CISCO Connect

Agents, Mythos, and Mayhem: Need for distributed firewalling

Cisco Hybrid Mesh Firewall

Steve Brewer
Security Account Executive, LinkedIn: @brewerstephen

Matt Gockel – CCNP Enterprise, CISSP
Security Solution Engineer, LinkedIn: @mgockel



10/13/2026

What is the biggest concern regarding AI for your business?

Option 1	Option 2	Option 3
Shadow AI (Claude, ChatGPT, etc)	**Unauthorized Agentic Activity**	**Malicious AI Attacks on Infra/Apps**

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

Agentic AI has changed the game for security



Agents supercharge external attacks

- Find and weaponize faster
- Automate lateral movement



Agents are a new insider threat

- Persistent at machine speed
- No judgement or consequences

Agents **fight back at machine speed** to solve for both

© 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

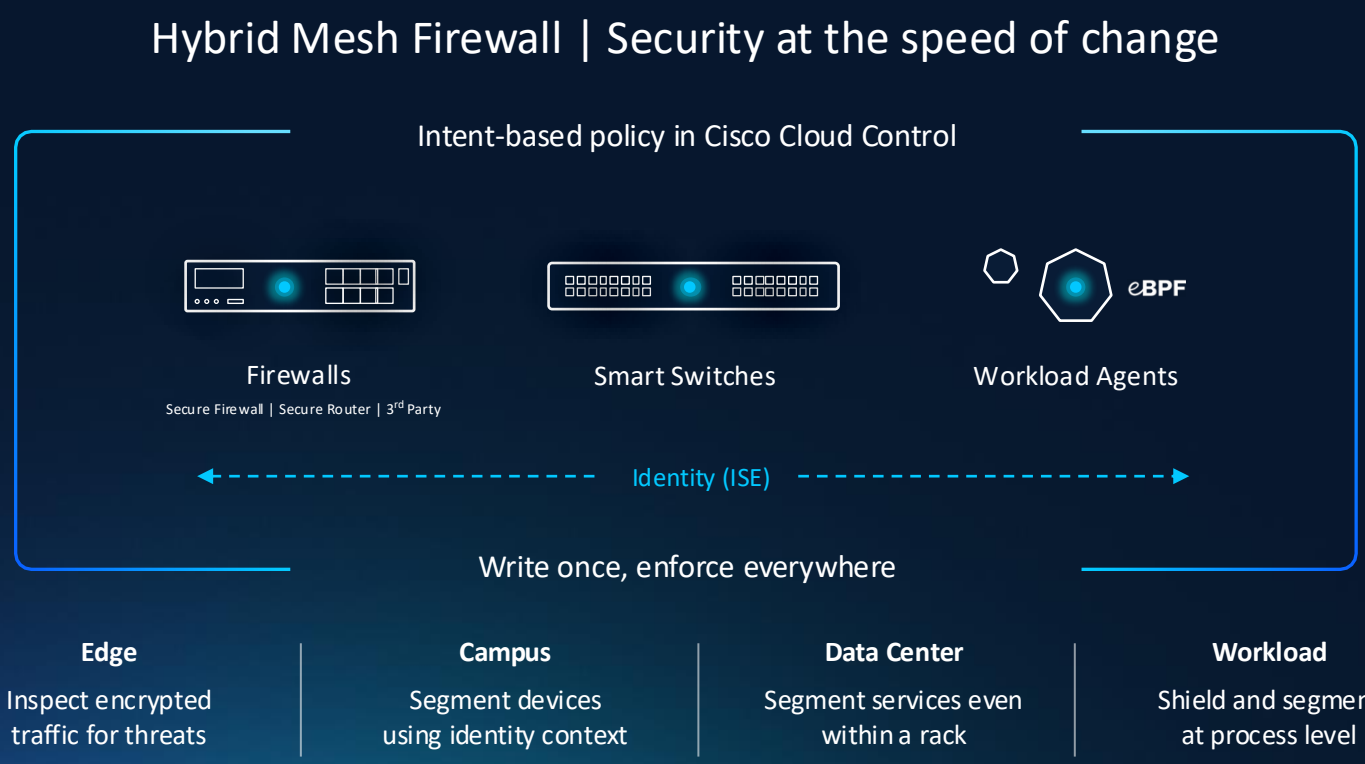
03 Detect & respond at machine speed & scale

