

# 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

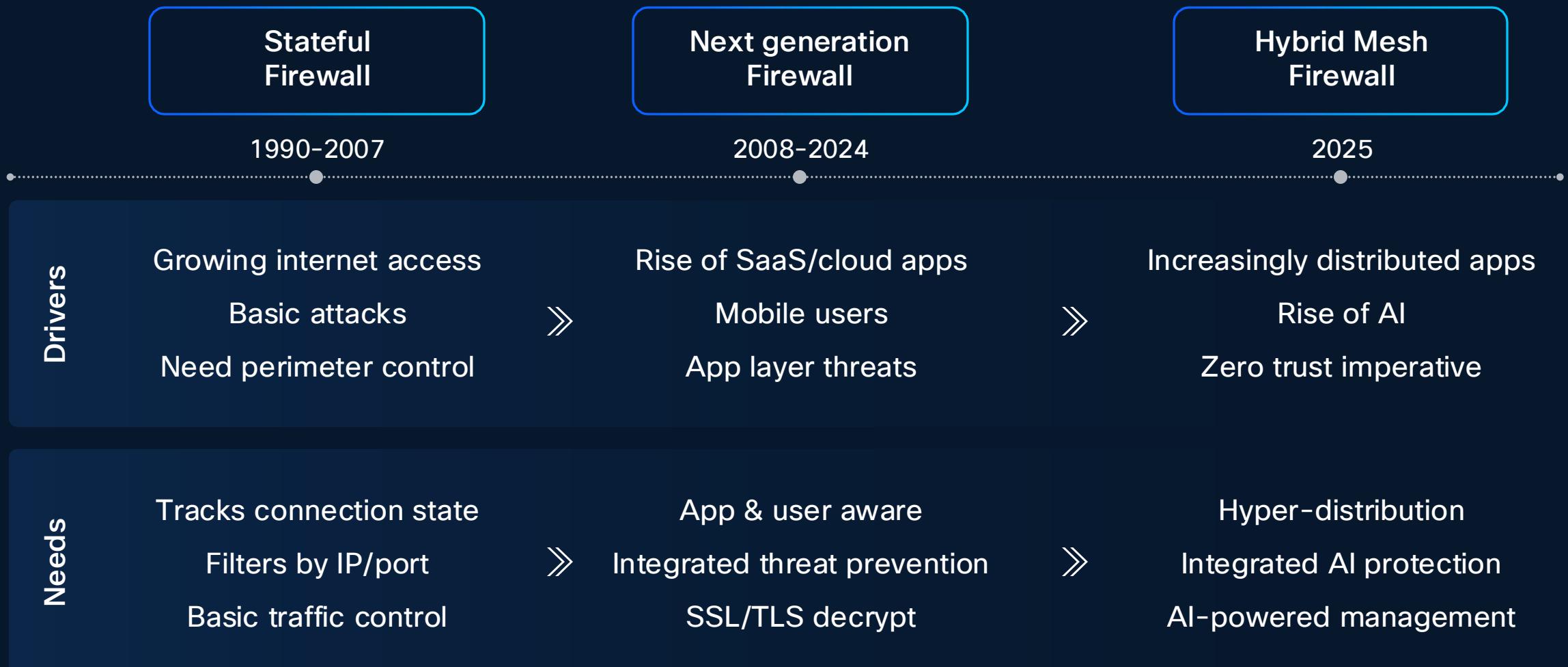
Highly distributed  
applications

Nothing can  
be trusted

More vulnerabilities,  
exploited faster

← AI adoption makes it more challenging →

# From Firewall to Firewalling



# Everyone Elses definition of Hybrid Mesh Firewall is limited



Unified management



Physical  
Firewall



Virtual  
Firewall



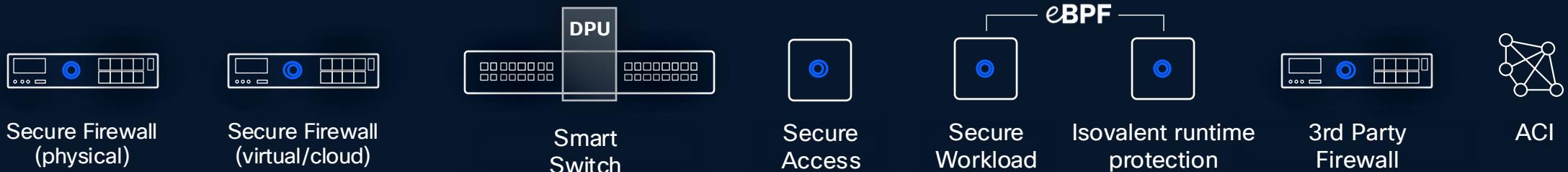
Cloud  
Firewall

“Boxes managed as one”

# 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

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

## Consolidated Management

Centralized assets & identity  
One network topology  
Unified posture  
Reporting, Logging, Analytics

## Advanced Capabilities

Agentic Ops  
Policy & Threat Intelligence  
Autonomous Segmentation  
Distributed Exploit Protection

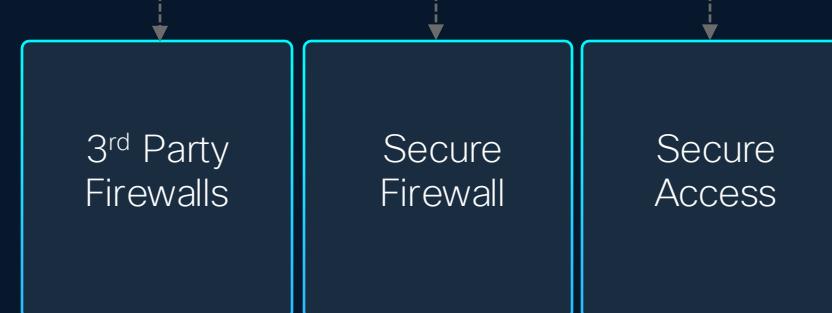
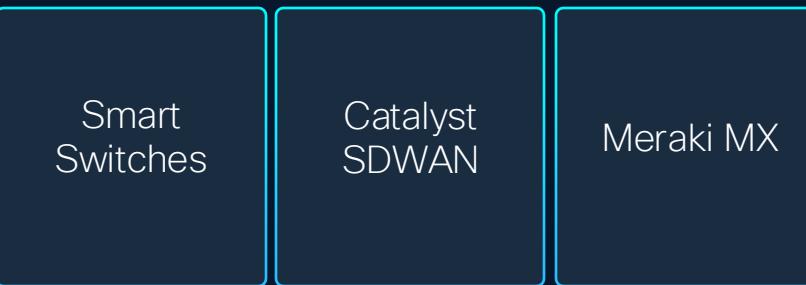
## Enforcement Orchestration

Cloud Firewall  
AI runtime protections

## Security Cloud Control



Mesh  
Policy

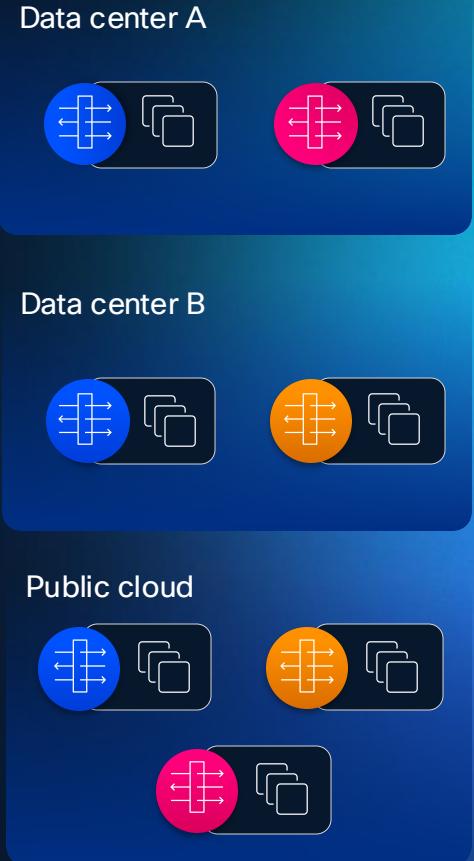


# Introducing Mesh Policy Engine

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

The screenshot shows the Cisco Security Cloud Control interface. The top navigation bar includes 'Policies' (Head revision: 320), 'Firewall-Policy-Update (Base revision: 319)', and 'B2B, B2C Policy'. The main content area is titled 'Policies' and shows a 'Changeset overview' for a 'Draft' changeset. It includes a 'Change summary' table with 00 entries for Rulesets, Rules, Endpoints, and Applications. Below this is a table of 'All Rulesets' with 48 results, showing columns for Name, Type, Install targets, Rules, and Description. The table lists various policies like 'HR Apps Access', 'Branch Policy', 'DMZ Security Policy', etc., with their respective details and enforcement points.



