CISCO
SECURE

CISCO The bridge to possible

From Firewall to the Future

John Wallace, CISSP

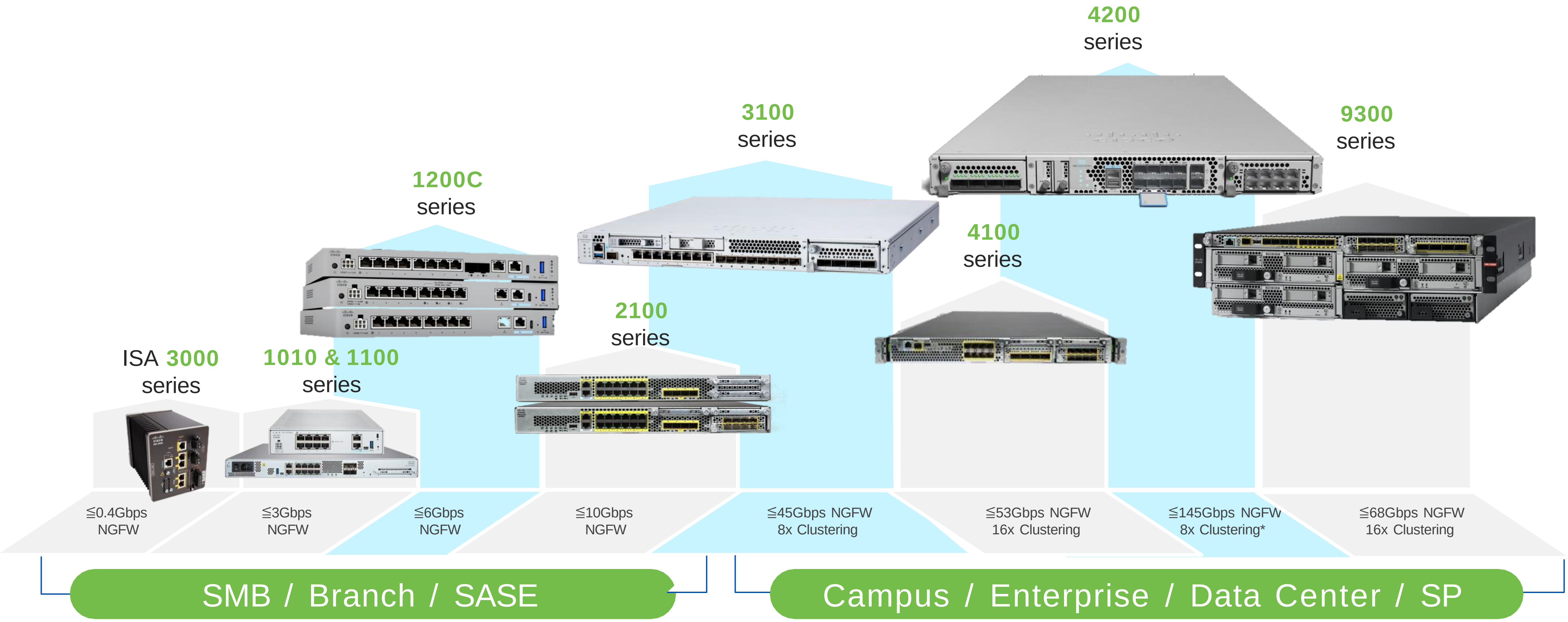
Security Advisor to Global SMB Partner Security Sales
Americas - Distribution Security Partner Account Manager
Global Mentee Initiative - Mentor

- Cisco Global Partner Security Sales
- 26+ Years in Enterprise Infrastructure
  - Implementation, Architecture, and Design. Specializations in Security, Application and Desktop delivery & End user experience.
- CISSP as of 10/21/22
- Drummer in a Cover Band
- SecTeam6 Alumni

CISCO SECURE

Cisco Secure Firewall Hardware

Full coverage, from IoT/OT & Branch / SASE to Enterprise/Carrier Class modular chassis



ISA 3000 series
≦0.4Gbps NGFW

1010 & 1100 series
≦3Gbps NGFW

1200C series
≦6Gbps NGFW

2100 series
≦10Gbps NGFW

3100 series
≦45Gbps NGFW 8x Clustering

4100 series
≦53Gbps NGFW 16x Clustering

4200 series
≦145Gbps NGFW 8x Clustering*

9300 series
≦68Gbps NGFW 16x Clustering

SMB / Branch / SASE

Campus / Enterprise / Data Center / SP

FTD 7.6+
ASA 9.22+

The New Secure Firewall 1200C Series

An SD-WAN enabled, high-performing, compact firewall for distributed enterprise branches

↑ > 3x Performance over rivals

↑ > 2x Price/Performance over rivals

1210CE - 1210CP - 1220CX

Enterprise-grade security

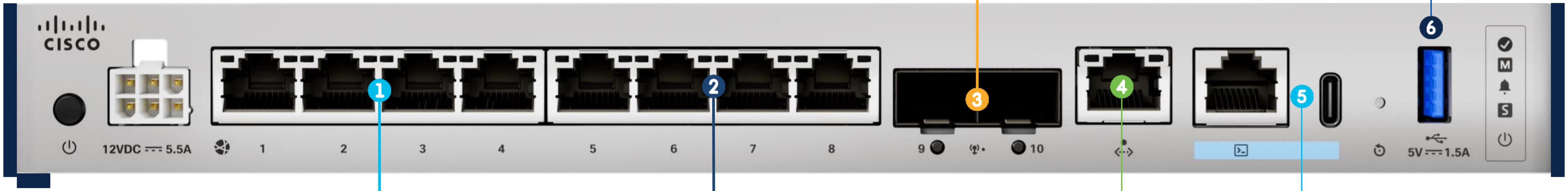
Increased performance, high efficiency and superior TCO

Cisco Secure Integrations

FTD 7.6+
ASA 9.22+

Secure Firewall 1200C Series Overview

Desktop form factor; optional rack mounting kit
Quiet fan for active cooling
External “brick-style” AC power adapter



2x SFP+
on CSF1220CX
model

USB 3
Type A

8x 1000BASE-T
Ethernet on
CSF1210CE
model

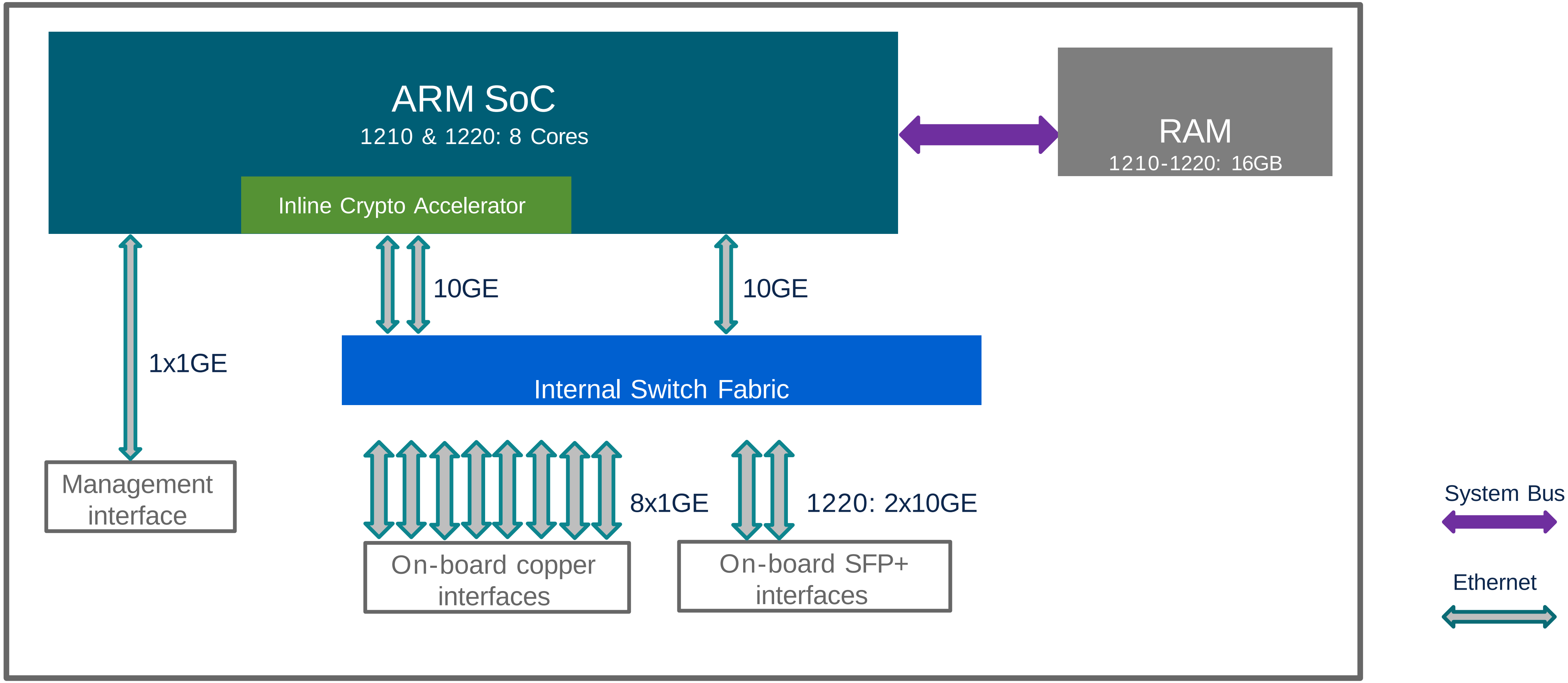
4 ports with UPoE+
on CSF1210CP model

Management
Ethernet

RJ-45 &
USB-C
console

FTD 7.6+
ASA 9.22+

Secure Firewall 1200C Series Architecture



FTD 7.6
ASA 9.22

Secure Firewall 1200C Performance

Model	Interfaces	PoE	FTD (FW+AVC+IPS) 1024B	FTD IPSec VPN 1024B FastPath	FTD TLS Decrypt/inspect
CSF1210CE	8x 1000BASE-T	-	*6 Gbps*	*5 Gbps*	*1.0 Gbps*
CSF1210CP	8x 1000BASE-T	4x UPoE+ (120W)	*6 Gbps*	*5 Gbps*	*1.0 Gbps*
CSF1220CX	8x 1000BASE-T, 2x SFP+	-	*9 Gbps*	*9 Gbps*	*1.5 Gbps*

Performance estimates are subject to change in final release.

Secure Firewall 4200 Series Appliance Multi-Instance & New Network Module

FTD 7.6+

Secure Firewall 4200 Series Multi-Instance

4200 series Multi-Instance feature functionality is identical to the Secure Firewall 3100 series, but it differs in the number of instances supported:

Secure Firewall Platform		Maximum Instance Count
4215		10
4225		14
4245		34

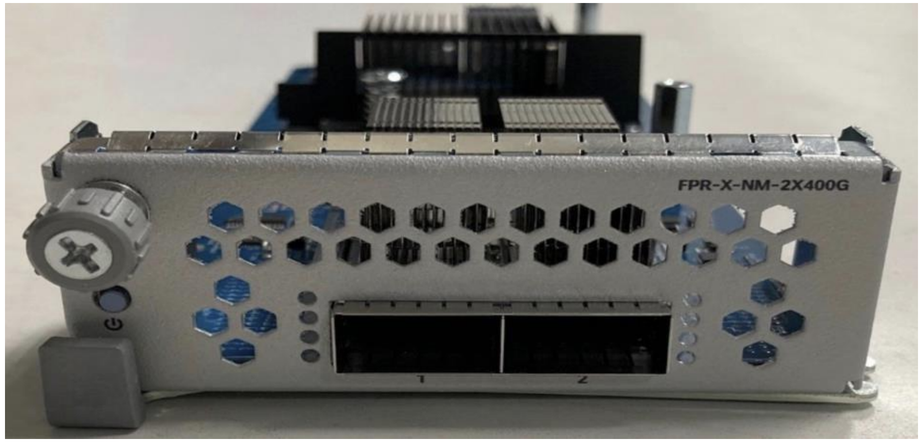
Also,

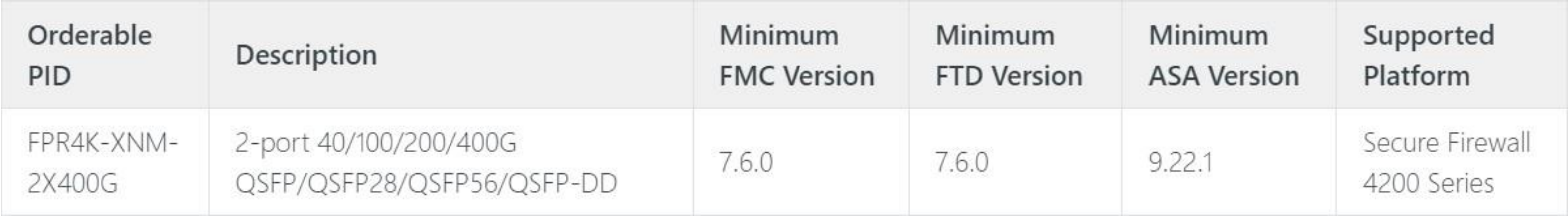
- New in this release is the ability to Convert the device from Native to Multi-Instance mode in FMC

FTD 7.6+
ASA 9.22+

2-Port 400 Gigabit Network Module

- Support for higher bandwidth requirements with a new 2-Port 400Gbps Network Module
- Hot pluggable – 2 x 40/100/200/400G
- Max. Bandwidth – 800Gbps (Full-duplex)





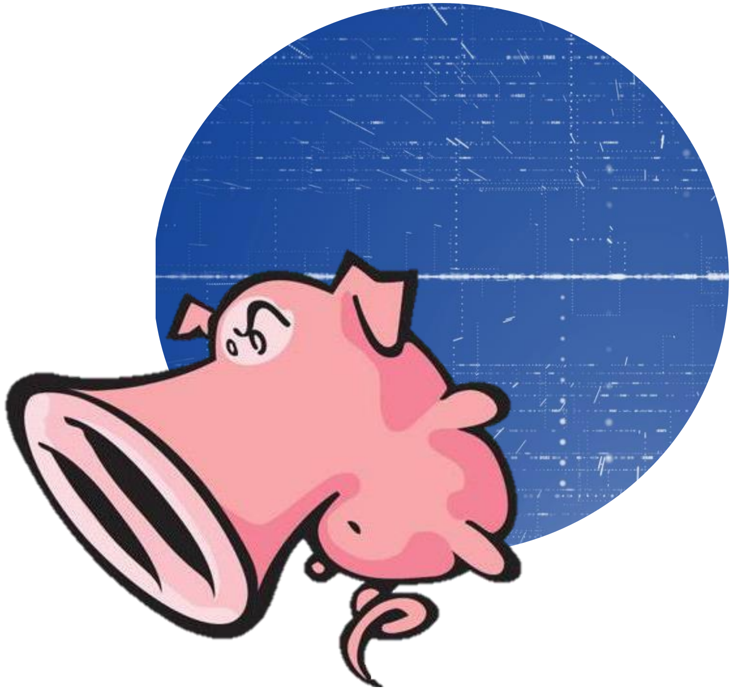
Orderable PID	Description	Minimum FMC Version	Minimum FTD Version	Minimum ASA Version	Supported Platform
FPR4K-XNM-2X400G	2-port 40/100/200/400G QSFP/QSFP28/QSFP56/QSFP-DD	7.6.0	7.6.0	9.22.1	Secure Firewall 4200 Series

Secure Firewall Threat Defense v7.6

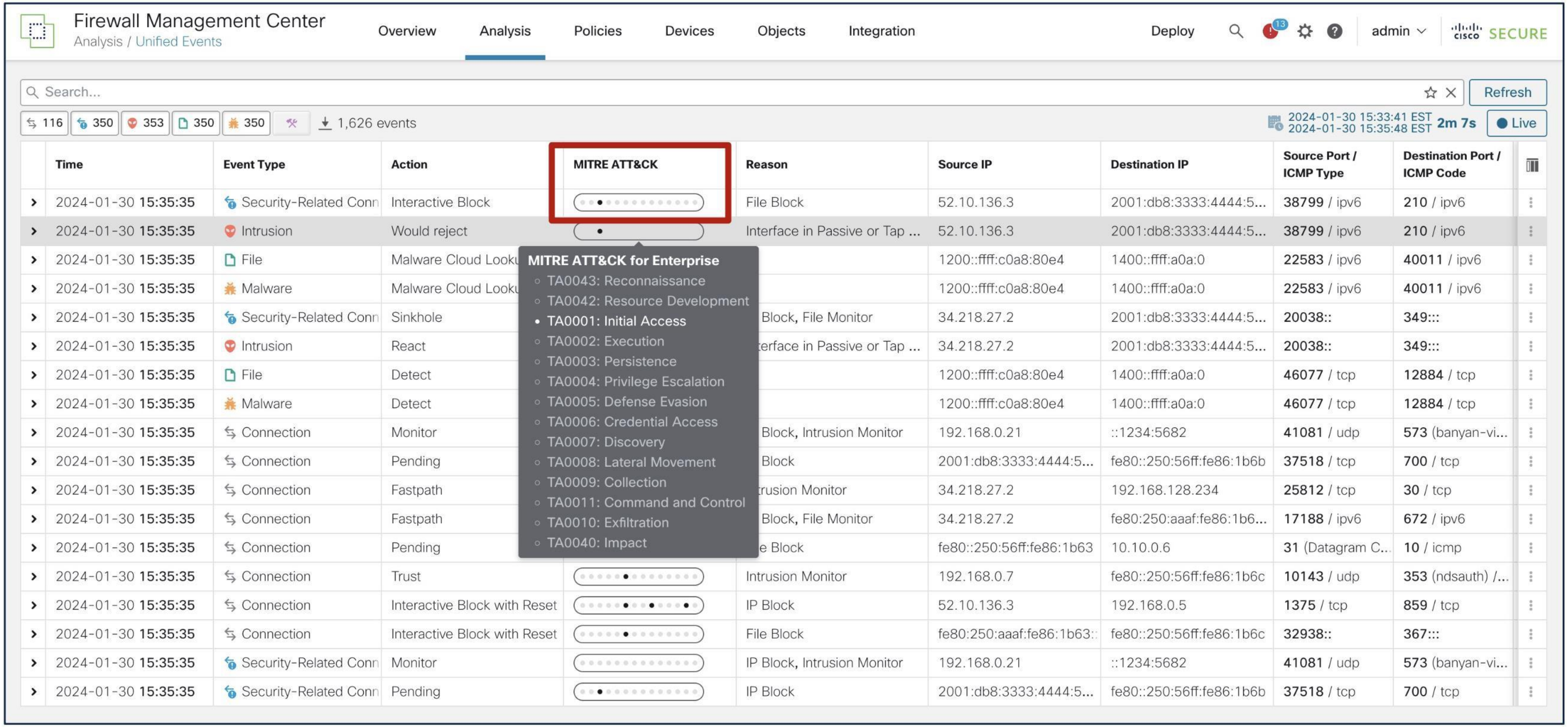
Machine Learning Exploit Detection

SnortML

- Traditional IPS rules are based on known and fixed patterns
  - Slight changes to payload patterns can evade static signatures
  - Undisclosed or new vulnerabilities take time to become signatures
- Neural detector uses machine learning to expand IPS capabilities
  - Detects known vulnerabilities and possible 0-days
  - Variants of known attack types without an individual Snort rule
  - Snort module looking at HTTP requests
- Machine learning algorithm trained continuously by Talos and delivered as a model file via LSP updates



