CISCO Connect

Hybrid Mesh Firewall: Firewalls Are Not What You Think They Are

Scott Wofford, USPS Segmentation Engineer

February 5, 2026

Agenda

1. Speaker=$(whoami)
2. Evolution of Firewalls
3. What is a Hybrid Mesh Firewall?
4. Why You Should Care
5. Cisco’s Approach
6. Nuts and Bolts
7. Conclusion & Q&A

Evolution of Firewalls

Generations of Firewalls

1st Gen Packet Filtering

Filters based on IP, Port, Protocol

2nd Gen Stateful Inspection

Tracks active connections

3rd Gen – Application Layer

Inspects packet content (Layer 7)

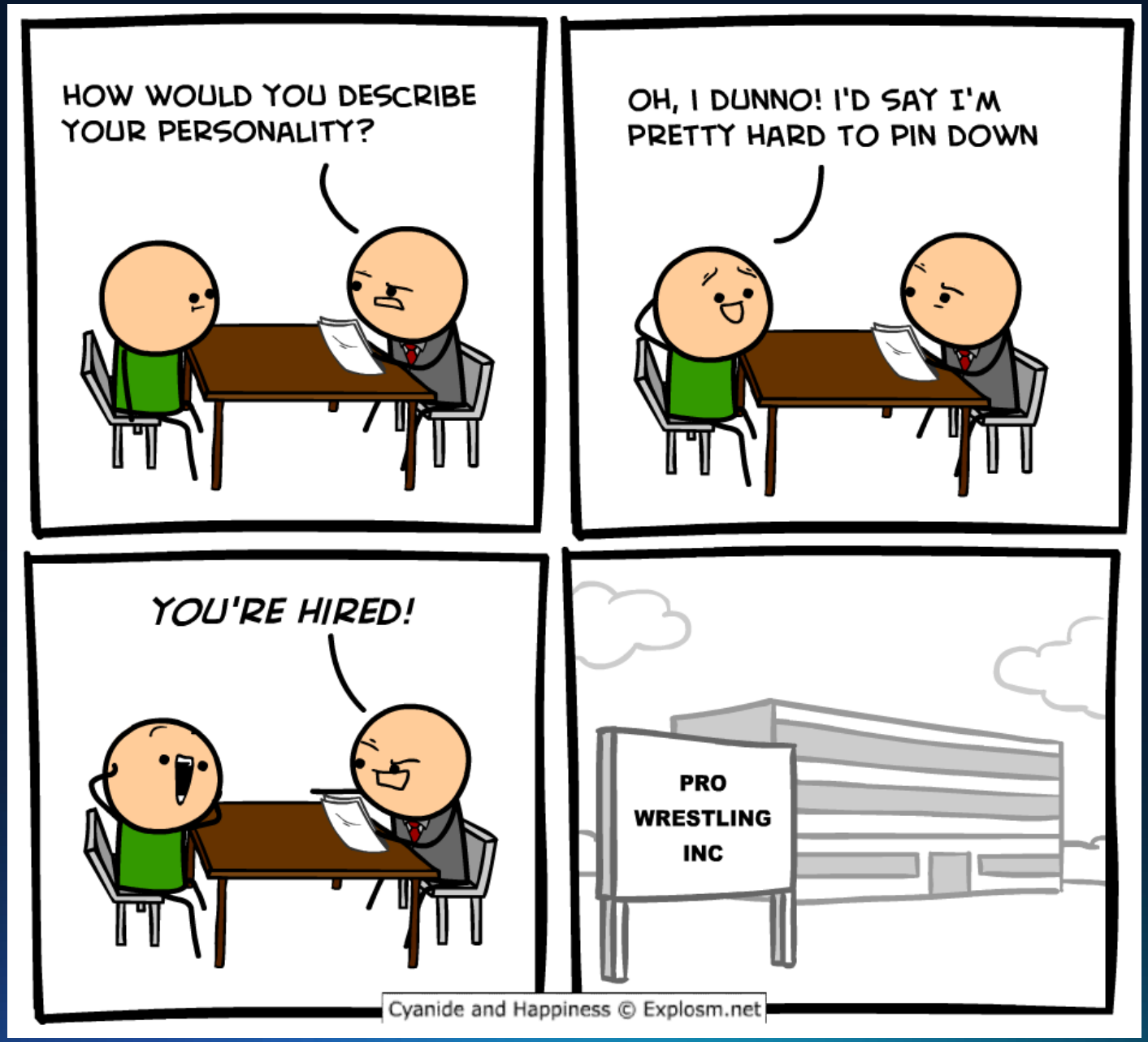
4th Gen NGFW

DPI, IPS/IDS, Malware Protecton, User Identity

What Is a Hybrid Mesh Firewall

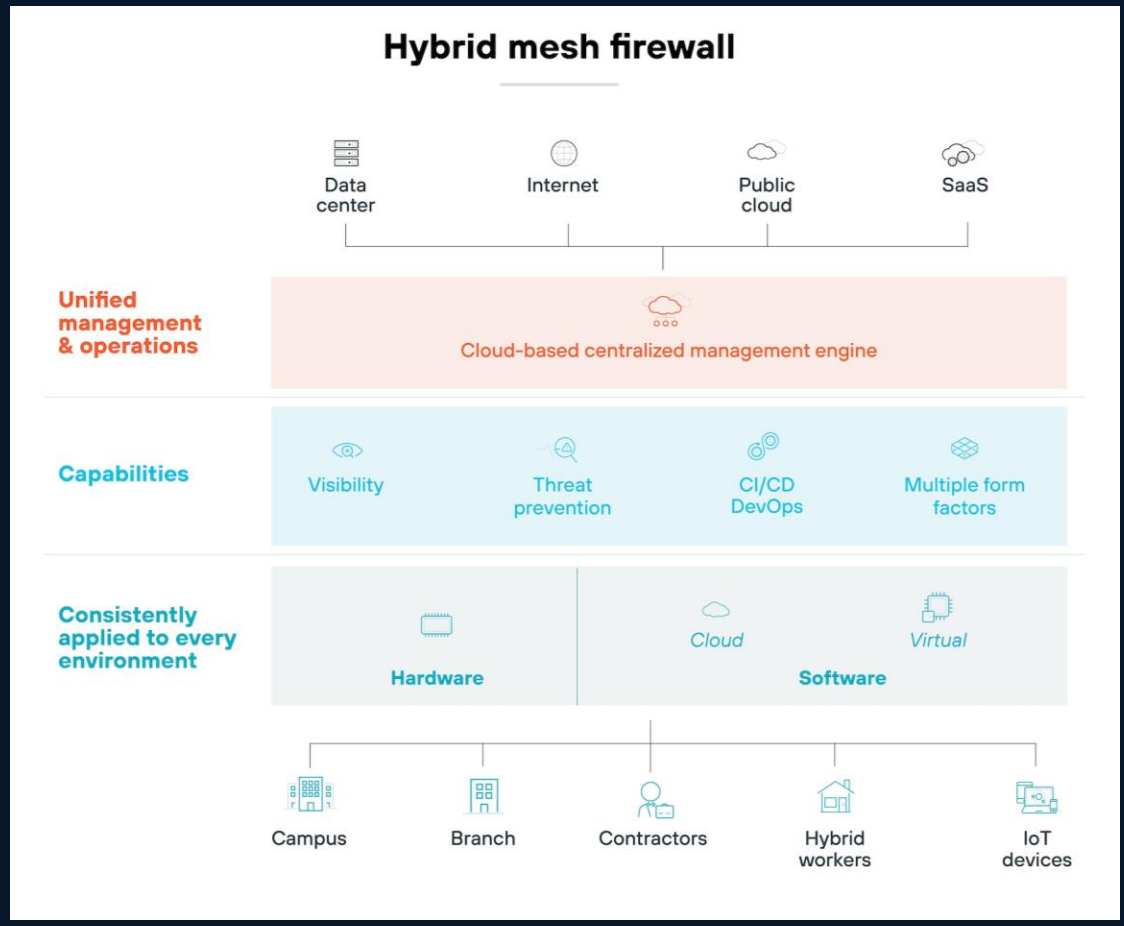
“A hybrid mesh firewall (HMF) is a multi-deployment mode firewall, including hardware, virtual appliance and cloud-based options, with a unified cloud-based management plane.”

