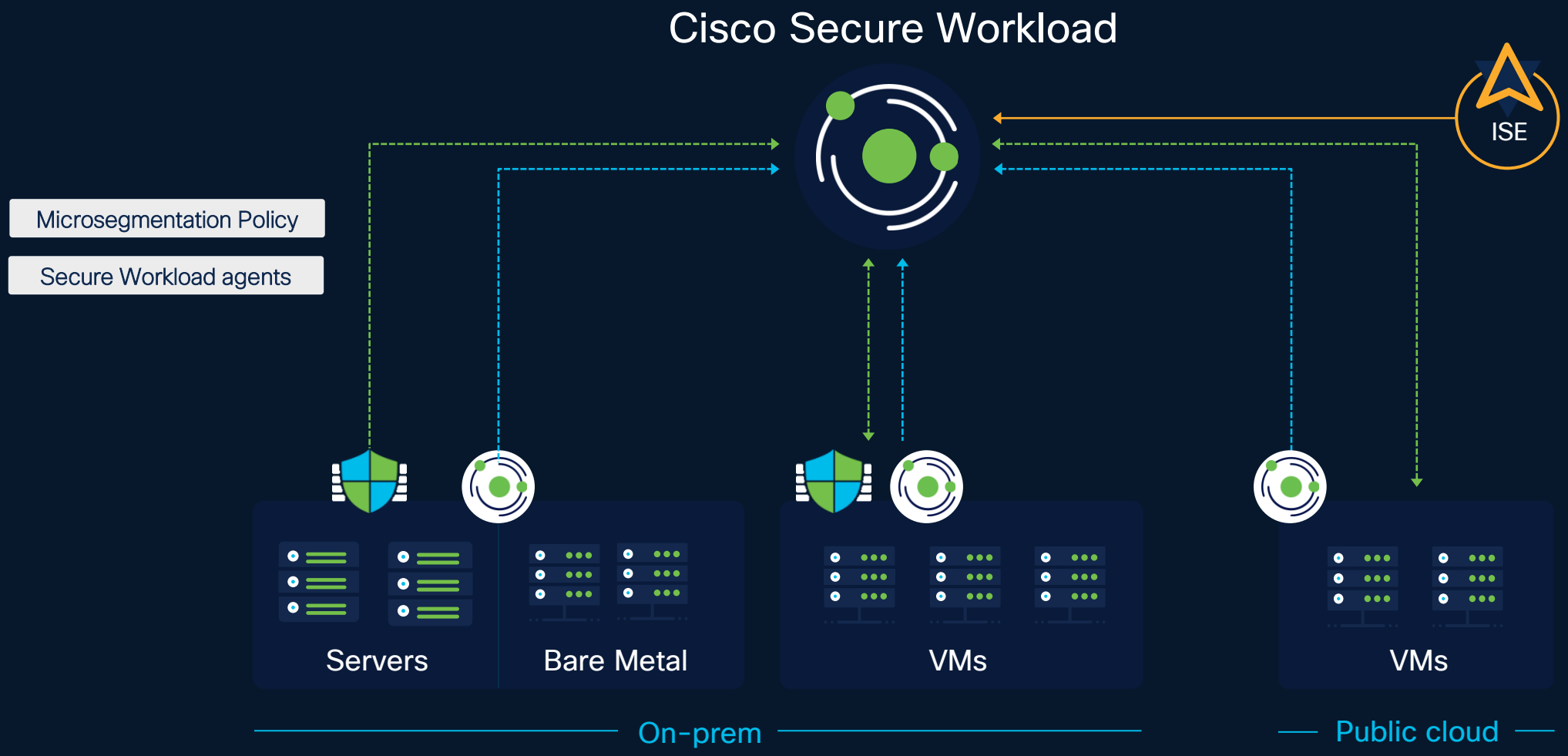
Modern
Distributed enforcement



Distributed stateful segmentation for every flow
Deep inspection for selected flows
Organic horizontal growth

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

Microsegmentation with Secure Workload



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

eBPF: Extending network controls into cloud-native workloads



Extends security and observability into cloud-native architectures

Process-level container and workload visibility without risks of kernel modules

Based on open-source Cilium and Tetragon, which Cisco shepherds

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

Infrastructure is the new target

Salt Typhoon Living off the network

- VALID CREDENTIALS
- CONFIG THEFT
- PIVOT CHAINS
- PACKET CAPTURE
- LOG WIPES



REDUCE EXPOSURE / MAINTAIN CONTINUITY / PLAN FOR THE PATCH

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

Source: Cisco Talos

SHIELDS UP

You can’t patch fast enough.