Security Event Contextual Enrichment

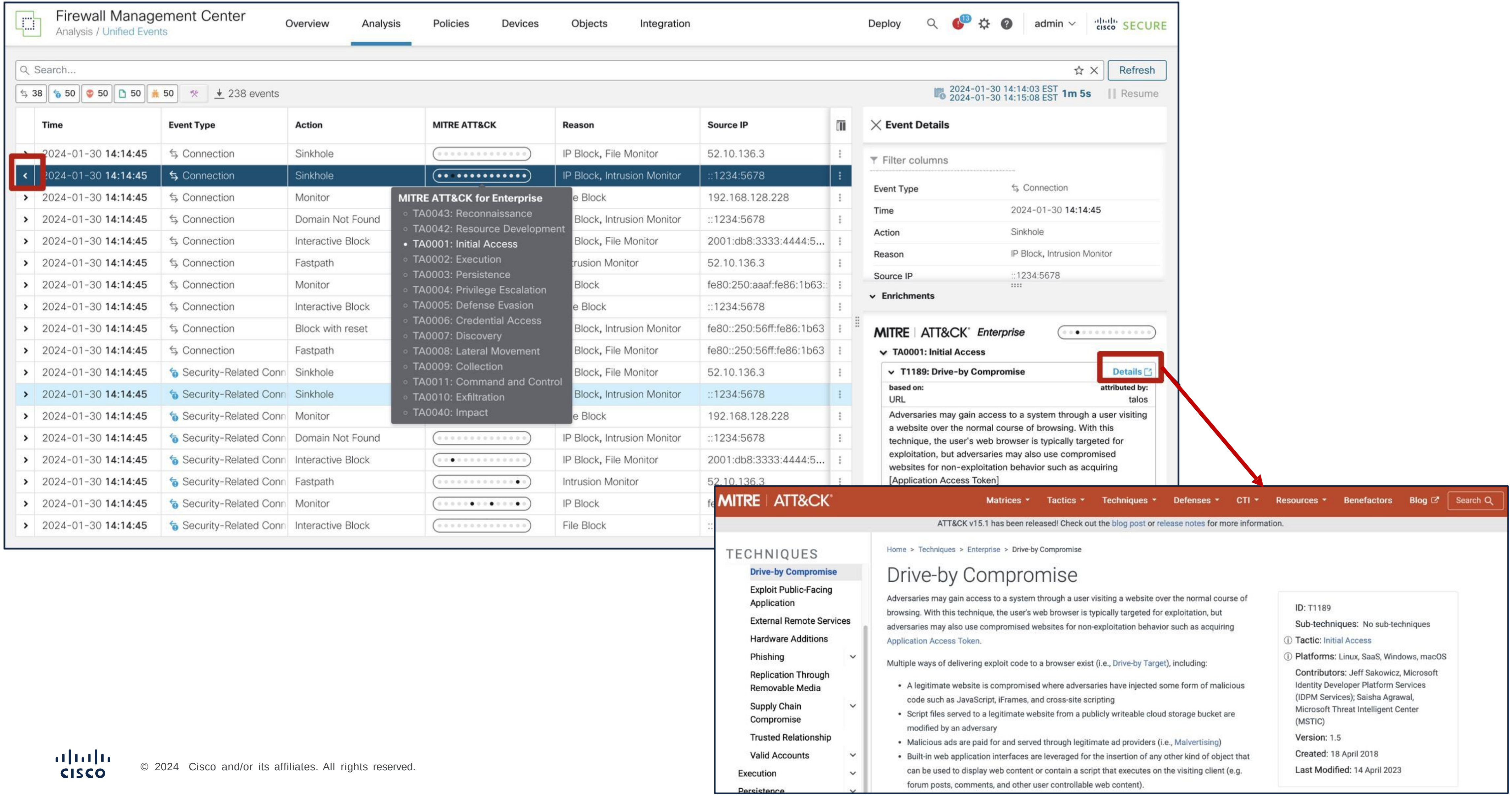


	Time	Event Type	Action	MITRE ATT&CK	Reason	Source IP	Destination IP	Source Port / ICMP Type	Destination Port / ICMP Code
›	2024-01-30 **15:35:35**	Security-Related Conn	Interactive Block	○○●○○○○○○○○○○○	File Block	52.10.136.3	2001:db8:3333:4444:5...	**38799** / ipv6	**210** / ipv6
›	2024-01-30 **15:35:35**	Intrusion	Would reject	●	Interface in Passive or Tap ...	52.10.136.3	2001:db8:3333:4444:5...	**38799** / ipv6	**210** / ipv6
›	2024-01-30 **15:35:35**	File	Malware Cloud Looku			1200::ffff:c0a8:80e4	1400::ffff:a0a:0	**22583** / ipv6	**40011** / ipv6
›	2024-01-30 **15:35:35**	Malware	Malware Cloud Looku			1200::ffff:c0a8:80e4	1400::ffff:a0a:0	**22583** / ipv6	**40011** / ipv6
›	2024-01-30 **15:35:35**	Security-Related Conn	Sinkhole		Block, File Monitor	34.218.27.2	2001:db8:3333:4444:5...	**20038**::	**349**:::
›	2024-01-30 **15:35:35**	Intrusion	React		terface in Passive or Tap ...	34.218.27.2	2001:db8:3333:4444:5...	**20038**::	**349**:::
›	2024-01-30 **15:35:35**	File	Detect			1200::ffff:c0a8:80e4	1400::ffff:a0a:0	**46077** / tcp	**12884** / tcp
›	2024-01-30 **15:35:35**	Malware	Detect			1200::ffff:c0a8:80e4	1400::ffff:a0a:0	**46077** / tcp	**12884** / tcp
›	2024-01-30 **15:35:35**	Connection	Monitor		Block, Intrusion Monitor	192.168.0.21	::1234:5682	**41081** / udp	**573** (banyan-vi...
›	2024-01-30 **15:35:35**	Connection	Pending		Block	2001:db8:3333:4444:5...	fe80::250:56ff:fe86:1b6b	**37518** / tcp	**700** / tcp
›	2024-01-30 **15:35:35**	Connection	Fastpath		rusion Monitor	34.218.27.2	192.168.128.234	**25812** / tcp	**30** / tcp
›	2024-01-30 **15:35:35**	Connection	Fastpath		Block, File Monitor	34.218.27.2	fe80:250:aaaf:fe86:1b6...	**17188** / ipv6	**672** / ipv6
›	2024-01-30 **15:35:35**	Connection	Pending		e Block	fe80::250:56ff:fe86:1b63	10.10.0.6	**31** (Datagram C...	**10** / icmp
›	2024-01-30 **15:35:35**	Connection	Trust	○○○○○●○○○○○○○○	Intrusion Monitor	192.168.0.7	fe80::250:56ff:fe86:1b6c	**10143** / udp	**353** (ndsauth) /...
›	2024-01-30 **15:35:35**	Connection	Interactive Block with Reset	○○○○○●○○●○○○●○	IP Block	52.10.136.3	192.168.0.5	**1375** / tcp	**859** / tcp
›	2024-01-30 **15:35:35**	Connection	Interactive Block with Reset	○○○○○●○○○○○○○○	File Block	fe80:250:aaaf:fe86:1b63::	fe80::250:56ff:fe86:1b6c	**32938**::	**367**:::
›	2024-01-30 **15:35:35**	Security-Related Conn	Monitor	○○○○○○○○○○○○○○	IP Block, Intrusion Monitor	192.168.0.21	::1234:5682	**41081** / udp	**573** (banyan-vi...
›	2024-01-30 **15:35:35**	Security-Related Conn	Pending	○○●○○○○○○○○○○○	IP Block	2001:db8:3333:4444:5...	fe80::250:56ff:fe86:1b6b	**37518** / tcp	**700** / tcp

MITRE ATT&CK for Enterprise

- ○ TA0043: Reconnaissance
- ○ TA0042: Resource Development
- ● TA0001: Initial Access
- ○ TA0002: Execution
- ○ TA0003: Persistence
- ○ TA0004: Privilege Escalation
- ○ TA0005: Defense Evasion
- ○ TA0006: Credential Access
- ○ TA0007: Discovery
- ○ TA0008: Lateral Movement
- ○ TA0009: Collection
- ○ TA0011: Command and Control
- ○ TA0010: Exfiltration
- ○ TA0040: Impact

Security Event Contextual Enrichment



Time	Event Type	Action	MITRE ATT&CK	Reason	Source IP
2024-01-30 **14:14:45**	Connection	Sinkhole		IP Block, File Monitor	52.10.136.3
2024-01-30 **14:14:45**	Connection	Sinkhole		IP Block, Intrusion Monitor	::1234:5678
2024-01-30 **14:14:45**	Connection	Monitor		e Block	192.168.128.228
2024-01-30 **14:14:45**	Connection	Domain Not Found		Block, Intrusion Monitor	::1234:5678
2024-01-30 **14:14:45**	Connection	Interactive Block		Block, File Monitor	2001:db8:3333:4444:5...
2024-01-30 **14:14:45**	Connection	Fastpath		rusion Monitor	52.10.136.3
2024-01-30 **14:14:45**	Connection	Monitor		Block	fe80:250:aaaf:fe86:1b63::
2024-01-30 **14:14:45**	Connection	Interactive Block		e Block	::1234:5678
2024-01-30 **14:14:45**	Connection	Block with reset		Block, Intrusion Monitor	fe80::250:56ff:fe86:1b63
2024-01-30 **14:14:45**	Connection	Fastpath		Block, File Monitor	fe80::250:56ff:fe86:1b63
2024-01-30 **14:14:45**	Security-Related Conn	Sinkhole		Block, File Monitor	52.10.136.3
2024-01-30 **14:14:45**	Security-Related Conn	Sinkhole		Block, Intrusion Monitor	::1234:5678
2024-01-30 **14:14:45**	Security-Related Conn	Monitor		e Block	192.168.128.228
2024-01-30 **14:14:45**	Security-Related Conn	Domain Not Found		IP Block, Intrusion Monitor	::1234:5678
2024-01-30 **14:14:45**	Security-Related Conn	Interactive Block		IP Block, File Monitor	2001:db8:3333:4444:5...
2024-01-30 **14:14:45**	Security-Related Conn	Fastpath		Intrusion Monitor	52.10.136.3
2024-01-30 **14:14:45**	Security-Related Conn	Monitor		IP Block	fe
2024-01-30 **14:14:45**	Security-Related Conn	Interactive Block		File Block	::

MITRE ATT&CK for Enterprise

- TA0043: Reconnaissance
- TA0042: Resource Development
- TA0001: Initial Access
- TA0002: Execution
- TA0003: Persistence
- TA0004: Privilege Escalation
- TA0005: Defense Evasion
- TA0006: Credential Access
- TA0007: Discovery
- TA0008: Lateral Movement
- TA0009: Collection
- TA0011: Command and Control
- TA0010: Exfiltration
- TA0040: Impact

Event Details

Filter columns

Event Type	Connection
Time	2024-01-30 **14:14:45**
Action	Sinkhole
Reason	IP Block, Intrusion Monitor
Source IP	::1234:5678

Enrichments

MITRE | ATT&CK *Enterprise*

TA0001: Initial Access

T1189: Drive-by Compromise Details

based on: URL

attributed by: talos

Adversaries may gain access to a system through a user visiting a website over the normal course of browsing. With this technique, the user's web browser is typically targeted for exploitation, but adversaries may also use compromised websites for non-exploitation behavior such as acquiring [Application Access Token]

ATT&CK v15.1 has been released! Check out the blog post or release notes for more information.

TECHNIQUES

- Drive-by Compromise
- Exploit Public-Facing Application
- External Remote Services
- Hardware Additions
- Phishing
- Replication Through Removable Media
- Supply Chain Compromise
- Trusted Relationship
- Valid Accounts
- Execution
- Persistence

Home > Techniques > Enterprise > Drive-by Compromise

Drive-by Compromise

Adversaries may gain access to a system through a user visiting a website over the normal course of browsing. With this technique, the user's web browser is typically targeted for exploitation, but adversaries may also use compromised websites for non-exploitation behavior such as acquiring Application Access Token.

Multiple ways of delivering exploit code to a browser exist (i.e., Drive-by Target), including:

- A legitimate website is compromised where adversaries have injected some form of malicious code such as JavaScript, iFrames, and cross-site scripting
- Script files served to a legitimate website from a publicly writeable cloud storage bucket are modified by an adversary
- Malicious ads are paid for and served through legitimate ad providers (i.e., Malvertising)
- Built-in web application interfaces are leveraged for the insertion of any other kind of object that can be used to display web content or contain a script that executes on the visiting client (e.g. forum posts, comments, and other user controllable web content).

ID: T1189

Sub-techniques: No sub-techniques

Tactic: Initial Access

Platforms: Linux, SaaS, Windows, macOS

Contributors: Jeff Sakowicz, Microsoft Identity Developer Platform Services (IDPM Services); Saisha Agrawal, Microsoft Threat Intelligent Center (MSTIC)

Version: 1.5

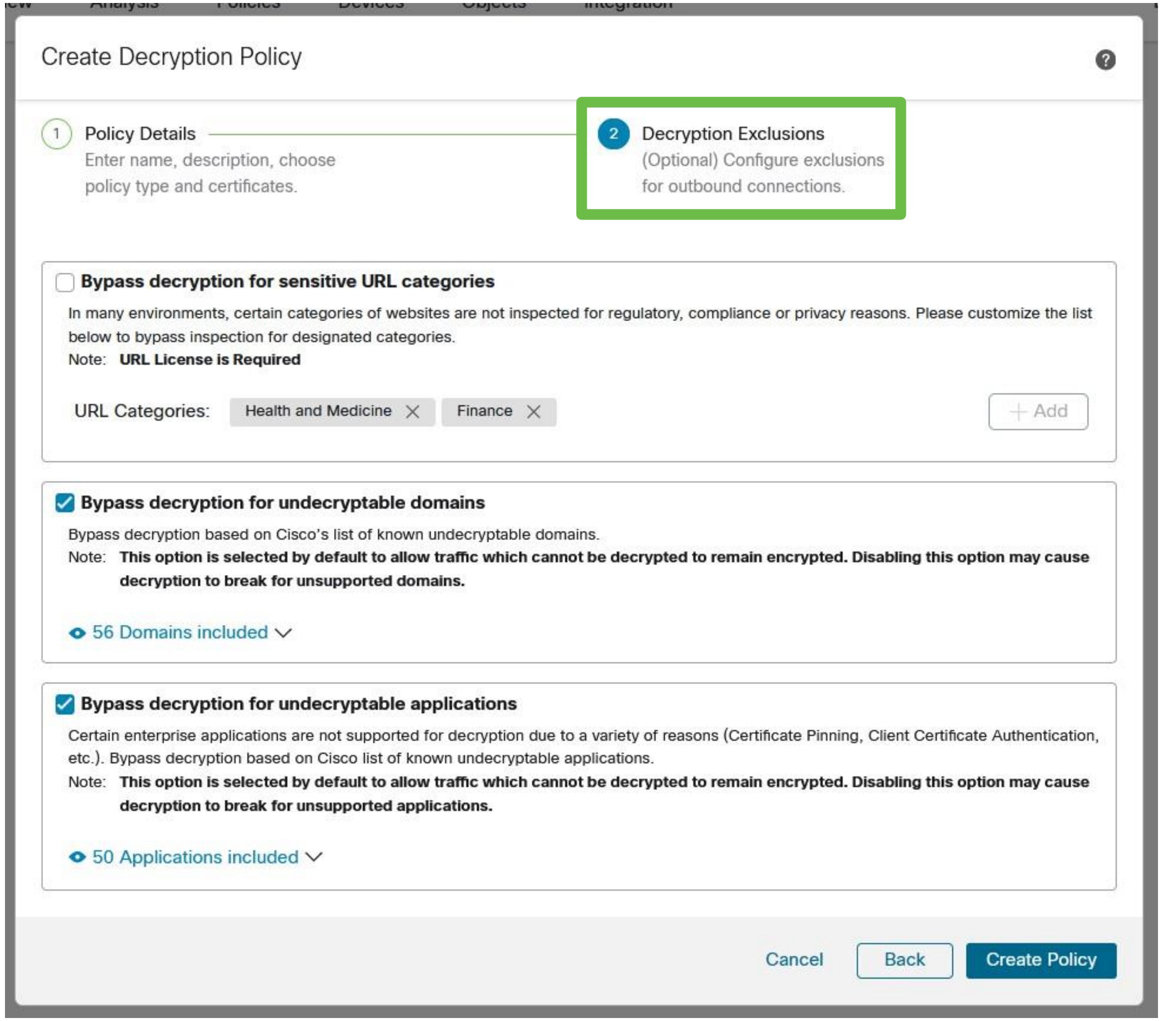
Created: 18 April 2018

Last Modified: 14 April 2023

Threat Protection

Decryption Tuning and Simplification

- Enhanced decryption policy wizard
  - New Decryption Exclusions section
  - Bypass decryption for sensitive URL categories (not enabled by default)
    - Quickly Add/Remove categories
  - Bypass decryption for undecryptable:
    - Domains
    - Applications



Create Decryption Policy

1 Policy Details
Enter name, description, choose policy type and certificates.

2 Decryption Exclusions
(Optional) Configure exclusions for outbound connections.

□ **Bypass decryption for sensitive URL categories**

In many environments, certain categories of websites are not inspected for regulatory, compliance or privacy reasons. Please customize the list below to bypass inspection for designated categories.

Note: **URL License is Required**

URL Categories: Health and Medicine ✕ Finance ✕ + Add

☑ **Bypass decryption for undecryptable domains**

Bypass decryption based on Cisco's list of known undecryptable domains.

Note: **This option is selected by default to allow traffic which cannot be decrypted to remain encrypted. Disabling this option may cause decryption to break for unsupported domains.**

56 Domains included

☑ **Bypass decryption for undecryptable applications**

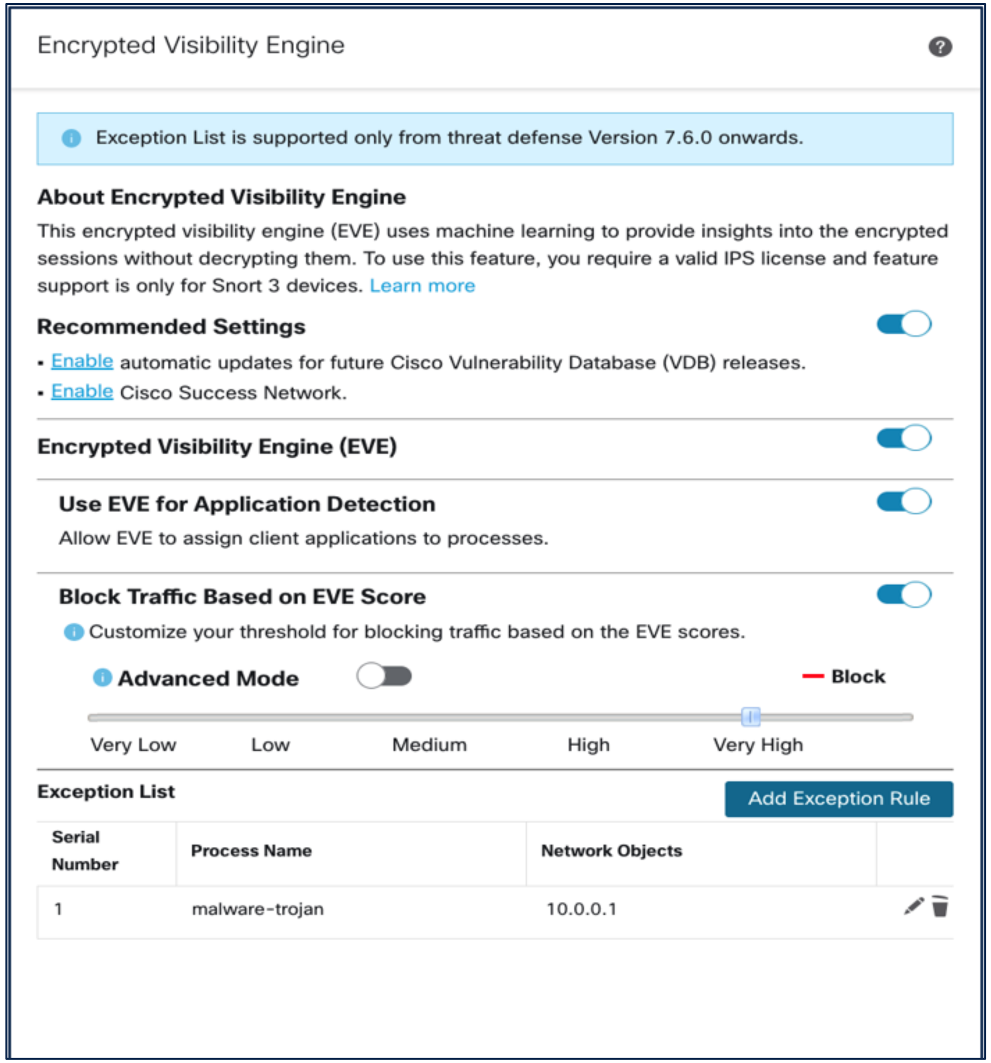
Certain enterprise applications are not supported for decryption due to a variety of reasons (Certificate Pinning, Client Certificate Authentication, etc.). Bypass decryption based on Cisco list of known undecryptable applications.

Note: **This option is selected by default to allow traffic which cannot be decrypted to remain encrypted. Disabling this option may cause decryption to break for unsupported applications.**

50 Applications included

Encrypted Visibility Engine Exceptions

- Encrypted Visibility Engine exclusion list
  - New option to define exceptions
  - Two exception categories:
    - Process Name
    - Network Object
  - Exceptions can be added directly from the Unified Event Viewer
    - Right-click “reason” column and select “Add EVE Exception Rule”
    - Option to review/modify before saving



Encrypted Visibility Engine

Exception List is supported only from threat defense Version 7.6.0 onwards.

About Encrypted Visibility Engine

This encrypted visibility engine (EVE) uses machine learning to provide insights into the encrypted sessions without decrypting them. To use this feature, you require a valid IPS license and feature support is only for Snort 3 devices. Learn more

Recommended Settings

- Enable automatic updates for future Cisco Vulnerability Database (VDB) releases.
- Enable Cisco Success Network.

Encrypted Visibility Engine (EVE)

Use EVE for Application Detection

Allow EVE to assign client applications to processes.

Block Traffic Based on EVE Score

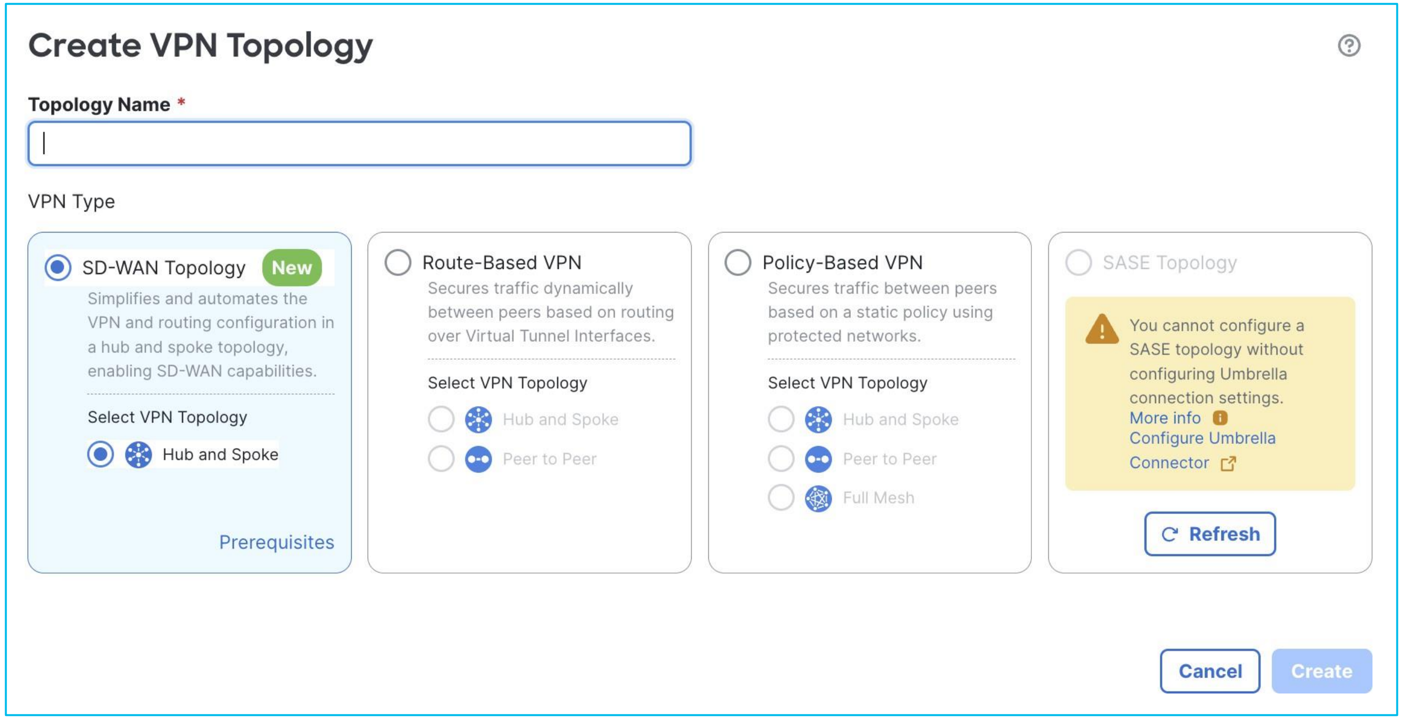
Customize your threshold for blocking traffic based on the EVE scores.

