



Put the Cisco AI Assistant to work

Make the most of Cisco AI Assistants

Prashanth Arun - Director, AI Software & Platforms
BRKAI-1623

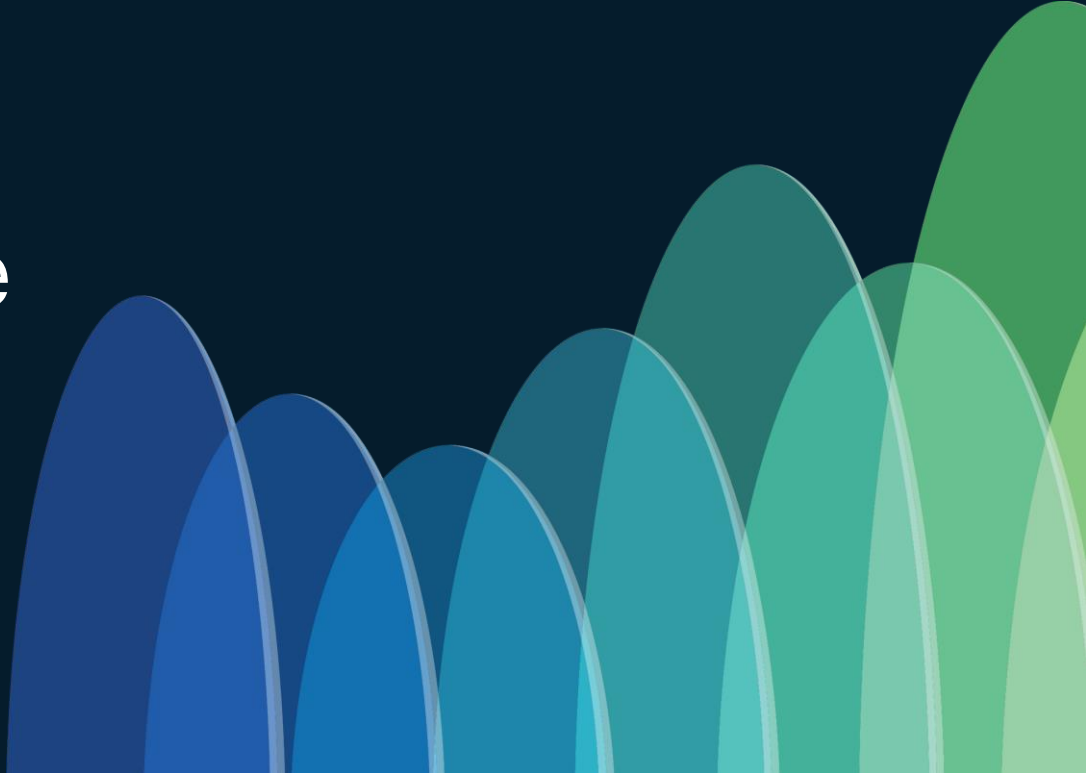
CISCO *Live!*



Agenda

- Artificial Intelligence in the Workplace today
- Cisco AI Assistants
- AI Assistants for Security
- AI Assistants for Networking
- Cisco Unified AI Assistant
- Conclusion

Artificial Intelligence in the Workplace today



AI is transforming the workplace

AI Assisted Collaboration & Productivity
Tools

Content Personalization &
Recommendations

Enhanced Decision Making &
Analytics

Automating Repetitive Tasks

Evaluating AI technology

Language Understanding &
Comprehension

Reasoning & Problem Solving

Code Generation

Image & Video Understanding

Frontiers of AI tech

General Intelligence & Reasoning

Autonomous Agents

Multi-Agent Orchestration

Adversarial Robustness

AI Assistant mission at Cisco

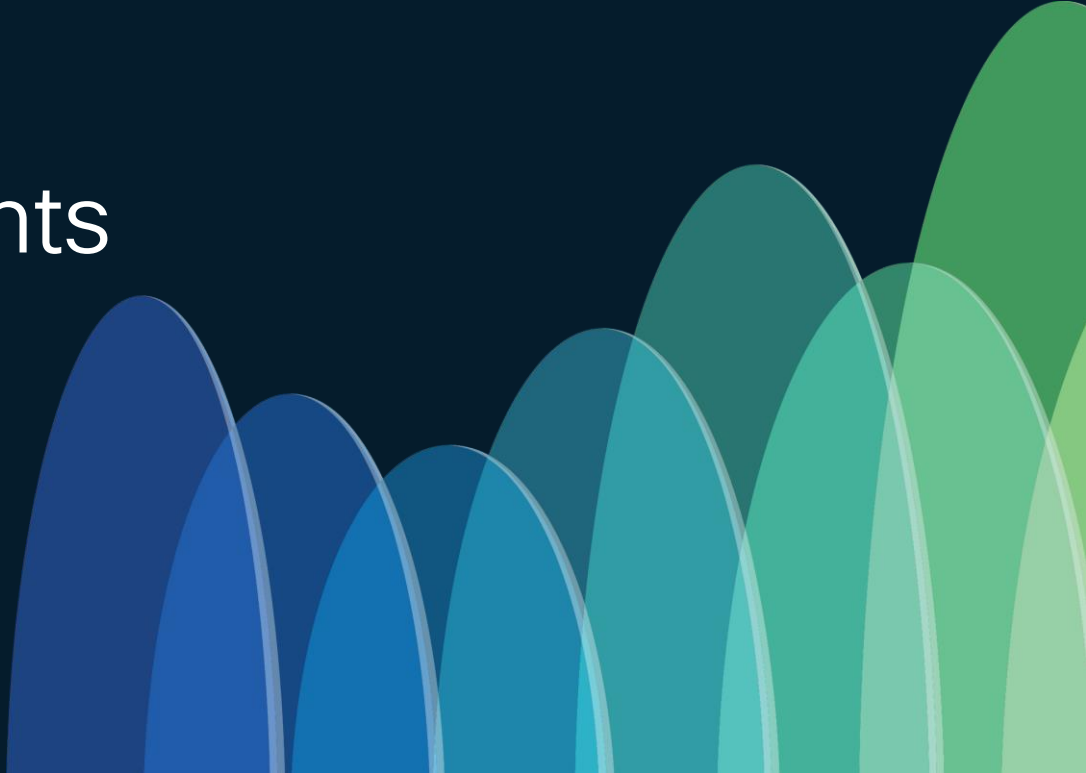
Providing Real-time Assistance & Collaboration