Gartner



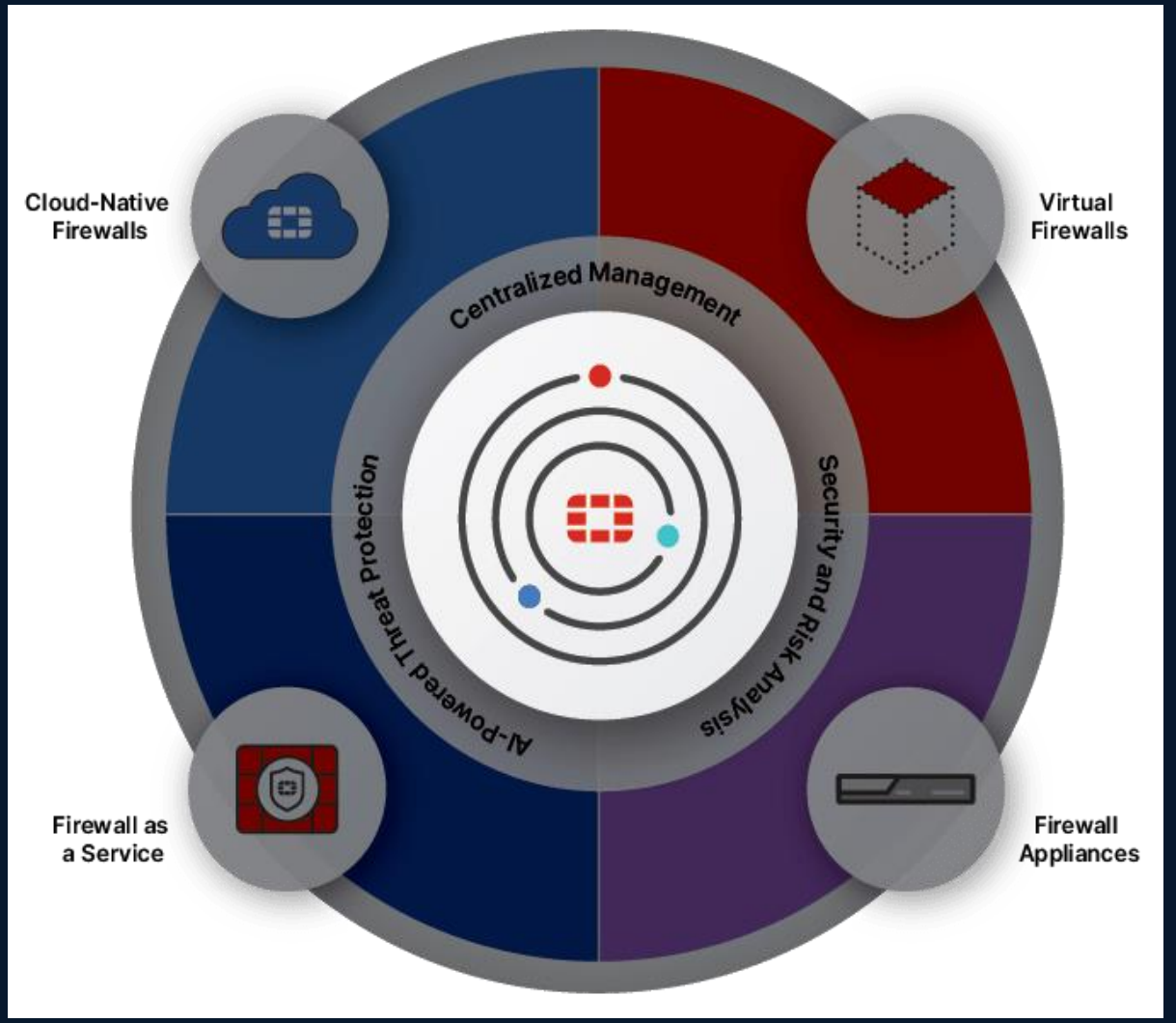
Manufacturer P's Approach

"A hybrid mesh firewall platform (HMF) is a single-vendor solution that unifies hardware, software, and cloud firewalls under one management system."



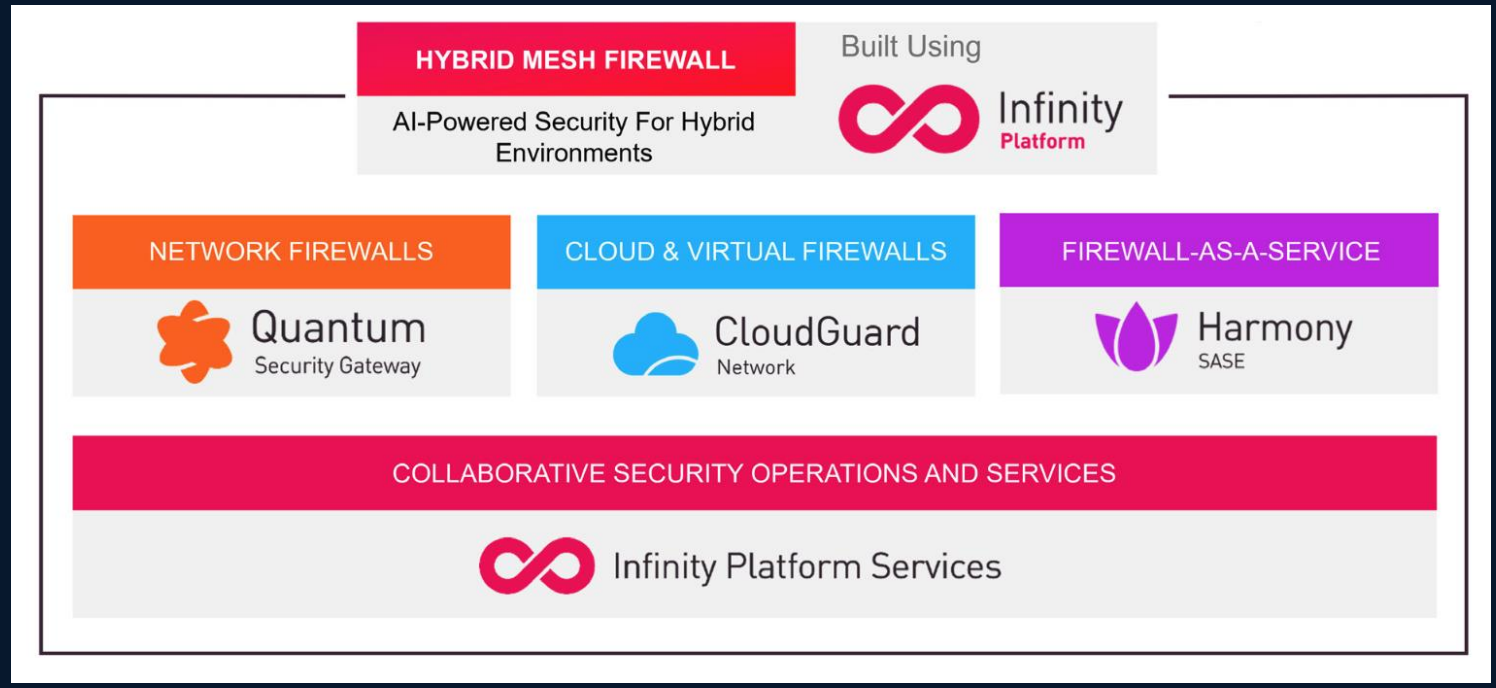
Manufacturer F's Approach

"Our approach unifies ... Firewalls (NGFWs) across on-premises, cloud, and hybrid environments with centralized management and analytics"



Manufacturer C's Approach

"Offering the agility to scale security anywhere… protects diverse environments across hybrid networks, workforce and clouds"



