Security Cloud Platform & Firewalls

Cisco Security Cloud Control

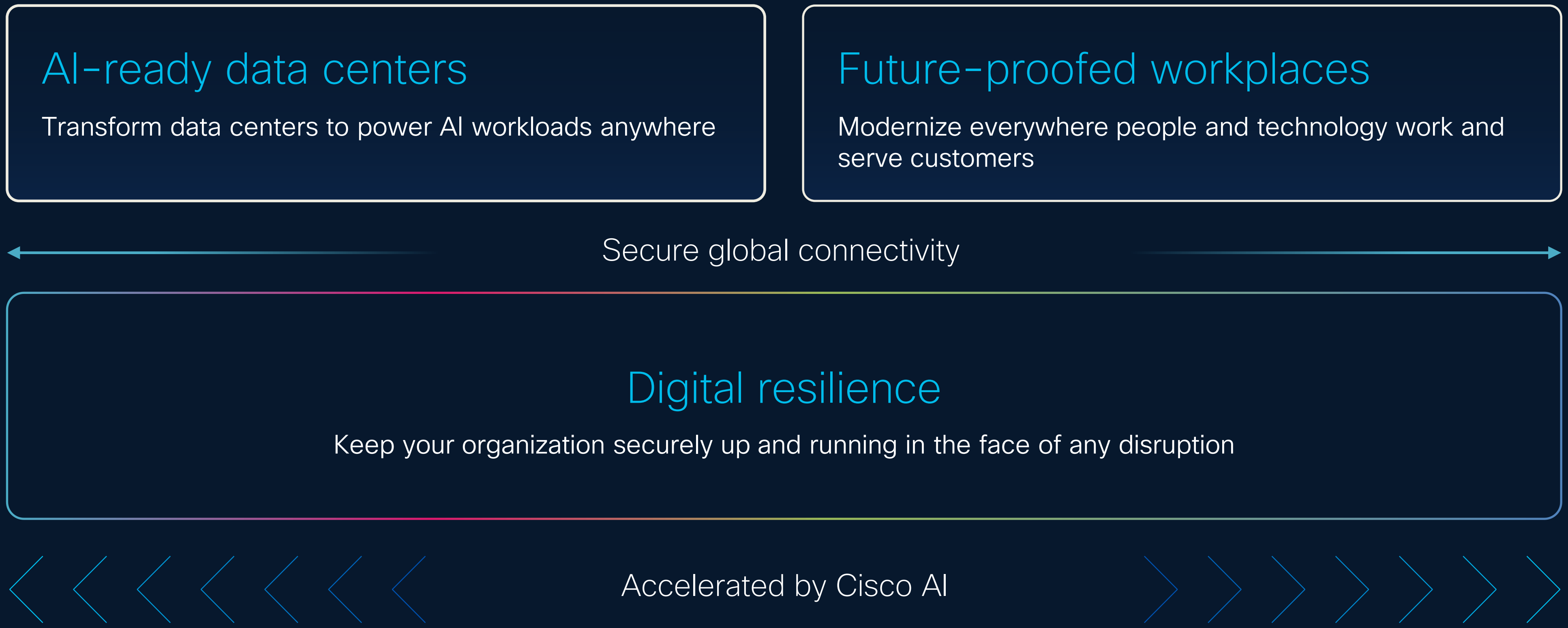
Christopher Hayre
Security SE
chhayre@cisco.com

Agenda

- The Platform
- Firewall management
- How to get started
- Additional platform use-cases

cisco Connect

Cisco powers how people and technology work together across the physical and digital worlds



AI-ready data centers

Transform data centers to power AI workloads anywhere

Future-proofed workplaces

Modernize everywhere people and technology work and serve customers

Secure global connectivity

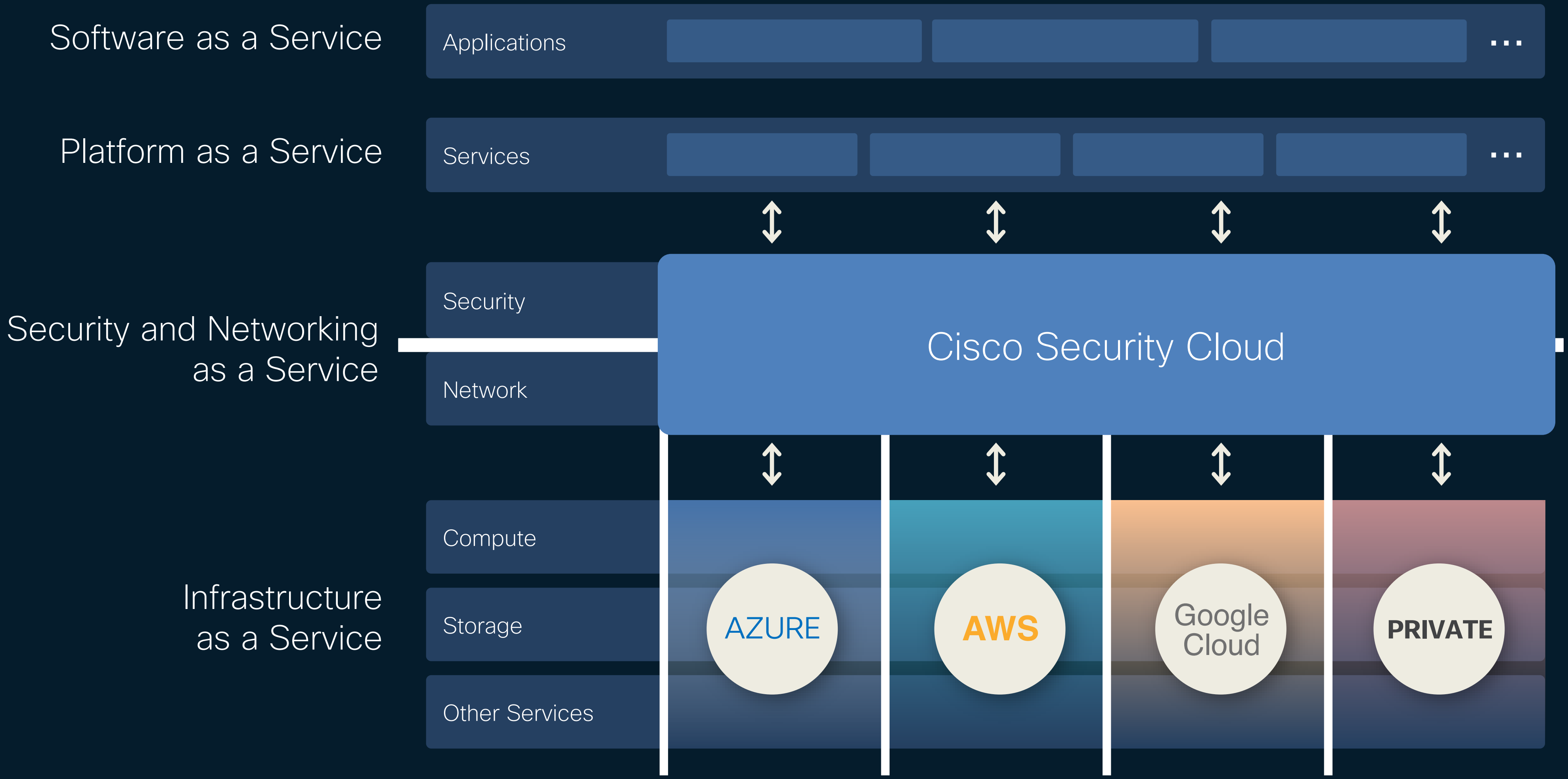
Digital resilience

Keep your organization securely up and running in the face of any disruption

Accelerated by Cisco AI

The Platform

Cisco Security Cloud

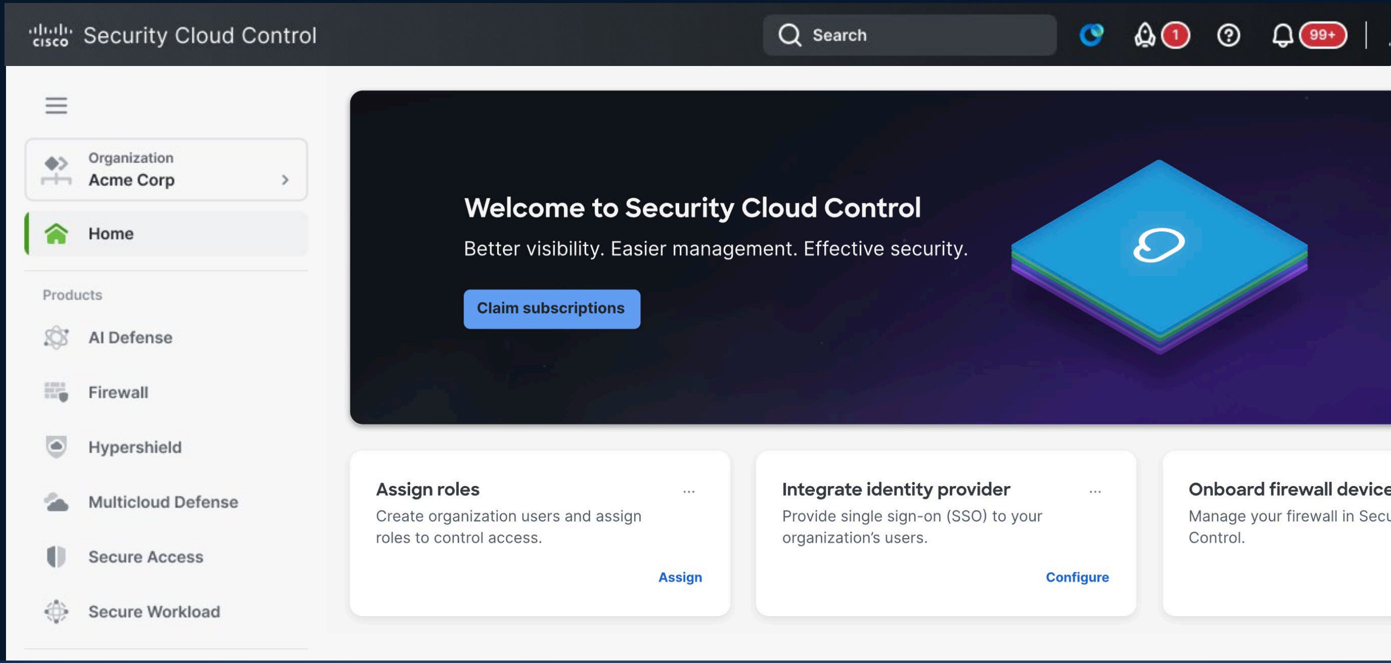


HOW CAN I BUY CISCO SECURITY CLOUD?
CISCO
CISCO
SEOUMET

What used to happen every time you bought a Cisco Security product?

Security Cloud Control

AI-native unified security management



Security Cloud Control

Search

1

99+

Organization
Acme Corp

Home

Products

- AI Defense
- Firewall
- Hypershield
- Multicloud Defense
- Secure Access
- Secure Workload

Welcome to Security Cloud Control

Better visibility. Easier management. Effective security.

Claim subscriptions

Assign roles

Create organization users and assign roles to control access.

Assign

Integrate identity provider

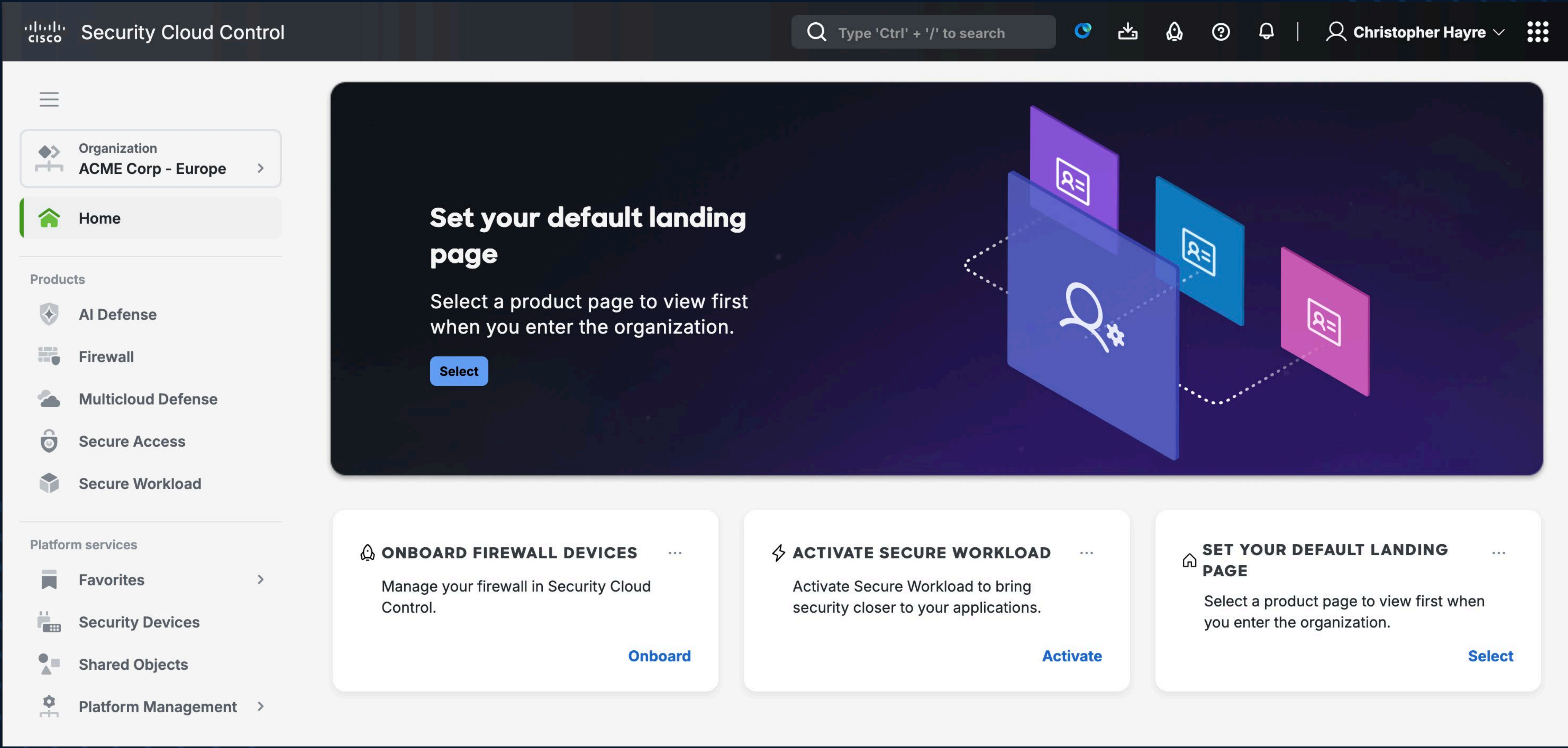
Provide single sign-on (SSO) to your organization's users.

Configure

Onboard firewall device

Manage your firewall in Secu
Control.

Secure Firewall | Multicloud Defense | Hypershield | Secure Workload | Secure Access | AI Defense



Security Cloud Control

Type 'Ctrl' + '/' to search

Christopher Hayre

Organization
ACME Corp - Europe

Home

Products

- AI Defense
- Firewall
- Multicloud Defense
- Secure Access
- Secure Workload

Platform services

- Favorites
- Security Devices
- Shared Objects
- Platform Management

Set your default landing page

Select a product page to view first when you enter the organization.

Select

ONBOARD FIREWALL DEVICES

Manage your firewall in Security Cloud Control.

Onboard

ACTIVATE SECURE WORKLOAD

Activate Secure Workload to bring security closer to your applications.

Activate

SET YOUR DEFAULT LANDING PAGE

Select a product page to view first when you enter the organization.

Select

Simplified user experience

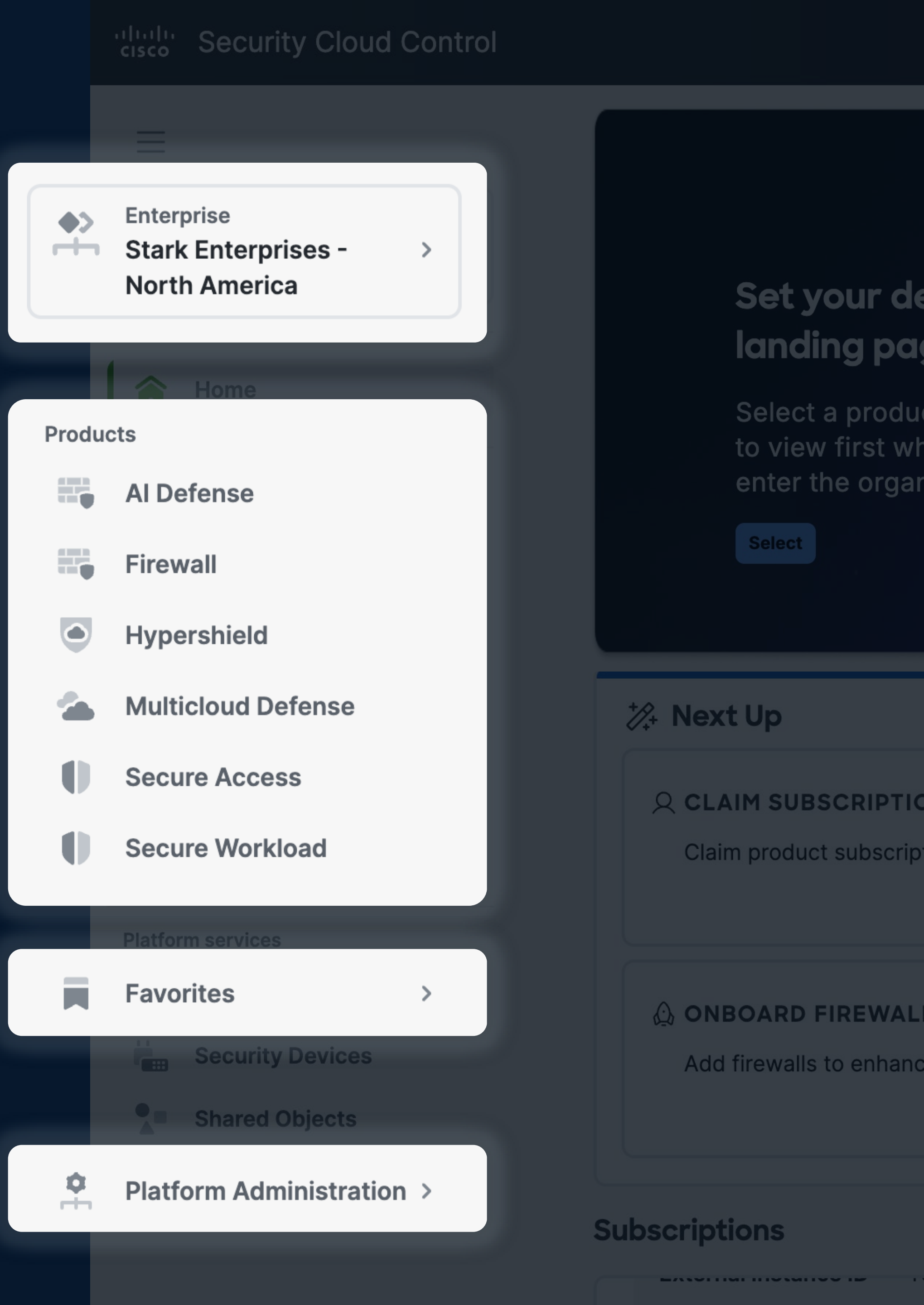
Faster time to value

Access full product capabilities
One integrated environment

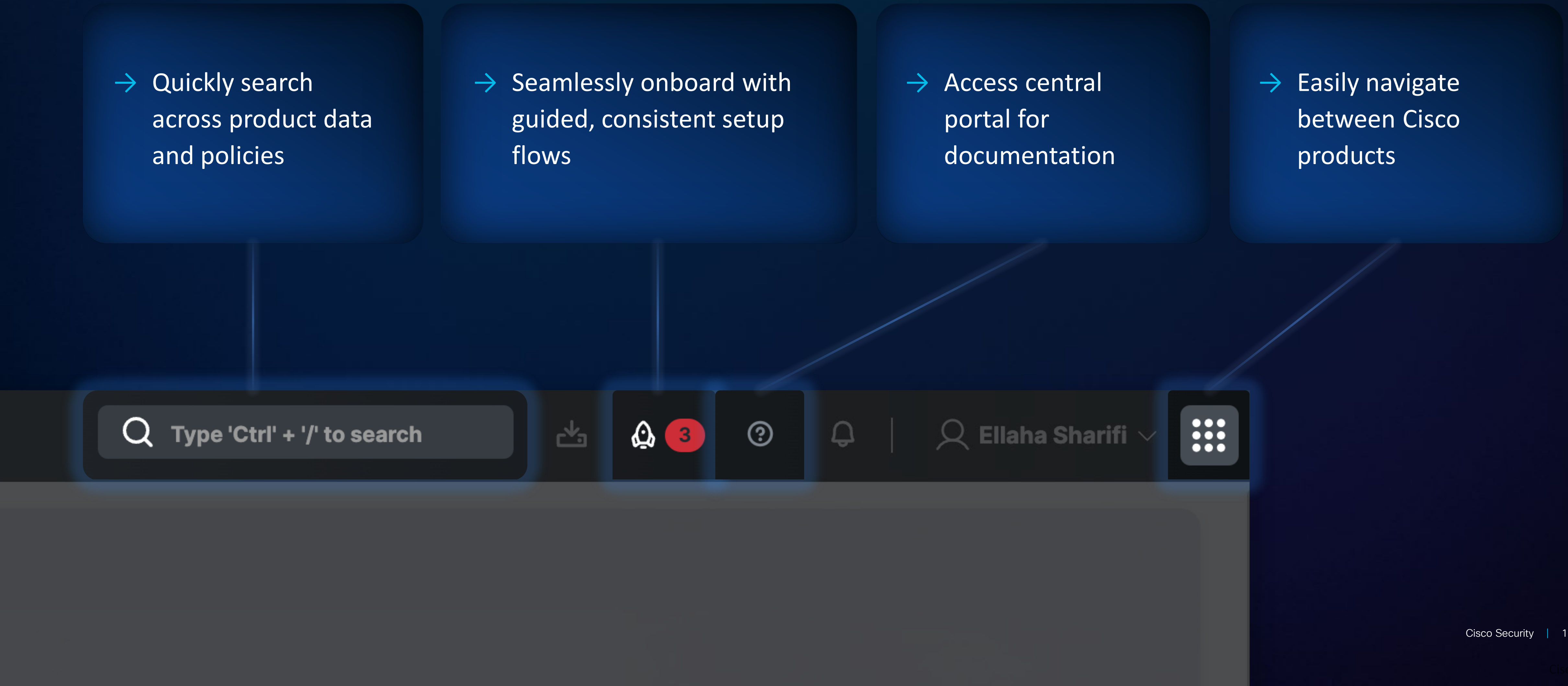
Efficiently onboard new products
Guided set-up experience