Enabling & streamlining workflows

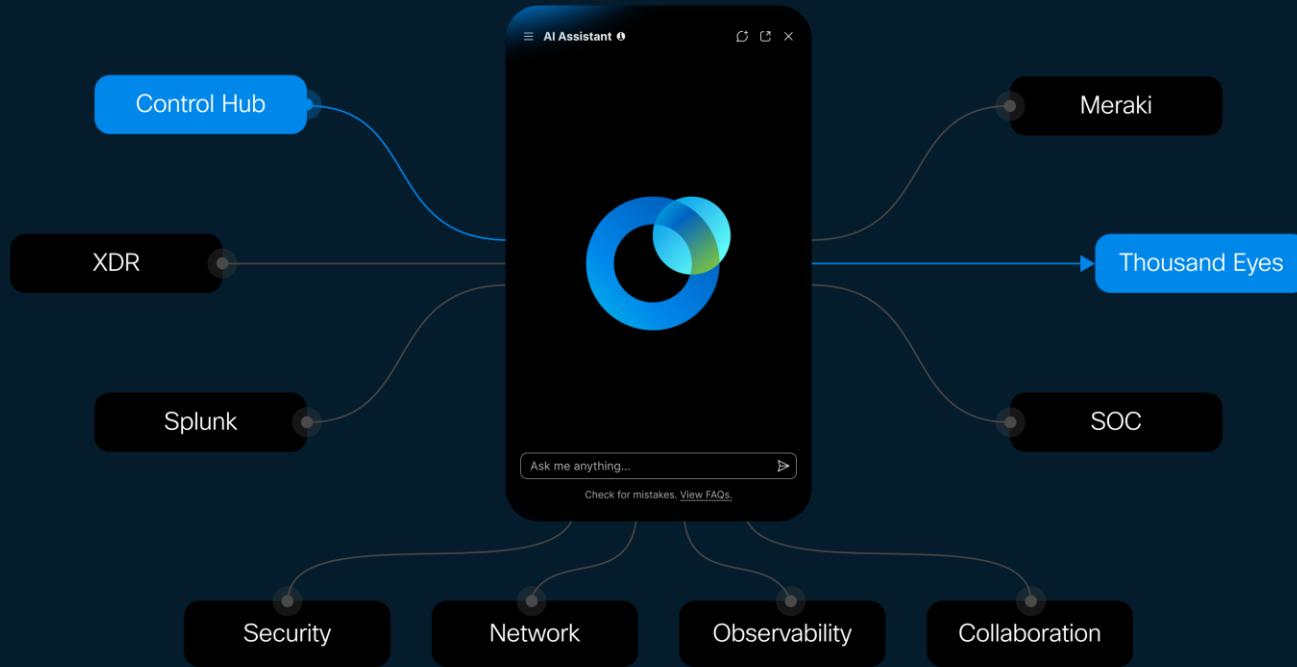
Enhancing User experience

Driving Innovation & Problem-solving

Cisco AI Assistants



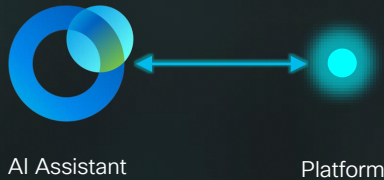
Cisco Assistant Ecosystem



AI Assistants Have “Skills”, Not Features

AI Skills

- **Definition:** Any action that a Cisco AI Assistant can performance.
- **Skills:** Troubleshooting, configuration, recommendations, etc.



Skills across AI Assistants

Documentation Search

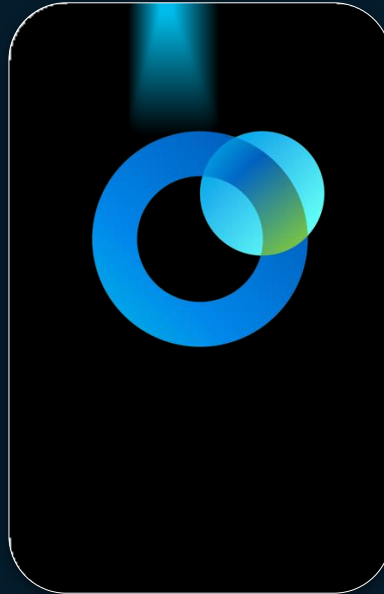
Search Cisco's product docs for clear, actionable, and simplified insights

