CISCO Engage | Tech Day

Cisco Hybrid Mesh Firewall

Unified Policy Across All Your Segmentation Points

Lou Norman CCIE, CISSP

December 2025

InfraGard
Partnership For Protection

Securing the enterprise is increasingly challenging

Highly distributed applications

Nothing can be trusted

More vulnerabilities, exploited faster

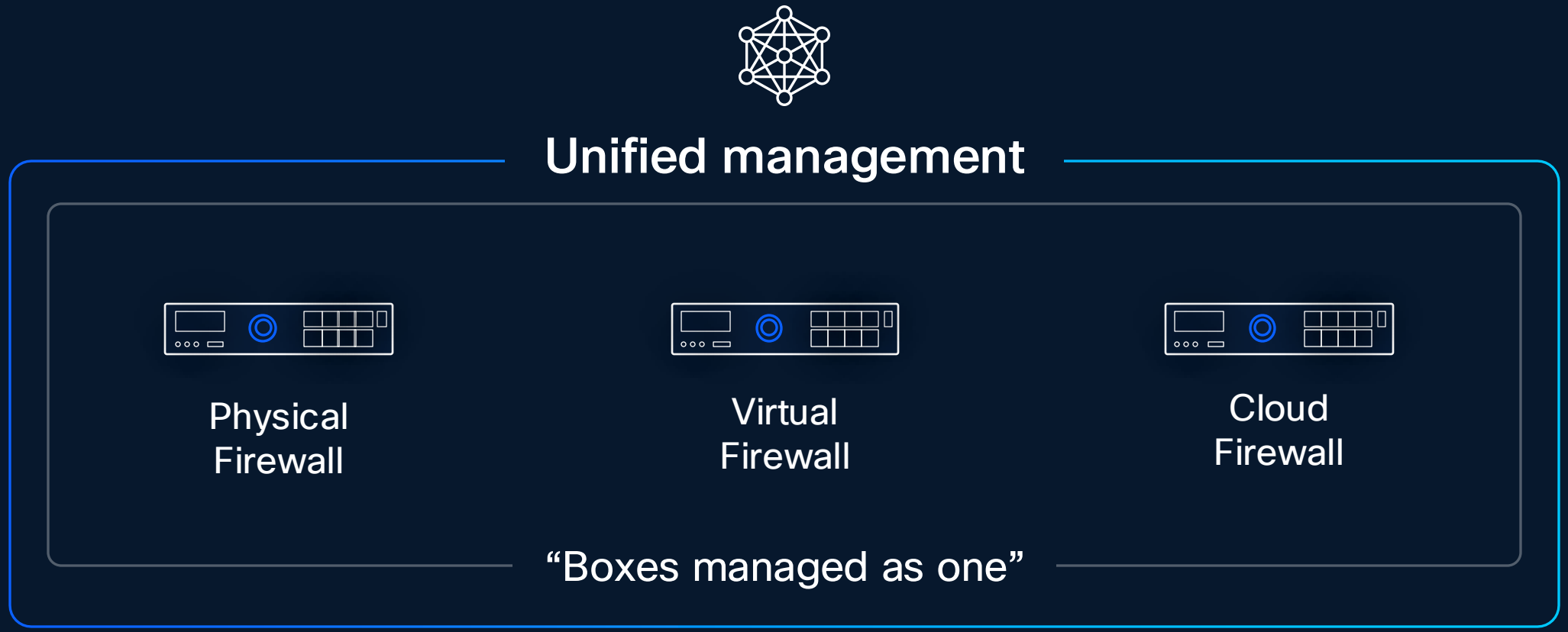
AI adoption makes it more challenging

cisco

From Firewall to Firewalling

	Stateful Firewall	Next generation Firewall	Hybrid Mesh Firewall
	1990-2007	2008-2024	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

Everyone Elses definition of Hybrid Mesh Firewall is limited



Cisco Hybrid Mesh Firewall goes broader and deeper

Security Cloud Control

Native enforcement points go deeper ⟷ Integrate with existing

Unified Management

Write policy once, enforce across the mesh

cisco

NEW

Security Cloud Control

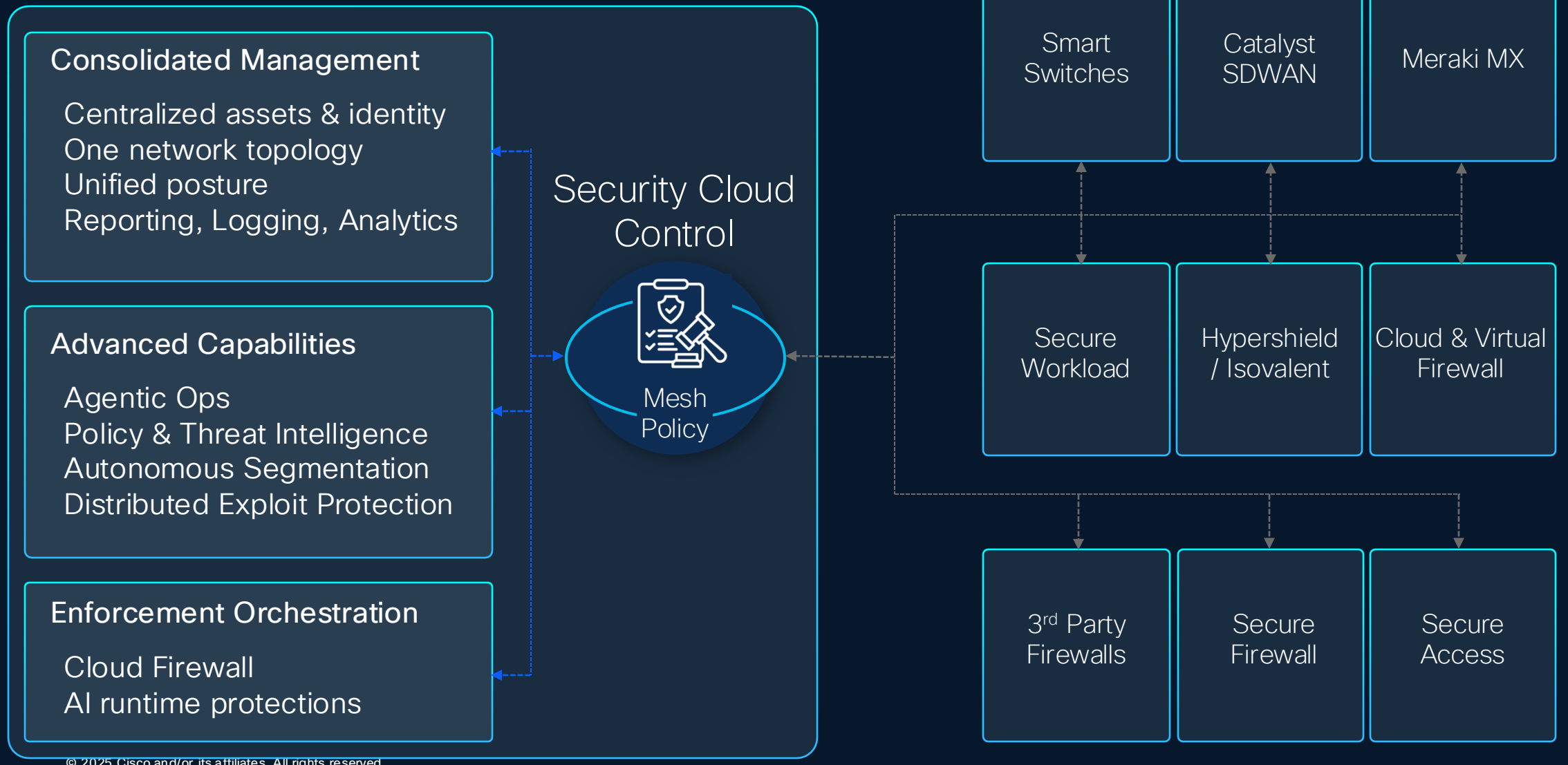
Now powering industry's first multi-vendor intent-based segmentation

Write policy once, enforce everywhere

Absorb and optimize existing rules

Change enforcement points, not policy

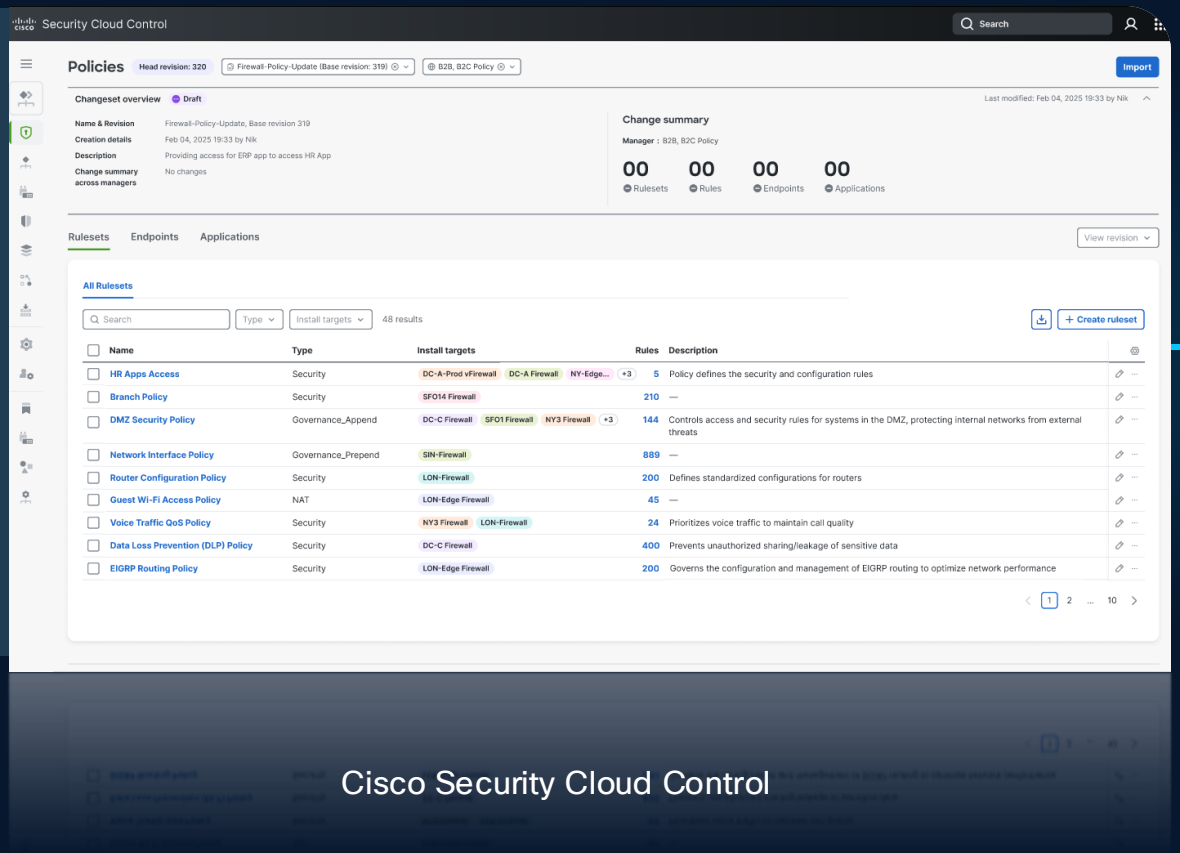
Security Cloud Control



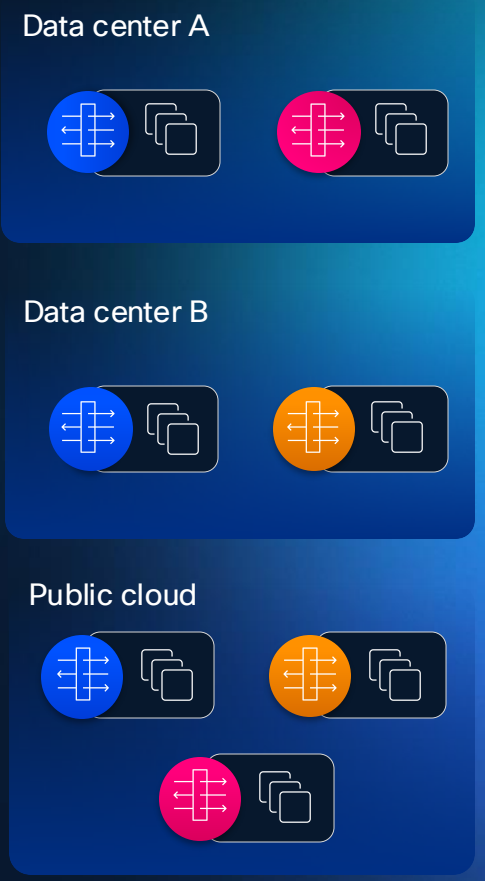
Introducing Mesh Policy Engine

Cisco is the only enterprise firewall vendor that extends policy to non-Cisco enterprise firewalls

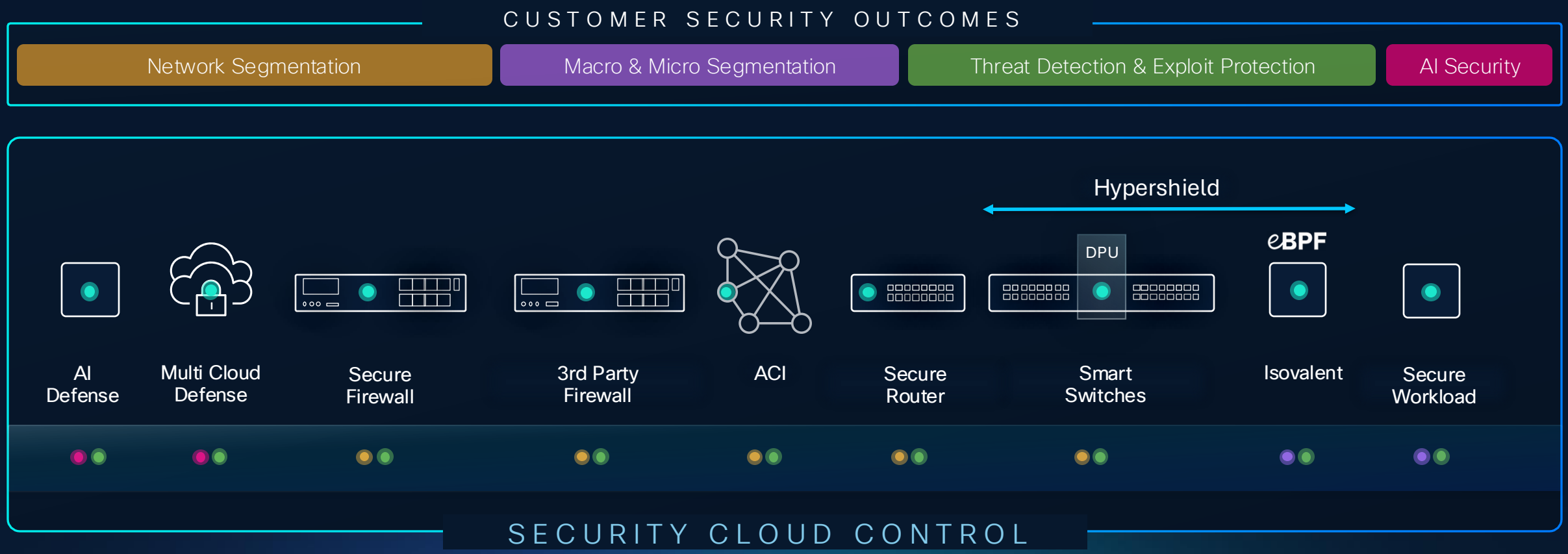
- A policy manager (not a device manager or policy converter)
- Retain the “what” and “where” of the policy **and** the “why”
- Change enforcement points, not policy
- Cisco plus the other enterprise firewall vendors