Why You Should Care

Securing the Enterprise Is Increasingly Challenging

Highly distributed applications

Nothing can be trusted

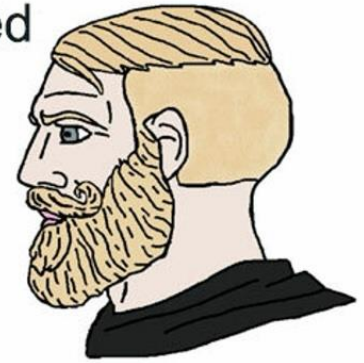
More vulnerabilities, exploited faster

AI adoption makes it more challenging

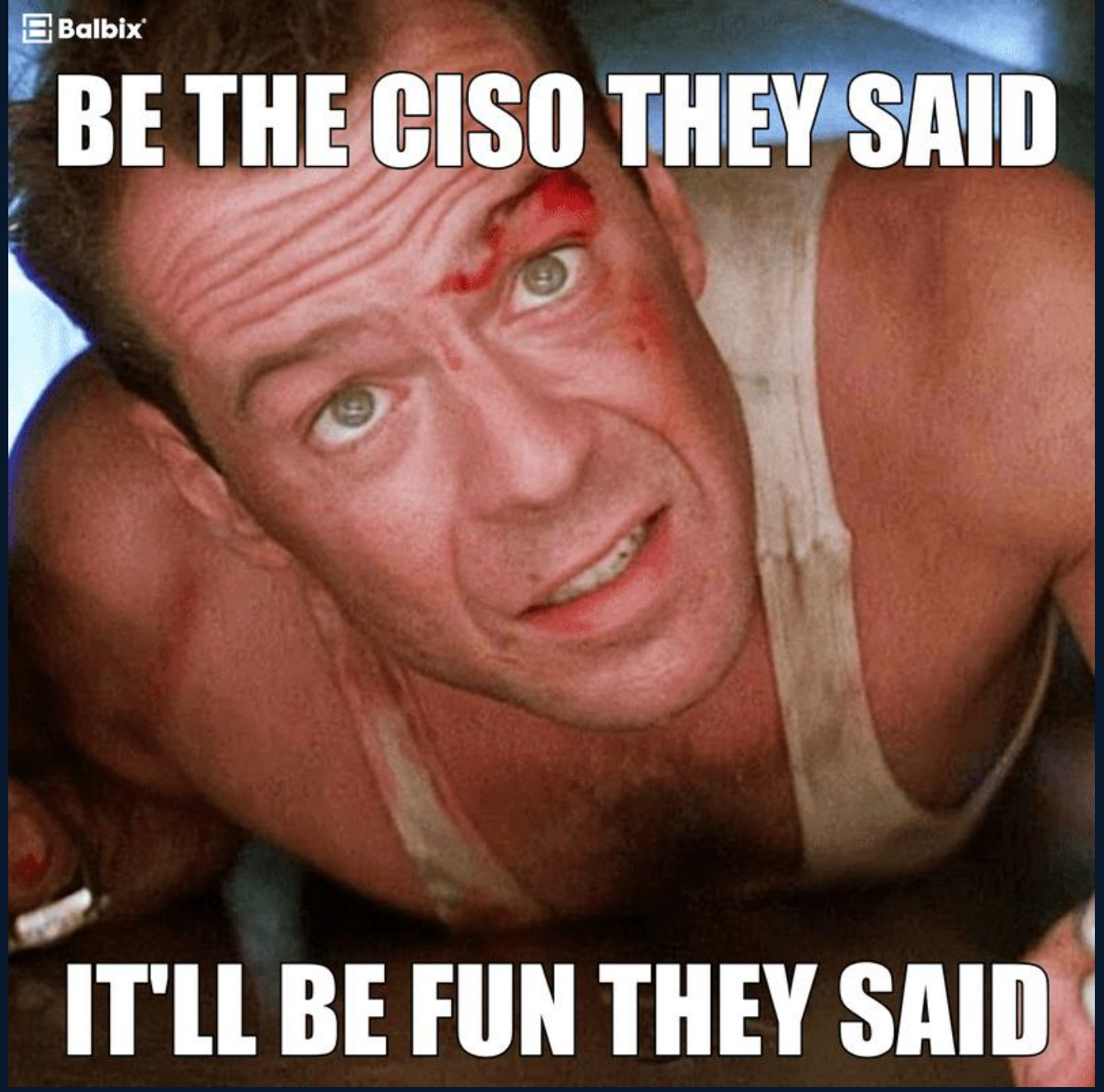
My parents at age 25

Let's get married

Yes



Me at age 25



Combating Firewall Admin Burnout

Cyber Professionals Stressed & Fatigued

CISOs reporting high stress levels

CISOs working 50-60 hours per week

- The State of Firewall Management
  - Proliferation of rules
  - Inactive Rule Problem
  - Impact on Network Performance & Security
- The Risks of Adding New Firewall Rules
  - IT Outages
  - Productivity Loss
  - Rule Conflicts & Ineffectiveness

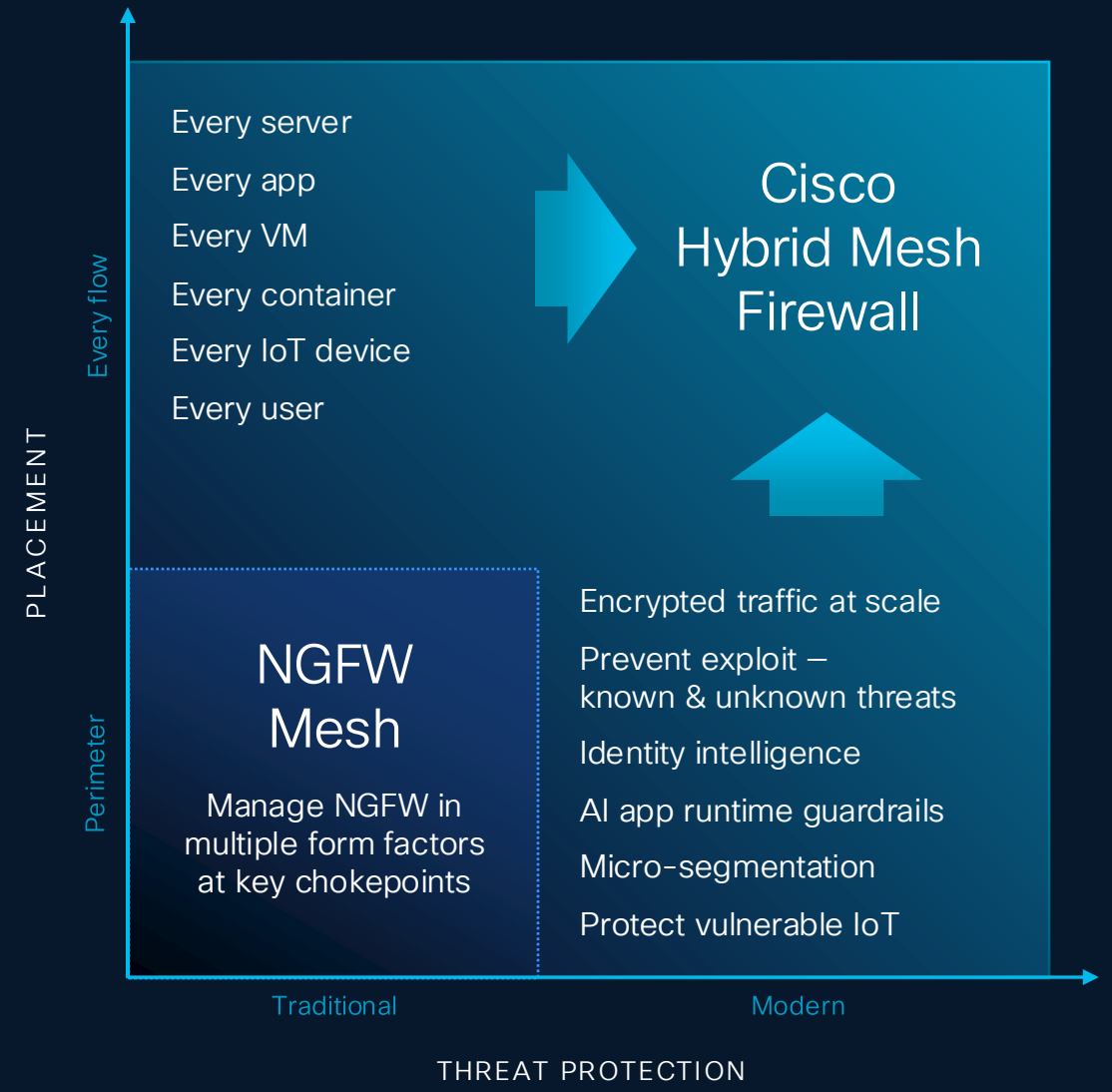
From the CISO

”...the value in Hybrid Mesh Firewalls lies in the ability to...”

