

Cisco Security Cloud Control – Bringing the Cisco Security Portfolio Together

cisco Live !

Anshul Kaushik
Solutions Engineer

Session ID: BRKSEC-2165

Your Speaker

Anshul Kaushik

- ankaushi@cisco.com
- CCIE Security #23790
- 23 Years in Industry, 20 with Cisco
- TAC – Presales – Channels
- Drive end to end Security Enablement
- Lives in Melbourne and like outdoors



Cisco Webex App

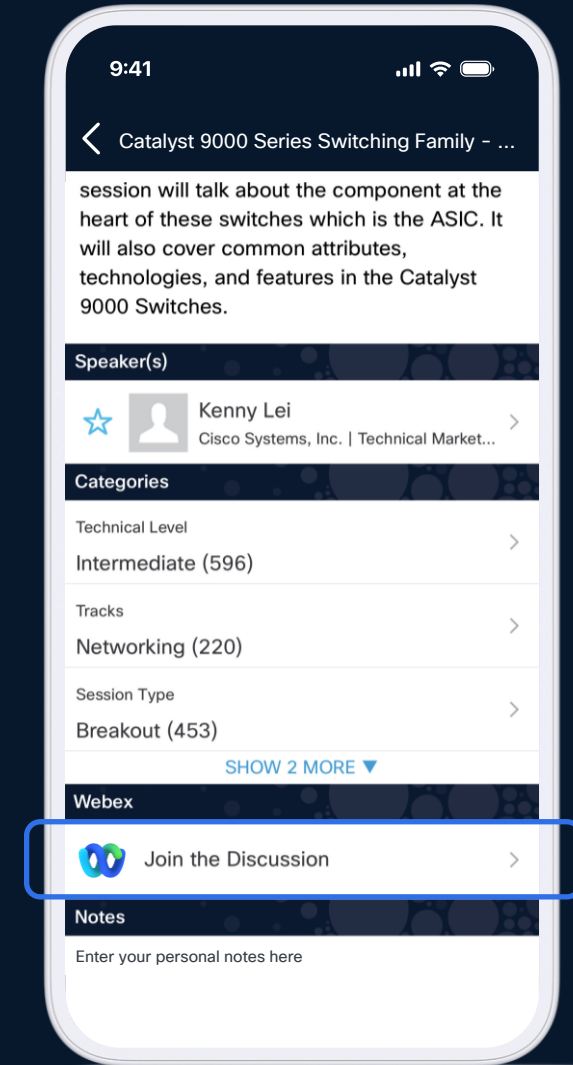
Questions?

Use Cisco Webex App to chat with the speaker after the session

How

- 1 Find this session in the Cisco Live Mobile App
- 2 Click “Join the Discussion”
- 3 Install the Webex App or go directly to the Webex space
- 4 Enter messages/questions in the Webex space

Webex spaces will be moderated by the speaker until 14 November 2025.



<https://ciscolive.ciscoevents.com/ciscolivebot/#BRKSEC-2165>

Agenda

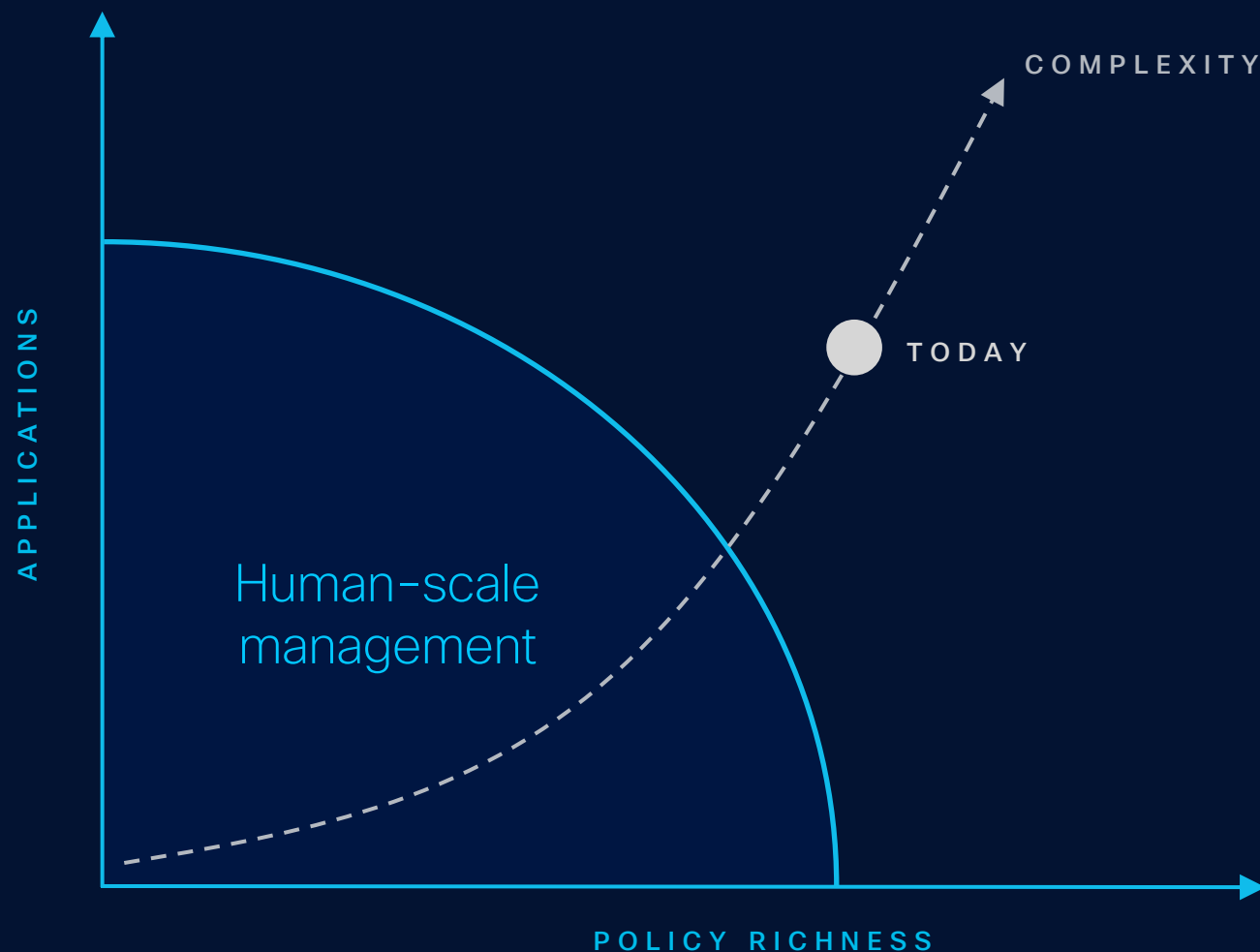
- 01 Why Security Cloud Control?
- 02 Getting Started with Security Cloud Control
- 03 Product Provisioning
- 04 User Management
- 05 Unified User Experience
- 06 SCC Firewall Management
- 07 A Look Ahead...What is Next?
- 08 Key Takeaways



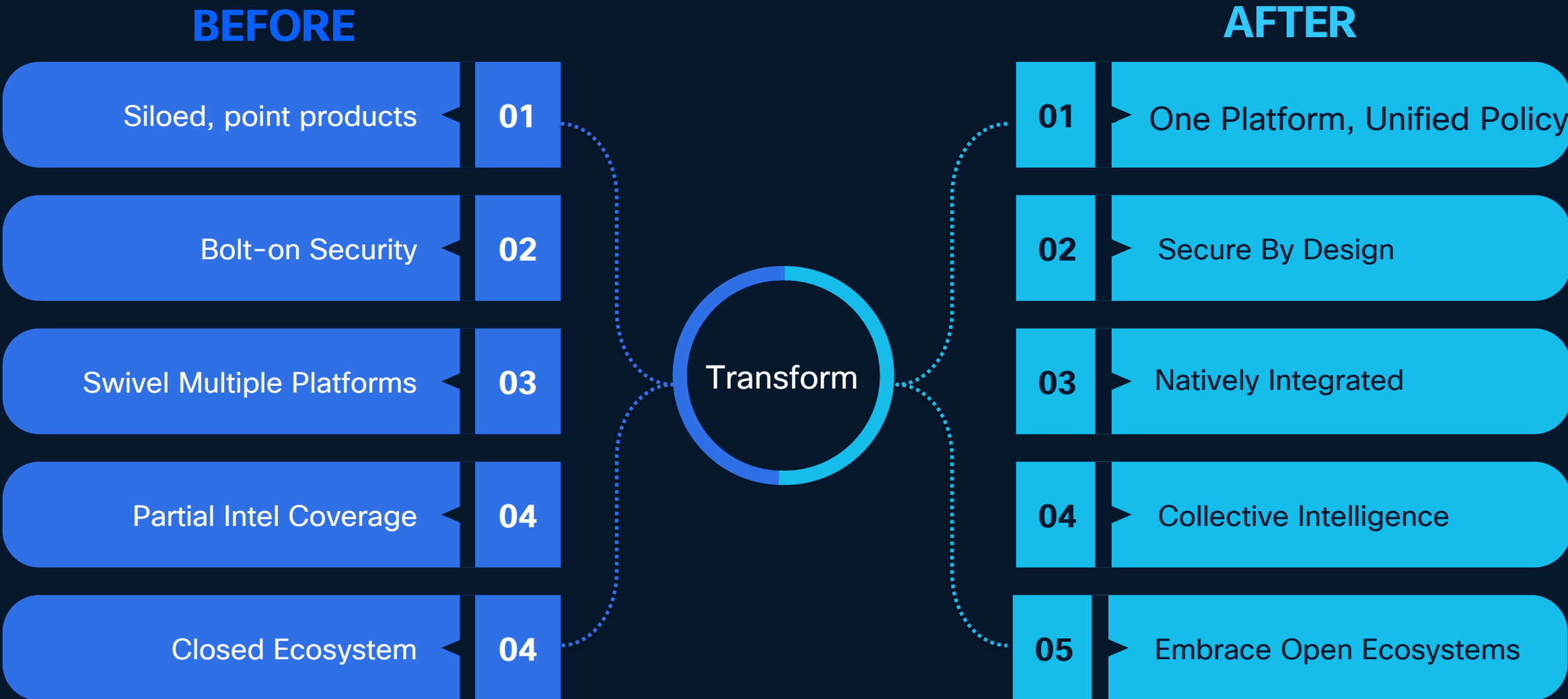
¹X-Force Threat Intelligence Index, IBM, 2024

ROOT CAUSE

Complexity has exceeded human scale



Simplified Operations, Protection and Resilience



Enhance protection and simplify operations with an integrated approach to security



**Simplified user
experience**

One console,
zero complexity



**Faster, more
intelligent security**

AI-driven insights,
real-time action



**Manage outcomes,
not products**

Centralized control,
measurable impact

Cisco Security Cloud Control



Unified Security Policy



Unified Agentic Ops



**Portfolio Value
Acceleration**

Unified Security Policy



Common Objects / Identity

Common identity and policy objects act as shared foundations between products.