Cisco Security Cloud Control

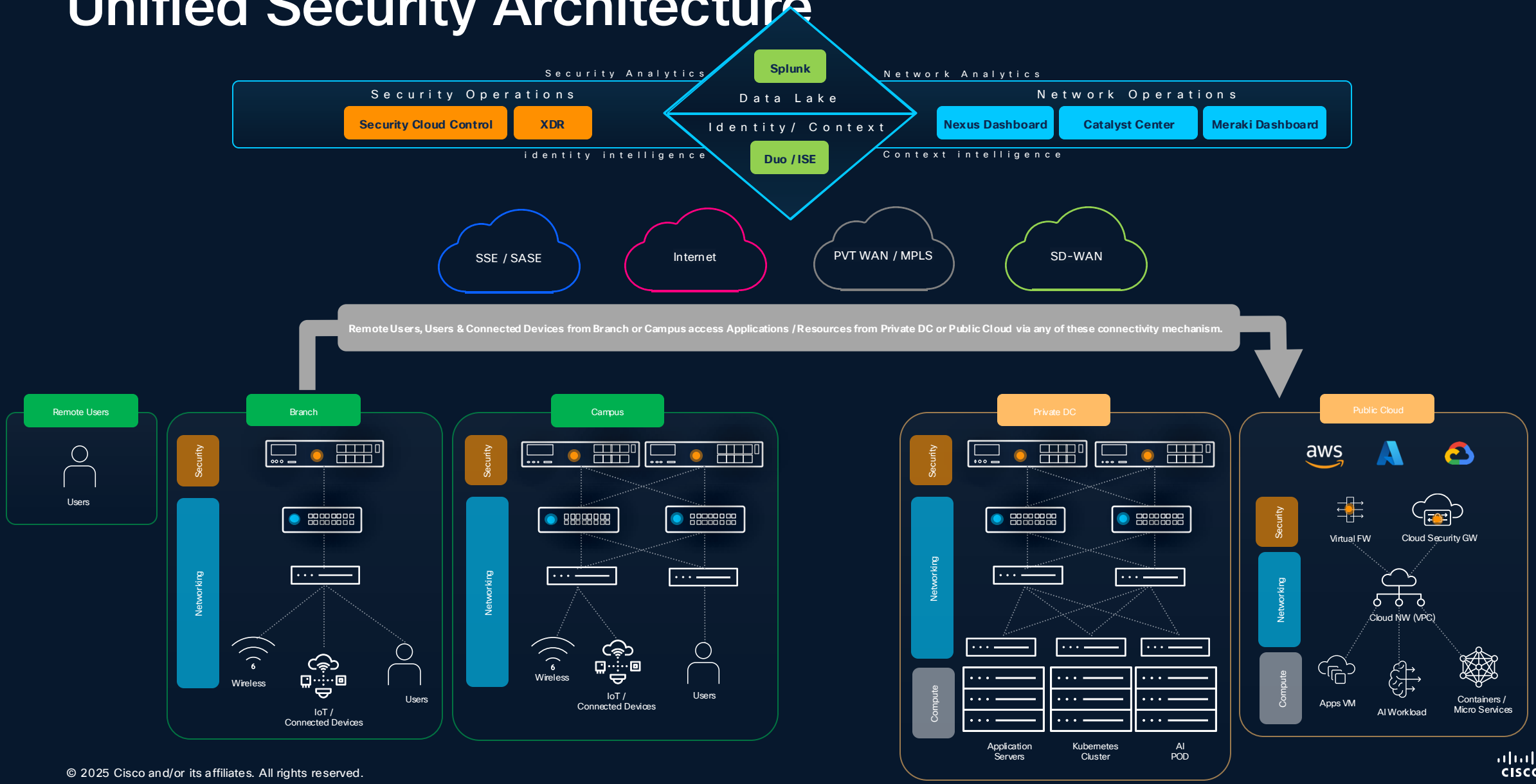


What is Cisco Hybrid Mesh Firewall



Write policy once, enforce across the mesh

Unified Security Architecture



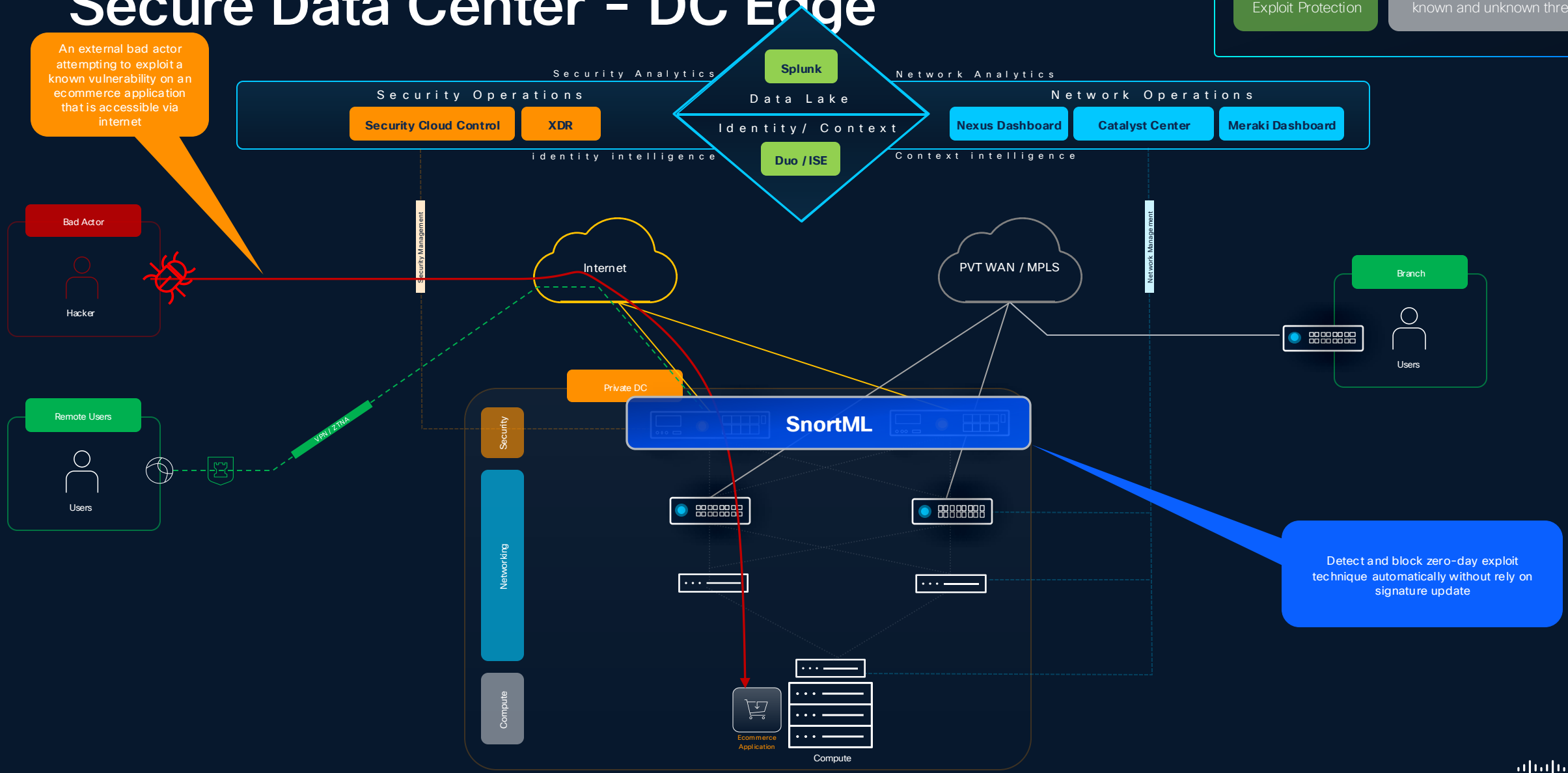
Secure Data Center – DC Edge

SECURITY OUTCOMES

Threat Detection & Exploit Protection

Detect and Protect against known and unknown threats

An external bad actor attempting to exploit a known vulnerability on an ecommerce application that is accessible via internet



Detect and block zero-day exploit technique automatically without rely on signature update