# What is Cisco Hybrid Mesh Firewall

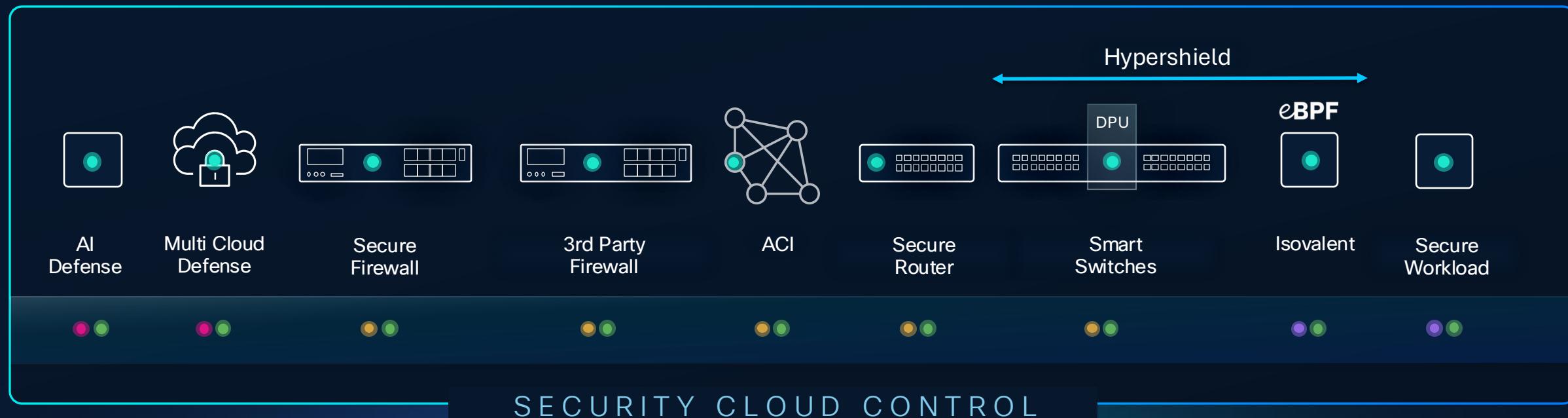
## CUSTOMER SECURITY OUTCOMES

Network Segmentation

Macro & Micro Segmentation

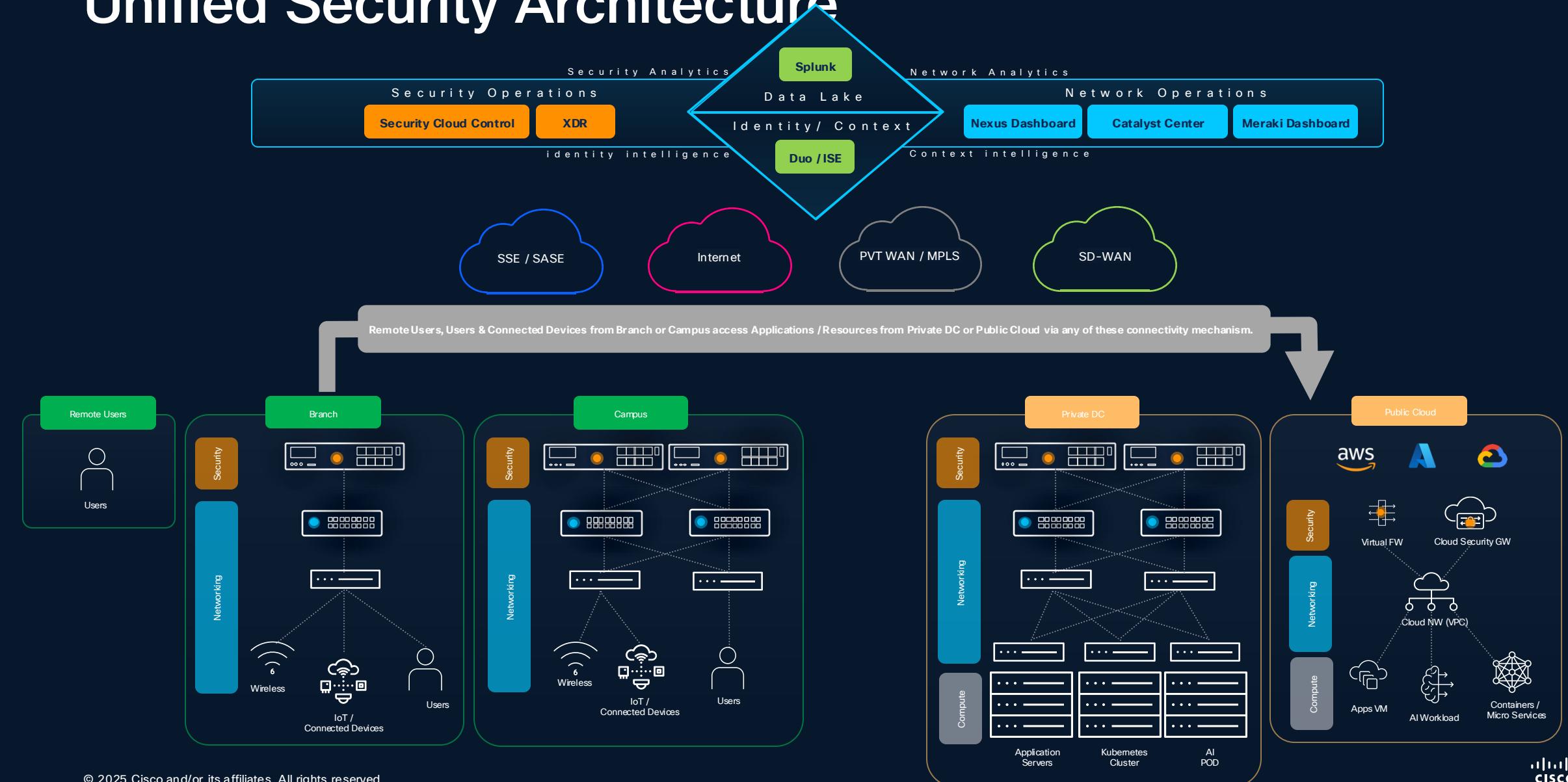
Threat Detection & Exploit Protection

AI Security

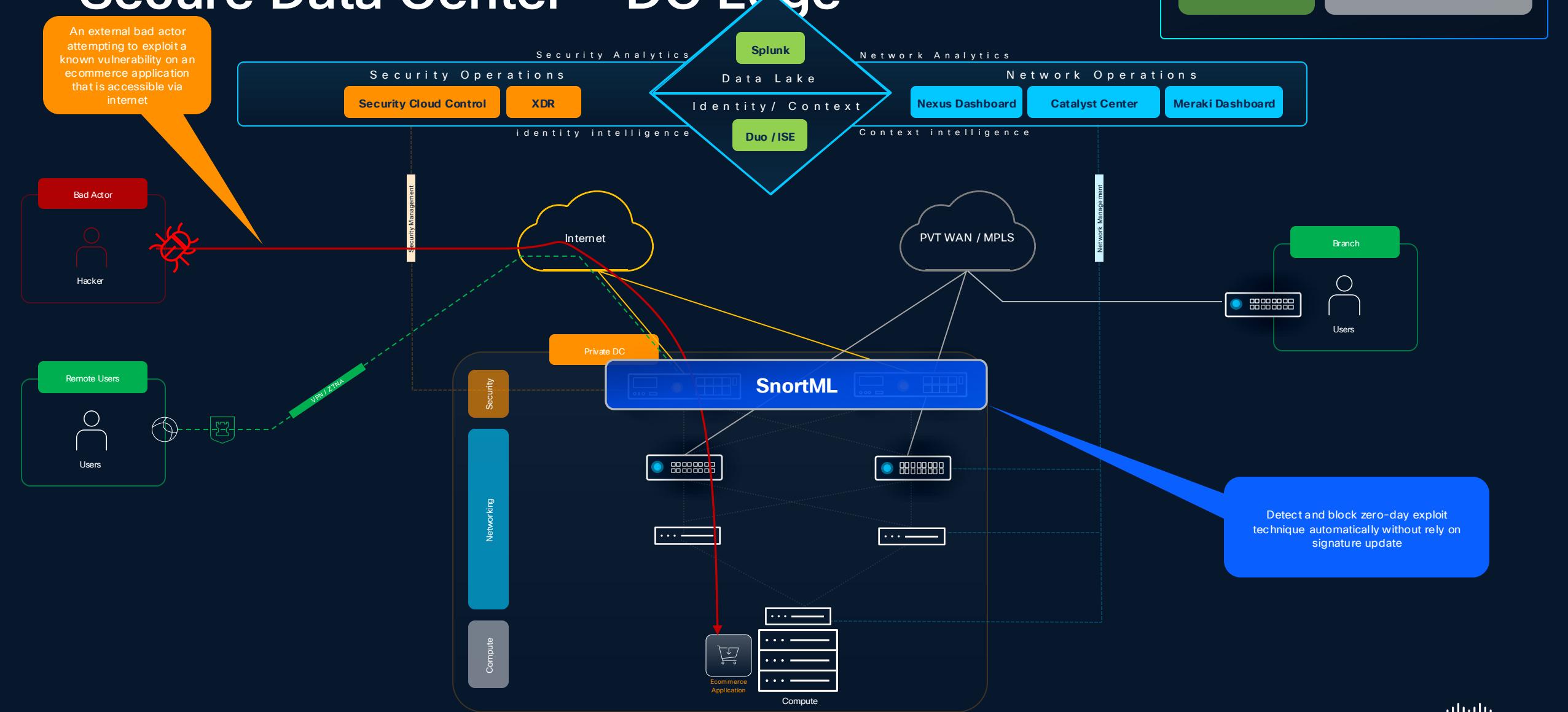


Write policy once, enforce across the mesh

# Unified Security Architecture



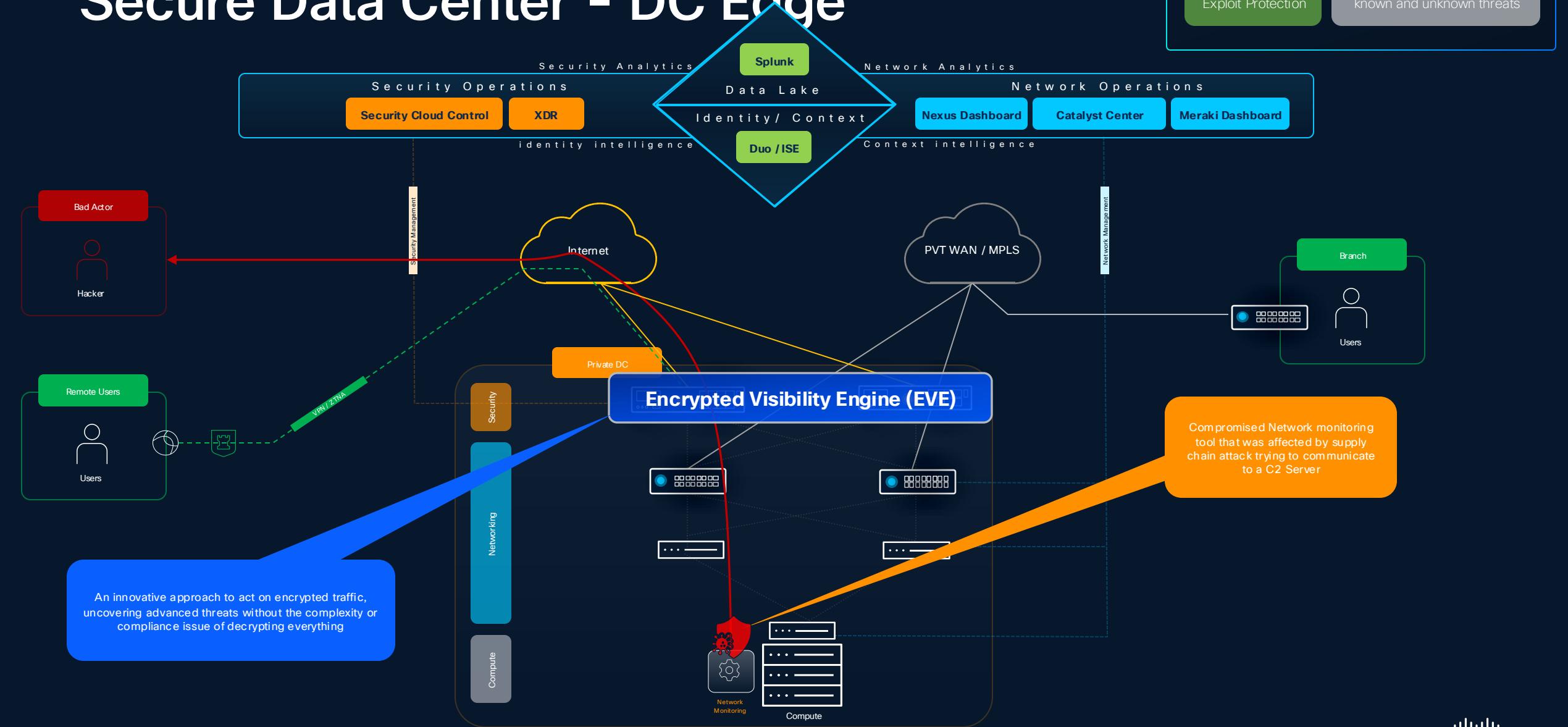
# Secure Data Center - DC Edge



# Secure Data Center - DC Edge

Threat Detection & Exploit Protection

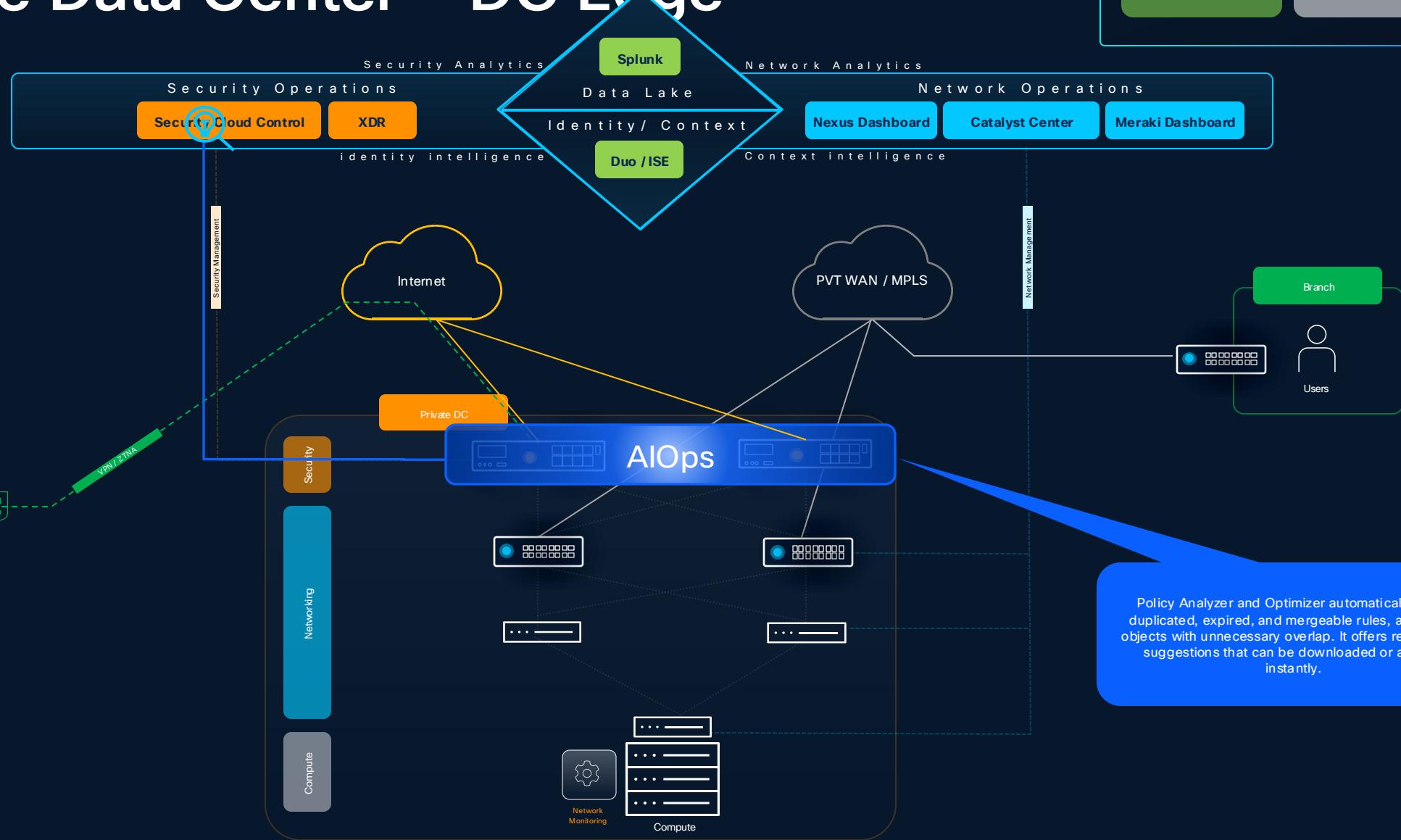
Detect and Protect against known and unknown threats