Topology and Relationships

Topology defines communication pathways between assets and security enforcement points



Asset Inventory

Shared information repository about assets provides a single location for posture across products.



Unified Policy

Intent-based policy that unifies enforcement across currently disparate enforcement points.



Unified Agentic Ops



Simplifying Complexity

Agentic Ops leverages AI to make advanced network and security expertise widely accessible and operational for all.



Automated Remediation

AI agents proactively identify and automatically resolve network and security issues before they impact operations.



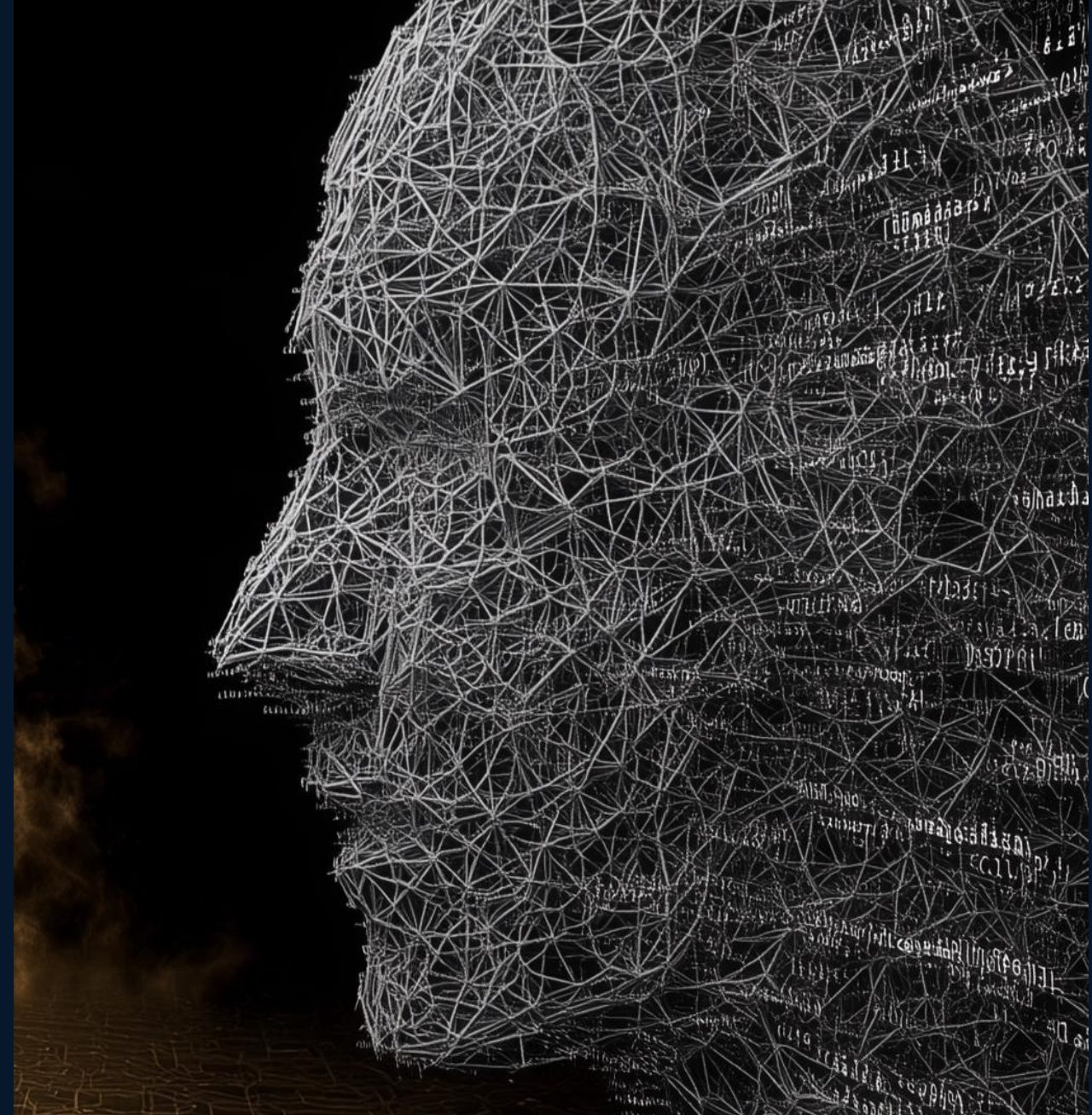
AI Incident Resolution

AI-native operators streamline the entire incident lifecycle, from detection to rapid and automated resolution.



Automated Intent-Based Networking

Agentic Ops translates high-level business intent directly into automated network configurations and security policies.



Portfolio Value Acceleration



Multi-Org and MSP

Centralized management simplifies operations for multi-organizational enterprises and MSPs, including sub-org management and RBAC.



Cisco Unified Identity

Cisco Unified Identity allows seamless connections to products and customers across Networking and Security.



Product-Led Growth

Accelerates adoption and value realization through intuitive experiences, integrated scorecards, and customer-initiated trials.



Product Expansion

Ensures seamless integration and management of Cisco's expanding security portfolio within a unified platform.



Agenda

- 01 Why Security Cloud Control?
- 02 Getting Started with Security Cloud Control
- 03 Product Provisioning
- 04 User Management
- 05 Unified User Experience
- 06 SCC Firewall Management
- 07 A Look Ahead...What is Next?
- 08 Key Takeaways



What is Cisco Security Cloud Control?



Cisco Security Cloud Control

An AI-Powered Security Platform

Define policy once and enforce anywhere



One Portal to Manage ALL Cisco SaaS Security Products

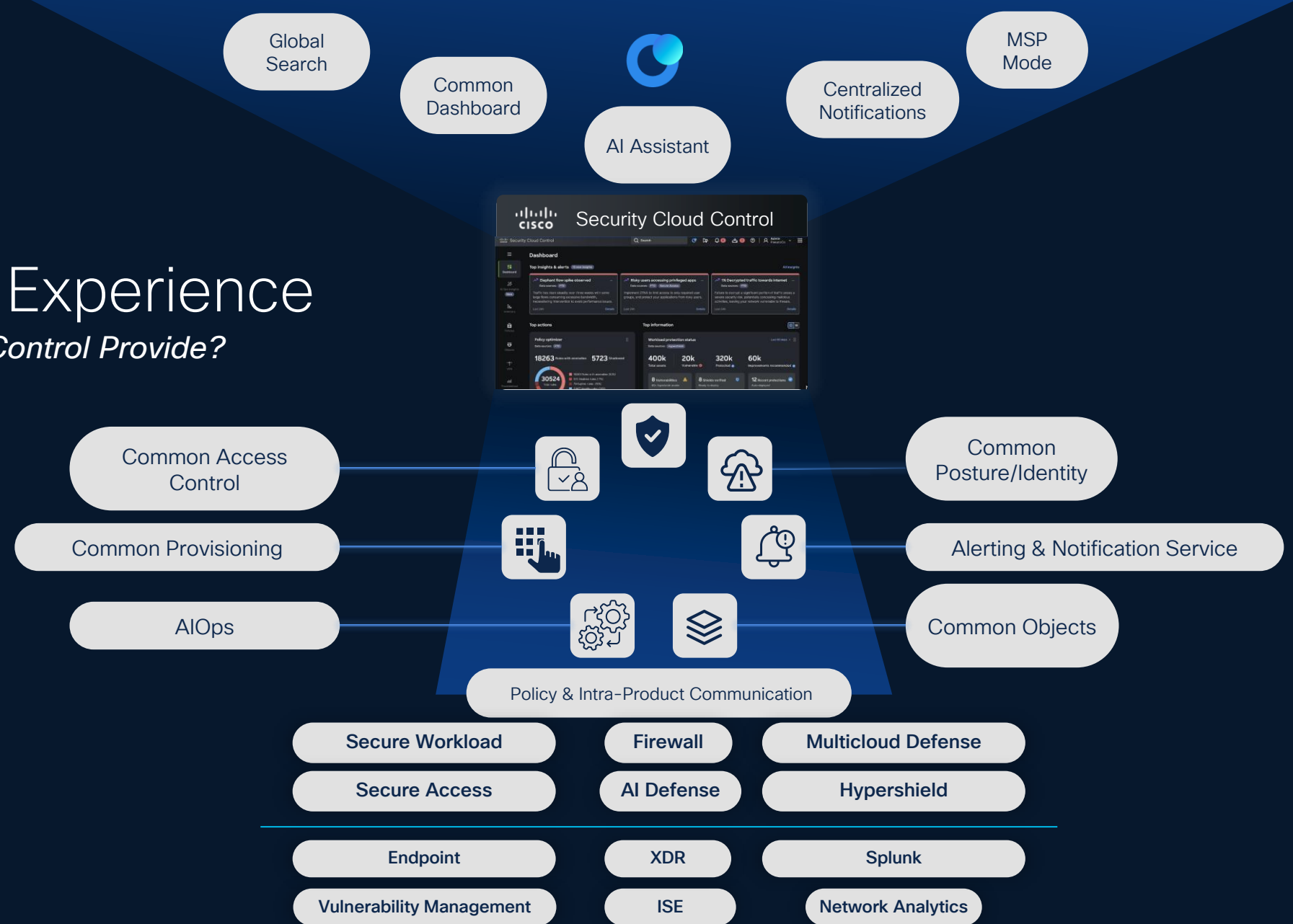
The screenshot shows the Cisco Security Cloud Control dashboard. The browser address bar displays `security.cisco.com/dashboard`. The dashboard header includes the Cisco logo and the text "Security Cloud Control". On the left, a sidebar contains a menu with "Organization Demo Red" and "Home". Below the menu is a "Products" section listing five items: AI Defense, Firewall, Hypershield, Multicloud Defense, and Secure Access, each with a corresponding icon. To the right of the sidebar, the main content area is titled "Home" and "Top Insights & Alerts" with a badge for "9 Active Insights". A prominent alert card titled "Network Throughput Anomaly" is displayed, indicating a data source of "FTD_Branch_1" and stating that "AIOPS has detected anomalous patterns in firewall throughput".

Annotations with arrows point from external labels to the product names in the sidebar:

- AI Defense** points to the AI Defense product.
- Hypershield** points to the Hypershield product.
- Secure Access** points to the Secure Access product.
- Firewall** points to the Firewall product.
- Multicloud Defense** points to the Multicloud Defense product.
- Mesh Policy** points to the Mesh Policy product.

A unified User Experience

What Does Security Cloud Control Provide?