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

Live Protect

Vulnerability shielding for Cisco 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.

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

NetSecOPEN independently validates Cisco Secure Firewall 6160

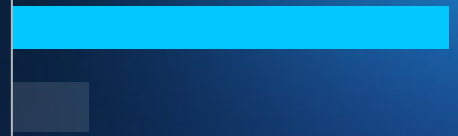


Our firewall hit the test tools' CPU limits and could've kept going

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

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

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

Cisco Encrypted Visibility Engine



Visibility to malicious flows in encrypted traffic without decryption

Machine learning (ML) technology

Processes 1 B+ TLS fingerprints

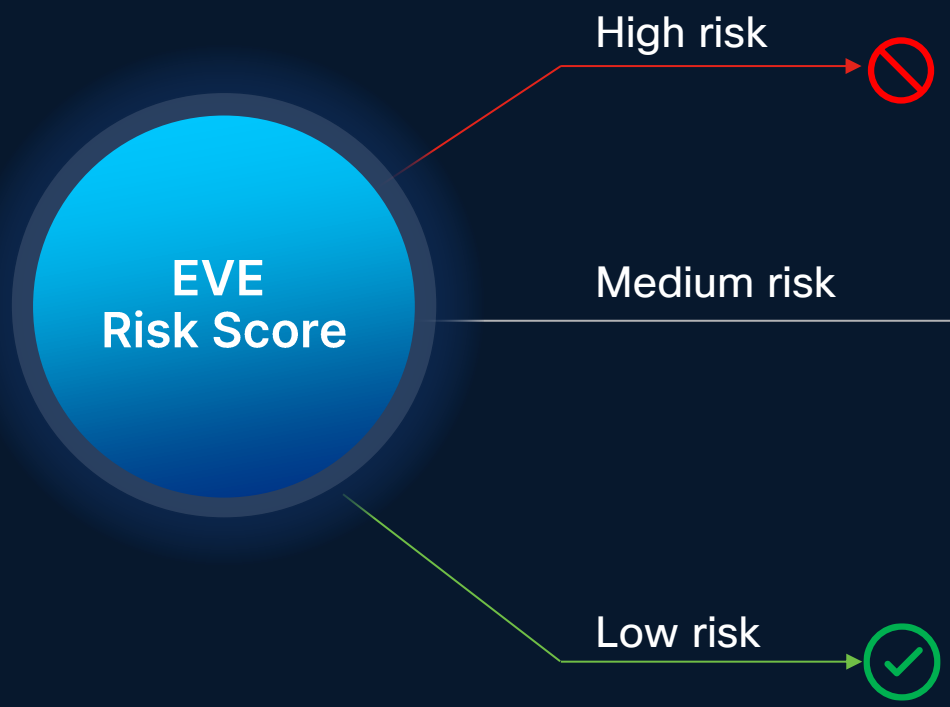
Processes 10 K+ malware samples daily

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

cisco

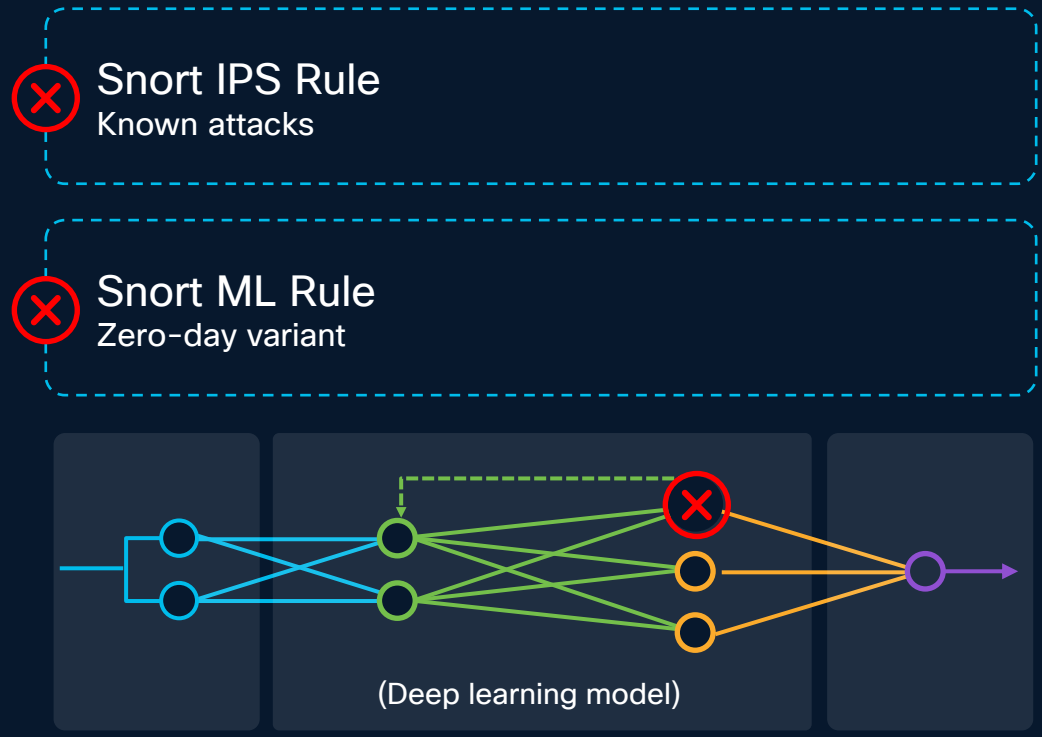
Next-Generation Traffic Inspection and Defense

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

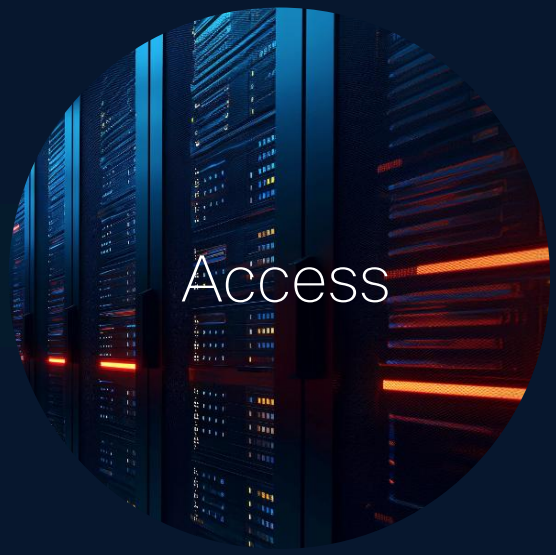
© 2026 Cisco and/or its affiliates. All rights reserved.