# Secure Data Center - DC Edge

Threat Detection & Exploit Protection

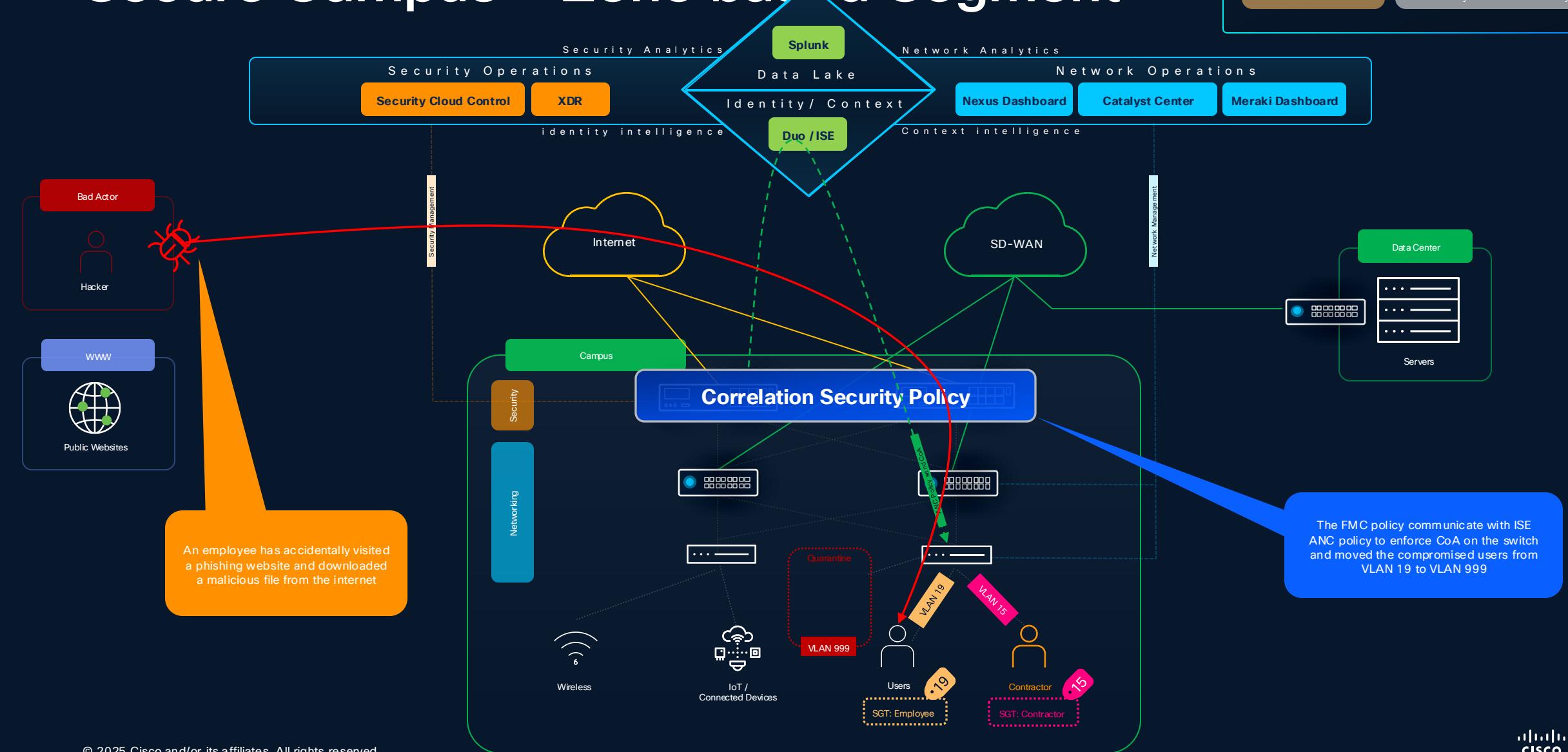
Detect and Protect against known and unknown threats



# Secure Campus - Zone based Segment

Network Segmentation

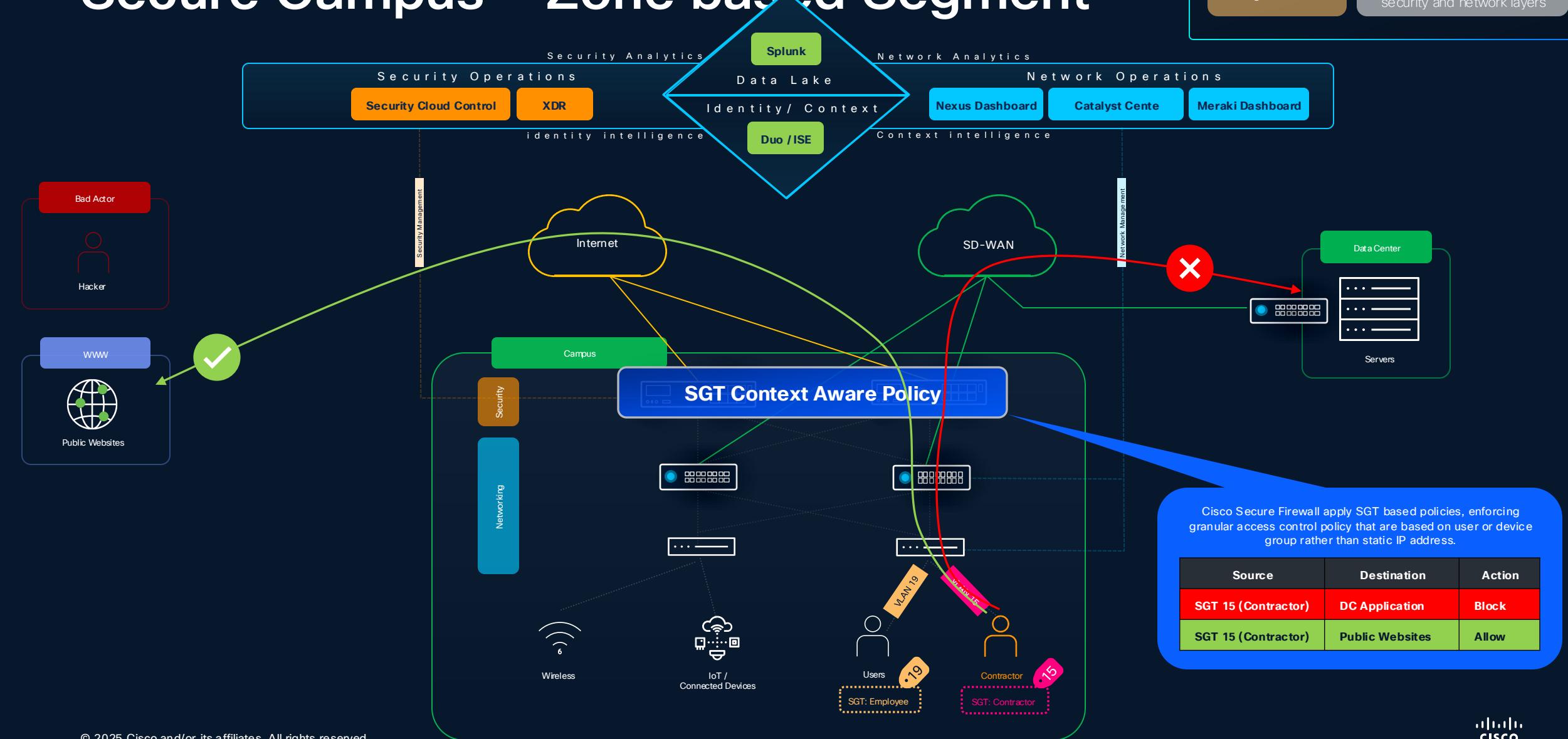
Securely apply context aware unified segmentation to both security and network layers



# Secure Campus - Zone based Segment

Network Segmentation

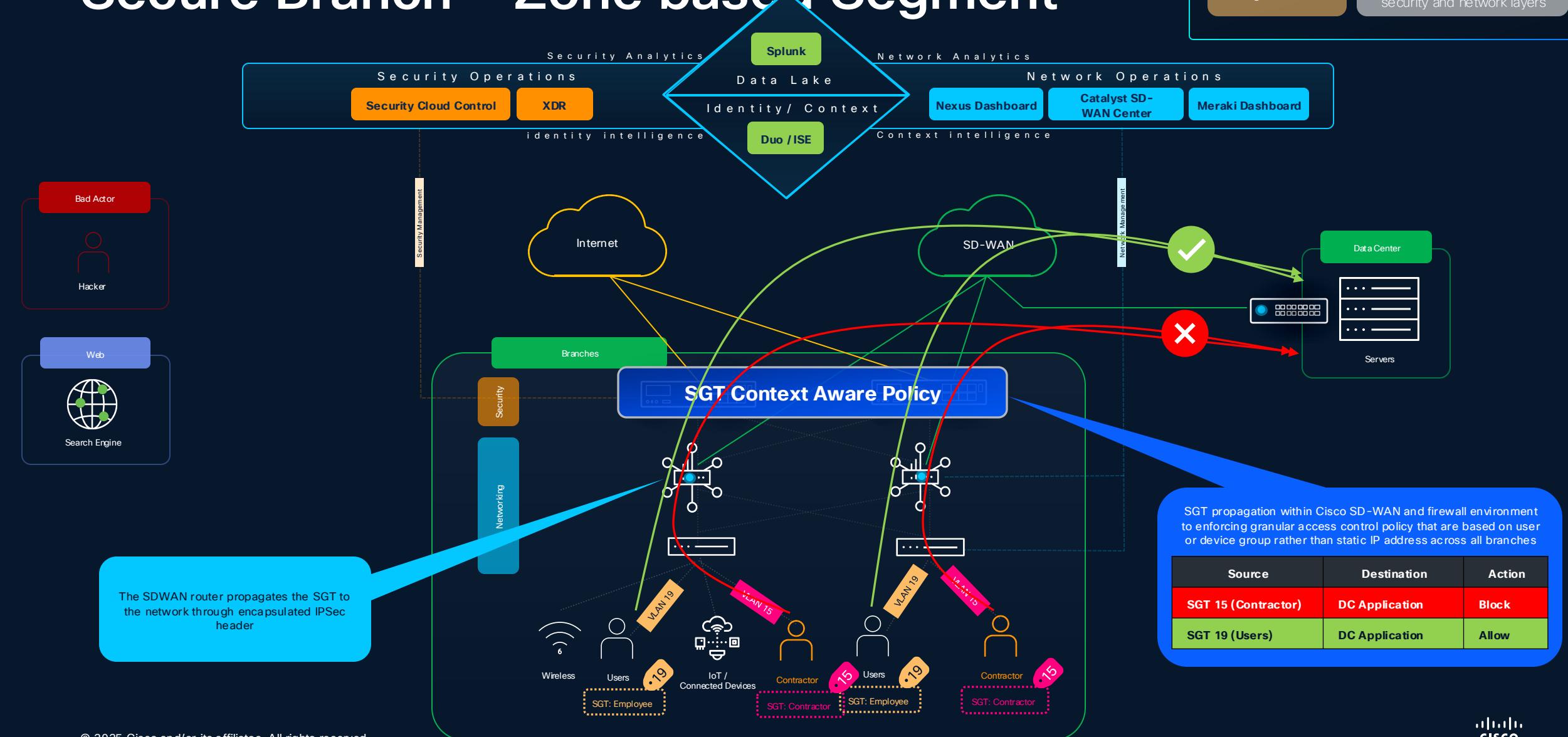
Securely apply context aware unified segmentation to both security and network layers