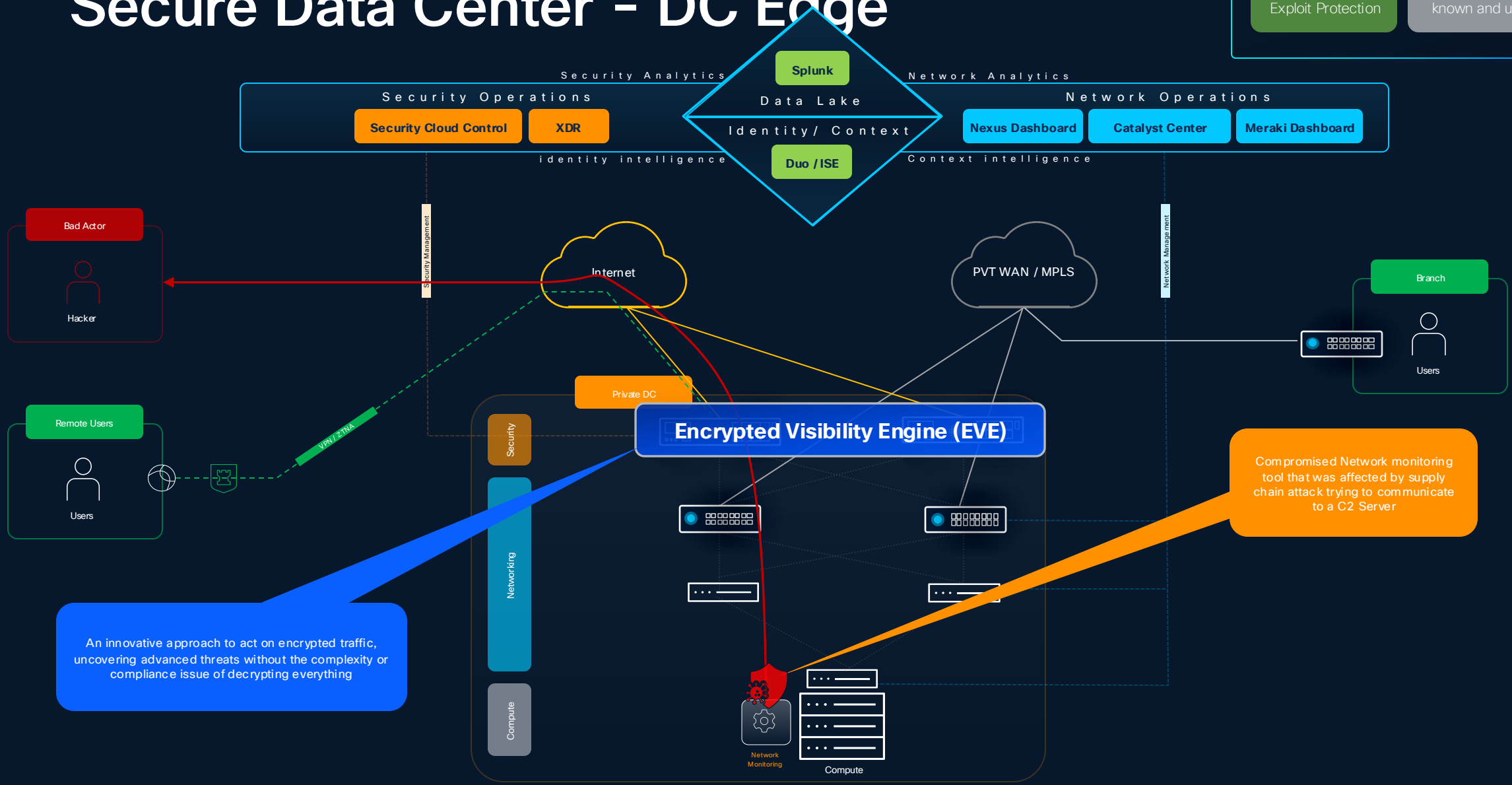
cisco

Secure Data Center – DC Edge

SECURITY OUTCOMES

Threat Detection & Exploit Protection

Detect and Protect against known and unknown threats

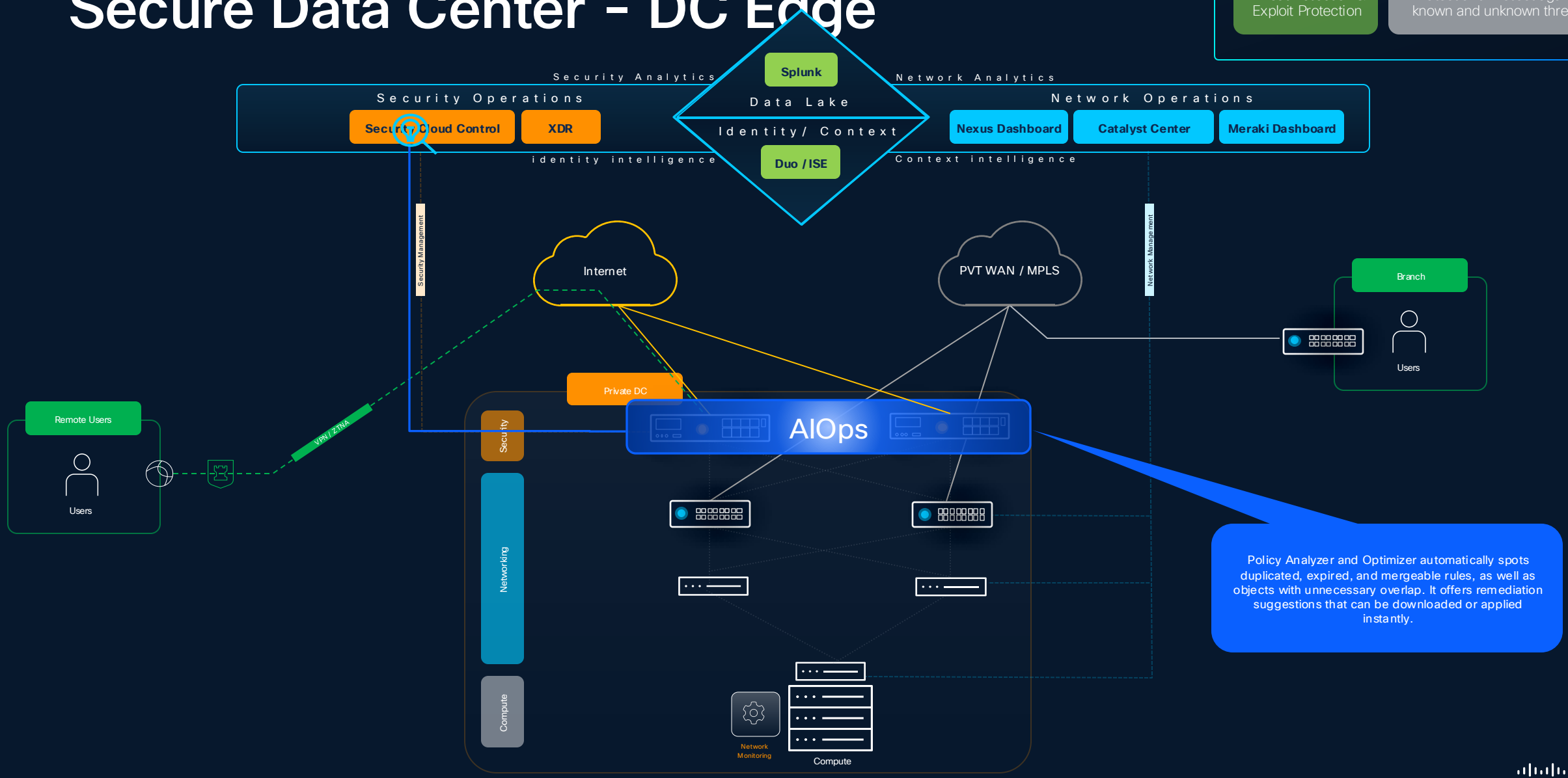


Secure Data Center – DC Edge

SECURITY OUTCOMES

Threat Detection & Exploit Protection

Detect and Protect against known and unknown threats

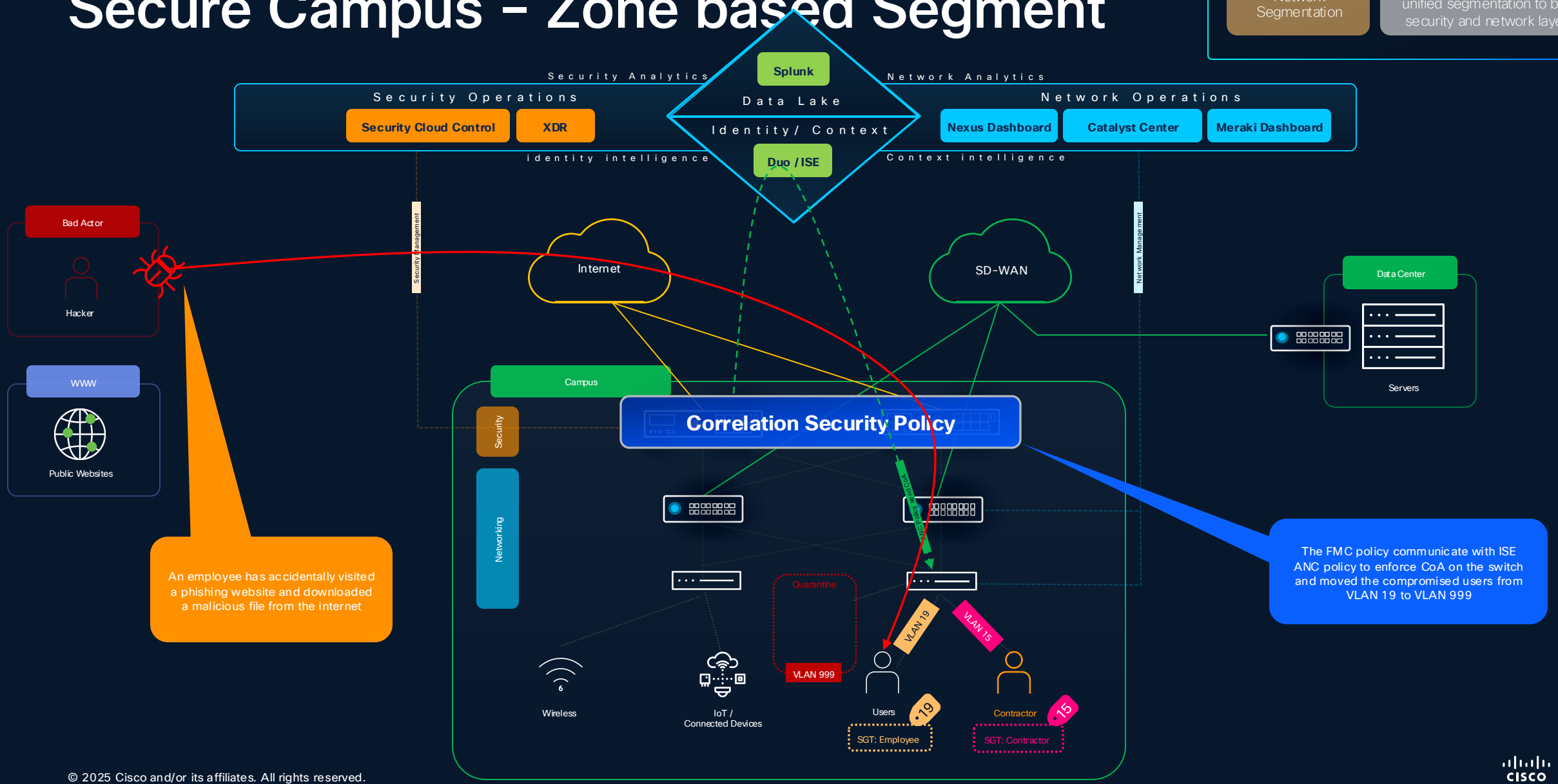


Secure Campus – Zone based Segment

SECURITY OUTCOMES

Network Segmentation

Securely apply context aware unified segmentation to both security and network layers

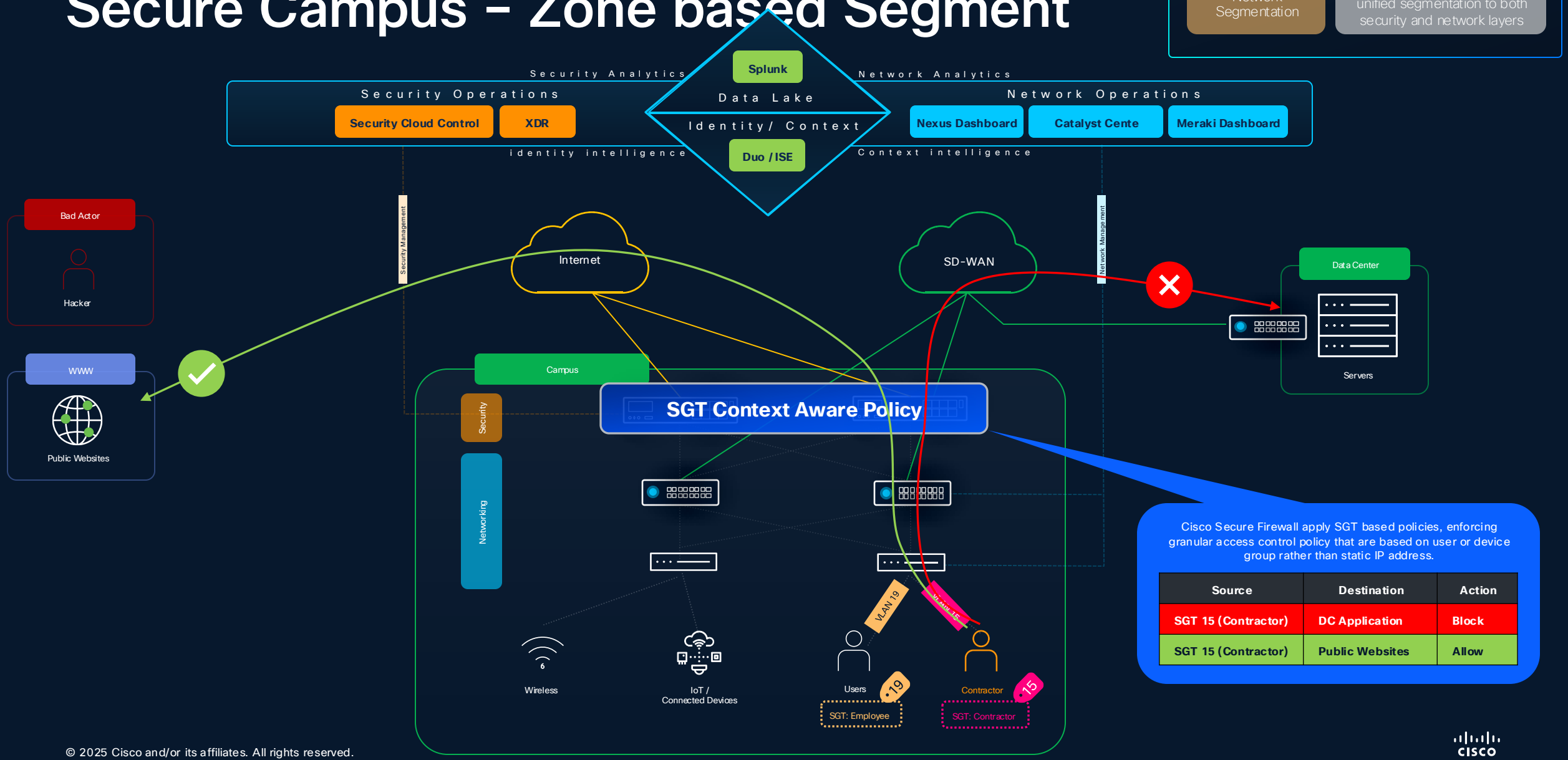


Secure Campus – Zone based Segment

SECURITY OUTCOMES

Network Segmentation

Securely apply context aware unified segmentation to both security and network layers



Cisco Secure Firewall apply SGT based policies, enforcing granular access control policy that are based on user or device group rather than static IP address.

Source	Destination	Action
SGT 15 (Contractor)	DC Application	Block
SGT 15 (Contractor)	Public Websites	Allow

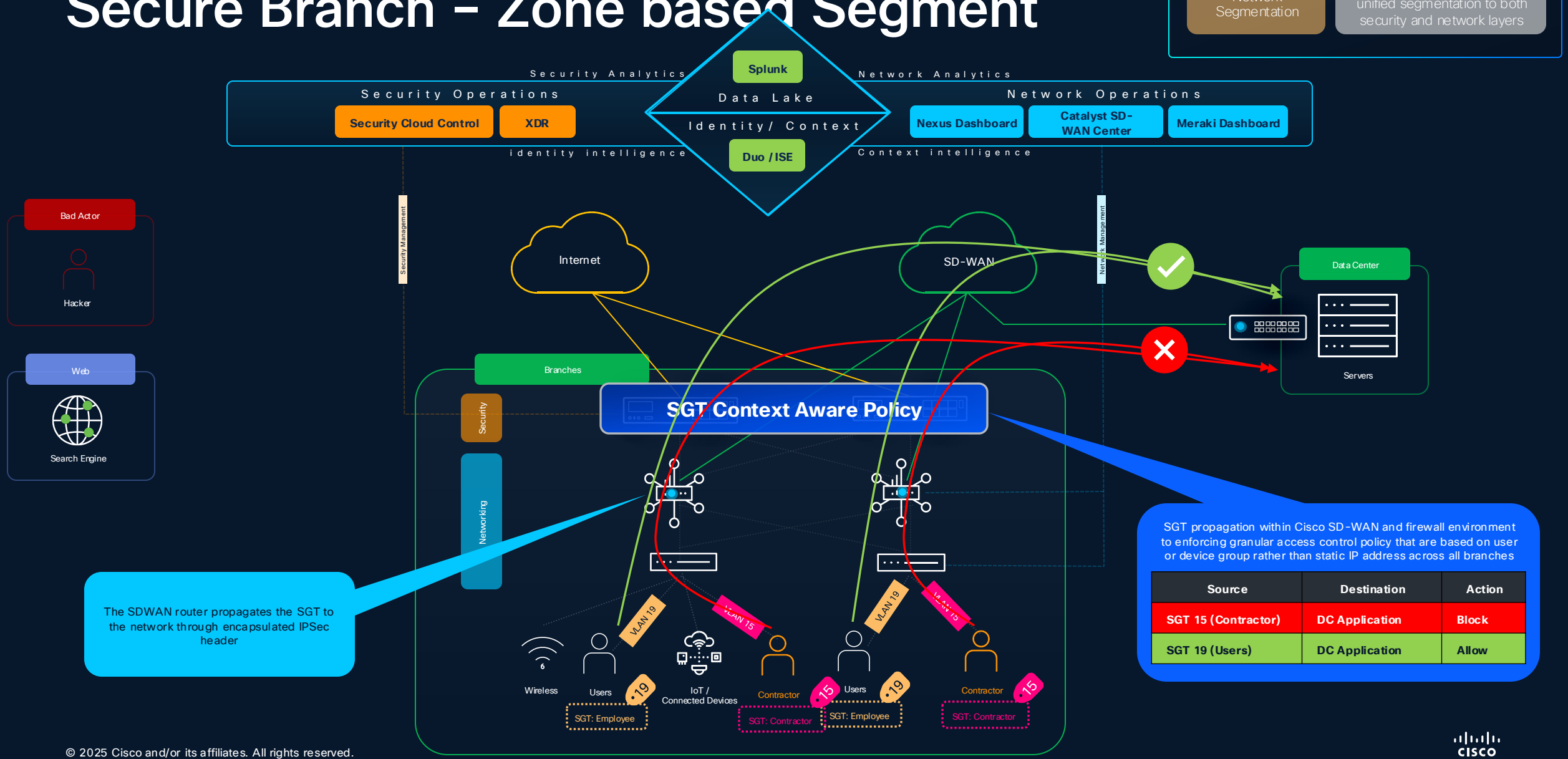
cisco

Secure Branch – Zone based Segment

SECURITY OUTCOMES

Network Segmentation

Securely apply context aware unified segmentation to both security and network layers