- **Enhance Security Posture**
- **Simplify Security Management**
- **Facilitate Advanced Threat Detection and Response**
- **Protect AI-Driven Applications**
- **Ensure Business Continuity and Compliance**
- **Deliver Scalability and Flexibility**

Cisco’s Approach

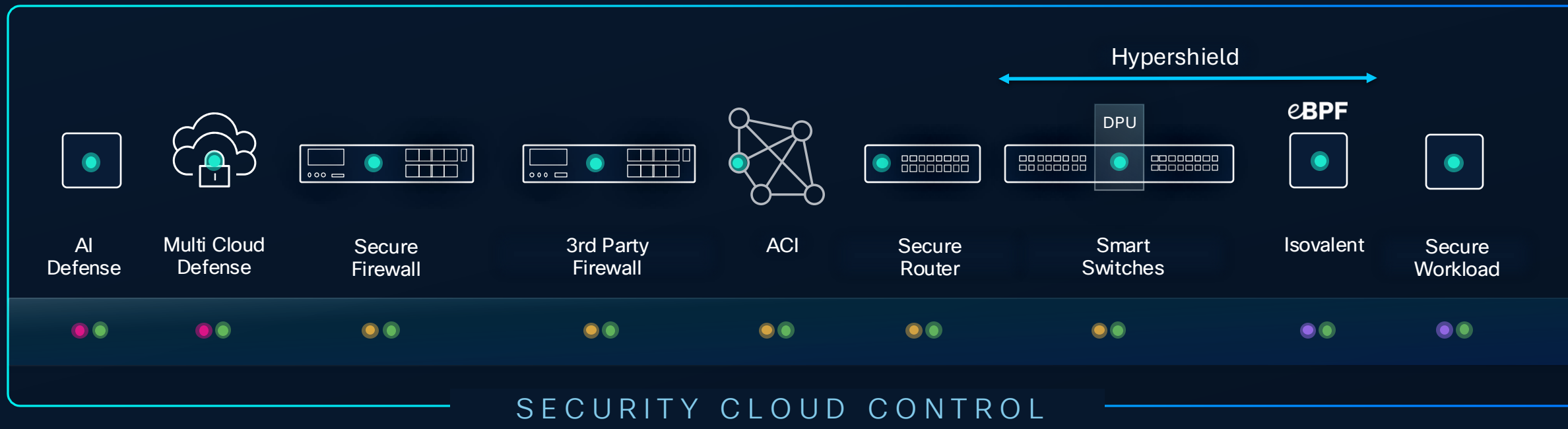
Firewalling Needs to Evolve to Meet Today's Challenges



Cisco Hybrid Mesh Firewall

CUSTOMER SECURITY OUTCOMES

Network Segmentation | Macro & Micro Segmentation | Threat Detection & Exploit Protection | AI Security



SECURITY CLOUD CONTROL

Write policy once, enforce across the mesh

Hybrid Mesh Firewall

Solving the Challenge of Management Complexity and Inconsistent Policy Enforcement

How the Cisco experience transforms security operations by centralizing management, enhancing security posture, and simplifying operations

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%**

cisco

NEW

Security Cloud Control

Industry's first multi-vendor intent-based policy

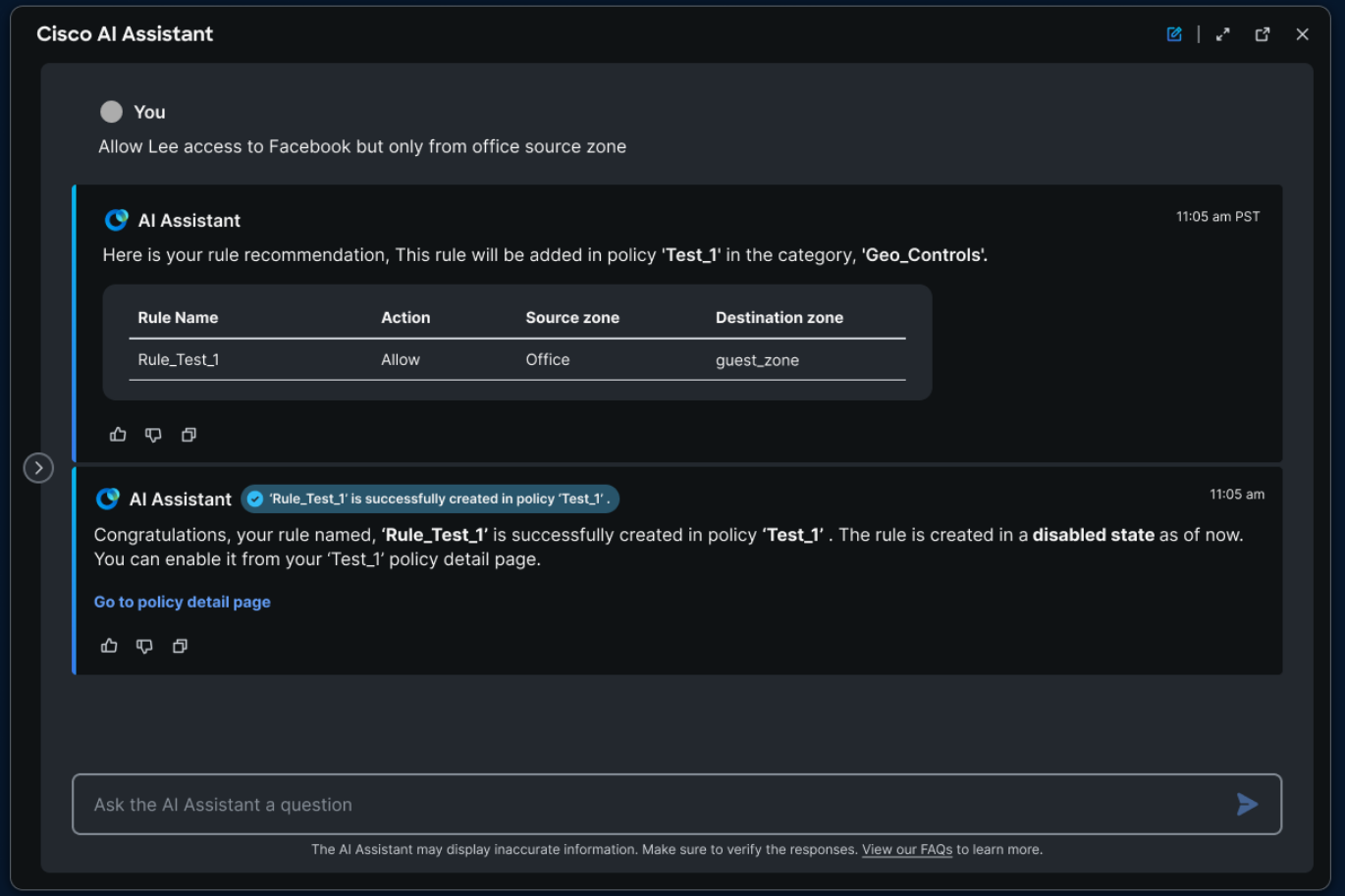
Absorb and optimize existing rules

Change enforcement points, not policy

No rip and replace

Reduce Management Overhead with AI Assistant

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



AI Assistance When You Need It

Nuts and Bolts

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 400 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