Exception List

Serial Number	Process Name	Network Objects
1	malware-trojan	10.0.0.1

SD-WAN Simplification

- New wizard-driven topology creation
  - Options for:
    - SD-WAN
    - Route / Policy-based VPNs
    - SASE (Umbrella)
  - Simplified Hub and Spoke topology definition
    - Auto-generation
    - Enable BGP on VPN overlay
    - Summary view of configuration



Create VPN Topology

Topology Name *

VPN Type

● SD-WAN Topology New
Simplifies and automates the VPN and routing configuration in a hub and spoke topology, enabling SD-WAN capabilities.
Select VPN Topology
● Hub and Spoke
Prerequisites

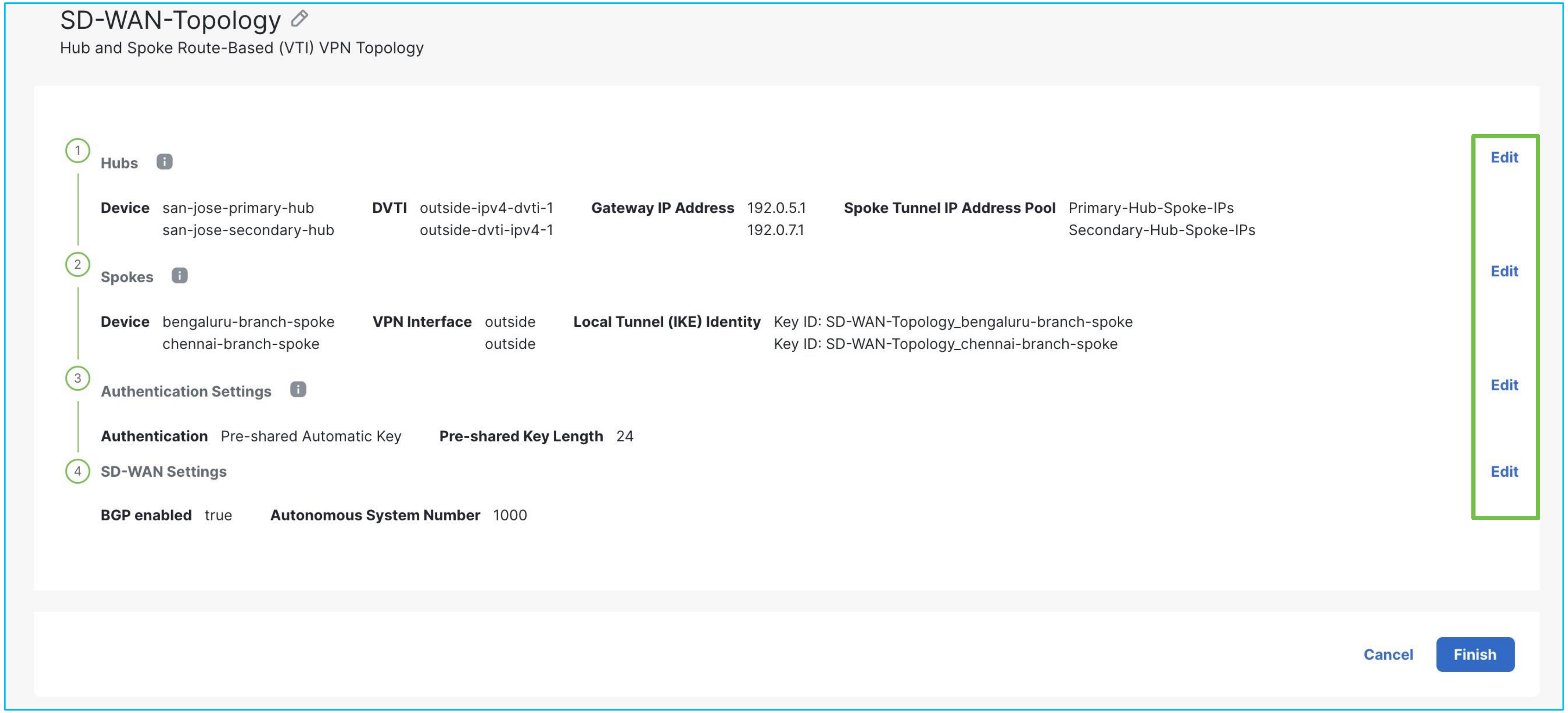
○ Route-Based VPN
Secures traffic dynamically between peers based on routing over Virtual Tunnel Interfaces.
Select VPN Topology
○ Hub and Spoke
○ Peer to Peer

○ Policy-Based VPN
Secures traffic between peers based on a static policy using protected networks.
Select VPN Topology
○ Hub and Spoke
○ Peer to Peer
○ Full Mesh

○ SASE Topology
You cannot configure a SASE topology without configuring Umbrella connection settings.
More info
Configure Umbrella Connector

SD-WAN Wizard Summary

- Users can modify any of the sections by clicking on the Edit icon to the right of each step



SD-WAN-Topology

Hub and Spoke Route-Based (VTI) VPN Topology

1 **Hubs** — Edit

Device		DVTI		Gateway IP Address		Spoke Tunnel IP Address Pool	
	san-jose-primary-hub san-jose-secondary-hub		outside-ipv4-dvti-1 outside-dvti-ipv4-1		192.0.5.1 192.0.7.1		Primary-Hub-Spoke-IPs Secondary-Hub-Spoke-IPs

2 **Spokes** — Edit

Device		VPN Interface		Local Tunnel (IKE) Identity	
	bengaluru-branch-spoke chennai-branch-spoke		outside outside		Key ID: SD-WAN-Topology_bengaluru-branch-spoke Key ID: SD-WAN-Topology_chennai-branch-spoke

3 **Authentication Settings** — Edit

Authentication Pre-shared Automatic Key **Pre-shared Key Length** 24

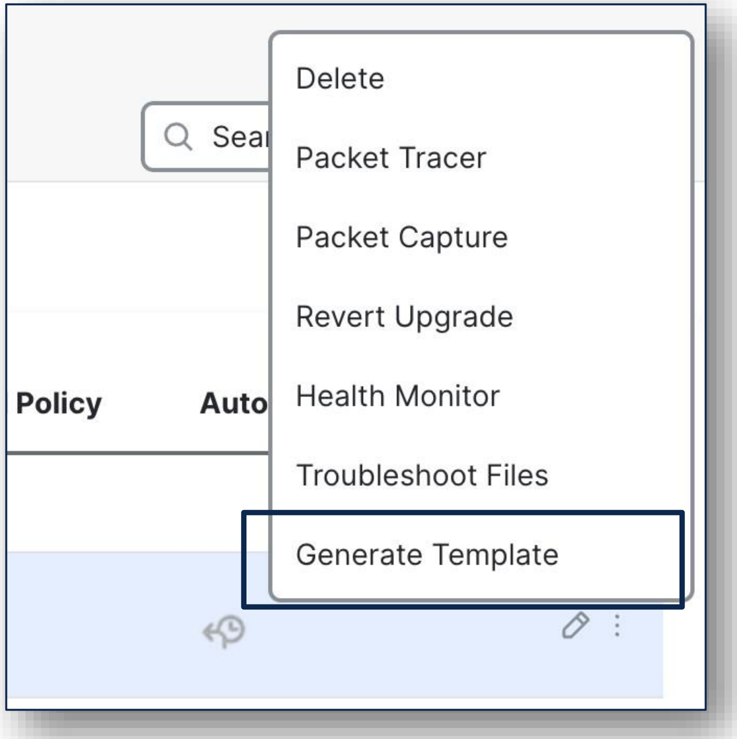
4 **SD-WAN Settings** — Edit

BGP enabled true **Autonomous System Number** 1000

SD-WAN

Device Templates for Bulk Provisioning

- Simplify SD-WAN/Branch rollouts at scale with Low-touch provisioning and device templates



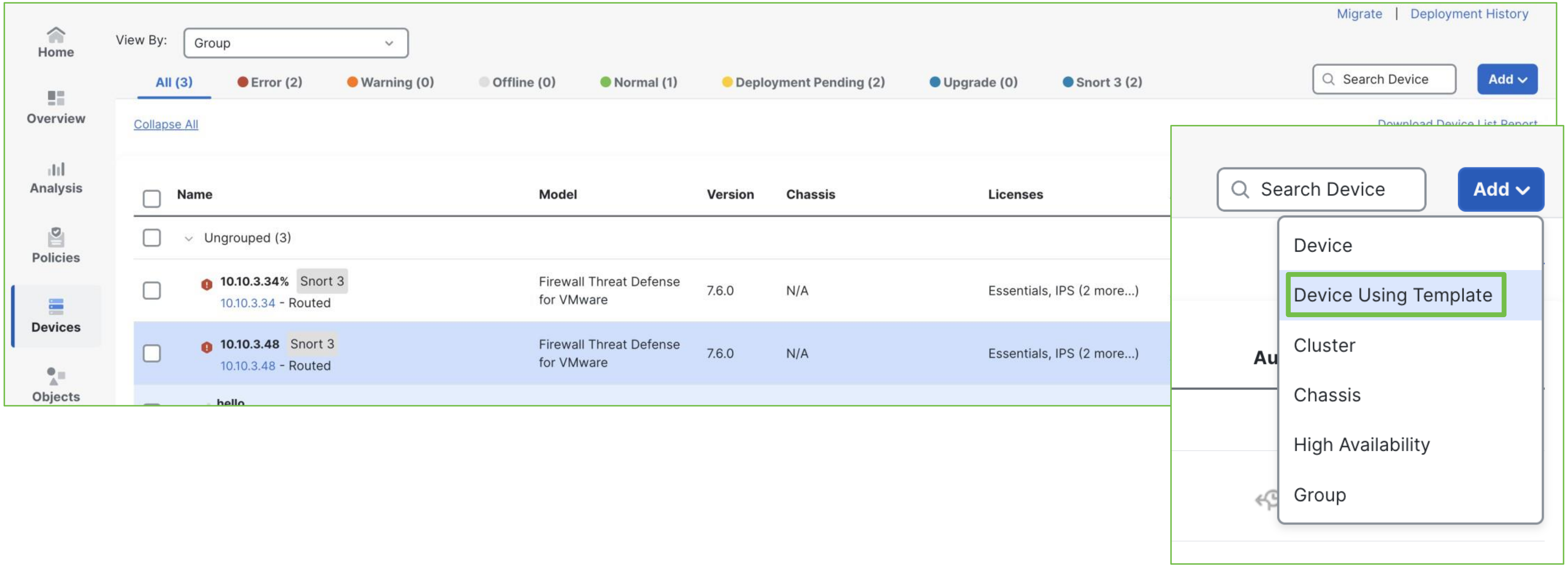
Create a new template

Generate from an existing device

Clone an existing template from one FMC to another

Device Templates for Bulk Provisioning

- New wizard for bulk pre-provisioning of devices using templates



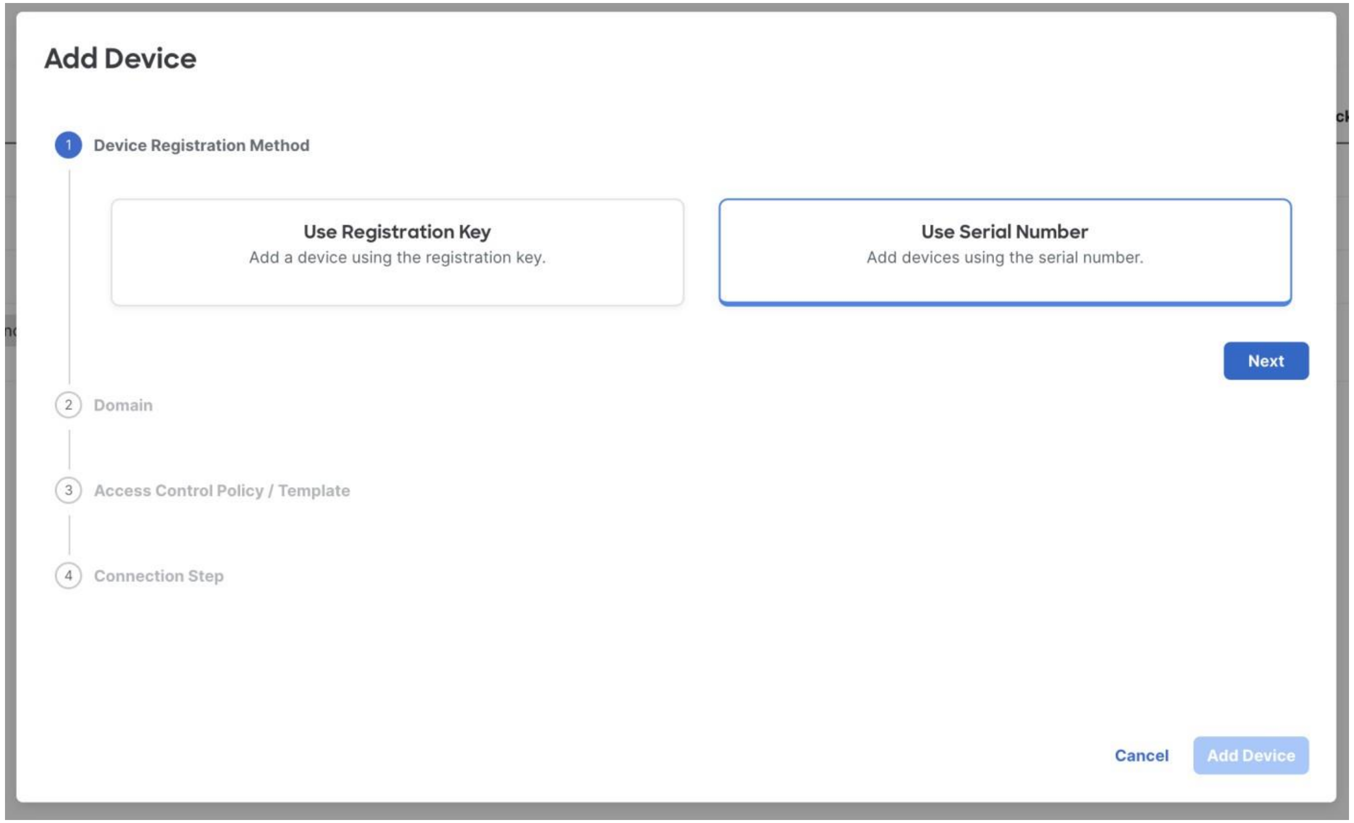
□	Name	Model	Version	Chassis	Licenses
□	Ungrouped (3)				
□	10.10.3.34% Snort 3 10.10.3.34 - Routed	Firewall Threat Defense for VMware	7.6.0	N/A	Essentials, IPS (2 more...)
□	10.10.3.48 Snort 3 10.10.3.48 - Routed	Firewall Threat Defense for VMware	7.6.0	N/A	Essentials, IPS (2 more...)
□	hello				

Device Templates for Bulk Provisioning

New Add device/devices wizard

The wizard has 4 steps:

1. Device registration method selection
2. Domain Selection
3. Template / Access Policy selection
4. File Upload



Add Device

1 Device Registration Method

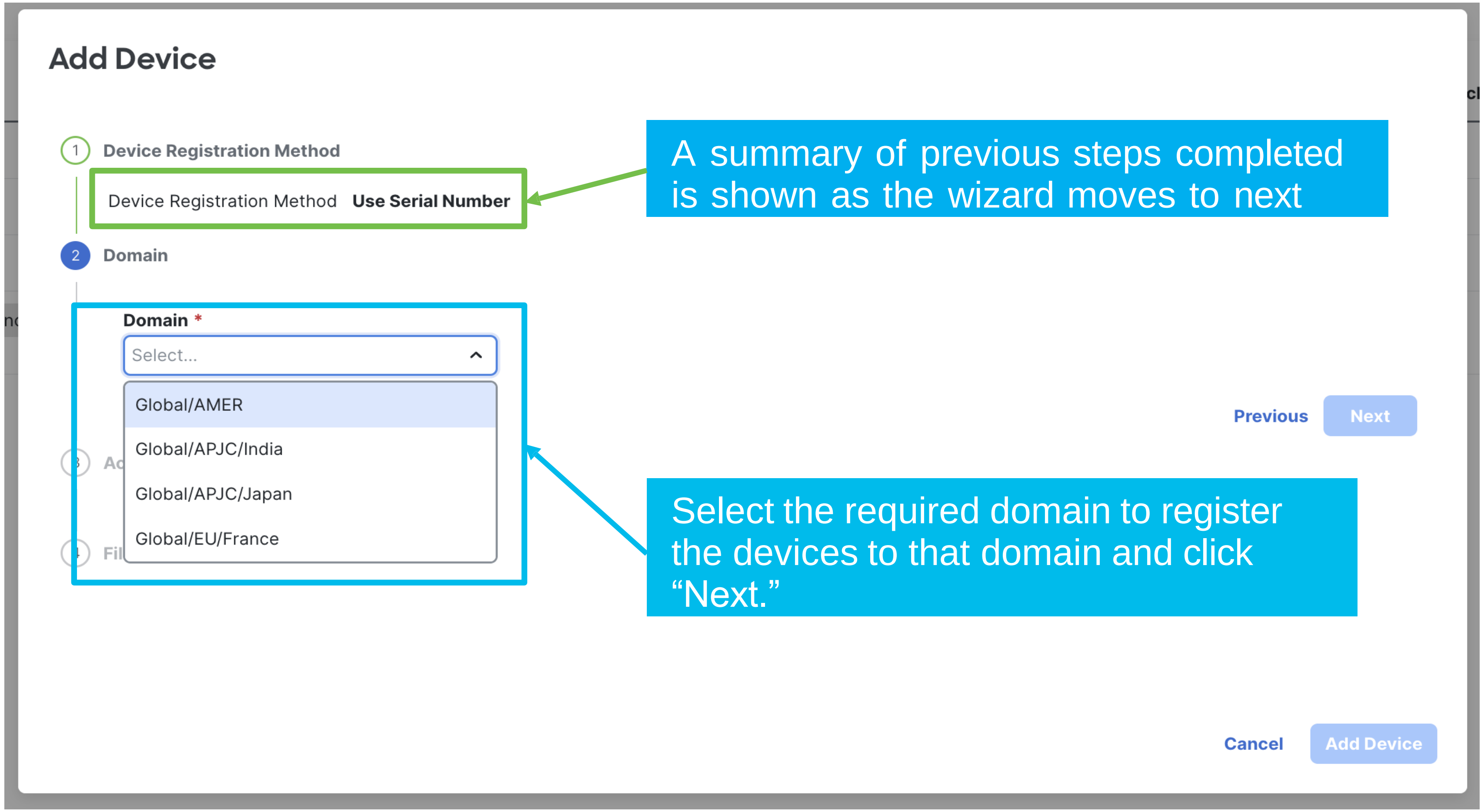
Use Registration Key
Add a device using the registration key.

Use Serial Number
Add devices using the serial number.

SD-WAN

Device Templates for Bulk Provisioning

- Domain selection – not applicable if Domains are not in use



Add Device

1 Device Registration Method

Device Registration Method **Use Serial Number**

2 Domain

Domain *

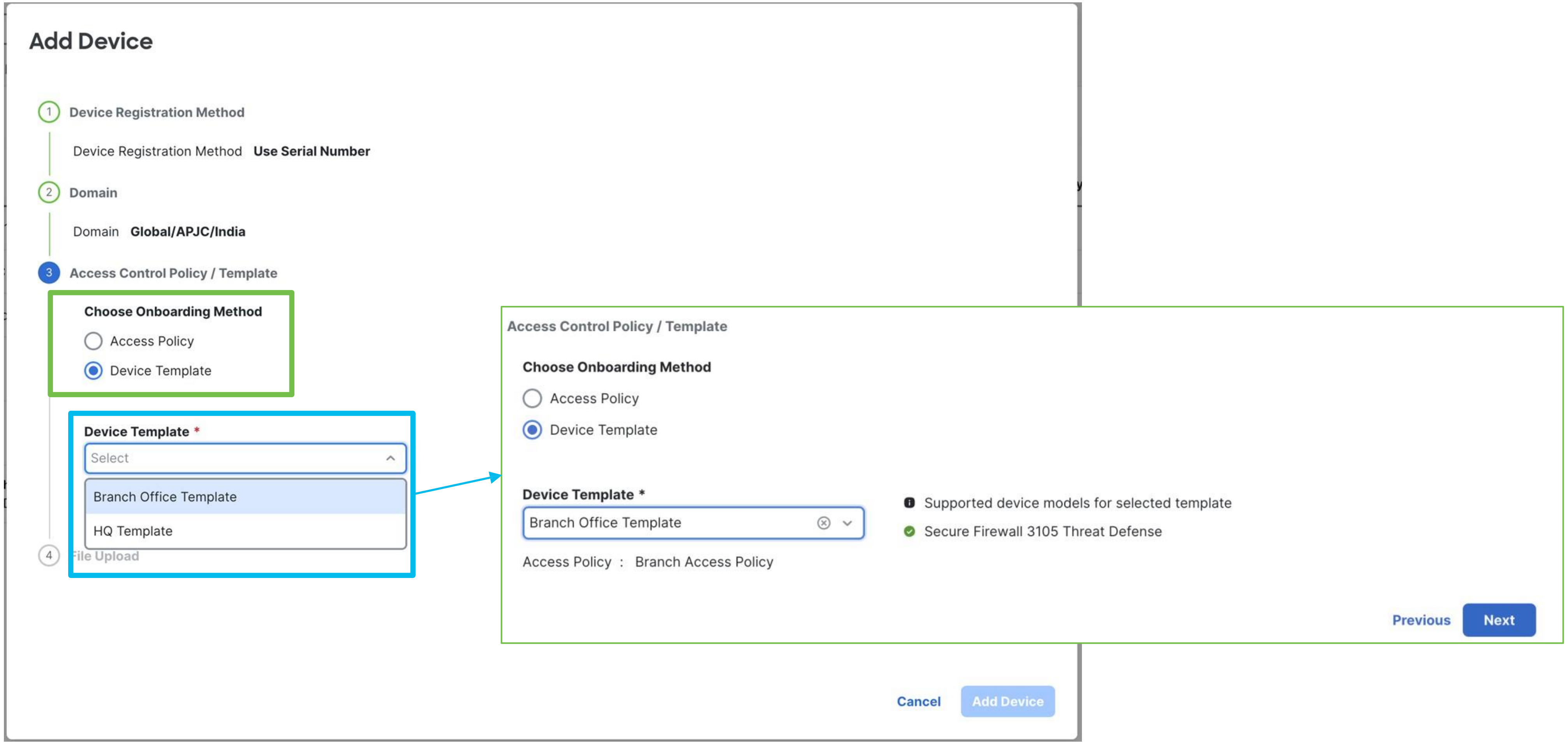
Select...