Identity Intelligence

Continuously assess you are
who you say you are

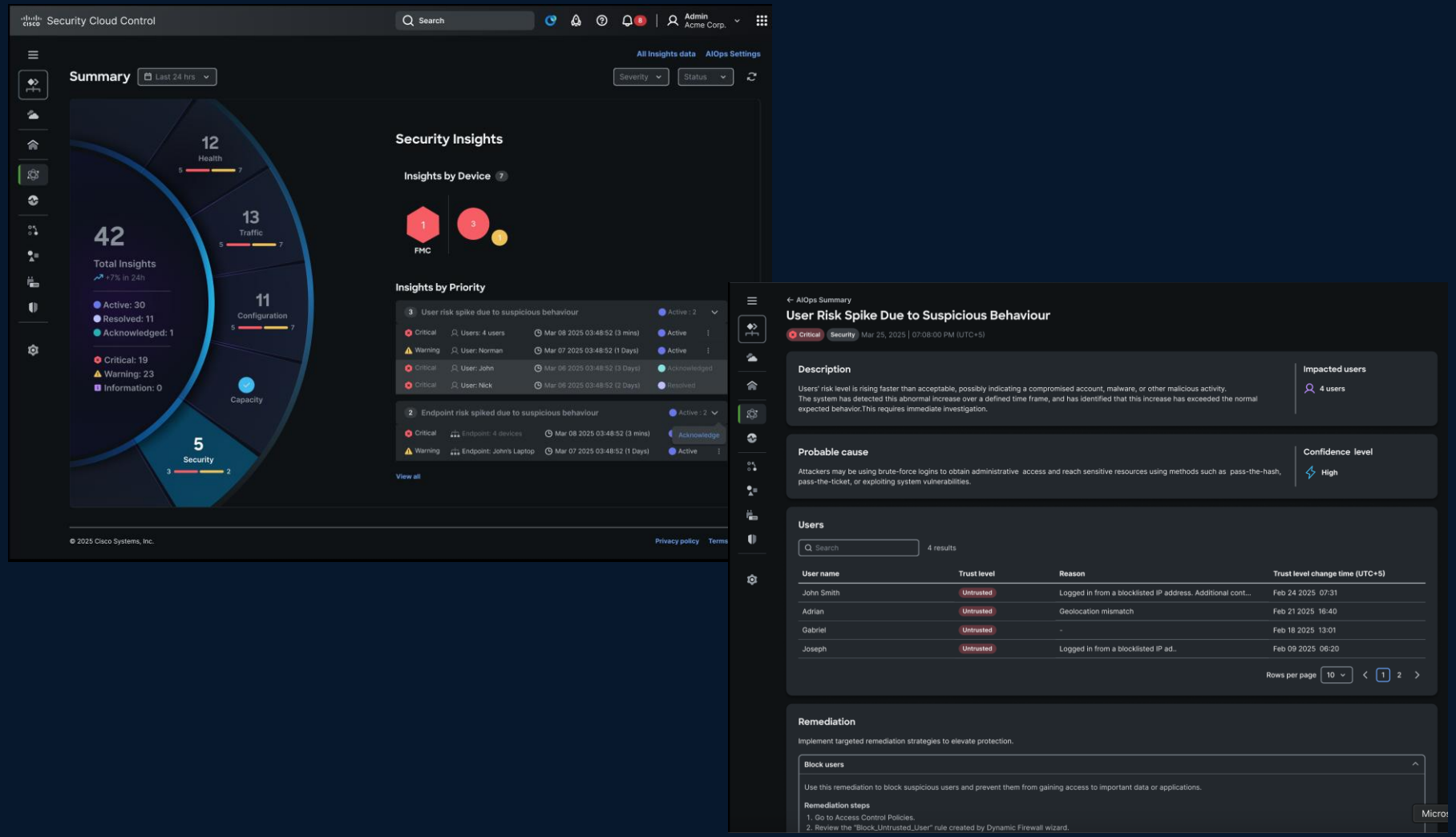


BLIN RUST



Works with existing IDPs

See into risky user behavior with Cisco Identity Intelligence

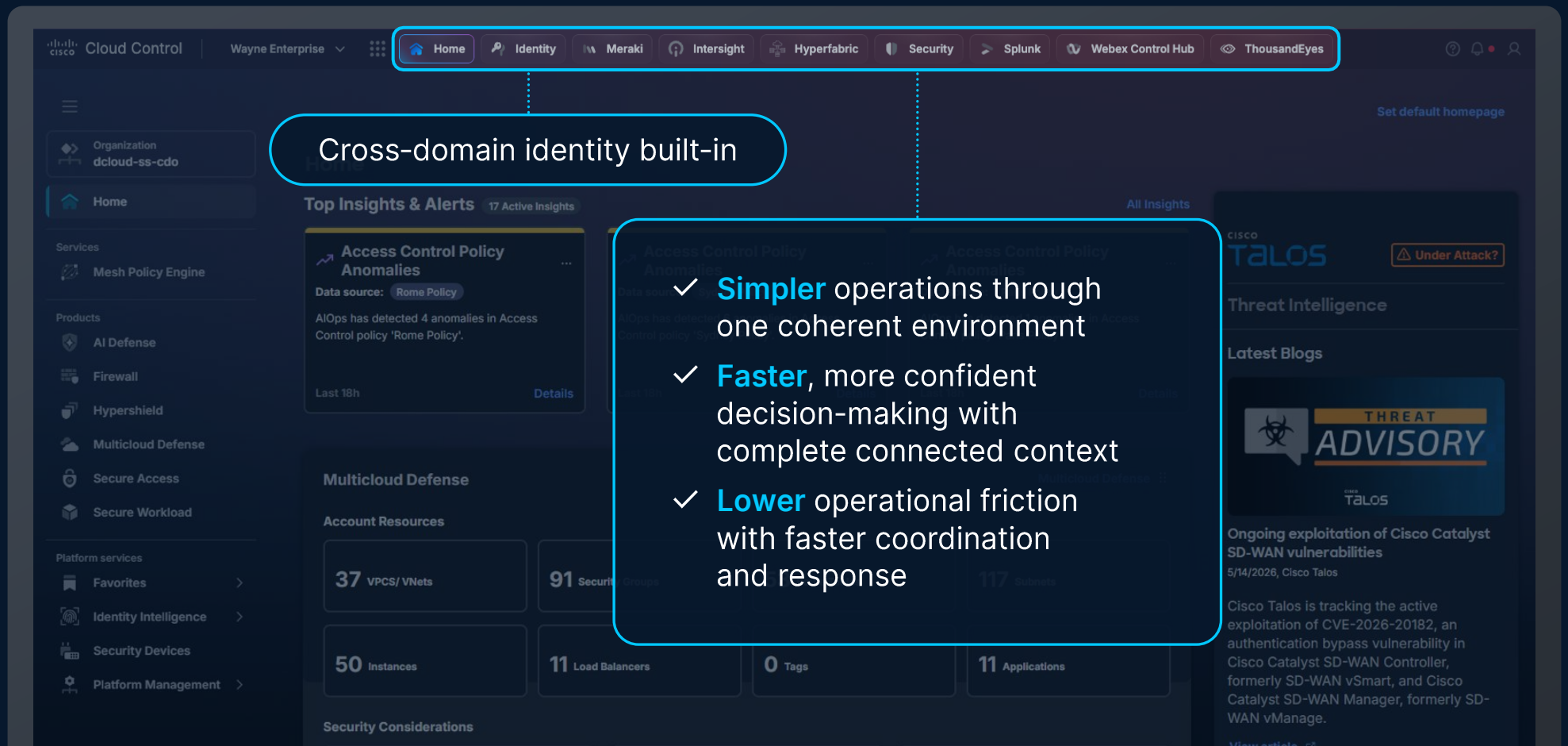


- Integrate Secure Firewall with Cisco Identity Intelligence to gain insights into risky users from AIOps
- Available in Firewall AIOps entitlement now

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

One platform, every domain

Security in Cloud Control



GA

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.



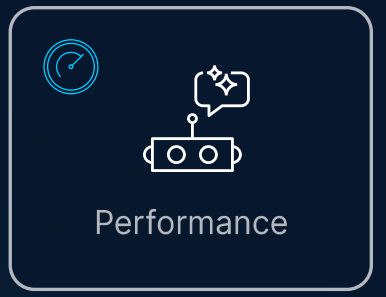
Example

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.