The SDWAN router propagates the SGT to the network through encapsulated IPSec header

SGT propagation within Cisco SD-WAN and firewall environment to enforcing granular access control policy that are based on user or device group rather than static IP address across all branches

Source	Destination	Action
SGT 15 (Contractor)	DC Application	Block
SGT 19 (Users)	DC Application	Allow

cisco

Our Firewall has comprehensive capabilities

Superior Threat Protection

Cisco Talos Security Intelligence

Application Control, Custom App Detectors

Intrusion Prevention

Automation, Remediation, & Integration

Malware Protection & Sandboxing

URL Filtering & Categorization

Firewall, Routing, NAT

High Availability & Scalability

VPN/ZTNA

TLS/QUIC Decryption

ML-Driven Encrypted Visibility Engine

Identity & Attribute Based Access Control

Configuration and Analytics Console

Cisco Firewall – Hardware Innovations

A high-performing firewall for every use case

Cisco Secure Firewall family performance at-a-Glance

PQC Ready Hardware

Branch		Campus	Data center		Cloud
NEW 				NEW 	
200 Series	**1200 Series**	**3100 Series**	**4200 Series**	**6100 Series**	**Public/Private**
2 Models	5 Models	5 Models	3 Models	2 Models	20+ cloud variants
Firewalling+IPS 1.5-2.5 Gbps	Firewalling+IPS 6-24 Gbps	Firewalling+IPS 10-45 Gbps	Firewalling+IPS 71-149 Gbps	Firewalling+IPS 280-400 Gbps	
IPSec VPN 1-2 Gbps	IPSec VPN 5-22 Gbps	IPSec VPN 5.5-39.4 Gbps	IPSec VPN 51-148 Gbps	IPSec VPN 280-350 Gbps	
TLS Decryption 0.75-1.25 Gbps	TLS Decryption 1-4.1 Gbps	TLS Decryption 3.2-11.5 Gbps	TLS Decryption 20-45 Gbps	TLS Decryption 90-120 Gbps	

Secure Firewall 220

At-a-glance

FTD 10.0

ASA 9.24

PQC Ready

- One Model - 220
- Flexibility to address all modern NGFW use cases
  - Network/Security SoC with 4 ARM cores design
- SoC-embedded accelerators for encryption and traffic processing
- Up to 1.5Gbps (1024B) for NGFW traffic profiles
- Up to 1 Gbps for IPsec VPN, and up to 0.5 Gbps for TLS 1.2/1.3

AVAILABLE DEC 2025

Cisco Secure Firewall 6100 Series

FTD 10.0+

ASA 9.24+

PQC Ready

- Flexibility to address all modern NGFW use cases
  - Two CPUs with 192-256 physical cores (384-512 with HT)
  - 12x 1/10/25/50GE (SFP56) and 4x 40/100/200GE (QSFP56) interfaces built in plus two Network Module bays
  - 1.5-2.3TB of RAM
  - Two NVMe slots, up to 7.2TB of RAID1 protected space
  - HVAC/HVDC/DC redundant PS
- Advanced FPGAs and one or two dedicated cryptographic hardware accelerators
- Clustering support on all models, up to 16x nodes
- Up to 400 Gbps for NGFW traffic profiles
  - up to 140 Gbps with 50% of TLS 1.2/1.3 mix
  - up to 350 Gbps for IPsec traffic

AVAILABLE DEC 2025

cisco

Introducing
New Firewall Management Center appliance

FMC x800 Series

Based out of UCS M8 Server

Manage up to 1500 FTDs
50% boost over 4700

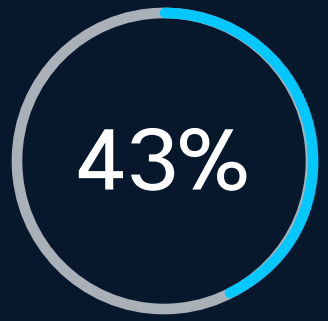
Improved event retention and event rate
2X vs FMC4700

Extended Lifecyle
Expected Sellable life till CY2030 and beyond

AVAILABLE Jan 2026

Firewall 10.0 Enhancements & Innovations

Release Adoption



Running Threat Defense Code
0 - 2 years

Running Threat Defense Code
older than 3 years

Running Threat Defense Code
older than 4 years

Low adoption prevents you from benefiting form the latest features and increased risk of potential quality and security issues.

Encrypted Visibility Engine
Simplified configuration of AI/ML-driven detection of apps and malware in encrypted traffic, without decrypting

Splunk Integration for Syslog
Seamless integration empowers administrators to effectively monitor and respond to potential threats in the network.

SnortML
Deep neural network engine to detect exploits, trained on malicious and benign traffic

Firewall

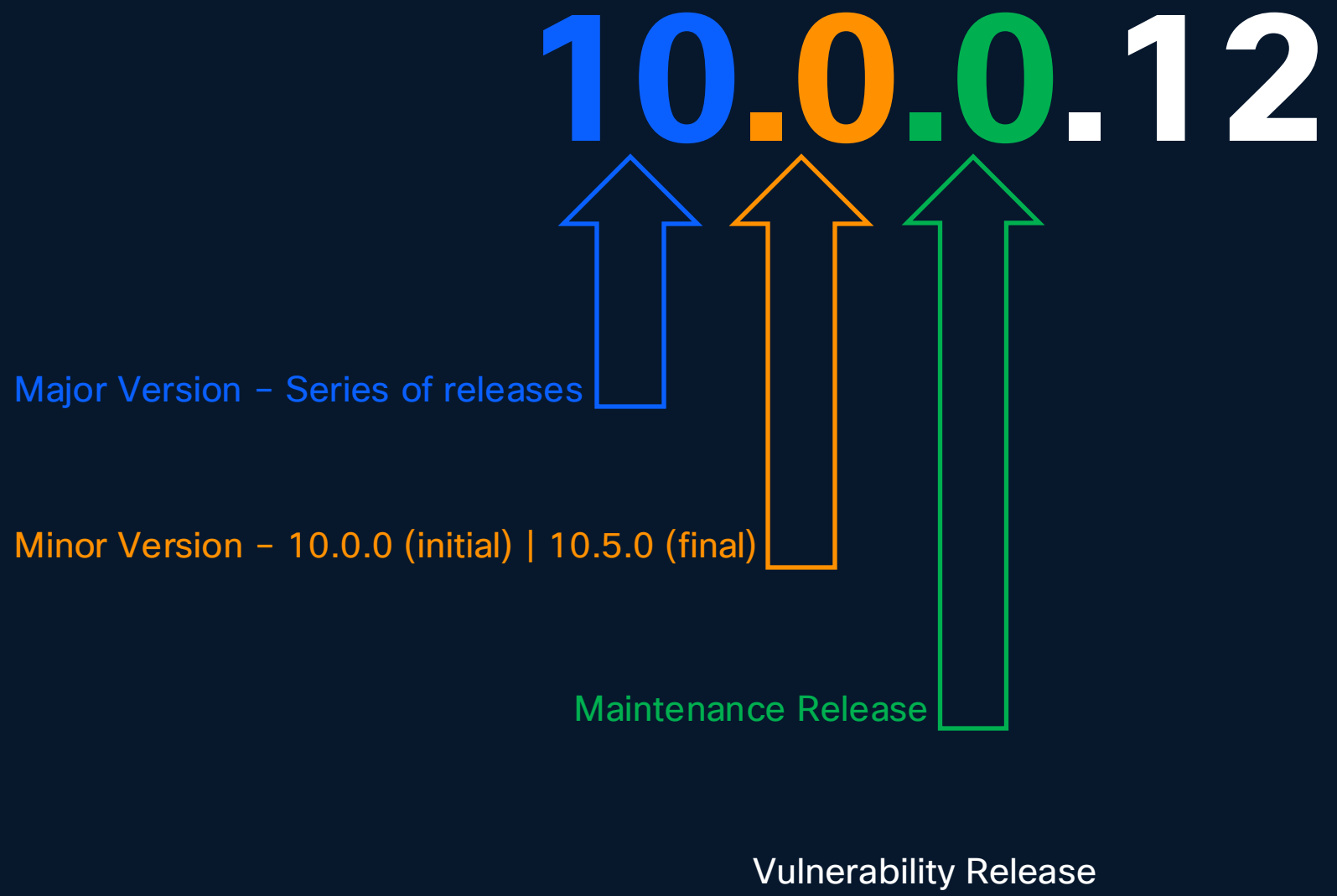
Simplified Decryption Policy Creation
Ease of use with the focus on **what** the policy should do, while less focus **how** to generate the policy.

Firewall Upgrade Hardening
Simple, swift, & error-free upgrades with less than 10-clicks from anywhere in the UI to a fully upgraded environment.

Cisco Security Intelligence
Associate an identity source with identity intelligence like Cisco Identity Intelligence (CII)

New Firewall Release Numbering

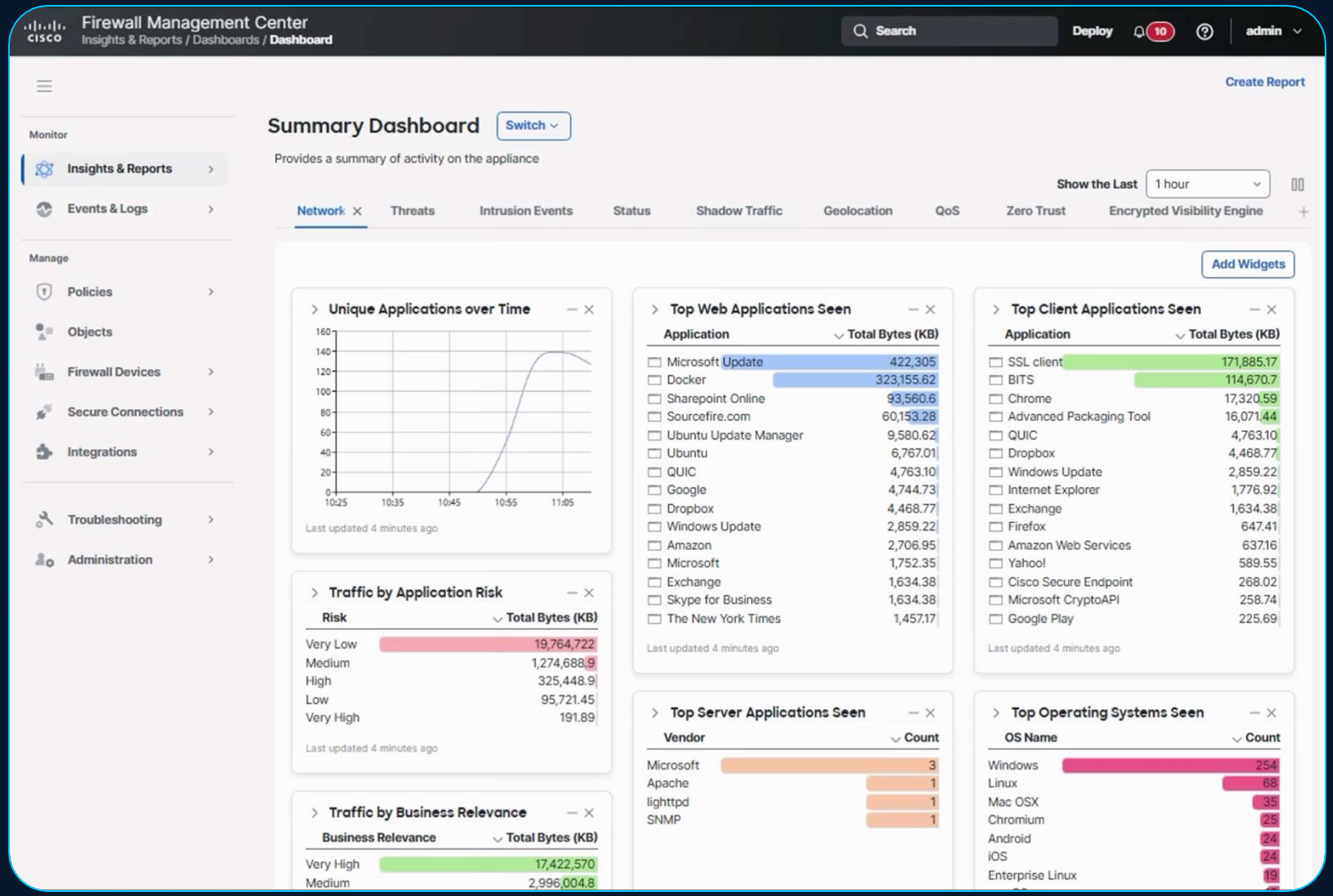
- Simplified release structure with consistent support and certification across all releases
- Each major release is now broken into two minor releases (eg. 10.0.0, 10.5.0)
- Example:
  - 10 – Major version that is specified by the first digit and indicates a series of releases
  - 10.0 – Initial minor version delivering new features/improvements
  - 10.5 – Final minor version delivering new features/improvements. Submitted for government certification.
  - 10.0.2 – Maintenance version that provides bug fixes and vulnerability protection on top of major version.
  - 10.5.2 – Maintenance version that provides bug fixes and vulnerability protection for the final minor version only and for all 10.x.x.x customers to move to for sustaining support.
  - 10.5.5.2 – Vulnerability Release based on the 10.5.5 Maintenance release.