- 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



© 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

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

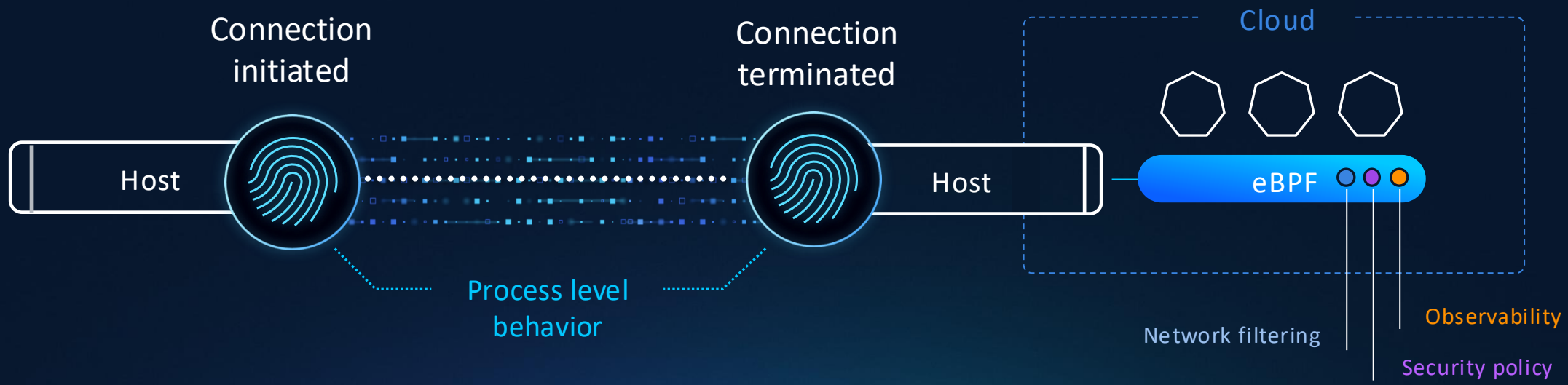


Single appliance, dual personality

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

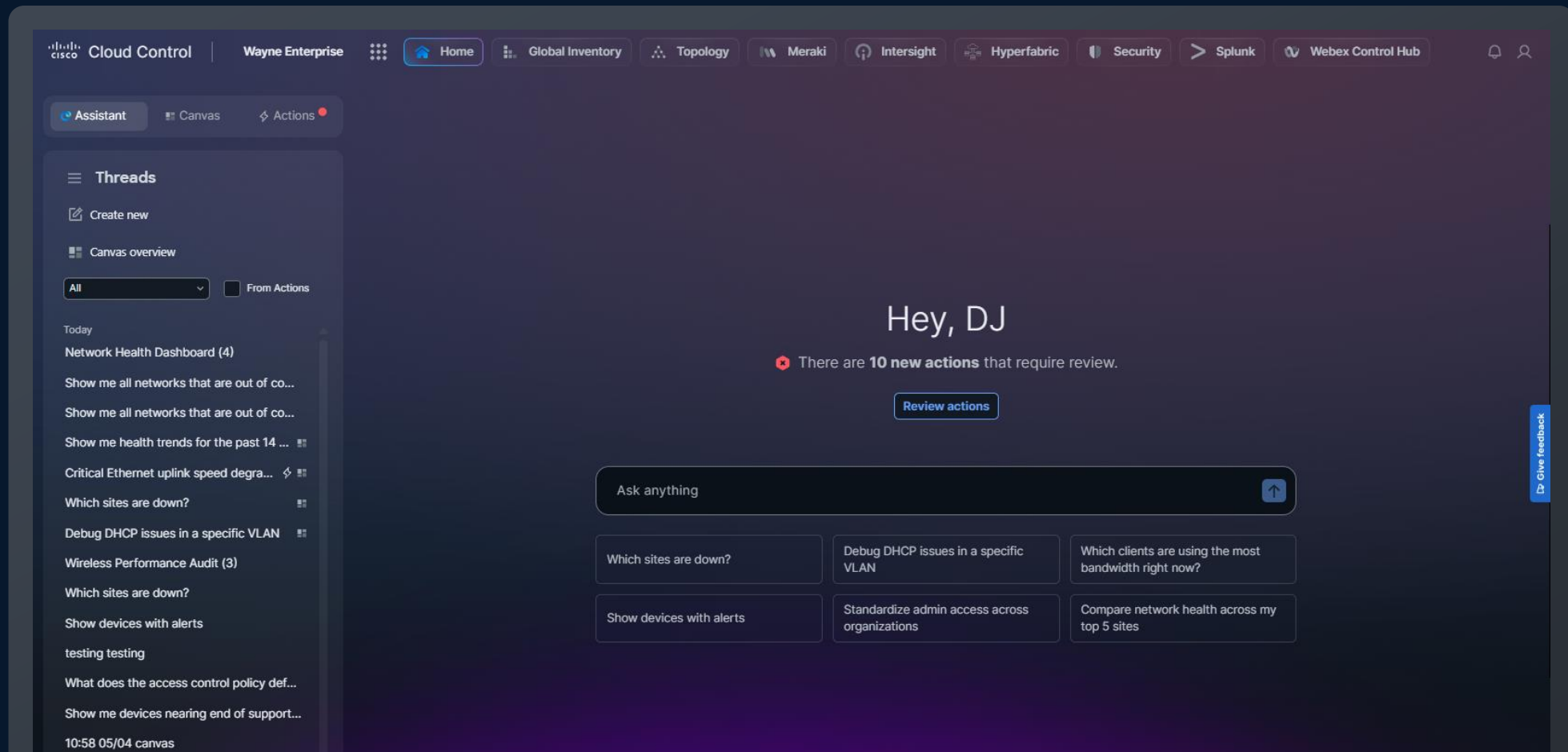
Segment effectively as apps change

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.

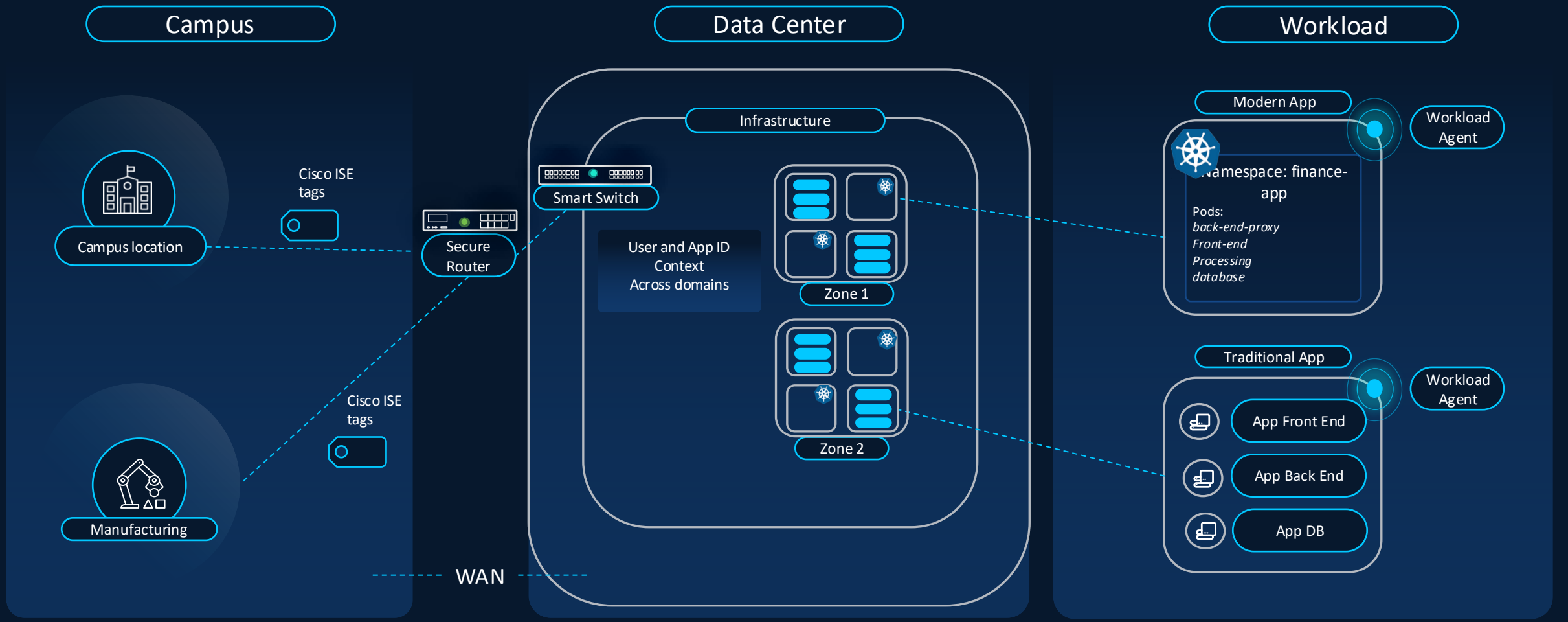
What level of Application segmentation are you doing today?

