CISCO Engage | Tech Day

Cisco Hybrid Mesh Firewall:

Unify Policy Across All Your Segmentation Points

Scott Wofford, USPS Segmentation Engineer

October 8, 2025

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)

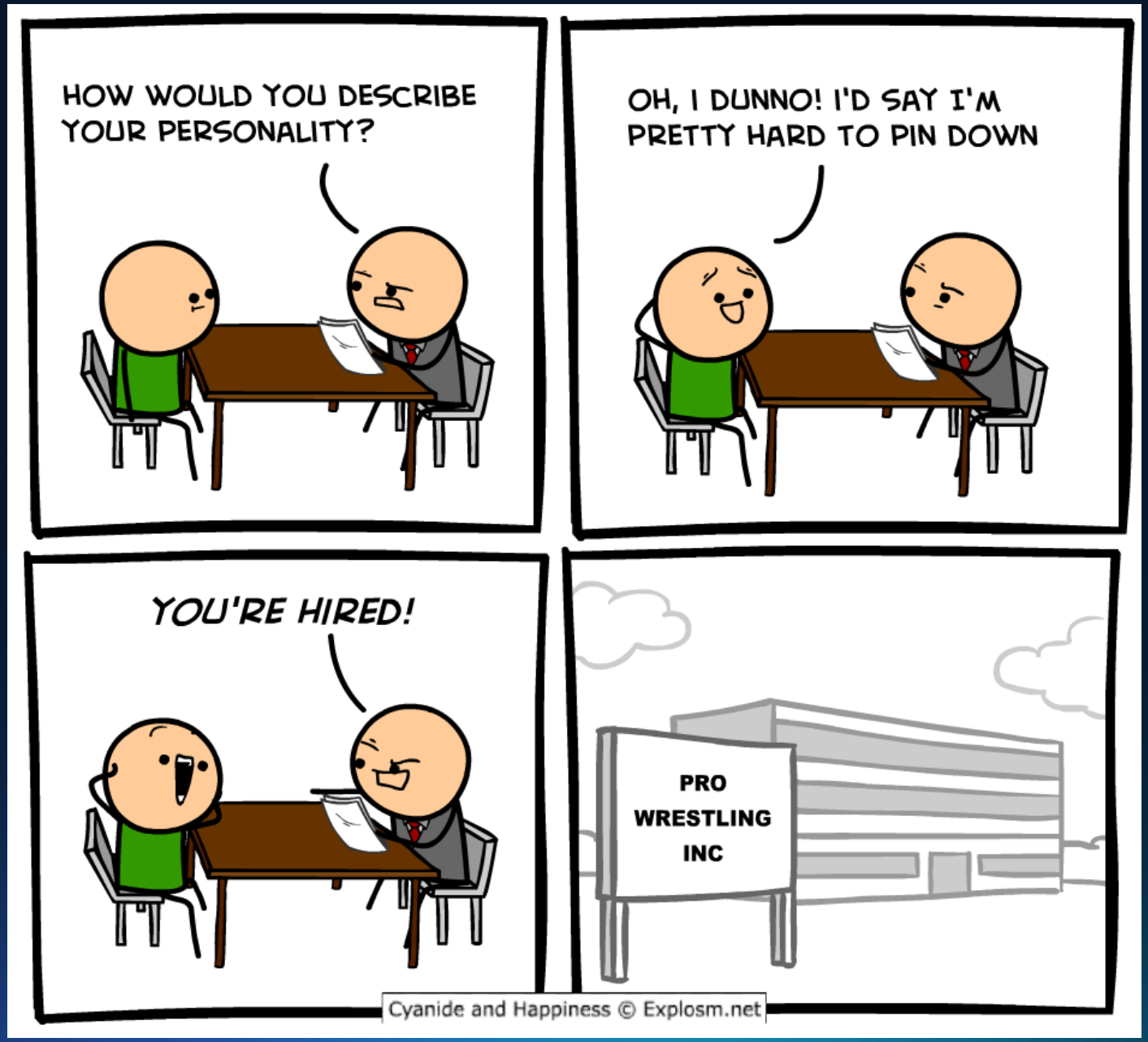
4th Gen NGFW

DPI, IPS/IDS, Malware Protecton, User Identity

What is a Hybrid Mesh Firewall

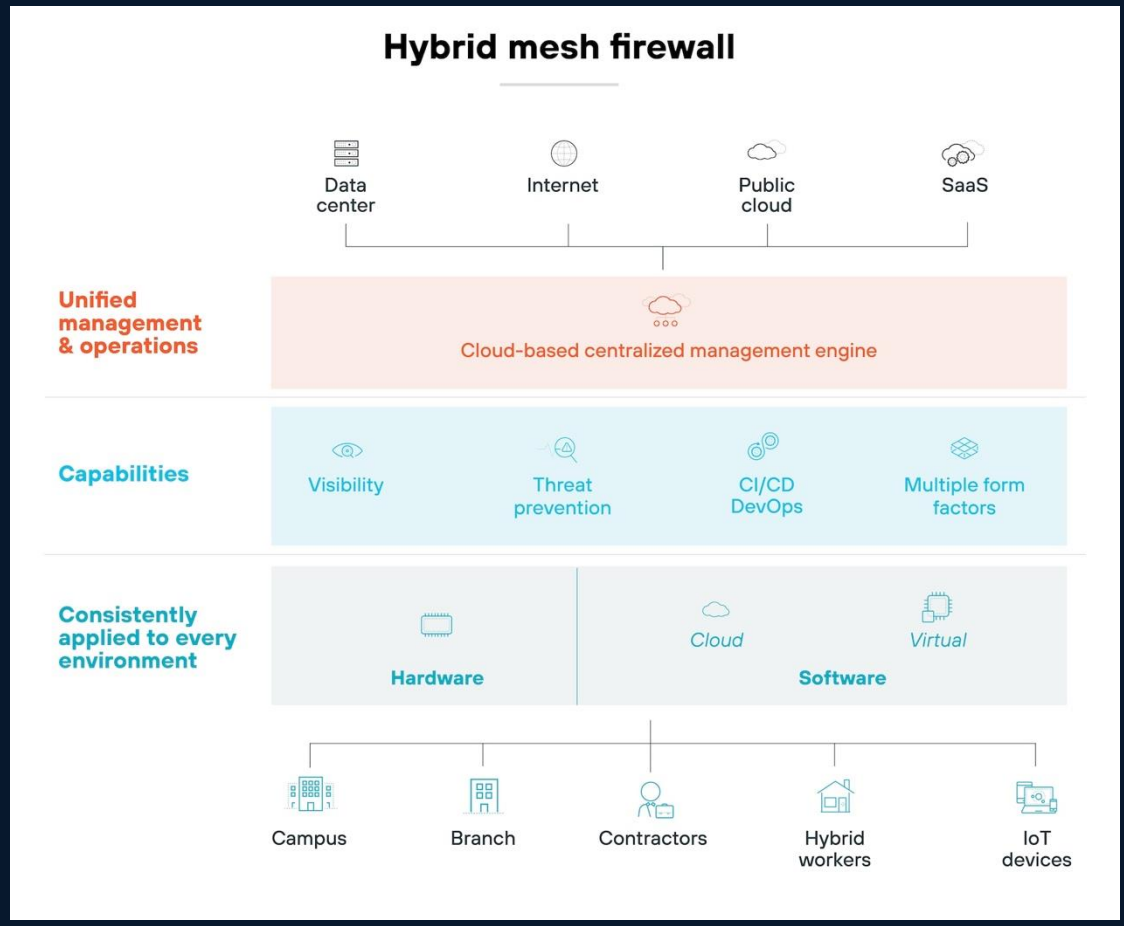
“A hybrid mesh firewall (HMF) is a multi-deployment mode firewall, including hardware, virtual appliance and cloud-based options, with a unified cloud-based management plane.”