Minimize learning curves
Consistent UX across products

Quickly access essential features
Customizable interface



Common search, help, and notifications



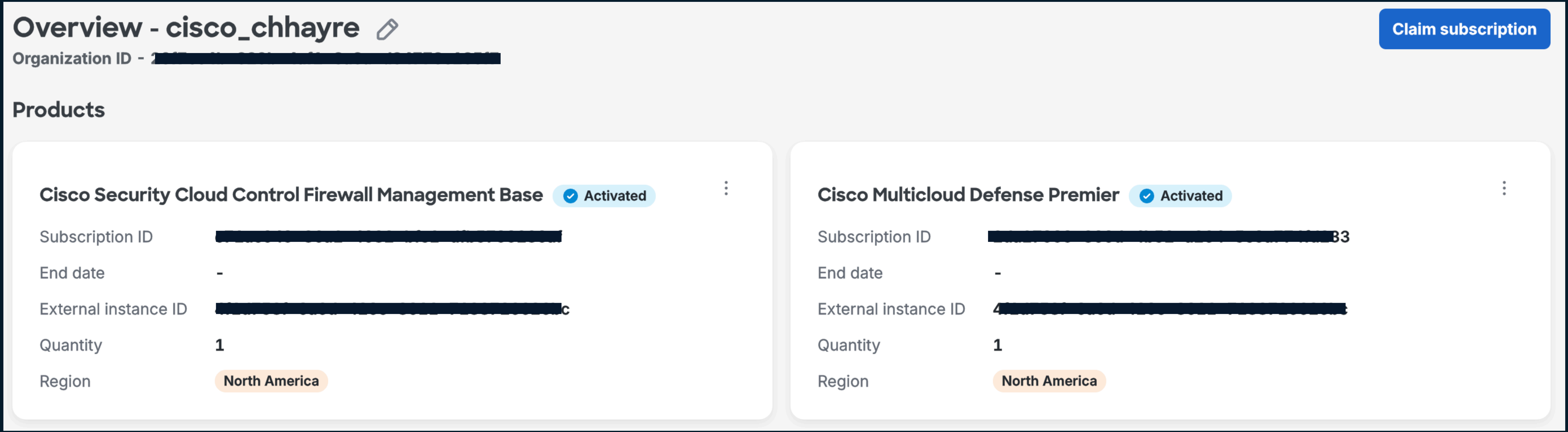
→ Quickly search across product data and policies

→ Seamlessly onboard with guided, consistent setup flows

→ Access central portal for documentation

→ Easily navigate between Cisco products

Onboarding and provisioning



Overview - cisco_chhayre

Organization ID - [redacted]

Claim subscription

Products

Cisco Security Cloud Control Firewall Management Base ✓ Activated

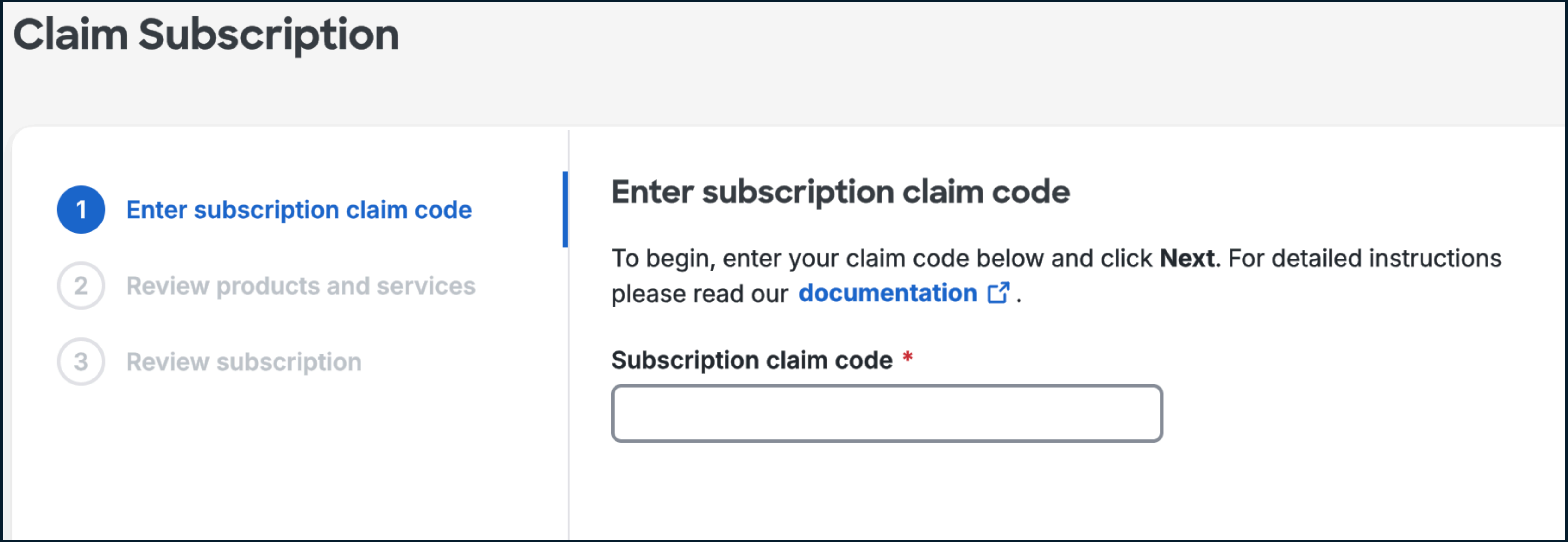
Subscription ID	[redacted]
End date	-
External instance ID	[redacted]
Quantity	1
Region	North America

Cisco Multicloud Defense Premier ✓ Activated

Subscription ID	[redacted]
End date	-
External instance ID	[redacted]
Quantity	1
Region	North America

cisco Connect

Onboarding and provisioning (continued)



Claim Subscription

1 Enter subscription claim code

2 Review products and services

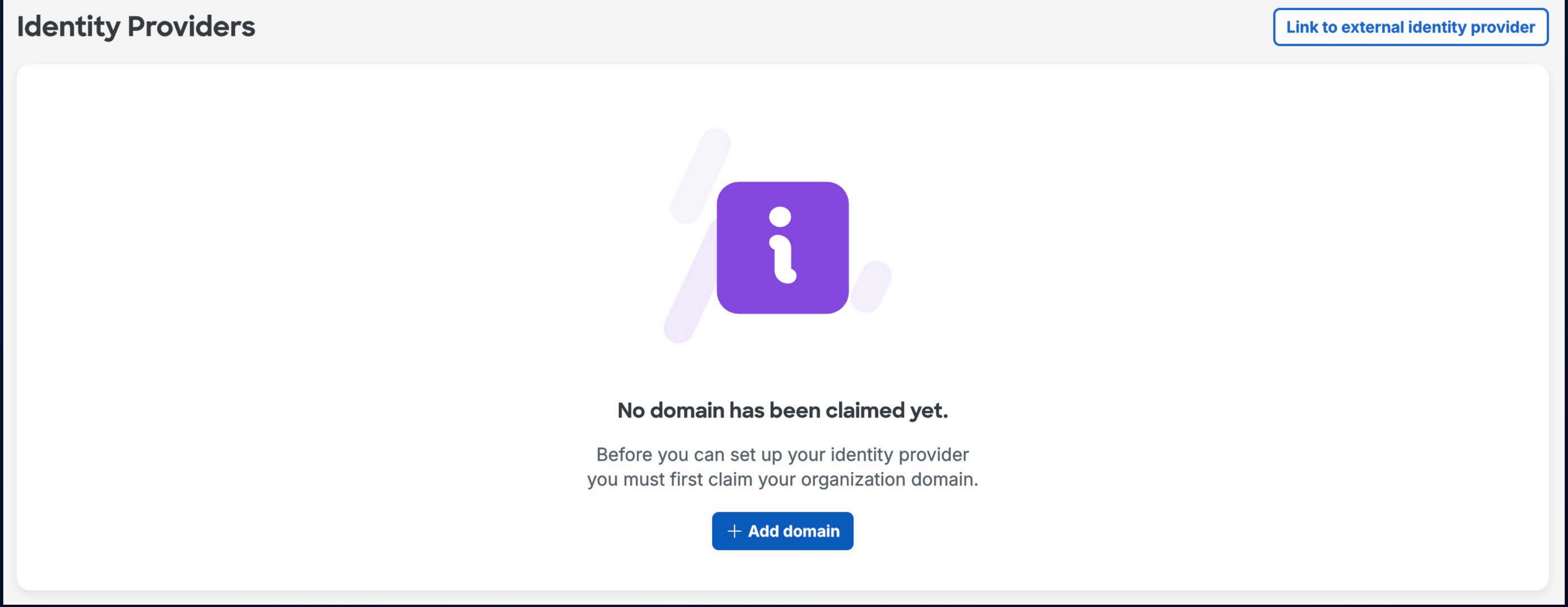
3 Review subscription

Enter subscription claim code

To begin, enter your claim code below and click **Next**. For detailed instructions please read our **documentation** .

Subscription claim code *

Bring your own identity (or use ours)



Identity Providers

No domain has been claimed yet.

Before you can set up your identity provider
you must first claim your organization domain.

Simplified user experience

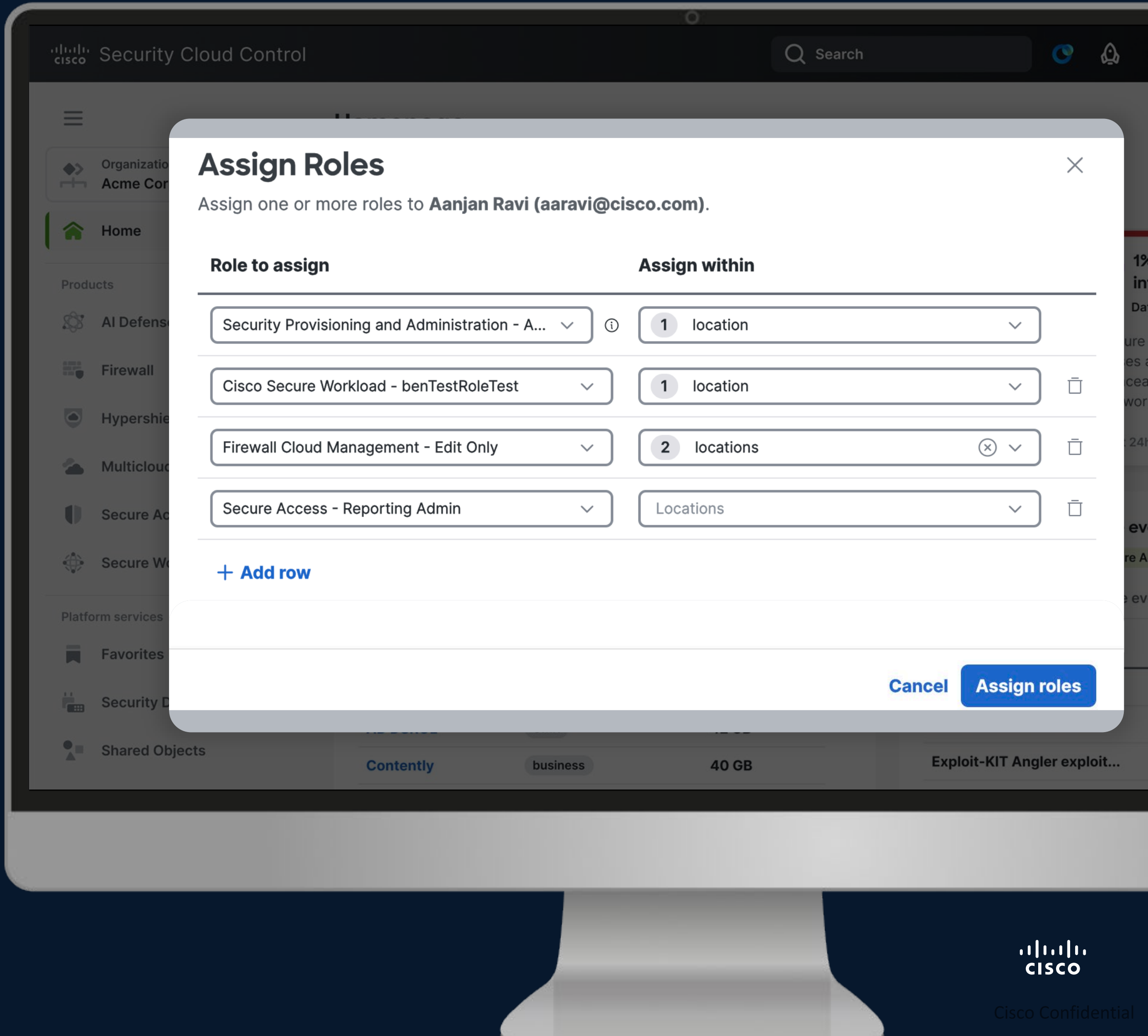
Centralized role-based access control (RBAC)

Accelerate access control
One interface

Streamline user management
Consolidated IDP integration

Strengthen compliance & oversite
Comprehensive audit log

Ease collaboration
Shared content across personas



Assign Roles

Assign one or more roles to **Aanjan Ravi (aaravi@cisco.com)**.

Role to assign	Assign within
Security Provisioning and Administration - A...	1 location
Cisco Secure Workload - benTestRoleTest	1 location
Firewall Cloud Management - Edit Only	2 locations
Secure Access - Reporting Admin	Locations

+ Add row

Cancel   Assign roles

Faster, more intelligent security

Unified AI Assistant

Single conversational interface

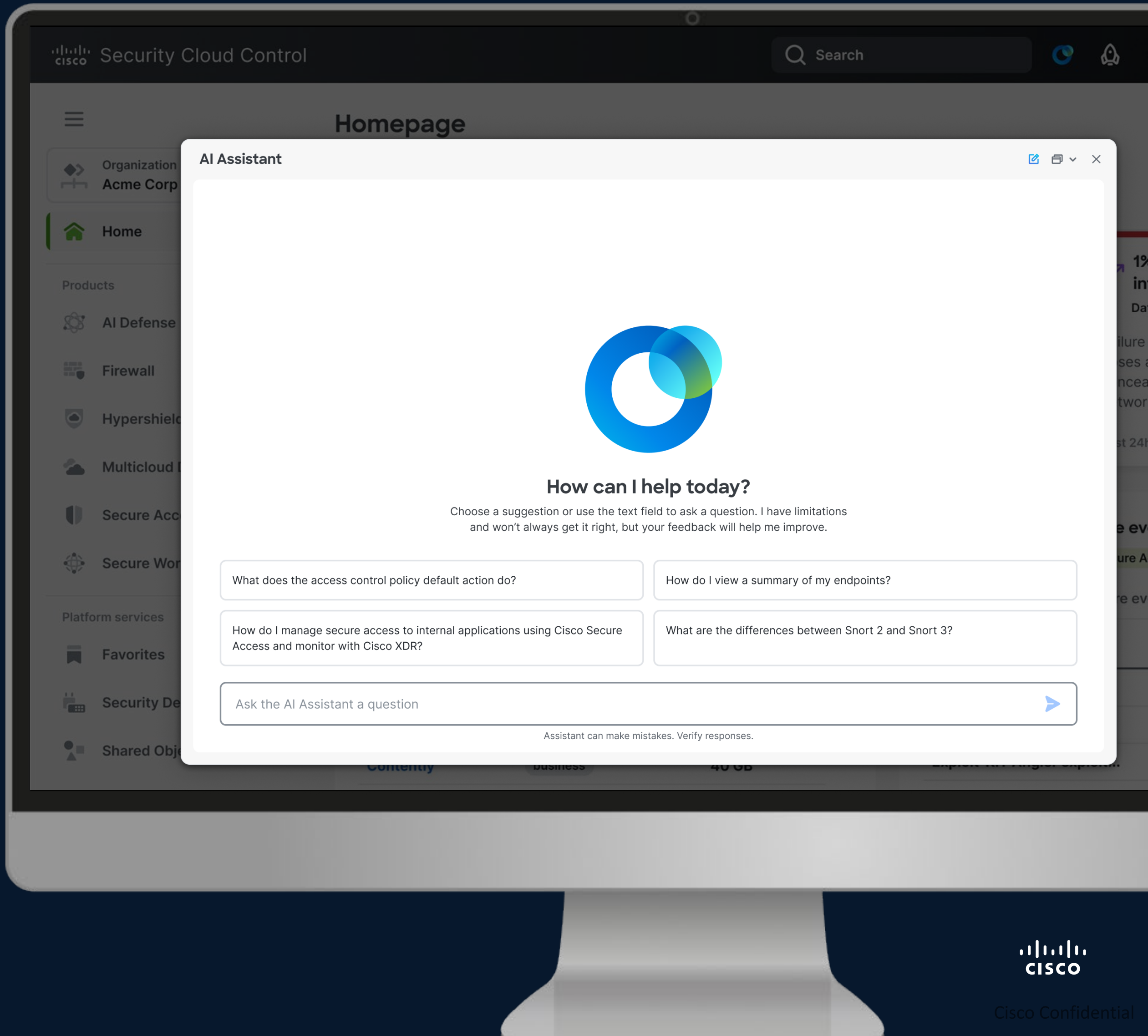
One assistant augments troubleshooting across products

Centralized product insights

Capabilities from Secure Firewall, Secure Access, and Hypershield

Unified knowledge hub

Documentation access across products for comprehensive guidance



How can I help today?

Choose a suggestion or use the text field to ask a question. I have limitations and won't always get it right, but your feedback will help me improve.

What does the access control policy default action do?

How do I view a summary of my endpoints?

How do I manage secure access to internal applications using Cisco Secure Access and monitor with Cisco XDR?

What are the differences between Snort 2 and Snort 3?

Ask the AI Assistant a question

Assistant can make mistakes. Verify responses.