Configuration Insights

Understanding & modifying configuration

Ticketing Integration with CX

Enables TAC case creation and modification



Troubleshooting help

Enables quick discovery of policies with fast, rich data responses on-demand

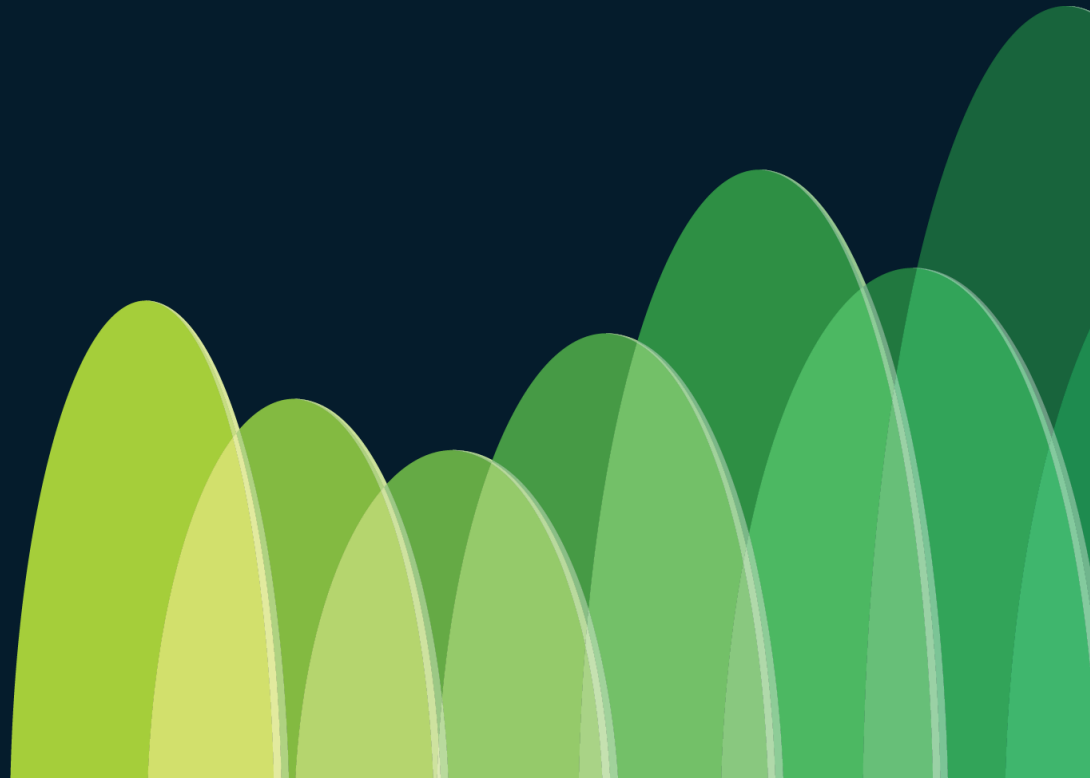
Recommended Actions

Proactively suggest actions to enable workflows and usage

AIOps Integration

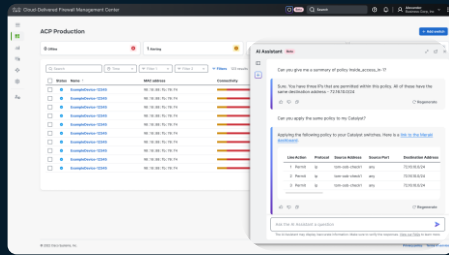
Insights into traffic, configuration, capacity to maintain operational capabilities

AI Assistants for Cisco Security



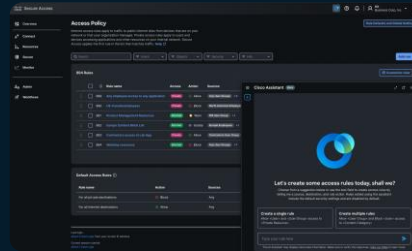
Cisco Security's Suite of AI Assistants

Firewall



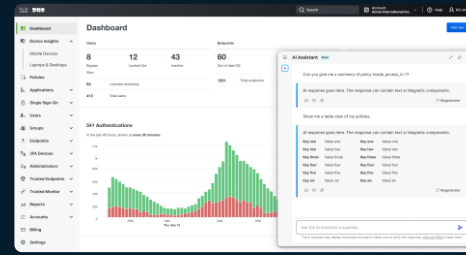
Block any **outbound** exfiltration to the IP address identified from the C&C

Secure Access



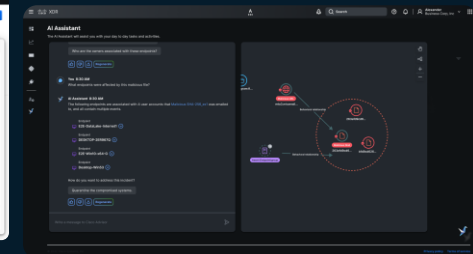
Ensure users **access** only resources they need securely

Duo



Lock affected user out of critical applications

XDR



Detect a **phishing attack** that has setup a C&C and is exfiltrating data outside the network.

AI Assistant for Firewall Management Center

Cisco Firewall AI Assistant Skills

Documentation Summarization

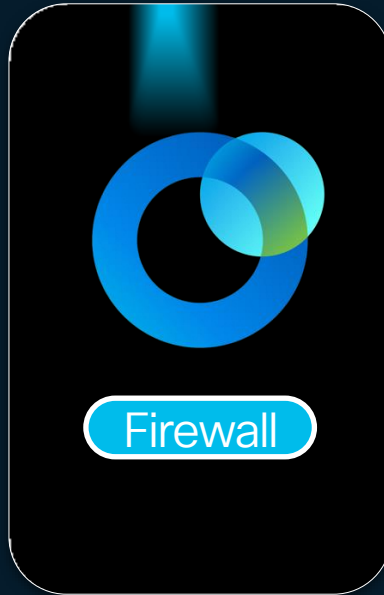
Search Cisco's product docs for clear, actionable, and simplified insights

Policy Rule Creation

Create policies with natural language

Ticketing Integration with CX

Enables TAC case creation and modification



Policy Insights

Enables quick discovery of policies with fast, rich data responses on-demand

Policy Analysis & Optimization

Proactively discover and remediate policy misconfigurations and anomalies

AIOps Integration

Insights into firewall traffic, configuration, capacity to enhance security posture.