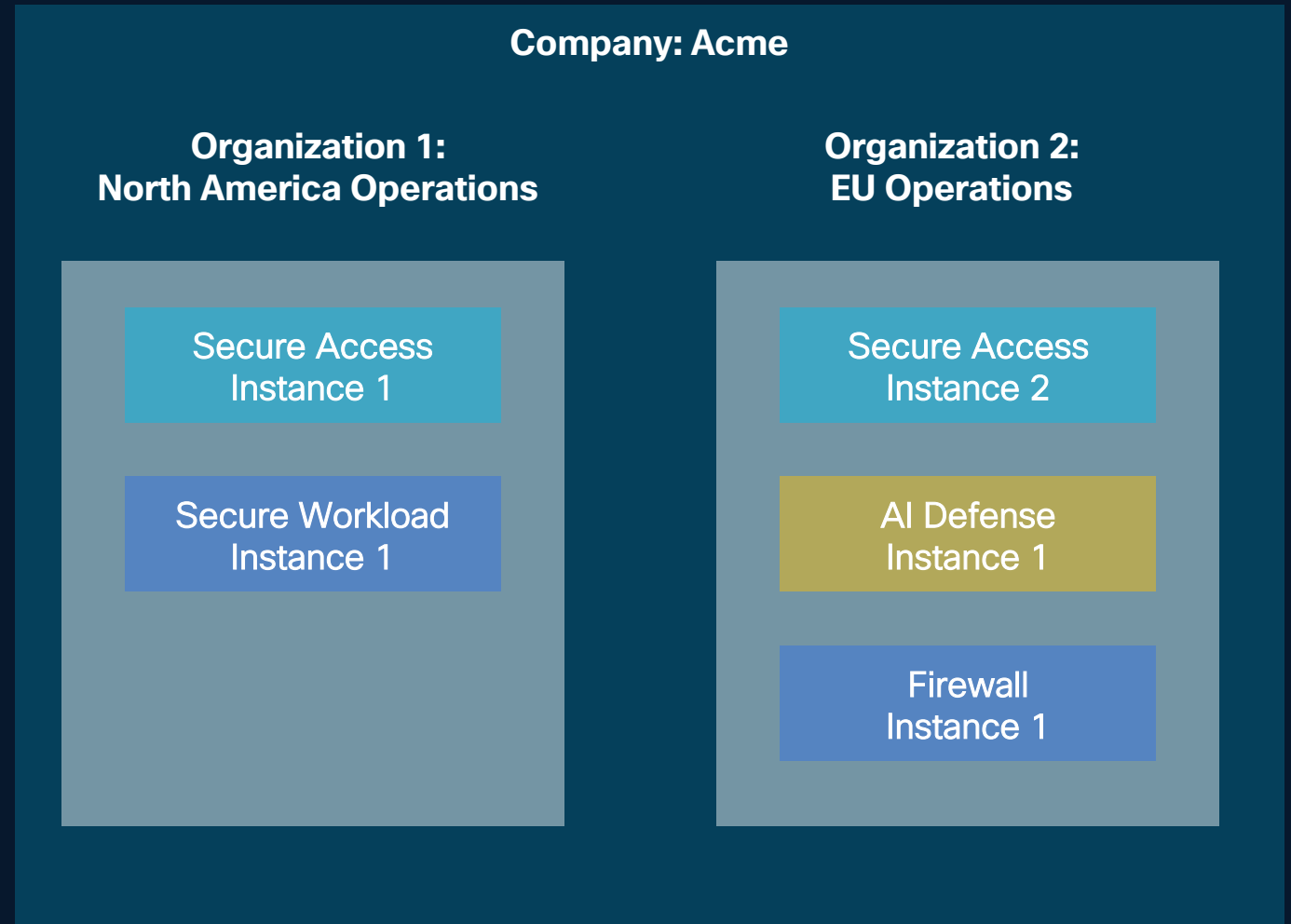
New to Security Cloud Control?

Getting Started

- No problem!
- Navigate to security.cisco.com, and create an organization.
- Creating an organization is free!
- Organizations are region specific.
- All Products that you enable for an organization will be in the same region.
- If you have a requirement to have regional separation of data, create a new organization in that region.

What is an “Organization” in Security Cloud Control?

- Trust boundary inside which products are provisioned
- Products in the same organization trust one another and share navigation in Security Cloud Control
- Can have a *single* instance of each product
- Must have a region set
- Per product region assignment after claiming aligned to Org region
- Can be renamed at any time



Organization creation region setting

Why might a customer require more than one Organization?

- You require more than one instance of a product (e.g. two Secure Access accounts / tenants)
- You have chosen different geographic regions for different products



Getting Started Demo



Security Cloud Sign On

Email

Continue

Don't have an account? [Sign up now](#)

Or

[Other login options](#)

[System status](#) [Policy statement](#)

Agenda

- 01 Why Security Cloud Control?
- 02 Getting Started with Security Cloud Control
- 03 Product Provisioning
- 04 User Management
- 05 Unified User Experience
- 06 SCC Firewall Management
- 07 A Look Ahead...What is Next?
- 08 Key Takeaways

Claiming and Activation

Product Provisioning

- Security Cloud Control Provides a Single Experience to Claim, Manage, and Activation Product Subscriptions.
- This vastly simplifies deployment of the Cisco Security Portfolio, both for our SaaS and non-SaaS products.
- Products are added with simple Claim codes, sent via e-mail.
- Claim codes are one time use.

Claim Subscription

1 Enter subscription claim code

2 Review products

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 *

Product & Subscriptions claim process

1. Claim subscription with claim code
2. Product and service activation status (start date etc.)
3. Action required to activate the product
4. Summary of products and their current activation state

Overview - Default Enterprise

Enterprise ID - a3e0b814-9749-4f1e-9db6-1bbd11edf785

1 [Claim subscription](#)

2 **Product and service activation status** **1**

Cisco Secure Endpoint Start date 12/09/2024 **3** [Action required](#)

4 **Products**

Cisco XDR **Activation in progress**

Essentials

Subscription ID	DevSub0104
End date	01/30/2025
External instance ID	-
Quantity	100
Region	Asia Pacific, Japan and China

Cisco Secure Email Threat Defense **Activated**

Cisco Secure Email Threat Defense

Subscription ID	DevSub0104
End date	01/30/2025
External instance ID	546ae0fe-db45-42a4-ac4b-dde866d12d3e
Quantity	100
Region	Australia

<https://security.cisco.com>

Customer journey to tenant and product onboarding

1

Initial
Claim
Email

Enable Cisco Security Cloud Control

Hi {Kt}!

Cisco has introduced Security Cloud Control to manage Cisco product subscriptions, user, group, and role access, and integration of your enterprise's Identity Provider. Please use the following claim code **ABCD-EFGH-IJKL-MNOP** to activate this feature. You will need a Cisco Security Cloud Sign On account to proceed.

1. Sign in to control.security.cisco.com with your Security Cloud Sign On account.

If this is your first time signing in to Security Cloud Control, a new enterprise will be created for you automatically, and associated with your account. If multiple enterprises are already associated with your account, select the desired enterprise from the **Enterprise** menu.

2. Follow the on screen instructions to enter your claim code **ABCD-EFGH-IJKL-MNOP** when prompted, and follow the on screen instructions to review and claim your prod subscription.

For help and detailed instructions on claiming your subscription, see the [Claiming a subscription](#).

For help claiming your subscription, contact our support team at tac@cisco.com or **1-800-553-2447** (US & Canada). You can find the support number for your region on Cisco's [support](#) website.

2

Sign into
security.cisco.com
with SCSO

Security Cloud Sign On

Email

Continue

Don't have an account? [Sign up now](#)

Or

[Other login options](#)

[System status](#) [Policy statement](#)

3

Create your
Organization

Create new organization

New organization name *

50 character limit

Region deployment *

This selection determines the deployment for all products and services added to this organization. [Read documentation.](#)

Cancel Create

4

Claim your
subscription

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 *

Claiming and Provisioning Demo

☰

 Enterprise
Propel-IT - North America

>

 Home

Products

 Firewall

Platform services

 Favorites

>

 Security Devices

 Shared Objects

 Platform Administration

>



Assign roles

Create organization users and assign roles to control access.

Assign

 **Other tasks**

 CLAIM SUBSCRIPTION

Claim subscriptions to activate instances in your organization.

Claim

 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

 INTEGRATE IDENTITY PROVIDER (IDP)

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

Configure

Agenda

- 01 Why Security Cloud Control?
- 02 Getting Started with Security Cloud Control
- 03 Product Provisioning
- 04 User Management
- 05 Unified User Experience
- 06 SCC Firewall Management
- 07 A Look Ahead...What is Next?
- 08 Key Takeaways

Unified User Management

User Management

- Secure Cloud Control provides one place to configure:
 - Users
 - User Permissions
 - User Groups
 - Identity Providers
- No longer will you need to go to each application to configure the same user again and again.
- Users for existing products will automatically be imported and those user will maintain their existing permissions.

Per Application Granular Control

User Management

- Each Product still maintains their own administrators and user administration hierarchy.
- Increased enterprise visibility of which users have access to which applications.
- Active Directory Integration supported out of the box
- Bring your own IdP!
- Activity Log tracks user management.

User Management Demo

☰

Enterprise

Propel-IT - North America

➤

Home

Products

AI Defense

Firewall

Hypershield

Multicloud Defense

Secure Access

Platform services

Favorites

➤

Security Devices

Shared Objects

Platform Administration

➤



Assign roles

Create organization users and assign roles to control access.

Assign

🛠️ Other tasks

🔍 CLAIM SUBSCRIPTION

Claim subscriptions to activate instances in your organization.

...

Claim

🏠 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

🔍 INTEGRATE IDENTITY PROVIDER (IDP)

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

...

Configure

Agenda

- 01 Why Security Cloud Control?
- 02 Getting Started with Security Cloud Control
- 03 Product Provisioning
- 04 User Management
- 05 Unified User Experience
- 06 SCC Firewall Management
- 07 A Look Ahead...What is Next?
- 08 Key Takeaways

Consolidated Navigation

Unified User Experience

- Multi-product support from the left navigation menu
- Common services, always available
 - User management
 - Favorites
 - Security Devices/Inventory
 - Common Objects
- Unified AI Assistant
- Shared Notifications
- Unified Product Documentation

Security Cloud Control User Interface

Summary

- New left navigation integrates product menus from across the portfolio
- Shown only when products are activated and users have access
- Services like search, AI Assistant, notifications, and help expressed globally
- Organizations isolate data and contain multiple products
- View entire organization from a single admin's standpoint

The screenshot displays the Cisco Security Cloud Control user interface. Key components are annotated with green labels and dashed blue boxes:

- Organization Switcher:** Located at the top left, showing the current organization as 'Stark Enterprises - North America'.
- Home:** The main dashboard area, featuring 'Top insights & alerts' and 'Micro App 1'.
- Top Nav:** The top navigation bar, including a search bar, user profile (Carter Briggs), and various status icons.
- User Profile:** A dropdown menu for the user profile.
- Side Nav:** The left navigation menu, categorized into 'Products' (AI Defense, Firewall, Hypershield, Multicloud Defense, Secure Access, Secure Workload) and 'Platform services' (Favorites, Security Devices, Shared Objects, Platform Management).
- Micro App 1:** A card displaying 'Top insights & alerts' with three alerts: 'Elephant flow spike observed', 'Risky users accessing privileged apps', and '1% Decrypted traffic towards internet'.
- Micro App 2:** A card displaying 'Asset connectivity status' with a donut chart showing 15% disconnected assets and a table of disconnected assets.