FMC UI Simplification

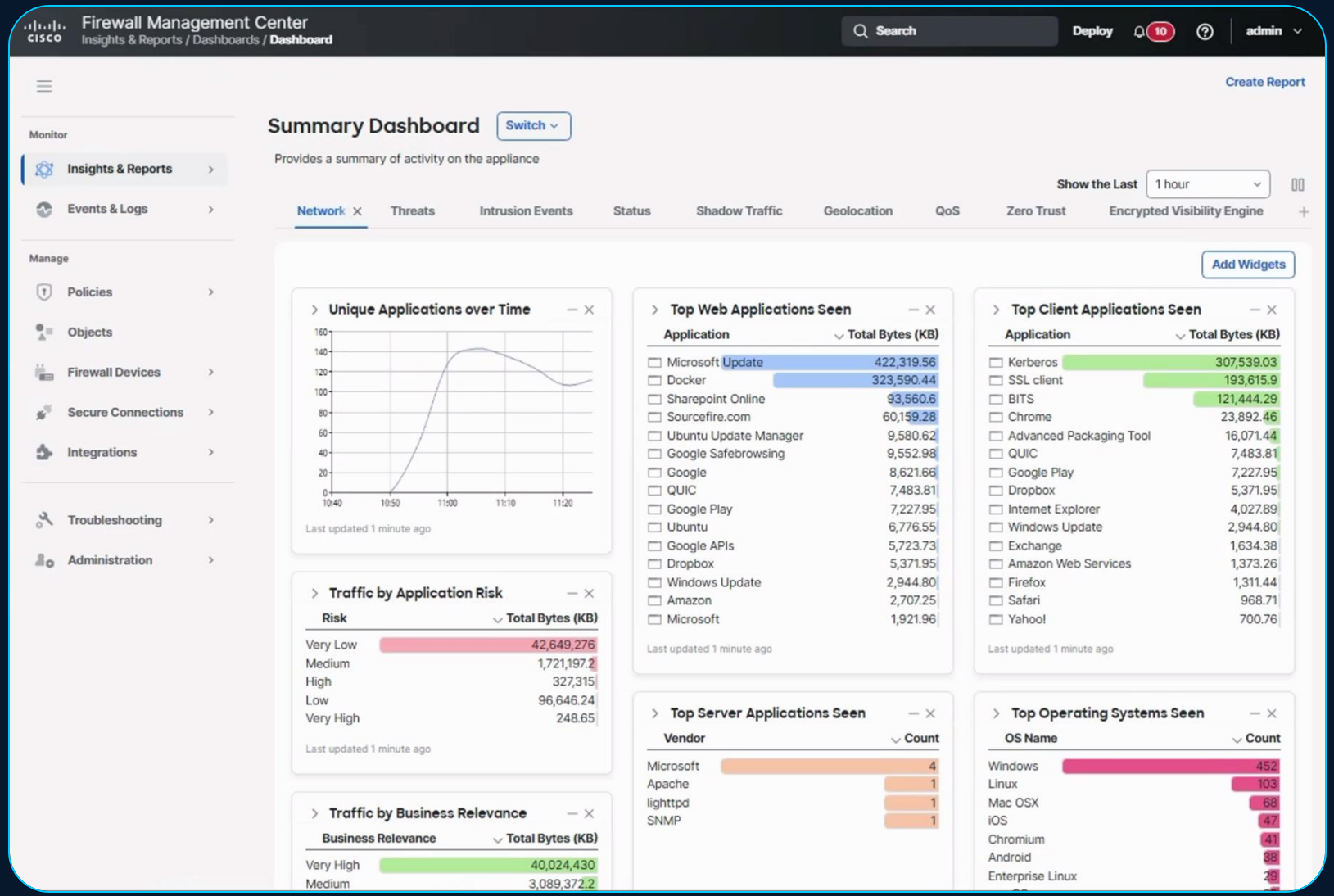
New Global Navigation

- New Navigation menu aligning to Security Cloud Control.
- Navigation Changes:
  1. Overview → Insights & Reports
  2. Analysis → Events & Logs
  3. New Secure Connection" menu.
  4. New Troubleshooting menu
  5. System menu moved from top-menu to left navigation - Administration
  6. New “Find in Menu” button in menu
  7. On Screen Assistance → Page-level Help
- Fully Customizable



Splunk Configuration on FMC

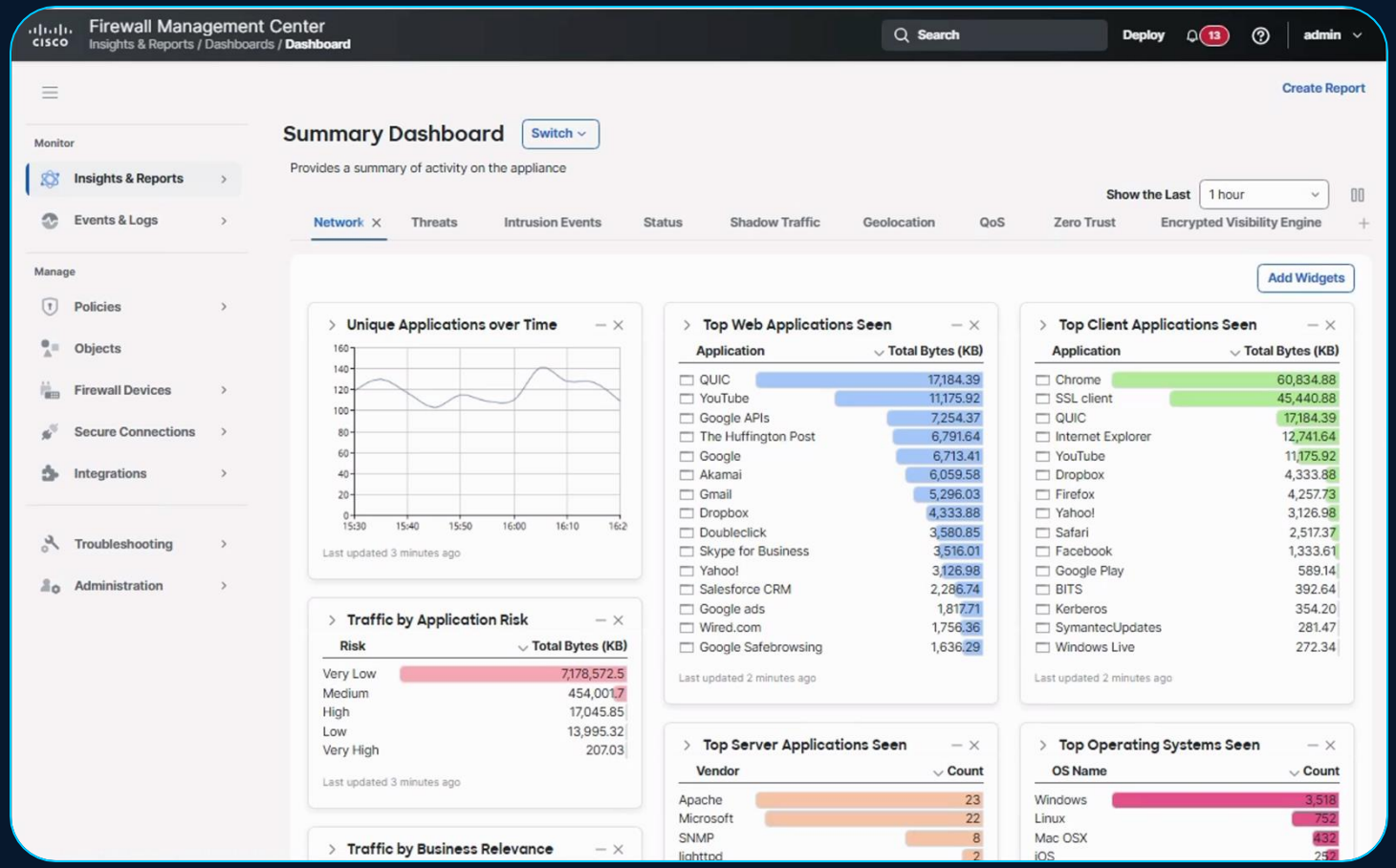
- Configurationis created at Integration > Splunk page on FMC UI.
- Each profile has 5 configuration sections:
  1. Destination
  2. Event
  3. Source
  4. Client certificates
  5. Summary
- Splunk profiles can be created targeting the same device(s) and are additive.
- Profiles are limited to leaf domains.

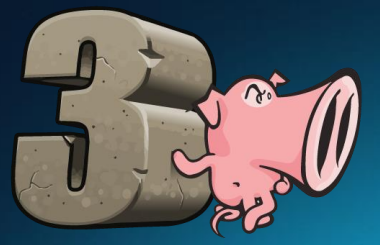


Identity Updates

What is Dynamic Firewall?

- The Dynamic Firewall feature helps associate an identity source (ISE or pxGrid Cloud) with identity intelligence like Cisco Identity Intelligence (CII) for user trust scores.
- Cisco Identity Intelligence (CII) – Collects user information from different identity sources (Duo or Entra ID) and classifies user patterns into five trust levels:
    1. Trusted
    2. Favorable
    3. Neutral
    4. Questionable
    5. Untrusted
- FMC can get the Untrusted and Questionable levels from CII and apply it to logins received from ISE or pxGrid Cloud.

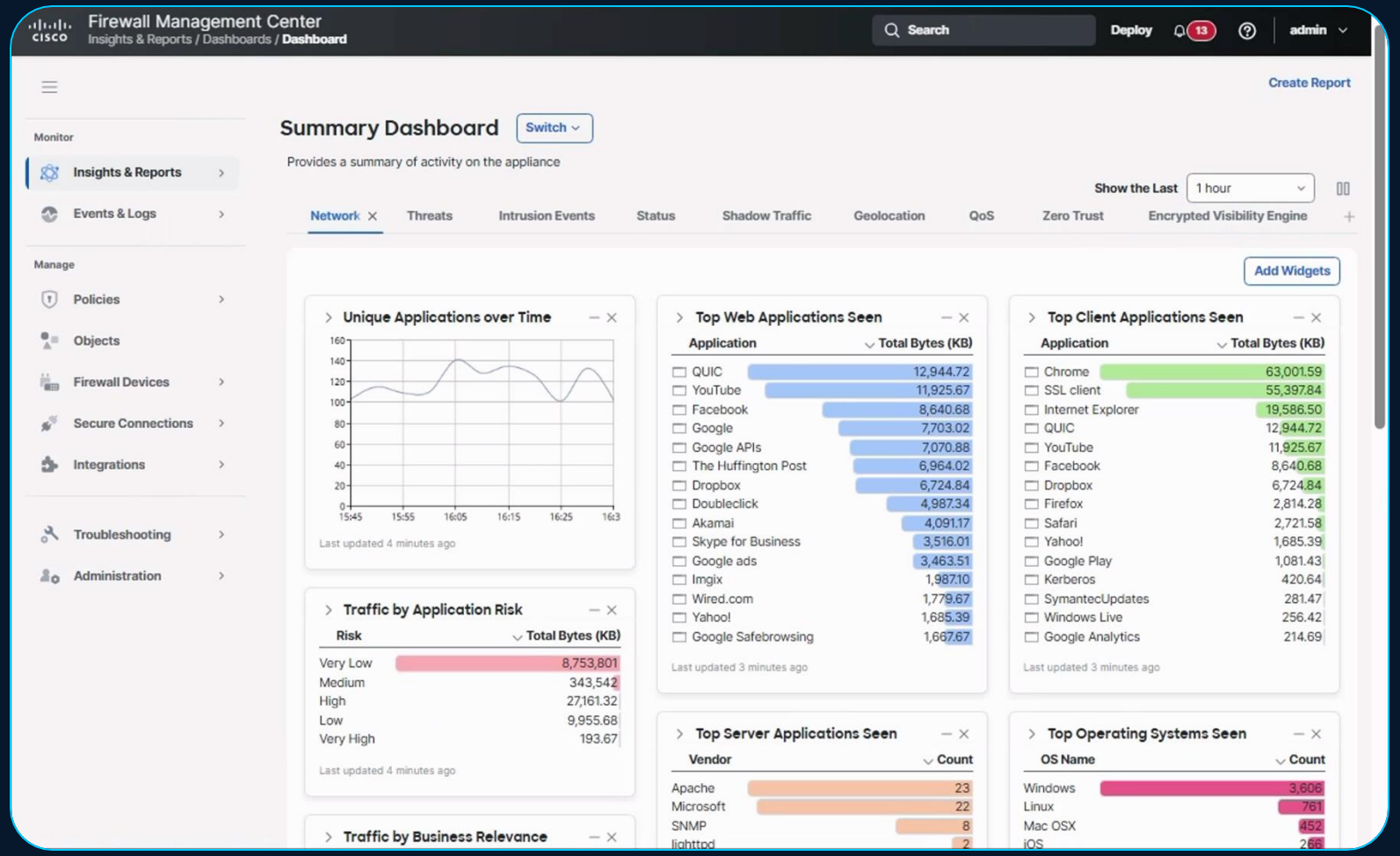




Threat Updates

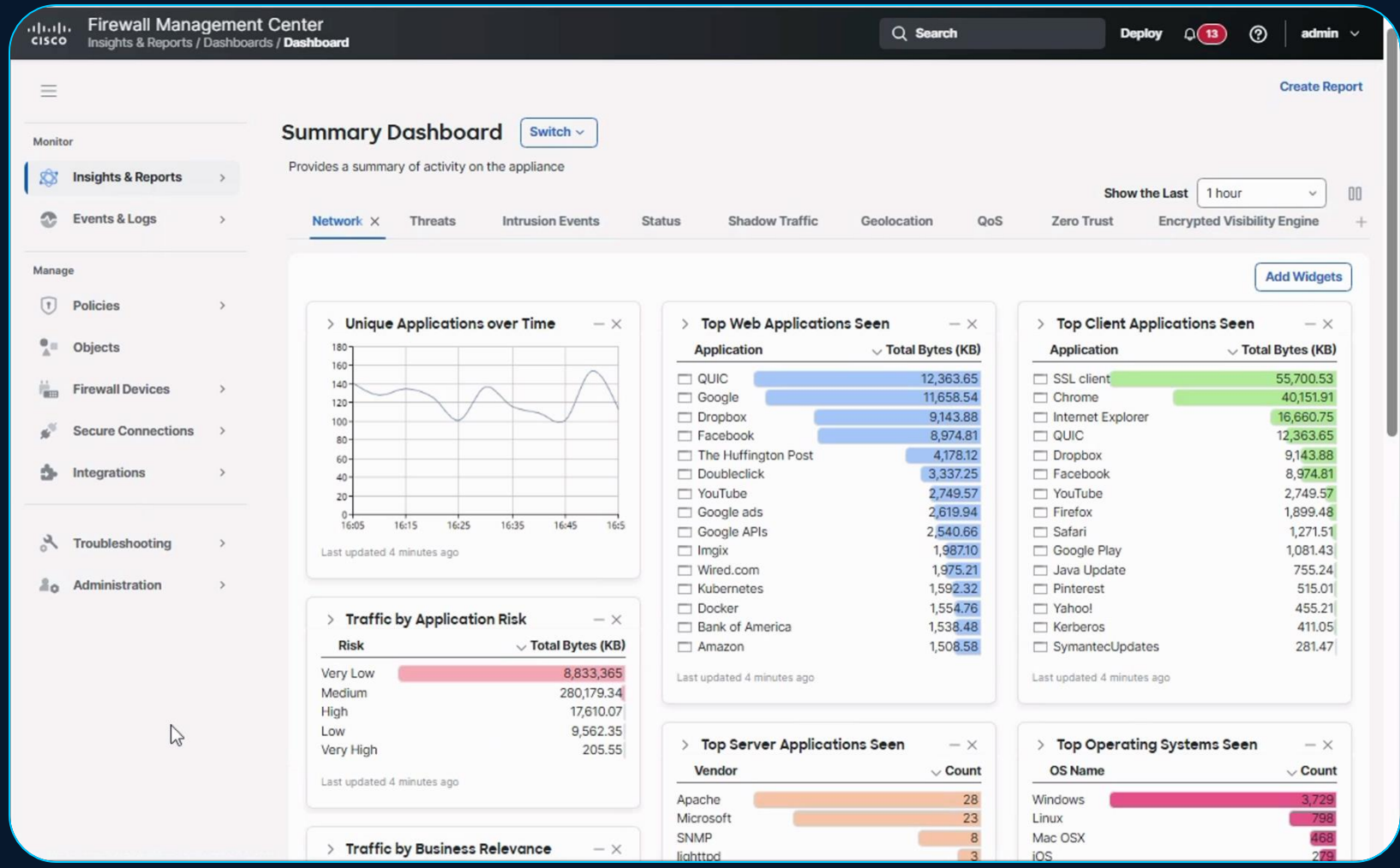
Simplifying EVE

- New Dashboard/Widgets
- Encrypted Visibility Engine (EVE) configuration moved from Advanced Settings to the main Access Control Policy page.
- Introduction of two modes: Monitor and Protect.
  - Protect mode, EVE monitors and blocks malicious connections based on the Block Threshold Level configured.
- 'Use EVE for Application Detection' option is no longer available; If EVE is enabled, it is used for client application detection.
- Simplified Block Threshold Configuration
  - The previous five-level threat score system has been replaced with just two levels – High and Very High.