Documentation Summarization

The screenshot displays the Cisco Defense Orchestrator (CDO) interface with the AI Assistant chat window open. The chat window shows a user asking, "How do I exclude Webex traffic from the remote access VPN?" and the AI Assistant providing a detailed response with a list of steps.

You

How do I exclude Webex traffic from the remote access VPN?

AI Assistant

You can exclude specific traffic, such as Webex, from the remote access VPN by using the dynamic split tunneling feature based on DNS domain names.

Here are the steps to follow:

1. From the **CDO home page**, click **Inventory**.
2. Locate the **Secure Firewall Threat Defense device** you want to apply this rule to.
3. Select the device and click **Device Overview** in the Device Management pane.
4. Configure the group policy to use Dynamic Split Tunnel:
 1. Choose **Devices > Remote Access**.
 2. Click **Edit** on the remote access VPN policy you want to configure for dynamic split tunneling.
 3. Click **Edit** on the required connection profile.
 4. Click **Edit Group Policy**.
5. Configure the Secure Client custom attribute:
 1. Click the **Secure Client** tab.
 2. Click **Custom Attributes** and then click **+**.
 3. Select **Dynamic Split Tunneling** from the Secure Client Attrib |

Ask the AI Assistant a question

[View User Guide](#) to learn more.

Policy Rule Creation

The screenshot shows the Cisco Defense Orchestrator AI Assistant interface. The main content area displays a confirmation message from the AI Assistant regarding the creation of a rule named 'Rules1'. The rule is configured to block Facebook traffic from source network 'fqdn_1' on the 'anna_acp1' policy. The rule is currently in a 'disabled state'.

AI Assistant Confirmation

Create a rule to block facebook over sourceNetwork fqdn_1

Here is your rule recommendation. This rule will be added in policy.

Rule Name	Action	Source Networks	Applications	Section	Policy Name
Rules1	BLOCK	fqdn_1	Facebook Comment, Facebook Games	DEFAULT	anna_acp1

Congratulations, your rule named **Rules1** is successfully created. The rule is created in a **disabled state** as of now. You can enable it from your policy detail page.

[Go to policy detail page](#)

Last data sync: about 20 hours ago

i Your feedback helps us improve the AI Assistant.

Ask the AI Assistant a question

[View User Guide](#) to learn more.

Policy Insights

The screenshot shows the Cisco Defense Orchestrator AI Assistant interface. A user has asked: "Can you scan my access control policies, except the raj-acp policy, and return the name of the user that last modified each policy with timestamp?". The AI Assistant has responded with a table of policy details.

AI Assistant
 The access control policies, excluding 'raj-acp', were reviewed. The names of the users who last modified each policy along with the timestamps were provided.

[Hide details](#)

#	Policy Name	Last Modified User	Last Modified Date
1	anna_acp2	Firepower System	2024-10-04 02:26:50+00:00
2	chuy_test1	Firepower System	2024-10-04 02:26:50+00:00
3	TEST1	Firepower System	2024-10-04 02:26:50+00:00
4	comparison_acp2	Firepower System	2024-10-04 02:26:50+00:00
5	ShTest	ethanz@cisco.com	2024-08-09 20:01:06+00:00
6	child_policy_1	Firepower System	2024-10-04 02:26:50+00:00