A summary of previous steps completed is shown as the wizard moves to next

Select the required domain to register the devices to that domain and click “Next.”

Device Templates for Bulk Provisioning

- Template selection



Add Device

1 Device Registration Method

Device Registration Method **Use Serial Number**

2 Domain

Domain **Global/APJC/India**

3 Access Control Policy / Template

Choose Onboarding Method

○ Access Policy

● Device Template

Device Template *

Select

Branch Office Template

HQ Template

4 File Upload

Cancel | Add Device

Access Control Policy / Template

Choose Onboarding Method

○ Access Policy

● Device Template

Device Template *

Branch Office Template

Supported device models for selected template

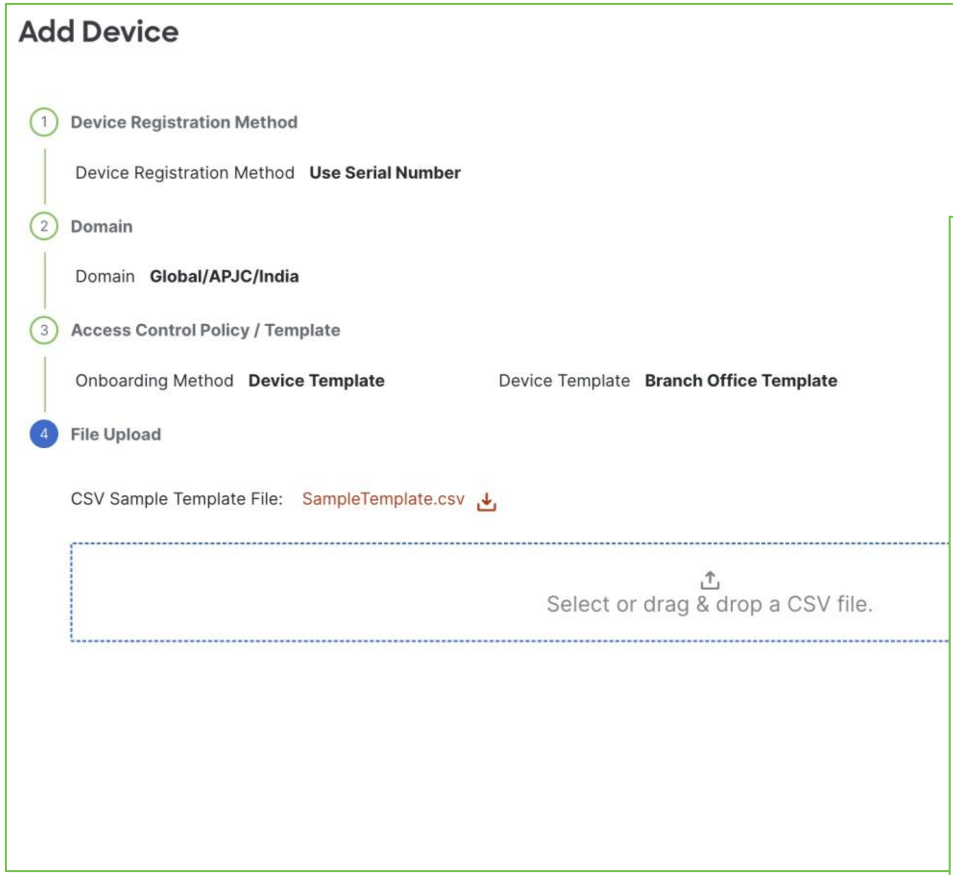
✓ Secure Firewall 3105 Threat Defense

Access Policy : Branch Access Policy

Previous | Next

Device Templates for Bulk Provisioning

- File Upload – used for provisioning bulk devices



Add Device

1. Device Registration Method

   Device Registration Method **Use Serial Number**

2. Domain

   Domain **Global/APJC/India**

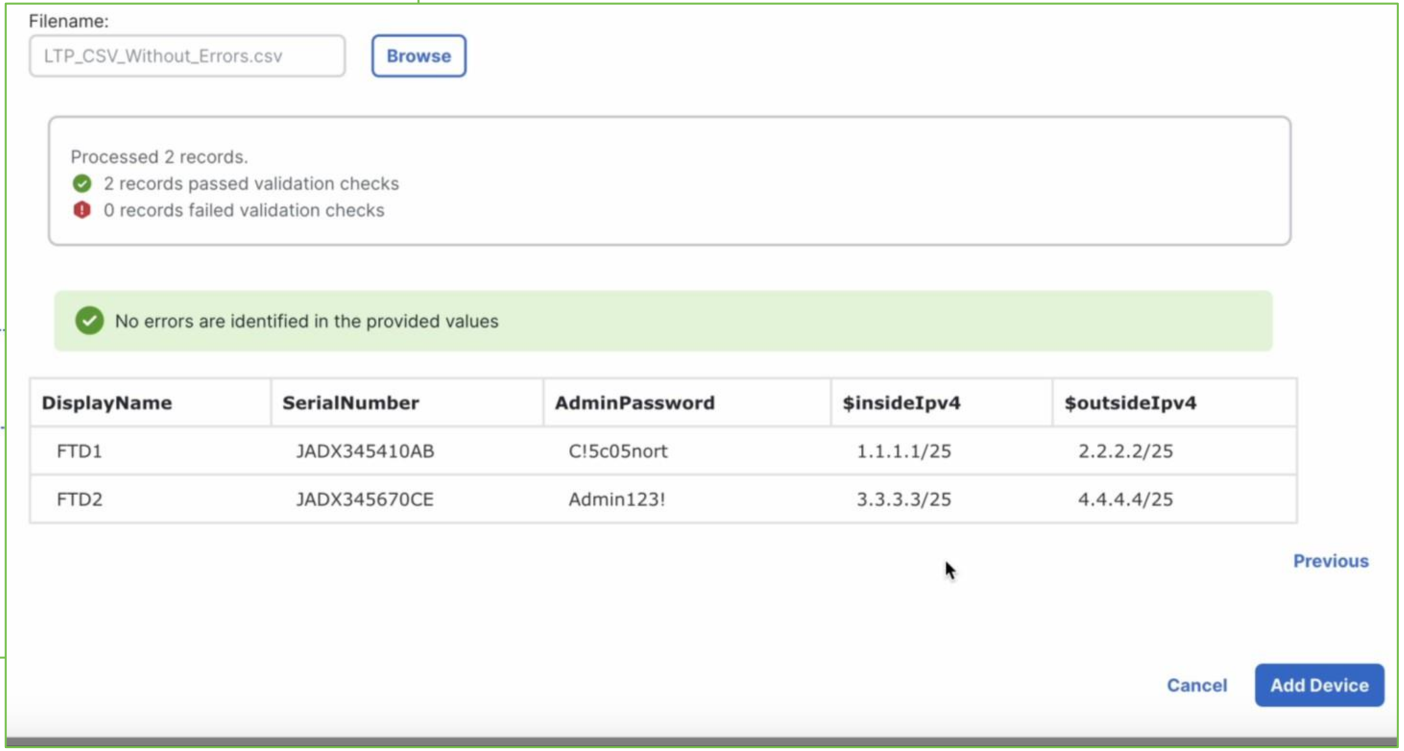
3. Access Control Policy / Template

   Onboarding Method **Device Template** Device Template **Branch Office Template**

4. File Upload

   CSV Sample Template File: SampleTemplate.csv

   Select or drag & drop a CSV file.



Filename: LTP_CSV_Without_Errors.csv

Processed 2 records.
✓ 2 records passed validation checks
! 0 records failed validation checks

✓ No errors are identified in the provided values

DisplayName	SerialNumber	AdminPassword	$insideIpv4	$outsideIpv4
FTD1	JADX345410AB	C!5c05nort	1.1.1.1/25	2.2.2.2/25
FTD2	JADX345670CE	Admin123!	3.3.3.3/25	4.4.4.4/25

Artificial Intelligence / Machine Learning

Enhanced User Experience

Cisco Cloud Onboarding

Cisco Defense Orchestrator (CDO) has replaced SecureX to allow customers to onboard FMC/FTD to Cisco Security Cloud.

- CDO now authorizes the FMC device to onboard to the cloud.
- SecureX registered FMCs/FTDs will continue to stay connected to Cisco Security Cloud, and for customers that have it enabled prior to 7.6, the integration will be seamlessly migrated over to CDO
- FMC to CDO integration required for advanced cloud features such as Policy Analyzer and AI Assistant

New to Secure Firewall 7.6

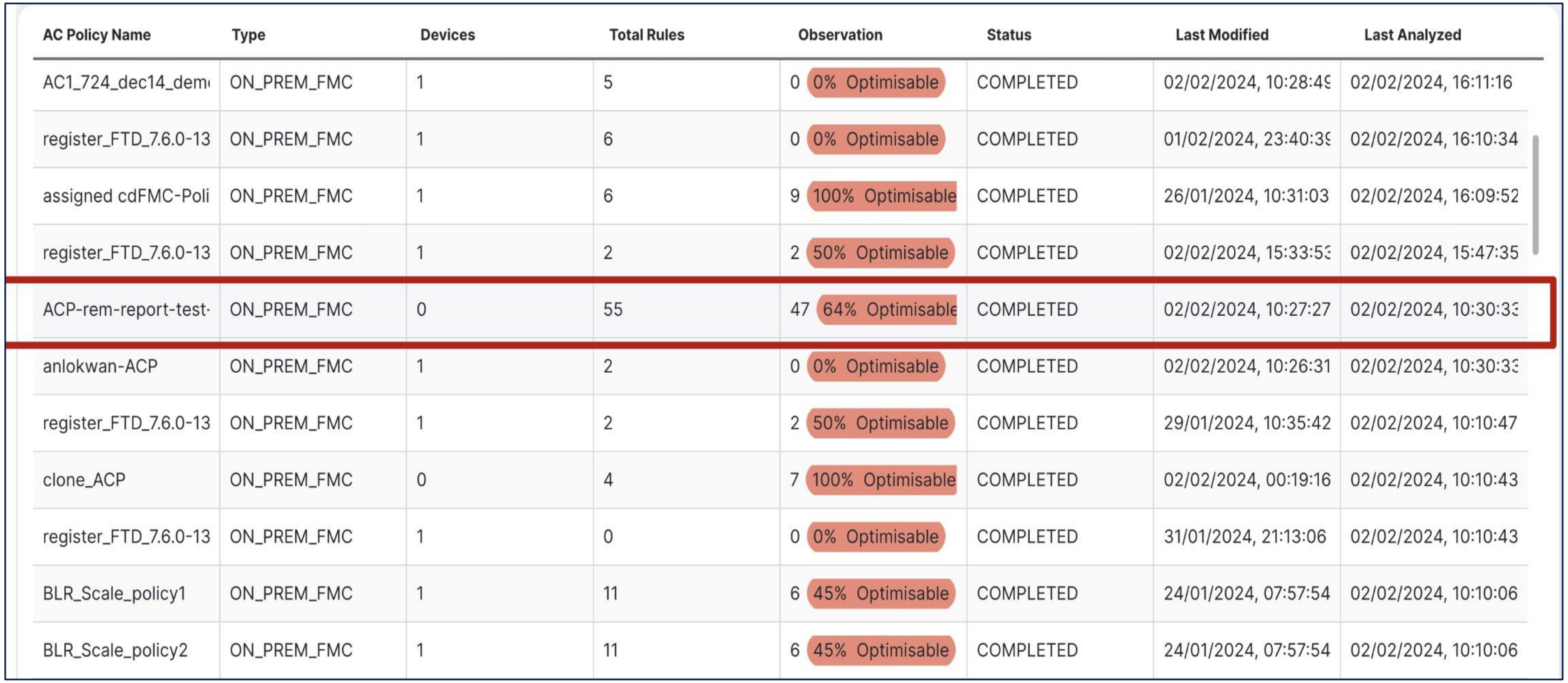
- FMC is registered to CDO by enabling Cisco Security Cloud
- CDO authorizes FMC during Cloud Onboarding
- SecureX ribbon is gone

Artificial Intelligence / Machine Learning

Enhanced User Experience

Policy Analyzer and Optimizer for on-premise and cloud-delivered Firewall Management Center

- Analysis
- Remediation
- Reporting



AC Policy Name	Type	Devices	Total Rules	Observation	Status	Last Modified	Last Analyzed
AC1_724_dec14_dem	ON_PREM_FMC	1	5	0 0% Optimisable	COMPLETED	02/02/2024, 10:28:49	02/02/2024, 16:11:16
register_FTD_7.6.0-13	ON_PREM_FMC	1	6	0 0% Optimisable	COMPLETED	01/02/2024, 23:40:39	02/02/2024, 16:10:34
assigned cdFMC-Poli	ON_PREM_FMC	1	6	9 100% Optimisable	COMPLETED	26/01/2024, 10:31:03	02/02/2024, 16:09:52
register_FTD_7.6.0-13	ON_PREM_FMC	1	2	2 50% Optimisable	COMPLETED	02/02/2024, 15:33:53	02/02/2024, 15:47:35
ACP-rem-report-test-	ON_PREM_FMC	0	55	47 64% Optimisable	COMPLETED	02/02/2024, 10:27:27	02/02/2024, 10:30:33
anlokwan-ACP	ON_PREM_FMC	1	2	0 0% Optimisable	COMPLETED	02/02/2024, 10:26:31	02/02/2024, 10:30:33
register_FTD_7.6.0-13	ON_PREM_FMC	1	2	2 50% Optimisable	COMPLETED	29/01/2024, 10:35:42	02/02/2024, 10:10:47
clone_ACP	ON_PREM_FMC	0	4	7 100% Optimisable	COMPLETED	02/02/2024, 00:19:16	02/02/2024, 10:10:43
register_FTD_7.6.0-13	ON_PREM_FMC	1	0	0 0% Optimisable	COMPLETED	31/01/2024, 21:13:06	02/02/2024, 10:10:43
BLR_Scale_policy1	ON_PREM_FMC	1	11	6 45% Optimisable	COMPLETED	24/01/2024, 07:57:54	02/02/2024, 10:10:06
BLR_Scale_policy2	ON_PREM_FMC	1	11	6 45% Optimisable	COMPLETED	24/01/2024, 07:57:54	02/02/2024, 10:10:06

* For On Prem FMC, the FMC should be onboarded/integrated with Cisco Defense Orchestrator.

Artificial Intelligence / Machine Learning

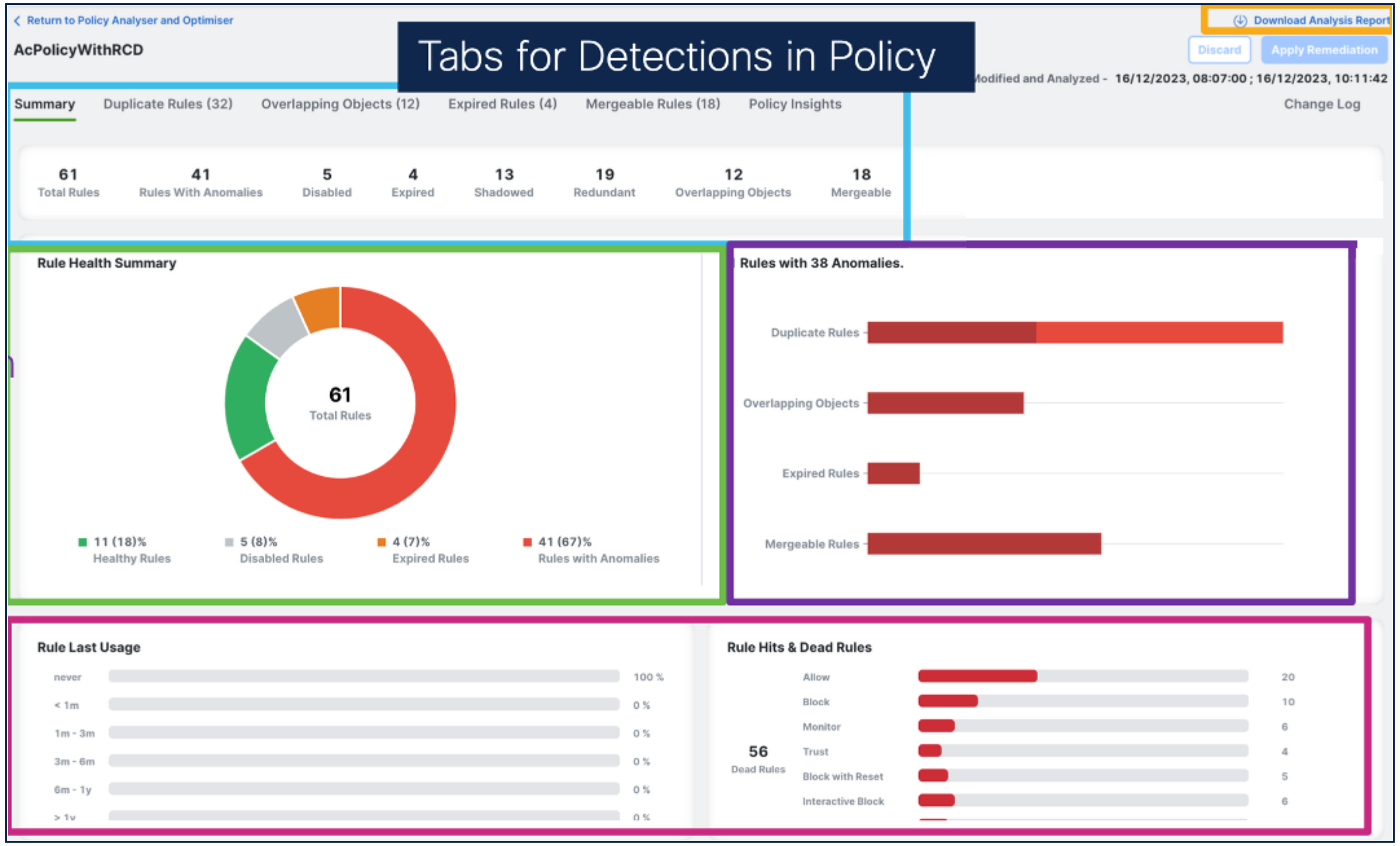
Enhanced User Experience

Policy Analyzer and Optimizer

Rule Health

Graphical Summary

Rule Hit Insights



Tabs for Detections in Policy

< Return to Policy Analyser and Optimiser

AcPolicyWithRCD

Modified and Analyzed - 16/12/2023, 08:07:00 ; 16/12/2023, 10:11:42

61	41	5	4	13	19	12	18
Total Rules	Rules With Anomalies	Disabled	Expired	Shadowed	Redundant	Overlapping Objects	Mergeable

Rule Health Summary

🟩 11 (18)% Healthy Rules
▨ 5 (8)% Disabled Rules
🟧 4 (7)% Expired Rules
🟥 41 (67)% Rules with Anomalies

Rules with 38 Anomalies.