Multi-vendor intent-based policy

Cloud Control



CISCO

paloalto NETWORKS

FORTINET

JUNIPER NETWORKS

Absorb and optimize existing rules

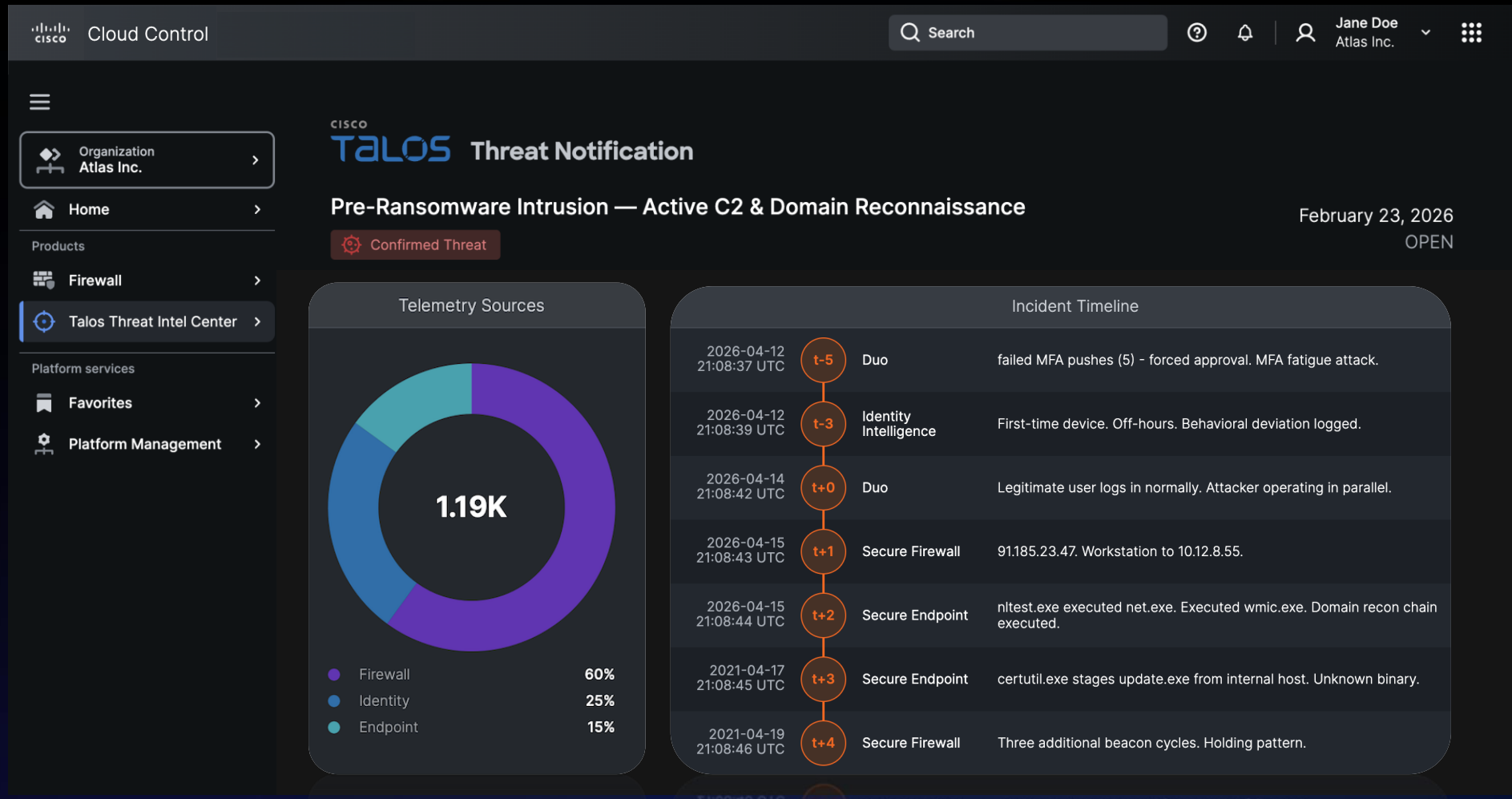
Change enforcement points, not policy

No rip and replace

NEW

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 Firewall Test Drive: https://cloudsecurity.cisco.com/firewall-test-drive

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

CISCO Connect

Thank you