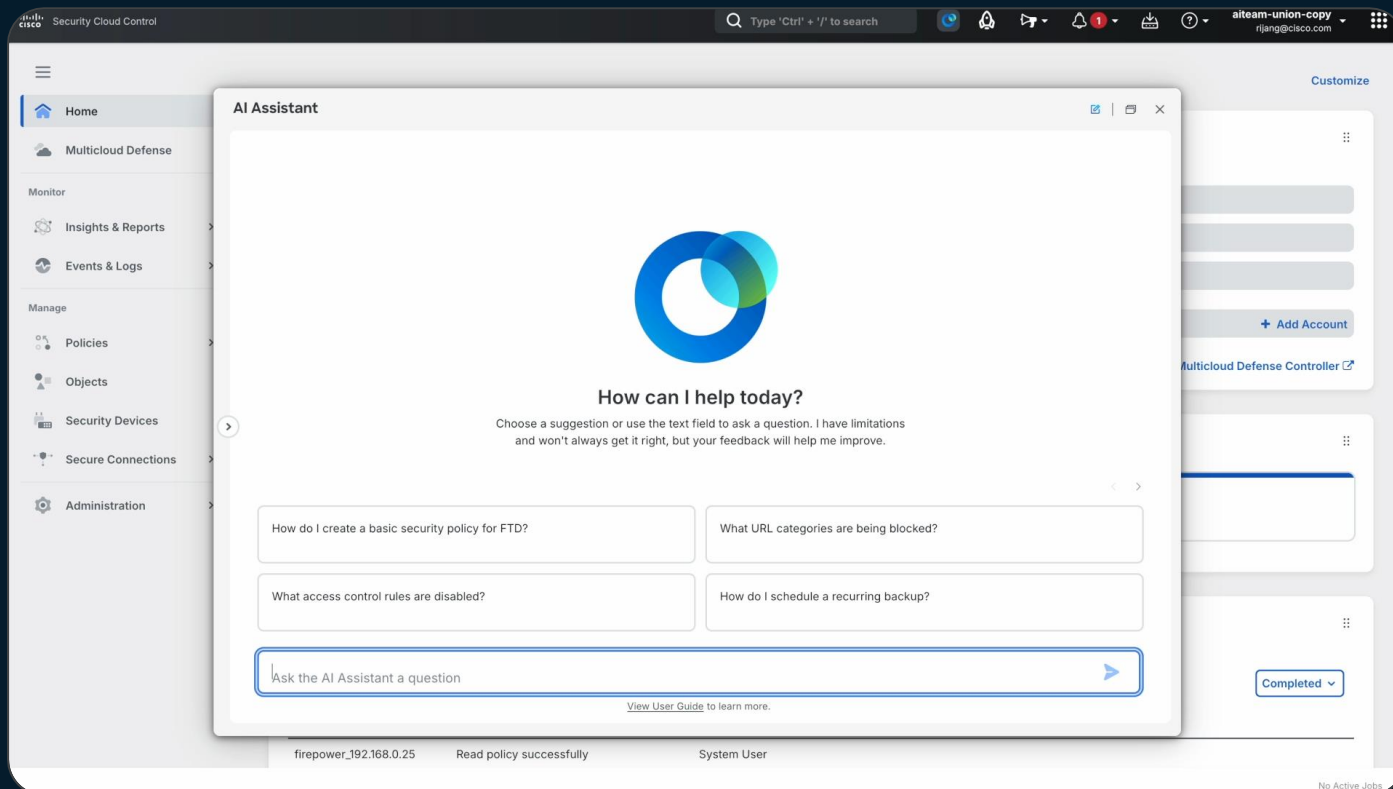
Ask the AI Assistant a question ▶

[View User Guide](#) to learn more.

Policy Analyzer & Optimizer

The screenshot displays the Cisco Defense Orchestrator AI Assistant interface. The main window shows a chat conversation where the user asks, "Show me duplicate rules for nyc_access_control_policy". The AI Assistant responds with a detailed analysis: "The NYC access control policy has 1358 redundant rules, 8612 shadowed rules, 15860 total rules, and 9970 duplicate rules." A horizontal bar chart visualizes the data, with 87% (8612) in red representing fully shadowed rules and 14% (1358) in blue representing fully redundant rules. Below the chart, four action buttons are provided: "Disable all redundant rules for policy 'nyc_access_control_policy'", "Disable all shadowed rules for policy 'nyc_access_control_policy'", "Disable fully shadowed rules for policy 'nyc_access_control_policy'", and "Disable fully redundant rules for policy 'nyc_access_control_policy'". A fifth button, "Disable all for policy 'nyc_access_control_policy'", is also visible. The interface includes a sidebar with navigation options like Dashboard, Multicloud Defense, Inventory, Configuration, Policies, Objects, VPN, Events & Monitoring, Analytics, Insights, Change Log, Jobs, Tools & Services, and Settings. The top right shows the user's profile and a "Quick Actions" menu with an "Onboard" button. The bottom of the chat window has a feedback message: "Your feedback helps us improve the AI Assistant." and a "View User Guide to learn more." link.

CX Ticketing



AI Assistant for Cisco Secure Access

Cisco Secure Access AI Assistant Skills

Documentation Summarization

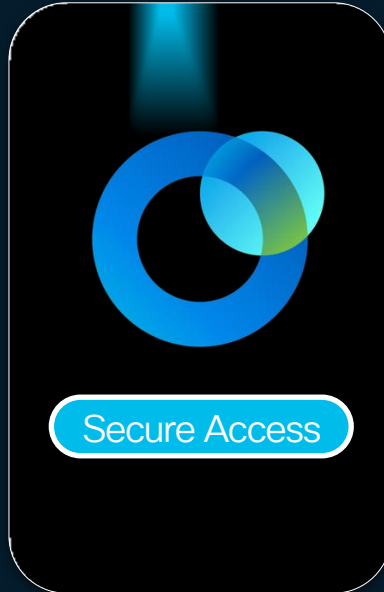
Search Cisco's product docs for clear, actionable, and simplified insights

Policy Rule Creation

Create policies with natural language

Troubleshooting User Access

Automates triaging for access issues



Policy Insights

Enables quick discovery of policies with fast, rich data responses on-demand

Policy Analysis & Optimization

Proactively discover and remediate policy misconfigurations and anomalies

Digital Experience Monitoring

Quick issue research, trend analysis, insights

Documentation

Quick Access to Documentation

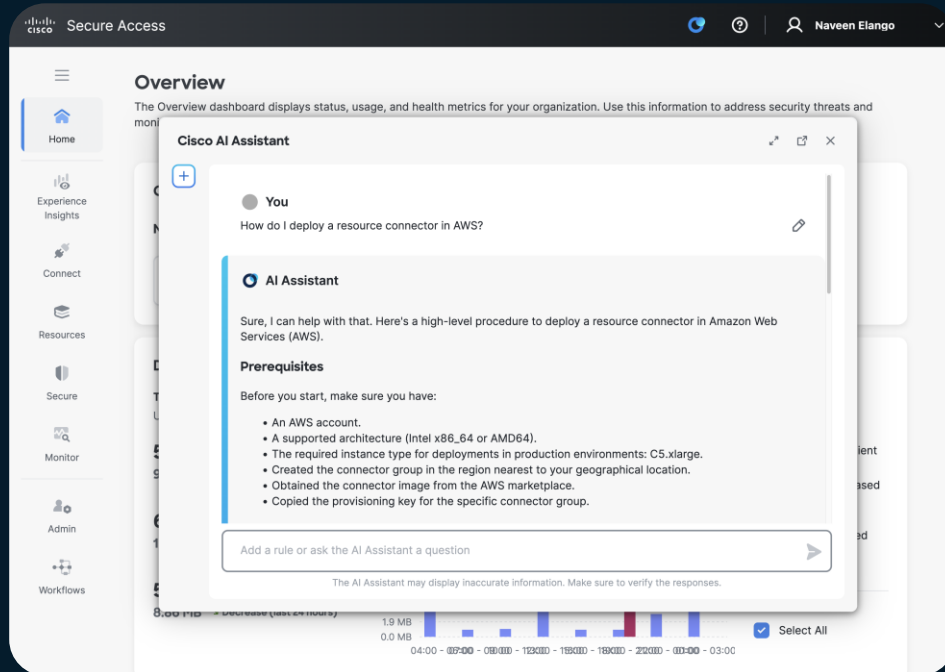
- Find relevant information directly within the dashboard.