Faster, more intelligent security

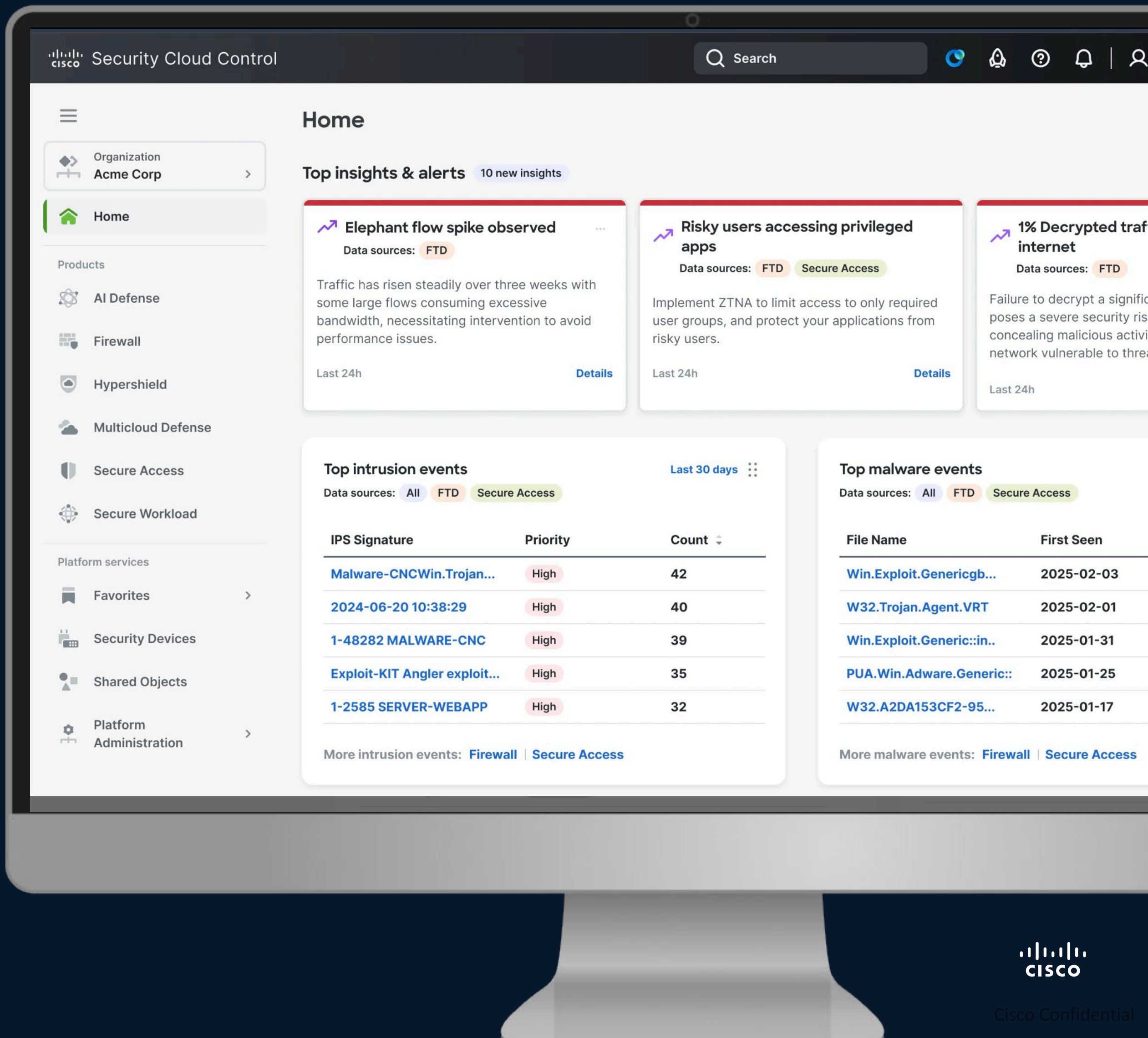
Informed decisions with AIOps

Discover patterns in security events
using predictive analytics

Quickly strengthen security posture
with AI-guided best practices

Reduce mean time to resolution
through risk-based prioritization

Get the most out of security spending
by leveraging the feature utilization overview



Home

Top insights & alerts 10 new insights

Elephant flow spike observed
Data sources: FTD
Traffic has risen steadily over three weeks with some large flows consuming excessive bandwidth, necessitating intervention to avoid performance issues.
Last 24h Details

Risky users accessing privileged apps
Data sources: FTD Secure Access
Implement ZTNA to limit access to only required user groups, and protect your applications from risky users.
Last 24h Details

1% Decrypted traf
internet
Data sources: FTD
Failure to decrypt a signific
poses a severe security ris
concealing malicious activi
network vulnerable to threa
Last 24h

Top intrusion events Last 30 days
Data sources: All FTD Secure Access

IPS Signature	Priority	Count
Malware-CNCWin.Trojan...	High	42
2024-06-20 10:38:29	High	40
1-48282 MALWARE-CNC	High	39
Exploit-KIT Angler exploit...	High	35
1-2585 SERVER-WEBAPP	High	32

More intrusion events: Firewall | Secure Access

Top malware events
Data sources: All FTD Secure Access

File Name	First Seen
Win.Exploit.Genericgb...	2025-02-03
W32.Trojan.Agent.VRT	2025-02-01
Win.Exploit.Generic::in..	2025-01-31
PUA.Win.Adware.Generic::	2025-01-25
W32.A2DA153CF2-95...	2025-01-17

More malware events: Firewall | Secure Access

Integrations & Common Services

Unified Endpoint Experience – Cisco Secure Client

- Zero Trust Network Access
- VPN
- Security Services Edge
- Observability
- Endpoint Detection and Response
- Posture
- Full Endpoint Visibility

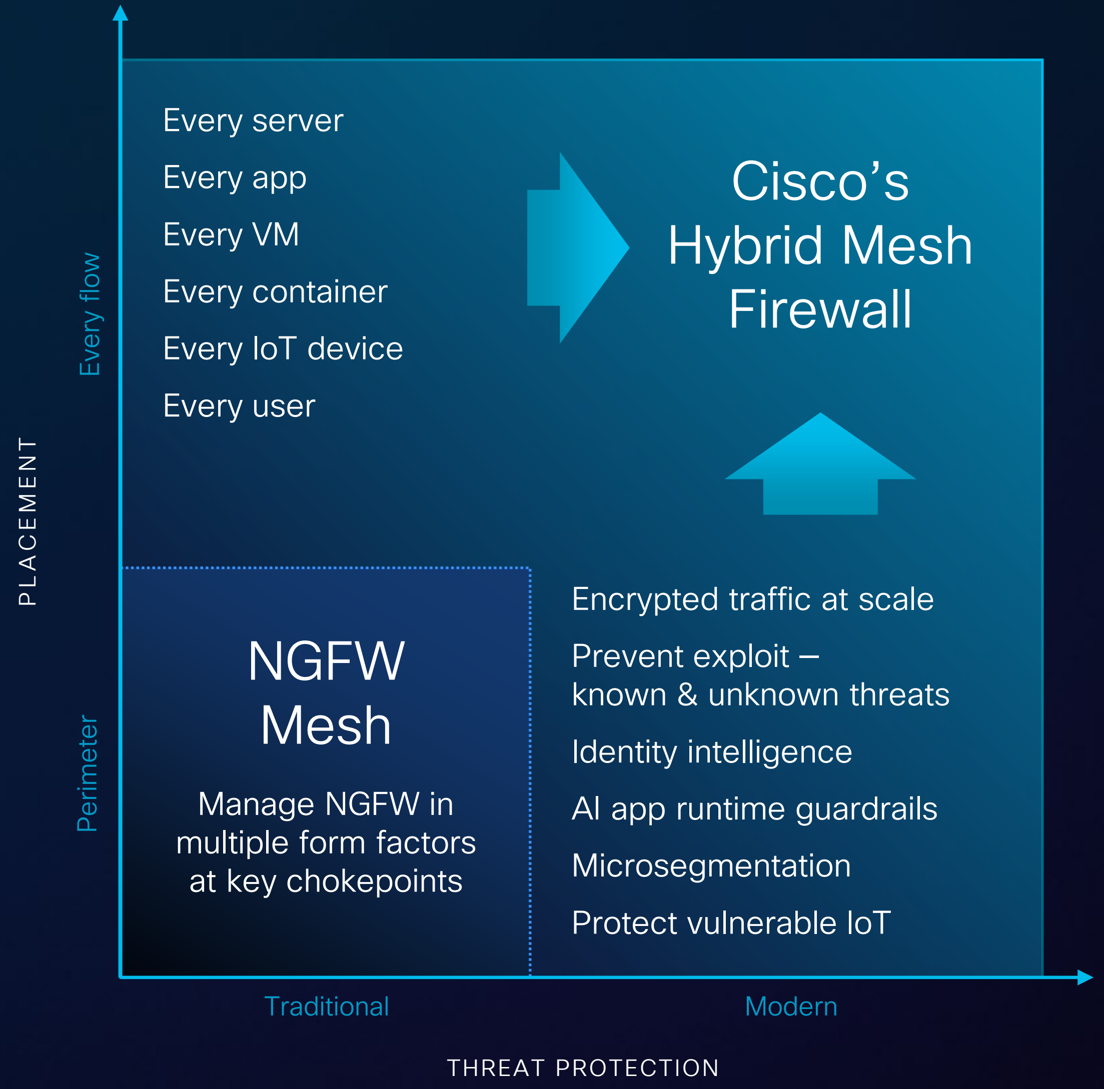
Cloud management capable

Firewall Management

Firewalling needs to evolve to meet today’s challenges

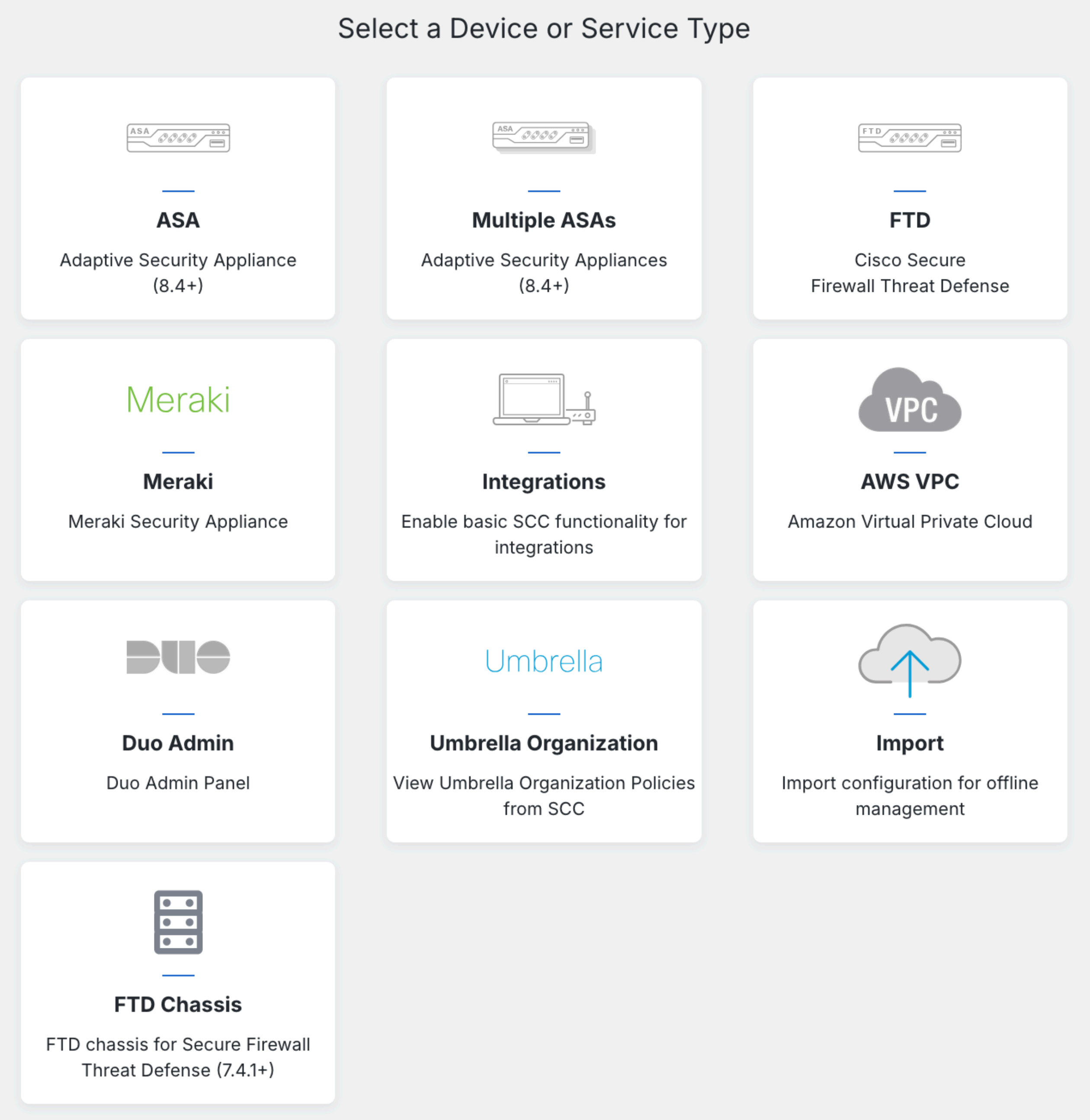
OUR NORTH STAR

Make it easy for organizations to reduce attack surface, prevent compromise, and stop lateral movement in the modern data center, cloud, campus, and factory



Unified Device Onboarding

For Network Security Devices



Select a Device or Service Type

ASA
Adaptive Security Appliance (8.4+)

Multiple ASAs
Adaptive Security Appliances (8.4+)

FTD
Cisco Secure Firewall Threat Defense

Meraki
Meraki Security Appliance

Integrations
Enable basic SCC functionality for integrations

AWS VPC
Amazon Virtual Private Cloud

Duo Admin
Duo Admin Panel

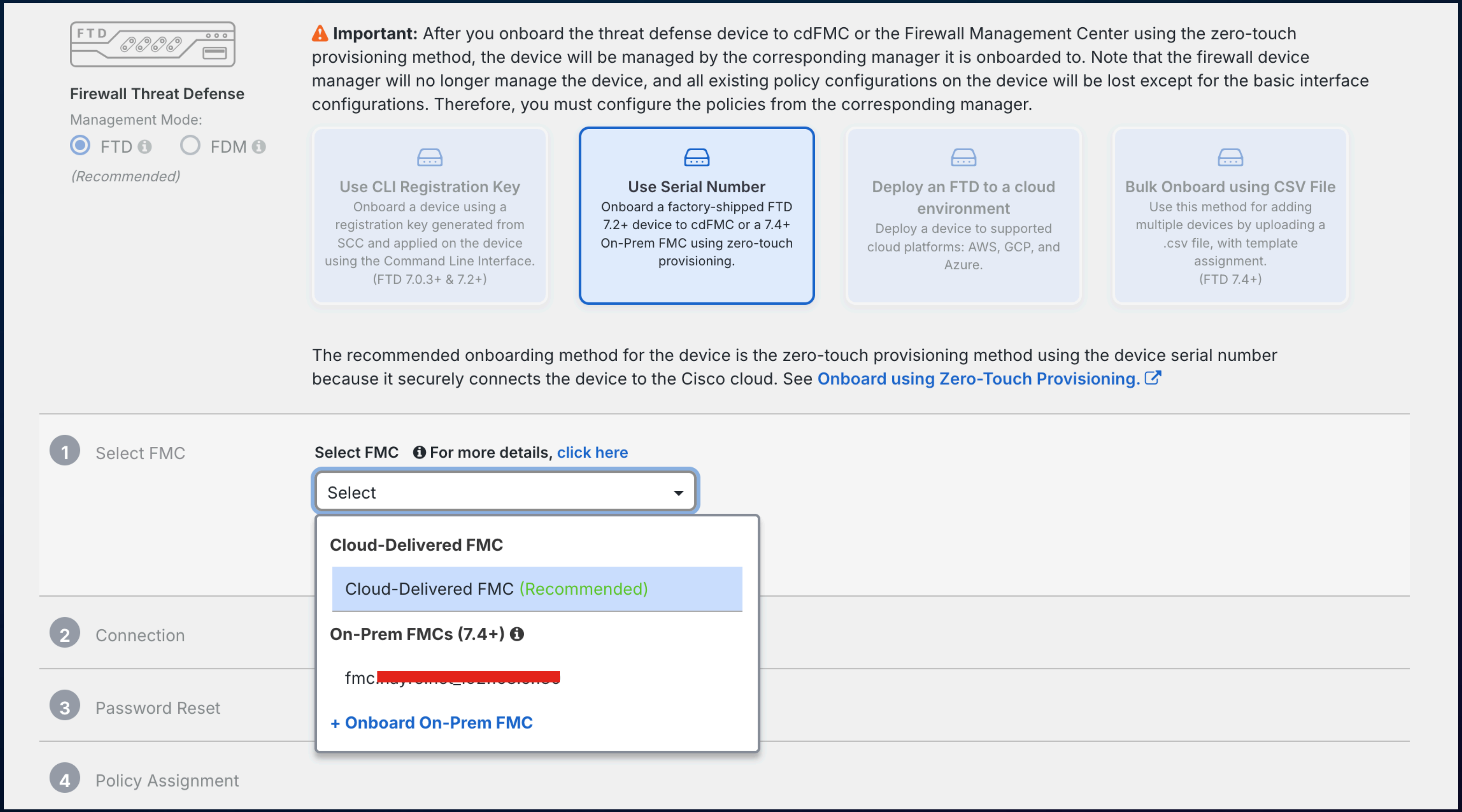
Umbrella Organization
View Umbrella Organization Policies from SCC

Import
Import configuration for offline management

FTD Chassis
FTD chassis for Secure Firewall Threat Defense (7.4.1+)

FTD 7.2+
FMC 7.4+ (on-prem)

Zero-touch Provisioning



FTD

Firewall Threat Defense

Management Mode:

● FTD ○ FDM

(Recommended)

⚠ **Important:** After you onboard the threat defense device to cdFMC or the Firewall Management Center using the zero-touch provisioning method, the device will be managed by the corresponding manager it is onboarded to. Note that the firewall device manager will no longer manage the device, and all existing policy configurations on the device will be lost except for the basic interface configurations. Therefore, you must configure the policies from the corresponding manager.

Use CLI Registration Key
Onboard a device using a registration key generated from SCC and applied on the device using the Command Line Interface. (FTD 7.0.3+ & 7.2+)

Use Serial Number
Onboard a factory-shipped FTD 7.2+ device to cdFMC or a 7.4+ On-Prem FMC using zero-touch provisioning.

Deploy an FTD to a cloud environment
Deploy a device to supported cloud platforms: AWS, GCP, and Azure.

Bulk Onboard using CSV File
Use this method for adding multiple devices by uploading a .csv file, with template assignment. (FTD 7.4+)

The recommended onboarding method for the device is the zero-touch provisioning method using the device serial number because it securely connects the device to the Cisco cloud. See **Onboard using Zero-Touch Provisioning.**

1 Select FMC

Select FMC ℹ **For more details, click here**

Select ▾

Cloud-Delivered FMC

Cloud-Delivered FMC (Recommended)

On-Prem FMCs (7.4+) ℹ

fmc[redacted]

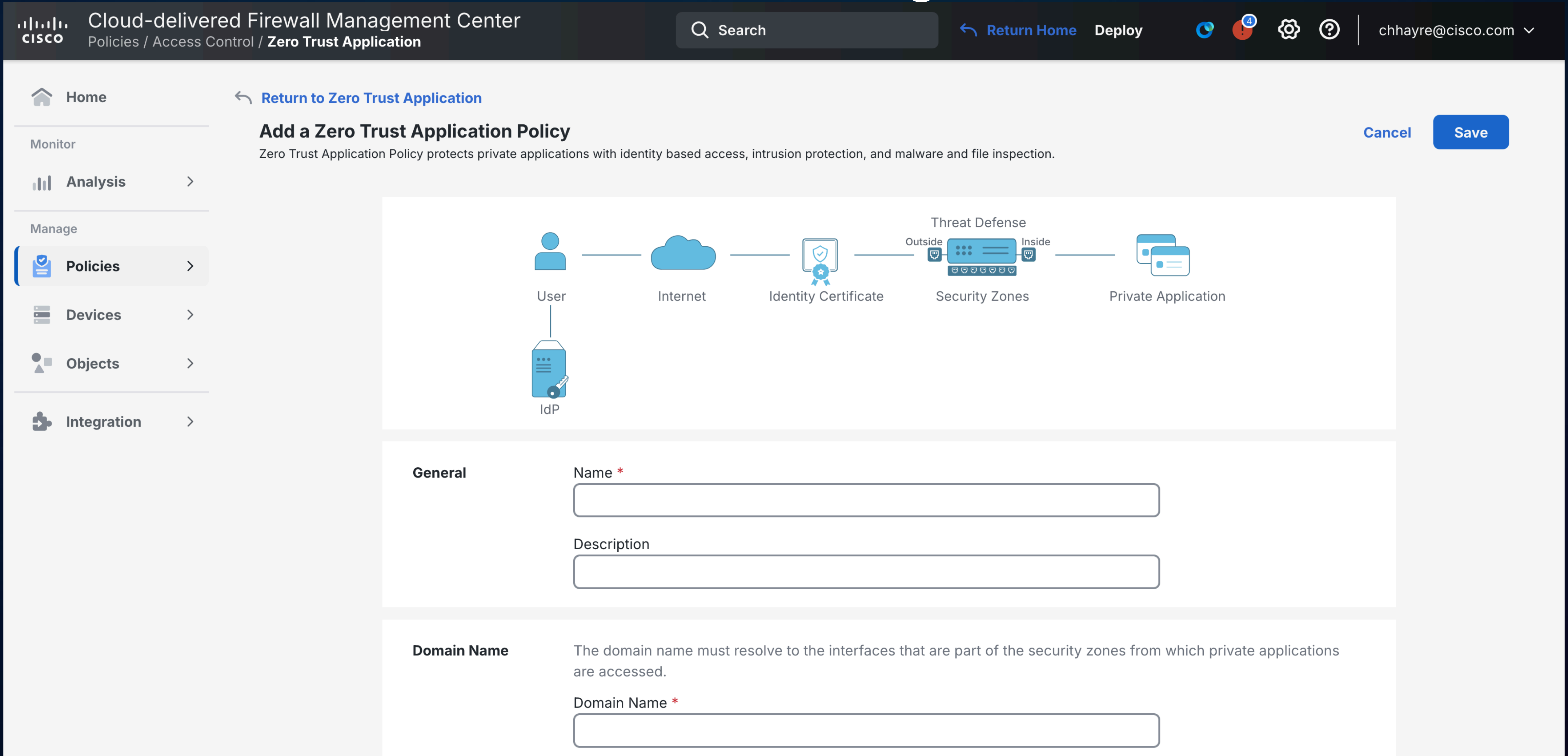
+ Onboard On-Prem FMC

2 Connection

3 Password Reset

4 Policy Assignment

Cloud-delivered Firewall Management Center



Add a Zero Trust Application Policy

Zero Trust Application Policy protects private applications with identity based access, intrusion protection, and malware and file inspection.

General

Name *

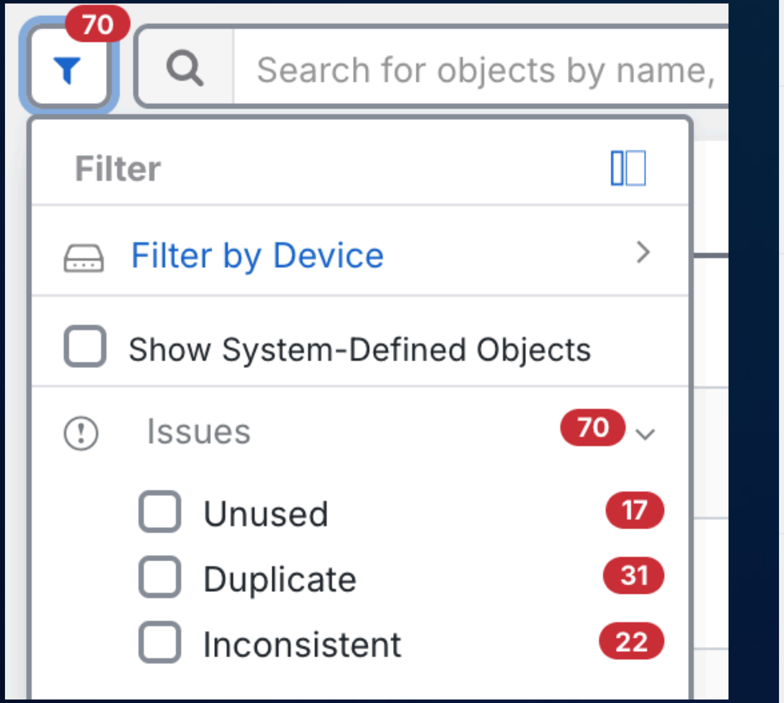
Description

Domain Name

The domain name must resolve to the interfaces that are part of the security zones from which private applications are accessed.