Option 1	Option 2	Option 3
VLANs /w Firewalls	**Software Defined Networking (ex: ACI)**	**Software Agents**

© 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.

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

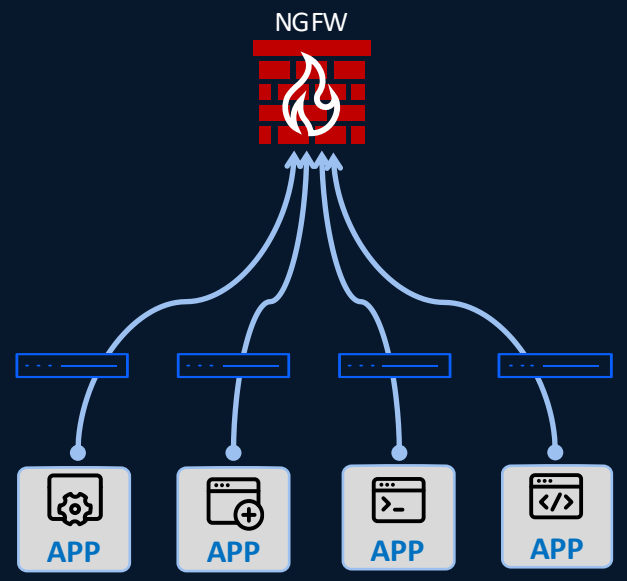


DISTRIBUTED | STATEFUL | SECURE | FUSED INTO THE FABRIC

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

Hyper-distributed security, without the bottlenecks

Traditional
Centralize chokepoint

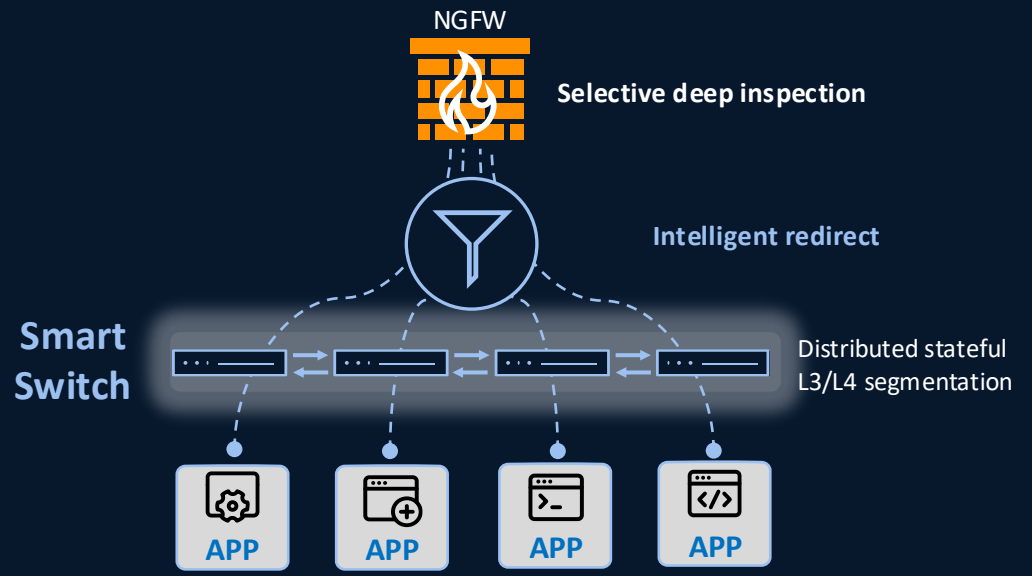


Performance bottlenecks

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.