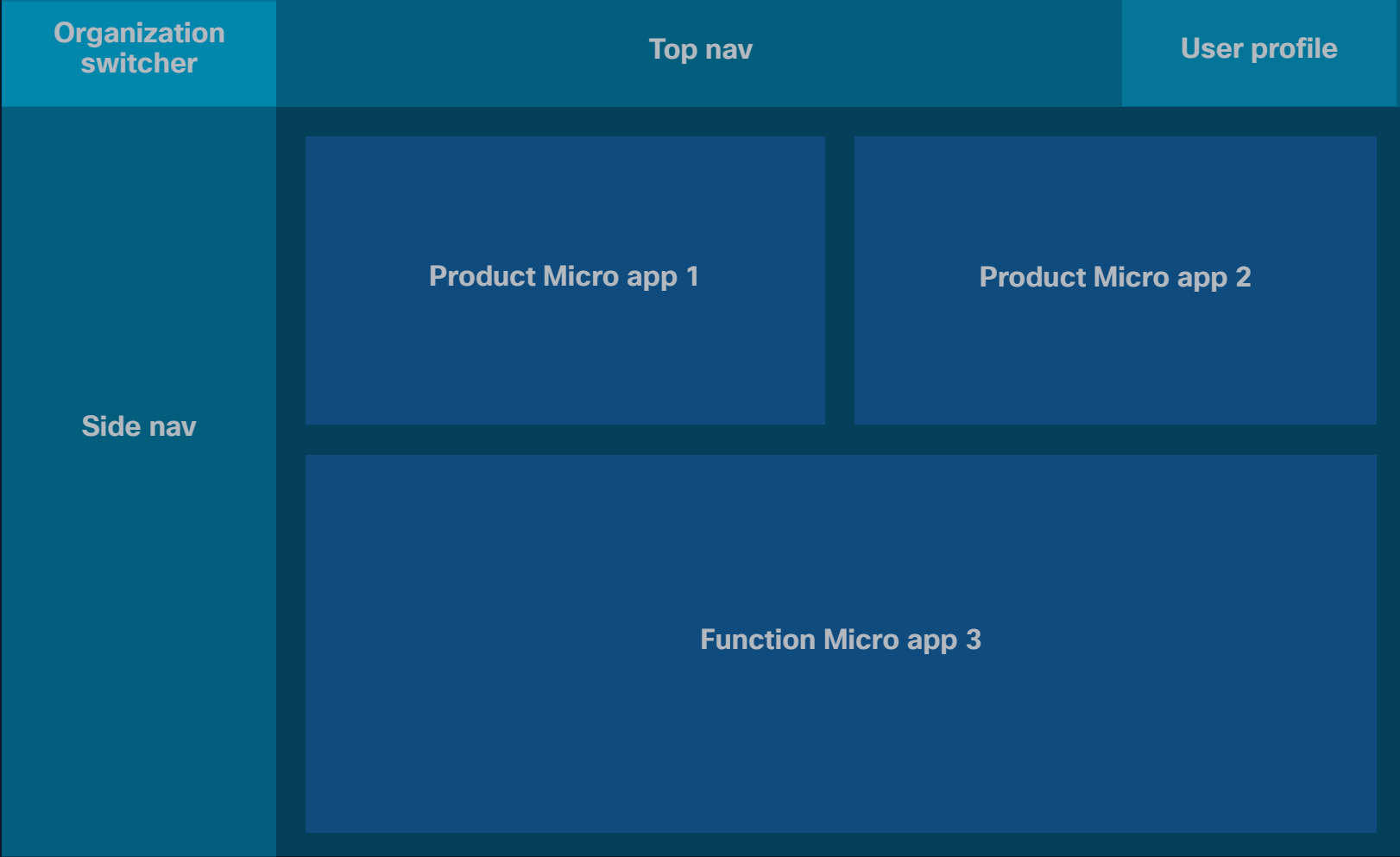
Asset connectivity status details:

Source	Count	24hr Δ
Firewall devices	250	↑ 11%
Universal ZTNA Firewall devices	45	↑ 5%
Network tunnel groups	36	—
Resource connectors	8	—
Cloud accounts	1	—
Tesseract security agents	12,942	↑ 4%
Workload agents	19	—

Security Cloud Control Microapp Architecture

Summary

- Host application that will support products as runtime microapps
- Built using Magnetic design systems and components
- Supports user preferences and accessibility



Unified Experience Demo

Enterprise
Stark Enterprises - North America

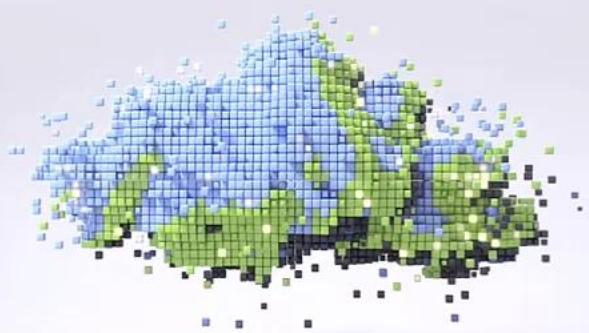
Home

Products

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

Platform services

- Favorites
- Security Devices
- Shared Objects
- Platform Administration



Assign roles

Create organization users and assign roles to control access.

Assign

Other tasks

CLAIM SUBSCRIPTION

Claim subscriptions to activate instances in your organization.

Claim

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

INTEGRATE IDENTITY PROVIDER (IDP)

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

Configure

Agenda

- 01 Why Security Cloud Control?
- 02 Getting Started with Security Cloud Control
- 03 Product Provisioning
- 04 User Management
- 05 Unified User Experience
- 06 **SCC Firewall Management**
- 07 A Look Ahead...What is Next?
- 08 Key Takeaways

Security Cloud Control Firewall Management

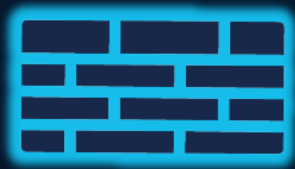
Bringing your firewall portfolio together with Security Cloud Control.



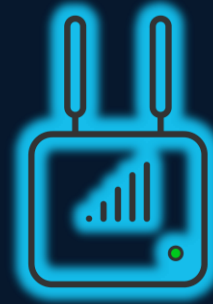
FTD



IOS*



ASA



Meraki MX*



Catalyst
SD-WAN



Manage security policy & appliances from the cloud

Security Cloud Control

Type 'Ctrl' + '/' to search

Aaron Hackney

Organization Demo Red

Platform menu

Firewall

Dashboard

Monitor

Insights & Reports

Events & Logs

Manage

Policies

Objects

Security Devices

Secure Connections

Administration

Platform services

Favorites

Security Devices

Shared Objects

Security Devices

Devices Templates

Search by Device Name, IP Address, or Serial Number

Displaying 13 of 13 results

All ASA AWS VPC Duo Admin Panel FTD IOS Meraki

	Name	Location	Version	Access Policy	Last Deploy	Configuration Status	Connectivity	Universal zero trus...	
☐	archon.hacksbrain.com_172.30.4.189_Orion FMC FTD	172.30.4.34:443	7.4.1	Orion-Edge	-	-	Unknown	NA	
☐	firepower_192.168.0.166_172.16.0.102 FMC FTD	172.16.0.102:443	7.2.9	ac	-	-	Unknown	NA	
☐	firepower_192.168.0.41_192.168.0.43 FMC FTD	192.168.0.43:443	7.2.9	ac	-	-	Unknown	NA	
☐	pashra_ftd_postman_test_byol_withmodel_piam FTD			Intrusion 1334	-	-	Pending	NA	
☐	pashra_ftd_postman_test_byol_withmodel_piam_1 FTD			Intrusion 1334	-	-	Pending	NA	
☐	test FTD			Default Access Control Policy	-	-	Pending	NA	
☐	u73c01p05-ftd-1010-3 FTD		7.4.1	MyMandatoryPolies	-	Not Synced	Online	NA	En
☐	u73c01p05-ftd-1010-4 FTD		7.4.1	MyMandatoryPolies	-	Not Synced	Online	NA	En
☐	vFMC-A_192.168.0.81_172.16.0.100 FMC FTD	172.16.0.100:443	7.2.9	ac	-	-	Unknown	NA	

Rows per page 50 1 - 13 of 13 1

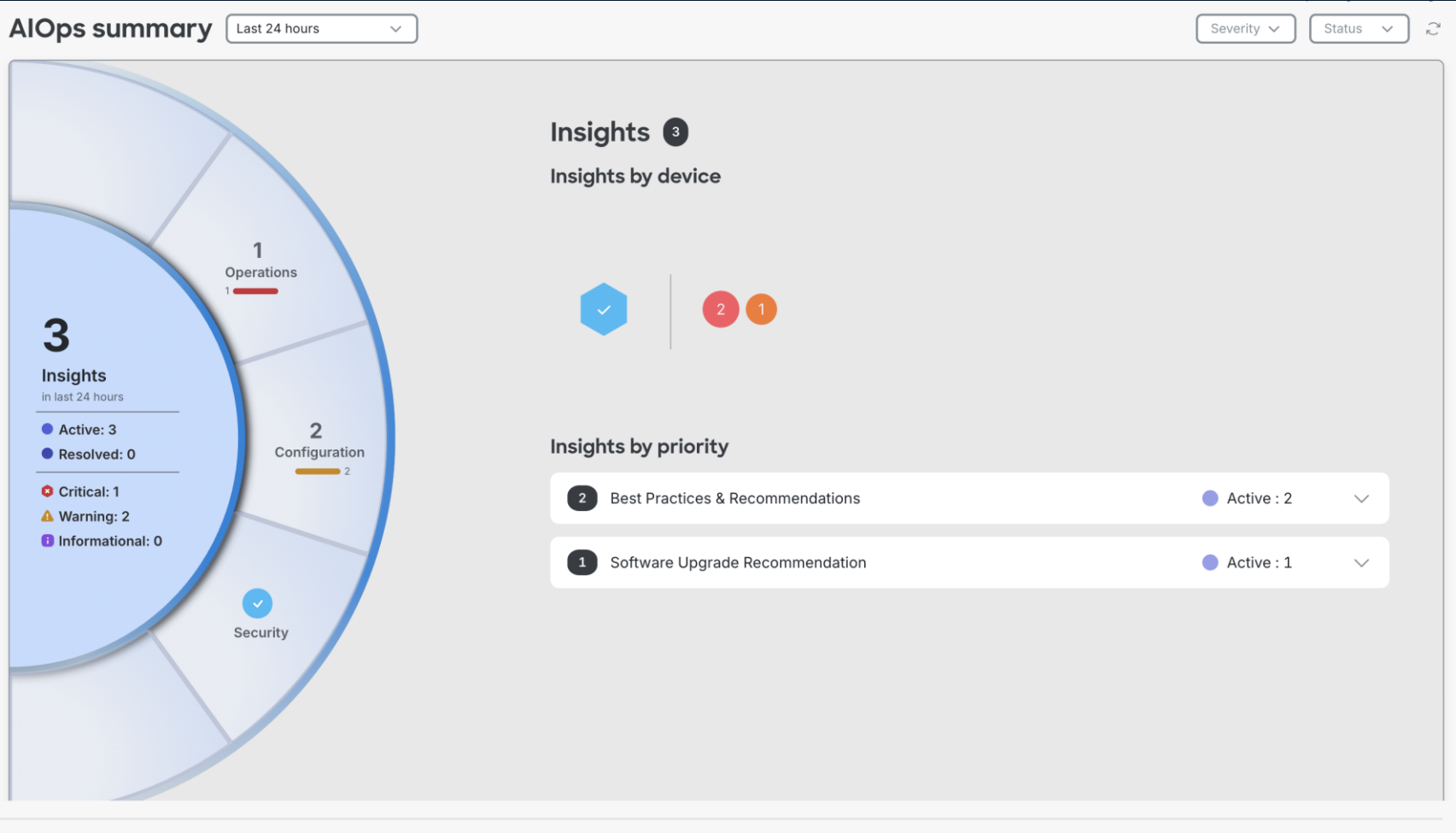


Make my life easier!