Rule Last Usage

never	100 %
< 1m	0 %
1m - 3m	0 %
3m - 6m	0 %
6m - 1y	0 %
> 1y	0 %

Rule Hits & Dead Rules

56
Dead Rules

Allow	20
Block	10
Monitor	6
Trust	4
Block with Reset	5
Interactive Block	6

Report Download

Anomalies

Rule Hit Insights

Artificial Intelligence / Machine Learning

Enhanced User Experience

AI Assistant

Assist

Policy and reporting

Find and report information on policies for faster queries, auditing, and reporting

Augment

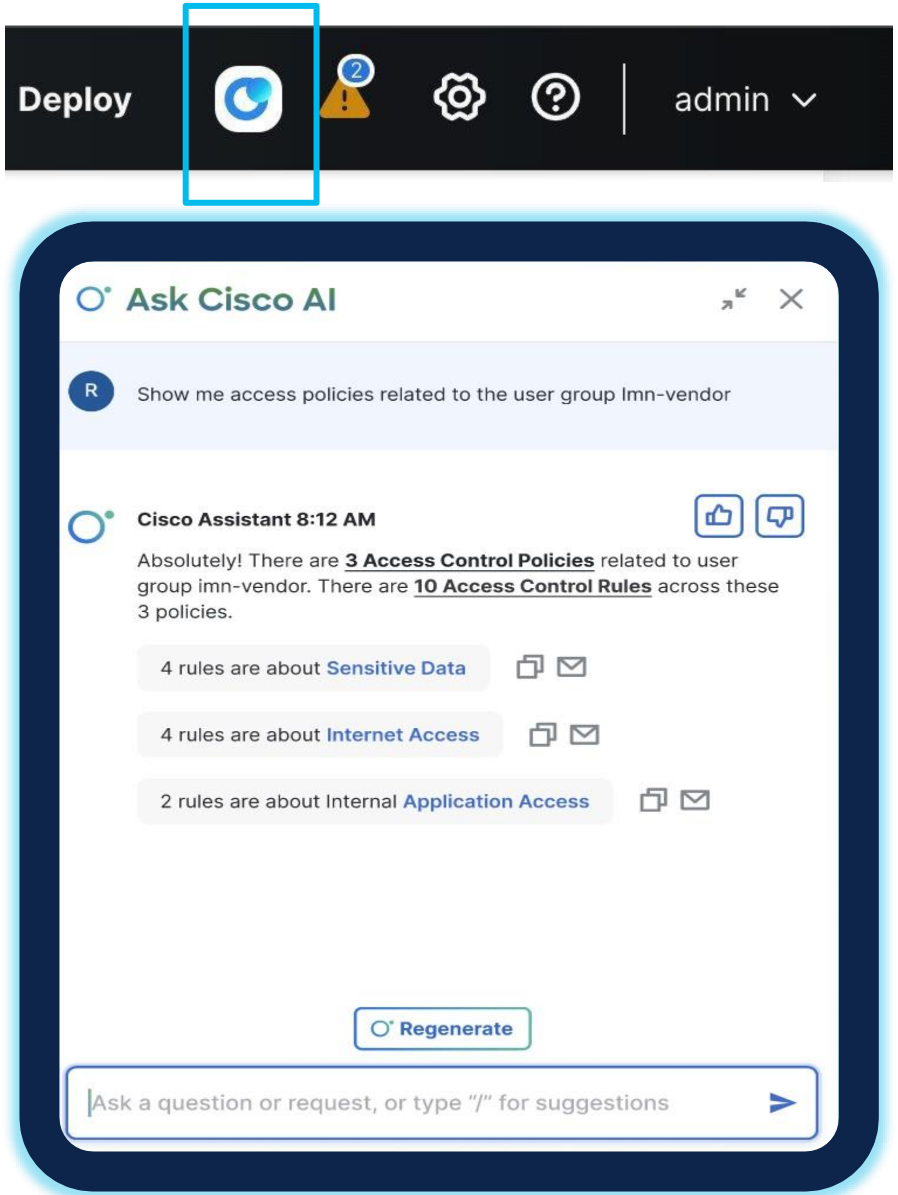
Troubleshooting and detection

Amalgamate all user guides for expedited resolution

Automate

Policy lifecycle management

Find and fix firewall rule misconfigurations for improved security and performance



Ask Cisco AI

R Show me access policies related to the user group lmn-vendor

Cisco Assistant 8:12 AM

Absolutely! There are **3 Access Control Policies** related to user group imn-vendor. There are **10 Access Control Rules** across these 3 policies.

4 rules are about Sensitive Data

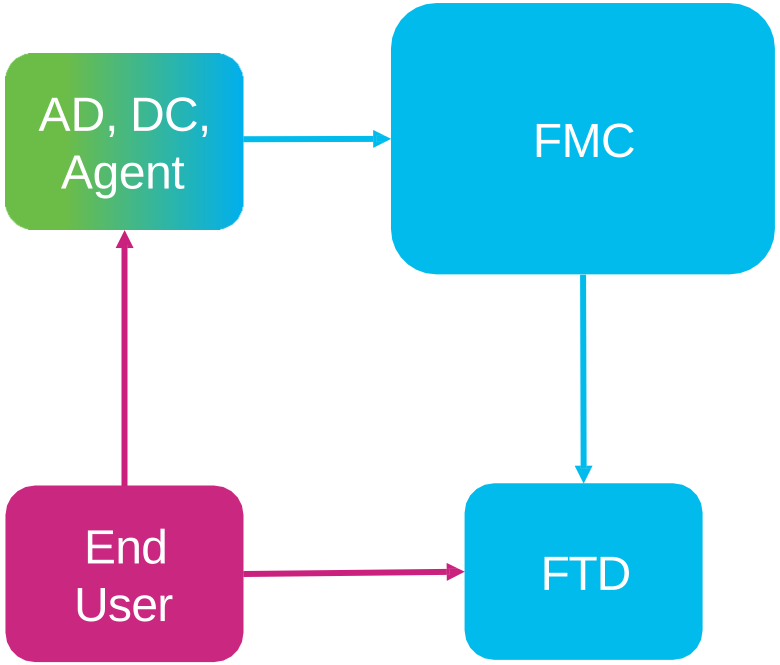
4 rules are about Internet Access

2 rules are about Internal Application Access

Identity Enhancements

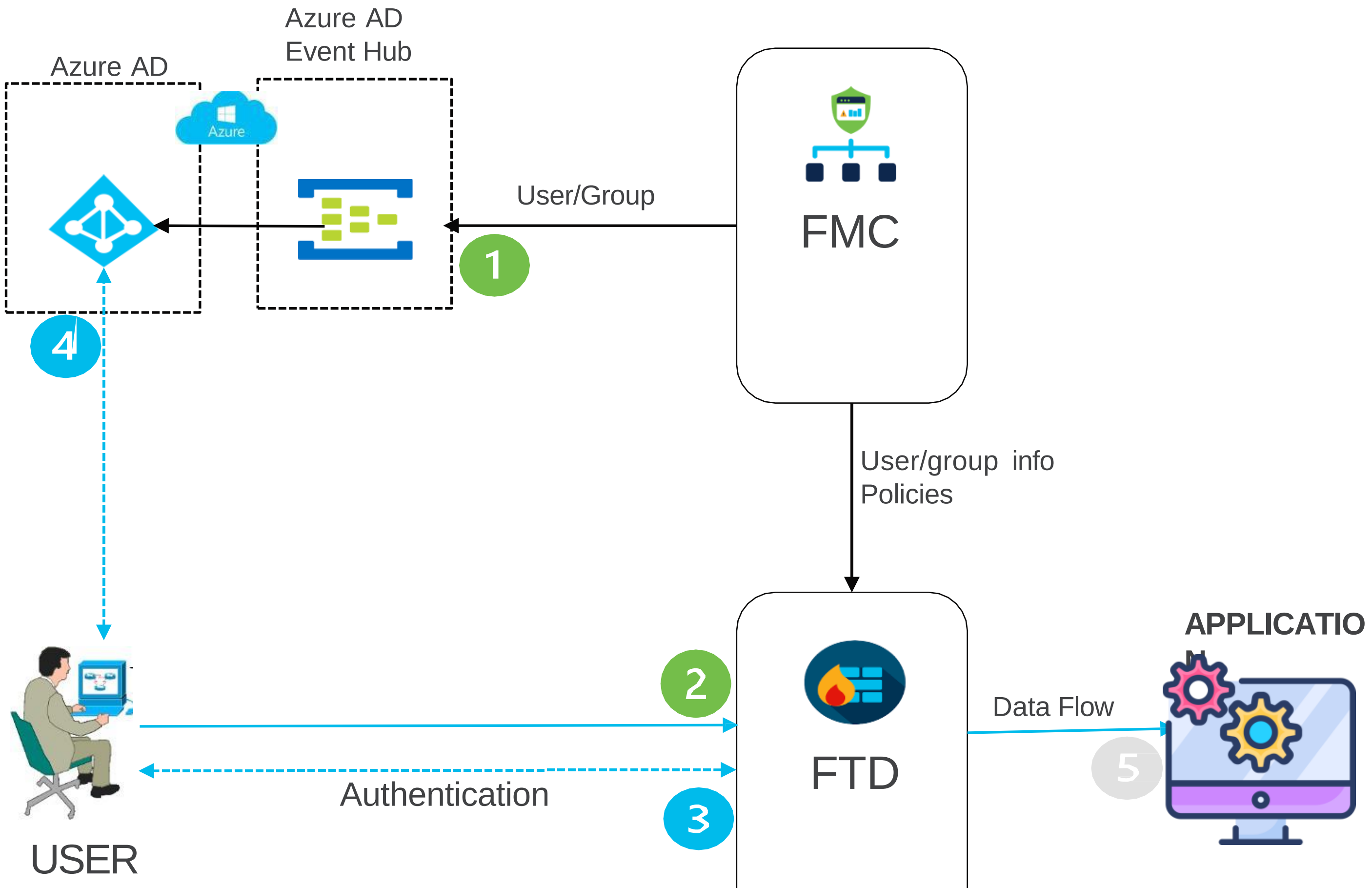
Passive Identity direct from MS Active Directory

- The Passive Identity Agent is an executable which reads end-user log on events from Active Directory (AD) and sends session data to an FMC.
  - The Passive Identity Agent is installed on a Windows machine that is joined to an AD.
- The Agent is configured on FMC and is designed to work with FTDs that are compatible with FMC 7.6.0.



Identity Enhancements

MS Azure Active Directory Active Authorization



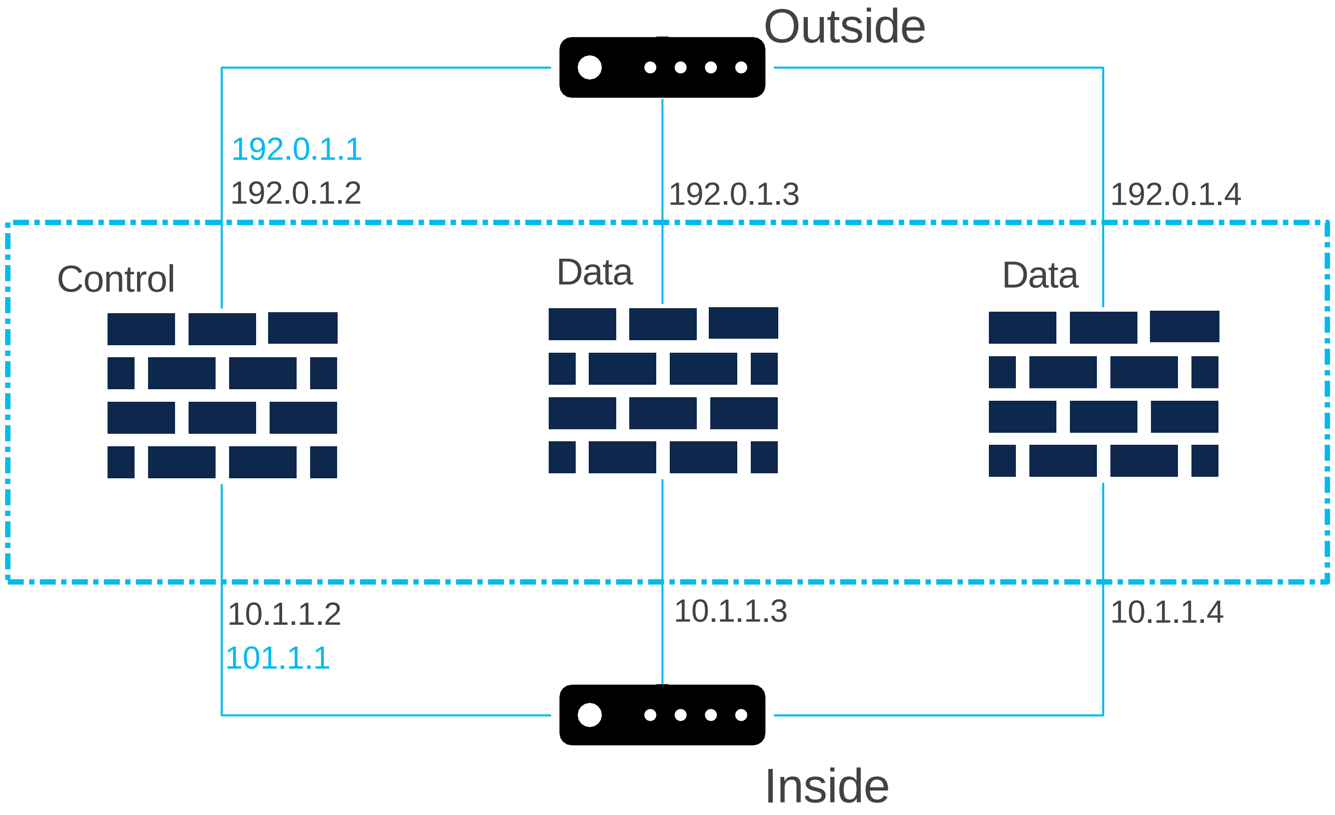
Cluster
FTD7.6+

Cluster Enhancements

Layer 3 insertion within hybrid data centers

Individual Interface Mode

- Layer 3
- Load-balancing via PBR or ECMP
- Routed mode
- 3100/4200/FTDv

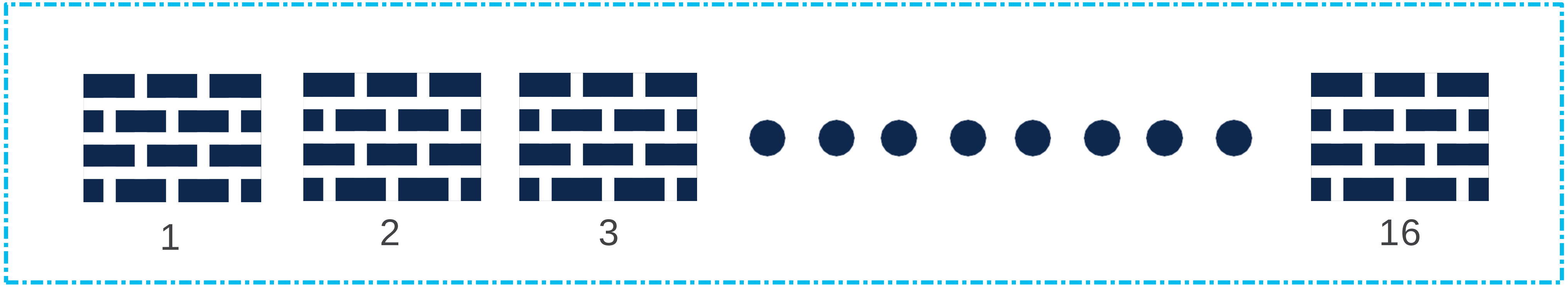


Cluster
FTD7.6+

Cluster Enhancements

Increased Cluster Scale for 3100 & 4200 series firewalls

- Scale up to 16 nodes (previously 8) in a single cluster
- Superior resilience and performance



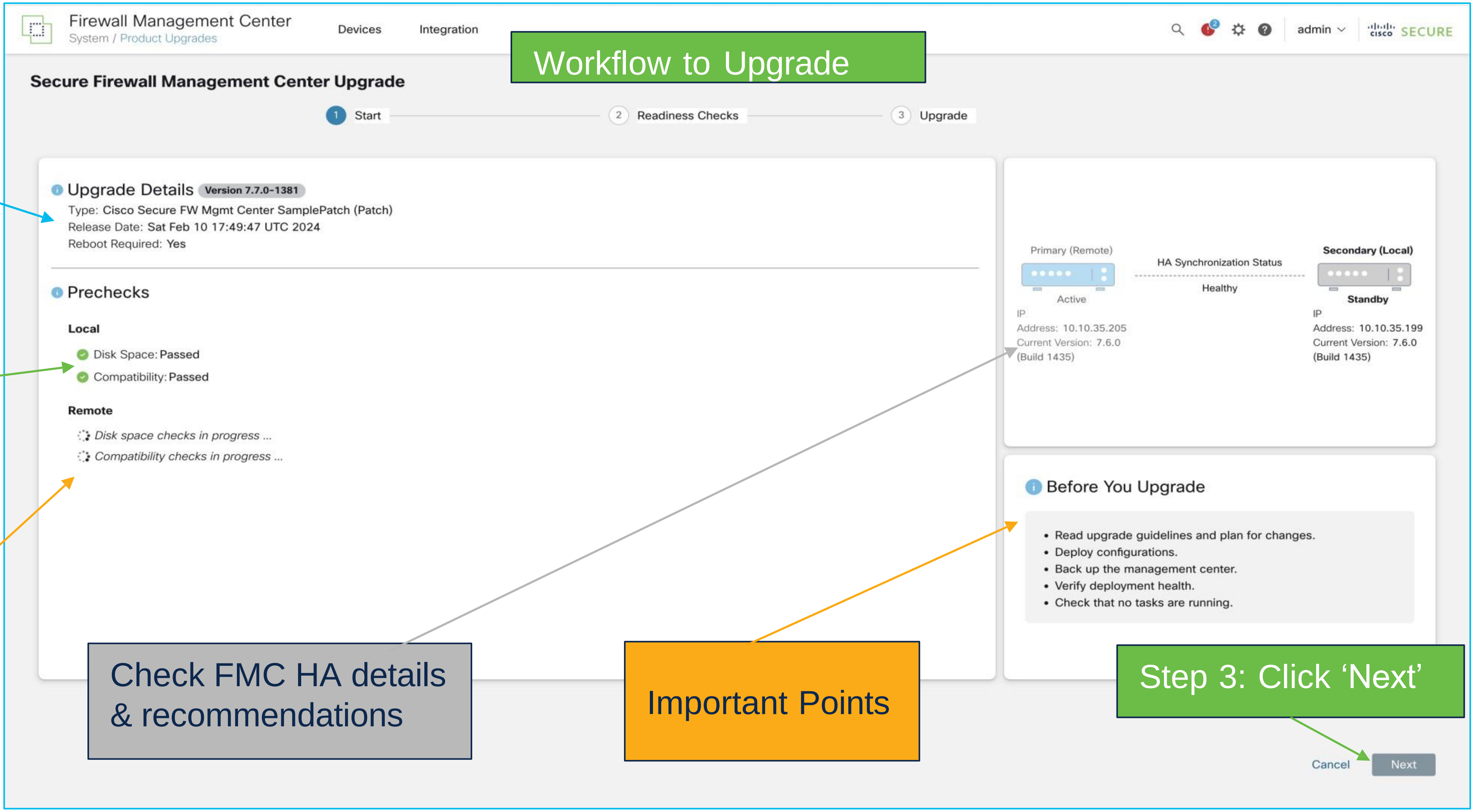
Secure Firewall Cluster

Management HA Upgrades

Check the upgrade details

Step 1: Check the local FMCs prechecks result

Step 2: Check the remote FMCs prechecks status



Workflow to Upgrade

Secure Firewall Management Center Upgrade

Upgrade Details Version 7.7.0-1381

Type: Cisco Secure FW Mgmt Center SamplePatch (Patch)
Release Date: Sat Feb 10 17:49:47 UTC 2024
Reboot Required: Yes

Prechecks

Local

- Disk Space: Passed
- Compatibility: Passed

Remote

- *Disk space checks in progress ...*
- *Compatibility checks in progress ...*

Primary (Remote)	HA Synchronization Status	Secondary (Local)
Active	Healthy	Standby
IP Address: 10.10.35.205 Current Version: 7.6.0 (Build 1435)		IP Address: 10.10.35.199 Current Version: 7.6.0 (Build 1435)

Before You Upgrade

- Read upgrade guidelines and plan for changes.
- Deploy configurations.
- Back up the management center.
- Verify deployment health.
- Check that no tasks are running.

Check FMC HA details & recommendations

Important Points

Step 3: Click ‘Next’

Management & Upgrades

Change Management Enhancement

New! Users with both Review and Modify Ticket permissions can take over a ticket and assign it to themselves or to another user (Administrators & Network Admins)

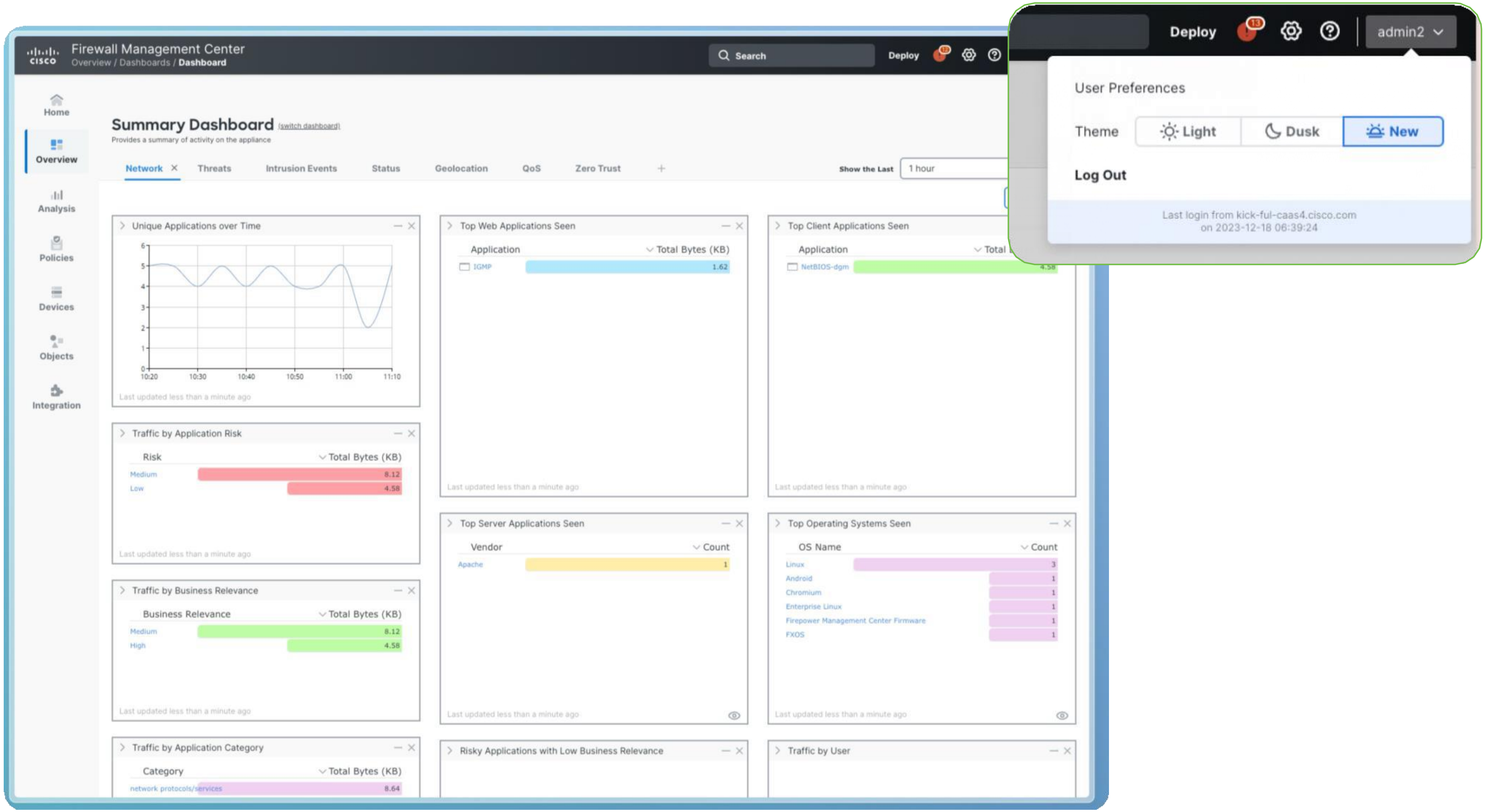
Administrator	Intrusion Admin	Network Admin	Security Approver
Review Ticket Modify Ticket Configuration*	Modify Ticket	Review Ticket Modify Ticket	Review Ticket