Simplifying the Decryption Policy

- Focus on what the policy should do, and not how to generate the policy.
- Option for Selective Decryption.
- Enhanced certificate management directly from the Decryption Policy creation page.
- Two policy modes:
  - Standard – Policies created and modified using the new interface. Default policy mode in 10.0
  - Legacy – Policies created and modified using the editor in 7.7 or lower.
- QUIC Decryption no longer experimental.



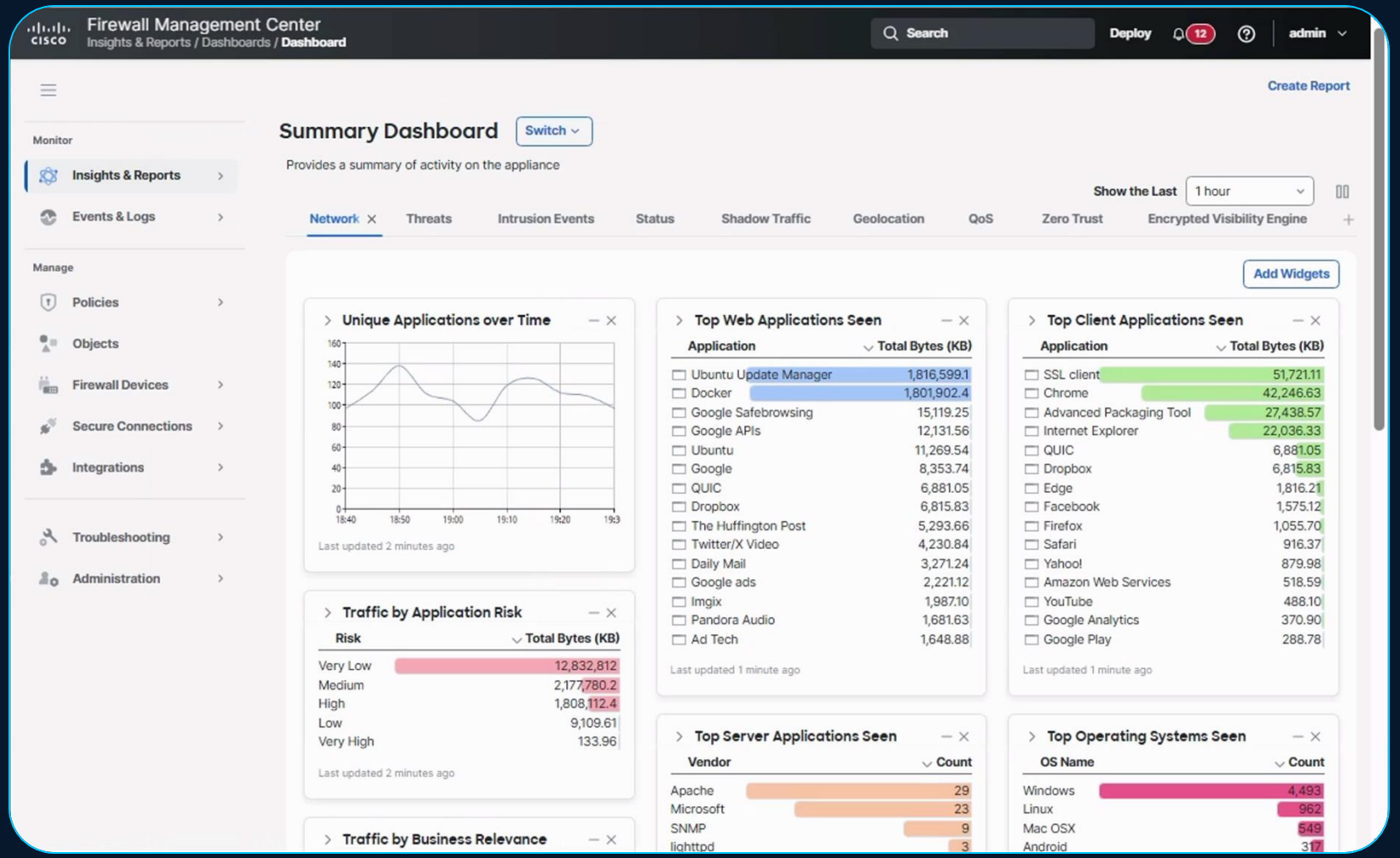
SnortML Update

- SnortML – Neural network-based exploit detector for Snort 3.
- In release 7.6, SnortML was introduced and provided support for SQL Injection HTTP server attack type.
- SnortML now supports HTTP command injection as well, with more coverage coming soon.
- Under-the-hood enhancements have improved performance and latency.

SD-WAN & VPN Enhancements

SGT Across VTI-based Tunnels

- Enable consistent and granular security policy enforcement and micro-segmentation across distributed network environments.
- Maintain identity-based security policies and micro-segmentation consistently across distributed sites.
- Goal: Extend identity-based segmentation and security policies seamlessly from the branch to the data center and cloud environments.



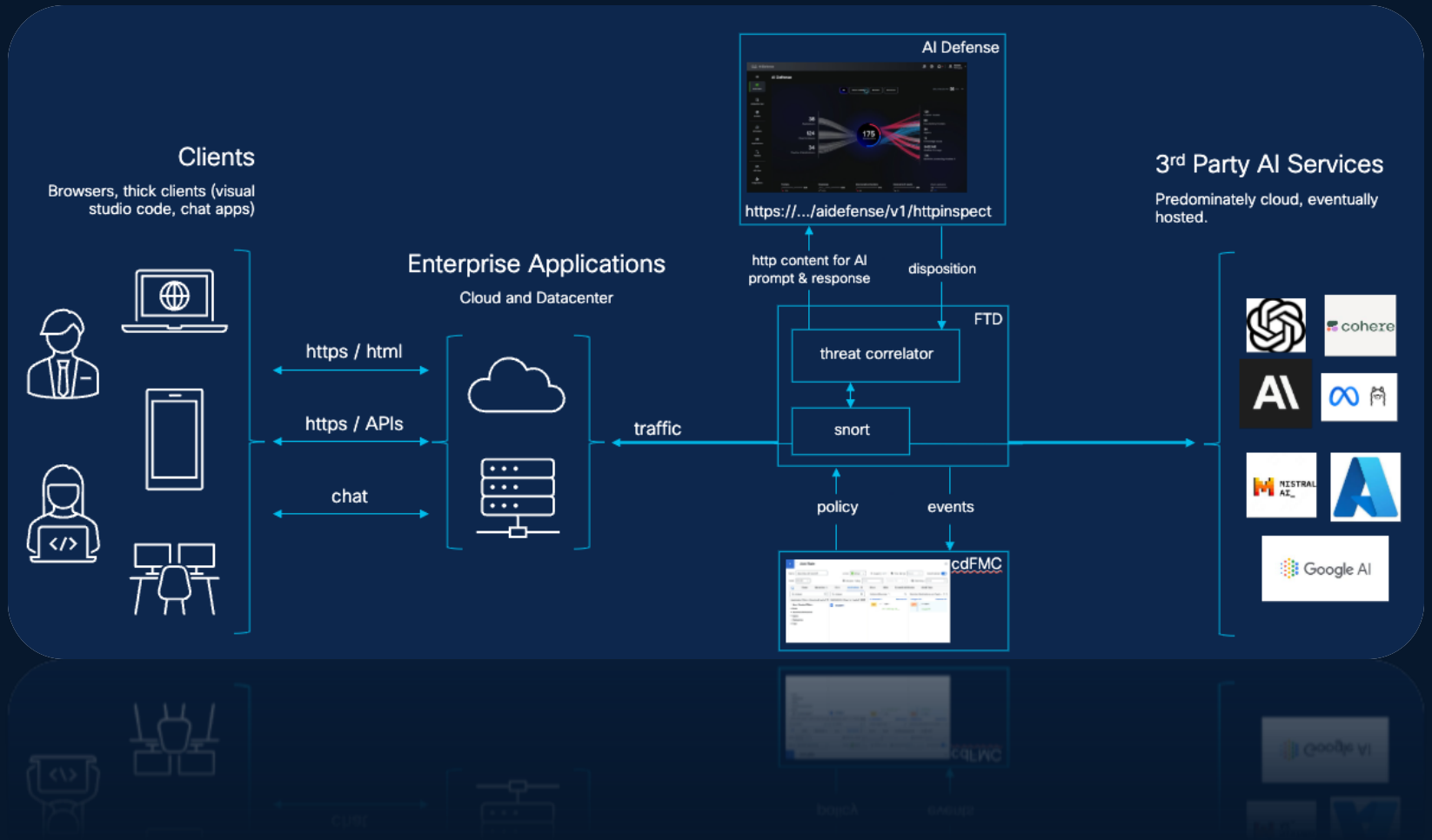
AI Security

Coming Soon

Firewall & AI Defense (cdFMC)

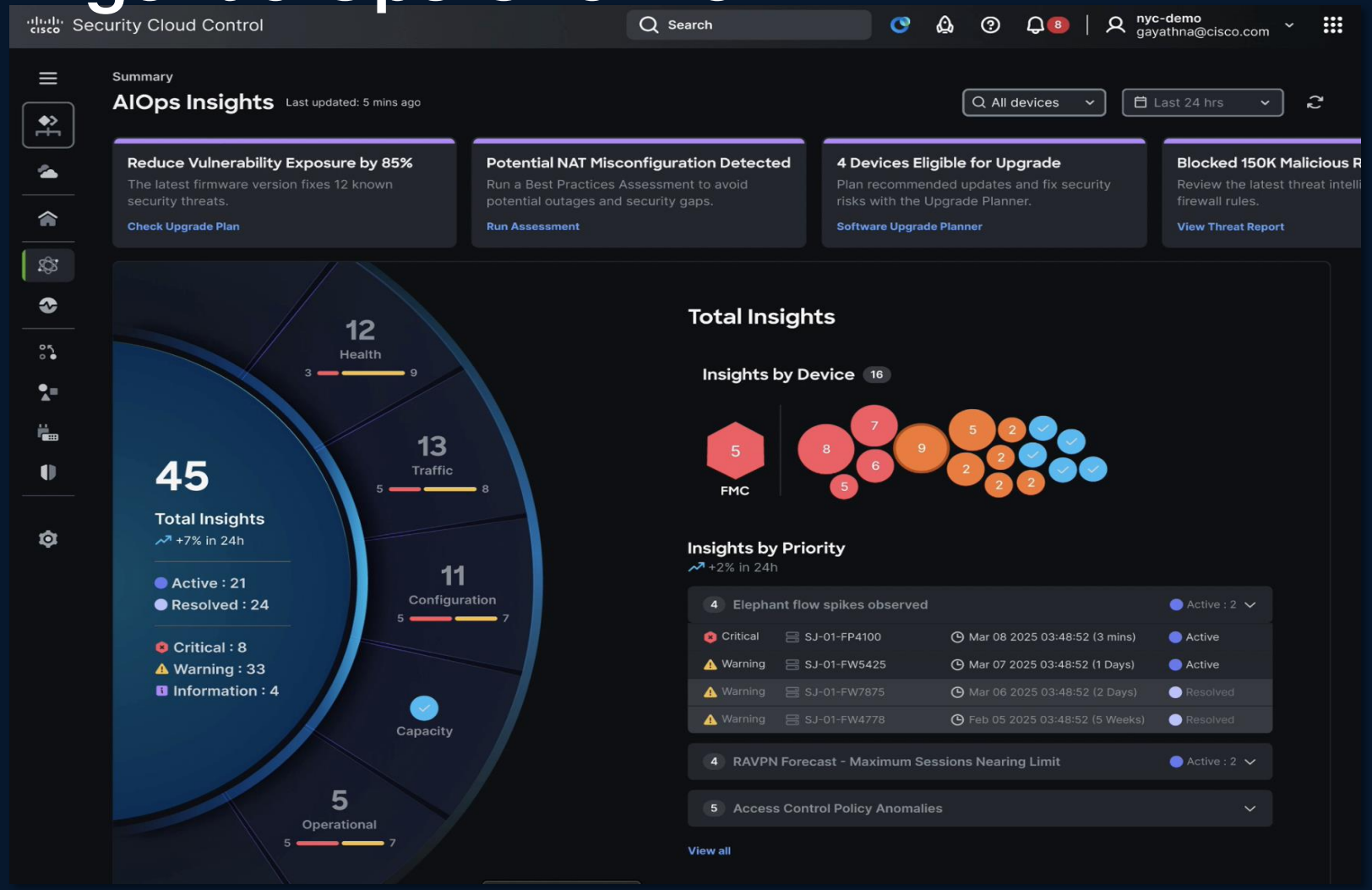
Gen AI Protection

- Intercept and Evaluate prompts between enterprise applications to 3rd party AI Services
- Initially managed from Security Cloud Control
- Phase 2 will bring AI Defense Integration to FMC – 10.5
- Recruiting motivated customers for feedback and testing now!



Operational Efficiency

Agentic Ops Overview



- Helps shift the paradigm from being reactive to proactive.
- Automatically triages and prioritizes issues based on risk, highlighting what matters most for the customers.
- Accelerates resolution by reducing both Mean Time to Detect (MTTD) and Mean Time to Resolve (MTTR).