AI Ops and Agentic AI Ops

AI Ops – Become more efficient, accurate, and adaptive



AI Ops – Become more efficient, accurate, adaptive



- Policy Analyzer and Optimization
- Best Practices and Recommendations
- Feature Adoption
- Software Upgrade Planner
- Agentic Troubleshooting and break/fix 
- End of life hardware and software notifications 
- Predictive Analytics (Elephant flows and more) 

AI Ops – Policy Analyzer and Optimization

- Review and optimize policies automatically
- Detect shadowed, redundant, overlapping, and unused rules
- Generate and export detailed analysis reports
- Apply optimization changes with a single click
- Supports FTDs managed by on-prem FMCs

AI Ops / Policy Analyzer and Optimizer

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

76 Total Rules

- 70 (92.1%) Healthy rules
- 5 (6.6%) Unhealthy rules
- 1 (1.3%) Disabled rules

Total 5 anomalies in 5 unhealthy rules

- Shadowed rules: 2 (40.0%)
- Expired rules: 0 (0.0%)
- Total overlap objects: 0 (0.0%)
- Redundant rules: 2 (40.0%)
- Mergeable rules: 1 (20.0%)
- Partial overlap objects: 0 (0.0%)

Search by Access Control Policy Name, Analysis Status, or Remediation Status Displaying 4 of 4 results

Access Control P	Devices	Total Rules	Observations	Analysis Status	Last Modified	Last Analyzed	Remediation Stat	Remediation Tim
☒ Edge-Firewall	1	68	4 (6% Optim	Completed	09/21/2025, 1	09/22/2025, 1		
☐ Paradise	1	8	1 (12% Optim	Completed	09/09/2025, 1	09/19/2025, 1		
☐ Default Acces	0	0	0 (0% Healthy	Completed	02/28/2025, 1	09/19/2025, 1		
☐ Default Acces	0	0	0 (0% Healthy	Completed	02/28/2025, 1	09/19/2025, 1		

Edge-Firewall

Devices: 1

Total Rules: 68

Observations: 4 (6% Optimizable)

Analysis Status: Completed

Last Modified: 09/21/2025, 11:00:39

Last Analyzed: 09/22/2025, 10:55:55

Remediation Status: Not Running

Hit Count Aggregation Status: Completed

Analysis Actions

- [View analysis details & optimize](#)
- [Download analysis report](#)

Remediation Actions

- [Remediation history \(0 version available\)](#)

Policy Observation

We found a total of 4 anomalies.

Duplicate Rules (3)

- Fully Shadowed Rules: 2
- Fully Redundant Rules: 1
- Overlapping Objects (0)

AI Ops / Policy Analyzer and Optimizer

Edge-Firewall

Policy last analyzed: 09/30/2025, 08:58:42 | Policy last modified: 09/30/2025, 08:53:45

Summary **Duplicate rules 3** **Expired rules 0** **Mergeable rules 1** **Overlapping objects 0** **Policy insights**

Fully Shadowed rules (2)

A shadowed rule is a rule that will never evaluate network traffic because the traffic matches the criteria of a preceding rule in the policy, and the preceding rule takes action before the shadowed rule can be matched. [Learn about Shadowed Rules](#)

☒ All 2 Fully Shadowed rules have been marked for disable. Click apply remediation to disable the rules. [Hide details](#) [Undo](#)

Observation - 1 ☒ 1 rule fully shadowed disabled

Observation - 2 ☒ 1 rule fully shadowed disabled

AI Ops – Software Upgrade Planner



- Highlights devices that are running code that may have newer versions available
- Highlights CVEs and bug fixes as published by PSIRT and Release Notes
- Clicking on the device takes you to the list of CVEs and bug fixes
- The CVE details page links to the Security Advisory page to learn more about the CVE
- Currently, we only provide details around high and critical CVEs
- Phase 2 will deep link to the upgrade process for the devices selected



AI Ops – Software Upgrade Planner



u73c01p05-ftd-1010-3

Last updated: 36 minutes ago

Requires upgrade

Cisco Firepower 1010 Threat Defense | Current version: 7.4.1

Recommended upgrades

Recommended version 1

7.4.2.4

Details

Security vulnerability fixes26

Bug fixes0

Release notes for Version 7.4.2.4

Golden version

7.6.2

Details

Security vulnerability fixes26

Bug fixes0

Release notes for Version 7.6.2

Recommended version 2

7.7.10.1

Details

Security vulnerability fixes26

Bug fixes0

Release notes for Version 7.7.10.1

Security vulnerability fixes

Bug fixes

Search

2Severity

26 results

CVE ID	Title	Impact	Description	CVSS score ⓘ	Available fixes
CVE-2025-20363	Cisco Secure Firewall Adaptive Security Appliance Sof...	Critical	A vulnerability in the web services of Cisco Secure Firewall A...	9.0	7.0.8, 7.0.8.1, 7.2.0
CVE-2025-20333	Cisco Secure Firewall Adaptive Security Appliance Sof...	Critical	A vulnerability in the VPN web server of Cisco Secure Firewa...	9.9	7.0.8.1, 7.2.9, 7.2.0
CVE-2024-20412	Cisco Firepower Threat Defense Software for Firepow...	Critical	A vulnerability in Cisco Firepower Threat Defense (FTD) Soft...	9.3	7.2.8, 7.2.8.1, 7.2.0
CVE-2024-20353	Cisco Adaptive Security Appliance and Firepower Thr...	High	A vulnerability in the management and VPN web servers for ...	8.6	7.0.6.2, 7.0.6.3, 7.0
CVE-2025-20224	Cisco IOS, IOS XE, Secure Firewall Adaptive Security ...	High	Multiple vulnerabilities in the Internet Key Exchange Version ...	8.6	7.0.8, 7.0.8.1, 7.2.0
CVE-2025-20225	Cisco IOS, IOS XE, Secure Firewall Adaptive Security ...	High	Multiple vulnerabilities in the Internet Key Exchange Version ...	8.6	7.0.8, 7.0.8.1, 7.2.0

AI Ops – Upgrade Planner Demo

Monitoring Docker cont...

Security Cloud Control

security.cisco.com/firewalls/unified-dashboard

Security Cloud Control

Type 'Ctrl' + '/' to search

Aaron Hackney

Organization Demo Red

Platform menu

Firewall

Dashboard

Monitor

Insights & Reports

Events & Logs

Manage

Policies

Objects

Security Devices

Secure Connections

Administration

Platform services

Favorites

Security Devices

Shared Objects

Dashboard

Top Insights & Alerts 9 Active Insights

Network Throughput Anomaly
Data source: FTD_Branch_1
AIOPS has detected anomalous patterns in firewall throughput
122d ago Details

Best practices and recommendations ...
Data source: Ottawa-SEC
AIOPS has detected 5 needs review checks.
89d ago Details

Best practices and recommendations ...
Data source: Toronto
AIOPS has detected 7 needs review checks.
89d ago Details

Top Actions

Policy Analyzer and Optimizer
Data Sources: FTD
23 Total Rules
21 Healthy Rules (91%)
1 Unhealthy Rules (4%)
1 Disabled Rules (4%)
Shadowed 0 0%
Redundant 1 100%
Details

Top Information

Overall Inventory
30 Total Devices
Issues 4
Pending Action 4
Other 7
Online 15
Device End-of-Life 0
View All Devices

RA VPN Sessions
No results found

© 2025 Cisco Systems, Inc.

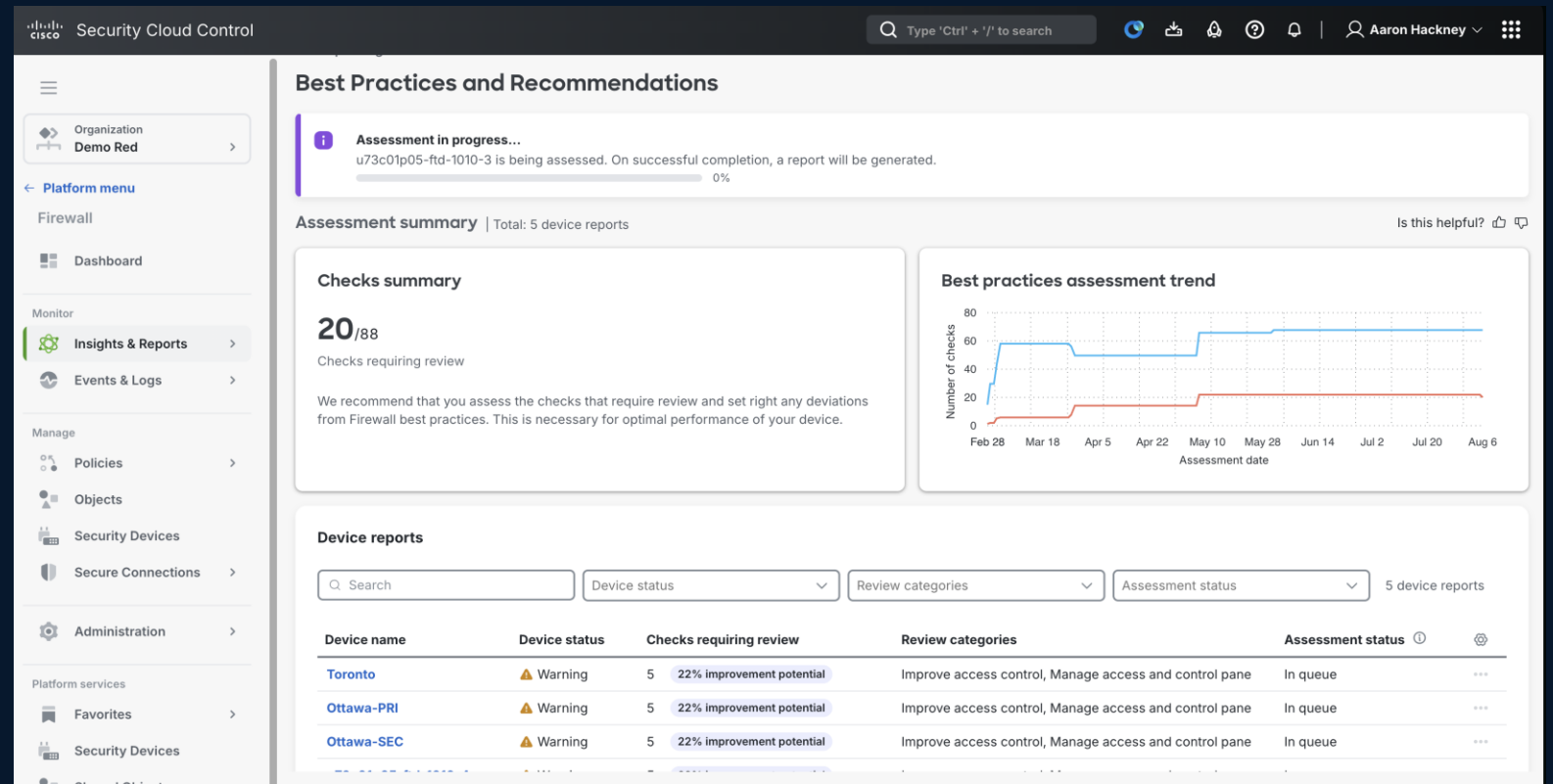
Privacy Policy General Terms



AI Ops – Best Practices and Recommendations



- Common FTD practices: logging, app detection, and more
- Common FMC practices: Scheduling VDB updates, variable sets, etc.
- Includes “HOW-TO” actions and documentation links



AI Ops – Best Practices and Recommendations FMC



Manage access and control pane

4

Total checks

2

Require review

Checks

Automatic VDB Updates Not Configured on Firepower Management Center

Requires review

Warning

Your Firepower Management Center currently lacks configuration for automatic Vulnerability Database (VDB) downloads and updates. Keeping your VDB up to date is crucial for enhancing application identification and improving threat detection capabilities. To configure automatic VDB updates, follow these steps:

1. Navigate to: System > Scheduling > Add Task
2. Create a Task: Set up tasks to download and install the VDB automatically.