Review Ticket ››› User(s) with this permission can assign the ticket to other users. Can also review and approve the tickets of other users

Modify Ticket ››› User(s) with this permission can create and use the ticket to make changes to FMC

Management & Upgrades

New Management User Interface



Firewall Management Center
Overview / Dashboards / **Dashboard**

Summary Dashboard (switch dashboard)
Provides a summary of activity on the appliance

Unique Applications over Time

Last updated less than a minute ago

Top Web Applications Seen

Application	Total Bytes (KB)
IGMP	1.62

Last updated less than a minute ago

Top Client Applications Seen

Application	Total
NetBIOS-dgm	4.58

Last updated less than a minute ago

Traffic by Application Risk

Risk	Total Bytes (KB)
Medium	8.12
Low	4.58

Last updated less than a minute ago

Top Server Applications Seen

Vendor	Count
Apache	1

Last updated less than a minute ago

Top Operating Systems Seen

OS Name	Count
Linux	3
Android	1
Chromium	1
Enterprise Linux	1
Firepower Management Center Firmware	1
FXOS	1

Last updated less than a minute ago

Traffic by Business Relevance

Business Relevance	Total Bytes (KB)
Medium	8.12
High	4.58

Last updated less than a minute ago

Traffic by Application Category

Category	Total Bytes (KB)
network protocols/services	8.64

Risky Applications with Low Business Relevance

Traffic by User

User Preferences

Theme: Light | Dusk | **New**

Log Out

Last login from kick-ful-caas4.cisco.com
on 2023-12-18 06:39:24

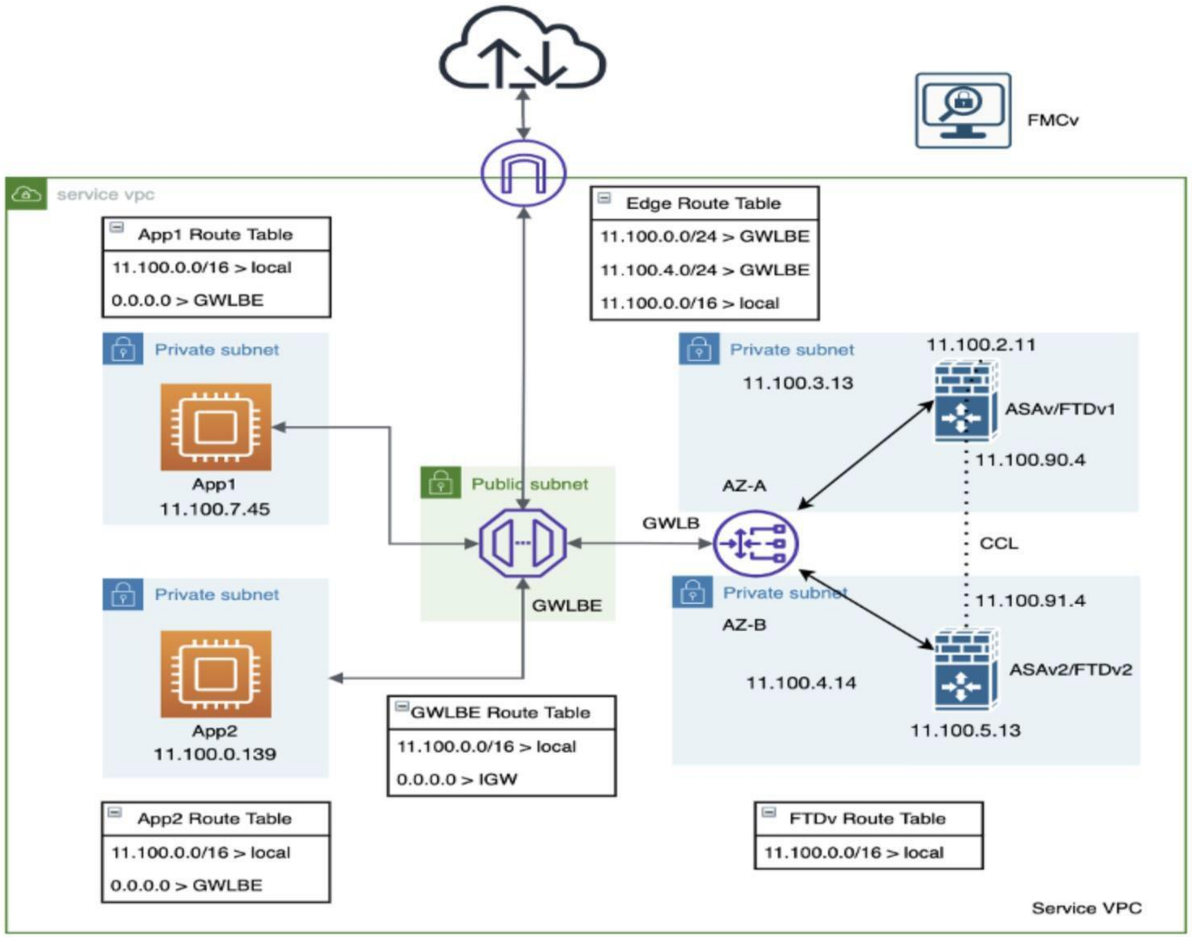
Public Cloud

Public Cloud Updates

Multi-Availability Zone Clustering with Autoscale in Amazon web Services

New in FTDv 7.6 / ASAv9.22.1

- ASAv/FTDv Clustering created on different Availability Zones (single or multiple AZ's, based on user requirement, with dynamic scaling enabled)
- Must be in the same Virtual Private Cloud (VPC), and therefore in the same region



App1 Route Table
11.100.0.0/16 > local
0.0.0.0 > GWLBE

Edge Route Table
11.100.0.0/24 > GWLBE
11.100.4.0/24 > GWLBE
11.100.0.0/16 > local

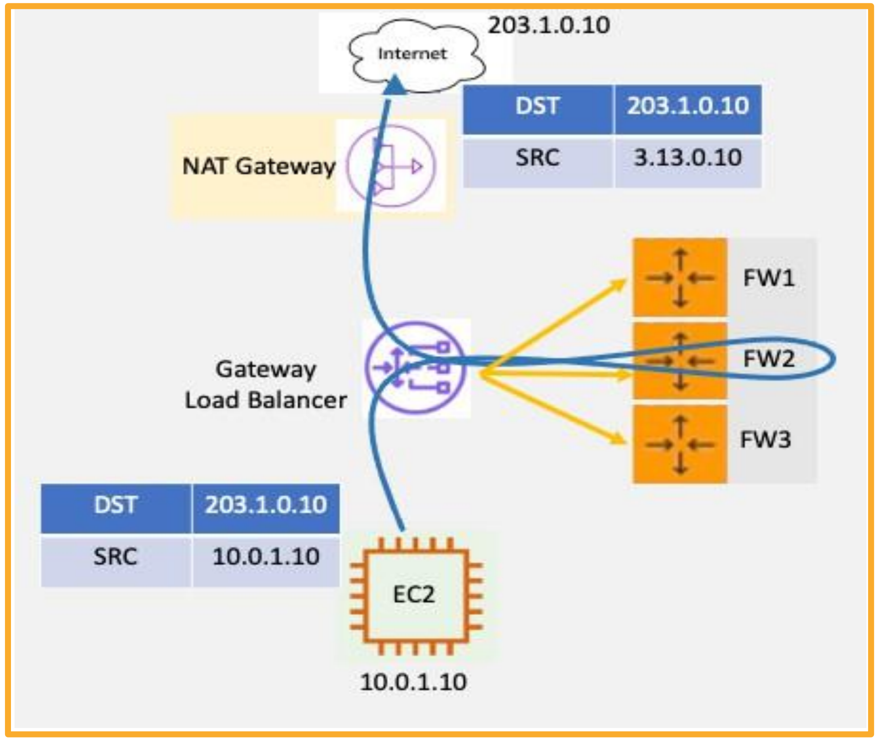
GWLBE Route Table
11.100.0.0/16 > local
0.0.0.0 > IGW

App2 Route Table
11.100.0.0/16 > local
0.0.0.0 > GWLBE

FTDv Route Table
11.100.0.0/16 > local

Public Cloud Updates

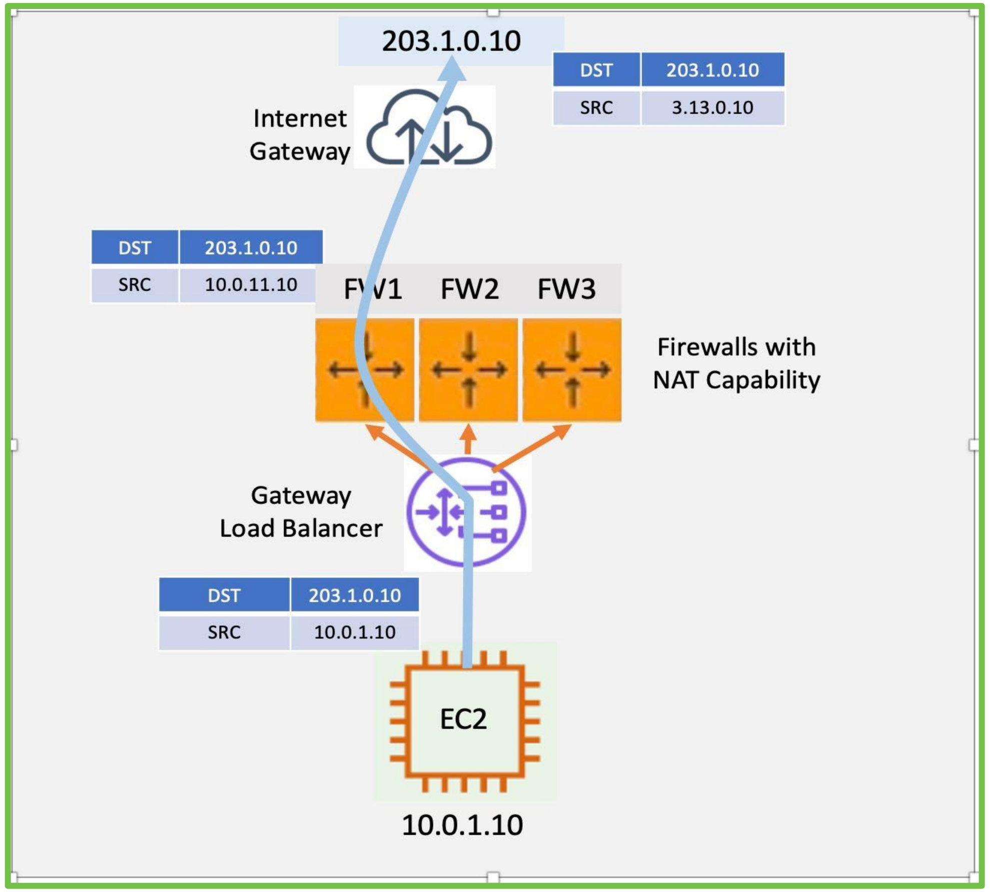
Dual-Arm Deployment with Gateway Load Balancing in Amazon web Services



DST	203.1.0.10
SRC	3.13.0.10

DST	203.1.0.10
SRC	10.0.1.10

AWS GWLB Single-Arm Egress Traffic Flow



DST	203.1.0.10
SRC	3.13.0.10

DST	203.1.0.10
SRC	10.0.11.10

DST	203.1.0.10
SRC	10.0.1.10

NEW: AWS GWLB Dual-Arm Egress Traffic Flow

Additional Resources

Public Information

Accessible & Shareable to Everyone

Cisco Secure Essentials Hub - Is the “Hub” or starting point where users can obtain information on Secure Firewall, Microsegmentation, & by Q4 FY24 – Multicloud Defense

Cisco Secure Firewall & Workload Youtube Channels – These channels provide product deep dives, integrations, release overviews, & highlights

Cisco DevNet Website – Houses various labs where users can learn about Firewall Automation for AWS, Azure, GCP & CDO.

Cisco Developer Website - offers Cloud templates to help users deploy firewalls in their preferred cloud provider environment, & Automation APIs allowing the exchange of security events, data and host information

Internal & Partner Information

Only available to Cisco Employees or Partners

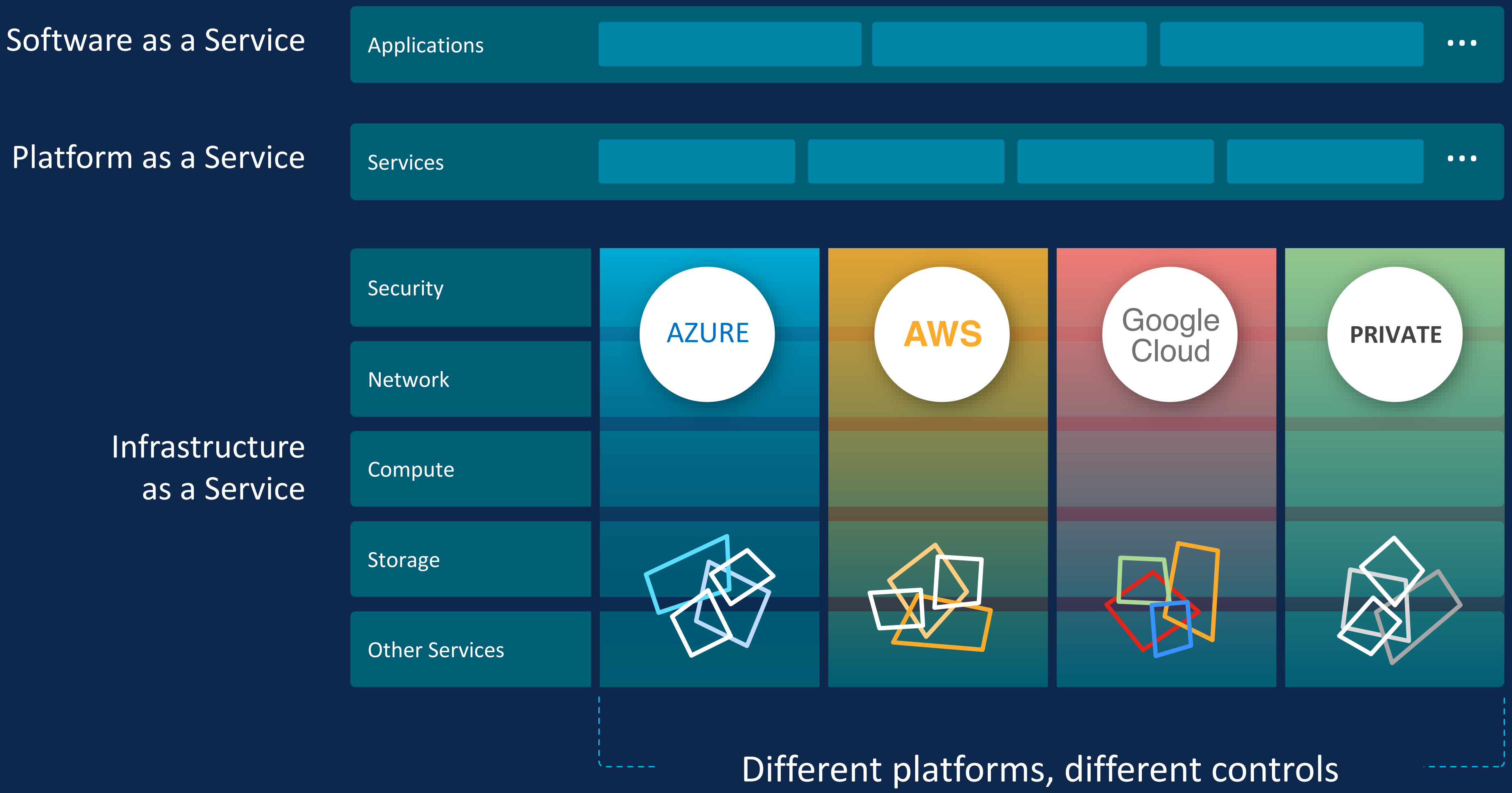
- SalesConnect (Firewall & Workload) – Houses in-depth technical documentation, best-practices, & demonstrations to help stakeholders realize the value of Firewall and Workload.

- Lab licensing

Cisco Security Cloud & Suites

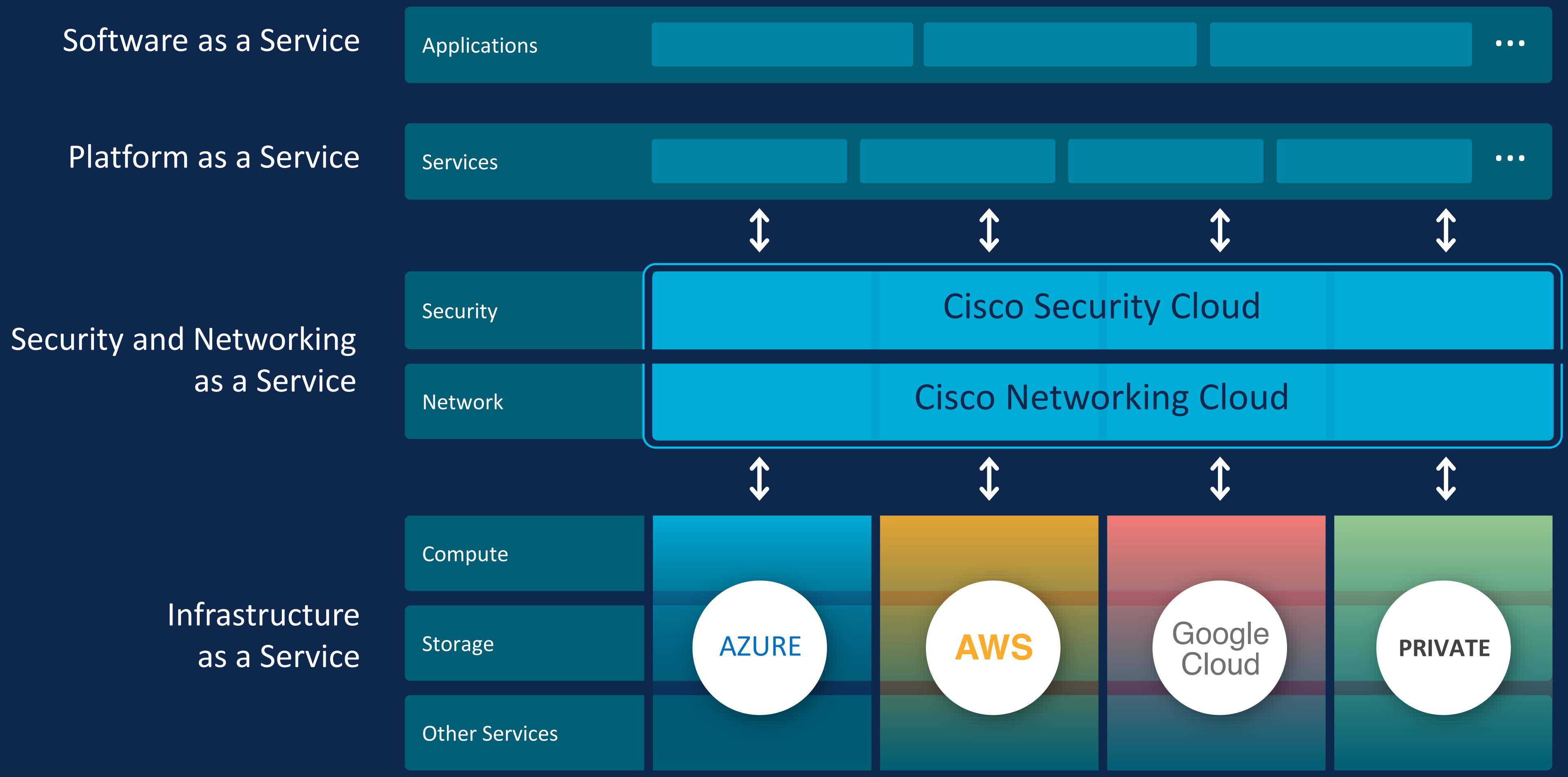
COALFIRE
Lookout
red canary
McAfee
passbase
Prove
CHECK POINT
FusionAuth
clearswift
okta
proofpoint
Security innovation is a
Ping Identity
sophos
solarwinds
U410
KnowBe4
deepwatch
FORCEPOINT
hackerone
axio
paloalto
CROWDSTRIKE
HUNTRESS
GoGuardian
NowSecure
VARONIS
DARKTRACE
RAPID7
zscaler