Contextual Citations

- Provides citations for clarity and reference.

Example Prompts

- “What are the key capabilities of Experience Insights?”
- “How do I change IPS profiles in Cisco Secure Access?”



Policy Creation

Flexible Rule Creation

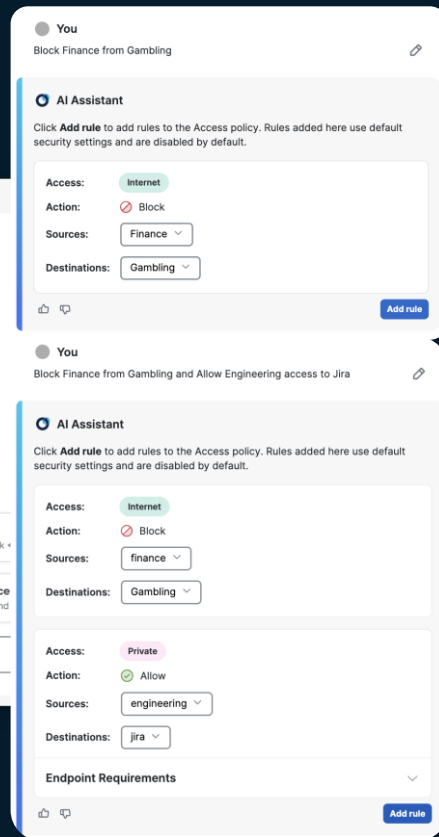
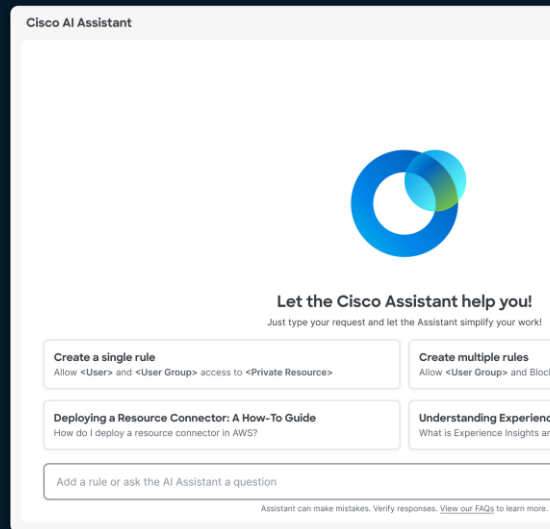
- Set up single or multiple rules at once.

Access Inference

- The assistant automatically identifies the type of access required.

Example Prompts

- “Allow *Lee* access to *Jira*”
- “Block *Finance* access to *gambling sites*”
- “Allow *HR* access to *Workday* and block *Engineering* from *streaming video*”



Troubleshooting

Private App Access Issue

- Resolve access issues to internal applications.

Multi-Agent Orchestration

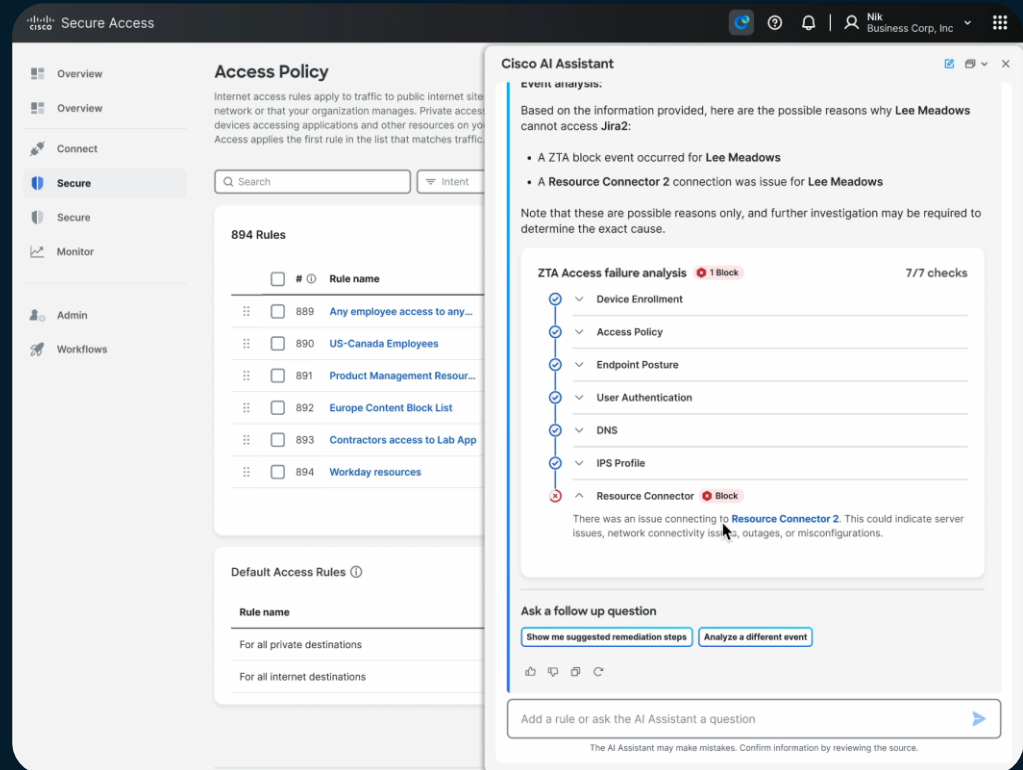
- Coordinate multiple agents to streamline troubleshooting.

Faster Time to Resolution

- Quickly identify and address the root cause of issues.

Example Prompt

- “Why can’t *Lee Parker* access Jira?”