Gartner



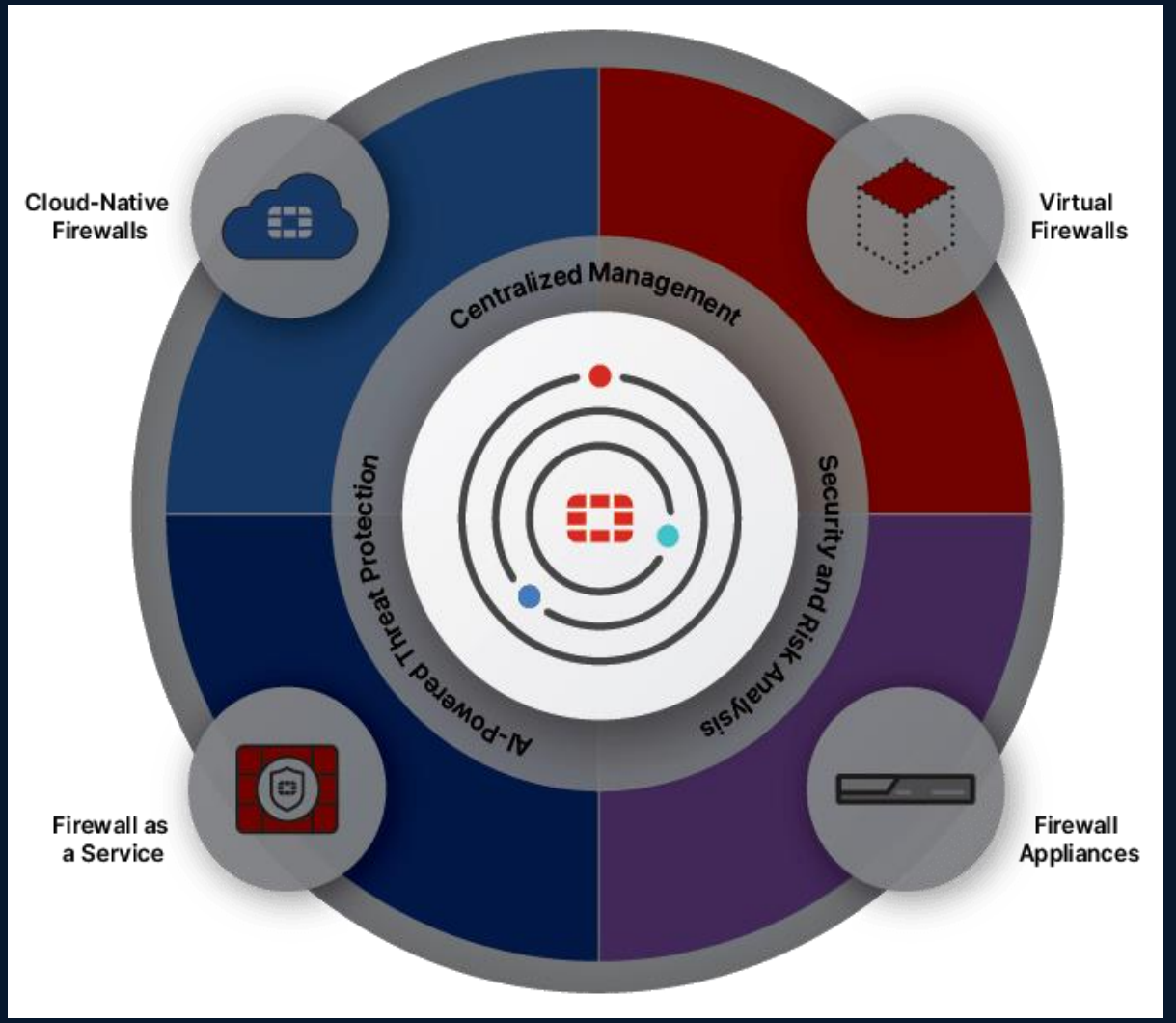
Manufacturer P's Approach

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



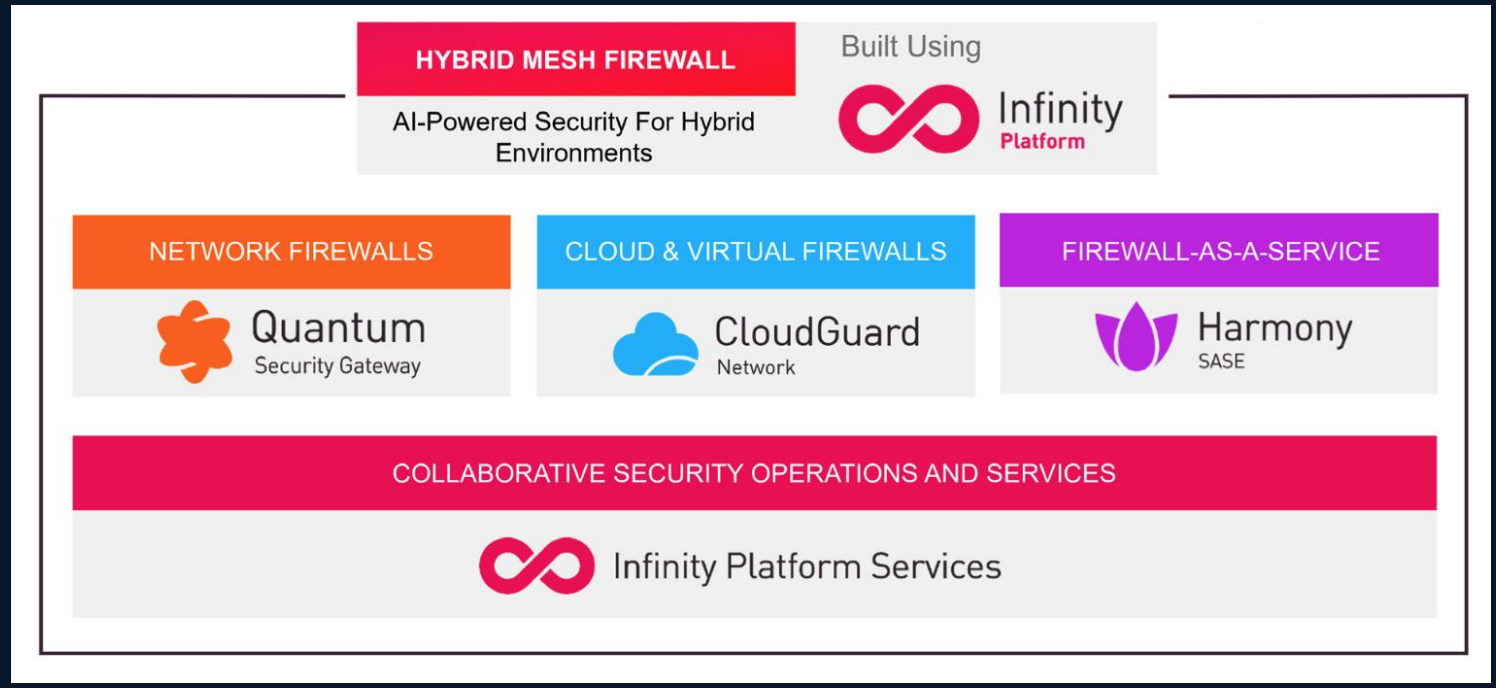
Manufacturer F's Approach

"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

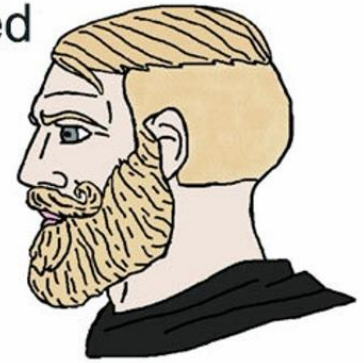
More vulnerabilities, exploited faster

AI adoption makes it more challenging

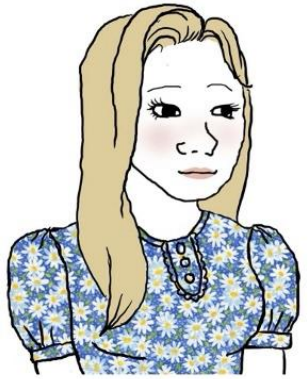
My parents at age 25

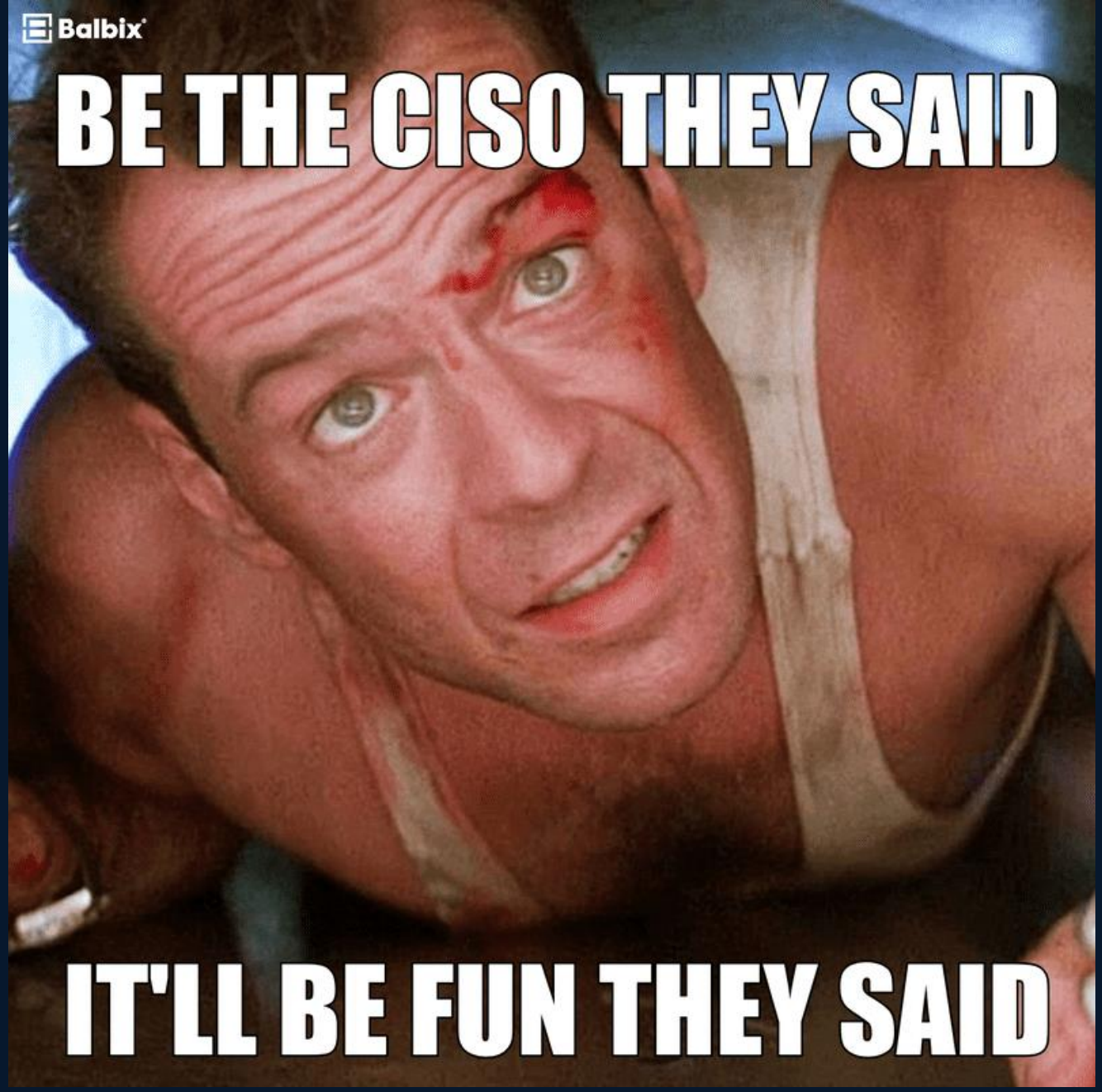
Let's get married

Yes



Me at age 25





Combating Firewall Admin Burnout