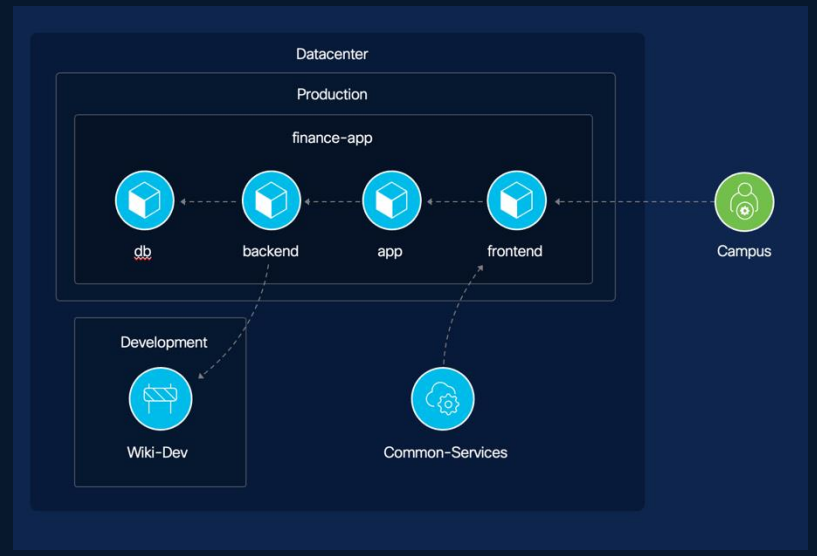
Automated Application Policy Discovery

Baseline workload protection posture

- Network communications
- Process behavior
- Labels
- SGT tags

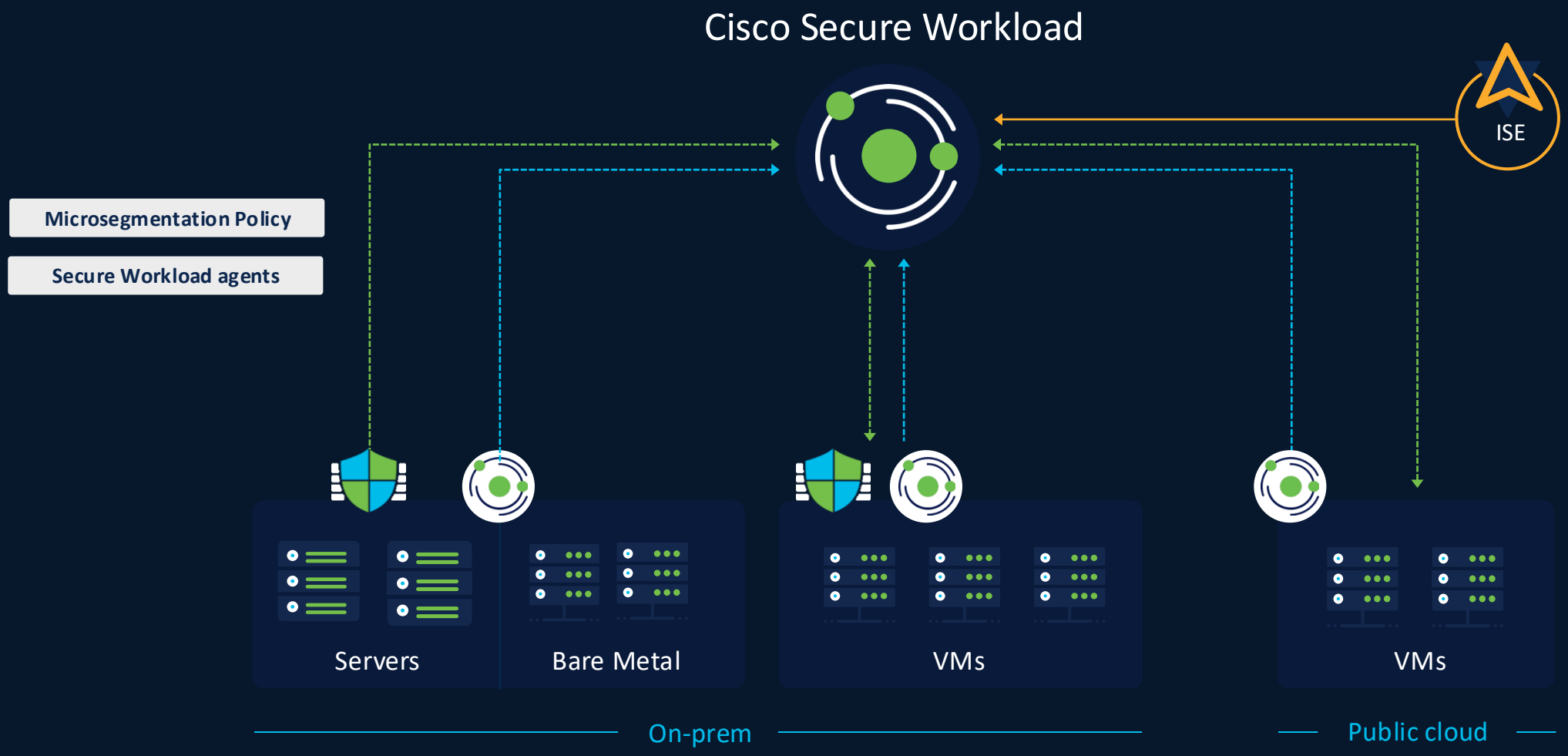
ISE

Secure Workload



© 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.

How often do you patch infrastructure?

Option 1

As Needed

Option 2

Every six months

Option 3

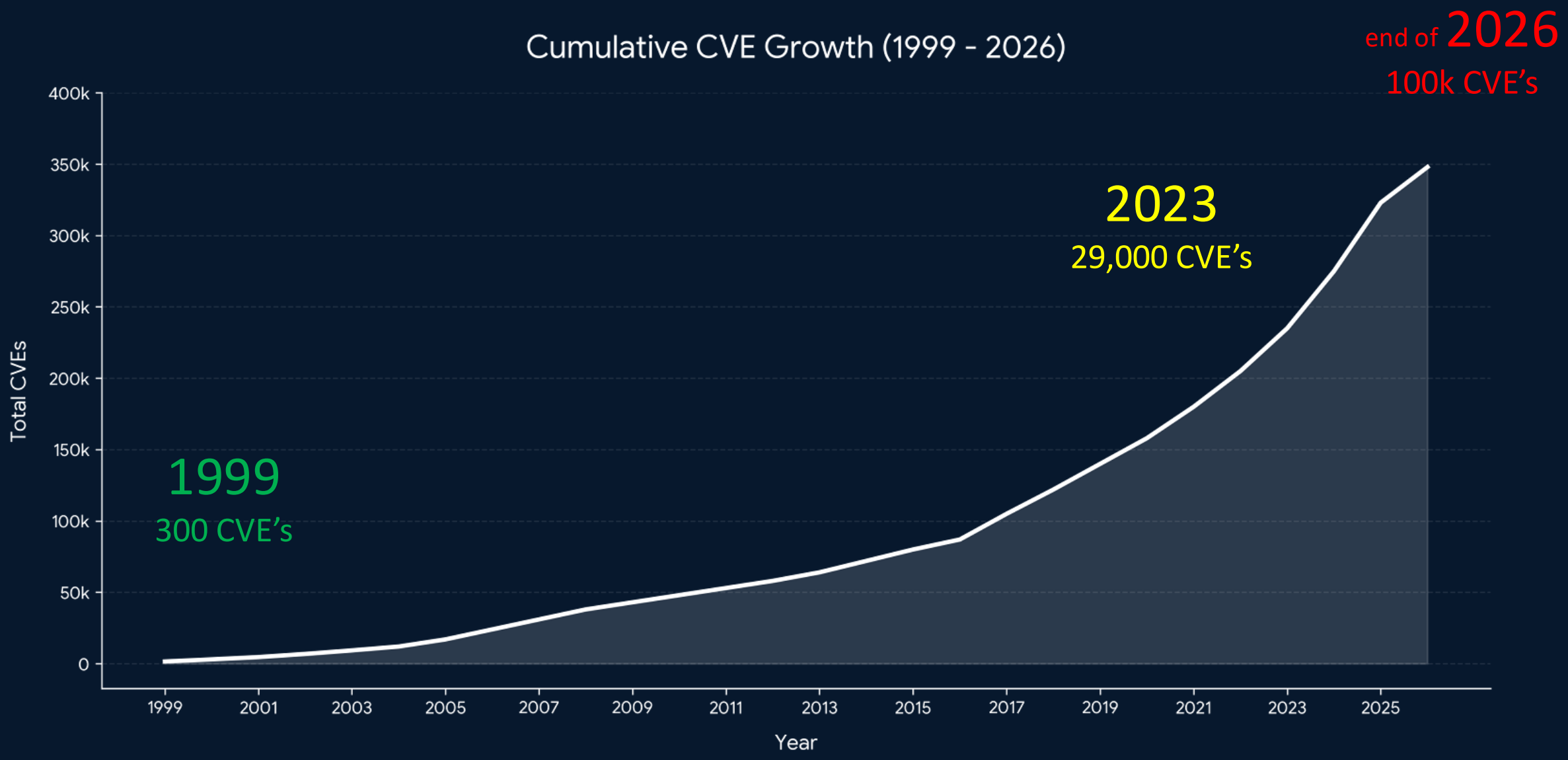
Once a year

Option 4

When we have time (just kidding we never have time)