For detailed instructions, refer to the [Cisco Firepower Management Center Configuration Guide](#).

All variable-sets have HOME_NET set to any

Requires review

Informational

All variable sets have the HOME_NET variable set to "any". This configuration means that the Intrusion Prevention System (IPS) will not use specific internal network IPs for any policy or rule, potentially reducing the effectiveness of your security measures.

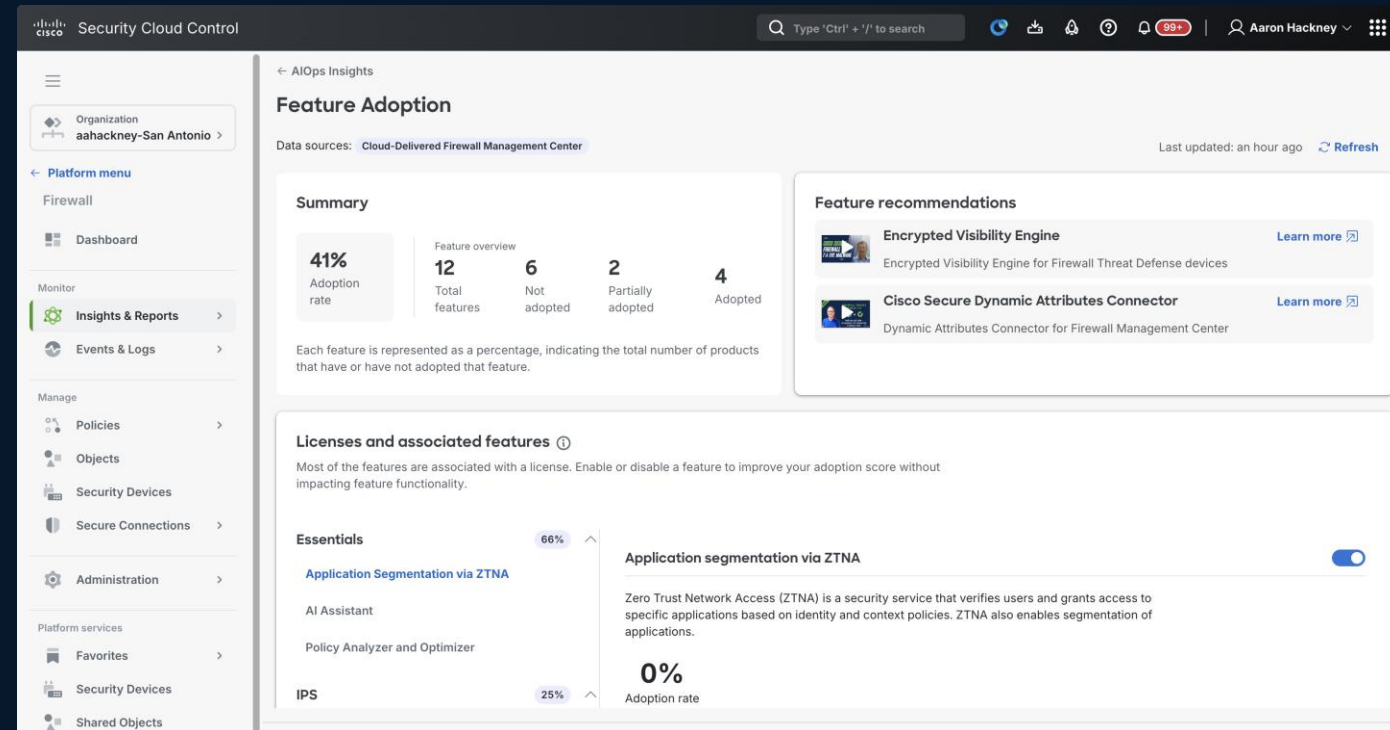
****Reference****

Please review and update the HOME_NET variable to reflect your internal network IPs to ensure optimal security performance. For detailed instructions on configuring the HOME_NET variable, refer to the config guide here:
<https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/management-center/device-config/720/management-center-device-config-72/objects-object-mgmt.html#ID-2243-000004e1>

AI Ops – Feature Adoption



- Maximize your FTD investment
- Discover new features and capabilities
- Understand license requirements
- Watch feature use-case videos
- Follow step-by-step enablement guides



You want a managed FMC in the cloud?



*No problem! We provide a Cloud Delivered FMC
in SCC Firewall Management (1200+ FTDs!!!!!!)*

Cloud-delivered FMC (cdFMC)



Truly cloud native – not just a “vm in the cloud”



SCALE is currently ~1500 FTDs, goal/future is 2000 from a single cdFMC



cdFMC is managed and maintained by SCC Firewall operations teams



You don't have to manage, maintain, patch the FMC – OPEX SAVING



No power or space required; all delivered from the cloud – OPEX SAVING



Focus on managing your security policy, not managing the manager



Management-plane or data-plane used to communicate with the cdFMC



FTD failsafe features like manual and auto-rollback in case of a config mistake

Cloud-delivered FMC (cdFMC) – All the things

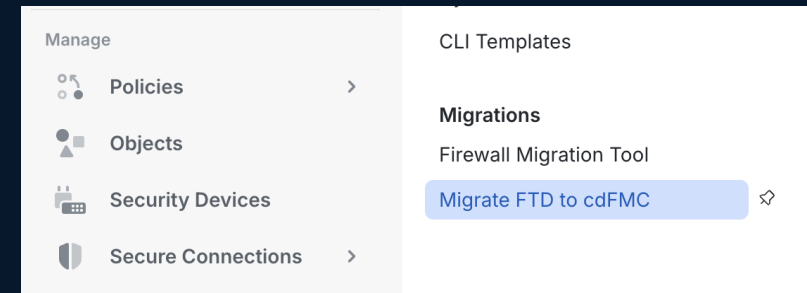
- SD-WAN
- Universal Zero Trust
- Passive Identity
- ISE Integration
- Cloud delivered CSDAC
- Identity Intelligence



Migrate an FTD from on-prem FMC to cdFMC



- On-prem FMC needs to run at LEAST FMC 7.2
- FMC 1000, 2500, or 4500 CAN RUN a special release FMC 7.4 for migration purposes. See [this guide](#).
- The FTD, policies, VPN configurations, objects, etc. will be moved to the cdFMC
- The FTD is unregistered from the on-prem FMC
- cdFMC becomes the manager of that FTD post-migration
- Auto-registers FTD to send events to cloud
- Tooling all provided by SCC Firewall Manager



Migrate other Firewalls to FTD Managed by cdFMC



- SCC Firewall provides a cloud instance of the Firewall Migration Tool (FMT)
- Supported Platforms for Migration Include:
 - ASA
 - Fortinet
 - Palo Alto Networks
 - Check Point

 Firewall Migration Tool (Version 7.7.10.1)

Select Source Configuration ⓘ

Source Firewall Vendor

Select Source ^

Cisco Legacy Firewalls

Cisco ASA (8.4+)

Cisco Secure Firewall Device Manager (7.2+)

Third Party Firewalls

Check Point (r75-r77)

Check Point (r80-r81)

Fortinet (5.0+)

Microsoft Azure **New**

Palo Alto Networks (8.0+)

Cloud Logging



Centralized logging for ASA, FTD, and Catalyst SD-WAN

Security Analytics and Logging (SAL)



- Per device or per Gig pricing tiers
- Retention from 90 days to 3 years+
- Scheduled reports exportable as CSV
- Datastore for Unified Events Viewer
- Live logs for troubleshooting
- Splunk integration



Security Analytics and Logging (SAL)



Organization
aahackney-San Antonio

Platform menu

Firewall

Dashboard

Monitor

Insights & Reports

Events & Logs

Manage

Policies

Objects

Security Devices

Secure Connections

Administration

Platform services

Favorites

Security Devices

Shared Objects

Event Logging

New Unified Event Viewer is now available for FTD Events! [Click here to launch](#)

Historical

Live

ResponderPort: "443"

Search

Storage Utilization

UTC Time

Local Time

All times shown in Local (EST)

Views

View 3

Date/Time	Device Type	Event Type	Sensor ID / Hostname	Initiator IP	Responder IP	Responder Port	Protocol	Action	Policy	Application
Waiting for matching events after 23:47:41.										
Sep 30, 2025, 23:46...	FTD	Conne...	paradise...	192.168.4...	17.253.127...	443	tcp	Allow	Paradise	HTTPS
<div><div><div>ClientApplicationRiskIndex</div><div>1</div></div><div><div>ConnectionDuration</div><div>227</div></div><div><div>ConnectionID</div><div>28749</div></div><div><div>ConnectorID</div><div>dee117bc-4f71-4bbc-9f1b-f0883ac5649d</div></div><div><div>Device</div><div>Paradise</div></div><div><div>DeviceIP</div><div>192.168.46.46</div></div><div><div>DeviceType</div><div>FTD</div></div><div><div>DeviceUUID</div><div>4f973622-192a-11ef-b86d-8386f7533b4a</div></div><div><div>EgressInterface</div><div>vti_1</div></div><div><div>EgressVRF</div><div>Local</div></div></div> <div><div><div>IngressInterface</div><div>wormhole-pv</div></div><div><div>IngressVRF</div><div>Local</div></div><div><div>IngressZone</div><div>wormhole-pv</div></div><div><div>InitiatorBytes</div><div>2129</div></div><div><div>InitiatorBytesDropped</div><div>0</div></div><div><div>InitiatorIP</div><div>192.168.44.50</div></div><div><div>InitiatorPackets</div><div>16</div></div><div><div>InitiatorPacketsDropped</div><div>0</div></div><div><div>InitiatorPort</div><div>57735</div></div></div> <div><div><div>ResponderPackets</div><div>23</div></div><div><div>ResponderPacketsDropped</div><div>0</div></div><div><div>ResponderPort</div><div>443</div></div><div><div>URL</div><div>https://gsp-ssl.ls.apple.com</div></div><div><div>VPN_Action</div><div>Encrypt</div></div><div><div>WebApplication</div><div>Web Browsing</div></div><div><div>WebApplicationID</div><div>4294967295</div></div><div><div>WebApplicationProductIVITYIndex</div><div>0</div></div><div><div>WebApplicationRiskIndex</div><div>0</div></div><div><div>Timestamp</div><div>Sep 30, 2025, 23:46:21</div></div></div>										

Sep 30, 2025, 23:35...