AgenticOps for Firewall

Configuration Insights

- Policy Analyzer and Optimizer
- Best Practice Recommendations
- Feature Adoption

Traffic and Capacity Insights

- Elephant Flow detection and remediation
- RAVPN Forecast - Maximum Sessions Nearing Limit

Operational Insights

- Software Upgrade Planner
- Renewal Upgrade Planner
- Internet & Application outage visibility

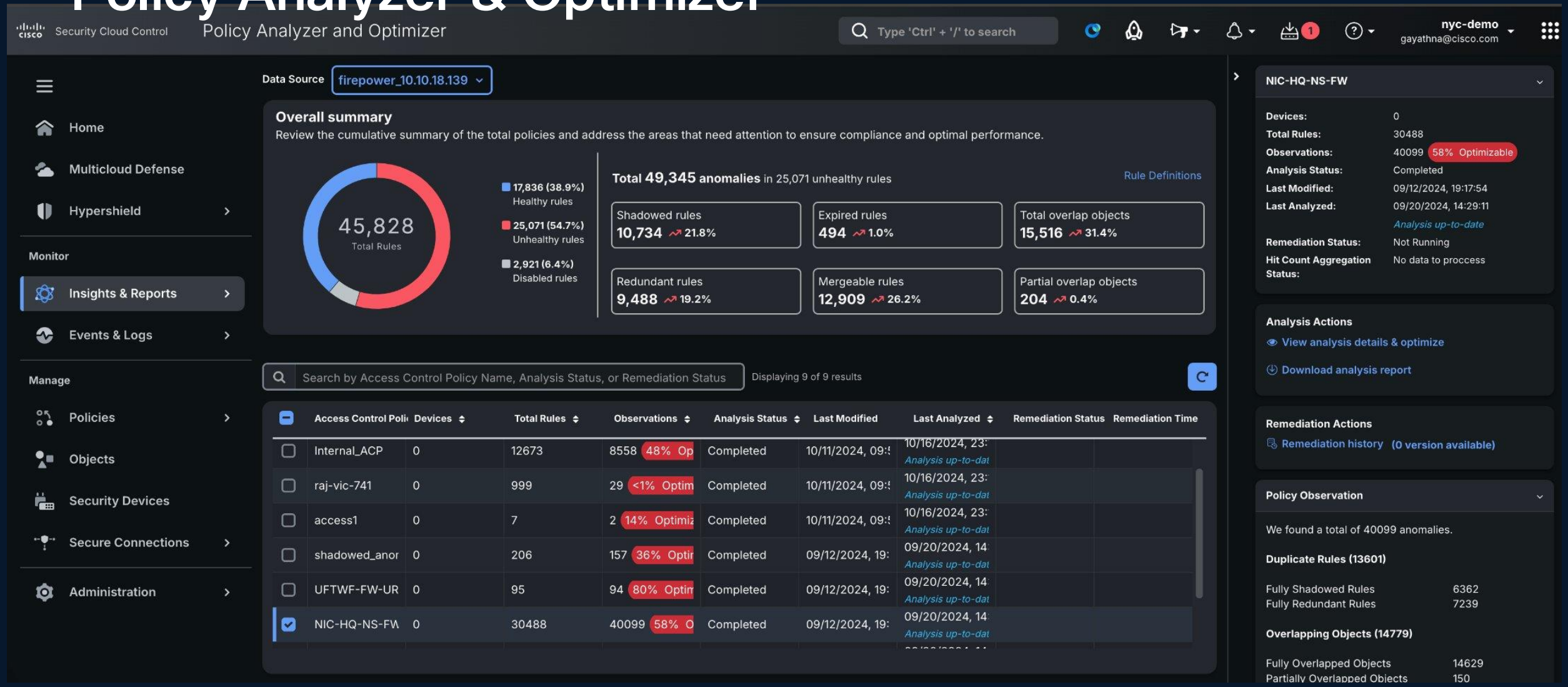
Security Insights

Visibility into User risks with CII Integration

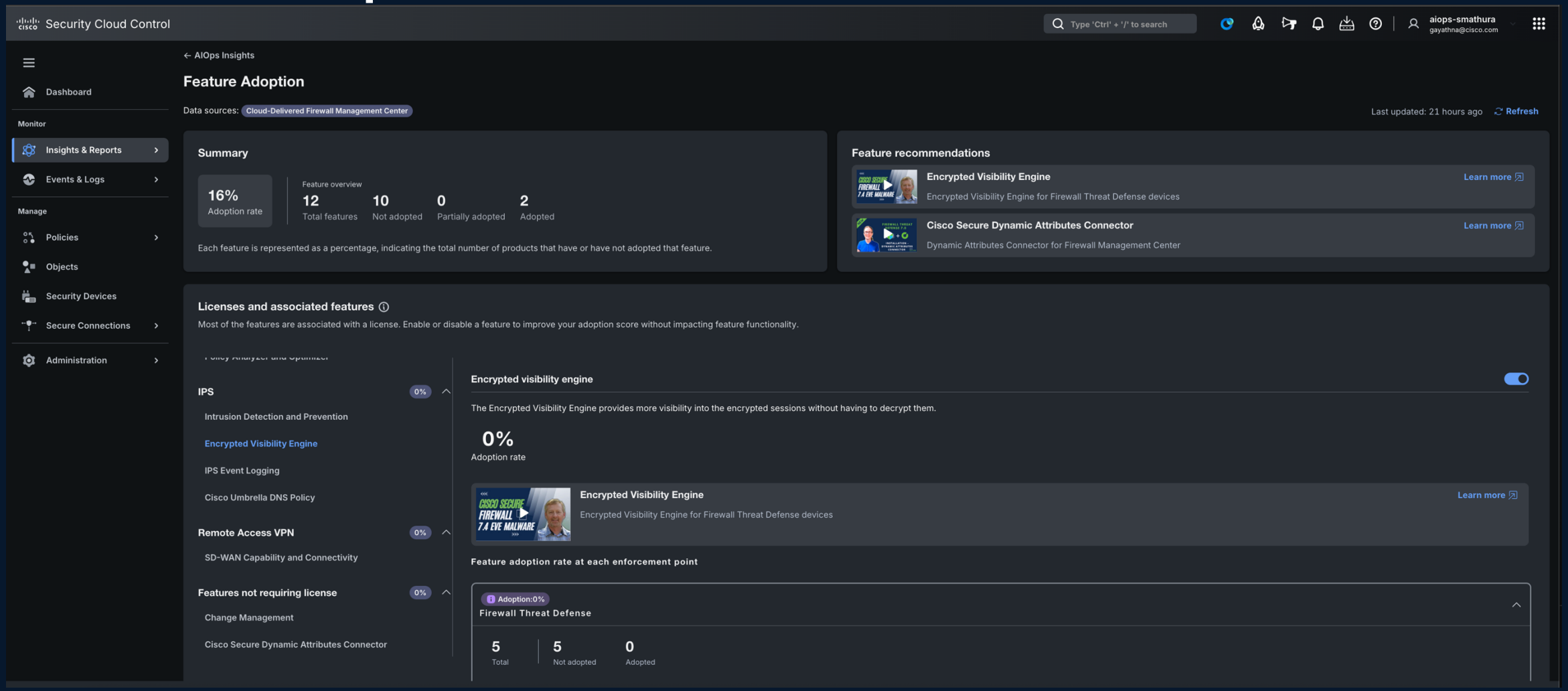
Agent Squad

Workforce as a Service (eg : Configuration & Troubleshooting support for VPN)
Self -healing Remediations