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

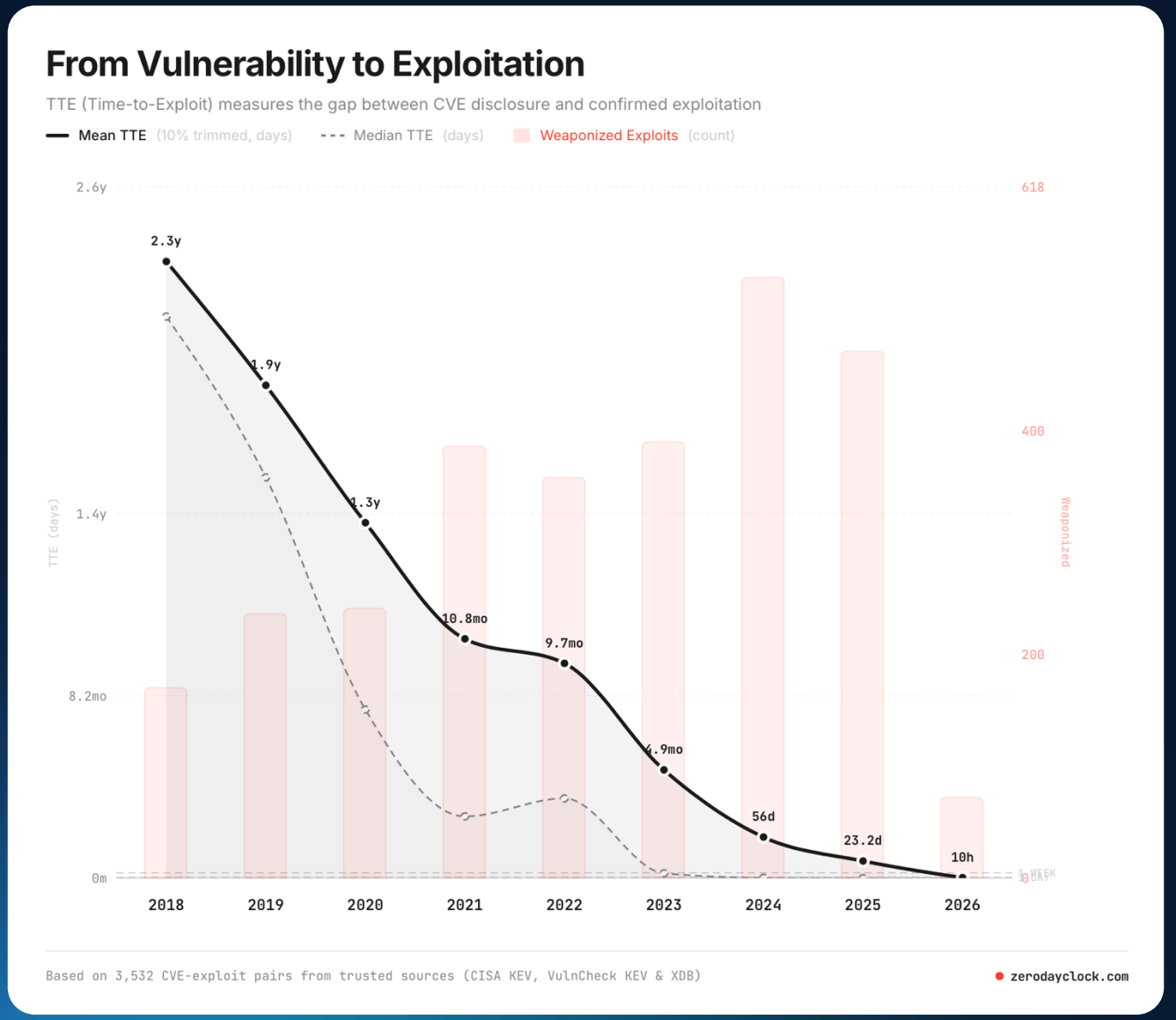
Implication #1: CVE Growth



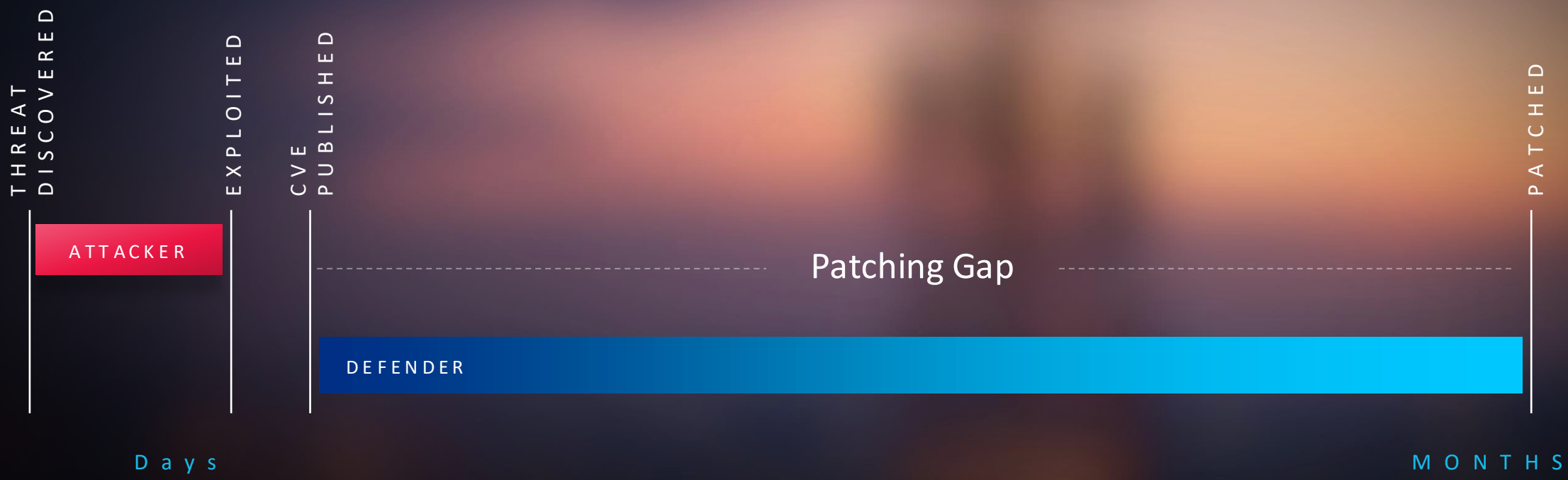
© 2026 Cisco and/or its affiliates. All rights reserved.