Digital Experience Monitoring

The screenshot displays the Cisco Secure Access AI Assistant interface. At the top, the user is identified as 'Nik Network Administrator'. The main content area is titled 'Experience Insights' and is powered by 'ThousandEyes'. It provides a summary of employee digital experience data and offers a 'Help' link. The interface is divided into three main sections under the 'AI Generated Action Center':

- Latency Alert Summary:** A donut chart shows 109 total devices with latency issues. The breakdown is: 70 devices (90 ms to 100 ms latency), 22 devices (75 ms to 90 ms latency), and 17 devices (68 ms to 90 ms latency). A button labeled 'Investigate latency issues' is present.
- Unhealthy Regions Detected:** A bar chart shows 1850/4500 unhealthy endpoints across four regions: United Kingdom (800), Germany (500), San Jose, CA (290), and Brazil (260). A button labeled 'Review unhealthy region' is present.
- Worst Performing SaaS Applications:** A bar chart shows the performance of three SaaS applications: Monday.com (230), SharePoint (198), and DocuSign (101). A button labeled 'View detailed performance' is present.

A disclaimer at the bottom states: 'The AI Assistant may display inaccurate information. Make sure to verify the responses. View our FAQs to learn more.'

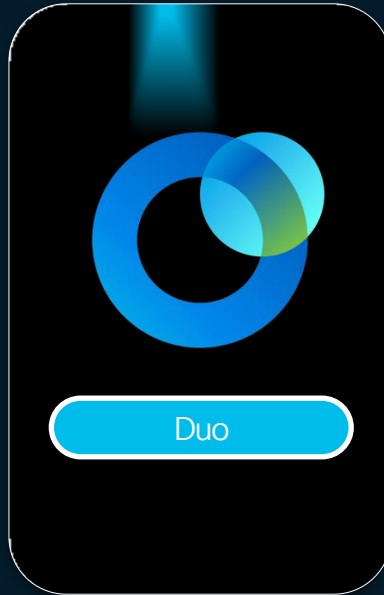
AI Assistant for Cisco Duo



Cisco Duo AI Assistant Skills

Documentation Summarization

Search Cisco's product docs for clear, actionable, and simplified insights



Troubleshooting User Access

Troubleshoots auth issues by looking at auth sequences, policy breakdown, group status, etc.