# Secure Branch - Zone based Segment

Network Segmentation

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



# Our Firewall has comprehensive capabilities

## Superior Threat Protection

Cisco Talos Security Intelligence



Configuration and Analytics Console

# Cisco Firewall – Hardware Innovations

# A high-performing firewall for every use case

Cisco Secure Firewall family performance at-a-Glance



Branch	Campus	Data center	Cloud
 <b>200 Series</b>	 <b>1200 Series</b>	 <b>3100 Series</b>	 <b>4200 Series</b>
2 Models	5 Models	5 Models	3 Models
Firewalling+IPS	Firewalling+IPS	Firewalling+IPS	Firewalling+IPS
1.5-2.5 Gbps	6-24 Gbps	10-45 Gbps	71-149 Gbps
IPSec VPN	IPSec VPN	IPSec VPN	IPSec VPN
1-2 Gbps	5-22 Gbps	5.5-39.4 Gbps	51-148 Gbps
TLS Decryption	TLS Decryption	TLS Decryption	TLS Decryption
0.75-1.25 Gbps	1-4.1 Gbps	3.2-11.5 Gbps	20-45 Gbps
		 <b>6100 Series</b>	20+ cloud variants
			 HyperFlex
			 KVM
			 vmWare ESXi
			 Microsoft Azure
			 alkira
			 EQUINIX
			 ORACLE CLOUD INFRASTRUCTURE

# Secure Firewall 220

## At-a-glance



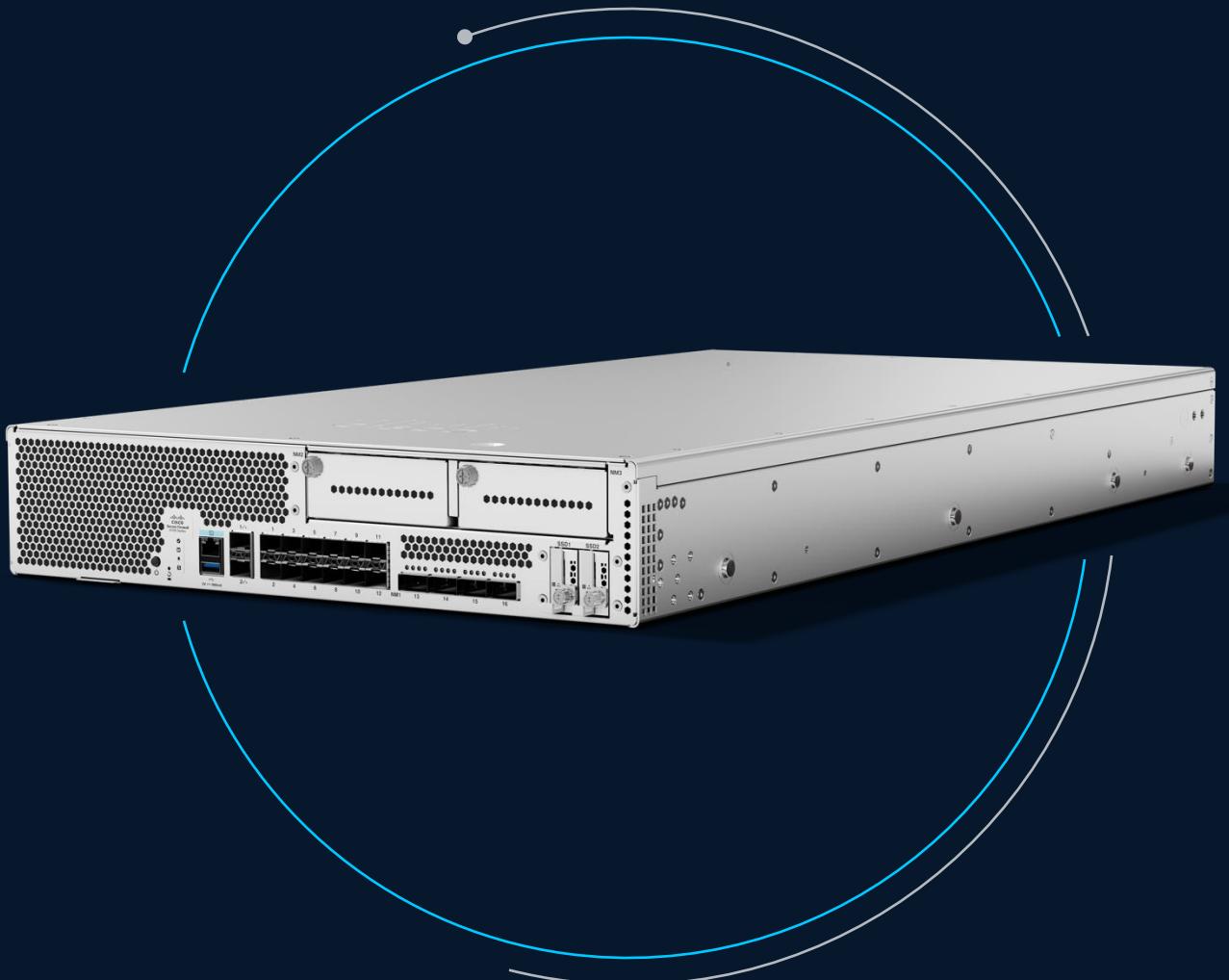
- One Model - 220
- Flexibility to address all modern NGFW use cases
  - Network/Security SoC with 4 ARM cores design
- SoC-embedded accelerators for encryption and traffic processing
- Up to 1.5Gbps (1024B) for NGFW traffic profiles
- Up to 1 Gbps for IPsec VPN, and up to 0.5 Gbps for TLS 1.2/1.3



# Cisco Secure Firewall 6100 Series



- 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



# 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 Lifecycle  
Expected Sellable life till CY2030 and beyond



# Firewall 10.0 Enhancements & Innovations

# Release Adoption



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

# Firewall

## 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

## 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

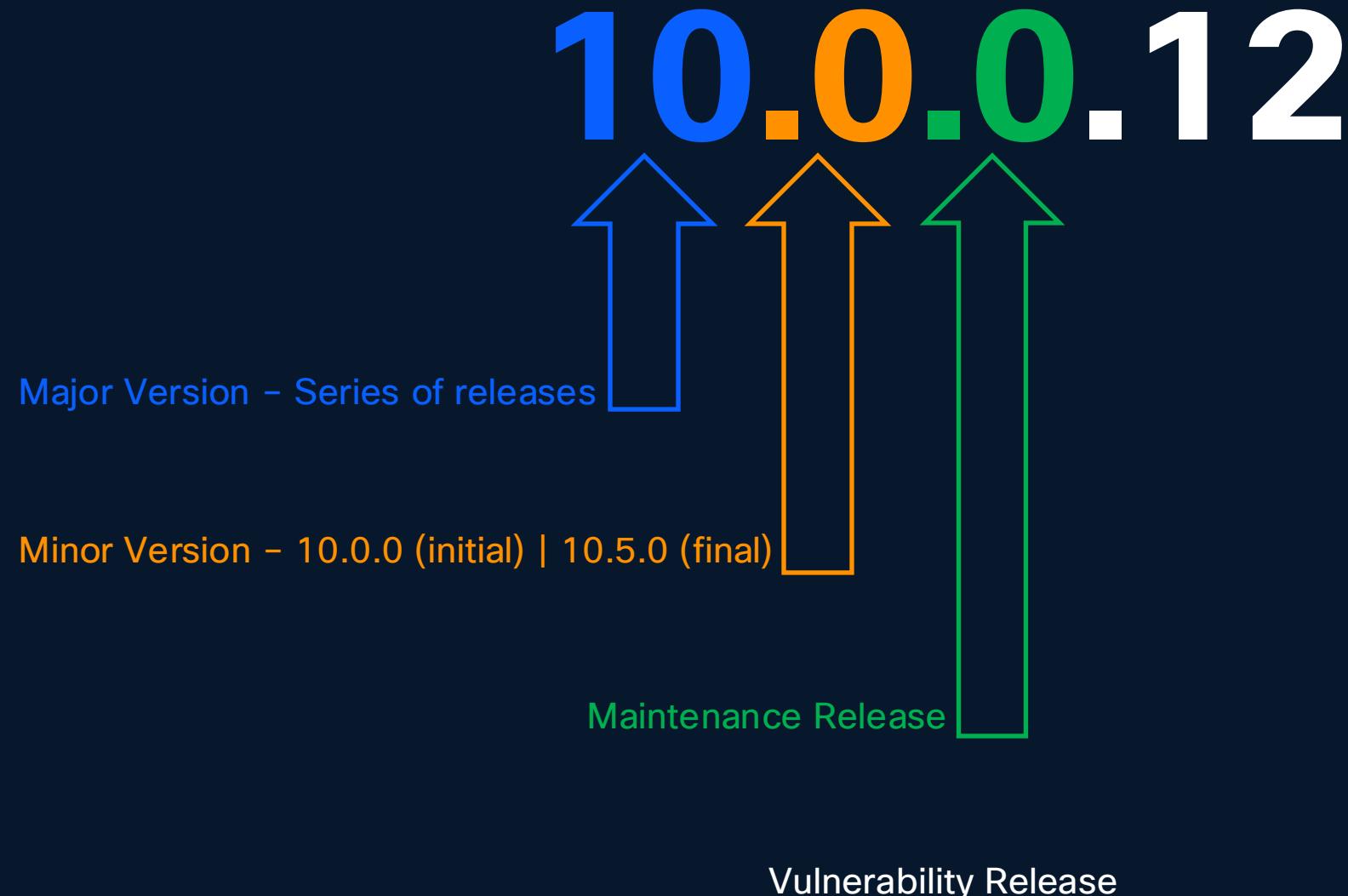
Simple, swift, & error-free upgrades with less than 10-clicks from anywhere in the UI to a fully upgraded environment.