Implication #2: Time to Exploit Collapse

The time it takes from CVE disclosure to an exploit has collapsed



AI-speed attacks compress the patching window. Minutes to exploit. Months to patch.



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

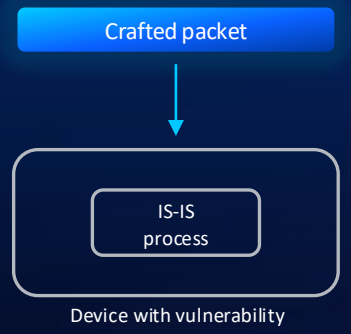
Continuous re-validation

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

Blocking an IS-IS denial-of-service attack with a Live Protect Shield

Example: CVE-2025-20241

The attack



- Crafted packets reach vulnerable IS-IS parser
- IS-IS process may restart
- Device reload creates DoS condition

Live Protect

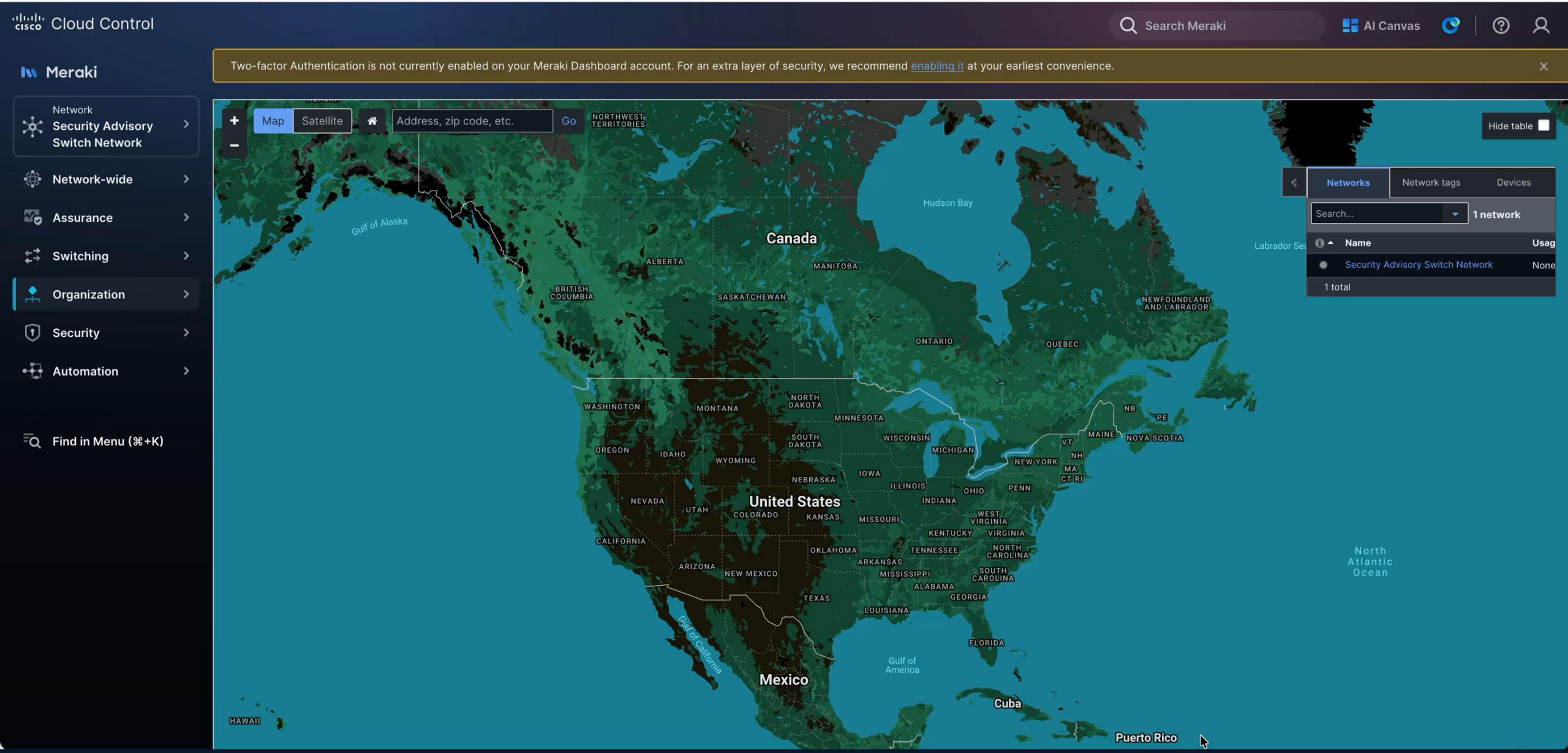


- Shield at vulnerable IS-IS function path
- Exploit condition blocked
- Normal IS-IS routing preserved

Operator benefit



- Avoid unplanned reloads / upgrades
- Preserve routing stability
- Patch through planned change control



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

Are you decrypting TLS traffic for inspection?

© 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

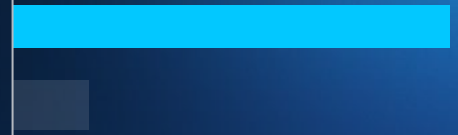
100%

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.

Next-Generation Traffic Inspection and Defense

Visibility to malicious flows in encrypted traffic without decryption

EVE
Risk Score

High risk

Medium risk

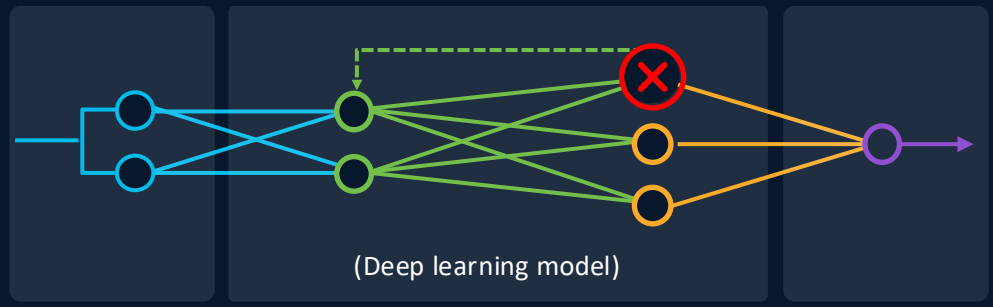
Low risk

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.