FTD

Conne...

FPR1150.h...

192.168.3...

35.160.57...

443

tcp

Allow

Edge-Firewall

HTTPS

Sep 30, 2025, 23:35...

FTD

Conne...

FPR1150.h...

172.30.4.33

52.217.123.9

443

tcp

Allow

Edge-Firewall

HTTPS



But what about ASA Devices?



ASA Appliance Management



- Shared Access-Policy
- Shared Objects (With FTD and more)
- Shared Platform Settings (Syslog, DNS, SSH, Sysopt)
- Interfaces
- Certificate Management
- Scheduled Upgrades
- Health Metrics 

Plus much, much more!

ASA Appliance Management



ASA Policies

Snuffy

Security Devices

Selected Access List

outside

+ Create Access List

Search rules

Displaying 150 of 259 results

Go to

Top

Bottom

Refresh

Reset

More

	Action	Protocol	Source	Port	SGT Gr	Destina	Port	SGT Gr	Logging	Remark	Hits (D	Edit
☐	1	Allow	TEST-ICMP	Any	Any	Any	Any	Any				
				+ Add Rule Here		+ Add Section Divider						
☐	2	Block	ip	Any	Any	Any	HOME	Any				
☐	3	Block	ip	172.30	Any	Any	192.16	Any				

outside

259 Access Control Entries

Details

Resources

outside / in

Actions

Assign Interfaces

Share

Copy

Delete

Device

Snuffy

Model

ASA v (V01)

Location

172.30.4.147:8443

Failover Mode

Not Configured

Disk Size

7.98 GB

Disk Usage

47.96 MB

☒ Schedule Upgrade

10/02/2025 02:39:30 PM

EST (UTC-05:00)

1 ASA Software Image

ASA Software Image 9.16(4)

☐ Skip Upgrade

Image Source

☒ Use SCC Image Repository

☐ Specify Image URL

Software Image

Select an Image

9.23(1.19) 179.3 MB

9.22(2.14) 160.52 MB

9.22(2.13) 160.51 MB

Continue

Select the ASA software image you want to upgrade to. Only compatible versions of ASA and ASDM are shown.

DNS must be properly configured on the device before attempting the upgrade. Please reference [Configure DNS on ASA](#) for details.

If you check "Skip Upgrade," the ASA software image on your device will not be changed. You may still upgrade ASDM.



ASA Health Monitoring

Need to enable in Administration -> General Settings

Enable ASA Health Monitoring ⓘ



Dashboard

Multicloud Defense

Monitor

Insights & Reports

Events & Logs

Manage

Policies

Objects

Security Devices

Secure Connections

Administration

Device Health Metrics

Device:

qe_team_asa_145

Duration:

Range

Date and time range:

22/09/2025, 20:58

 →

30/09/2025, 20:58

Reset date range

Auto-refreshed every 5 mins

View Security Devices

2 items selected ⓘ

Up to 4 interfaces can be selected at a time for comparison

Reset

Interface	Logical Name	Link Status	Overruns ⓘ	Underruns ⓘ	Dropped Packets ⓘ	L2 Decodes	Input Errors Avg	Output Errors	Input Packets ⓘ
☒	Management0/0	management	UP	0	0	10.4K	0	0	103
☐	GigabitEthernet0/4	GigabitEthernet0/4	DOWN	0	0	0	0	0	0
☐	GigabitEthernet0/7	GigabitEthernet0/7	DOWN	0	0	0	0	0	0
☒	GigabitEthernet0/1	outside	UP	0	0	46	0	0	76
☐	GigabitEthernet0/0	inside	UP	0	0	46	0	0	77
☐	GigabitEthernet0/2	GigabitEthernet0/2	DOWN	0	0	0	0	0	0
☐	GigabitEthernet0/5	GigabitEthernet0/5	DOWN	0	0	0	0	0	0

Rows per page:

30

 1 - 10 of 10 <

1

 >

500B

Bytes

0B

September 23 04:04

Time

September 29 09:2



Notifications



Get notifications of important events

SCC Platform Notifications



- Notifications can be send via email or HTTP/S (Webhook)
- Webhooks can be sent to Webex, Slack, and MS Teams
- Webhooks can also be sent to generic endpoints
- HTTP payload contains the notification in json

Notification Settings
Add the email address of the person who will receive notifications, and specify the message service type for that person.

Email subscribers

Email address	Added on	Actions
aahackne@cisco.com	2/7/2025	Edit
willsilv@cisco.com	11/30/2023	Edit

Service Integrations
Security Cloud Control can forward notifications to specified messaging applications or services. You need to generate a webhook URL from your messaging application. Security Cloud Control will forward notifications for the events selected above. [Learn more](#)

Name	Service Type	Actions
XDR-Webhook	CUSTOM	Edit
Splunk-TCP-65150	CUSTOM	Edit
Webex-Channel-Notify	WEBEX	Edit

Edit Service Integration

- ☒ Upgrades
 - ☒ Failed
 - ☒ Started
 - ☒ Succeeded
- ☒ Migrate FTD to cdFMC
 - ☒ Failed
 - ☒ Started
 - ☒ Succeeded
 - ☒ Commit pending
- Device events**
 - ☒ All device events
 - ☒ Went offline
 - ☒ Back online
 - ☒ Conflict detected
 - ☒ HA state changed
 - ☒ Site-to-site session disconnected
 - ☒ Certificate expiring
 - ☒ Device approaching end of life
- Event Log Reports**
 - ☒ All report events
 - ☒ Report generation started
 - ☒ Report generation completed
 - ☒ Report generation failed

SCC Platform Notifications

Webhook to Webex

CDO Webhook Notifications

Public

MessagesPeople (6)ContentMeetings+ Apps

Log in to [Security Cloud Control](#) for more details.

Event Report Generation "Media_Server_Connections" has completed

Query Name: Media_Server_Connections

Tenant: cisco_aahackne

Time: Tue, 30 Sep 2025 09:01:08 UTC

Log in to [Security Cloud Control](#) for more details.

CDO-NOTIFY-TEST 8:55 AM

Cloud-delivered FMC Deployment running

Deployment job in progress. [Total: 1 | Succeeded: 0 | Failed: 0]

Tenant: CDO_cisco_aahackne

Time: Tue, 30 Sep 2025 13:55:05 UTC

Log in to [Security Cloud Control](#) for more details.

CDO-NOTIFY-TEST 8:56 AM

Cloud-delivered FMC Deployment succeeded

Deployment job succeeded. [Total: 1 | Succeeded: 1 | Failed: 0]

Tenant: CDO_cisco_aahackne

Time: Tue, 30 Sep 2025 13:56:49 UTC

Log in to [Security Cloud Control](#) for more details.

Seen by

Webhook to Splunk

1

Time

Event

✓

9/29/25
1:01:56.000 AM

{ "uid": "4a6ceee4-77d8-4f3b-90a7-324aadbdef25", "timestamp": 1759125712776, "type": "SAL_QUERY", "tenantUid": "44dcd3bf-e608-40db-a588-e9150da988de", "tenantName": "CDO_cisco_aahackne", "details": { "salQueryEvent": "QUERY_COMPLETED", "salQueryName": "Daily_Security_events", "salQueryUid": "1f83a60a-f791-403f-8f8c-bc3e8d0b7cea", "queryCriteria": "(timestamp:[20230101165606000 TO 20230823180739680]) AND (DeviceType:FTD OR DeviceType:\$isEmpty OR DeviceType:\$isNull) AND (EventType:FileEvent OR EventType:IntrusionEvent OR EventType:MalwareEvent OR (EventType:ConnectionEvent AND ((NOT IP_ReputationSI_Category:\$isEmpty) OR (NOT URL_SI_Category:\$isEmpty) OR (NOT DNS_SI_Category:\$isEmpty))))", "searchString": "", "salStatus": "COMPLETE", "swcJobId": "de8cbbac", "swcFileName": "Daily_Security_events_de8cbbac.csv.gz" } }

Show syntax highlighted

Event Actions

Type	Field	Value	Actions
Selected	details.swcFileName	Daily_Security_events_de8cbbac.csv.gz	▼
	host	notify.hacksbrain.com:65150	▼
	source	http:scc-cisco_aahackne-notify	▼
	sourcetype	httpevent	▼
Event	details.queryCriteria	(timestamp:[20230101165606000 TO 20230823180739680]) AND (DeviceType:FTD OR DeviceType:\$isEmpty OR DeviceType:\$isNull) AND (EventType:FileEvent OR EventType:IntrusionEvent OR EventType:MalwareEvent OR (EventType:ConnectionEvent AND ((NOT IP_ReputationSI_Category:\$isEmpty) OR (NOT URL_SI_Category:\$isEmpty) OR (NOT DNS_SI_Category:\$isEmpty))))	▼
	details.salQueryEvent	QUERY_COMPLETED	▼
	details.salQueryName	Daily_Security_events	▼
	details.salQueryUid	1f83a60a-f791-403f-8f8c-bc3e8d0b7cea	▼
	details.salStatus	COMPLETE	▼
	details.searchString		▼
	details.swcJobId	de8cbbac	▼
	fileName	Daily_Security_events_de8cbbac.csv.gz	▼
	formatted_date	2025-09-29 01:01:52	▼
	salQueryName	Daily_Security_events	▼
	salStatus	COMPLETE	▼
	status	COMPLETE	▼
	tenantName	CDO_cisco_aahackne	▼
	tenantUid	44dcd3bf-e608-40db-a588-e9150da988de	▼
	timestamp	1759125712776	▼
	type	SAL_QUERY	▼
	uid	4a6ceee4-77d8-4f3b-90a7-324aadbdef25	▼



SCC cdFMC Notifications



Cloud-delivered Firewall Management Center

Policies / Actions / Alerts / Alerts

Q

Search

Deploy

aahackne@cisco.com

▼

Monitor

Analysis

Alerts

Manage

Policies

Devices

Objects

Integration

Create Alert

Name	Type	In Use	Enabled
Graylog	Syslog	Not Used	☒
Health-Alerts	Email	Not Used	☐
Splunk-65150-tls	Webhook	In Use	☐
Splunk-65151-clear-text	Webhook	In Use	☒

Edit Webhook Alert Configuration

Name

Splunk-65151-clear-text

URL

notify.hacksbrain.com:65151/ser...