Domain Name *

Single-click object cleanup



70

Search for objects by name,

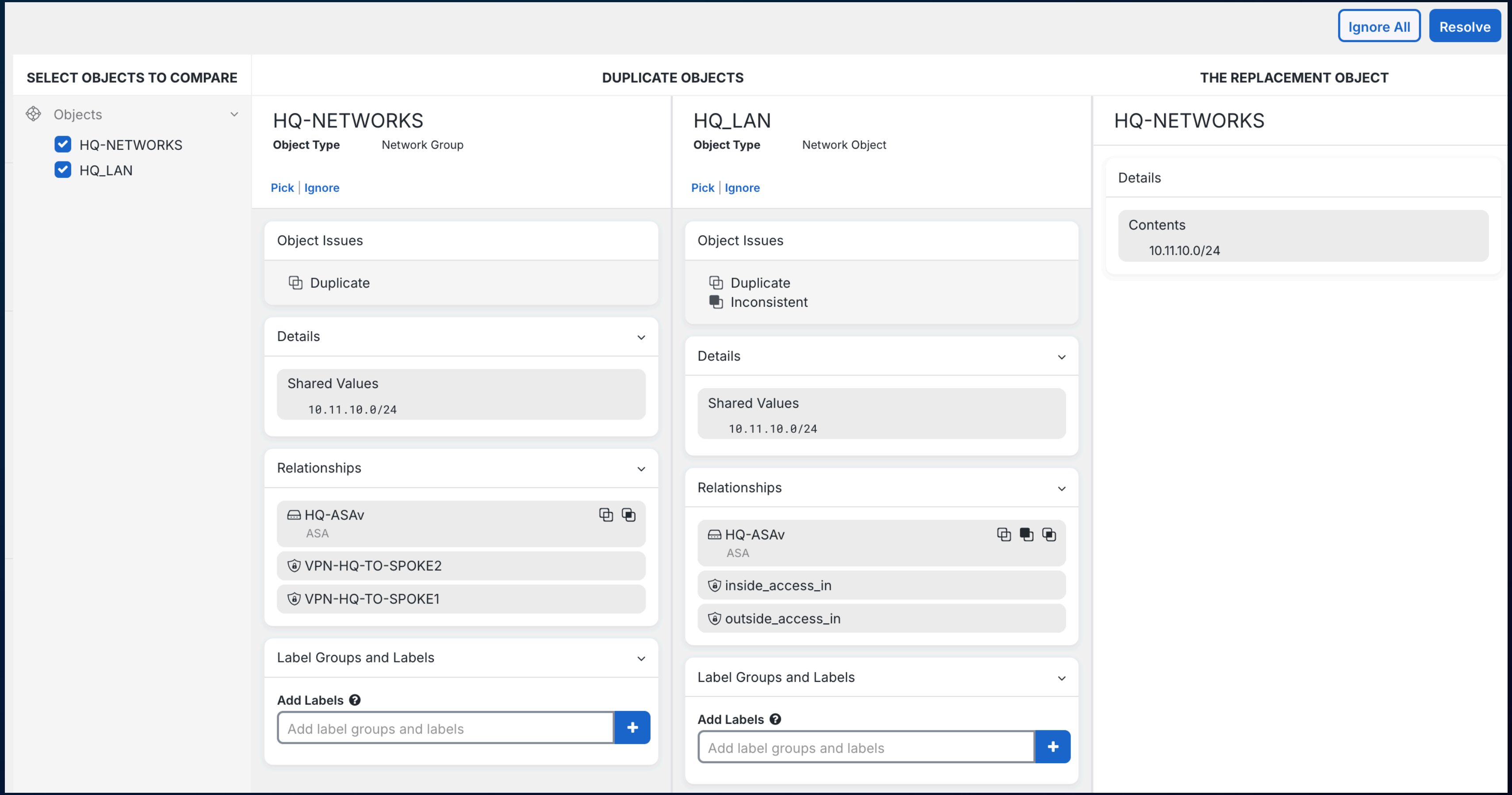
Filter

Filter by Device

□ Show System-Defined Objects

Issues 70

□ Unused	17
□ Duplicate	31
□ Inconsistent	22



Ignore All | Resolve

SELECT OBJECTS TO COMPARE

Objects

☑ HQ-NETWORKS

☑ HQ_LAN

DUPLICATE OBJECTS

HQ-NETWORKS

Object Type Network Group

Pick | Ignore

Object Issues

Duplicate

Details

Shared Values

`10.11.10.0/24`

Relationships

HQ-ASAv
ASA

VPN-HQ-TO-SPOKE2

VPN-HQ-TO-SPOKE1

Label Groups and Labels

Add Labels

Add label groups and labels +

HQ_LAN

Object Type Network Object

Pick | Ignore

Object Issues

Duplicate

Inconsistent

Details

Shared Values

`10.11.10.0/24`

Relationships

HQ-ASAv
ASA

inside_access_in

outside_access_in

Label Groups and Labels

Add Labels

Add label groups and labels +

THE REPLACEMENT OBJECT

HQ-NETWORKS

Details

Contents

10.11.10.0/24

Enhance security

Optimize policies tailored to your environment

Policy analyzer and optimizer

Minimize misconfigurations and downtime

Improve firewall performance

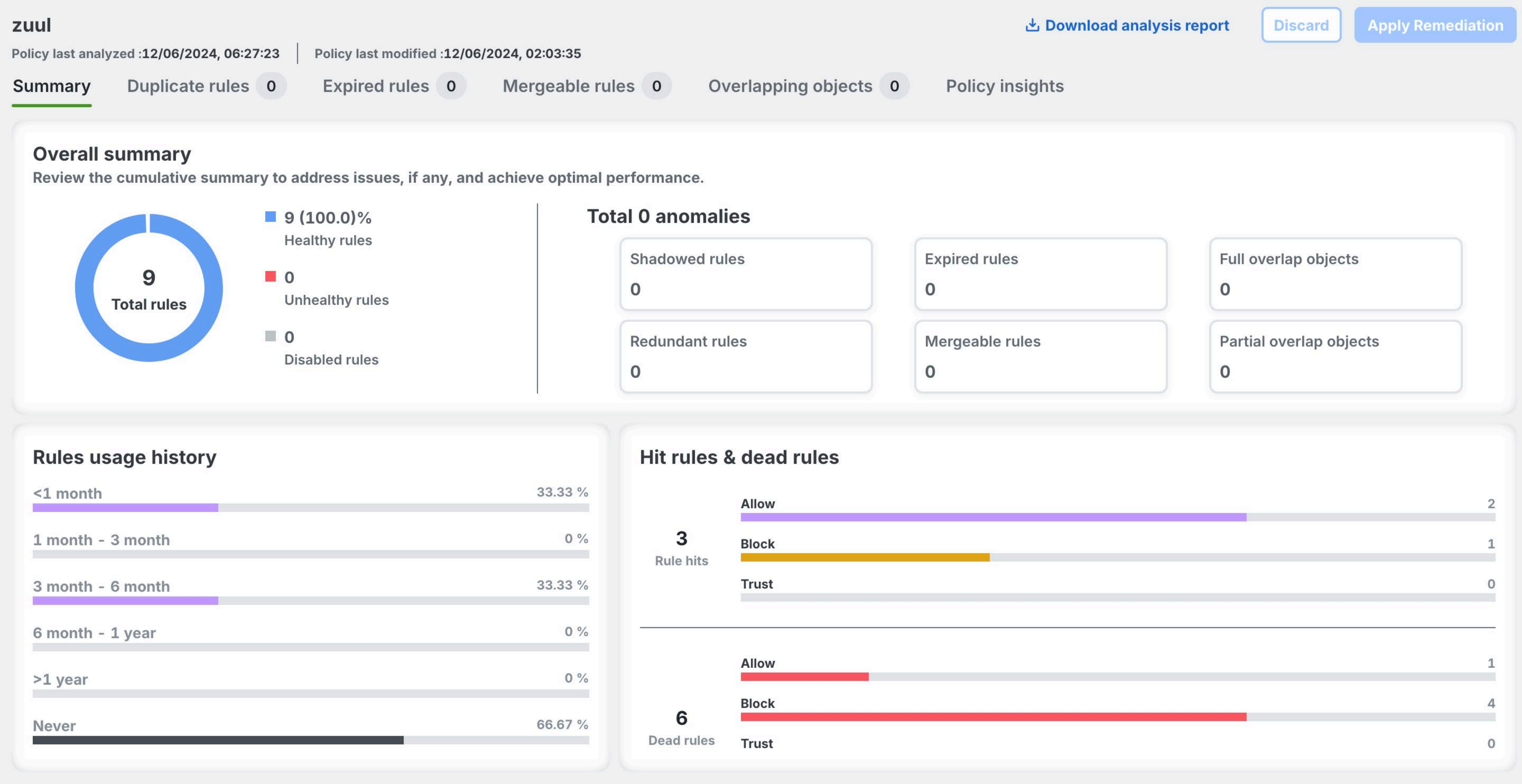
Speed up policy deployment and updates

Aid collaboration with the AI Assistant

Address issues such as overlapping, hidden, or overly broad rules

Improve overall security posture

Policy Analysis and Optimizer



zuul

Download analysis report | Discard | Apply Remediation

Policy last analyzed :12/06/2024, 06:27:23 | Policy last modified :12/06/2024, 02:03:35

Summary | Duplicate rules 0 | Expired rules 0 | Mergeable rules 0 | Overlapping objects 0 | Policy insights

Overall summary

Review the cumulative summary to address issues, if any, and achieve optimal performance.

9 Total rules

- 🟦 9 (100.0)% Healthy rules
- 🟥 0 Unhealthy rules
- ⬜ 0 Disabled rules

Total 0 anomalies

Shadowed rules 0	Expired rules 0	Full overlap objects 0
Redundant rules 0	Mergeable rules 0	Partial overlap objects 0

Rules usage history

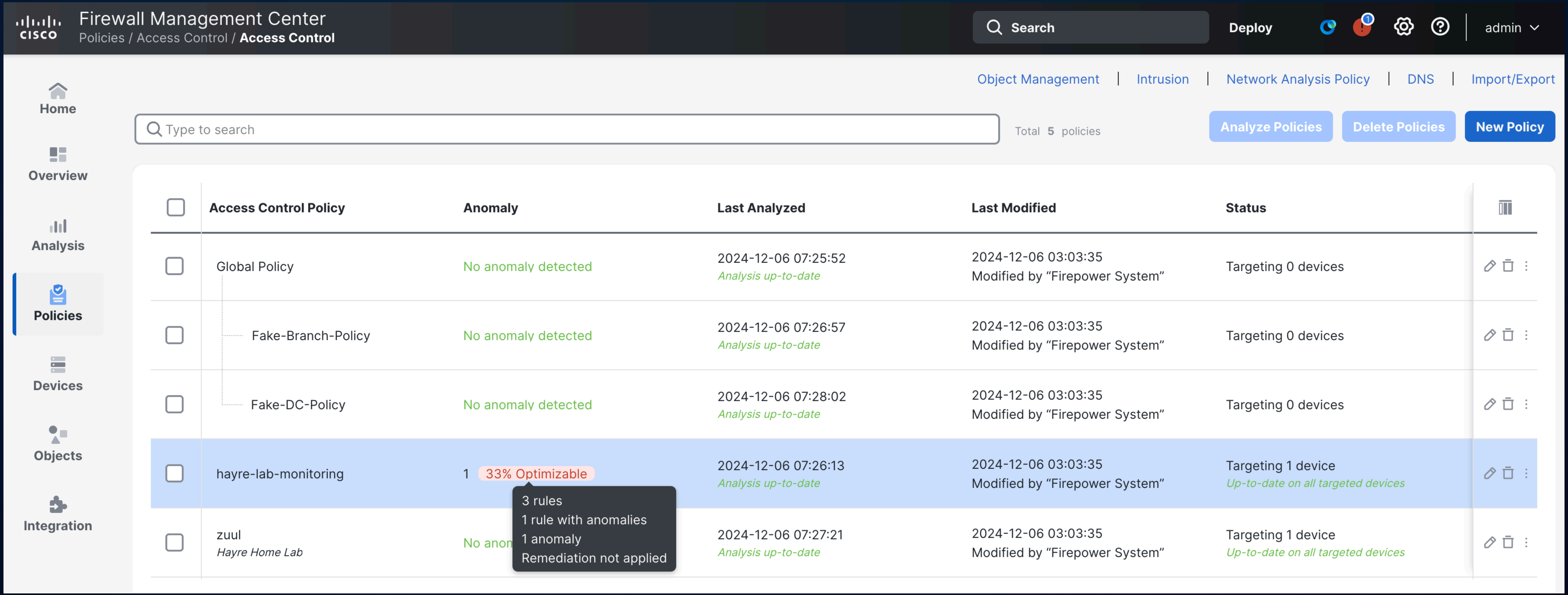
<1 month	33.33 %
1 month - 3 month	0 %
3 month - 6 month	33.33 %
6 month - 1 year	0 %
>1 year	0 %
Never	66.67 %

Hit rules & dead rules

3 Rule hits	Allow	2
	Block	1
	Trust	0
6 Dead rules	Allow	1
	Block	4
	Trust	0

FMC 7.6+ (on-prem)

Policy Analysis and Optimizer for on-prem

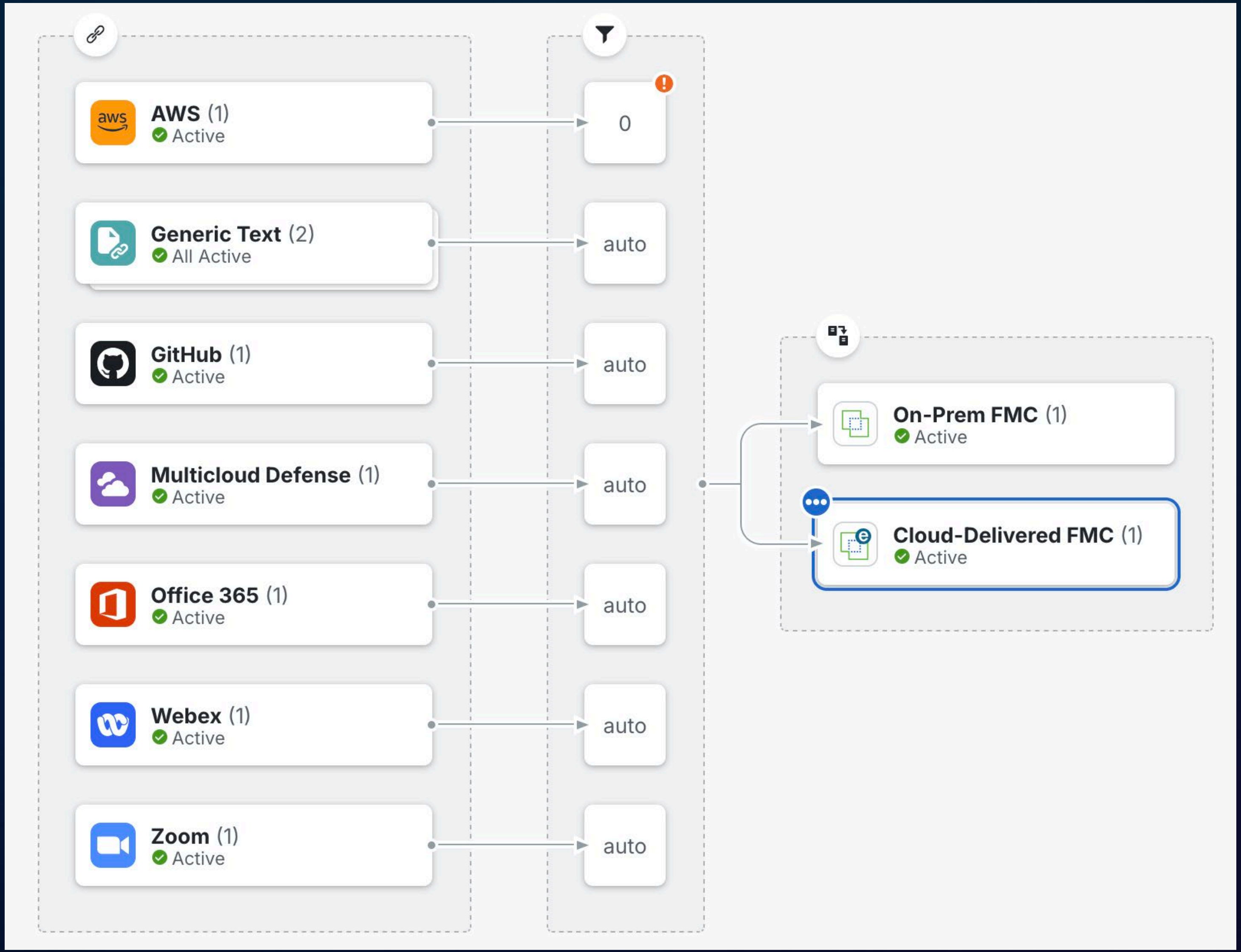

cisco
Firewall Management Center
Policies / Access Control / **Access Control**
Search
Deploy
admin
Home
Overview
Analysis
Policies
Devices
Objects
Integration
Object Management | Intrusion | Network Analysis Policy | DNS | Import/Export
Type to search
Analyze Policies
Delete Policies
New Policy

Total 5 policies

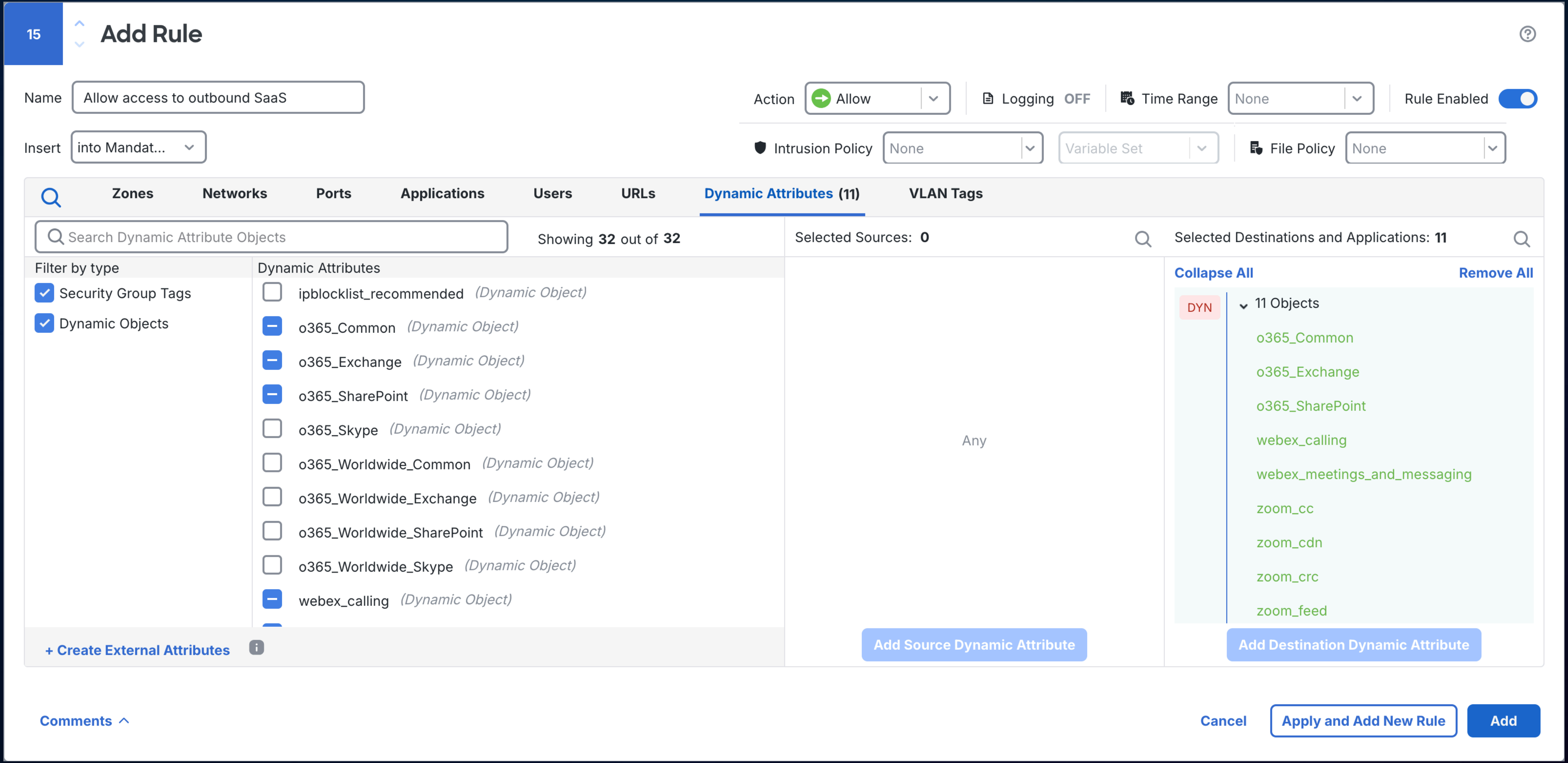
□	Access Control Policy	Anomaly	Last Analyzed	Last Modified	Status
□	Global Policy	No anomaly detected	2024-12-06 07:25:52 *Analysis up-to-date*	2024-12-06 03:03:35 Modified by “Firepower System”	Targeting 0 devices
□	Fake-Branch-Policy	No anomaly detected	2024-12-06 07:26:57 *Analysis up-to-date*	2024-12-06 03:03:35 Modified by “Firepower System”	Targeting 0 devices
□	Fake-DC-Policy	No anomaly detected	2024-12-06 07:28:02 *Analysis up-to-date*	2024-12-06 03:03:35 Modified by “Firepower System”	Targeting 0 devices
□	hayre-lab-monitoring	1 33% Optimizable	2024-12-06 07:26:13 *Analysis up-to-date*	2024-12-06 03:03:35 Modified by “Firepower System”	Targeting 1 device *Up-to-date on all targeted devices*
□	zuul *Hayre Home Lab*	No anon	2024-12-06 07:27:21 *Analysis up-to-date*	2024-12-06 03:03:35 Modified by “Firepower System”	Targeting 1 device *Up-to-date on all targeted devices*

3 rules
1 rule with anomalies
1 anomaly
Remediation not applied

Dynamic Attribute Connector



Dynamic Firewall Objects



15 **Add Rule**

Name: Allow access to outbound SaaS

Insert: into Mandat...