Multiple clouds makes tool sprawl worse



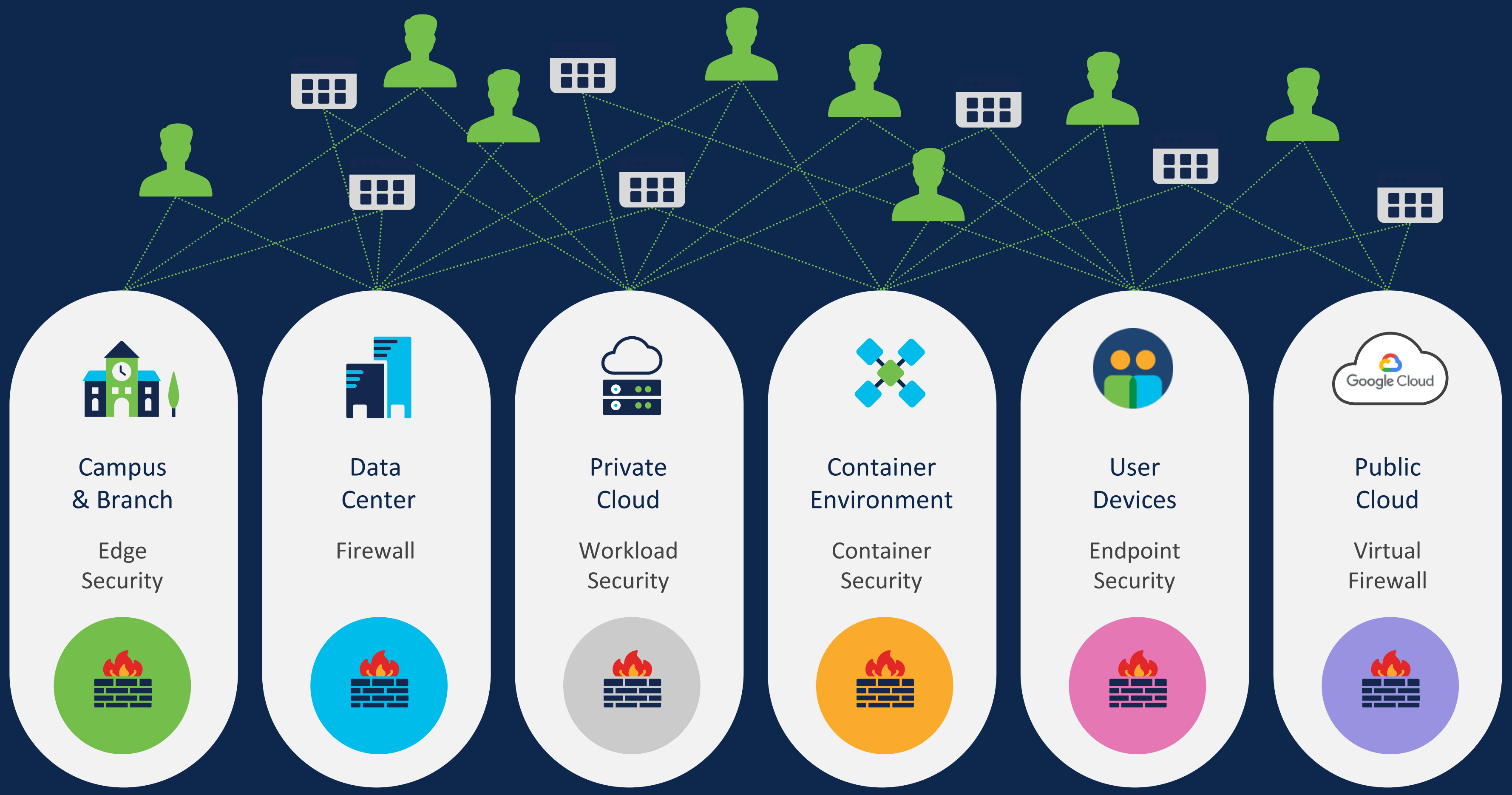
Different platforms, different controls

Introducing Cisco Security Cloud



Problem: Product Complexity Across Hybrid Environments

Security Focuses on Siloed Outcomes



Campus & Branch

Edge Security

Data Center

Firewall

Private Cloud

Workload Security

Container Environment

Container Security

User Devices

Endpoint Security

Public Cloud

Virtual Firewall

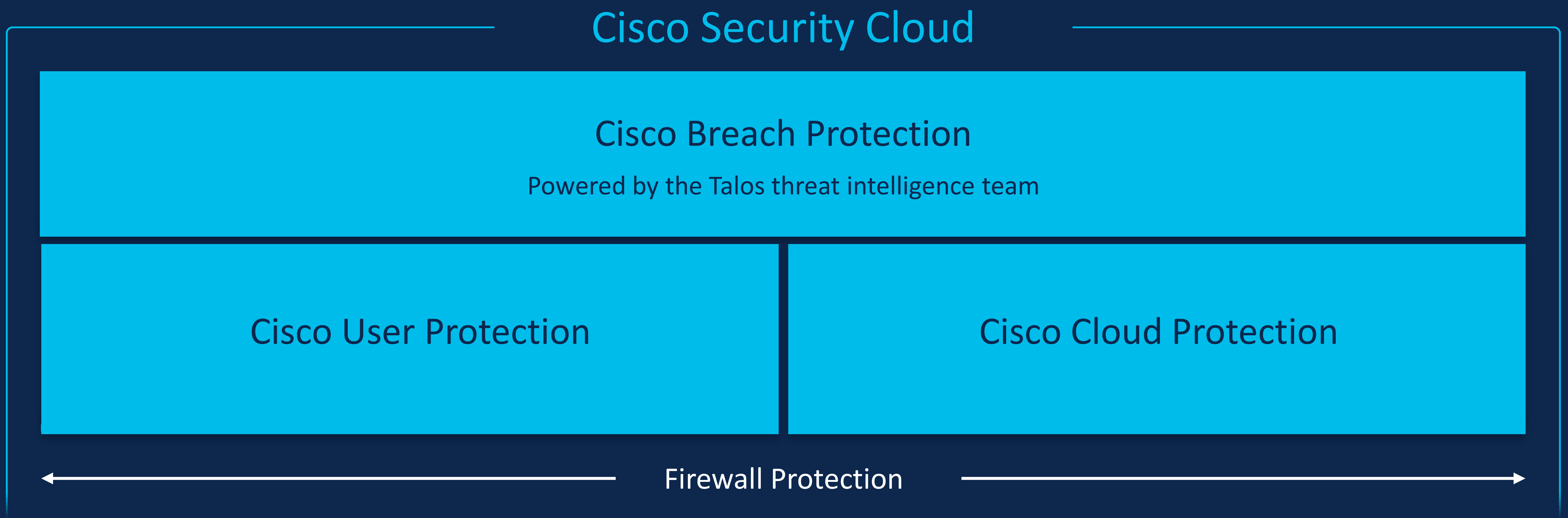
Multiple teams and organizations cover multiple dynamic environments

Each with own policy models and enforcement points

Inconsistent and siloed islands of policy controls

In dynamic environments, “misconfigurations” are often deliberate trade-offs

Security that only Cisco can deliver



Cisco Security Cloud

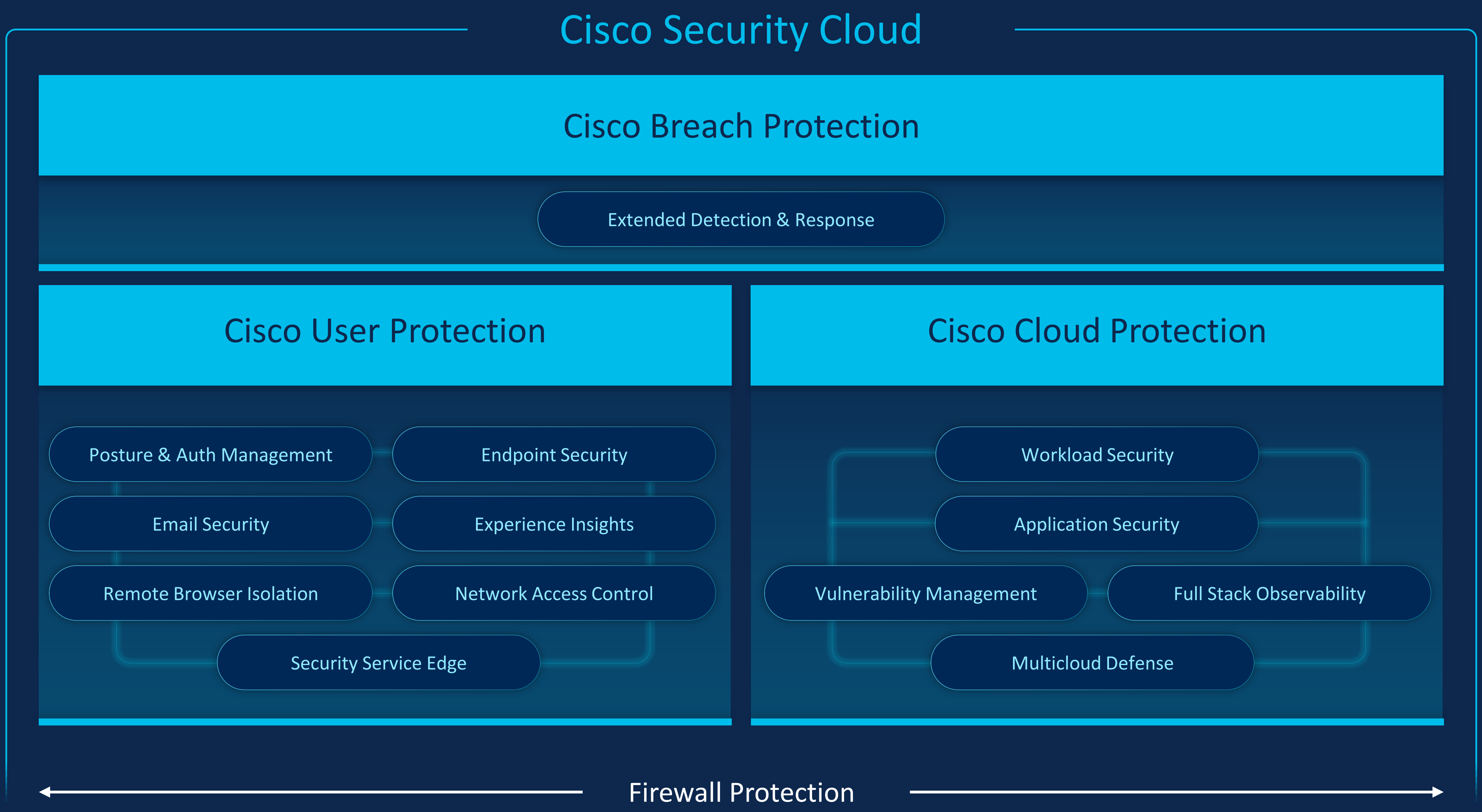
Cisco Breach Protection

Powered by the Talos threat intelligence team

Cisco User Protection

Cisco Cloud Protection

Firewall Protection



Cisco Security Cloud

Cisco Breach Protection

- Extended Detection & Response

Cisco User Protection

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

Cisco Cloud Protection

- Workload Security
- Application Security
- Vulnerability Management
- Full Stack Observability
- Multicloud Defense

Firewall Protection

Cisco Security Suites

Better Efficacy | Better Experiences | Better Economics

User Protection

The Cisco User Protection Suite protects against all attack vectors that target users while providing seamless and secure access to any application, on any device, from anywhere to implement zero trust, with zero friction.

Better Efficacy
Defend against all user attack vectors

Better Experiences
One simple experience for secure access to all apps (not just some)

Better Economics
Centralize policy management for traditional and modern apps

Cloud Protection

Cisco Cloud Protection Suite simplifies operations, optimizes resources, and reduces risk with comprehensive security and pervasive visibility for hybrid and multi-cloud networks, workloads, and applications.

Better Efficacy
Stop lateral movement of attacks

Better Experiences
Simplify multicloud security operations

Better Economics
Consolidate management of security policy

Breach Protection

Cisco Breach Protection Suite empowers security teams to simplify operations and accelerate response across the most prominent attack vectors including email, endpoints, network, and cloud.

Better Efficacy
Detect and respond to sophisticated threats like ransomware

Better Experiences
Significantly accelerate incident response

Better Economics
Achieve Tier 2 outcomes from Tier 1 analysts

Introducing security only Cisco can deliver

Cisco User Protection Suite

Posture & Auth Management

Endpoint Security

Email Security

Experience Insights

Remote Browser Isolation

Security Service Edge

Email Threat Defense

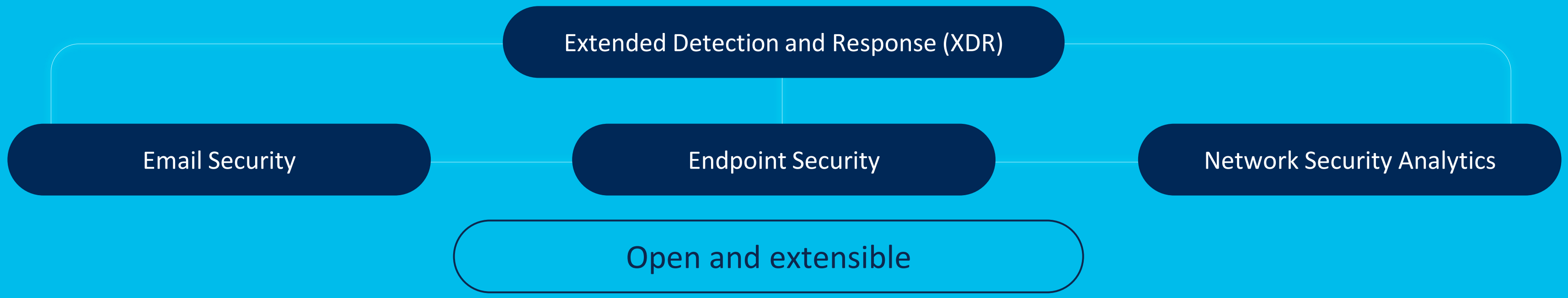
Cisco Secure Access

Secure Endpoint

Duo

Introducing security only Cisco can deliver

Cisco Breach Protection Suite



Extended Detection and Response (XDR)

Email Security

Endpoint Security

Network Security Analytics

Open and extensible

Cisco XDR

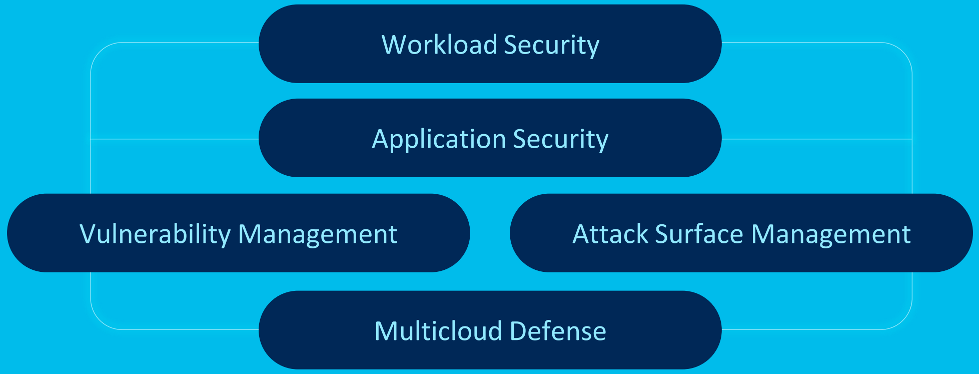
Cisco Email Threat Defense

Cisco Secure Endpoint

Cisco Secure Network Analytics

Introducing security only Cisco can deliver

Cisco Cloud Protection Suite



Workload Security

Application Security

Vulnerability Management

Attack Surface Management

Multicloud Defense

Cisco Multicloud Defense

Cisco Vulnerability Management

Cisco Secure Workload

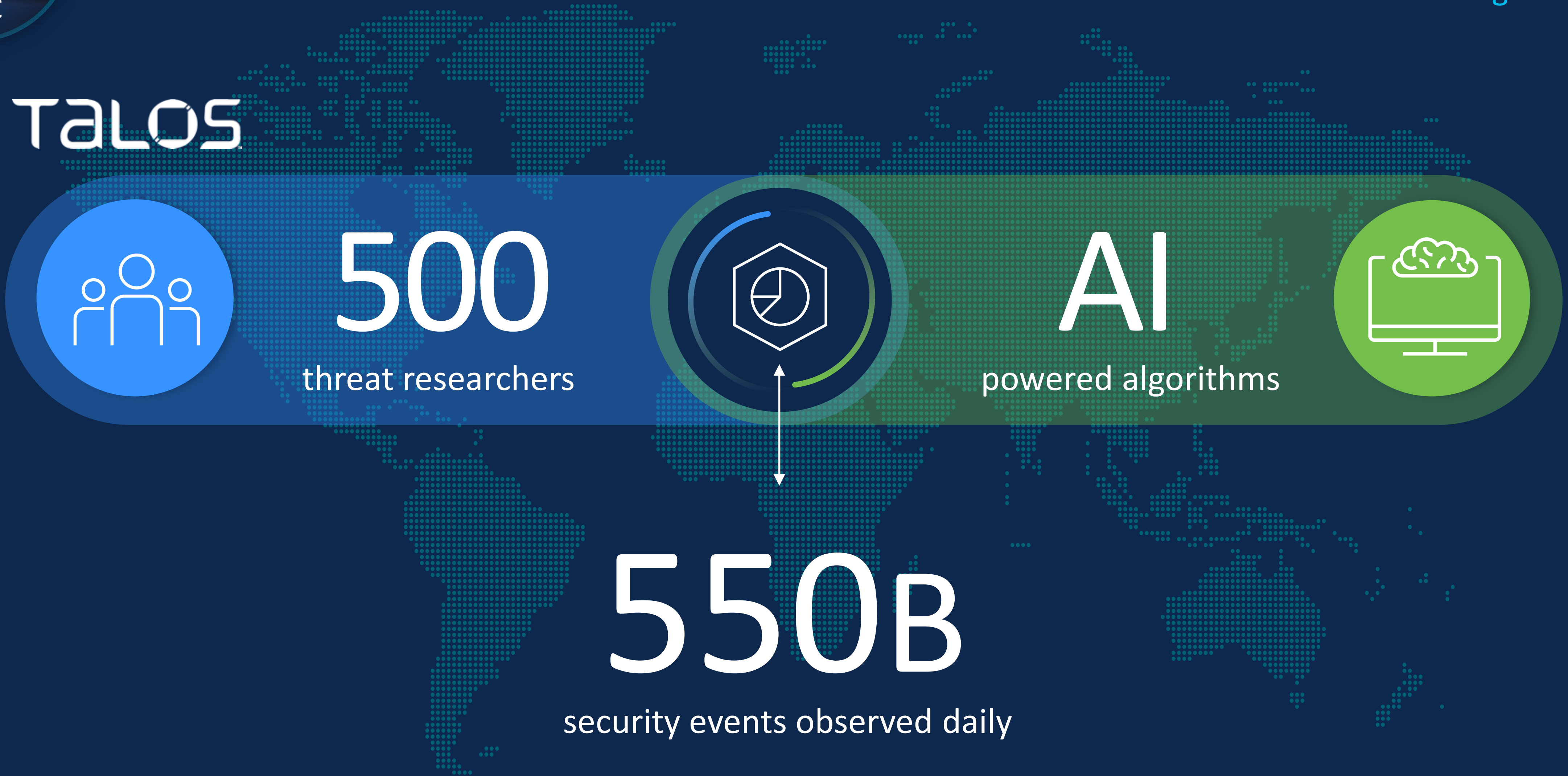
Cisco Attack Surface Management

Cisco Cloud Application Security

Talos powers the Cisco portfolio with intelligence

Research and Intelligence

TALOS



500

threat researchers

AI

powered algorithms

550B

security events observed daily

Cisco XDR | 3rd Party Integrations (partial list)

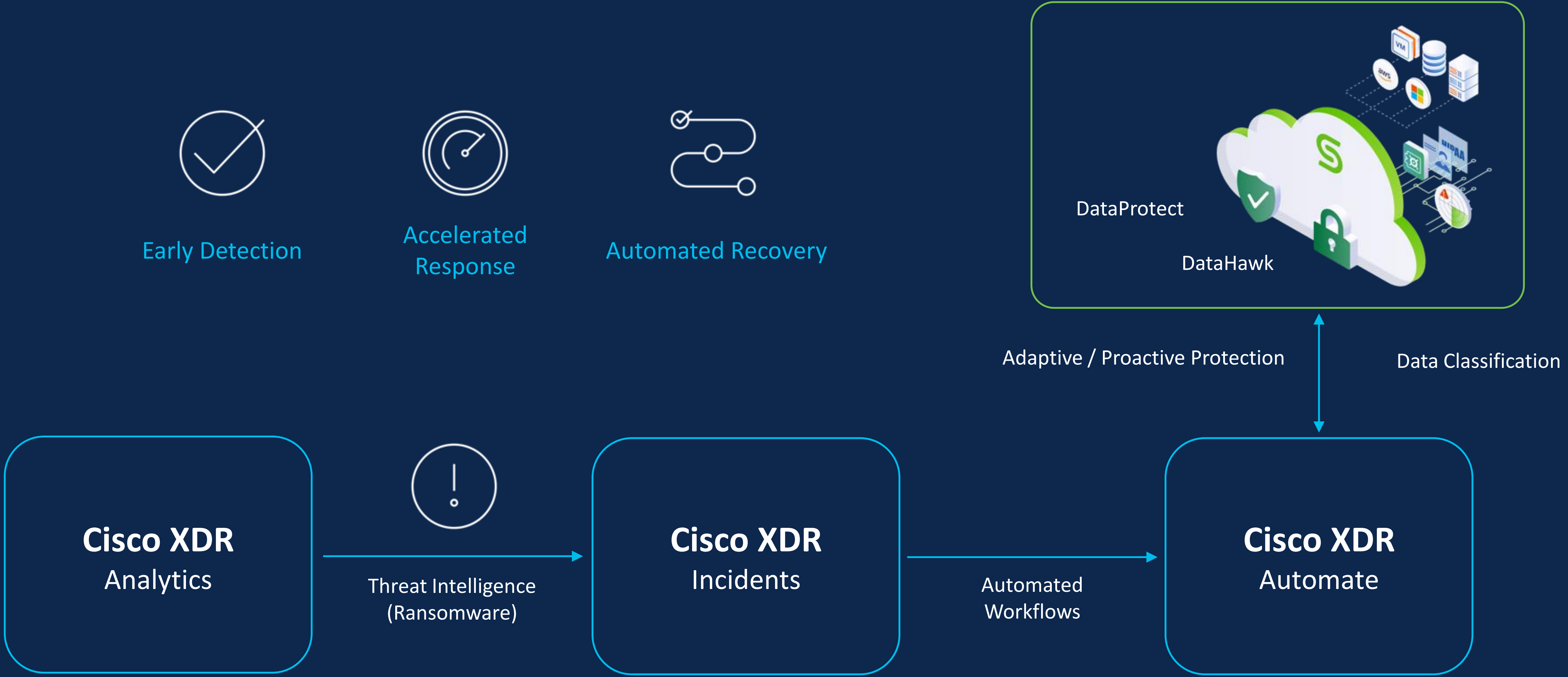
- APIVoid
- AbuseIPDB IP Checker
- Akamai
- AlienVault Open Threat Exchange
- Amazon GuardDuty
- Bastille Networks
- Censys
- Cohesity Data Cloud
- CrowdStrike
- CyberCrime Tracker
- Cybereason
- Darktrace Respond & Detect
- Devo
- Exabeam