## 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

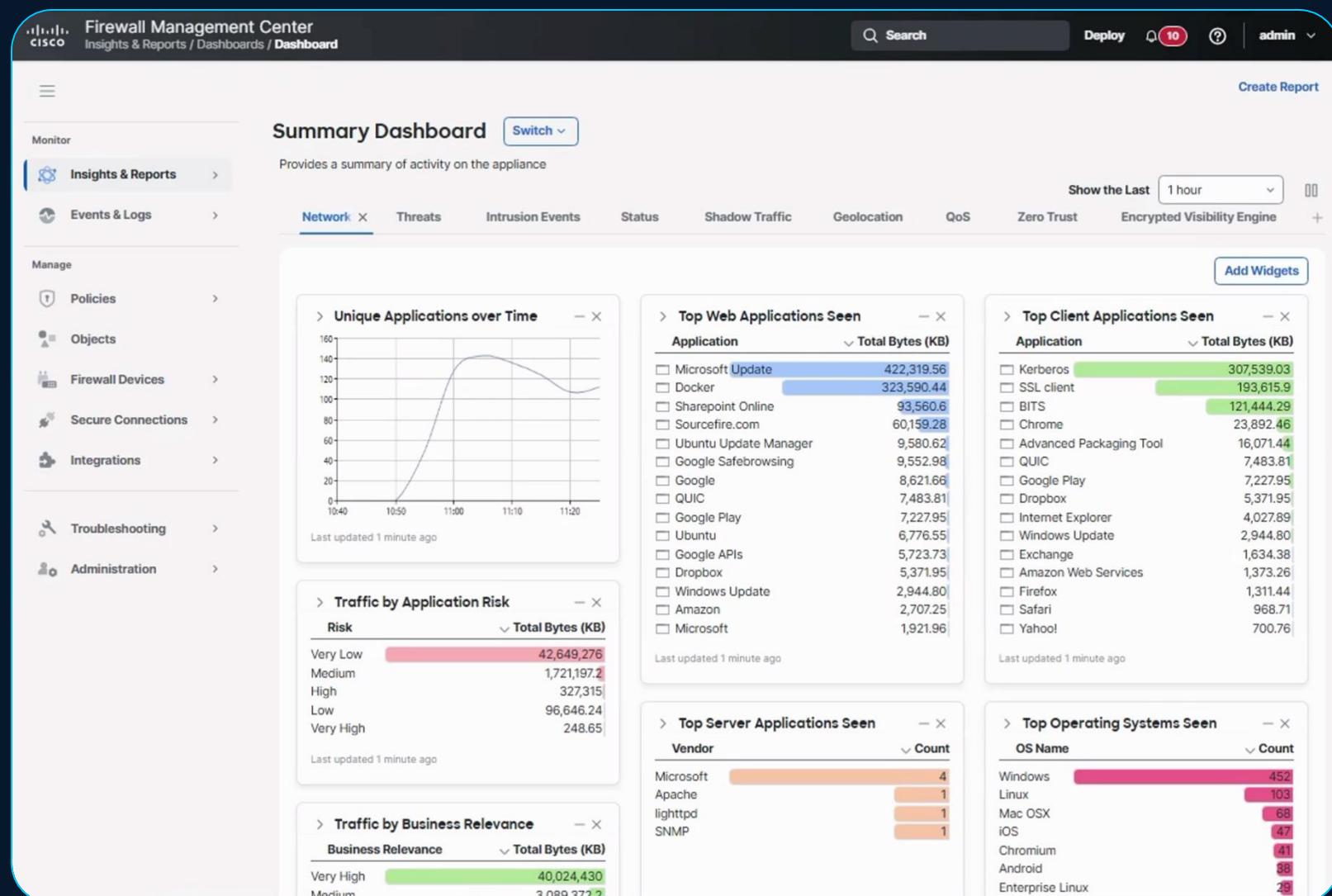
# New Global Navigation

- 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**

The screenshot shows the Firewall Management Center's Summary Dashboard. The left sidebar includes sections for Monitor, Insights & Reports (selected), Events & Logs, Manage (Policies, Objects, Firewall Devices, Secure Connections, Integrations), Troubleshooting, and Administration. The main dashboard features several widgets: a line chart for 'Unique Applications over Time' showing a sharp increase from 10:25 to 11:05; a bar chart for 'Top Web Applications Seen' with Microsoft Update at the top; a bar chart for 'Top Client Applications Seen' with SSL client at the top; a bar chart for 'Top Server Applications Seen' with Microsoft at the top; a bar chart for 'Top Operating Systems Seen' with Windows at the top; and two smaller charts for 'Traffic by Application Risk' and 'Traffic by Business Relevance'.

# Splunk Configuration on FMC

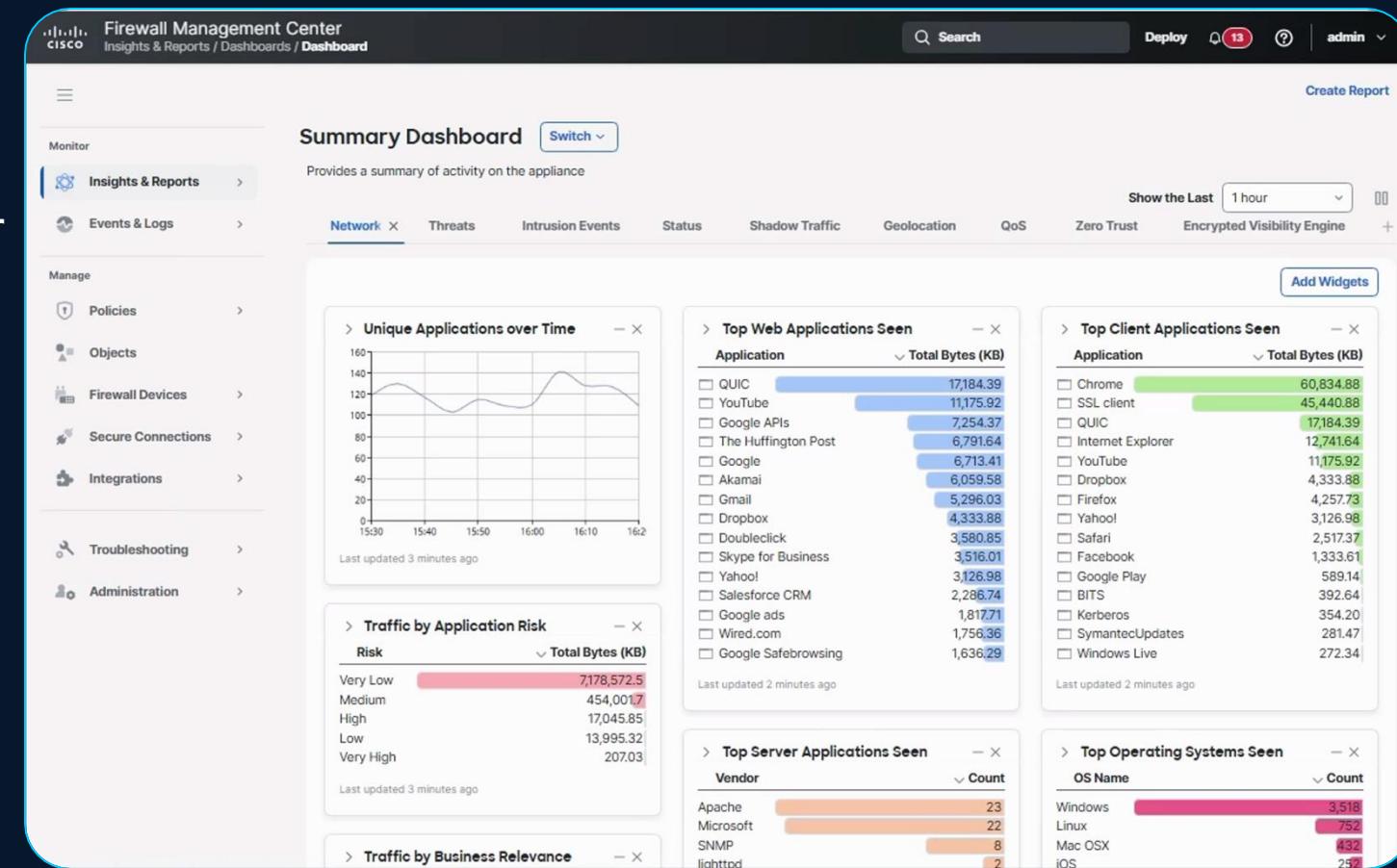
- Configuration is created at [Integration > Splunk](#) page on FMC UI.
- Each profile has 5 configuration sections:
  1. Destination
  2. Event
  3. Source
  4. Client certificates
  5. Summary
- Splunk profiles can be created targeting the same device(s) and are additive.
- Profiles are limited to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