Cisco Encrypted Visibility Engine

Visibility to malicious flows in encrypted traffic without decryption

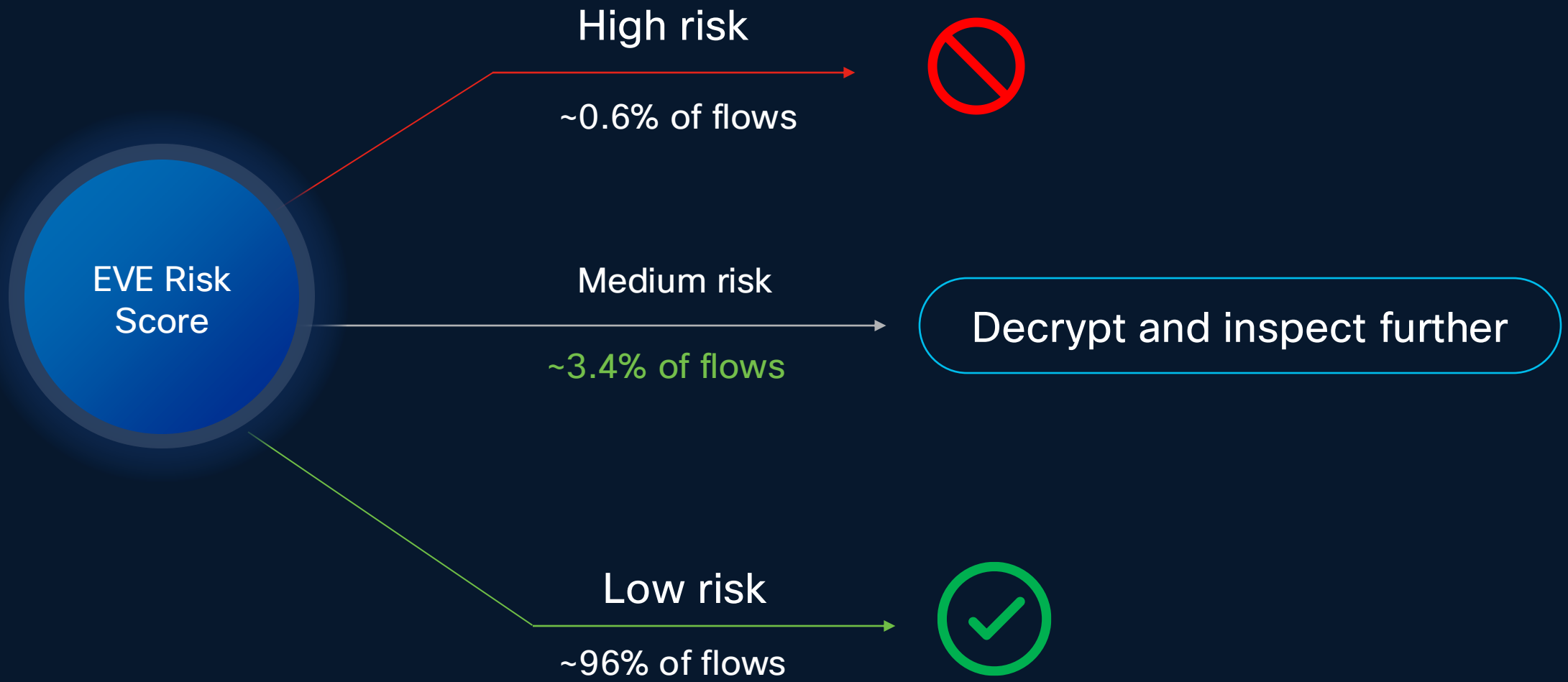
Machine learning (ML) technology

Processes **1 B+** TLS fingerprints

Processes **10 K+** malware samples daily

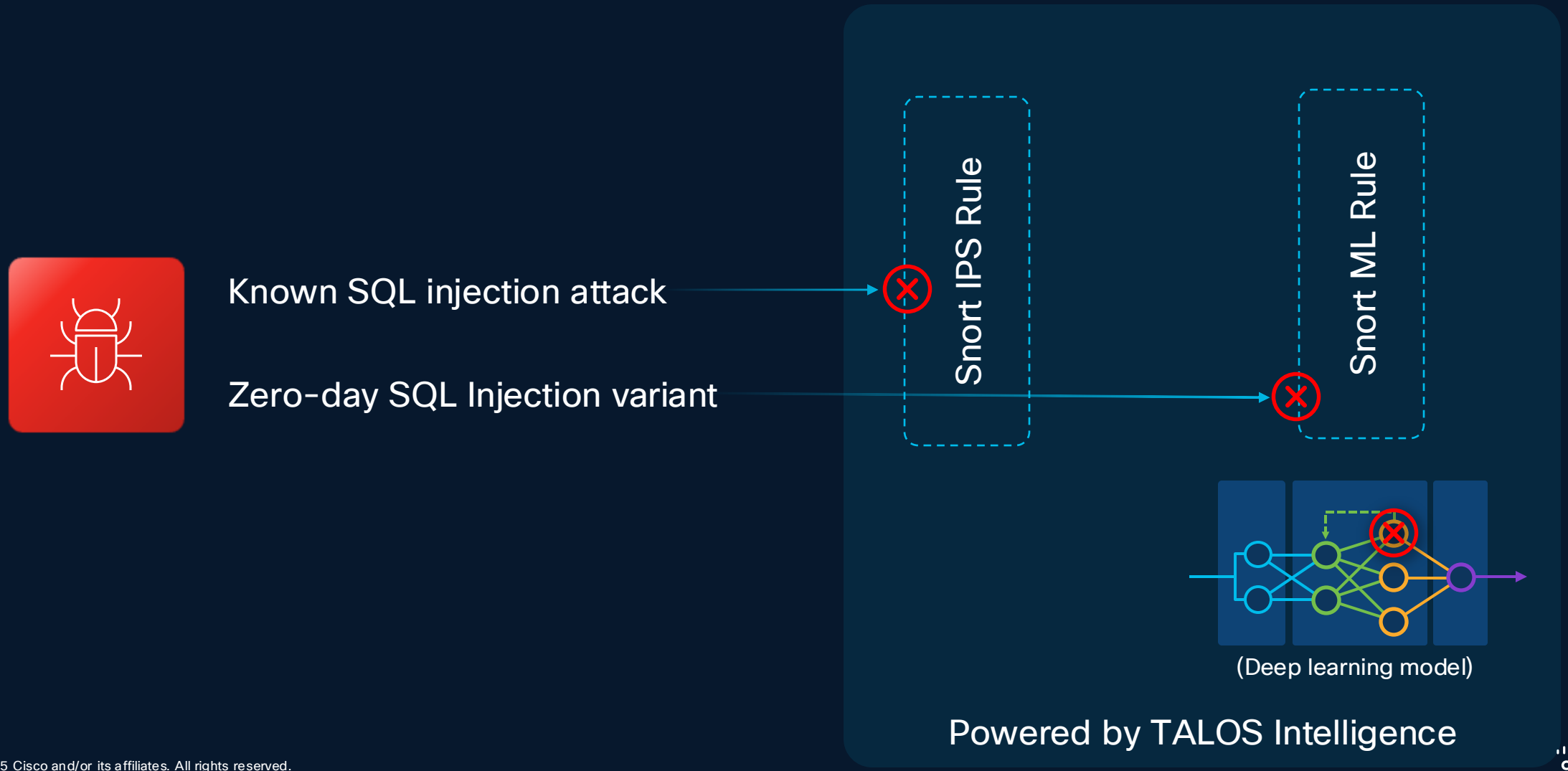
Eve Changes the Game on Decryption

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



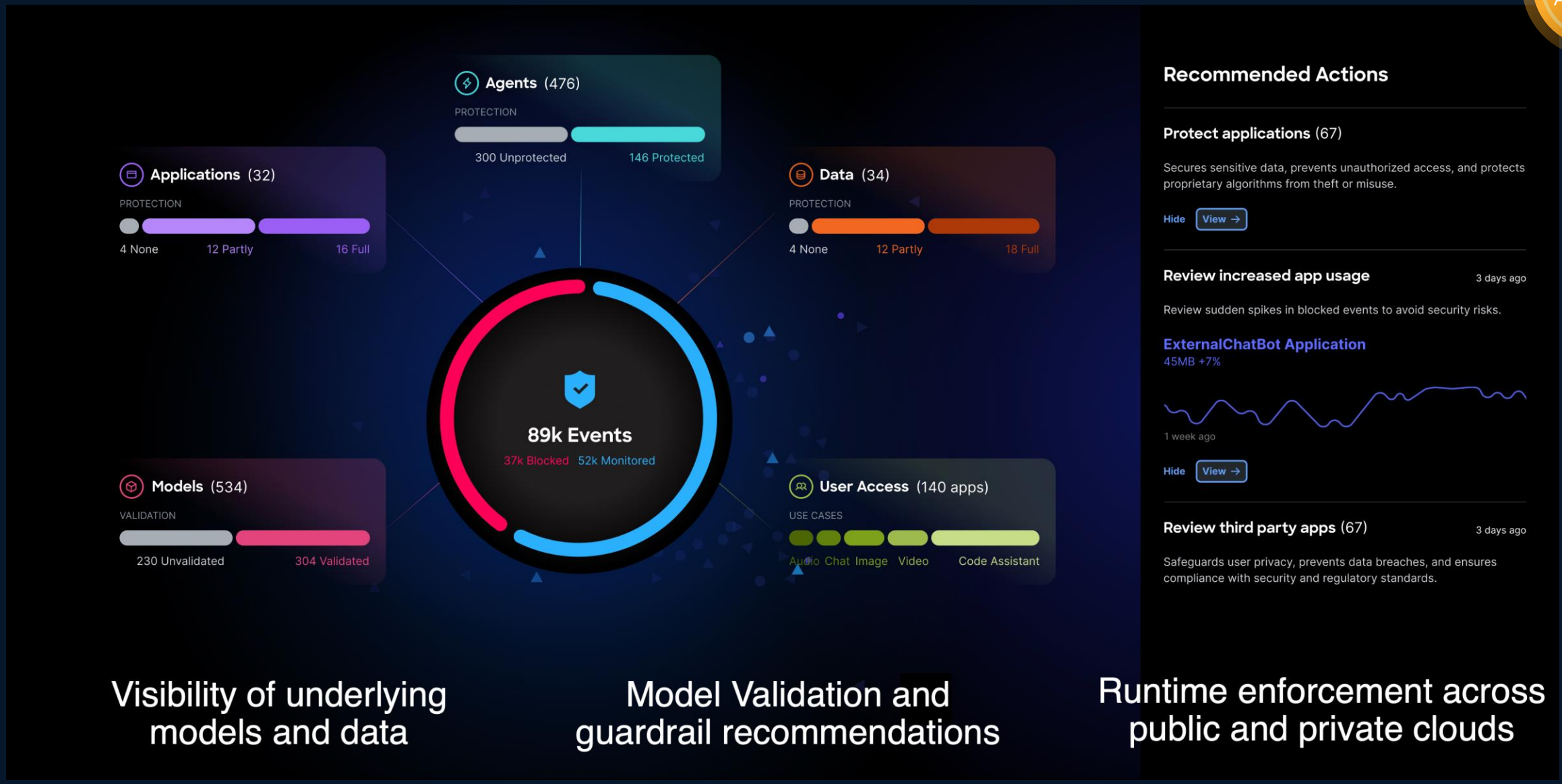
The Leading IDPS, Now with Zero-Day Protection

Snort ML extends IDPS protection to unknown variants of common attacks



AI Defense

EARLY ACCESS



Visibility of underlying models and data

Model Validation and guardrail recommendations

Runtime enforcement across public and private clouds

AI Model Protection Reference Architecture

Objective

This architecture simulates a real-world enterprise use-case for implementing and operationalizing AI application development and usage.