65%

Cyber Professionals Stressed & Fatigued

95%

CISOs reporting high stress levels

88%

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

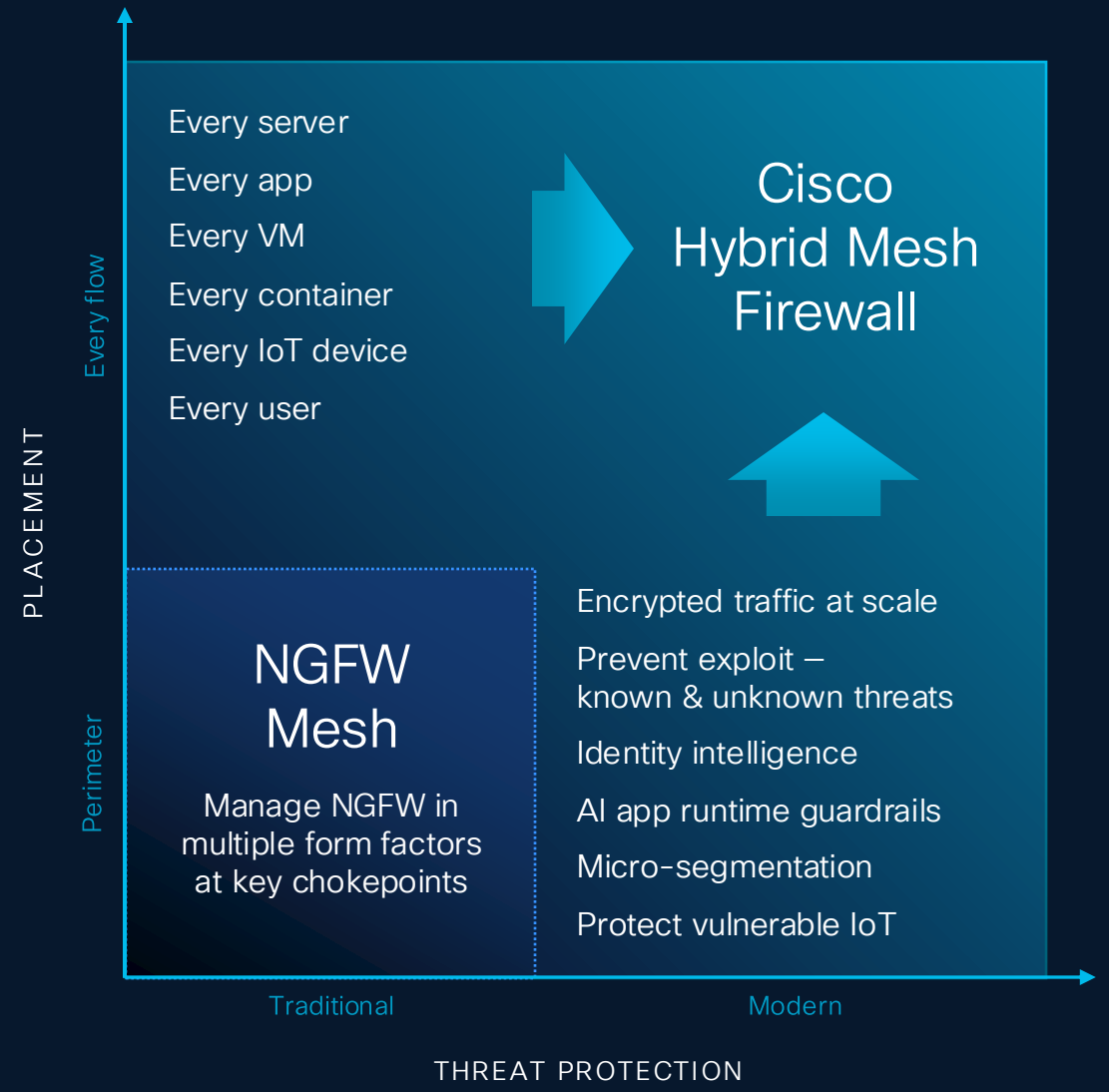
From the CISO

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

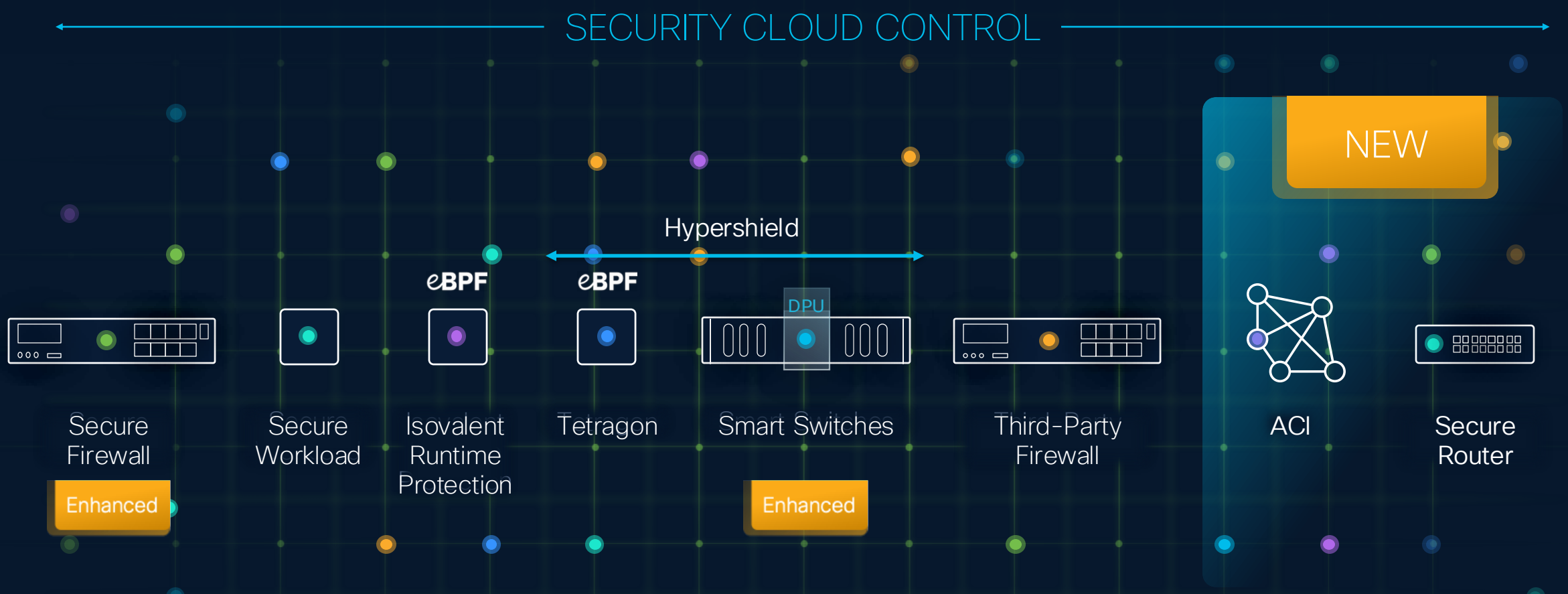
- **Enhance Security Posture**
- **Simplify Security Management**
- **Facilitate Advanced Threat Detection and Response**
- **Protect AI-Driven Applications**
- **Ensure Business Continuity and Compliance**
- **Deliver Scalability and Flexibility**