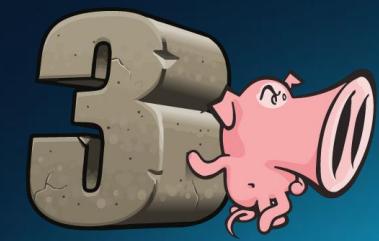


# Identity Updates

# 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.

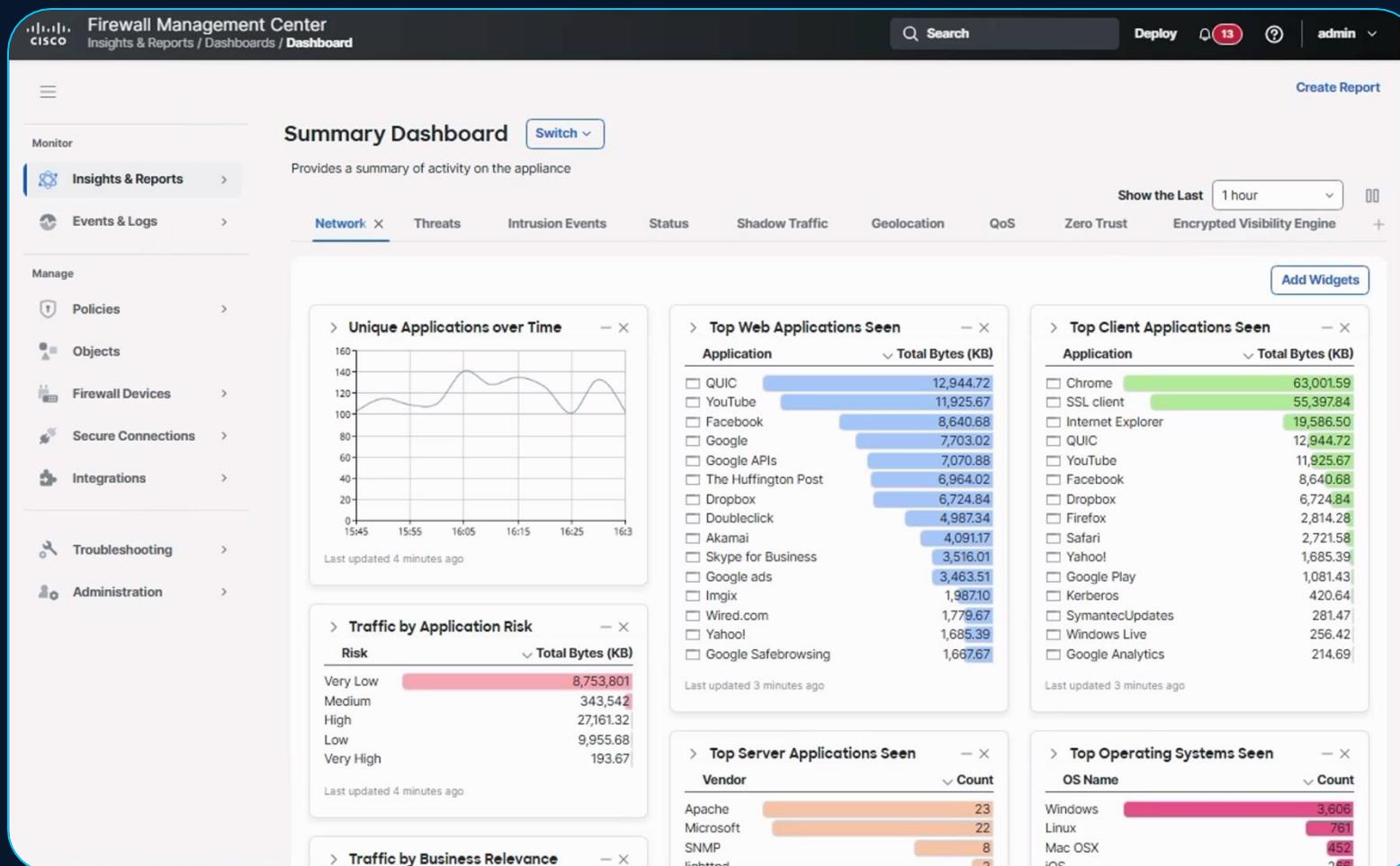




# Threat Updates

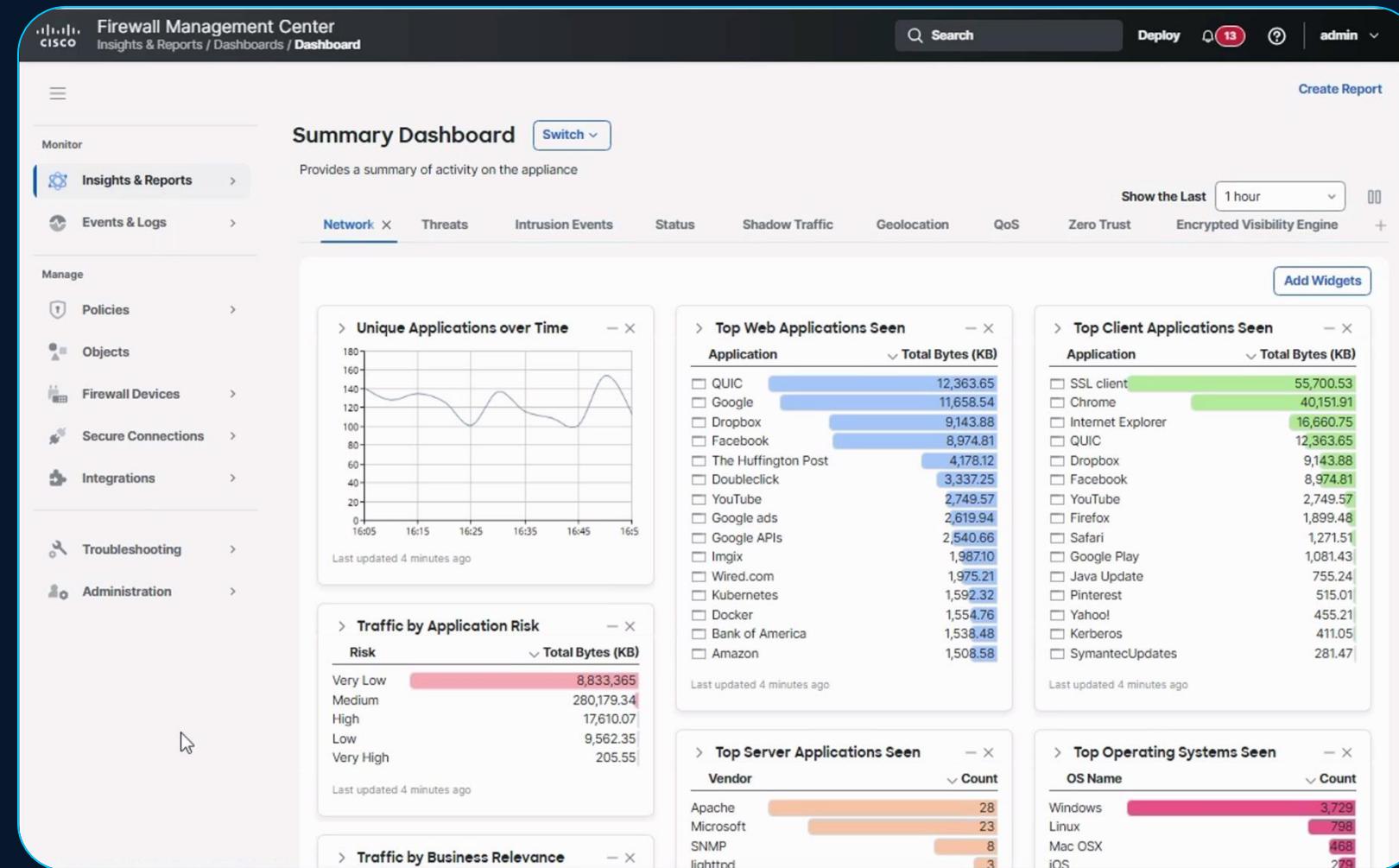
# Simplifying EVE

- 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

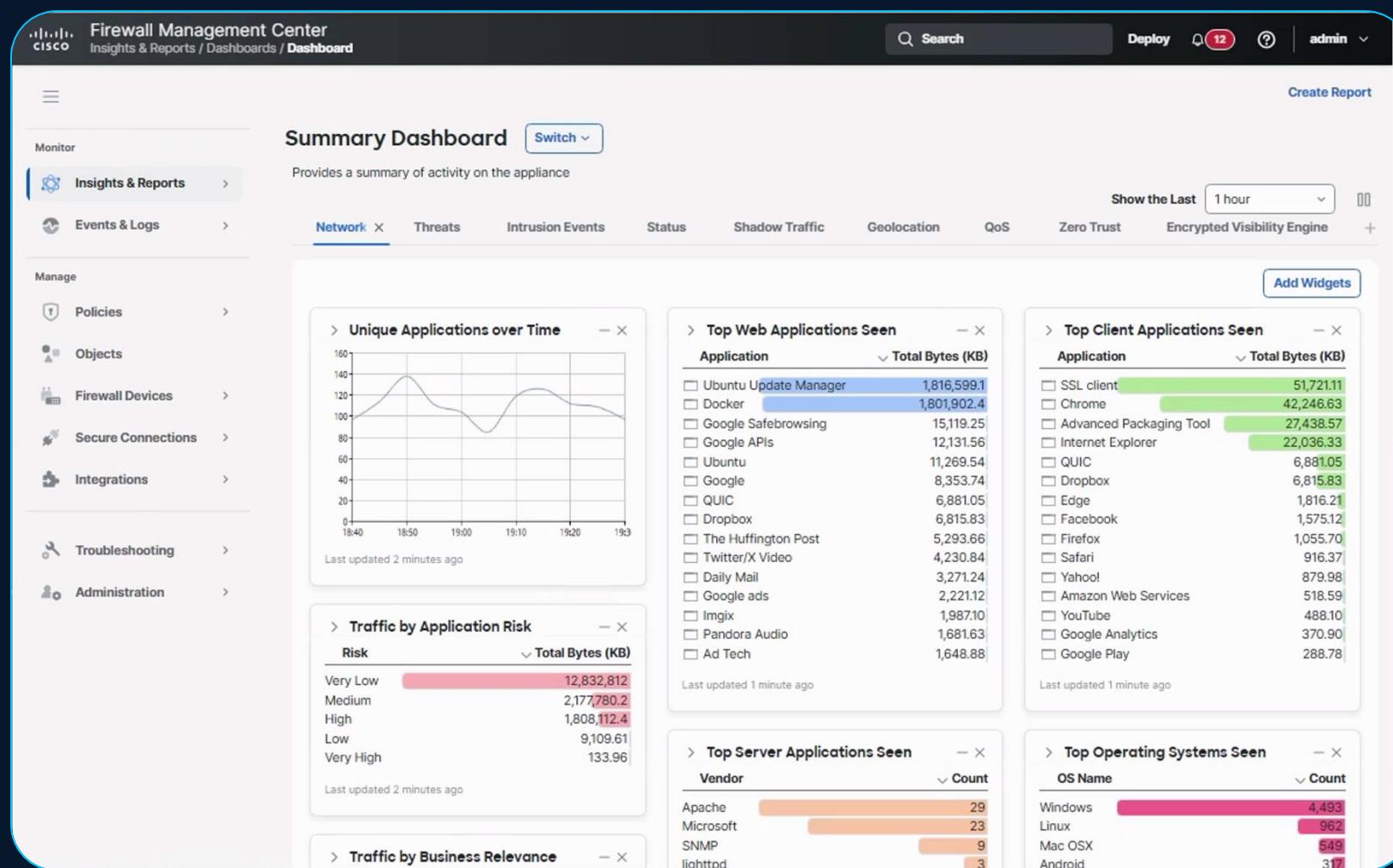
- SnortML – Neural network-based exploit detector for Snort 3.
- In release 7.6, SnortML was introduced and provided support for **SQL Injection** HTTP server attack type.
- SnortML now supports **HTTP command injection** as well, with more coverage coming soon.
- Under-the-hood enhancements have improved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