Architecture Layout

- **Security Cloud Control and Enforcement Points**– Unified plane for firewall policy control and visibility management
- **Cisco AI Defense**– a purpose-built solution that protects against the unique safety and security threats to GenAI
- **Security Cloud Control** – Unified plane for firewall policy control and visibility management
- **Large Language Models**– an artificial intelligence program trained on a massive amount of text data to understand, generate, and process human language.

Scenarios

- **AI Discovery** – Uncover shadow AI usage (workloads and users), applications, models and data
- **AI App and User Protection** – Protection is the art of placing guardrails and other types of AI ‘access policies’ to secure data and defend against runtime threats
- **Vulnerability Detection** – Model validation is an advanced automated testing service designed to assess the security, privacy, and safety of AI models and applications

Protection: Guardrail Categories

Security

- Prompt Injection
- Denial of service
- Cybersecurity and hacking
- Code presence
- Adversarial content
- Malicious URL

Privacy

- IP Theft
- PII
- PCI
- PHI
- Source code

Safety

- Financial harm
- User harm
- Societal harm
- Reputational harm
- Toxic content

Relevancy (Coming Soon)

- Content moderation
- Hallucination
- Off-topic content

Map guardrails to standards and frameworks:

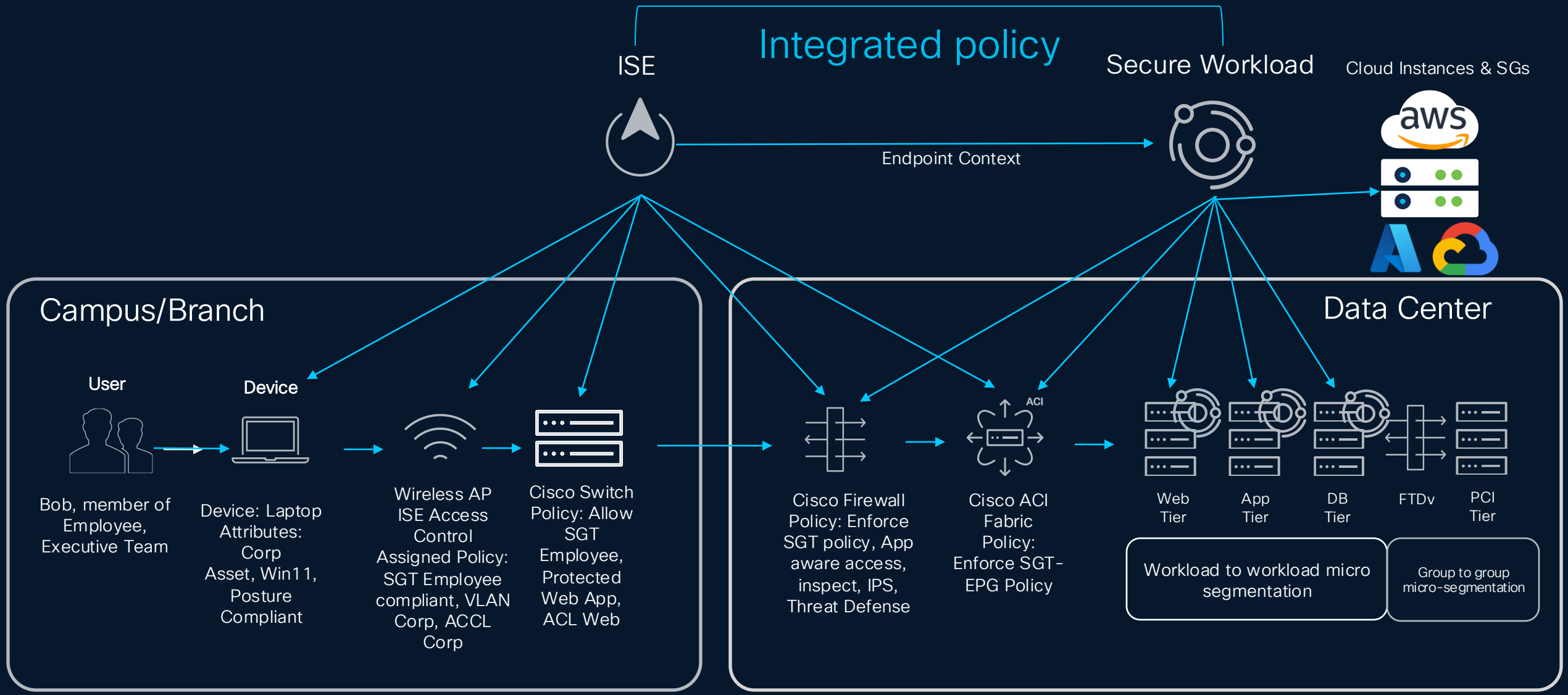
OWASP

MITRE ATLAS

Guardrails can be modified to fit industry, use case, or preferences

cisco

Cisco's Zero Trust Segmentation Strategy



Traditional Segmentation for Workloads

All types of workloads

Windows | Linux | Cloud

Virtual Machine

BareMetal

SaaS delivered

Get started quickly without hardware investment

Confident outcomes

Speed up time to value with implementation services

Extend Hybrid Mesh Firewall Policy Enforcement to Cisco ACI fabric

NEW

Automate segmentation policy discovery

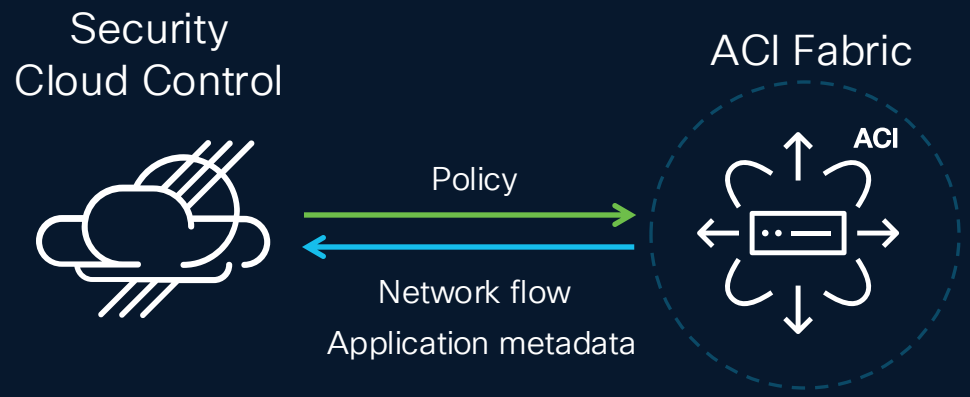
With AI-driven deep visibility into application behavior and dependencies

Optimal fit policy enforcement on ACI

With complete automated switching and app infrastructure knowledge

Zero friction to adoption

With agentless visibility and segmentation



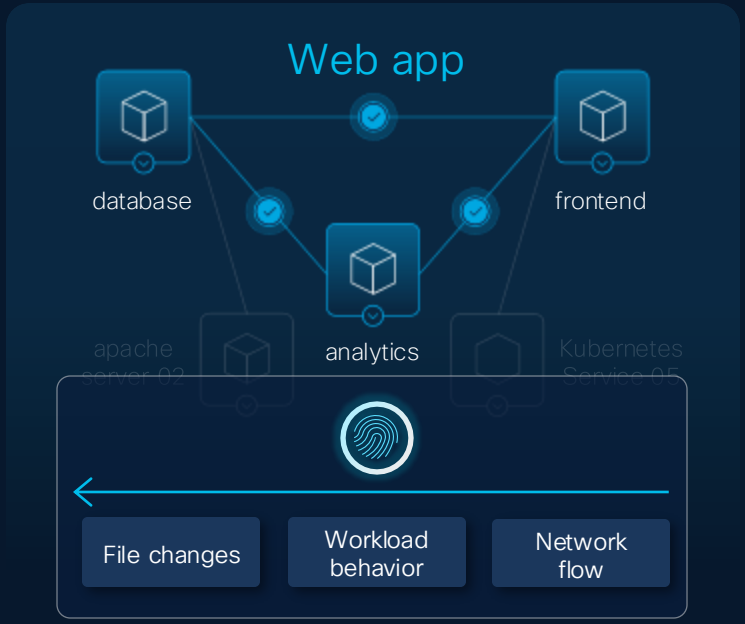
Cloud-Native Segmentation for Kubernetes