Action: Allow

Logging OFF

Time Range: None

Rule Enabled

Intrusion Policy: None

Variable Set

File Policy: None

Showing 32 out of 32

Filter by type

- ☑ Security Group Tags
- ☑ Dynamic Objects

Dynamic Attributes

- □ ipblocklist_recommended *(Dynamic Object)*
- ⊟ o365_Common *(Dynamic Object)*
- ⊟ o365_Exchange *(Dynamic Object)*
- ⊟ o365_SharePoint *(Dynamic Object)*
- □ o365_Skype *(Dynamic Object)*
- □ o365_Worldwide_Common *(Dynamic Object)*
- □ o365_Worldwide_Exchange *(Dynamic Object)*
- □ o365_Worldwide_SharePoint *(Dynamic Object)*
- □ o365_Worldwide_Skype *(Dynamic Object)*
- ⊟ webex_calling *(Dynamic Object)*

Selected Sources: 0

Any

Selected Destinations and Applications: 11

DYN 11 Objects

- o365_Common
- o365_Exchange
- o365_SharePoint
- webex_calling
- webex_meetings_and_messaging
- zoom_cc
- zoom_cdn
- zoom_crc
- zoom_feed

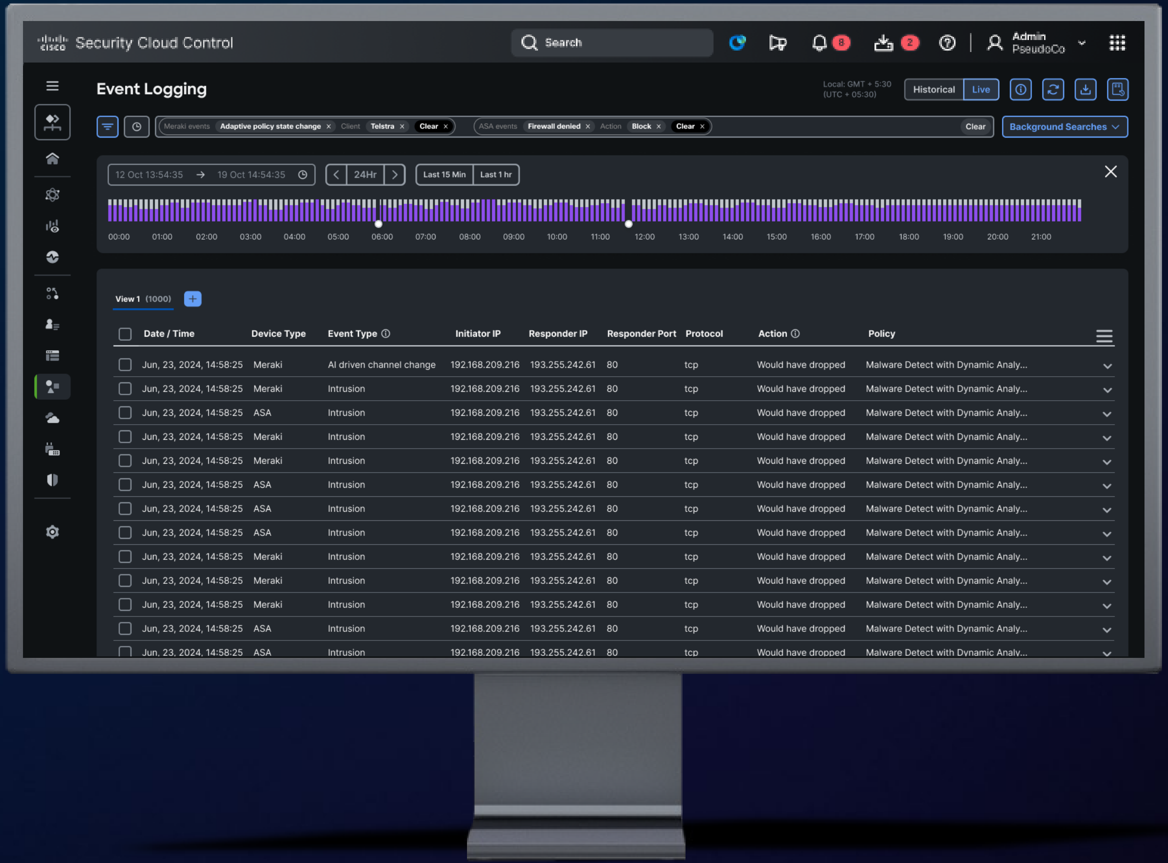
Simplify operations

Achieve instant visibility into network and security logging

Centralize event viewing and log retention for 90 days (default) up to 3 years

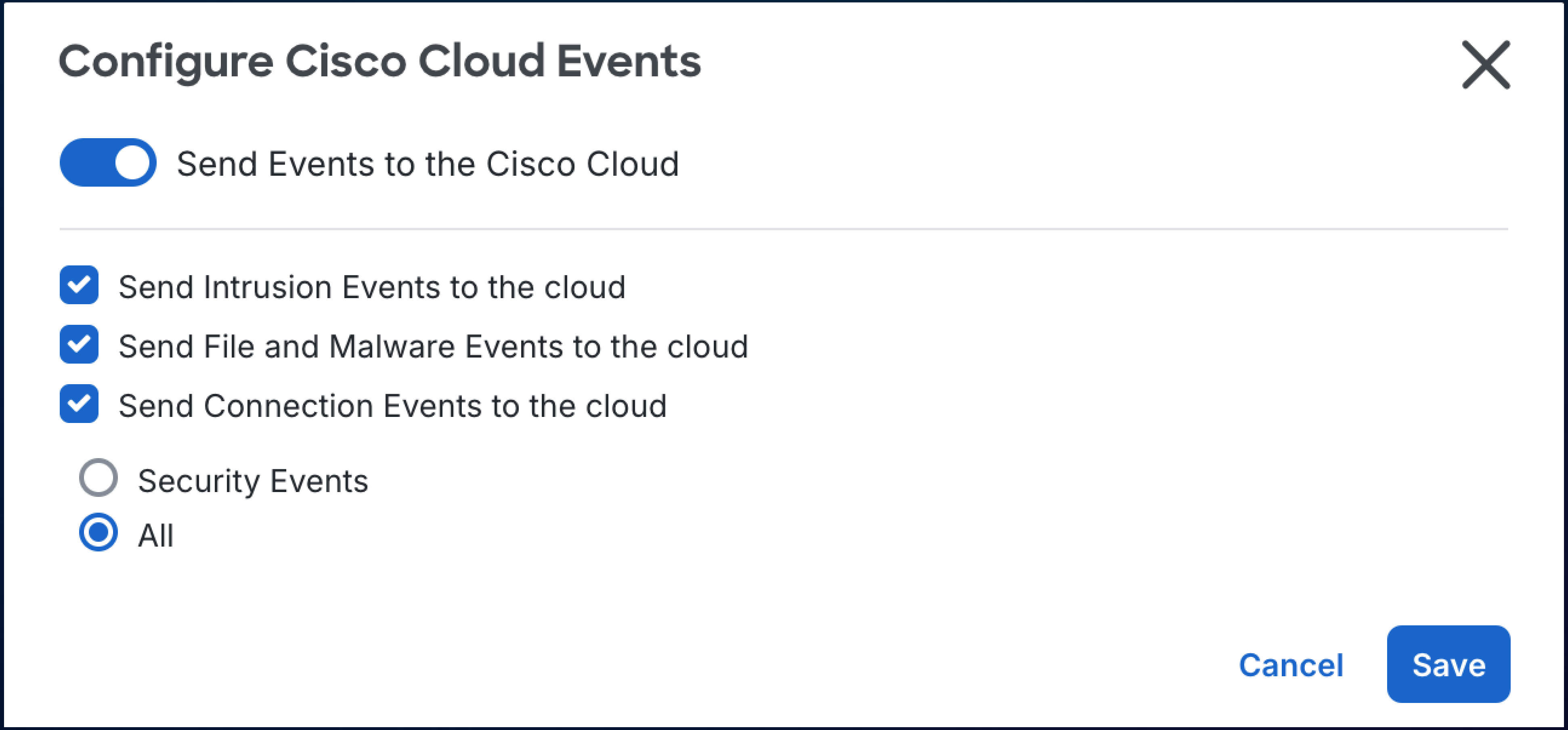
Supports **all** FTD & ASA firewall devices

Scales to 200,000 events per second



□	Date / Time	Device Type	Event Type ⓘ	Initiator IP	Responder IP	Responder Port	Protocol	Action ⓘ	Policy
□	Jun, 23, 2024, 14:58:25	Meraki	AI driven channel change	192.168.209.216	193.255.242.61	80	tcp	Would have dropped	Malware Detect with Dynamic Analy...
□	Jun, 23, 2024, 14:58:25	Meraki	Intrusion	192.168.209.216	193.255.242.61	80	tcp	Would have dropped	Malware Detect with Dynamic Analy...
□	Jun, 23, 2024, 14:58:25	ASA	Intrusion	192.168.209.216	193.255.242.61	80	tcp	Would have dropped	Malware Detect with Dynamic Analy...
□	Jun, 23, 2024, 14:58:25	Meraki	Intrusion	192.168.209.216	193.255.242.61	80	tcp	Would have dropped	Malware Detect with Dynamic Analy...
□	Jun, 23, 2024, 14:58:25	Meraki	Intrusion	192.168.209.216	193.255.242.61	80	tcp	Would have dropped	Malware Detect with Dynamic Analy...
□	Jun, 23, 2024, 14:58:25	ASA	Intrusion	192.168.209.216	193.255.242.61	80	tcp	Would have dropped	Malware Detect with Dynamic Analy...
□	Jun, 23, 2024, 14:58:25	ASA	Intrusion	192.168.209.216	193.255.242.61	80	tcp	Would have dropped	Malware Detect with Dynamic Analy...
□	Jun, 23, 2024, 14:58:25	ASA	Intrusion	192.168.209.216	193.255.242.61	80	tcp	Would have dropped	Malware Detect with Dynamic Analy...
□	Jun, 23, 2024, 14:58:25	Meraki	Intrusion	192.168.209.216	193.255.242.61	80	tcp	Would have dropped	Malware Detect with Dynamic Analy...
□	Jun, 23, 2024, 14:58:25	Meraki	Intrusion	192.168.209.216	193.255.242.61	80	tcp	Would have dropped	Malware Detect with Dynamic Analy...
□	Jun, 23, 2024, 14:58:25	Meraki	Intrusion	192.168.209.216	193.255.242.61	80	tcp	Would have dropped	Malware Detect with Dynamic Analy...
□	Jun, 23, 2024, 14:58:25	ASA	Intrusion	192.168.209.216	193.255.242.61	80	tcp	Would have dropped	Malware Detect with Dynamic Analy...
□	Jun. 23. 2024. 14:58:25	ASA	Intrusion	192.168.209.216	193.255.242.61	80	tcp	Would have dropped	Malware Detect with Dynamic Analy...

How easy is it to send event data?



Configure Cisco Cloud Events

● Send Events to the Cisco Cloud

☑ Send Intrusion Events to the cloud

☑ Send File and Malware Events to the cloud

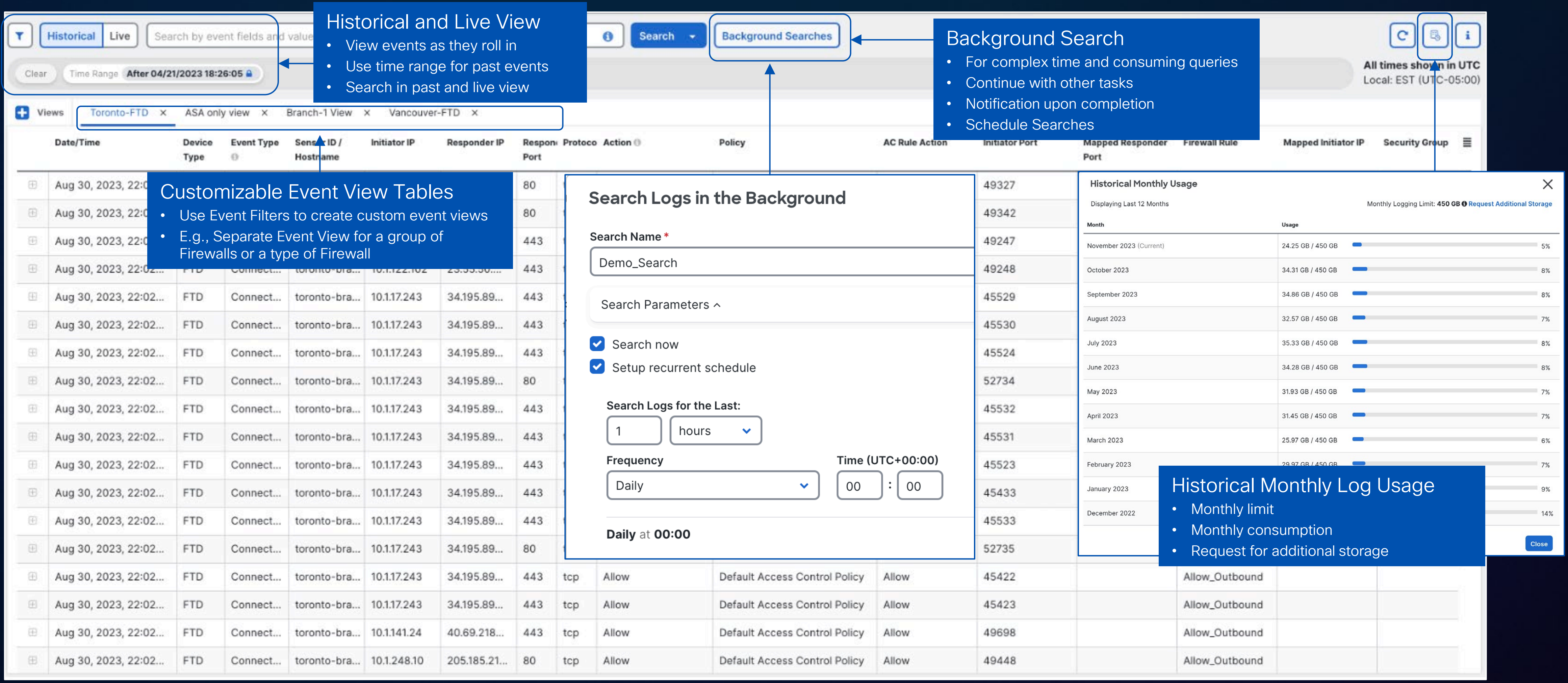
☑ Send Connection Events to the cloud

○ Security Events

● All

Unified event viewer

Consolidated event view for ASA and FTD



Time Range After 04/21/2023 18:26:05

All times shown in UTC
Local: EST (UTC-05:00)

Historical and Live View

- View events as they roll in
- Use time range for past events
- Search in past and live view

Background Search

- For complex time and consuming queries
- Continue with other tasks
- Notification upon completion
- Schedule Searches

Customizable Event View Tables

- Use Event Filters to create custom event views
- E.g., Separate Event View for a group of Firewalls or a type of Firewall

Date/Time	Device Type	Event Type	Sensor ID / Hostname	Initiator IP	Responder IP	Respon Port	Protoco	Action	Policy	AC Rule Action	Initiator Port	Mapped Responder Port	Firewall Rule	Mapped Initiator IP	Security Group
Aug 30, 2023, 22:0						80					49327				
Aug 30, 2023, 22:0						80					49342				
Aug 30, 2023, 22:0						443					49247				
Aug 30, 2023, 22:02...						443					49248				
Aug 30, 2023, 22:02...	FTD	Connect...	toronto-bra...	10.1.17.243	34.195.89...	443					45529				
Aug 30, 2023, 22:02...	FTD	Connect...	toronto-bra...	10.1.17.243	34.195.89...	443					45530				
Aug 30, 2023, 22:02...	FTD	Connect...	toronto-bra...	10.1.17.243	34.195.89...	443					45524				
Aug 30, 2023, 22:02...	FTD	Connect...	toronto-bra...	10.1.17.243	34.195.89...	80					52734				
Aug 30, 2023, 22:02...	FTD	Connect...	toronto-bra...	10.1.17.243	34.195.89...	443					45532				
Aug 30, 2023, 22:02...	FTD	Connect...	toronto-bra...	10.1.17.243	34.195.89...	443					45531				
Aug 30, 2023, 22:02...	FTD	Connect...	toronto-bra...	10.1.17.243	34.195.89...	443					45523				
Aug 30, 2023, 22:02...	FTD	Connect...	toronto-bra...	10.1.17.243	34.195.89...	443					45433				
Aug 30, 2023, 22:02...	FTD	Connect...	toronto-bra...	10.1.17.243	34.195.89...	443					45533				
Aug 30, 2023, 22:02...	FTD	Connect...	toronto-bra...	10.1.17.243	34.195.89...	80					52735				
Aug 30, 2023, 22:02...	FTD	Connect...	toronto-bra...	10.1.17.243	34.195.89...	443	tcp	Allow	Default Access Control Policy	Allow	45422		Allow_Outbound		
Aug 30, 2023, 22:02...	FTD	Connect...	toronto-bra...	10.1.17.243	34.195.89...	443	tcp	Allow	Default Access Control Policy	Allow	45423		Allow_Outbound		
Aug 30, 2023, 22:02...	FTD	Connect...	toronto-bra...	10.1.141.24	40.69.218...	443	tcp	Allow	Default Access Control Policy	Allow	49698		Allow_Outbound		
Aug 30, 2023, 22:02...	FTD	Connect...	toronto-bra...	10.1.248.10	205.185.21...	80	tcp	Allow	Default Access Control Policy	Allow	49448		Allow_Outbound		

Search Logs in the Background

Search Name *: Demo_Search

Search Parameters ^

☑ Search now

☑ Setup recurrent schedule

Search Logs for the Last: 1 hours

Frequency: Daily

Time (UTC+00:00): 00 : 00

Daily at **00:00**

Historical Monthly Usage

Displaying Last 12 Months

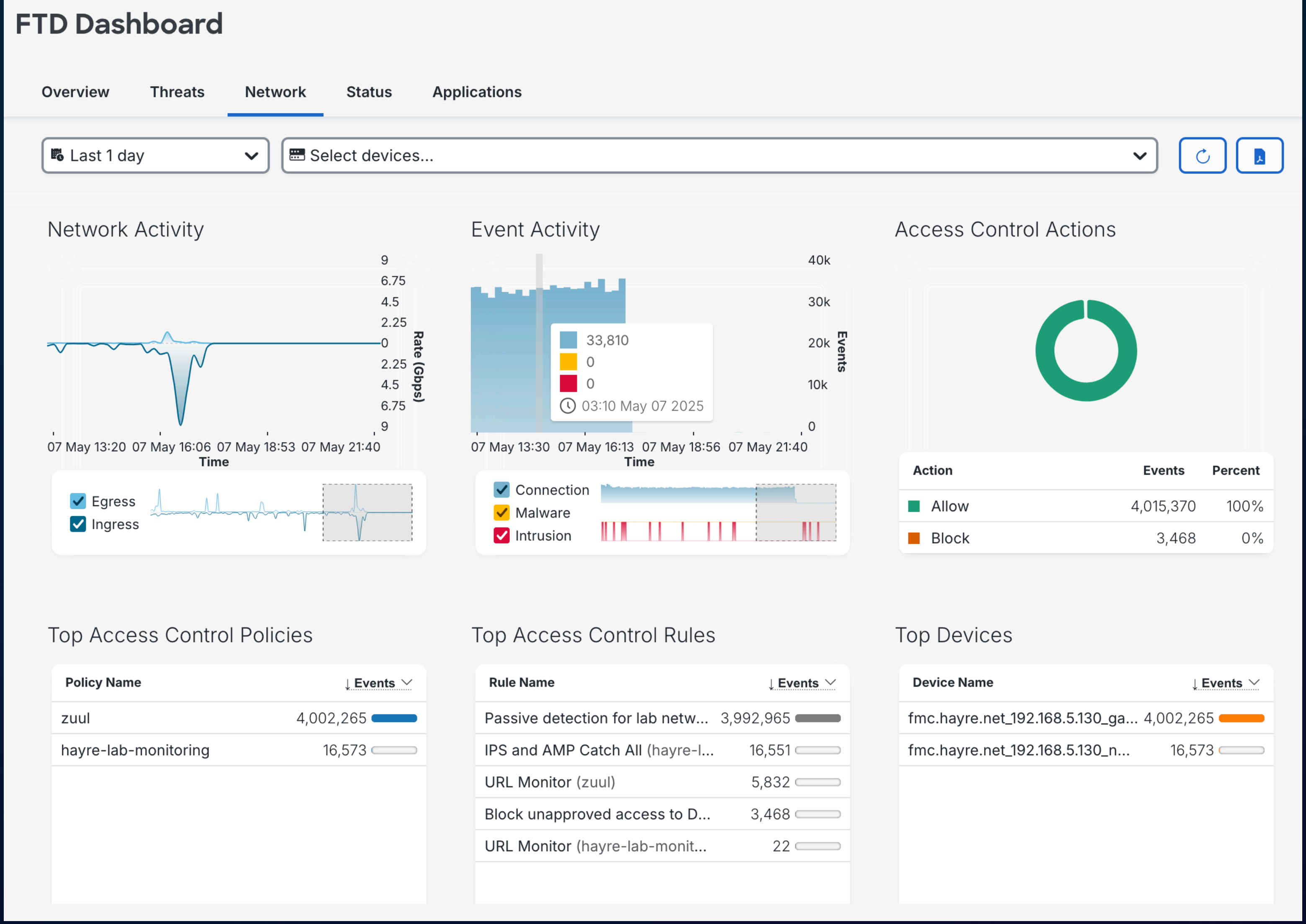
Monthly Logging Limit: **450 GB** Request Additional Storage

Month	Usage	
November 2023 (Current)	24.25 GB / 450 GB	5%
October 2023	34.31 GB / 450 GB	8%
September 2023	34.86 GB / 450 GB	8%
August 2023	32.57 GB / 450 GB	7%
July 2023	35.33 GB / 450 GB	8%
June 2023	34.28 GB / 450 GB	8%
May 2023	31.93 GB / 450 GB	7%
April 2023	31.45 GB / 450 GB	7%
March 2023	25.97 GB / 450 GB	6%
February 2023	29.97 GB / 450 GB	7%
January 2023		9%
December 2022		14%

Historical Monthly Log Usage

- Monthly limit
- Monthly consumption
- Request for additional storage

Dashboards



FTD Dashboard

Last 1 day

Select devices...