Organization
acme-netsec
Home

Products
Firewall
Hypershield
Multicloud Defense

Platform services
Favorites
Security Devices
Shared Objects
Platform Management

Home

Set default homepage

Top Insights & Alerts

32 Active Insights

All Insights

High Traffic Caused by Elephant Flow

Data source:

AIOps has detected high traffic on the firewall caused by 1 flow, potentially leading to performance duress in Snort cores.

97d ago Details

RAVPN Forecast - Maximum Sessions Nearing Limit

Data source:

AIOps has forecasted that the number of RAVPN sessions will reach capacity in '9' days

176d ago Details

Best practices and recommendations

Data source: NGFWTG

AIOps has detected 5 needs review checks.

6d ago Details

Multicloud Defense

Multicloud Defense

Account Resources

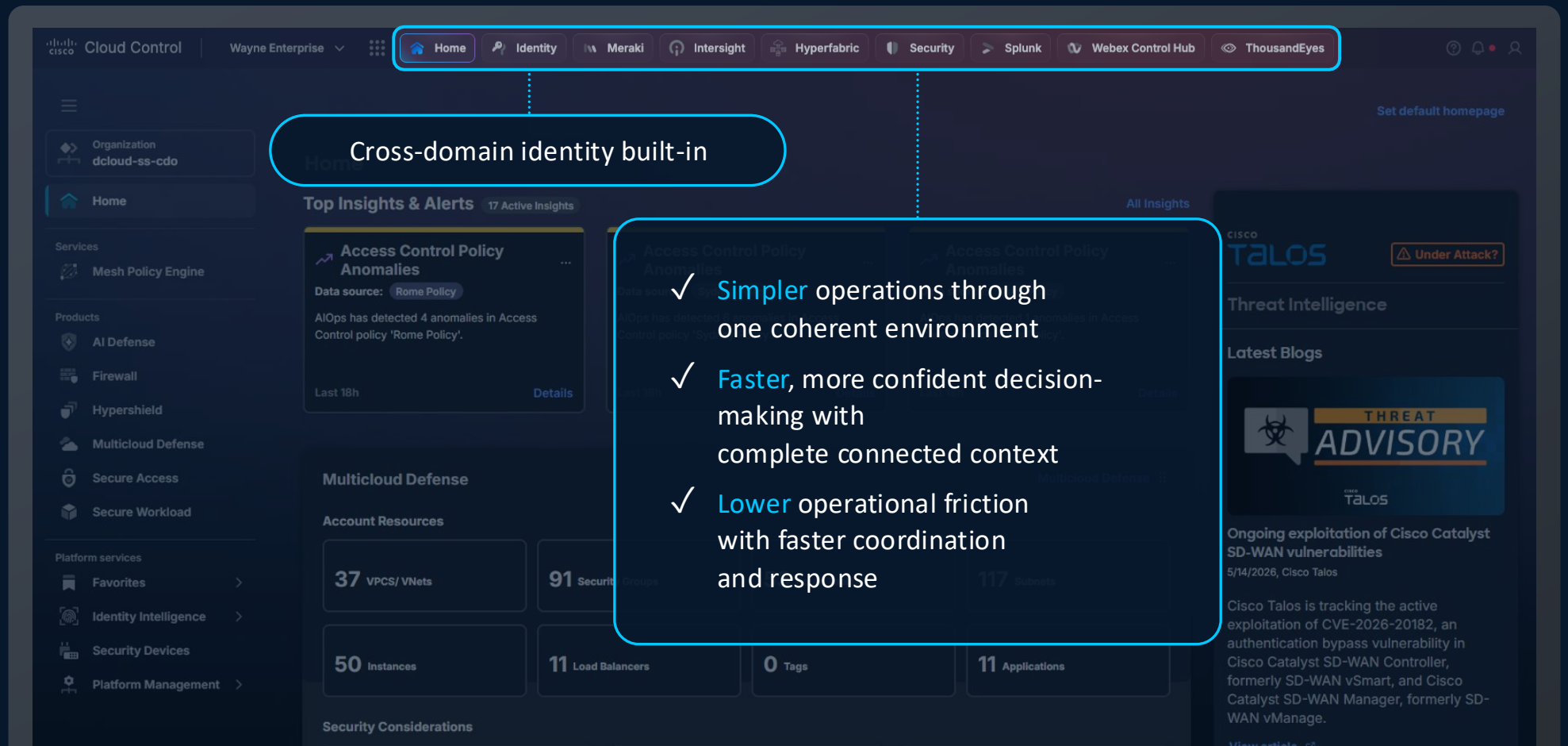
93 VPCS/ VNets	208 Security Groups	124 Route Tables	289 Subnets
151 Instances	33 Load Balancers	0 Tags	33 Applications