Cisco’s Approach

Firewalling needs to evolve to meet today's challenges



Cisco Hybrid Mesh Firewall



Write policy once, enforce across the mesh

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

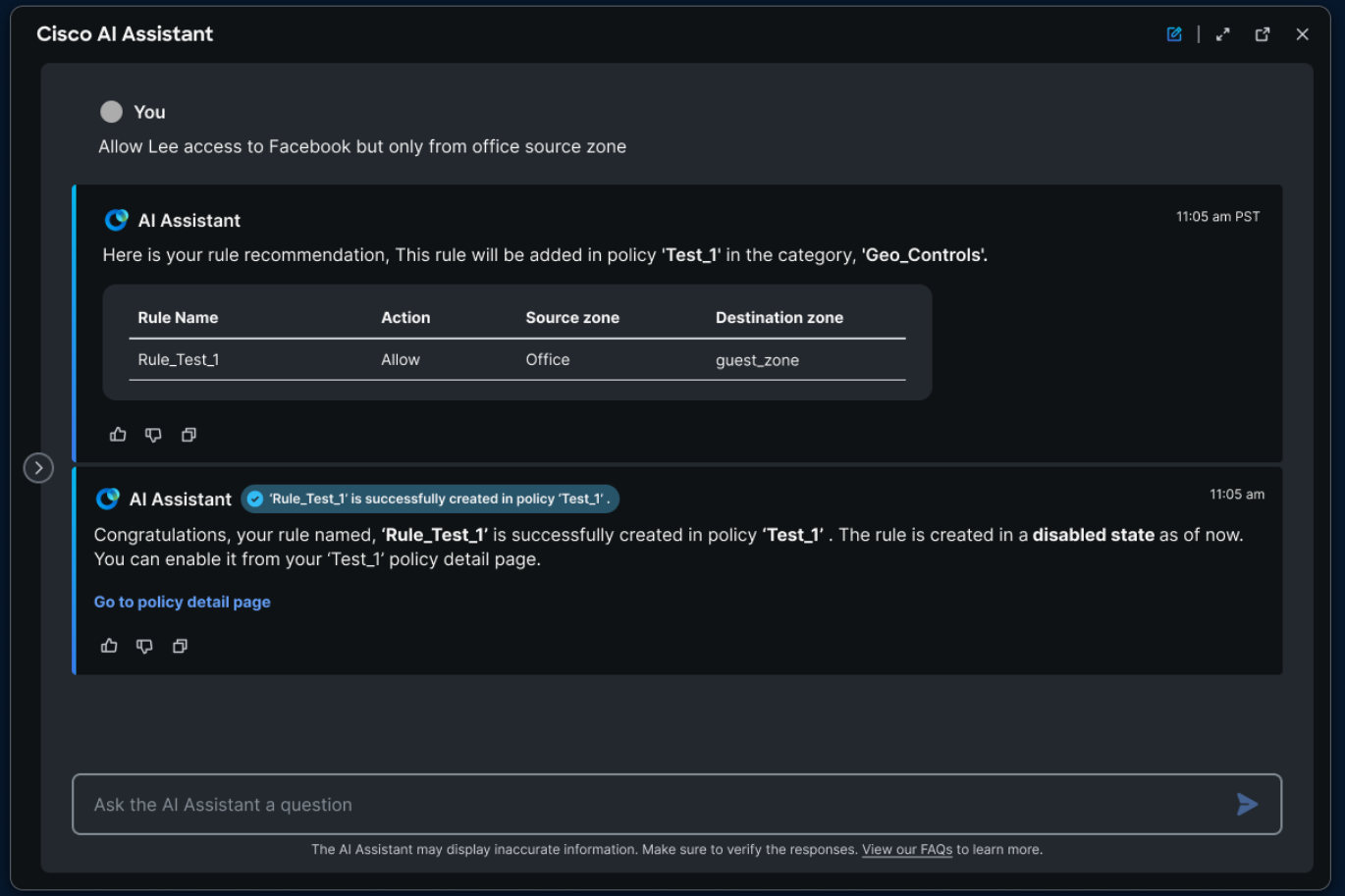
Absorb and optimize existing rules

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

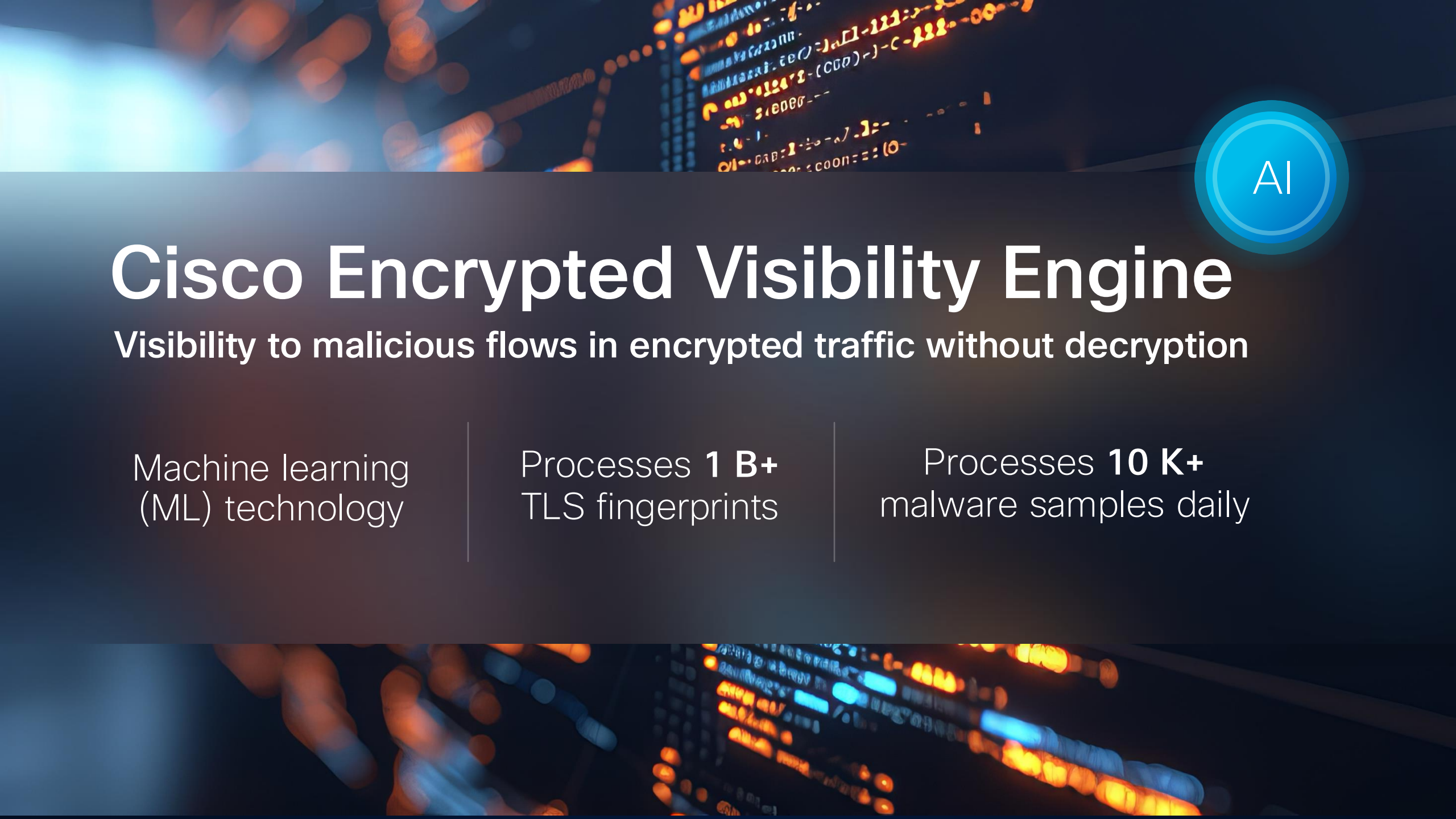
alkira

rackspace technology

EQUINIX

Alibaba Cloud

ORACLE CLOUD INFRASTRUCTURE



Cisco Encrypted Visibility Engine