Discover microservice interactions

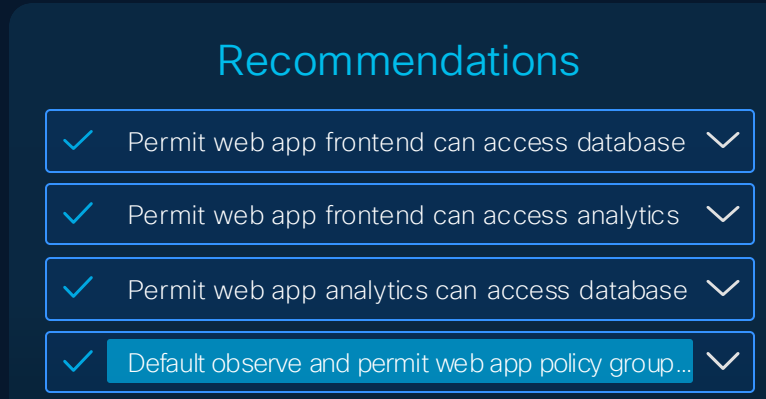
Enforce policies in the Kubernetes fabric

Autonomous Segmentation

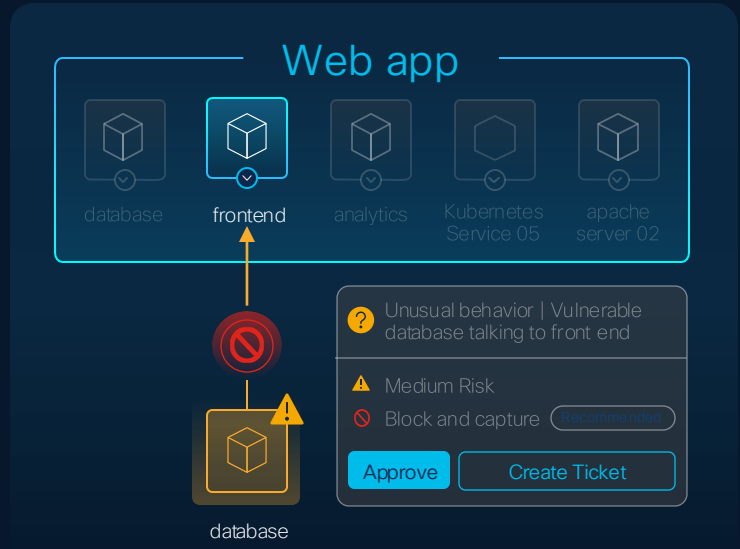
FUTURE



Complete understanding of changing app behavior from network to workload to pre-prod



Flexible segmentation rules that help avoid app fragility



Policies updated to stricter rules in response to suspicious events

cisco

Cisco Data Center Switch + Hypershield
Best of Breed Platforms for DC Services

Cisco N9300 Series Smart Switch *(1H 2025)*

24-port 100G

- 800G Stateful Services Throughput
- 4.8T Silicon One + AMD DPUs
- 1 RU

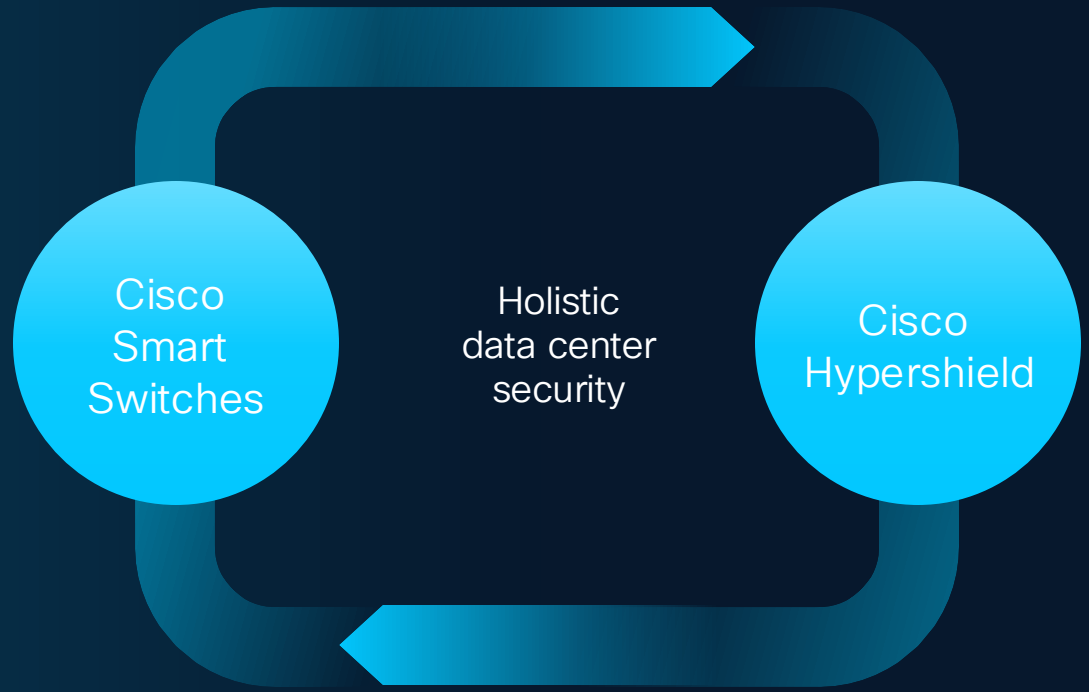
Cisco N9300 Series Smart Switch (2H 2025)

48-port 25G, 6-port 400G, 2-port 100G)

- 800G Stateful Services Throughput
- 4.8T Silicon One + AMD DPUs
- 1 RU

Security Infused Into the Data Center Fabric

Use cases



- Cloud Edge
- Zone-based segmentation
- Data Center Interconnect (DCI)

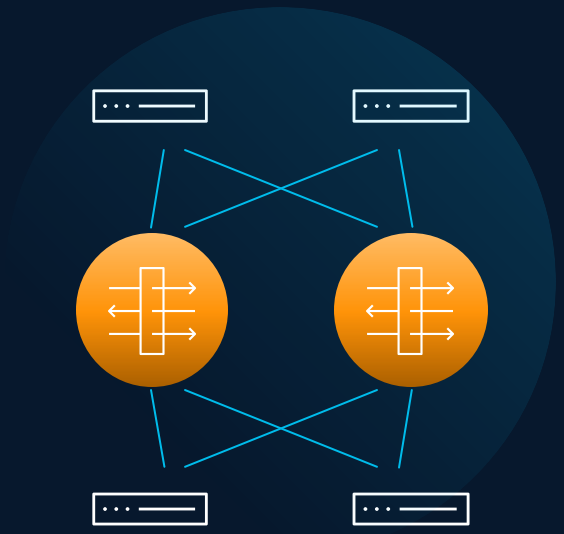
N9324C-SE1U

- Top of Rack Segmentation & Enforcement

N9348Y2C6D-SE1U & N9324C-SE1U

L4 Switch Fabric Segmentation Delivers: Simplified Network Insertion

Before:



2x firewalls

+4x switches

After:

Just 2x N9324C Smart Switches

Journey to Success with Microsegmentation

Prioritize Applications

Select high-value applications to target

Gain Visibility

See and understand what the application is doing.

Add Context

Integrate with systems of record.

Model the Policy

Enable automatic discovery and manual definition.

Policy Simulation

Test & validate the policy.