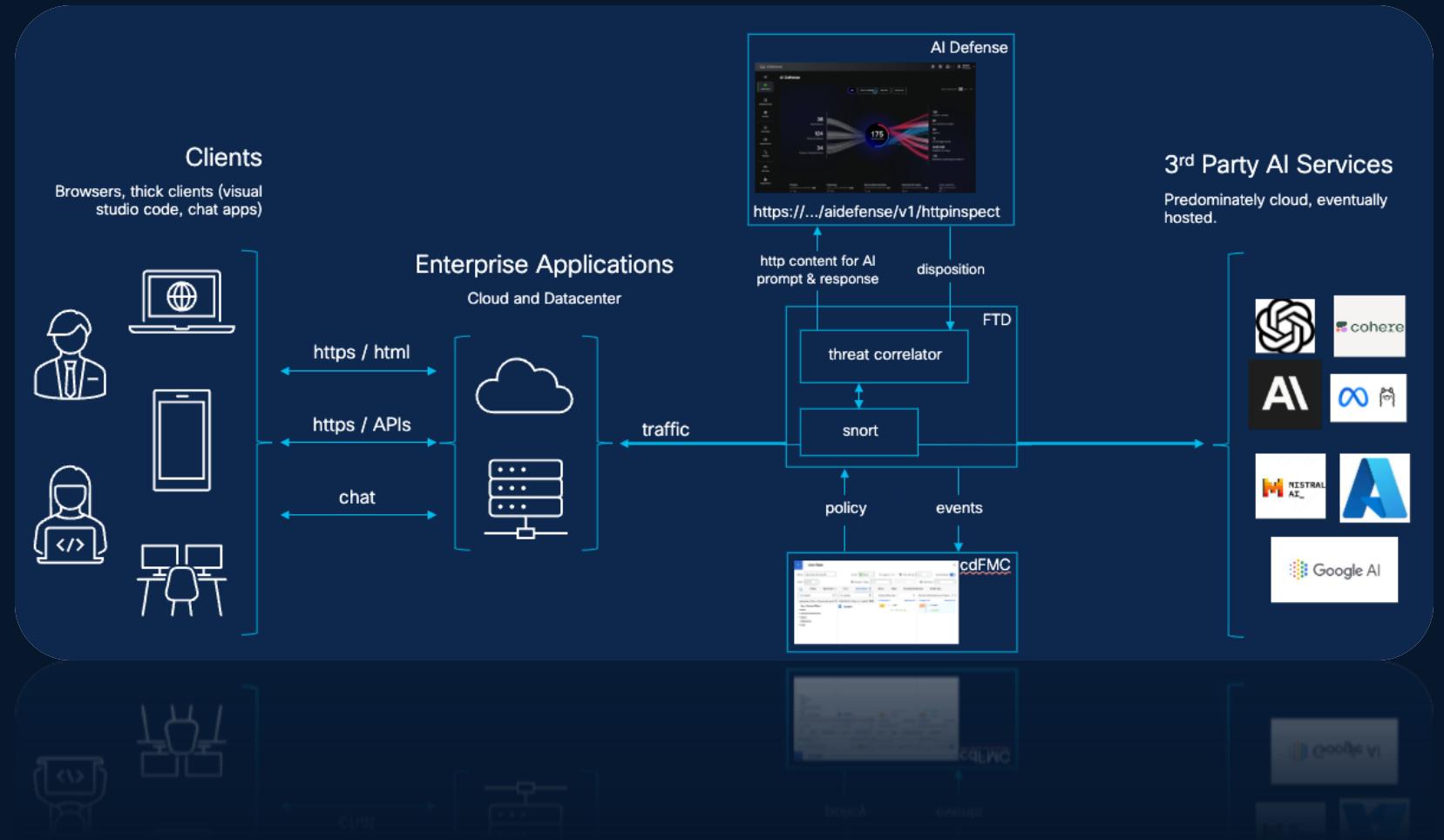


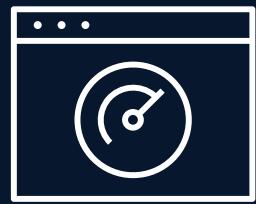
# AI Security

# Firewall & AI Defense (cdFMC)

## Gen AI Protection

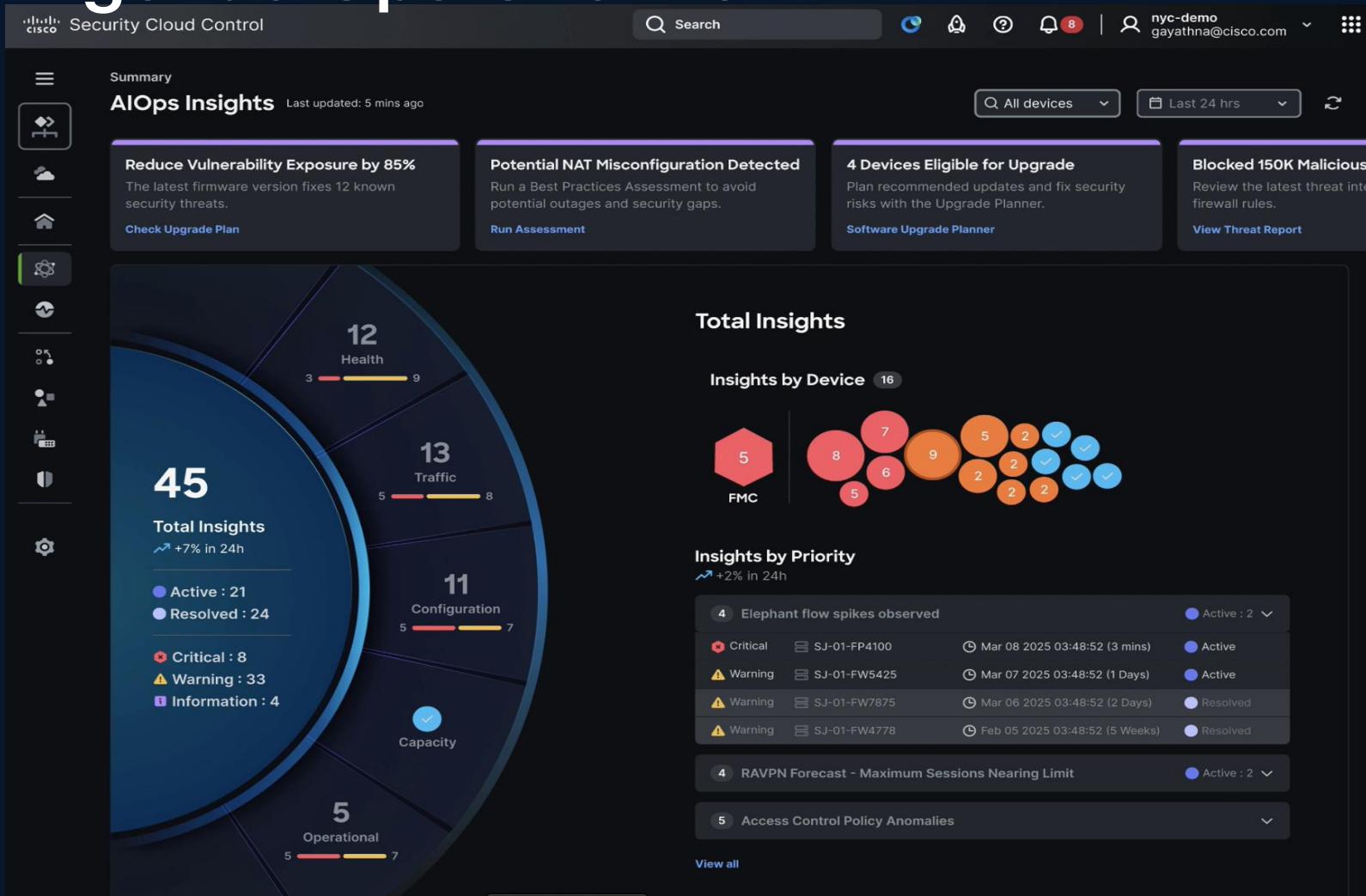
- Intercept and Evaluate prompts between enterprise applications to 3rd party AI Services
- Initially managed from Security Cloud Control
- Phase 2 will bring AI Defense Integration to FMC – 10.5
- Recruiting motivated customers for feedback and testing now!





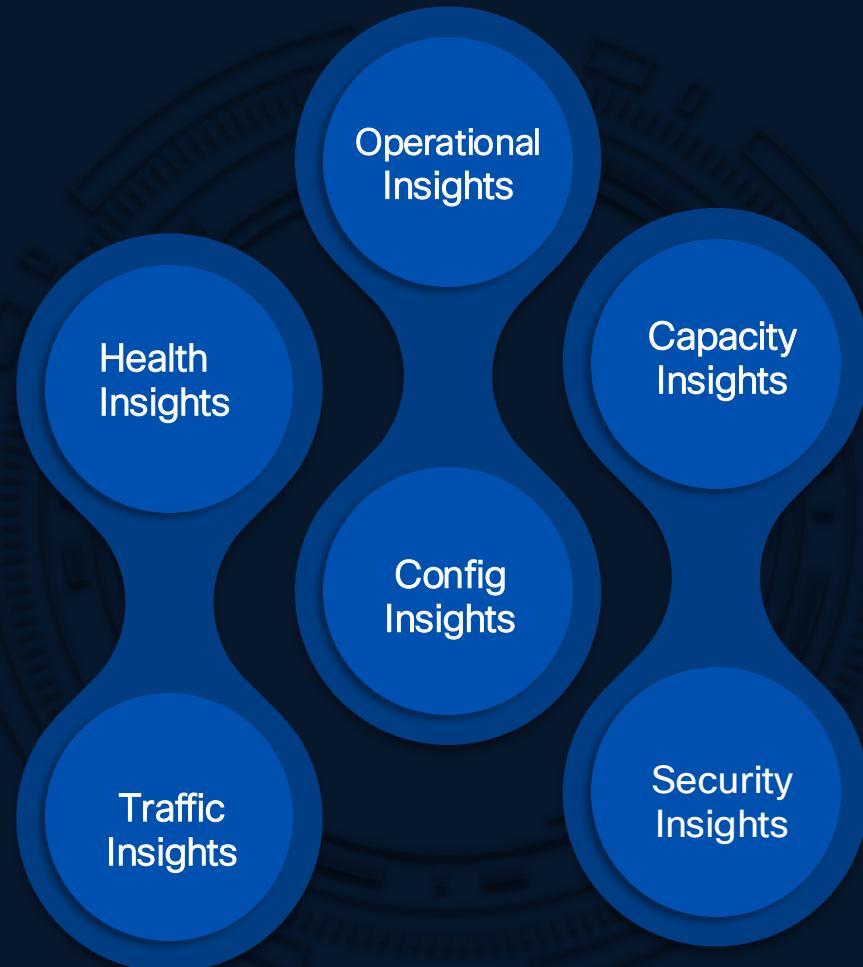
# Operational Efficiency

# 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

Security Cloud Control Policy Analyzer and Optimizer

Type 'Ctrl' + '/' to search

1 1 ? nyc-demo gayathna@cisco.com

**Overall summary**  
Review the cumulative summary of the total policies and address the areas that need attention to ensure compliance and optimal performance.

**45,828 Total Rules**

**17,836 (38.9%) Healthy rules**  
**25,071 (54.7%) Unhealthy rules**  
**2,921 (6.4%) Disabled rules**

**Total 49,345 anomalies in 25,071 unhealthy rules**

**Rule Definitions**

Shadowed rules <b>10,734 ↗ 21.8%</b>	Expired rules <b>494 ↗ 1.0%</b>	Total overlap objects <b>15,516 ↗ 31.4%</b>
Redundant rules <b>9,488 ↗ 19.2%</b>	Mergeable rules <b>12,909 ↗ 26.2%</b>	Partial overlap objects <b>204 ↗ 0.4%</b>

**Devices:** 0  
**Total Rules:** 30488  
**Observations:** 40099 **58% Optimizable**  
**Analysis Status:** Completed  
**Last Modified:** 09/12/2024, 19:17:54  
**Last Analyzed:** 09/20/2024, 14:29:11 **Analysis up-to-date**  
**Remediation Status:** Not Running  
**Hit Count Aggregation Status:** No data to process

**Analysis Actions**  
[View analysis details & optimize](#)  
[Download analysis report](#)

**Remediation Actions**  
[Remediation history \(0 version available\)](#)

**Policy Observation**  
We found a total of 40099 anomalies.

**Duplicate Rules (13601)**  
Fully Shadowed Rules 6362  
Fully Redundant Rules 7239

**Overlapping Objects (14779)**  
Fully Overlapped Objects 14629  
Partially Overlapped Objects 150

Access Control Policy	Devices	Total Rules	Observations	Analysis Status	Last Modified	Last Analyzed	Remediation Status	Remediation Time
Internal_ACP	0	12673	8558 <b>48% Opt</b>	Completed	10/11/2024, 09:16	10/16/2024, 23:59 <i>Analysis up-to-date</i>		
raj-vic-741	0	999	29 <1% Optim	Completed	10/11/2024, 09:16	10/16/2024, 23:59 <i>Analysis up-to-date</i>		
access1	0	7	2 <b>14% Optimiz</b>	Completed	10/11/2024, 09:16	10/16/2024, 23:59 <i>Analysis up-to-date</i>		
shadowed_anor	0	206	157 <b>36% Optim</b>	Completed	09/12/2024, 19:17	09/20/2024, 14:29 <i>Analysis up-to-date</i>		
UFTWF-FW-UR	0	95	94 <b>80% Optim</b>	Completed	09/12/2024, 19:17	09/20/2024, 14:29 <i>Analysis up-to-date</i>		
<b>NIC-HQ-NS-FW</b>	0	30488	40099 <b>58% Opt</b>	Completed	09/12/2024, 19:17	09/20/2024, 14:29 <i>Analysis up-to-date</i>		

© 2025 Cisco and/or its affiliates. All rights reserved.

CISCO

# Feature adoption

Security Cloud Control

← AIOps Insights

## Feature Adoption

Data sources: Cloud-Delivered Firewall Management Center

Last updated: 21 hours ago 

Adoption rate: 16% (12 Total features, 10 Not adopted, 0 Partially adopted, 2 Adopted)

Each feature is represented as a percentage, indicating the total number of products that have or have not adopted that feature.

### Licenses and associated features

Most of the features are associated with a license. Enable or disable a feature to improve your adoption score without impacting feature functionality.

**IPS** (0%)

- Intrusion Detection and Prevention
- Encrypted Visibility Engine**
- IPS Event Logging
- Cisco Umbrella DNS Policy

**Remote Access VPN** (0%)

- SD-WAN Capability and Connectivity

**Features not requiring license** (0%)

- Change Management
- Cisco Secure Dynamic Attributes Connector

### Encrypted visibility engine

The Encrypted Visibility Engine provides more visibility into the encrypted sessions without having to decrypt them.

Adoption rate: 0%

 **Encrypted Visibility Engine**  
Encrypted Visibility Engine for Firewall Threat Defense devices 

### Feature adoption rate at each enforcement point

 **Firewall Threat Defense**  
Adoption: 0%  
5 Total, 5 Not adopted, 0 Adopted

### Feature recommendations

 **Encrypted Visibility Engine**  
Encrypted Visibility Engine for Firewall Threat Defense devices 

 **Cisco Secure Dynamic Attributes Connector**  
Dynamic Attributes Connector for Firewall Management Center 

# Best Practice Recommendations

Security Cloud Control

Best practices assessment ①

10 Total checks | 4 Require review ①

Improve access control ④

Manage access and control pane ①

Checks

① Requires review | ② Informational Allow rule configured without an associated Intrusion or File policy

The Access Control Policy on this device is configured with one or more access control rules that are set to an action of "Allow" without the addition of an Intrusion or File Policy.

If the intent is to exclude the matching traffic from inspection, the rule should either be changed to an action of "Trust" and moved towards the top of the policy, or moved into the Pre-filter policy with an action of "Fastpath".

① Requires review | ② Informational Network Discovery Policy should be configured to discover protected hosts

The Network Discovery policy on this device is not configured according to best practices. To optimize performance and security, ensure the policy includes a defined protected network and is set to discover both Applications and Hosts. This configuration supports Adaptive Profiling and Impact Flags, enhancing the device's ability to monitor and respond to network activities effectively.