Visibility to malicious flows in encrypted traffic without decryption

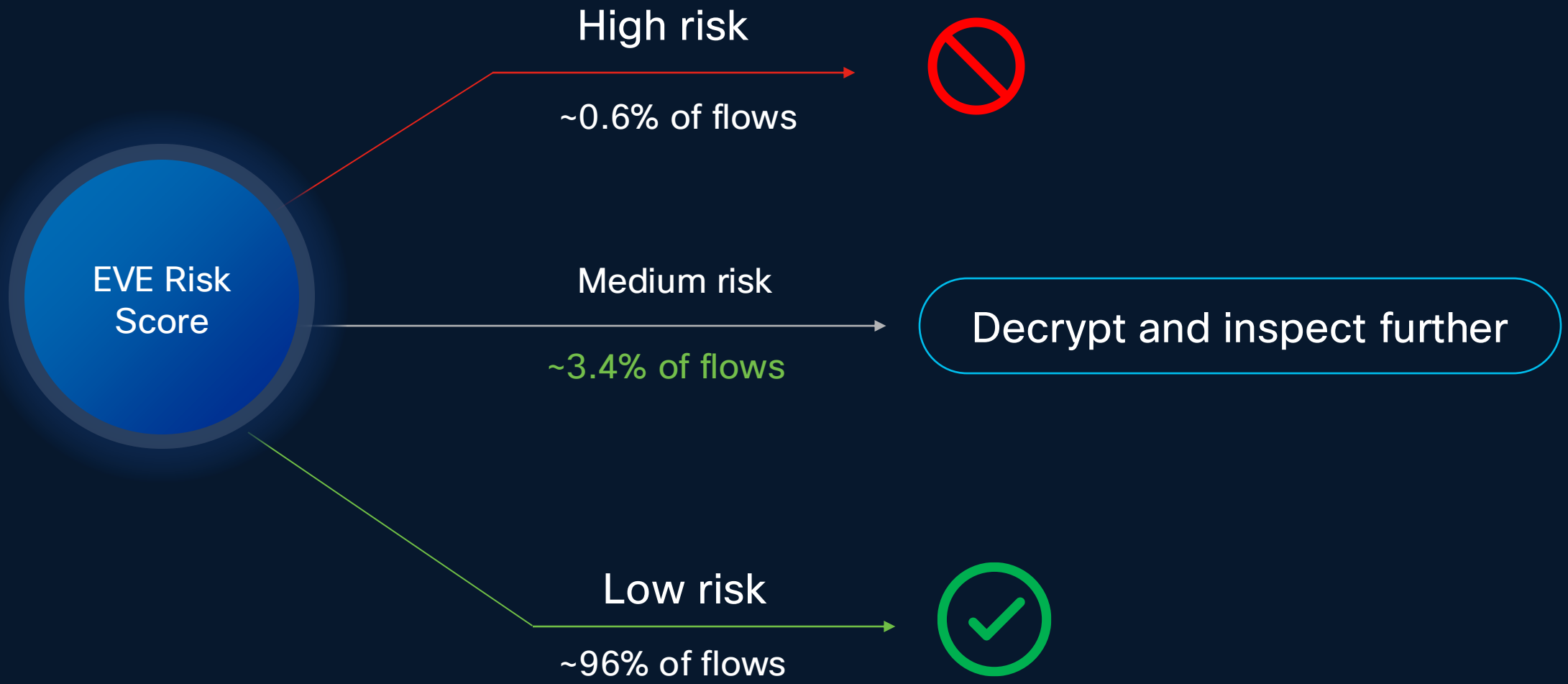
Machine learning (ML) technology

Processes **1 B+** TLS fingerprints

Processes **10 K+** malware samples daily

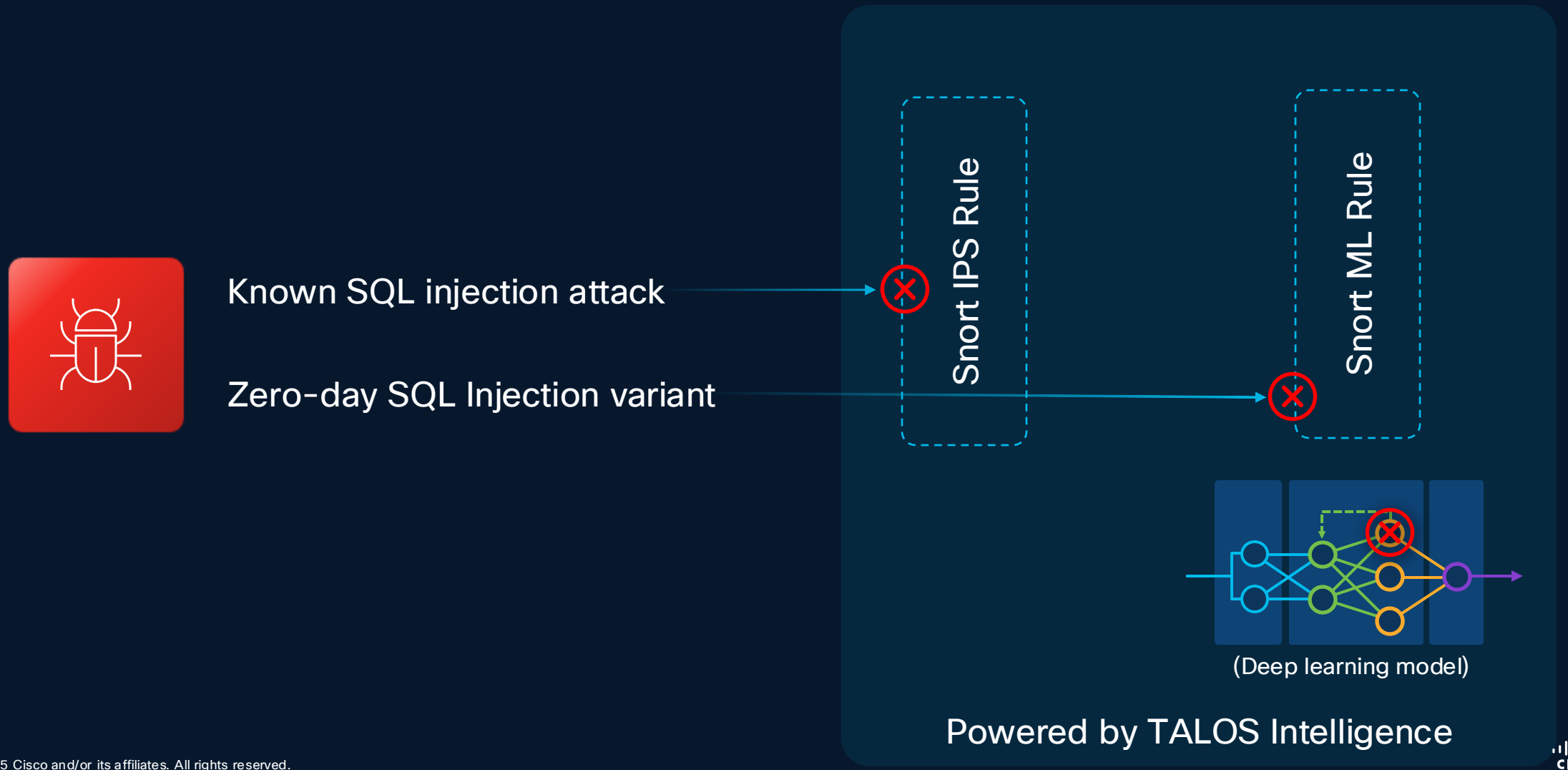
Eve changes the game on decryption

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

Recommended Actions

Protect applications (67)

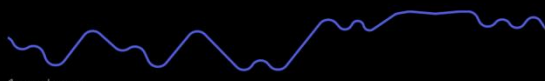
Secures sensitive data, prevents unauthorized access, and protects proprietary algorithms from theft or misuse.