Enforce Policy

Enforce micro-segmentation and automate the policy lifecycle

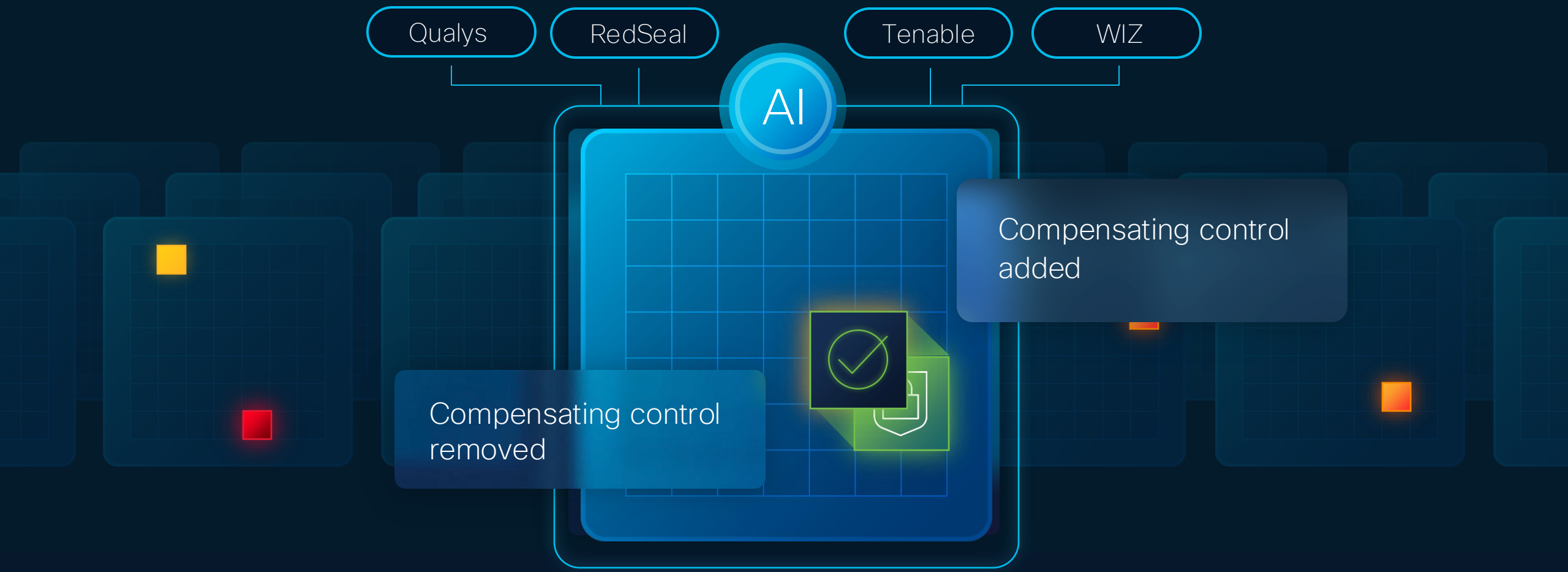
Operate, Automate, and Refine

Visibility enables compliance monitoring and continuous improvement.

Patching Is Hard

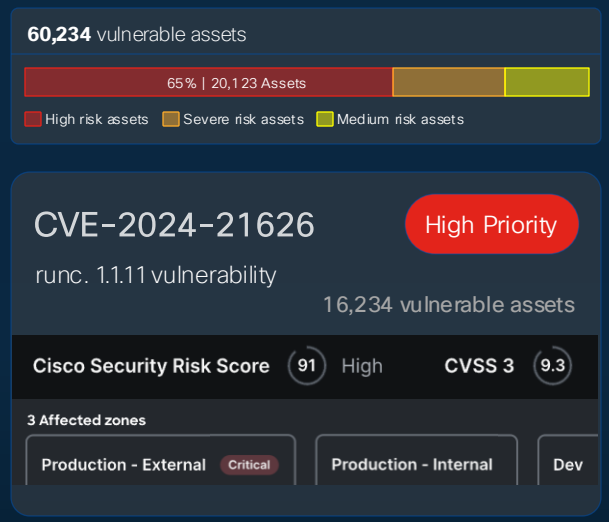
Distributed Exploit Protection

FUTURE



Closing the Exploit Gap With Automated Workflows

FUTURE



Data-driven vulnerability prioritization

+19 threat and exploit intel feeds

+12.7B managed vulnerabilities

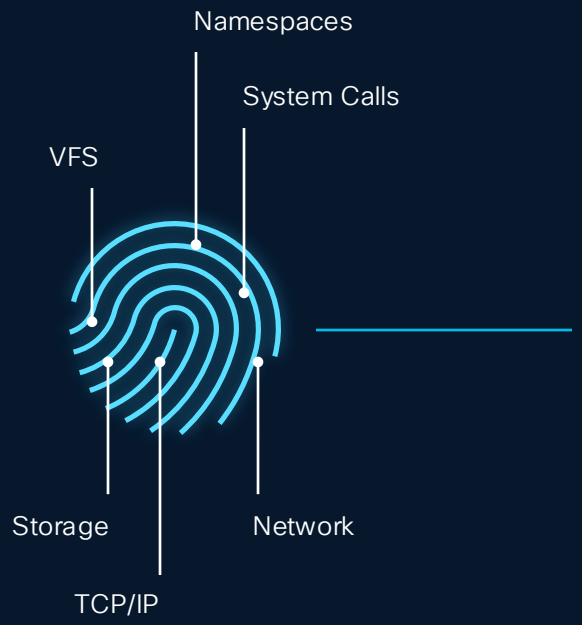
+1B security events processed monthly

Surgical mitigating control that keeps application running

Tested against live production traffic to earn trust and increase confidence

Proactive Defense With Unknown Vulnerability Protection

FUTURE



APP IDENTITY

VALIDATED

dir traversal → file read

/var/www → httpd → /etc/apache2/ httpd_conf

SUSPICIOUS

CWE-78
OS command injection

CWE-200
Unauthorized access to sensitive information

MALICIOUS

Web shell payload → Saved in PHP dir → Execute web shell

Application-specific behavior analysis | Common weakness enumeration and analysis

cisco

Cisco Security Cloud

Cisco Breach Protection

- Extended Detection & Response
- Network Detection & Response
- Email Security
- Managed Detection & Response

Cisco User Protection

- Posture & Auth Management
- Endpoint Security
- Email Security
- Identity Security
- Remote Browser Isolation
- Security Service Edge
- Network Access Control

Cisco Cloud Protection

- Workload Security
- Container Networking & Security
- Virtual Firewall
- Hypershield
- Multicloud Defense

Firewall | SD-WAN

Supercharged by **Identity Intelligence and AI**

Cisco Security Suites Composition

User Protection

$/user, min 100 users

Advantage	Secure Access Advantage (Secure Internet & Private Access) Duo Advantage Email Threat Defense Secure Endpoint Advantage Identity Services Engine (ISE) Premier
Essentials	Secure Access Essential (Secure Internet & Private Access) Duo Advantage Secure Email Threat Defense

Breach Protection

$/user, min 100 users

Premier	Cisco XDR Premier (Managed XDR) Cisco Talos Incident Response Cisco Technical Security Assessments Email Threat Defense Secure Endpoint Premier Secure Network Analytics Cisco Telemetry Broker
Advantage	Cisco XDR Advantage Secure Email Threat Defense Secure Endpoint Premier Secure Network Analytics Cisco Telemetry Broker
Essentials	Cisco XDR Essentials Secure Email Threat Defense Secure Endpoint Advantage

Cloud Protection

Segmentation: $/workload, min 25 workloads
Gateway: $/virtual firewall, min 10 firewalls

Essentials Segmentation	Secure Workload SaaS Hypershield Isovalent Enterprise Platform[1]
Essentials Gateway	Secure Virtual Firewall (FTD-30) with Threat Licensing Multicloud Defense Premier Firewall Management Software[2]

[1] Future inclusion with Security Cloud Control | [2] Delivered through Security Cloud Control

Wrapping Things Up

Capturing Industry and Customer Mindshare

IDC MarketScape LEADER 2025

Hybrid Firewall

Leader in Worldwide Enterprise Hybrid Firewall 2025

FORRESTER WAVE LEADER 2024

Secure Firewall

Leader in Enterprise Firewall

Secure Workload

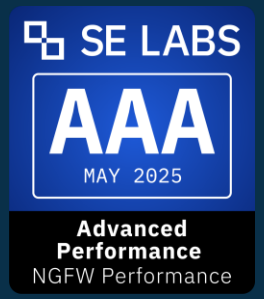
Leader in Microsegmentation

Secure Firewall

Cybersecurity Excellence Award

Secure Firewall

First in industry to receive AAA rating in Advanced Performance



Secure Firewall

2024 Best Next Gen Firewall

NetSecOPEN

University of New Hampshire InterOperability Laboratory

Secure Firewall

Best inspected throughput

Next Steps

See why we were ranked a leader in the 2025 IDC MarketScape for Enterprise Hybrid Firewall:

https://www.cisco.com/c/en/us/products/security/idc-worldwide-enterprise-hybrid-firewall-vendor-assessment-2025.html

Pick a date and join our segmentation workshop:

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

Request a personalized demo with a Firewall Expert: https://www.cisco.com/c/en/us/products/security/firewalls/get-started.html

Q&A

Thank you


CISCO