Action	Events	Percent
🟩 Allow	4,015,370	100%
🟧 Block	3,468	0%

Top Access Control Policies

Policy Name	↓ Events
zuul	4,002,265
hayre-lab-monitoring	16,573

Top Access Control Rules

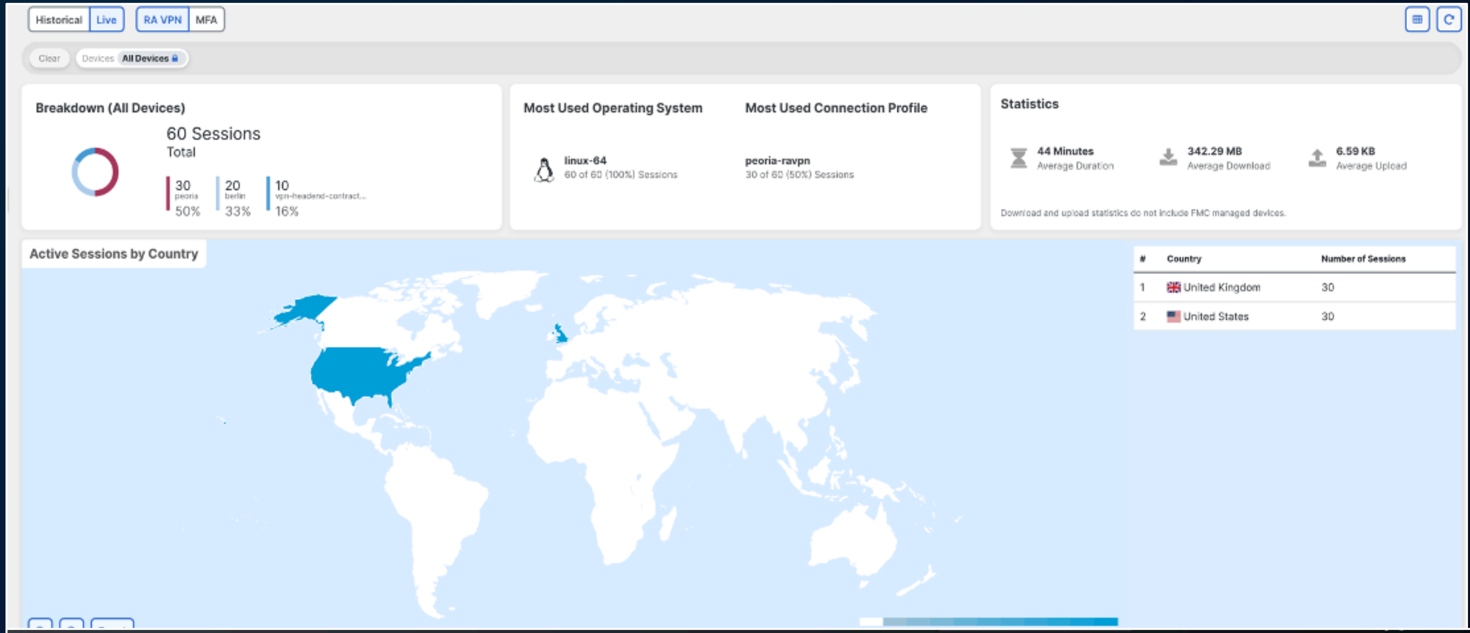
Rule Name	↓ Events
Passive detection for lab netw...	3,992,965
IPS and AMP Catch All (hayre-l...	16,551
URL Monitor (zuul)	5,832
Block unapproved access to D...	3,468
URL Monitor (hayre-lab-monit...	22

Top Devices

Device Name	↓ Events
fmc.hayre.net_192.168.5.130_ga...	4,002,265
fmc.hayre.net_192.168.5.130_n...	16,573

Consolidated RA-VPN monitoring dashboard

- Consolidated RAVPN dashboard
  - Customers who have both ASA and FTD as VPN headends
  - Customers migrating their VPN deployment from ASA to FTD
- Filter, search, and export the data
- Historical reporting of VPN sessions
- Usage patterns
- Ability to terminate sessions
- FMC customers adopting Security Cloud Control have the same look and feel as the RAVPN dashboard



Breakdown (All Devices)

60 Sessions
Total

30 peoria 50%
20 berlin 33%
10 vpn-headend-contract... 16%

Most Used Operating System

linux-64
60 of 60 (100%) Sessions

Most Used Connection Profile

peoria-ravpn
30 of 60 (50%) Sessions

Statistics

44 Minutes
Average Duration

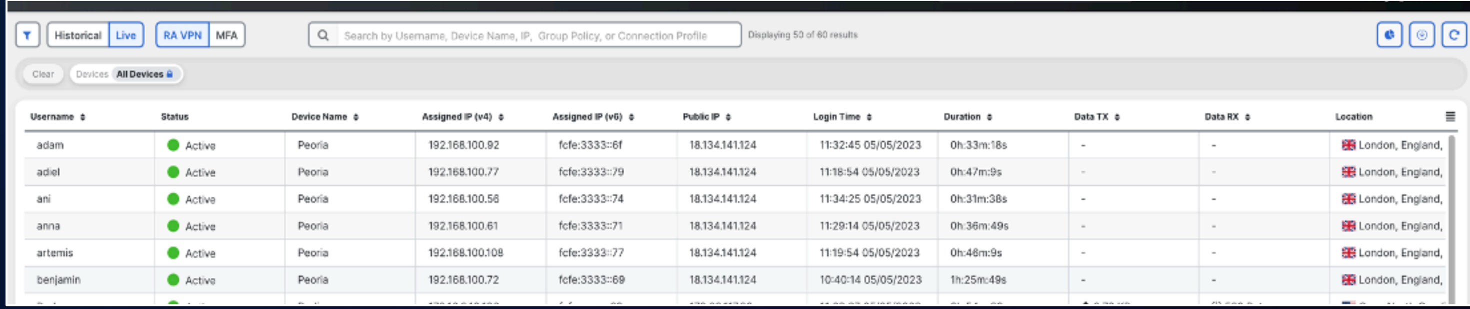
342.29 MB
Average Download

6.59 KB
Average Upload

Download and upload statistics do not include FMC managed devices.

Active Sessions by Country

#	Country	Number of Sessions
1	United Kingdom	30
2	United States	30

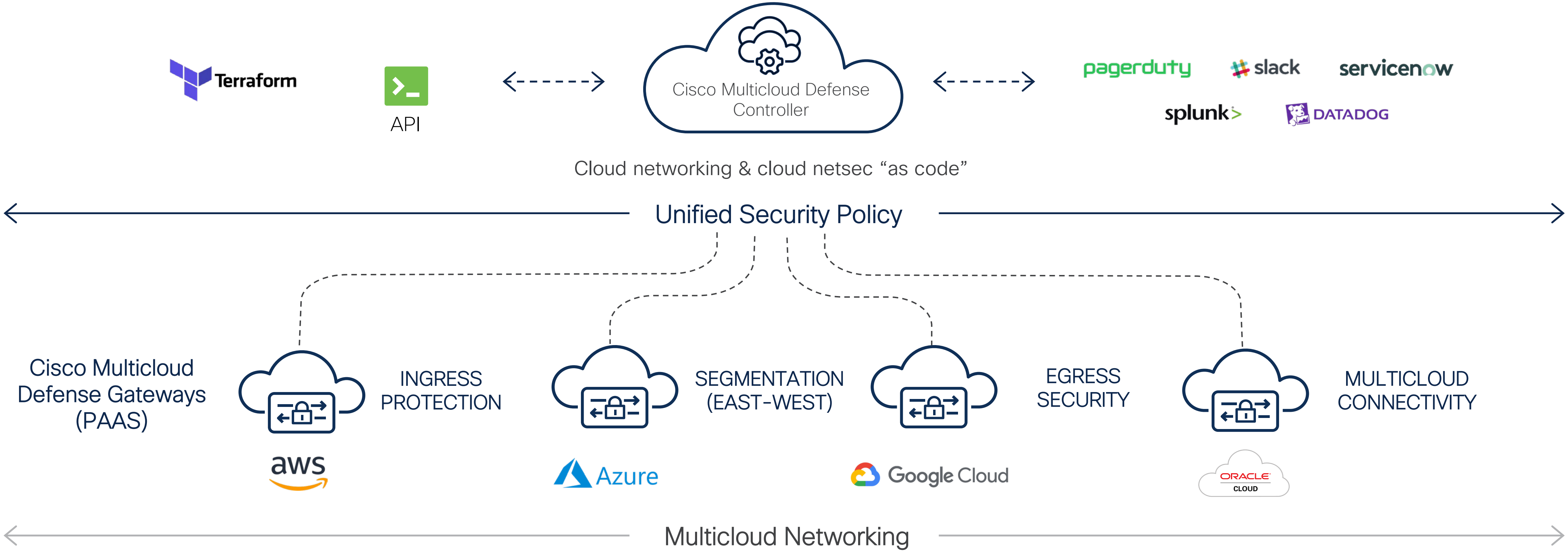

Historical
Live
RA VPN
MFA
Search by Username, Device Name, IP, Group Policy, or Connection Profile
Clear
Devices
All Devices

Displaying 50 of 60 results

Username	Status	Device Name	Assigned IP (v4)	Assigned IP (v6)	Public IP	Login Time	Duration	Data TX	Data RX	Location
adam	Active	Peoria	192.168.100.92	fcfe:3333::6f	18.134.141.124	11:32:45 05/05/2023	0h:33m:18s	-	-	London, England,
adiel	Active	Peoria	192.168.100.77	fcfe:3333::79	18.134.141.124	11:18:54 05/05/2023	0h:47m:9s	-	-	London, England,
ani	Active	Peoria	192.168.100.56	fcfe:3333::74	18.134.141.124	11:34:25 05/05/2023	0h:31m:38s	-	-	London, England,
anna	Active	Peoria	192.168.100.61	fcfe:3333::71	18.134.141.124	11:29:14 05/05/2023	0h:36m:49s	-	-	London, England,
artemis	Active	Peoria	192.168.100.108	fcfe:3333::77	18.134.141.124	11:19:54 05/05/2023	0h:46m:9s	-	-	London, England,
benjamin	Active	Peoria	192.168.100.72	fcfe:3333::69	18.134.141.124	10:40:14 05/05/2023	1h:25m:49s	-	-	London, England,

Cisco Multicloud Defense

Combining multicloud networking, automation, and cloud-native network security controls



Cisco Multicloud Defense Controller

Cloud networking & cloud netsec "as code"

Unified Security Policy

Cisco Multicloud Defense Gateways (PAAS)

INGRESS PROTECTION

SEGMENTATION (EAST-WEST)

EGRESS SECURITY

MULTICLOUD CONNECTIVITY

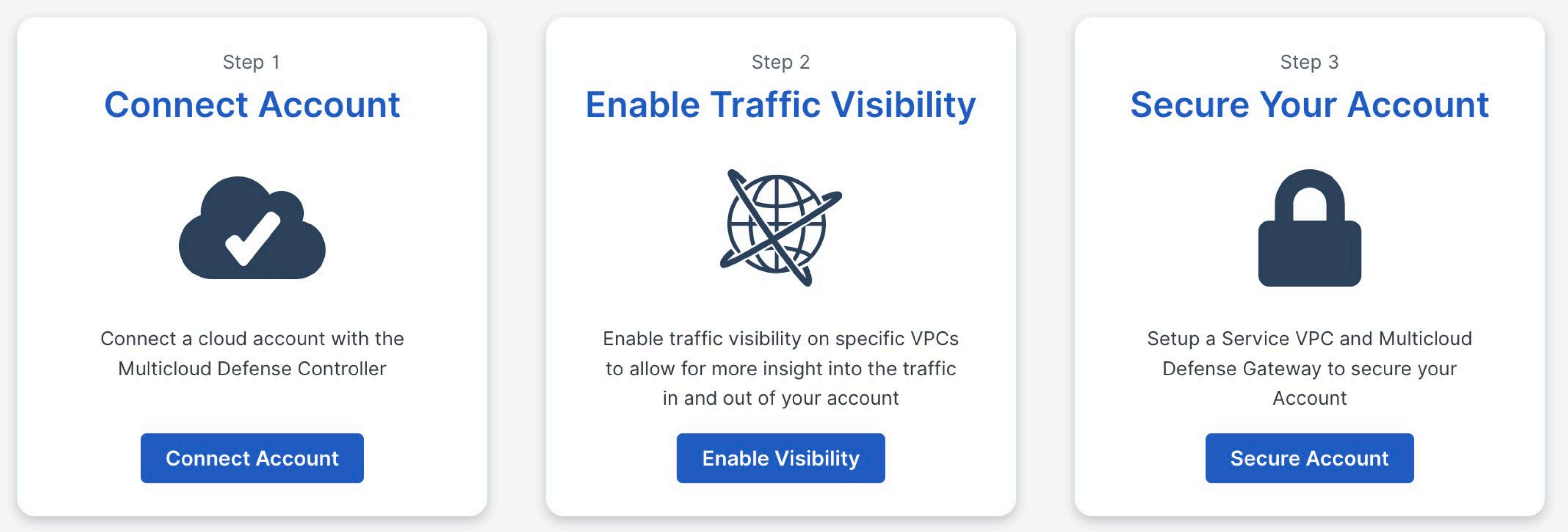
Multicloud Networking

NETWORK VISIBILITY

ROUTING & CONNECTIVITY

SECURITY AUTOMATION

Enabling Multicloud Defense Control



Step 1

Connect Account

Connect a cloud account with the Multicloud Defense Controller

Step 2

Enable Traffic Visibility

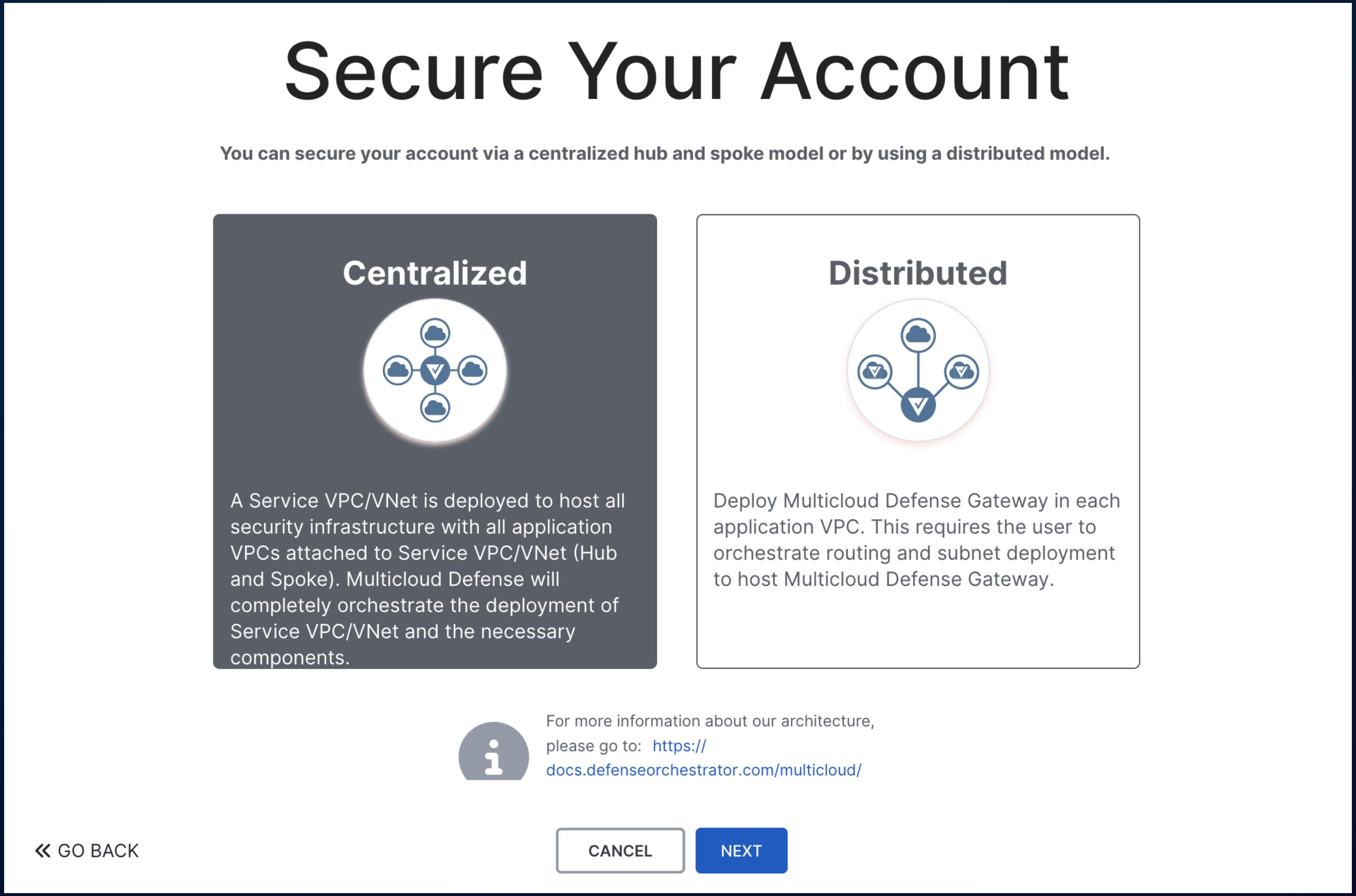
Enable traffic visibility on specific VPCs to allow for more insight into the traffic in and out of your account

Step 3

Secure Your Account

Setup a Service VPC and Multicloud Defense Gateway to secure your Account

Turning enforcement on in public cloud



Secure Your Account

You can secure your account via a centralized hub and spoke model or by using a distributed model.