Hide View →

Review increased app usage 3 days ago

Review sudden spikes in blocked events to avoid security risks.

ExternalChatBot Application
45MB +7%



1 week ago

Hide View →

Review third party apps (67) 3 days ago

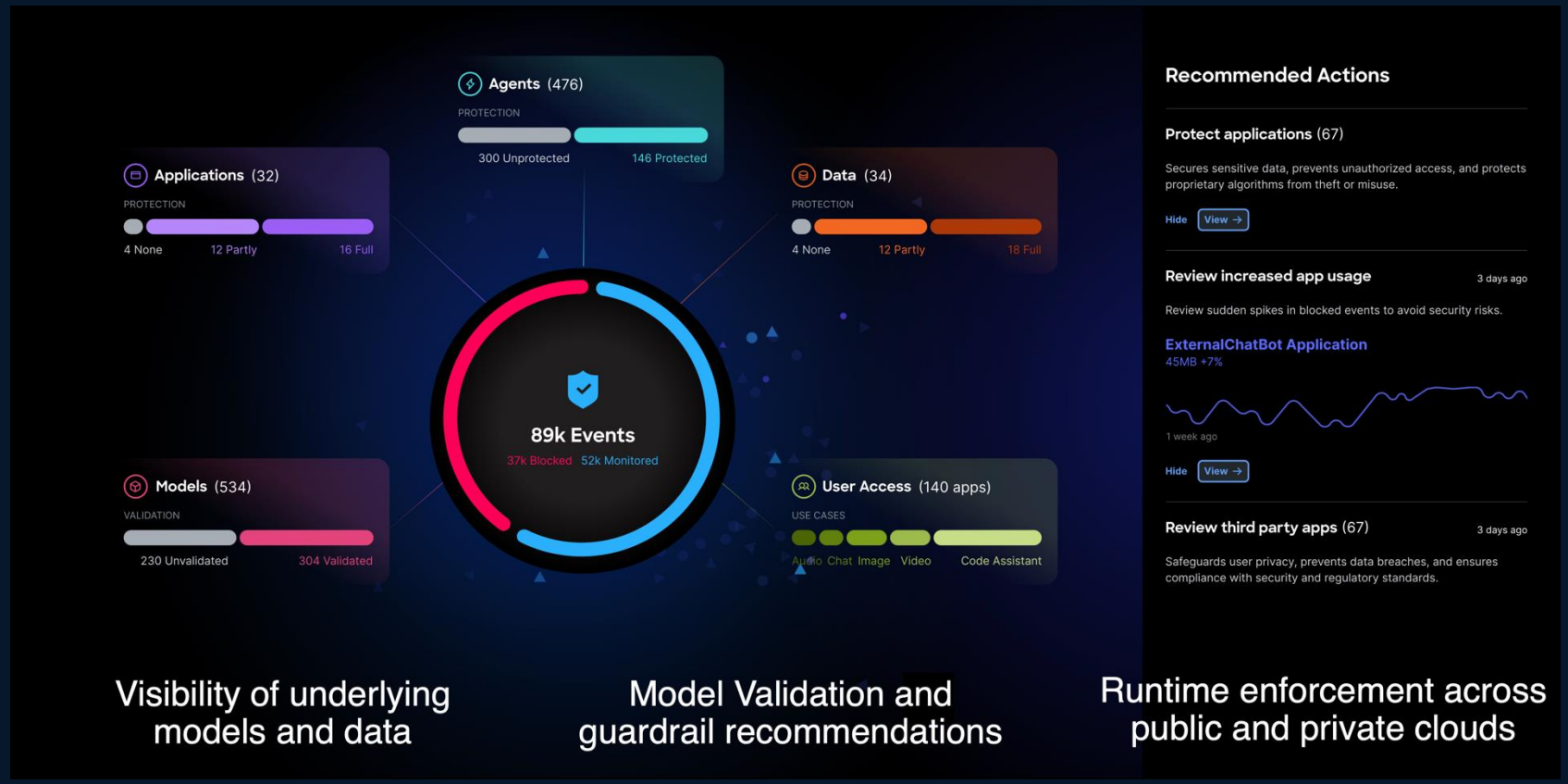
Safeguards user privacy, prevents data breaches, and ensures compliance with security and regulatory standards.

Visibility of underlying models and data

Model Validation and guardrail recommendations

Runtime enforcement across public and private clouds

Delivered via the Hybrid Mesh Firewall



Cisco Security Cloud Enforcement Points

- Multicloud Defense
- Secure Firewall (FUTURE)
- Hypershield (FUTURE)

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

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

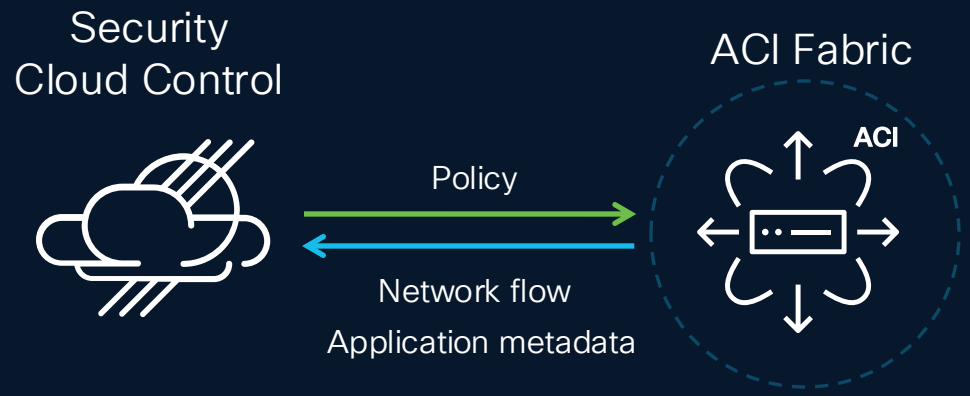
With AI-driven deep visibility into application behavior and dependencies

Optimal fit policy enforcement on ACI

With complete automated switching and app infrastructure knowledge

Zero friction to adoption

With agentless visibility and segmentation



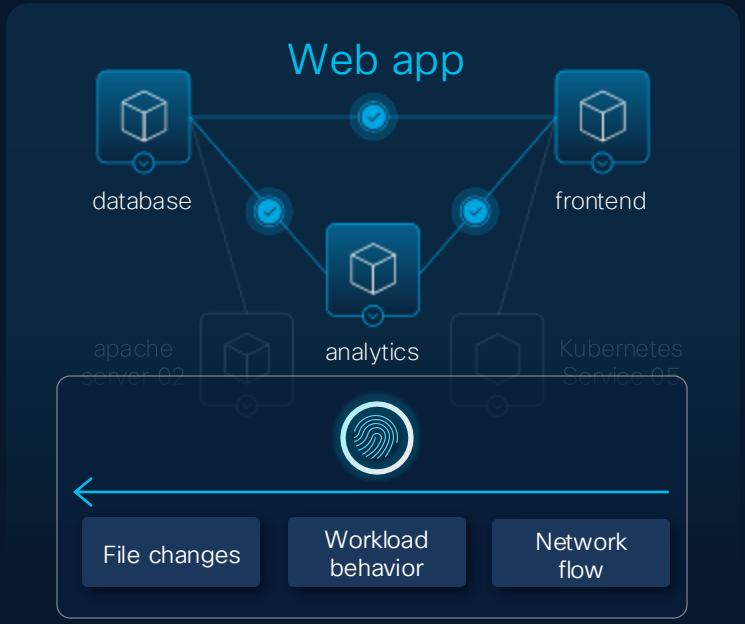
Cloud-native segmentation for Kubernetes