- ExtraHop Reveal(s) 360
- Farsight Security
- Google Chronicle
- Generic Serverless Relay
- Google Safe Browsing
- Graylog
- Have I Been Pwned
- IBM X-Force Exchange
- IsItPhishing
- Ivanti Neurons
- Jamf Pro
- LogRhythm
- MISP
- Microsoft Azure AD

- Microsoft Defender Endpoint
- Microsoft Graph Security
- Microsoft intune
- Palo Alto Networks AutoFocus
- Palo Alto Networks Cortex XDR
- Pulsedive
- Qualys IOC
- Radware Cloud DDoS Protection
- Radware Cloud WAF
- Recorded Future
- SecureX CESA Relay
- SecurityTrails
- SentinelOne Endpoint
- ServiceNow Threat Intelligence

- Shodan
- Signal Sciences WAF
- Sixgill Darkfeed
- Splunk Relay module
- SpyCloud Account Takeover Prevention
- Sumo Logic Cloud SIEM
- Sumo Logic Log Mgmt
- Threatscore Cyberprotect
- Trent Vision One
- VMWare Workspace ONE UEM
- VirusTotal
- alphaMountain.ai Threat Intelligence
- urlscan.io

Full Cycle Automated Threat Response and Recovery* Cohesity and Cisco XDR Integration: Extended Detection and Response AND RECOVERY



Early Detection

Accelerated Response

Automated Recovery

DataProtect

DataHawk

Adaptive / Proactive Protection

Data Classification

Cisco XDR
Analytics

Threat Intelligence
(Ransomware)

Cisco XDR
Incidents

Automated
Workflows

Cisco XDR
Automate

* Includes Cohesity as the first data protection solution provider

The Cisco Advantage

Zero trust architecture, with consistent macro and micro-segmentation

Complete protection for all traffic across the network, clouds, and VPCs

Pervasive visibility, validates security posture and prioritize risks to the business

Modernize application security

60% of attacks involve lateral movement

Source: Intelligent CISO 2021

Cisco Security Cloud Momentum

300K+
security customers

2.8M
new malware samples/day

TALOS
550B
security events observed/day

AI Powered Detections
Exposed top 3 ransomware 2023 threat campaigns
(Yashma, Rhysida, MortalKobat)

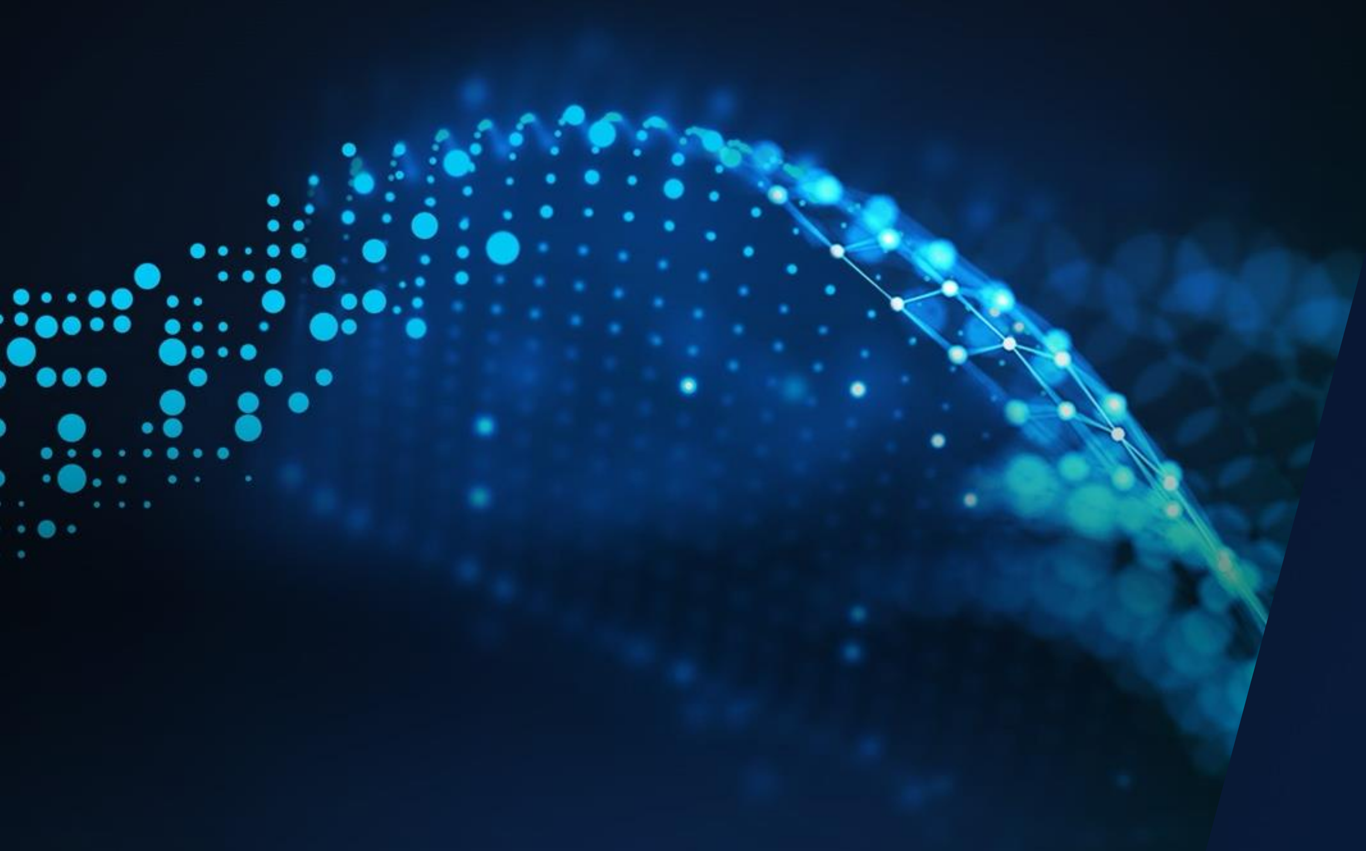
TALOS
200+
vulnerabilities discovered/year

Source: Cisco internal metrics

The bridge to possible

Cisco Hypershield

Cybersecurity basics are tough.

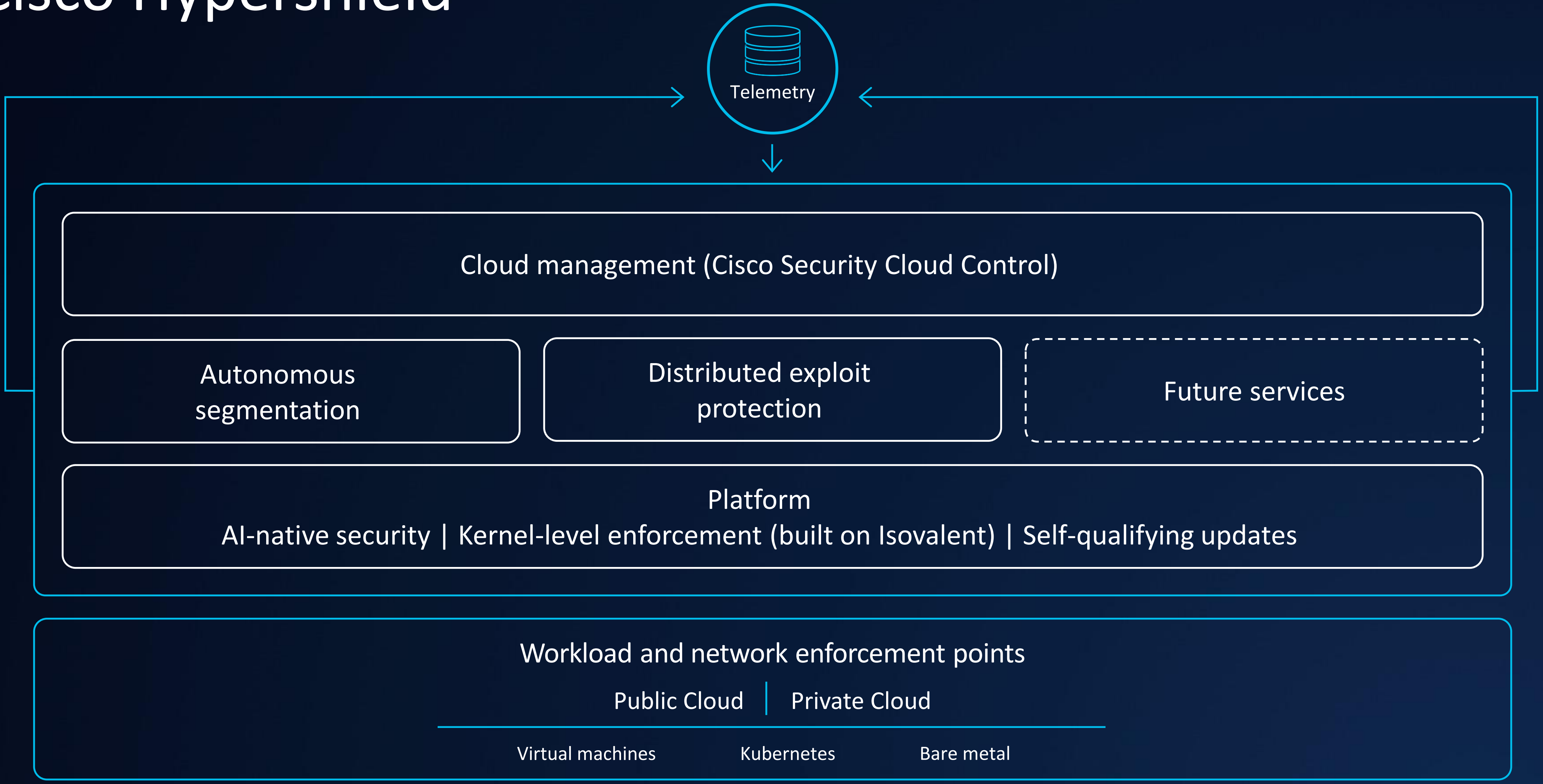


Segmentation is hard

Patching is hard

Upgrading is hard

Cisco Hypershield



Telemetry
Cloud management (Cisco Security Cloud Control)
Autonomous segmentation
Distributed exploit protection
Future services
Platform
AI-native security | Kernel-level enforcement (built on Isovalent) | Self-qualifying updates
Workload and network enforcement points
Public Cloud
Private Cloud
Virtual machines
Kubernetes
Bare metal

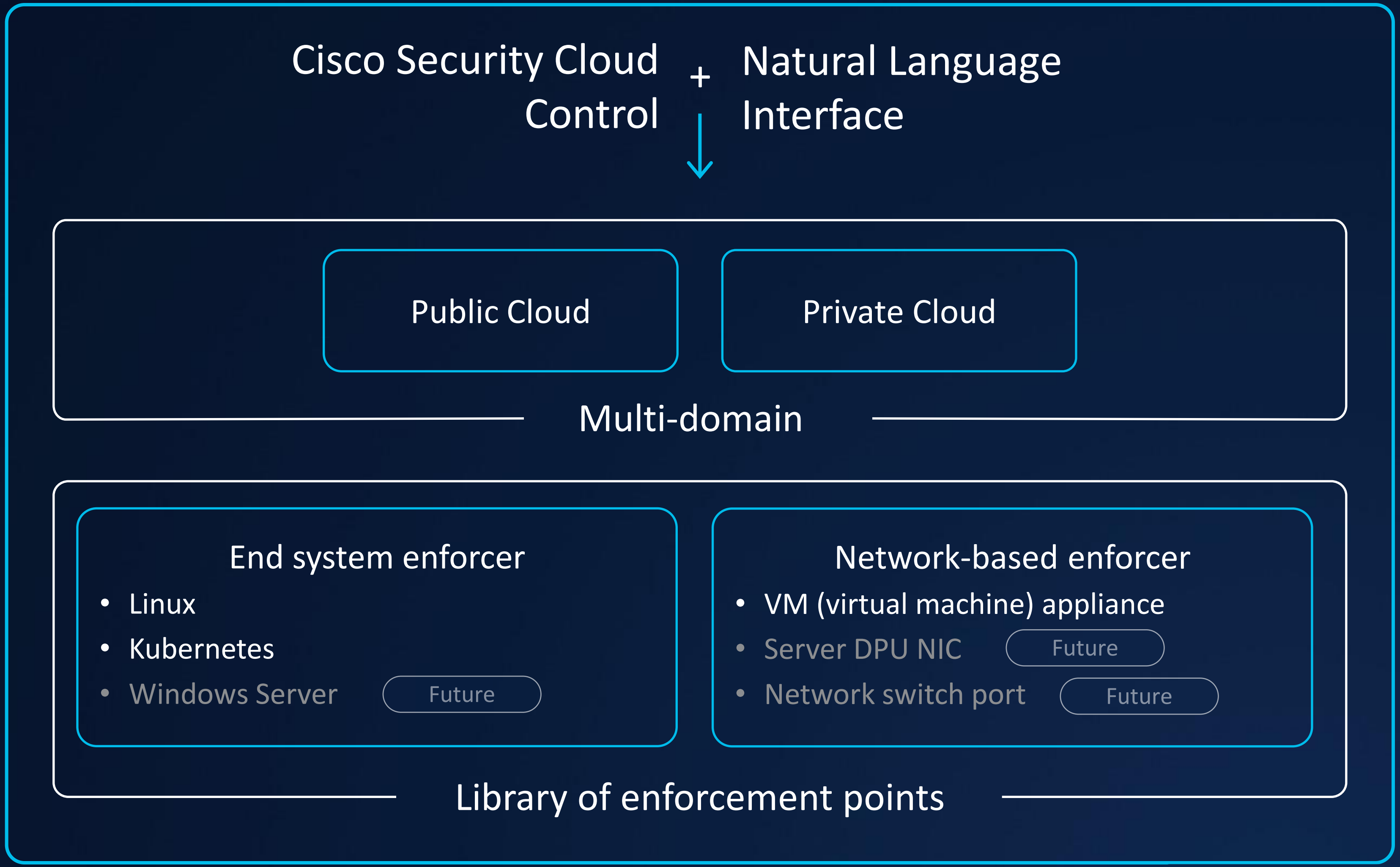
Manage globally, enforce locally

Includes

- Unified management
- Single global policy
- Intelligent placement of shields
- Integrations with cloud/app/infra metadata

Environments

- Kubernetes
- Cloud – Private/Public
- On-prem



Cisco Security Cloud Control + Natural Language Interface

Public Cloud

Private Cloud

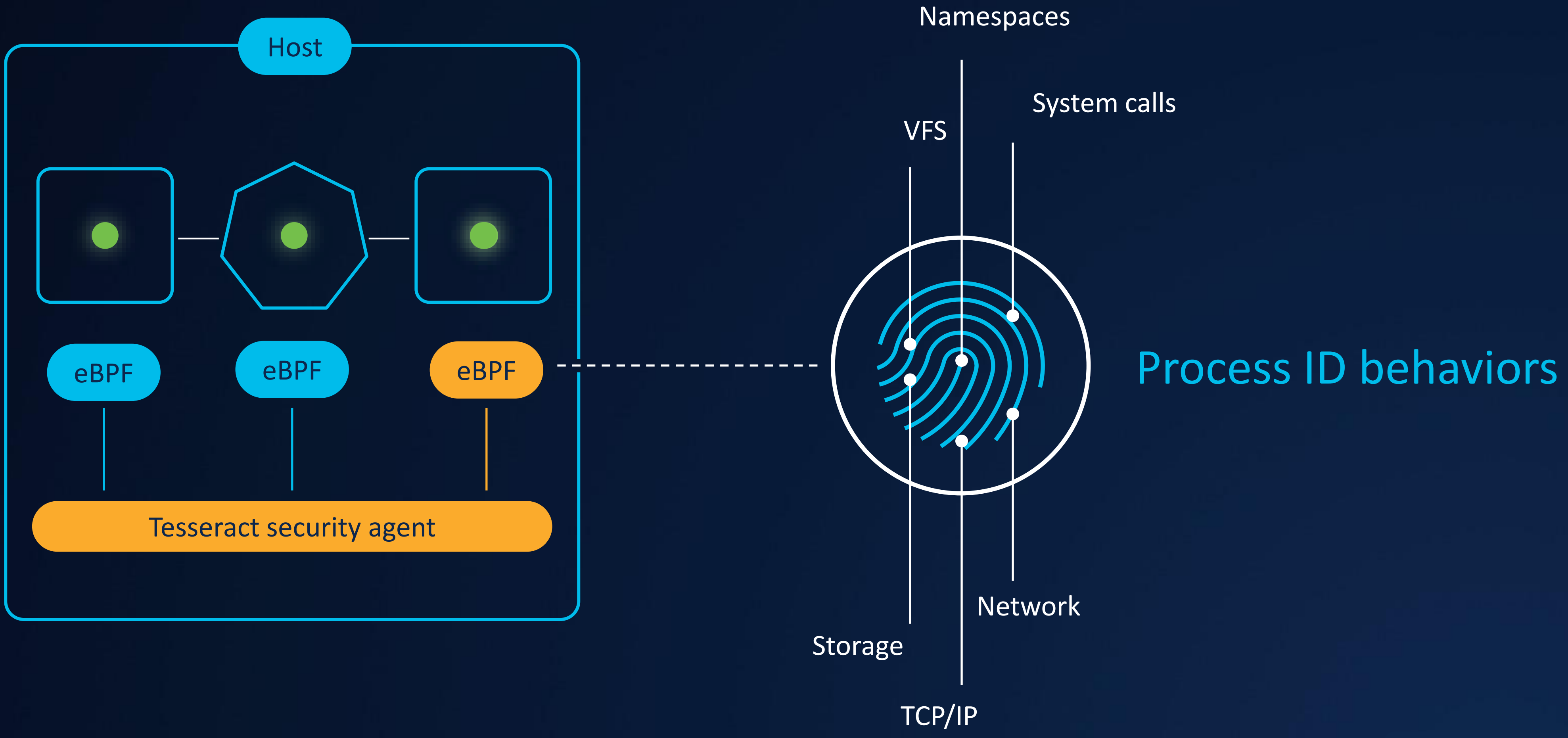
Multi-domain

End system enforcer
- Linux
- Kubernetes
- Windows Server Future

Network-based enforcer
- VM (virtual machine) appliance
- Server DPU NIC Future
- Network switch port Future

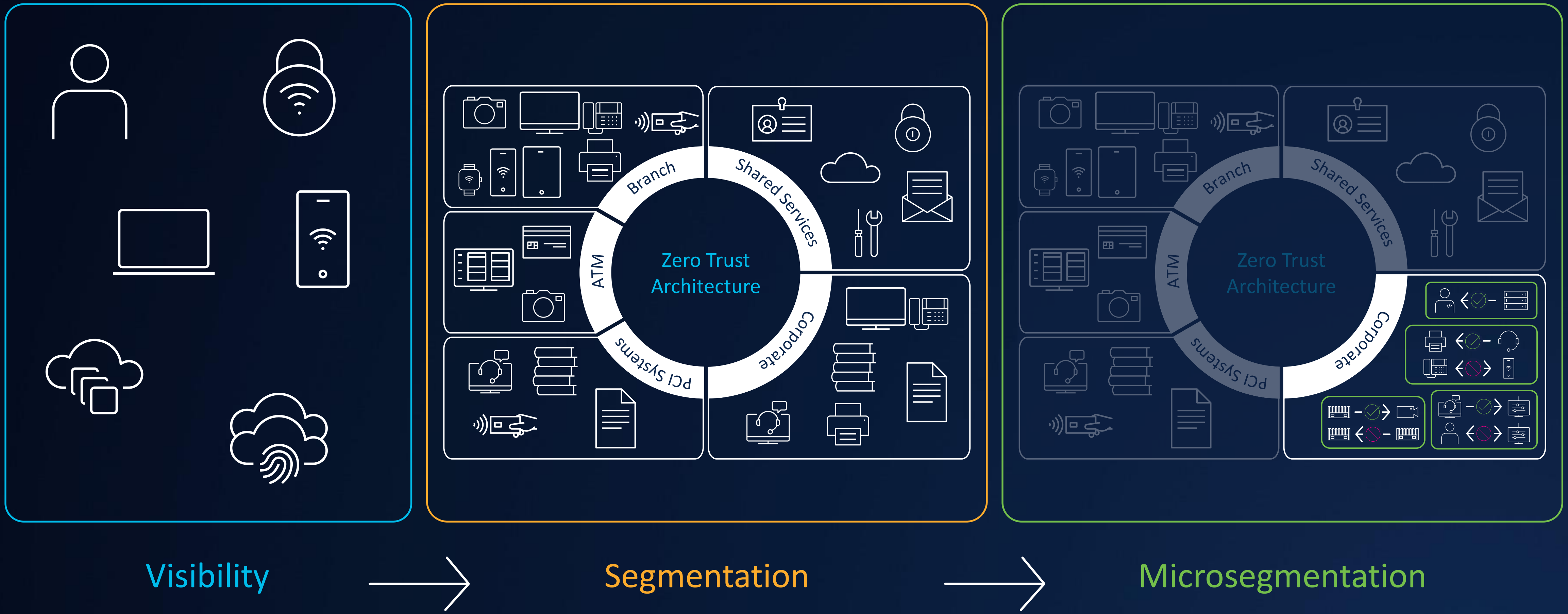
Library of enforcement points

Deep visibility and enforcement in the workload built on Isovalent Tetragon



Segmentation addresses main customer concerns

Compliance and reduction of attack surface with microsegmentation



Visibility → Segmentation → Microsegmentation

Why Cisco?

Only Cisco provides network and application microsegmentation

Only Cisco offers persistent and pervasive enforcement across all environments

The entire Cisco segmentation portfolio is integrated

Securing the AI-ready Data Center

1

Cisco Security innovation momentum

Open the conversation with Cisco Hypershield

2

Every customer is focused on segmentation

Cisco's segmentation portfolio is meeting today's and future needs – talk to your customer now

3

Cisco is poised to win

Understand the qualification criteria and position the best suitable solution

The bridge to possible