Centralized

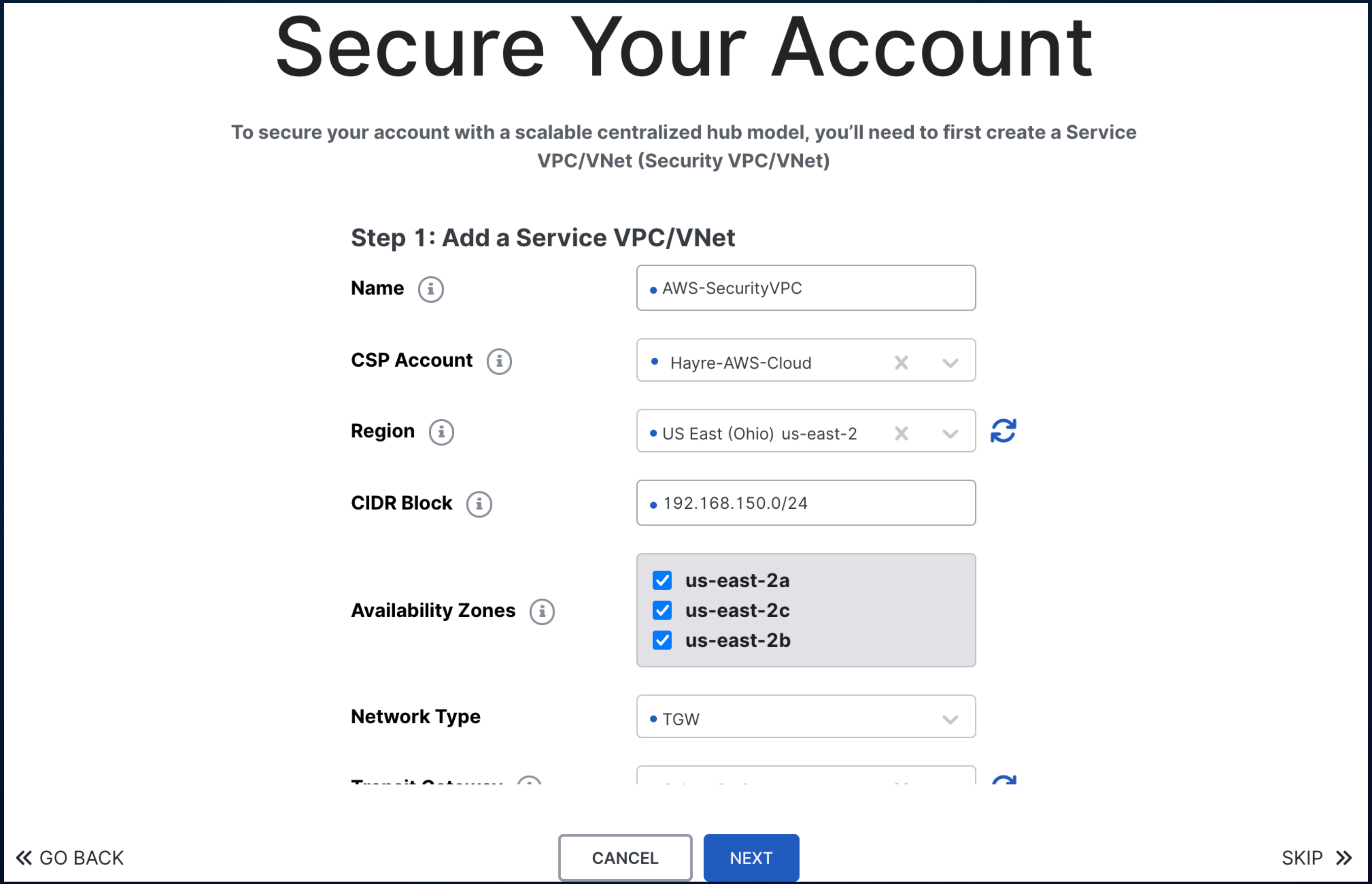
A Service VPC/VNet is deployed to host all security infrastructure with all application VPCs attached to Service VPC/VNet (Hub and Spoke). Multicloud Defense will completely orchestrate the deployment of Service VPC/VNet and the necessary components.

Distributed

Deploy Multicloud Defense Gateway in each application VPC. This requires the user to orchestrate routing and subnet deployment to host Multicloud Defense Gateway.

For more information about our architecture, please go to: https://docs.defenseorchestrator.com/multicloud/

Turning enforcement on in public cloud



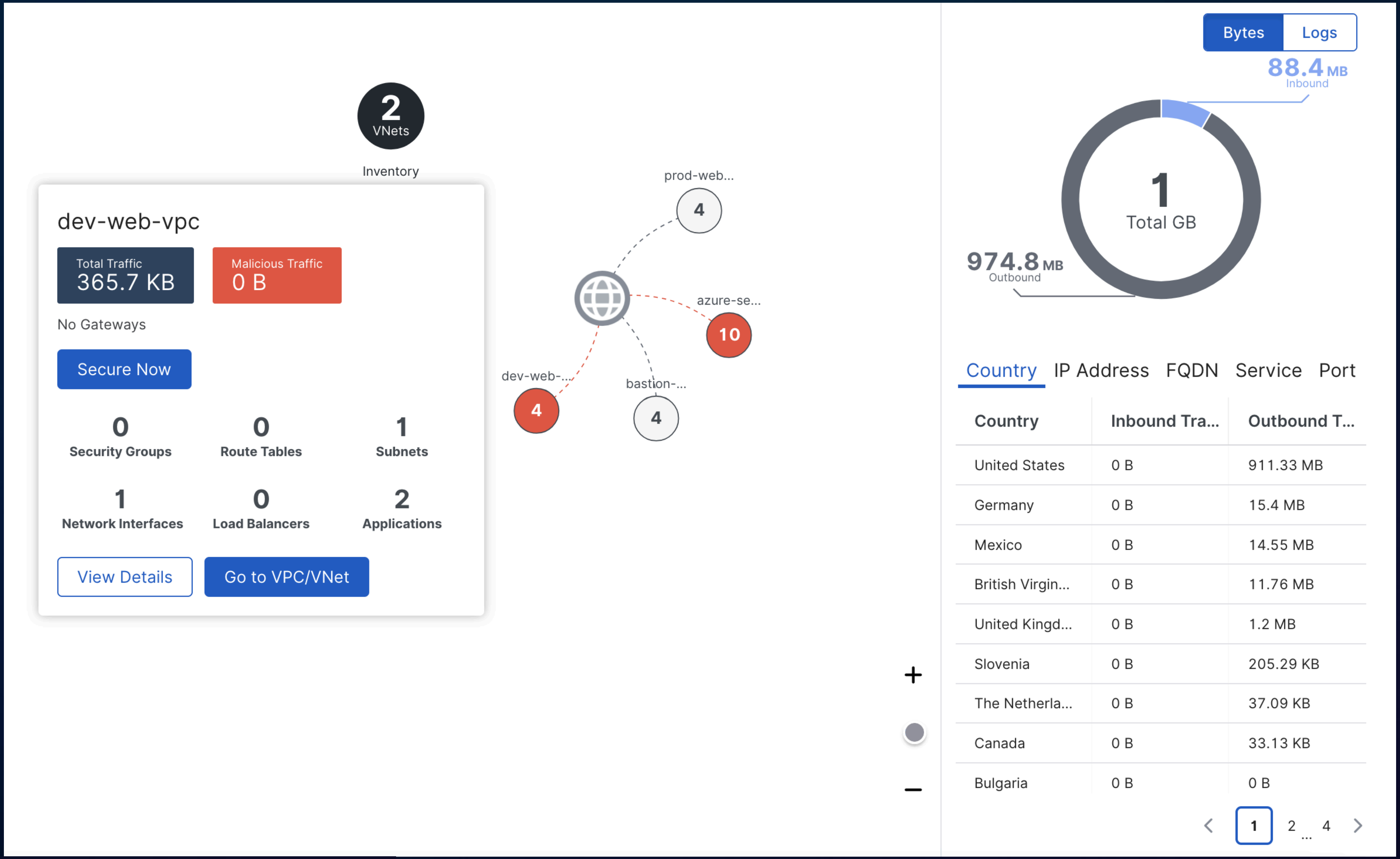
Secure Your Account

To secure your account with a scalable centralized hub model, you'll need to first create a Service VPC/VNet (Security VPC/VNet)

Step 1: Add a Service VPC/VNet

Name	AWS-SecurityVPC
CSP Account	Hayre-AWS-Cloud
Region	US East (Ohio) us-east-2
CIDR Block	192.168.150.0/24
Availability Zones	☑ us-east-2a ☑ us-east-2c ☑ us-east-2b
Network Type	TGW

Actionable visibility and insights



dev-web-vpc

Total Traffic 365.7 KB

Malicious Traffic 0 B

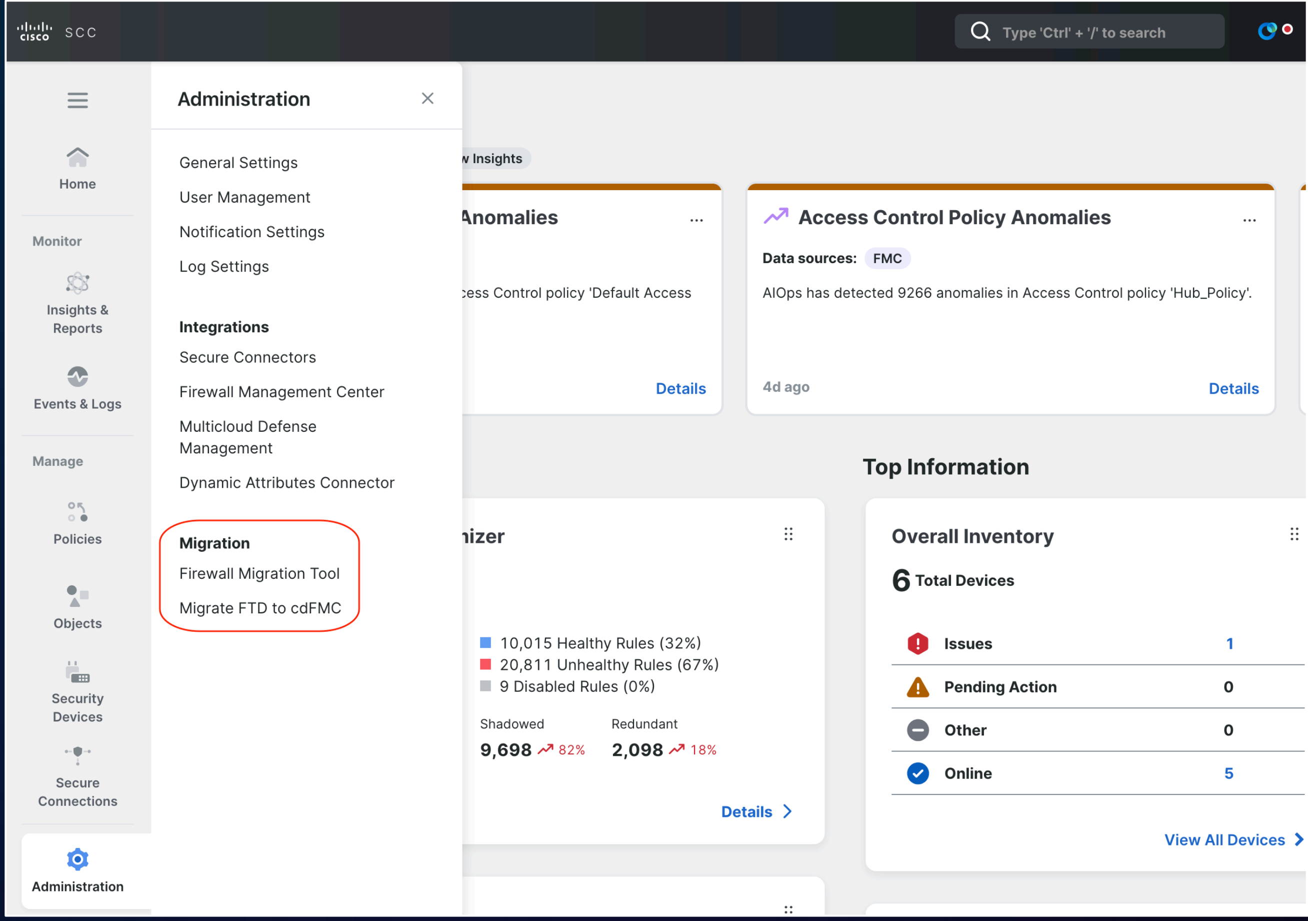
No Gateways

0 Security Groups	0 Route Tables	1 Subnets
1 Network Interfaces	0 Load Balancers	2 Applications

Country	Inbound Tra...	Outbound T...
United States	0 B	911.33 MB
Germany	0 B	15.4 MB
Mexico	0 B	14.55 MB
British Virgin...	0 B	11.76 MB
United Kingd...	0 B	1.2 MB
Slovenia	0 B	205.29 KB
The Netherla...	0 B	37.09 KB
Canada	0 B	33.13 KB
Bulgaria	0 B	0 B

Migration support in Security Cloud Control

- Easy migration workflow to move the management of firewalls from an on-prem FMC to cloud-delivered Security Cloud Control
  - The migration will move the policies, objects, licenses, and anything associated with the firewall
- Firewall migration tool natively hosted in Security Cloud Control
  - Easily migrate from ASA or 3rd party firewalls to Security Cloud Control-managed FTDs



ess Control policy 'Default Access

Data sources: FMC

AIOps has detected 9266 anomalies in Access Control policy 'Hub_Policy'.

4d ago

- 🟦 10,015 Healthy Rules (32%)
- 🟥 20,811 Unhealthy Rules (67%)
- ⬜ 9 Disabled Rules (0%)

Shadowed	Redundant
9,698 82%	2,098 18%

6 Total Devices

Issues	1
Pending Action	0
Other	0
Online	5

How to get started

What to expect with Security Cloud Control

Cloud assist features for FMC customers

- Device & service inventory view
- Unified object view
- Global search
- AI Assistant for on-prem FMC
- Policy Optimizer for on-prem FMC
- Remote Access VPN monitoring
- Site-to-site VPN config and monitoring
- Dynamic attribute connector
- Hosted Firewall Migration Tool
- Unified notifications and alerting

Licensed Features (subscription)

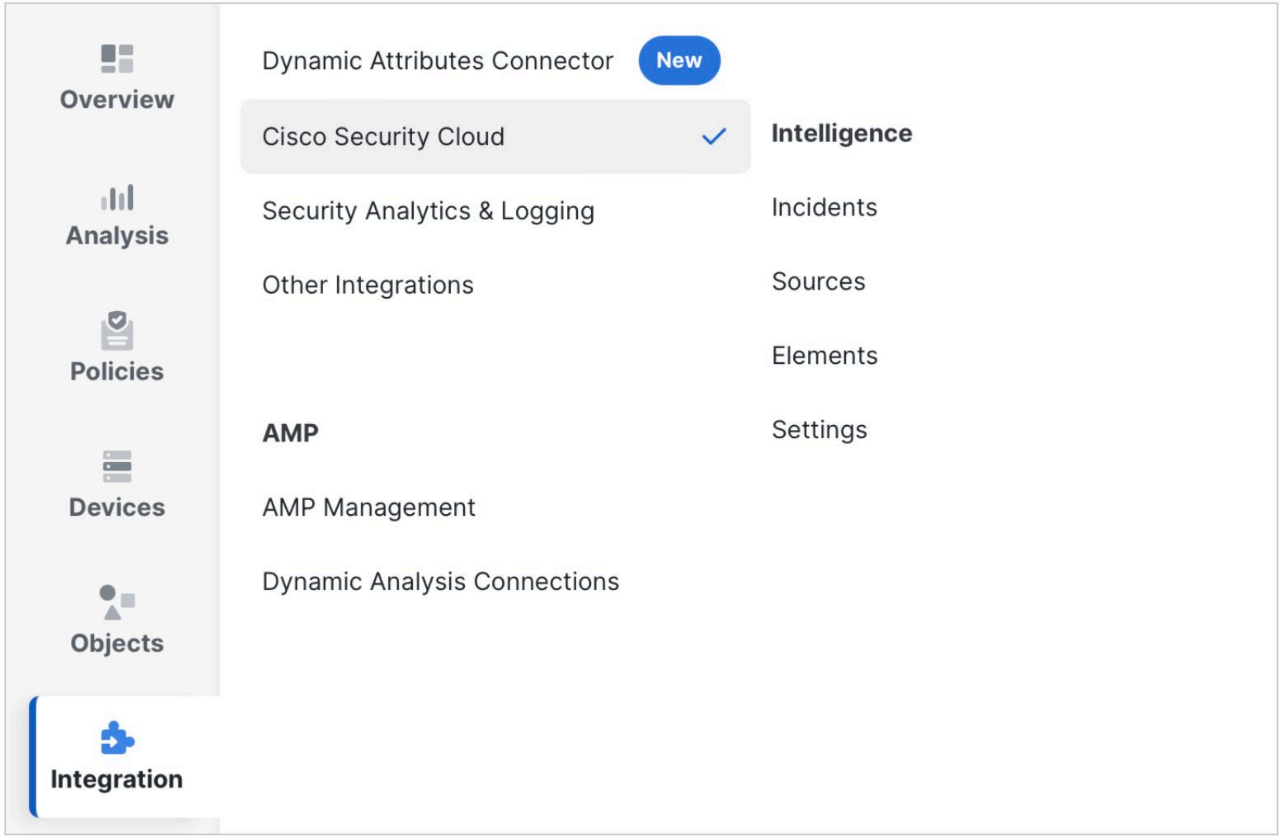
- FTD Management
- ASA Management
- Multicloud Defense
- Secure Access
- Secure Workload
- AI Defense
- Hypershield
- Security Logging and Troubleshooting
- Meraki MX Policy & Object Management

Integrate your on-prem FMC today!

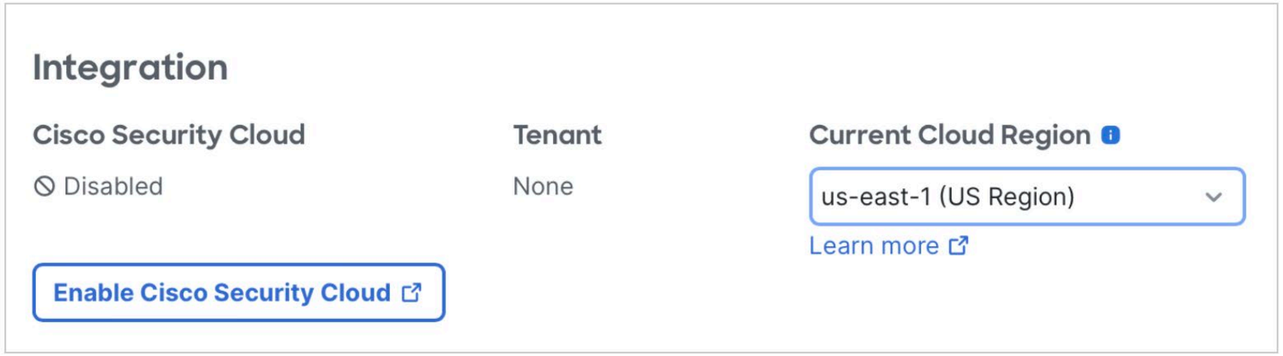
https://secure.cisco.com/secure-firewall/docs/cisco-security-cloud-integration

Configuration Process

1. In Firewall Management Center, navigate to **Integration > Cisco Security Cloud**.



2. From the drop-down list select your desired region in **Current Cloud Region**. Then click **Enable Cisco Security Cloud**.



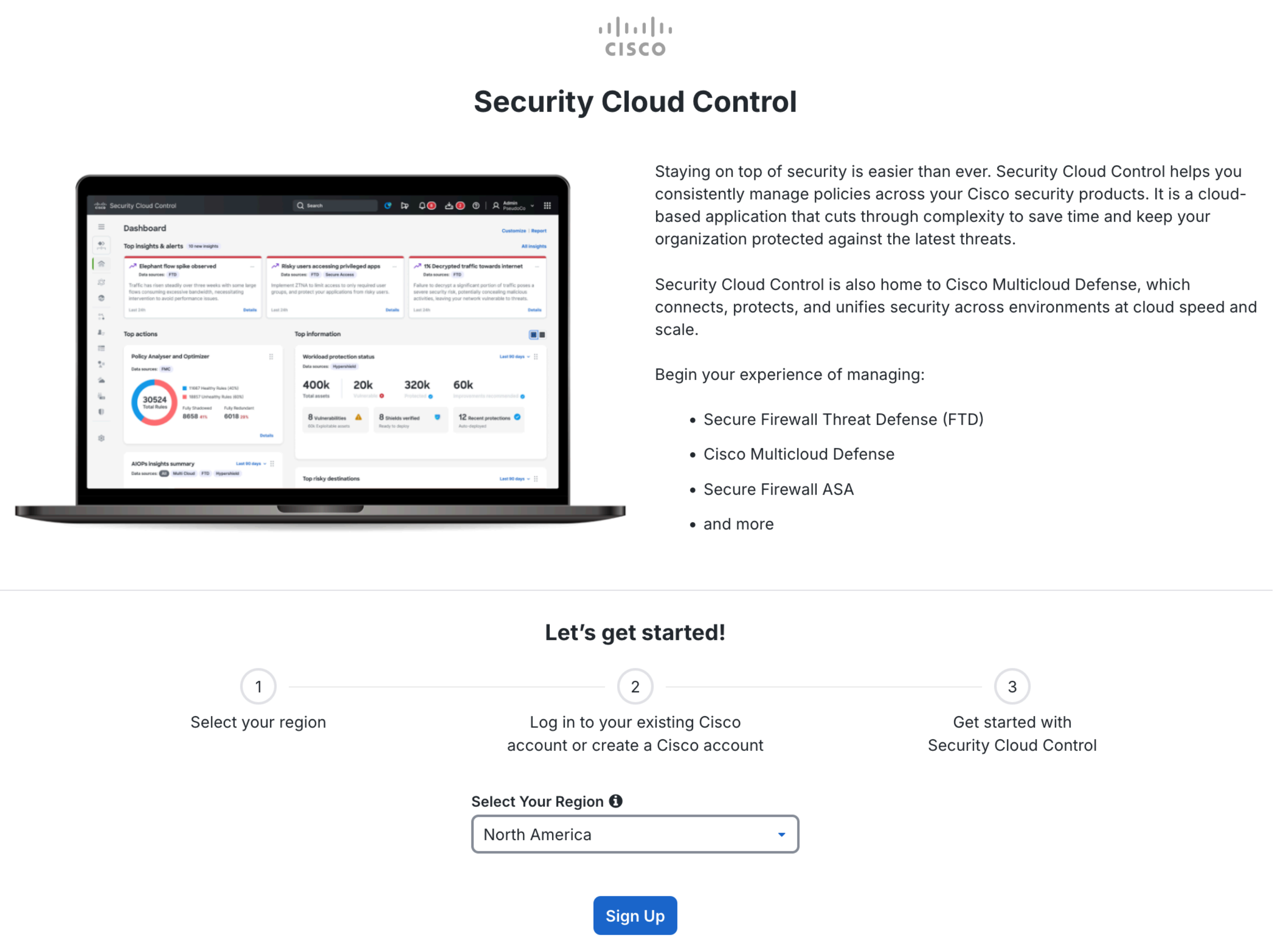
Integration

Cisco Security Cloud	Tenant	Current Cloud Region
Disabled	None	us-east-1 (US Region)

Ready to try Cisco Security Cloud Control?

getcdo.com

Need logging, firewall management or Multicloud? Talk to me after the session.