TLS Type

None

Alert Configuration is in use by 1 Policy:

Test Connection

Cancel

Save



Automation



A rich public API lets you automate all the things...

SCC Firewall Manager Public API



- Single API gateway for both Firewall Manager API calls and cdFMC API calls
- Simple bearer-token header authentication
- Well documented searchable API reference with examples
- cdFMC API is also searchable from here

<https://developer.cisco.com/docs/cisco-security-cloud-control-firewall-manager>

SCC Firewall Manager Public API



Documentation

All

Cisco Security Cloud Control (SCC)

Security Cloud Control Firewall Manager API Documentation

Search docs

BETA

Change Requests

Changelogs

Command Line Interface

Connectors

Tenant Management

Commands

Inventory

ASA Interfaces

Device Upgrades

Device Health

Remote Access Monitoring

MSP Inventory

MSP Tenant Management

MSP User Management

Device Upgrades

Upgrade ASA device

Operation Id: upgradeAsaDevice

Description: This asynchronous operation upgrades the ASA firmware and ASDM software versions on the device. Note: Newly detected or modified certificates will be automatically approved.

POST /v1/inventory/devices/asas/{deviceId}/upgrades/trigger

Request Parameters

Path

deviceUid required | string

The unique identifier, represented as a UUID, of the device in Security Cloud Control.

Request body

Schema Definition

Example Body

UpgradeAsaDeviceInput

Configuration

Parameters

Code Snippets

Curl

Python

Nodejs

Copy

curl -L --request POST \n--url https://api.us.security.cisco.com/firewall/v1/inventory/\n--header 'Content-Type: application/json' \n--header 'Accept: application/json' \n--data '{\n \"asdmVersion\": \"7.6(2)\" or \"7.6(2).openjre\", \n \"softwareVersion\": \"9.4(1)\" \n}'



Agenda

- 01 Why Security Cloud Control?
- 02 Getting Started with Security Cloud Control
- 03 Product Provisioning
- 04 User Management
- 05 Unified User Experience
- 06 SCC Firewall Management
- 07 A Look Ahead...What is Next?
- 08 Key Takeaways

A Look Ahead with Security Cloud Control

What Can You Expect Soon?

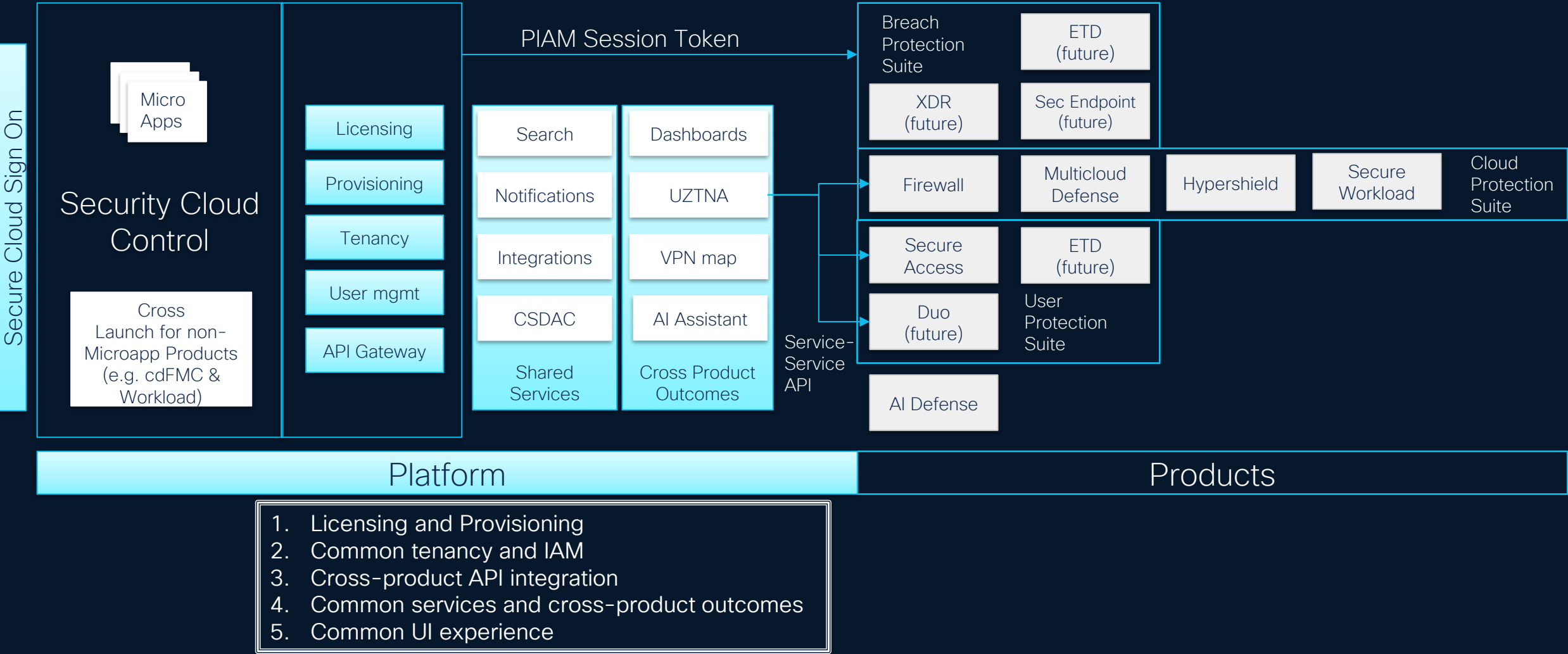
- More Products!
- ZTA
- Centralized User Context Service
- Customer Initiated Trials
- Duo Integration
- Next Gen SASE
- Shared Audit Logging
- Secure Cloud Client Management
- Unified API Gateway
- Managed Service Provider (MSP) Features

Security Cloud Control Platform Architecture

Legend

Platform

Products
(Micro-app)



Security Cloud Control MSP Portal

SCC Multi-Org Benefits

NEW

Streamlined Management and Maintenance:

Centralized management and maintenance reduce administrative duties, complexity, and cost.

Scalability and Flexibility:

Enterprises can easily scale their security infrastructure up or down based on demand without compromising security. The shared resource model allows for dynamic allocation of resources, which is crucial for organizations with fluctuating needs or rapid growth.

Cost Efficiency

Multi-tenant solutions reduce operational and infrastructure expenses by sharing resources across numerous tenants.

Enhanced Data Privacy and Isolation:

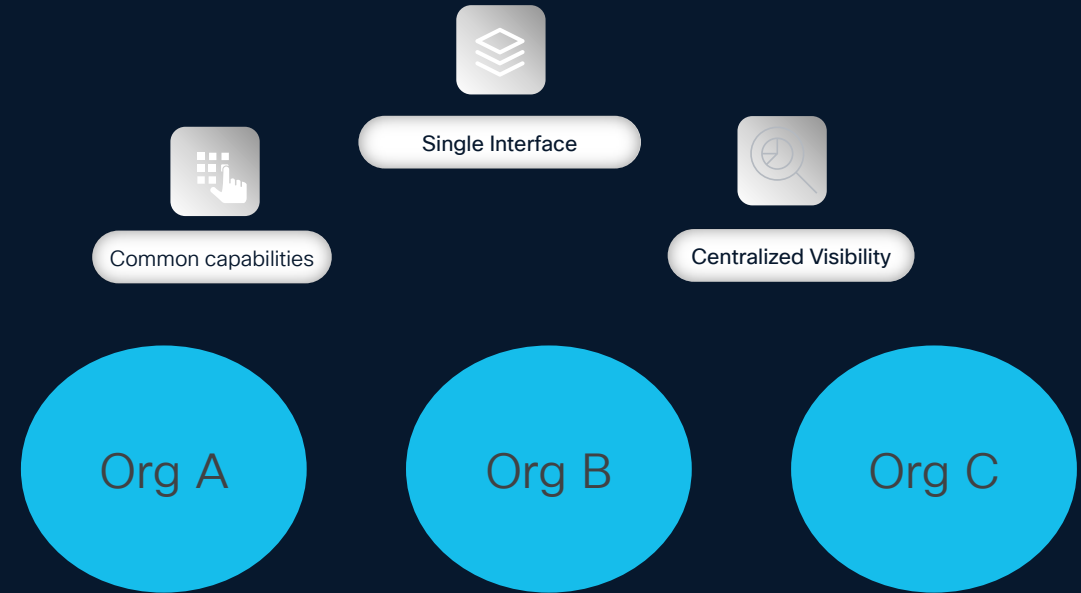
A core feature of multi-tenancy is the logical separation and isolation of sensitive information. Each tenant's data is kept private and secure, preventing unauthorized access between tenants.

SCC Multi-Org View for Enterprise customers

NEW

Use-Cases:

1. Mergers and Acquisitions (M&A)
2. Divisions and Business Units
3. International Subsidiaries and Regional Offices:
4. Franchise Models



NEW

One interface. Multiple customers.

Manager View

An efficient workspace to streamline day-to-day customer management and reduce complexity

Quickly switch between customers

Easily assign and control access to customer deployments and integrate with your identity provider

The screenshot displays the Cisco Security Cloud Control Manager View interface. The left sidebar contains navigation options under 'Manager Administration' (Managed Organizations, Subscriptions, Admin Access, Domains, Identity Providers, Activity Log, Manager Details) and 'Products' (Secure Access). The main content area is titled 'Administrator Access' and shows a table of administrator groups. The table has columns for Group name, Type, Description, and Applies to. The groups listed are 'Acme Solutions - Manager Admin Group' (Local), 'Steelworks Corp Admin Group' (Local), and 'All Products Administrator' (System). A 'Map identity provider' button is visible in the top right corner of the table area.

Group name	Type	Description	Applies to
Acme Solutions - Manager Admin Group	Local	—	Acme Solutions
Steelworks Corp Admin Group	Local	—	Some managed organizations
All Products Administrator	System	Add users to this group to give them administrator access to all products in this enterprise	Acme Solutions

Agenda

- 01 Why Security Cloud Control?
- 02 Getting Started with Security Cloud Control
- 03 Product Provisioning
- 04 User Management
- 05 Unified User Experience
- 06 SCC Firewall Management
- 07 A Look Ahead...What is Next?
- 08 Key Takeaways

Key Takeaways

- Unified Security Management across various enforcement points.
- No Disruption, Immediate Entitlement for existing CDO customers.
- Consistent Cross-Product Policy & Visibility.
- Seamless Integration with Cisco Secure Trial Console for Trials.

Before you go!

Create your FREE SCC Organization
And start your free SCC Firewall Manager trial

<https://security.cisco.com>

Complete your session evaluations



Complete a minimum of 4 session surveys and the Overall Event Survey to claim a Cisco Live T-Shirt.



Earn up to 800 points by completing all surveys and climb the Cisco Live Challenge leaderboard.



Level up and earn exclusive prizes!



Complete your surveys in the Cisco Live Events app.

Continue your education



Visit the Cisco Stand for related demos



Book your one-on-one Meet the Expert meeting



Attend the interactive education with Capture the Flag, and Walk-in Labs



Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand

Thank you

CISCO Live !