Remediation:

This document provides detailed instructions to configure your Network Discovery policy correctly. Follow the steps outlined in the [Configuring Network Discovery Policies guide](#)

① Requires review | ② Informational The Access Control Policy is using applications. To ensure optimal performance and security, it is recommended to enable early application det...

To ensure optimal performance and security, it is recommended to enable early application detection and server identity in your Access Control Policy (ACP). This is particularly important for traffic encrypted with TLS 1.3, as the certificates are encrypted. Enabling this feature allows the system to decrypt the certificate only, keeping the connection encrypted, and ensures that traffic matches access rules using application or URL filtering. You do not need to create a separate SSL decryption rule.

Action Required: Navigate to the Advanced Section of your ACP Policy to enable this feature.

① Requires review | ② Informational Default Action in Access Control Policy should have logging enabled

The default action in your Access Control Policy currently lacks logging, which is crucial for gaining visibility into the traffic managed by this action. It is recommended to enable logging to ensure comprehensive monitoring and security. For optimal configuration, consider the following logging actions:

- Block: Log at the beginning
- IPS: Log at the end
- Allow: Log at the end

Enabling these settings will help you maintain a robust security posture and provide valuable insights into network traffic.

In order to configure the desired action, navigate to Policies -- Access Control -- Select the ACP -- Edit the default action

# Traffic & Capacity Insights

aloha Security Cloud Control cisco

Type 'Ctrl' + '/' to search

aiops-smathura gayathra@cisco.com

## RAVPN Forecast - Maximum Sessions Nearing Limit

Critical Traffic & Capacity Aug 21 2025 | 03:30:00 UTC

### Summary

The current trend of RAVPN user sessions is rapidly approaching the firewall's maximum capacity, posing a significant risk of user connectivity issues. This forecast outlines current active and idle sessions to proactively address potential disruptions. Based on the current trend, firewall 'smathura\_ftd\_ver76\_ip77' will reach the RAVPN maximum user sessions in 6 days

### Impacted resources

smathura\_ftd\_ver76\_ip77

### Probable cause

#### Probable Cause

The high demand for RAVPN connections coupled with insufficient capacity allocation and ineffective session management is leading to strained RAVPN head-ends and potential performance issues.

### Confidence level

Medium

### RAVPN session forecast and breach point

Aug 21 2025 - Oct 10 2025 | 250 Max RAVPN capacity | Aug 27 2025 Predicted Breach Time

Forecast trend | 161 (64%) Minimum | 216.5 (87%) Average | 272 (109%) Maximum

RAVPN session breach threshold

RAVPN active connections | Forecasted RAVPN active connections | RAVPN idle connections | Forecasted RAVPN idle connections

### Remediation

Implement targeted remediation strategies to alleviate the strain on overloaded RAVPN headend and ensure optimal performance.

**Reduce RAVPN Idle Timeout:**

Reduce the idle timeout for RAVPN connections. This will disconnect inactive sessions and free up resources on the head-ends. While reducing the idle timeout improves resource management, it is important to find the balance to avoid frequent disconnects for active users. Consider user needs and typical usage patterns while setting the new timeout value.

**Use RAVPN Load Balancer:**

RAVPN Load Balancer distributes VPN client connections across multiple firewalls in a cluster, enhancing performance and availability. It is a built-in functionality and doesn't require an external load balancer.

No Active Jobs

# Software Upgrade Planner

Security Cloud Control

← AIOps Insights

## Software Upgrade Planner

Last updated: 21 minutes ago [Download Report](#) [Go to product upgrade](#)

**Device summary**  
6 / 6 Upgrade recommendations available

**Security vulnerability and bug fixes**  
20 Total available fixes **19** Security vulnerability fixes **1** Bug fixes

**Search:** Search

Device	Current version	Recommended versions ⓘ
smathura_ftd_ver76_ip76 Cisco Secure Firewall Threat Defense for VMware FTD	7.6.0	7.6.1 11 CVEs fixed 7.7.10 11 CVEs fixed
smathura_ftd_ver76_ip77 Cisco Secure Firewall Threat Defense for VMware FTD	7.6.0	7.6.1 11 CVEs fixed 7.7.10 11 CVEs fixed
FTD-Pune-BPR Cisco Secure Firewall Threat Defense for VMware FTD	7.6.0	7.6.1 11 CVEs fixed 7.7.10 11 CVEs fixed
smathura_cluster_82_83_84 Cisco Secure Firewall Threat Defense for VMware Cluster	7.6.0	7.6.1 11 CVEs fixed 7.7.10 11 CVEs fixed
FTDHA-Ver77_ip78_ip79 Cisco Secure Firewall Threat Defense for VMware High Availability	7.7.0	7.7.10 5 CVEs fixed
smathura_ftd_ver77_ip80 Cisco Secure Firewall Threat Defense for VMware FTD	7.7.0	7.7.10 5 CVEs fixed

Rows per page: 8 [1](#)

# Renewal Upgrade Planner

The screenshot shows the Cisco Security Cloud Control interface with the following details:

- Header:** Security Cloud Control, Search bar, Notifications, Admin (Acme Corp.)
- Breadcrumbs:** AIOps Insights > Upcoming End-of-Life for BLR-05-FW2100
- Device Status:** Critical (red), Operational (green), Jan 9, 2025 | 07:08:00
- Description:** Device BLR-05-FW2100 (Cisco Firepower 2100) is approaching its End-of-Life (EOL) date on November 15, 2025. Cisco no longer provides software updates, security patches, or technical support, which may pose operational and security risks. EOL Date Remaining time: 220 days.
- Impacted device:** BLR-05-FW2100
- Device with similar Model:**

Device name	Location	Software version	Last supported version
BLR-887	10.10.7.252 : 448	6.4.1	7.2
MUM-818	10.10.5.352 : 443	6.4	7.4
BLR-898	10.10.8.258 : 443	6.4.2	7.4
VPN-9888	10.10.5.357 : 445	6.4.2	7.4
ZTNA-821	10.10.8.922 : 443	7.4	7.4
- Cisco's recommended - Renewal upgrade devices:**
  - Cisco Firepower 1000 Series:** OS version 7.8, Form Rack mounted, Throughput 1.4 Gbps (1x faster), Performance Up to 15K VPN sessions, Interfaces 1-5 Gbps Interfaces. [View data sheet](#)
  - Cisco Secure Firewall 3100 Series:** OS version 7.8, Form Rack mounted, Throughput 2.0 Gbps (1x faster), Performance Up to 30K VPN sessions, Interfaces 1-7 Gbps Interfaces. [View data sheet](#)
  - Cisco Secure Firewall 4200 Series:** OS version 7.8, Form Rack mounted, Throughput 2.4 Gbps (1x faster), Performance Up to 50K VPN sessions, Interfaces 1-10 Gbps Interfaces. [View data sheet](#)
  - Cisco Firepower 1000 Series:** OS version 7.8, Form Rack mounted, Throughput 1.4 Gbps (1x faster), Performance Up to 15K VPN sessions, Interfaces 1-5 Gbps Interfaces. [View data sheet](#)
- Product Recycling:** Our commitment to lifecycle management. The Cisco Takeback and Recycle program helps businesses properly dispose of surplus products that have reached their end of useful life. The program is open to all business users of Cisco equipment and its associated brands and subsidiaries. [Know more](#)
- Talk with expert:** Get a call from Sales, Call Sales 1-800-121-3117 (9:00am-6:00pm). [Submit request](#)

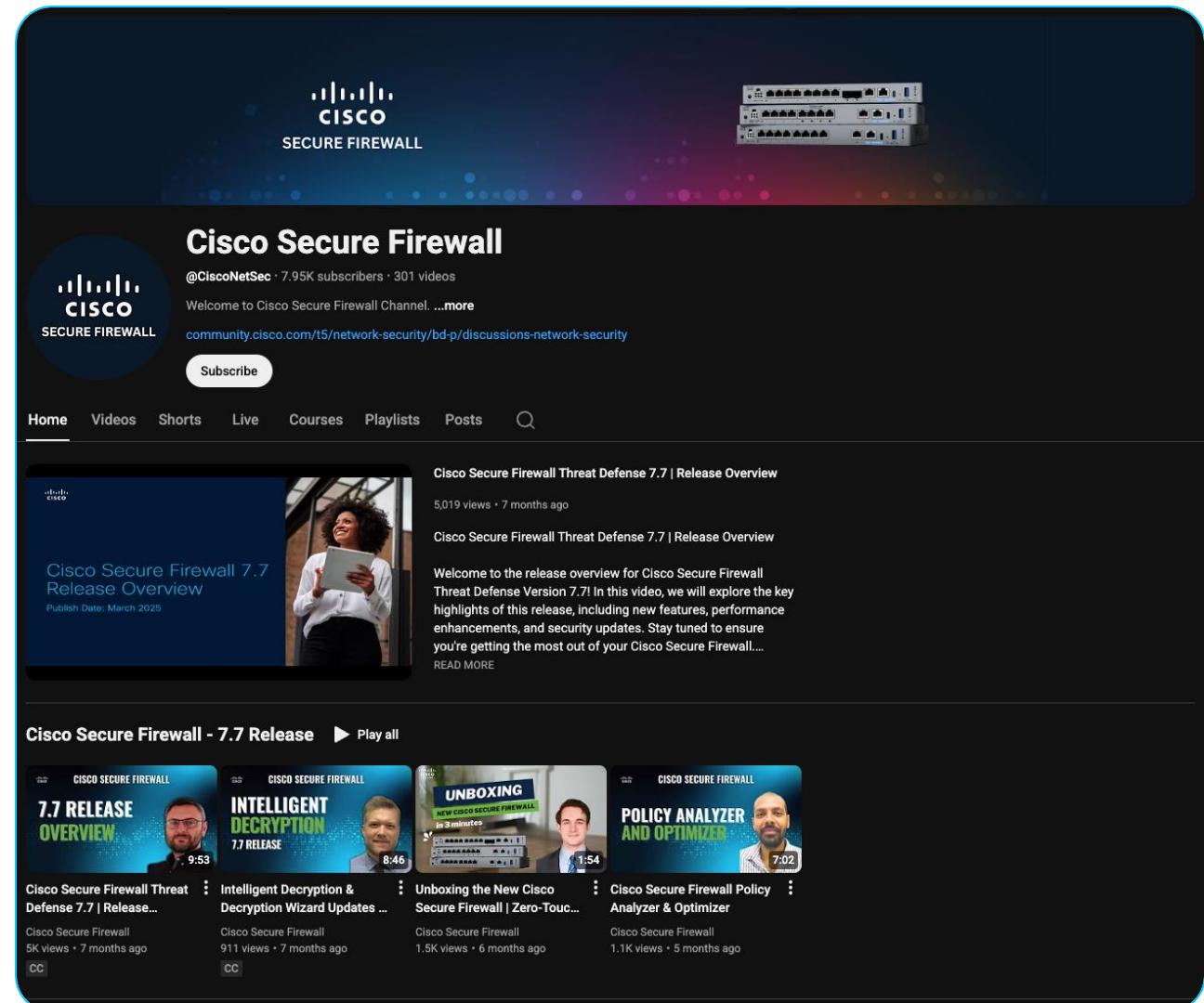
- List ASAs and FTDs reaching End of Life (EOL) in the tenant.
- Recommends FTD models to renew/refresh with based on newer models released.
- Provides quick access to data sheets & release notes for further details on the specification.
- In product notifications and reports about EOL available for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



Cisco Secure Essentials

**CISCO SECURE ESSENTIALS**

Welcome to the Cisco Secure Essentials Hub. Here you'll find comprehensive guides, documentation, videos, and more to help you work with Cisco Secure Firewall, Microsegmentation, and Multicloud Defense solutions.

**LET'S GET STARTED!**

**Cisco Secure Firewall Essentials Hub**

**Cisco Secure Multicloud Defense Essentials Hub**

**Cisco Secure Microsegmentation & More Essentials Hub**

READ

WATCH

READ

WATCH

READ

WATCH

Thank you