Discover microservice interactions

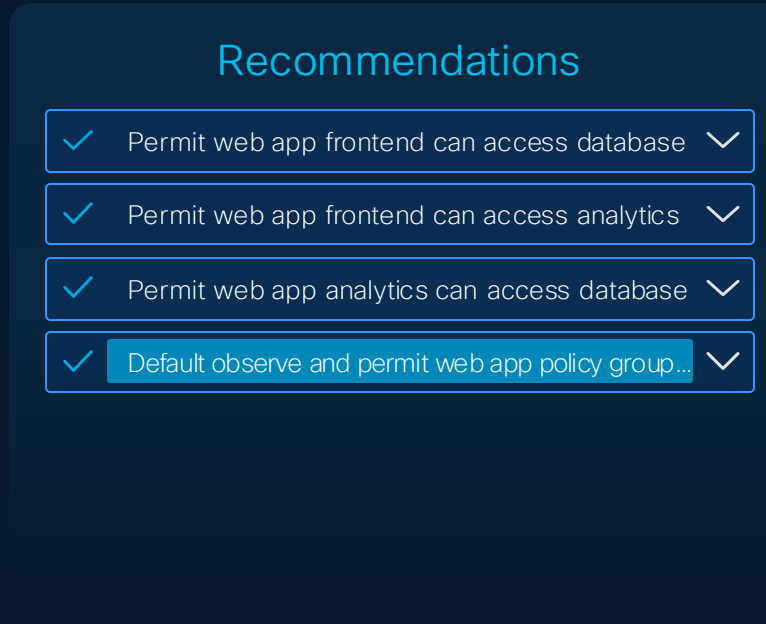
Enforce policies in the Kubernetes fabric

Autonomous Segmentation

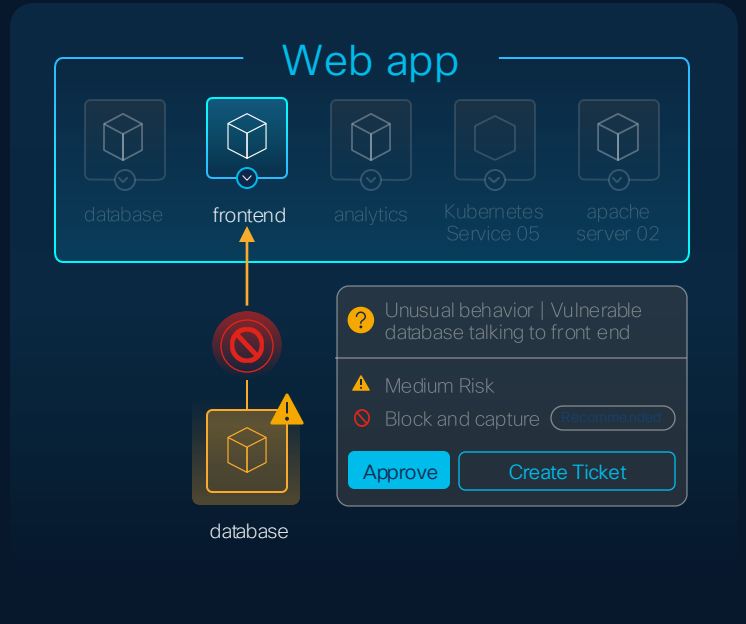
FUTURE



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



Flexible segmentation rules that help avoid app fragility

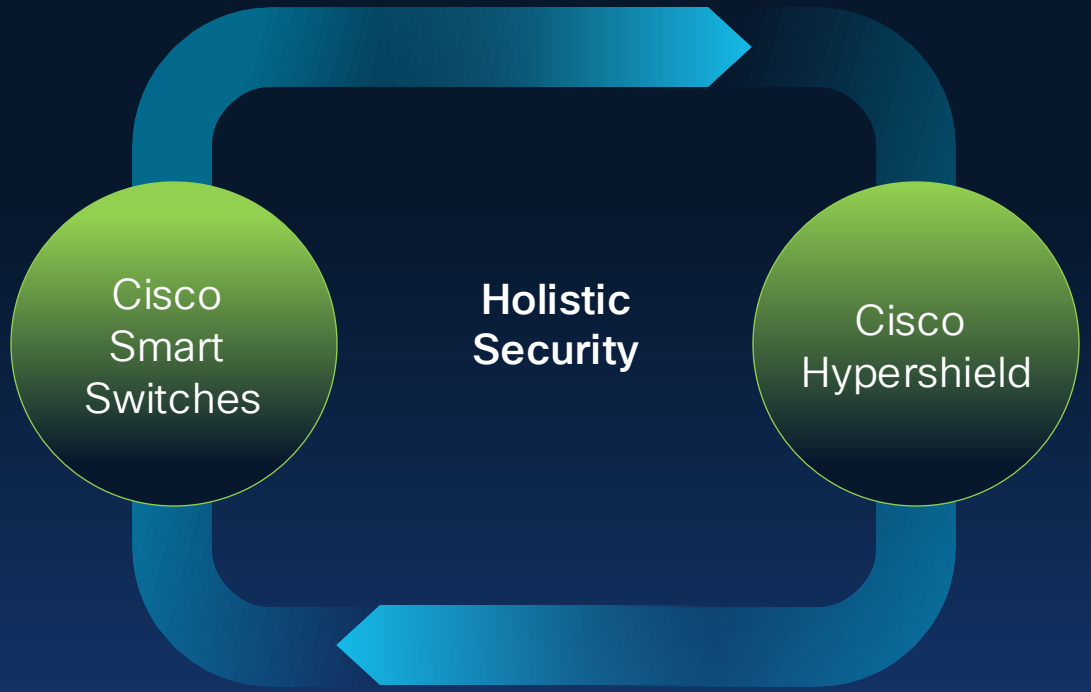


Policies updated to stricter rules in response to suspicious events

cisco

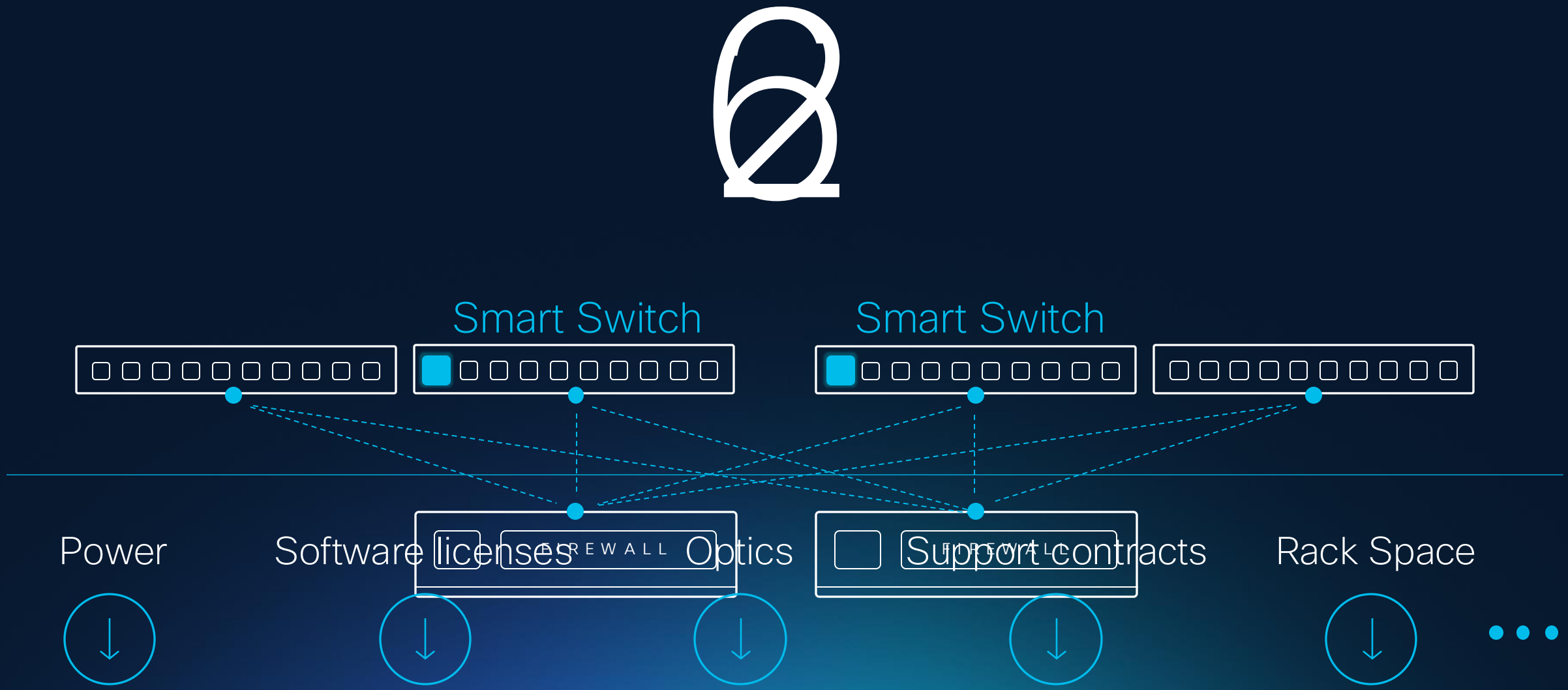
Enable segmentation using the same switch fabric