Security Cloud Control

Staying on top of security is easier than ever. Security Cloud Control helps you consistently manage policies across your Cisco security products. It is a cloud-based application that cuts through complexity to save time and keep your organization protected against the latest threats.

Security Cloud Control is also home to Cisco Multicloud Defense, which connects, protects, and unifies security across environments at cloud speed and scale.

Begin your experience of managing:

- Secure Firewall Threat Defense (FTD)
- Cisco Multicloud Defense
- Secure Firewall ASA
- and more

Let's get started!

1. Select your region
2. Log in to your existing Cisco account or create a Cisco account
3. Get started with Security Cloud Control

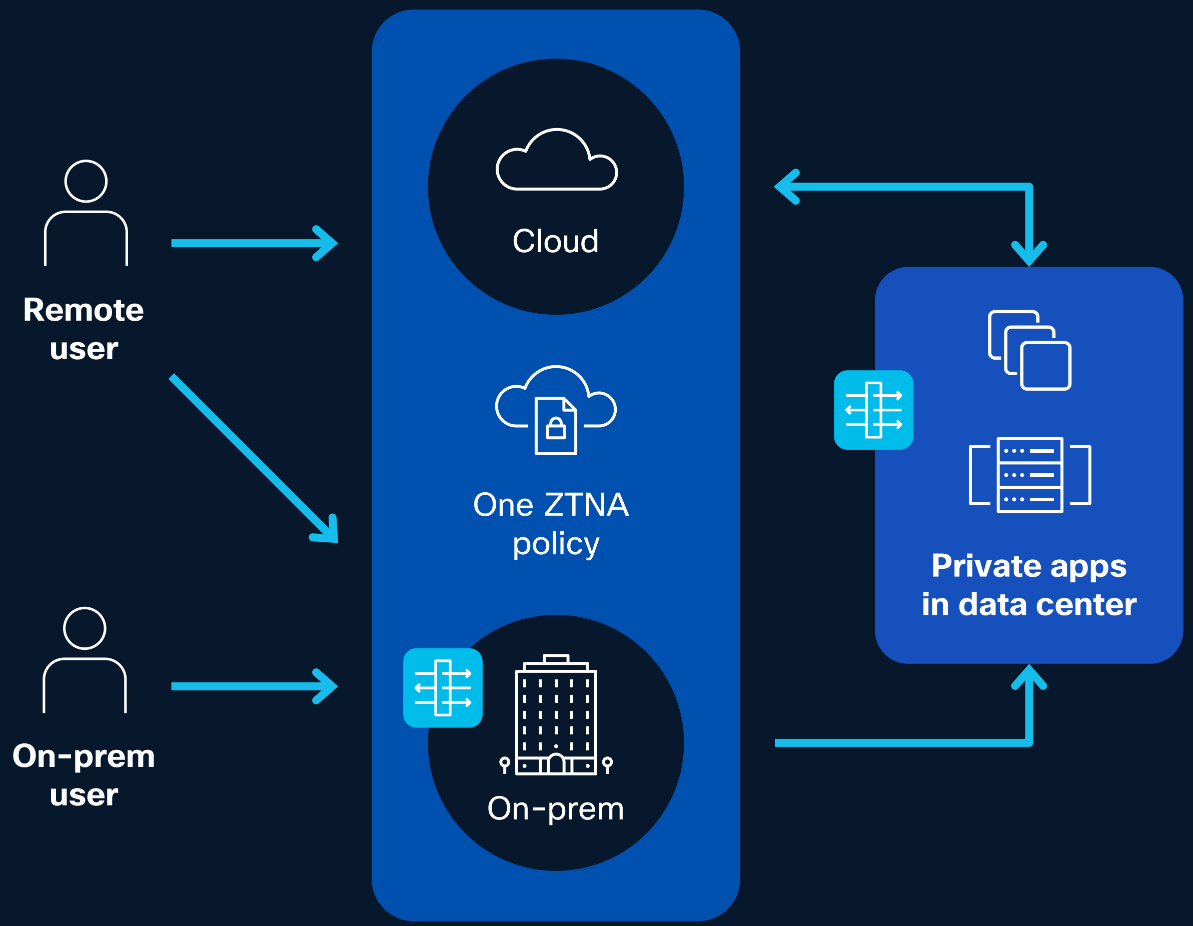
Select Your Region: North America

Sign Up

Additional platform use-cases

Manage security outcomes, not products

ZTNA across hybrid environments



One policy, simplified access

For all users, everywhere

Improved user experience

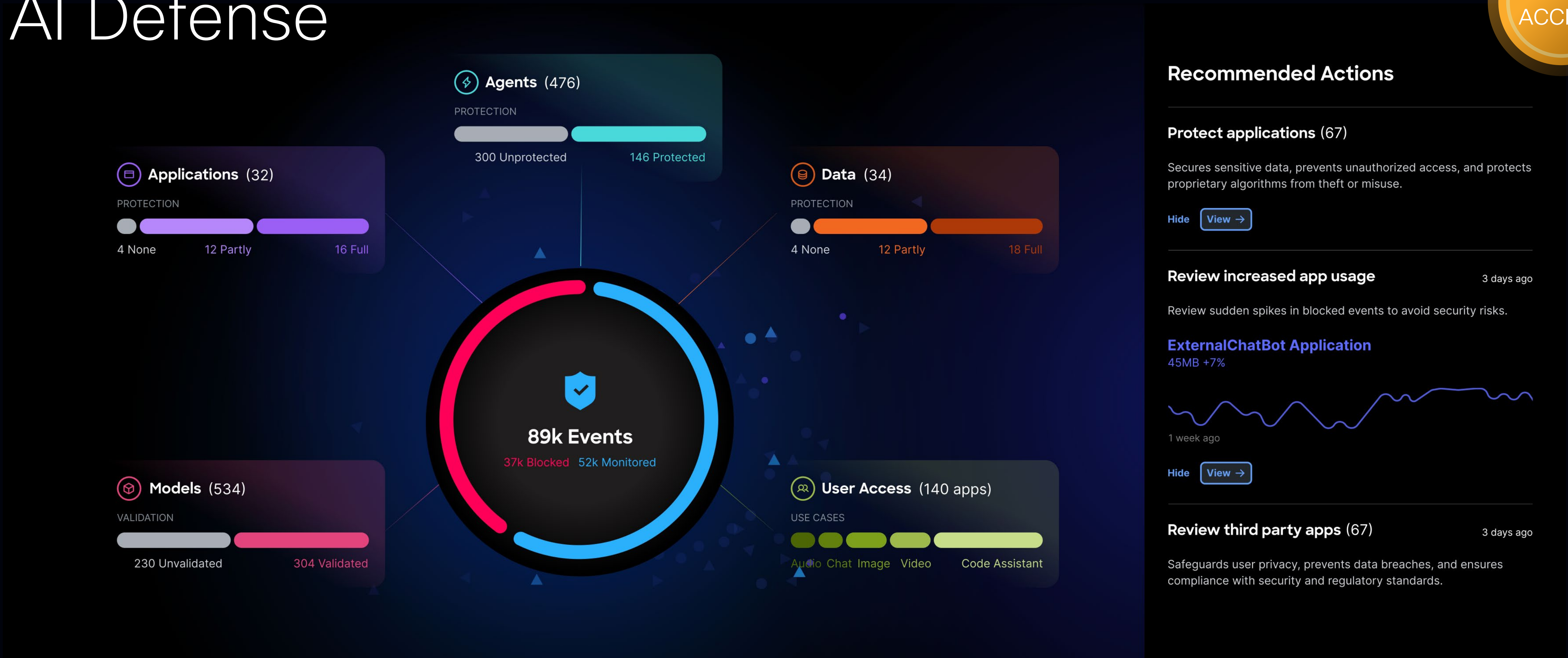
Reduced latency whether on-prem or remote

In-country data sovereignty

For private application traffic

AI Defense

EARLY ACCESS



Recommended Actions

Protect applications (67)

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

Hide View →

Review increased app usage 3 days ago

Review sudden spikes in blocked events to avoid security risks.

ExternalChatBot Application
45MB +7%

Review third party apps (67) 3 days ago

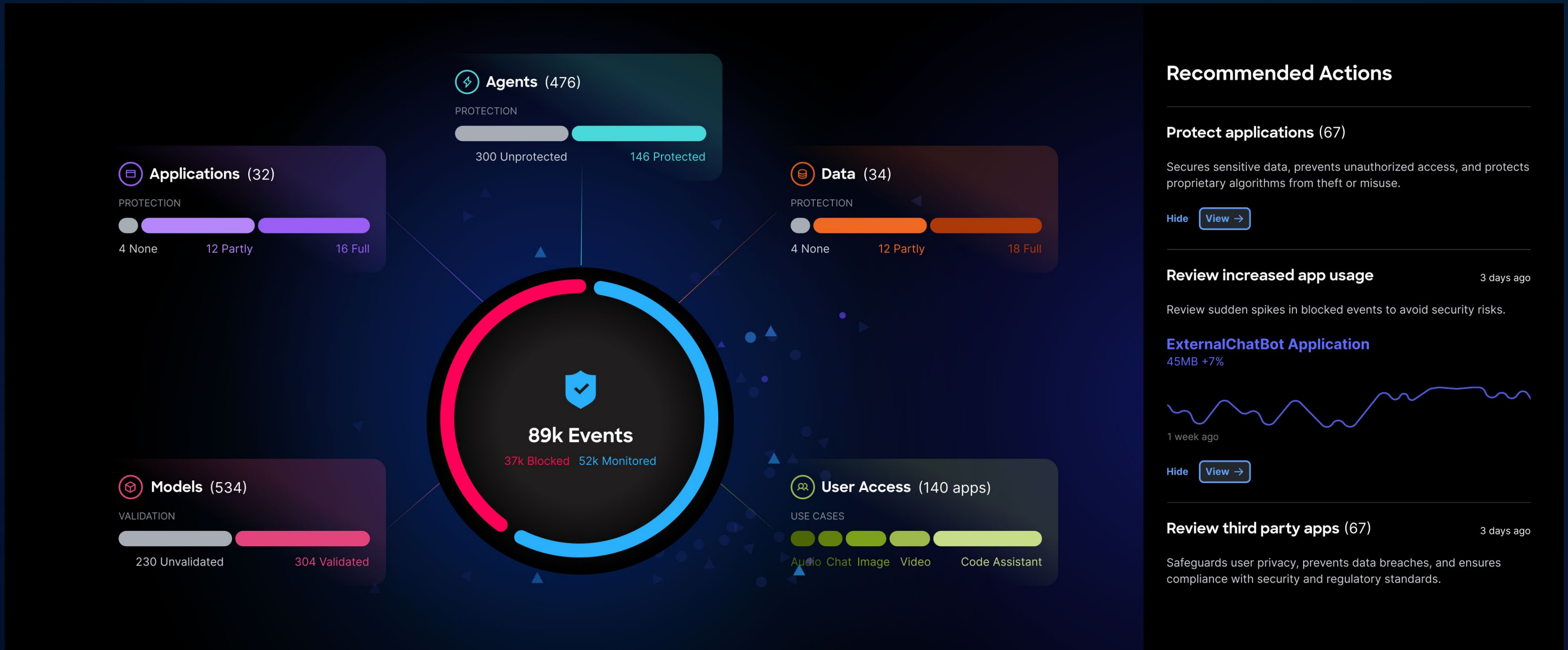
Safeguards user privacy, prevents data breaches, and ensures compliance with security and regulatory standards.

Visibility of underlying models and data

Model Validation and guardrail recommendations

Runtime enforcement across public and private clouds

Delivered via the Hybrid Mesh Firewall



Agents (476)
PROTECTION
300 Unprotected 146 Protected

Applications (32)
PROTECTION
4 None 12 Partly 16 Full

Data (34)
PROTECTION
4 None 12 Partly 18 Full

89k Events
37k Blocked 52k Monitored

Models (534)
VALIDATION
230 Unvalidated 304 Validated

User Access (140 apps)
USE CASES
Audio Chat Image Video Code Assistant

Recommended Actions

Protect applications (67)

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

Hide View →

Review increased app usage 3 days ago

Review sudden spikes in blocked events to avoid security risks.

ExternalChatBot Application
45MB +7%

1 week ago

Hide View →

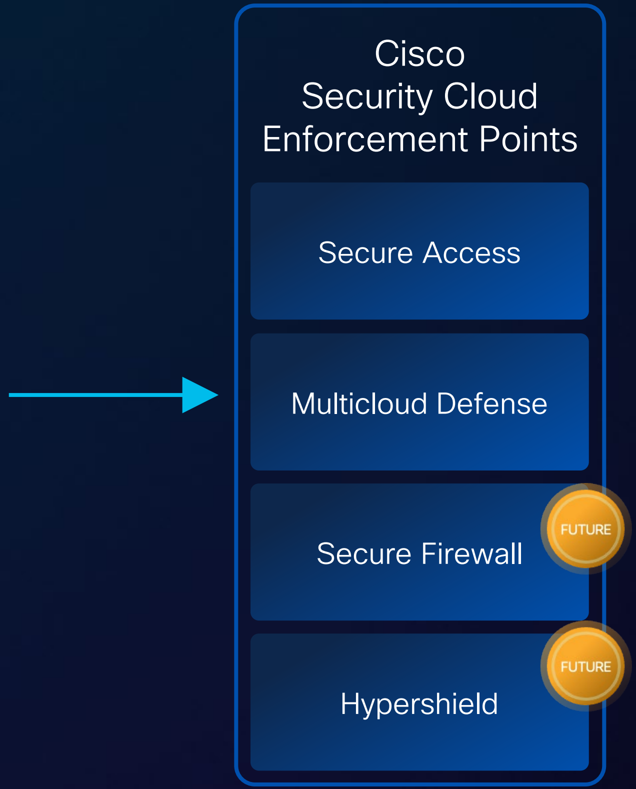
Review third party apps (67) 3 days ago

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

Visibility of underlying models and data

Model Validation and guardrail recommendations

Runtime enforcement across public and private clouds



Cisco Security Cloud Enforcement Points

Secure Access

Multicloud Defense

Secure Firewall

FUTURE

Hypershield

FUTURE

Segmentation for workloads

All types of workloads

Windows | Linux | Cloud

VM

Virtual Machine

BareMetal

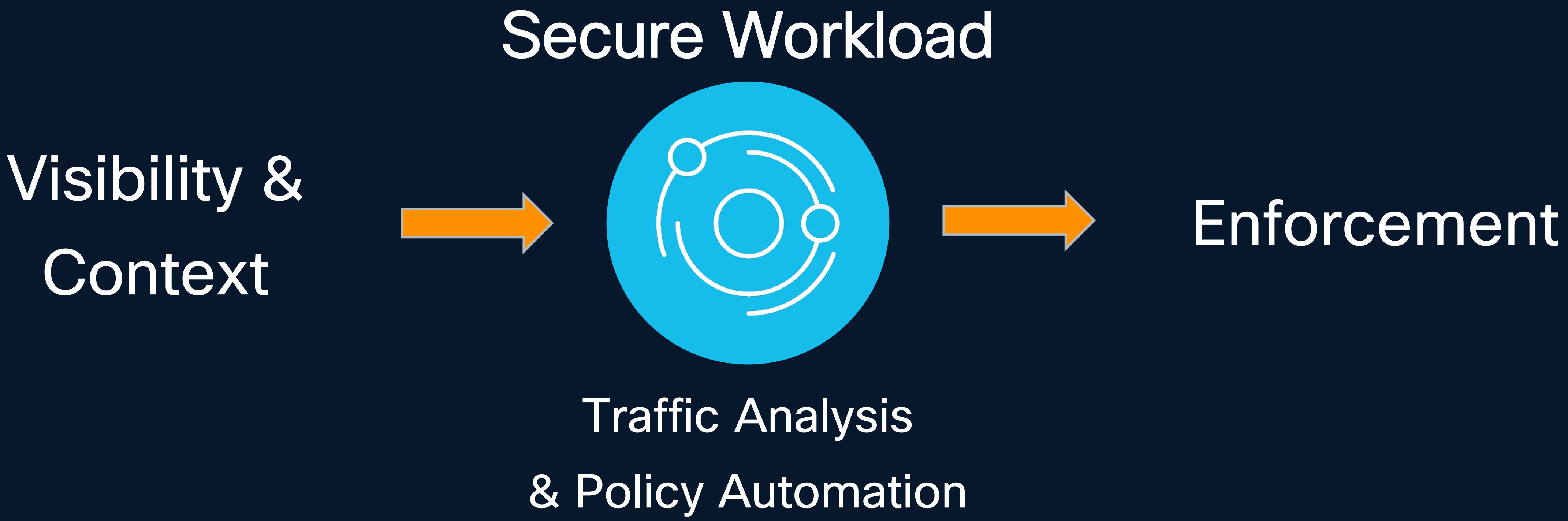
SaaS delivered

Get started quickly without hardware investment

Confident outcomes

Speed up time to value with implementation services

Automating your microsegmentation



Visibility & Context

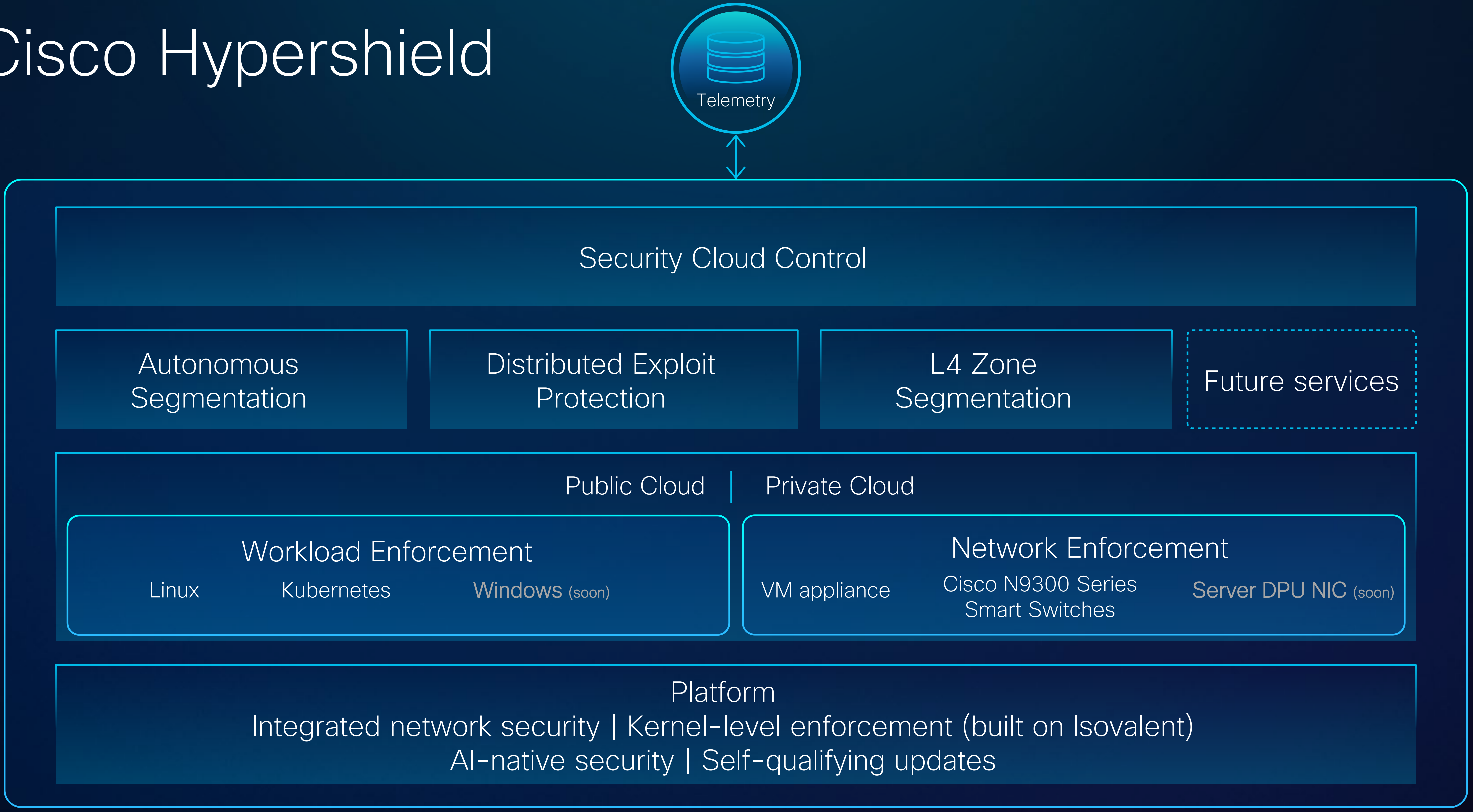
Secure Workload

Traffic Analysis

& Policy Automation

Enforcement

Cisco Hypershield



Telemetry

Security Cloud Control

Autonomous Segmentation

Distributed Exploit Protection

L4 Zone Segmentation

Future services

Public Cloud | Private Cloud

Workload Enforcement

Linux

Kubernetes

Windows (soon)

Network Enforcement

VM appliance

Cisco N9300 Series Smart Switches

Server DPU NIC (soon)

Platform

Integrated network security | Kernel-level enforcement (built on Isovalent)

AI-native security | Self-qualifying updates

Thank you

#CiscoConnect