Security Considerations

33 Applications not protected	80 VPCs/VNets not protected	0 Service VPC/VNets without Gateways

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



Absorb and optimize existing rules

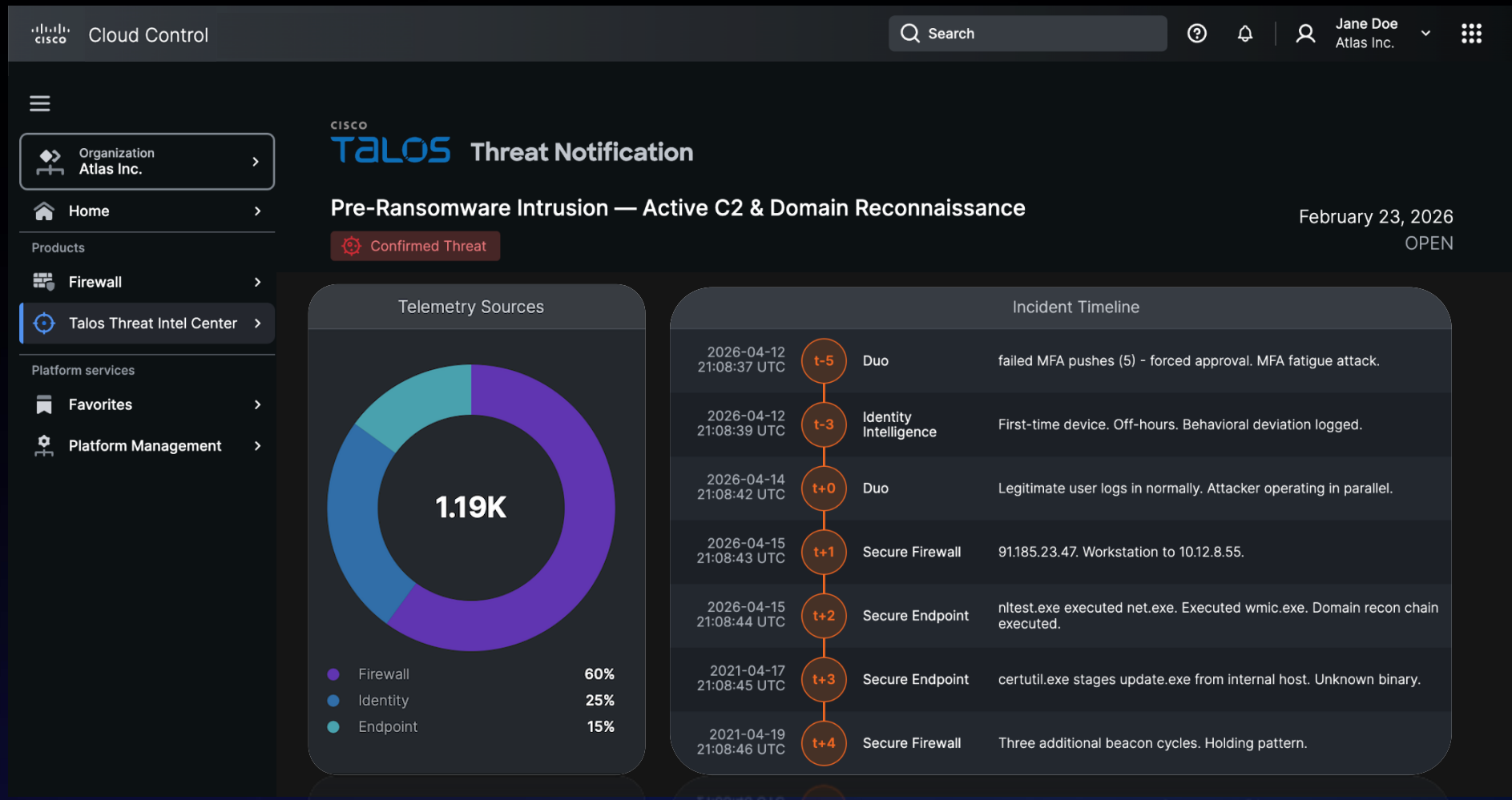
Change enforcement points, not policy

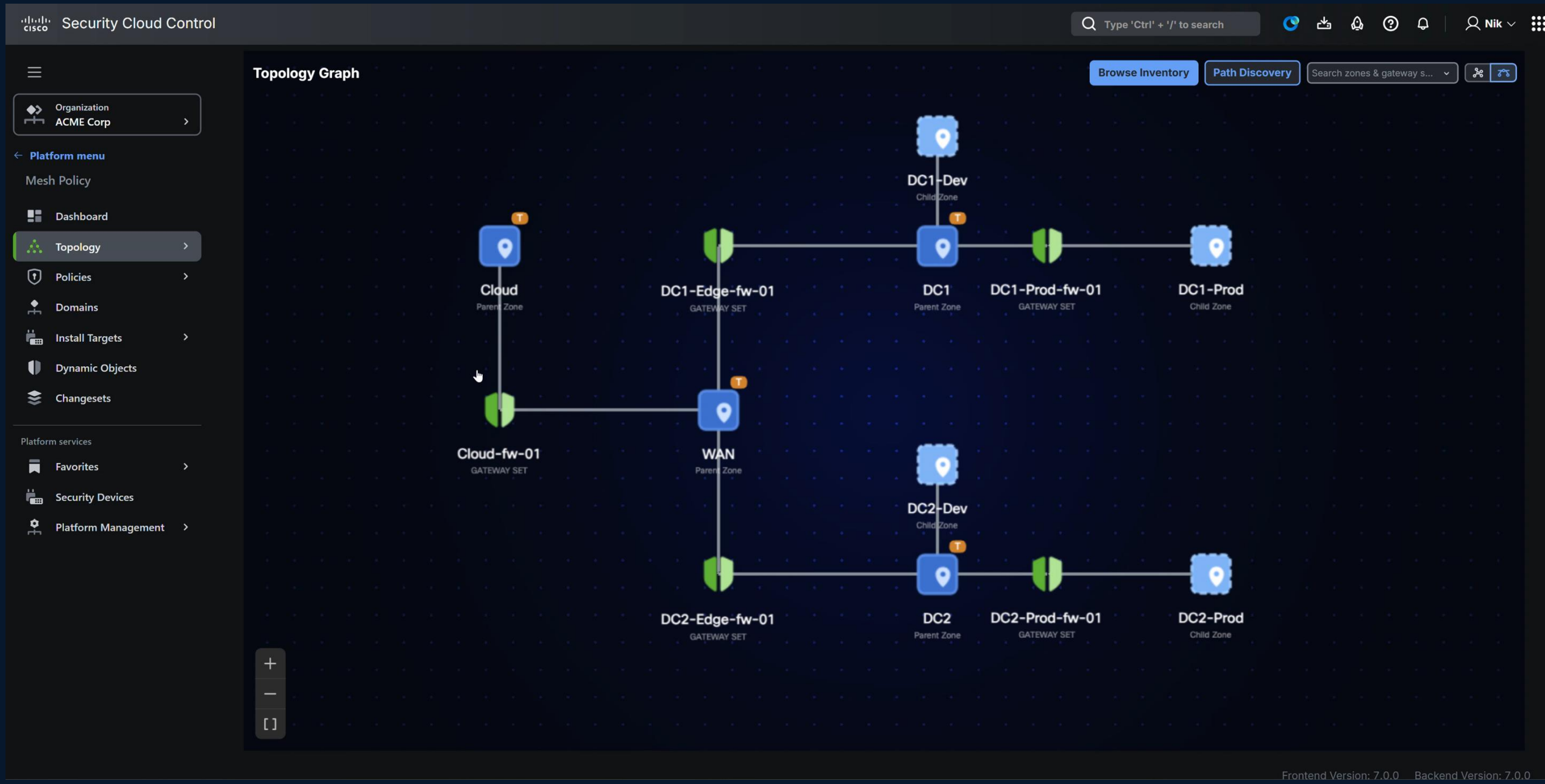
No rip and replace

NEW

Introducing Cisco Talos Threat Hunting

A helping hand for the Mythos era





© 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 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 Connect

Thank you