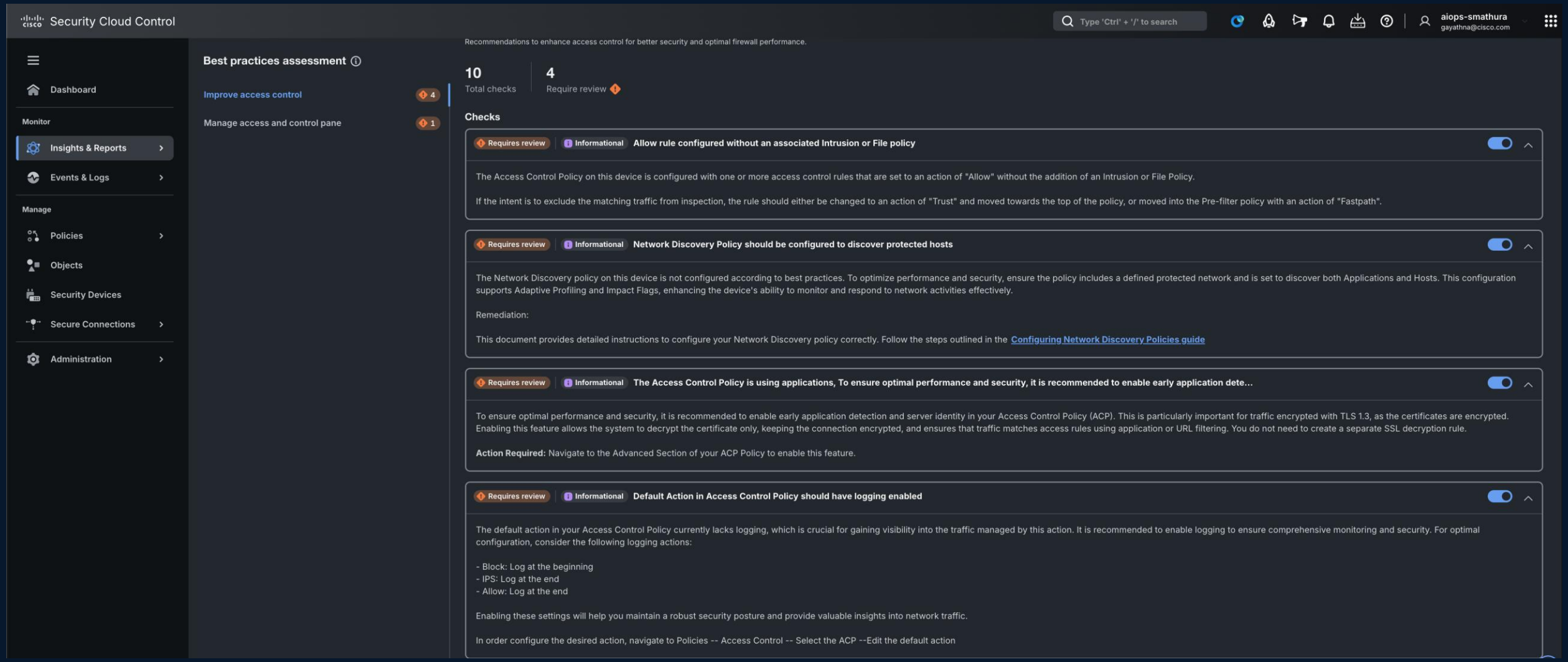
Policy Analyzer & Optimizer



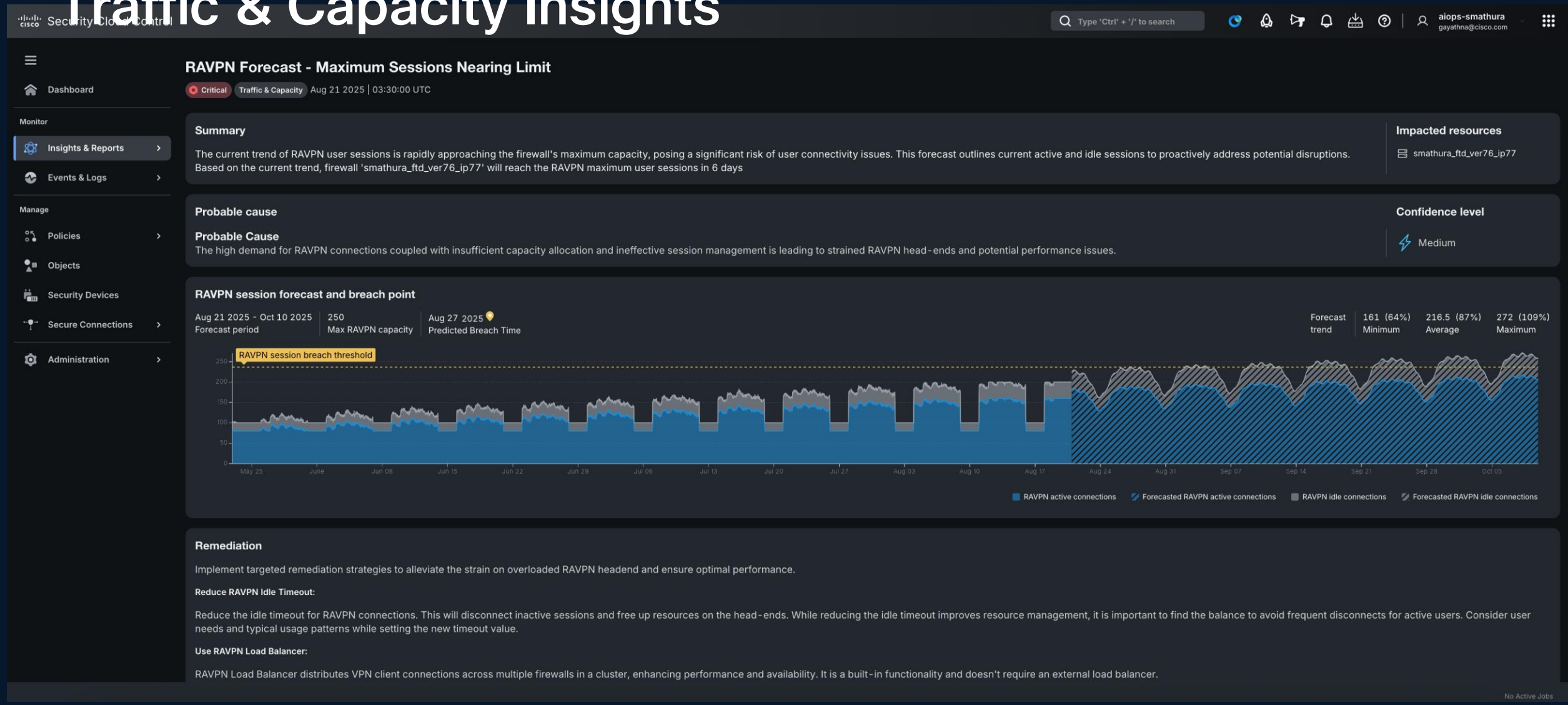
Feature adoption



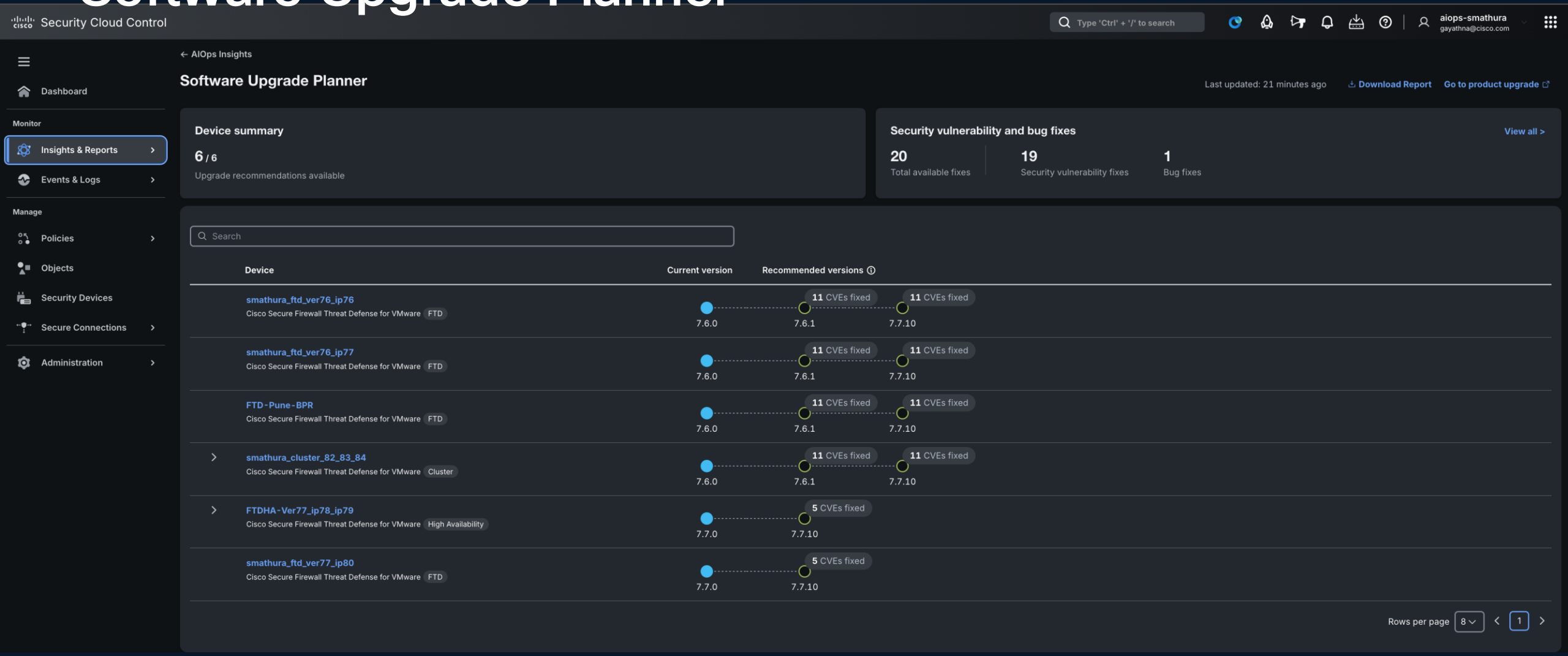
Best Practice Recommendations



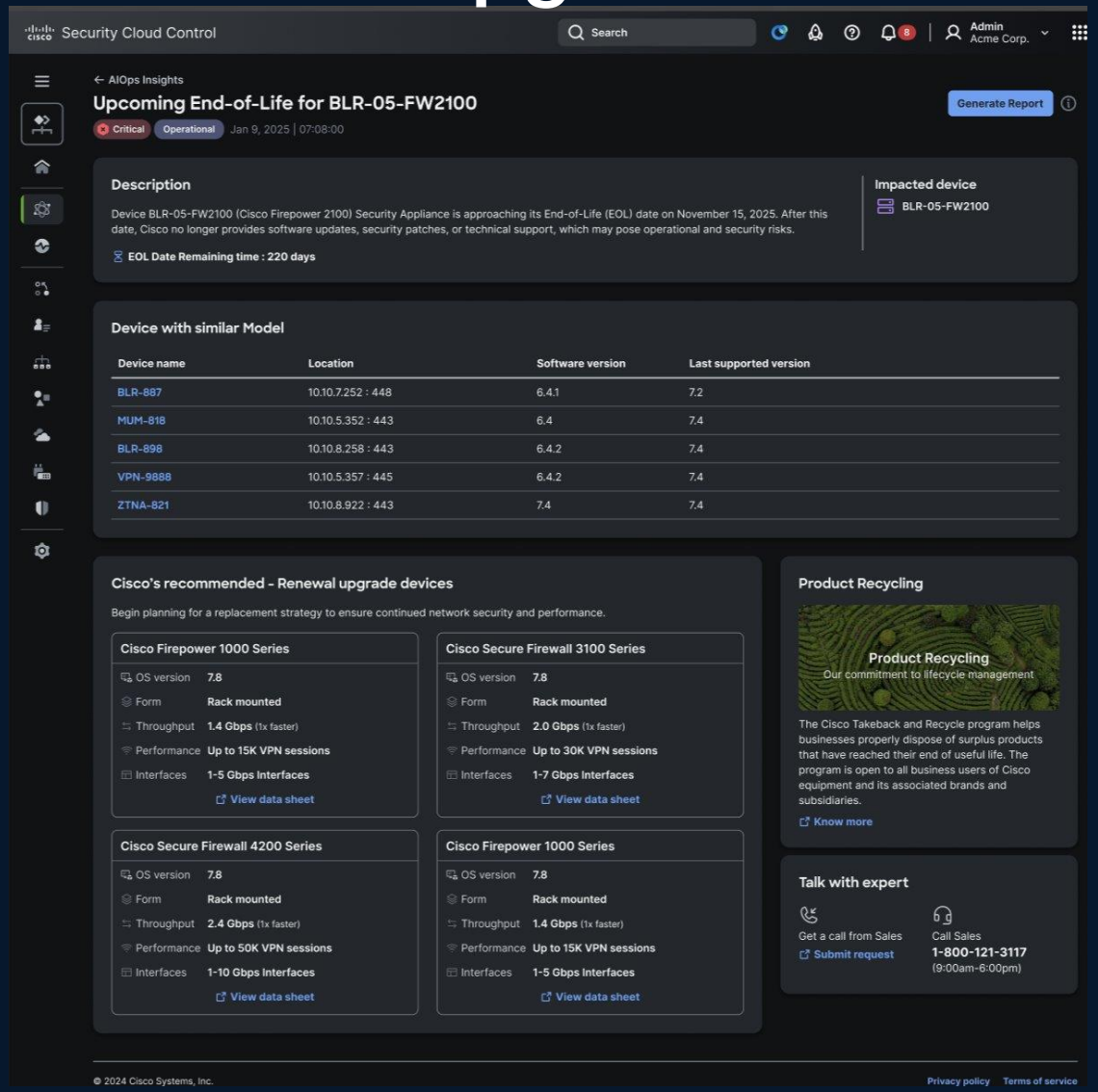
Traffic & Capacity Insights



Software Upgrade Planner



Renewal Upgrade Planner



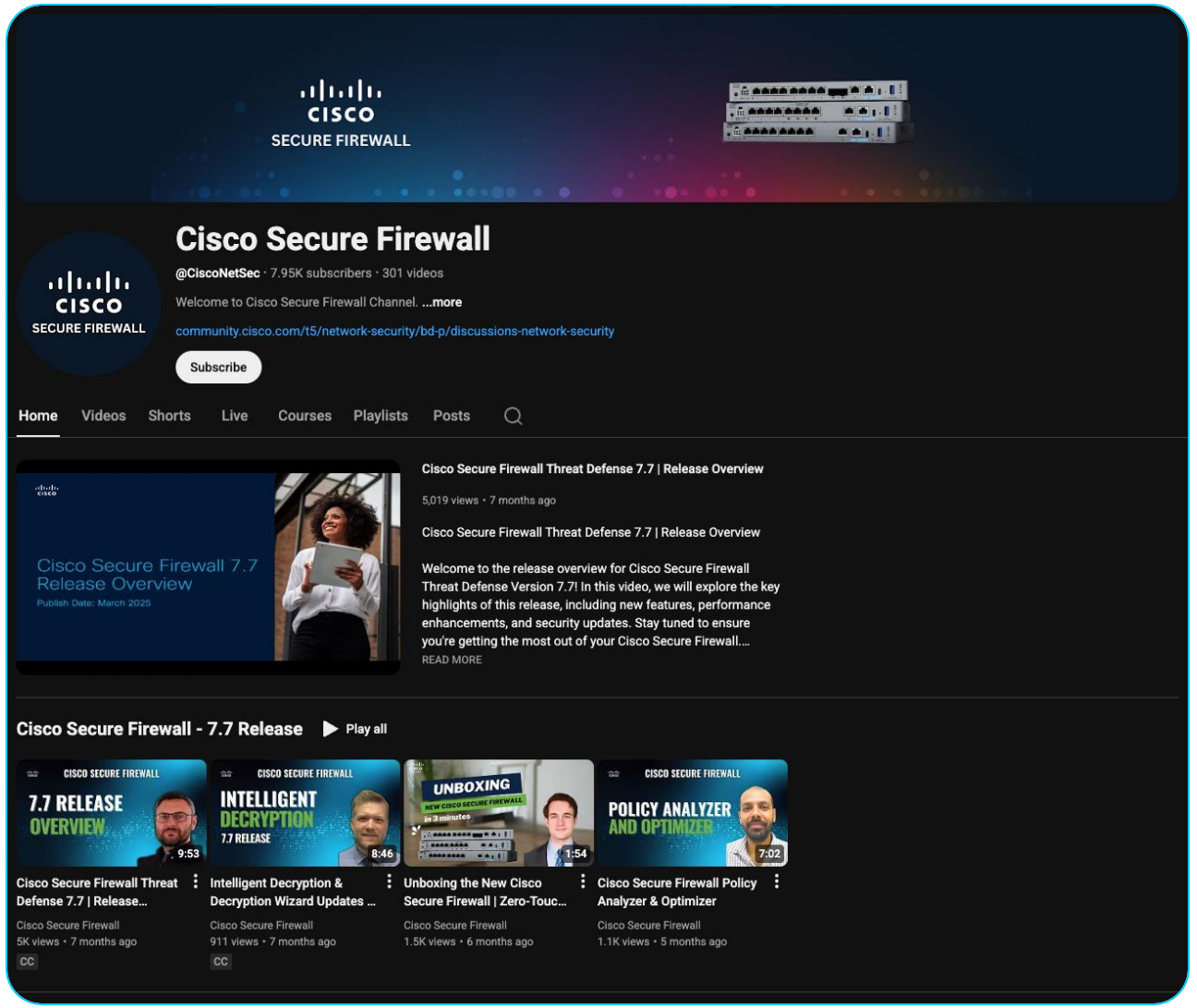
- List ASAs and FTDs reaching End of Life (EOL) in the tenant.
- Recommends FTD models to renew/refresh with based on newer models released.
- Provides quick access to data sheets & release notes for further details on the specification.
- In product notifications and reports about EOL available for customers

Resources

Secure Firewall YouTube Channel

- Latest demos and tutorials
- Includes multiple playlists
  - New features
  - Troubleshooting tips
  - How-to guides
- Along with 100s of other videos highlighting feature deep dive and best practices

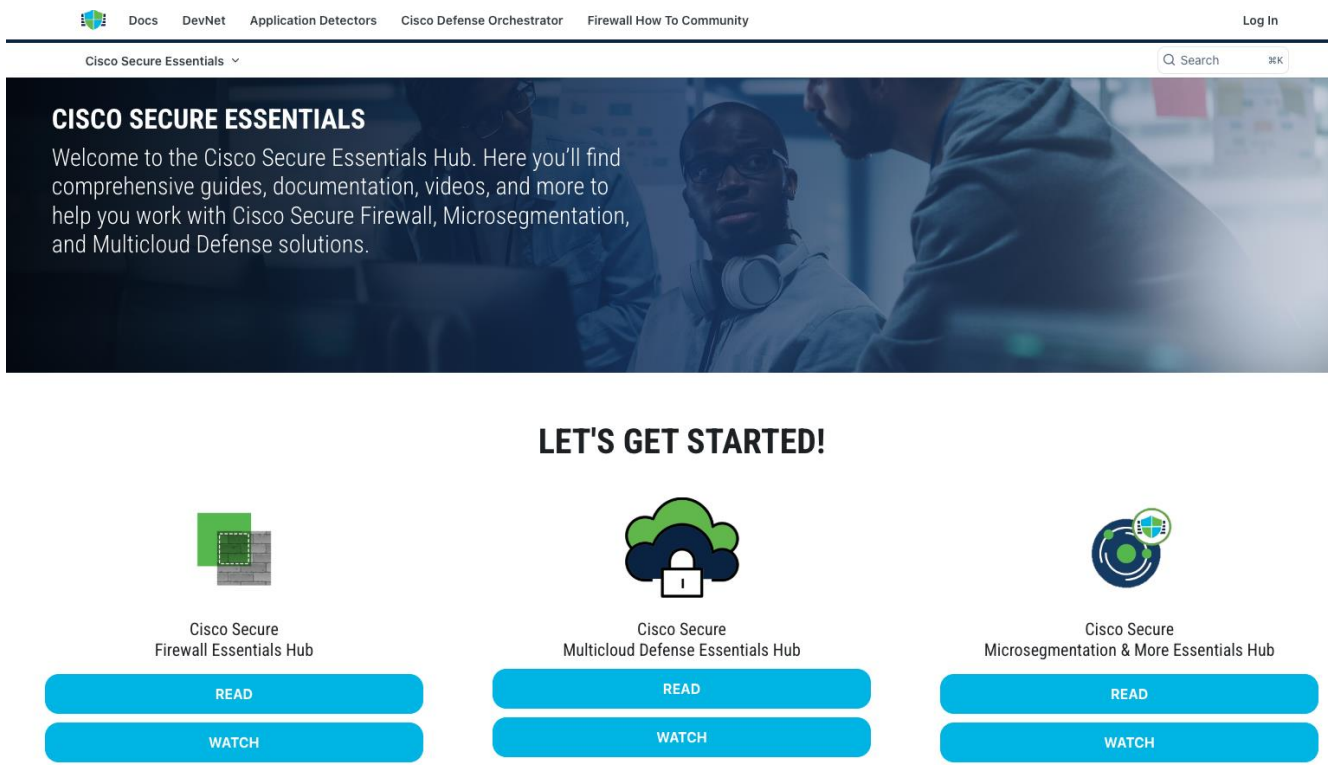
cs.co/sfYouTube



Simplified One Pager and How to

- Feature highlights – One Pager
- Step-by-step guidance
- Best practices
- Use cases and deployment guides

secure.cisco.com



Thank you