Infusing security into the network fabric



Segmentation use cases

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



Introducing Cisco Smart Switch

NEW

Network + Security
in one switch

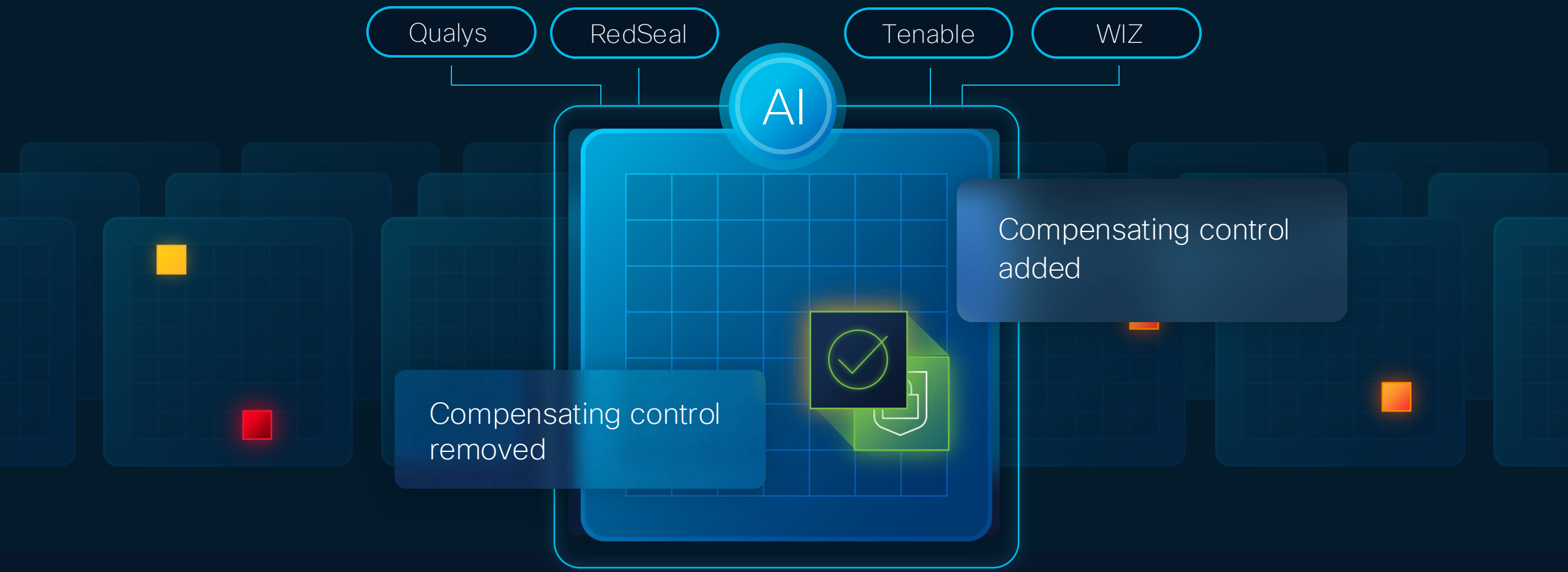
Separate workflows and
separate data flows for
networking and security

Up to 84% TCO savings

Patching is hard

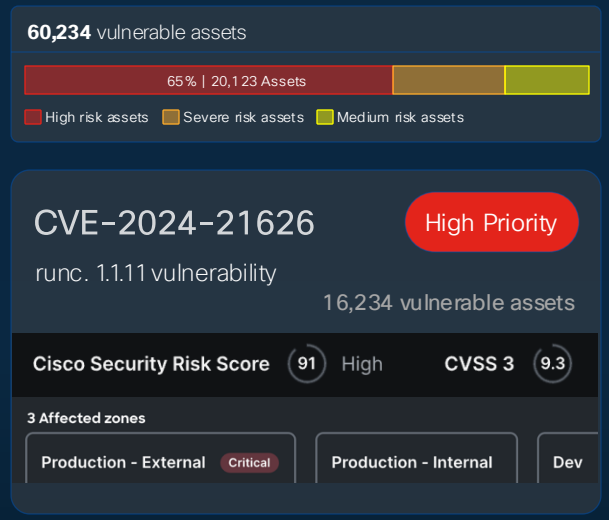
Distributed Exploit Protection

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

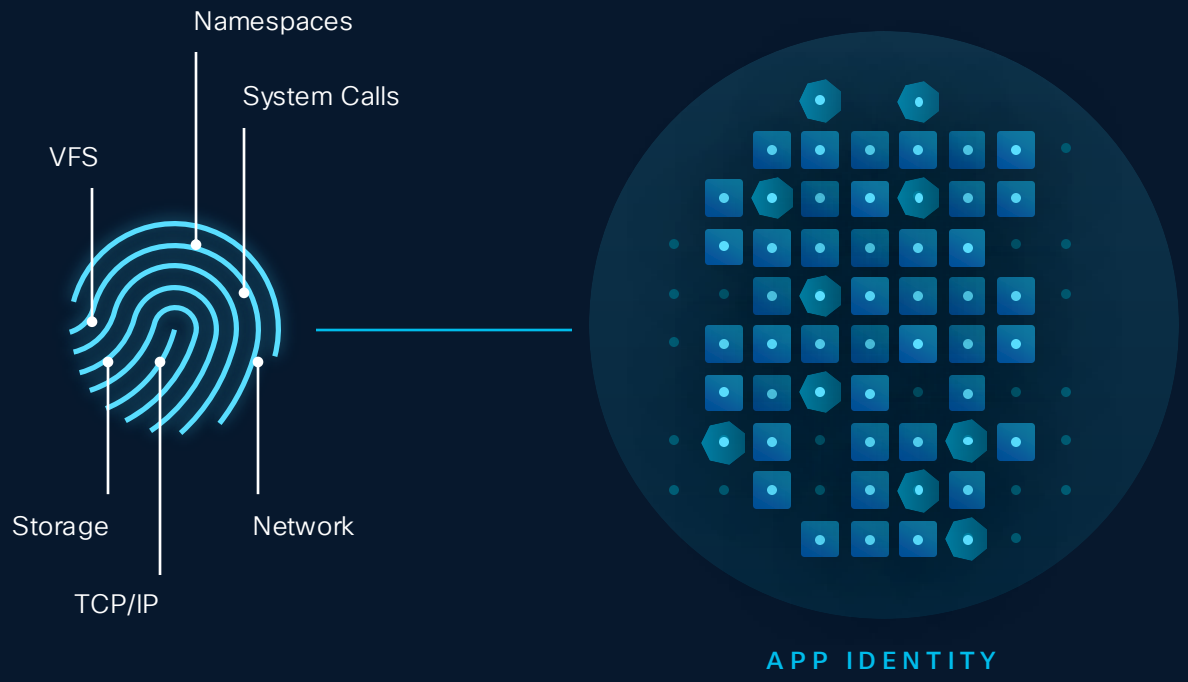
Surgical mitigating control that keeps application running

Tested against live production traffic to earn trust and increase confidence

cisco

Proactive defense with unknown vulnerability protection

FUTURE



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

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

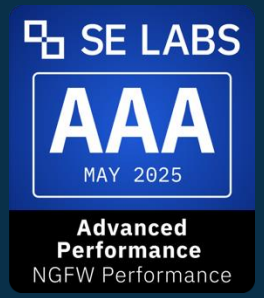
Leader in Microsegmentation

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

Secure Firewall

Best inspected throughput

cisco

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