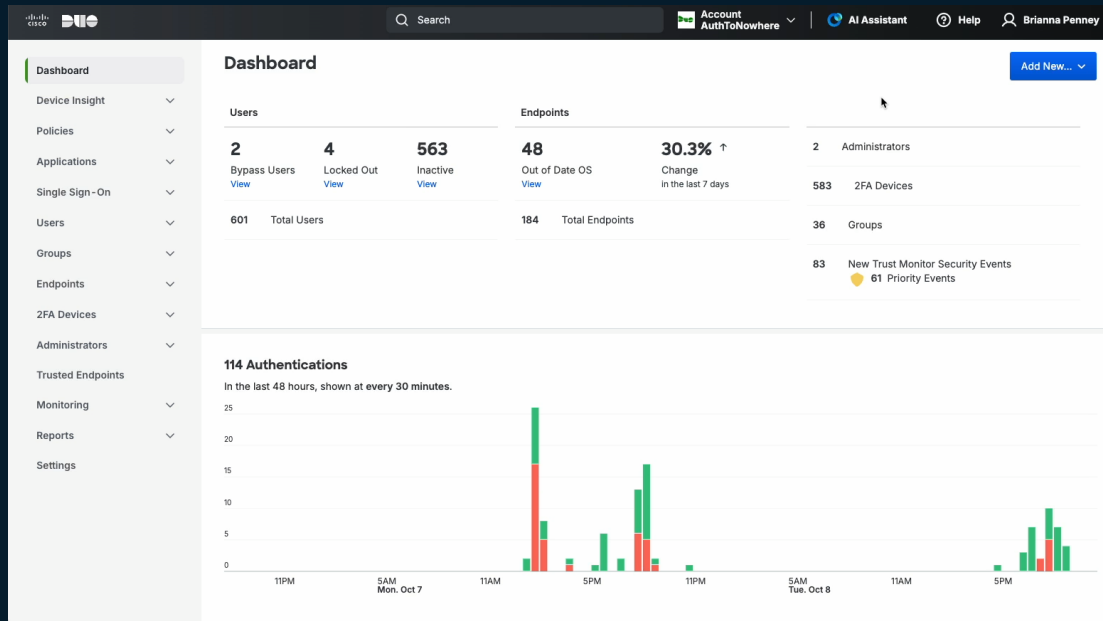
User Access Troubleshooting

Remediating User Access Issues

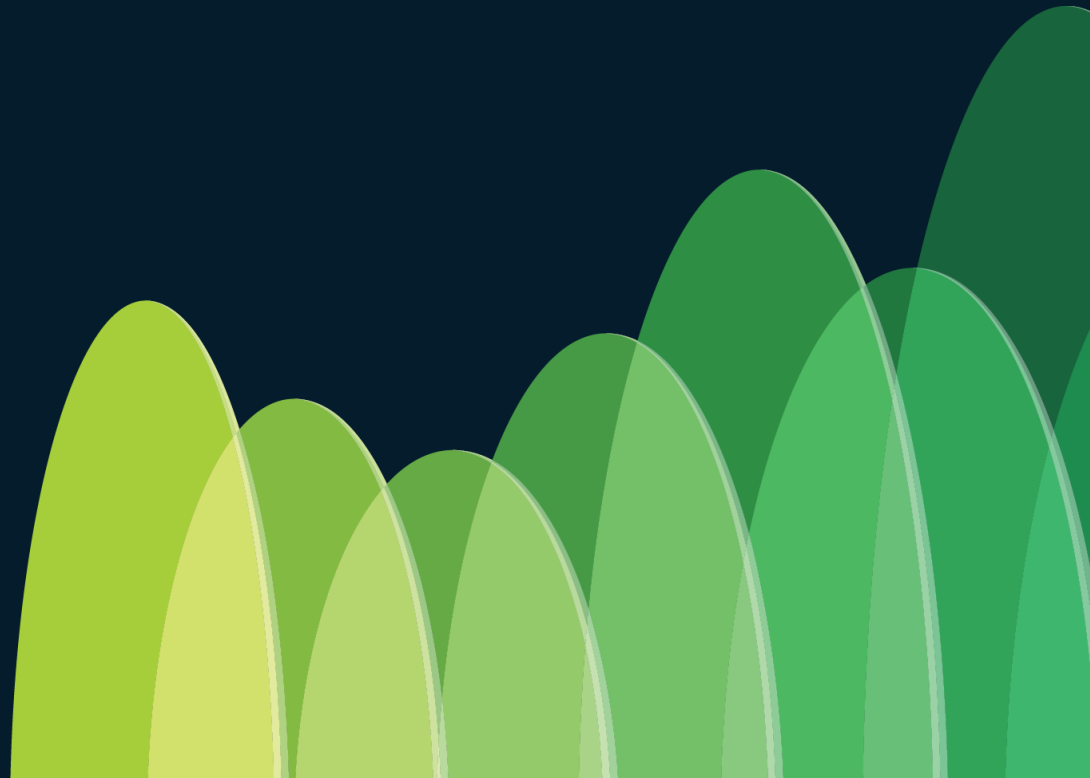
- Assists administrators in identifying why end users are unable to authenticate, including:
 - Authentication sequence analysis
 - Policy breakdowns
 - Group status checks
 - Etc.

Example Prompt

- “Why can’t *cdedmundo* login?”



AI Assistant for Cisco XDR



AI Assisted Threat Event Management

Investigate, prioritize, respond, and recover **from one AI-assisted console**

Command every response and action with **AI-driven automation**

Get confident verdict with **cross-domain telemetry** and **threat intelligence enrichment**

The screenshot shows the Cisco XDR 'Incidents' console. A table of incidents is displayed with columns for 'Status', 'Priority', and 'Name'. The first incident, 'Suspected Malicious URL on ip-192-168-249-115', has a priority score of 780, which is highlighted with a red circle and a mouse cursor. Other incidents include 'Insider Threat Attack Chain for Cisco Demo', 'Confirmed Threat Watchlist Hit on kali', and 'Potential System Process Impersonation on desktop-v8tp7ng'.

Status	Priority	Name
Incident Reported	780	Suspected Malicious URL on ip-192-168-249-115
	1000	Insider Threat Attack Chain for Cisco Demo (dclco-dcloud-rg)
	1000	Confirmed Threat Watchlist Hit on kali
	1000	Potential System Process Impersonation on desktop-v8tp7ng
	1000	Persistent Remote Control Connections on I-07526927/cx7529064
	1000	Confirmed Threat Watchlist Hit on I-03175846/c83ace88
	1000	Demo_AMP_Threat_Audit in group Triage @ 20230329 02:09:27
	624	New Log Sessions (Geographic) on I-07526927/cx7529064
	625	Demo_Threat_Hunting_2 in group Audit @ 20230516 02:16:09
	623	Demo_Threat_Hunting_2 in group Audit @ 20230408 02:16:09
	623	Demo_Threat_Hunting_2 in group Audit @ 20230316 02:16:09
	622	slate in group Endpoint Isolation Group @ 20230512 16:01:43
	622	Demo_Timba in group Triage @ 20230509 02:09:01
	622	Demo_TechCrypt in group Protect @ 20230329 02:17:21

Suspected Malicious URL on ip-192-168-249-115

Priority **780** Status Incident Report...

Reported by **Cisco XDR Analytics (cisco-dcloud-rtp)** 18 hours ago

Unassigned

MITRE

Priority score breakdown

780 | **78** Detection Risk | **10** Asset Value at Risk

Short description

The device communicated with a suspected malicious URL. The alert uses the Suspected Malicious URL observation and requires URL data provided by firewalls via the Cisco Security Analytics and Logging (SAL) integration or Enhanced Netflow.

Cisco XDR AI Assistant Skills

Documentation Summarization

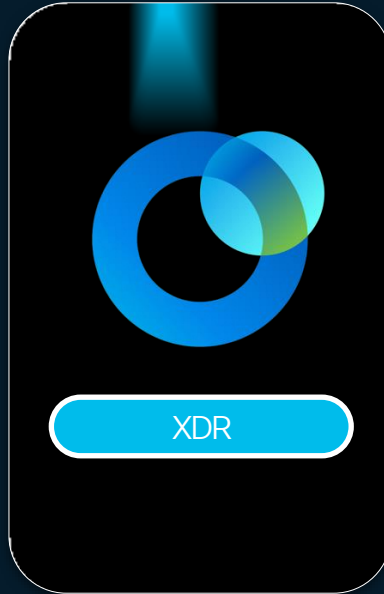
Provides concise incident summary to enable quick understanding of an ongoing incident.

Respond and Remediate

Automate response actions, create Webex War rooms, and generate incident reports

AI-Generated Notes

Automatic generation of incident investigation notes of manual actions for XDR audit logs



Explain and Recommend

Provides recommendations to remediate incidents, thereby reducing response times

Interpret Incidents

Ask natural language questions to rapidly understand an ongoing incident

Preemptive Detection & Response

Augment attack chain detection in XDR with recommended response actions

- Control Center
- Incidents**
- Investigate
- Intelligence
- Automate
- Assets
- Administration

← Incidents

1000 Open

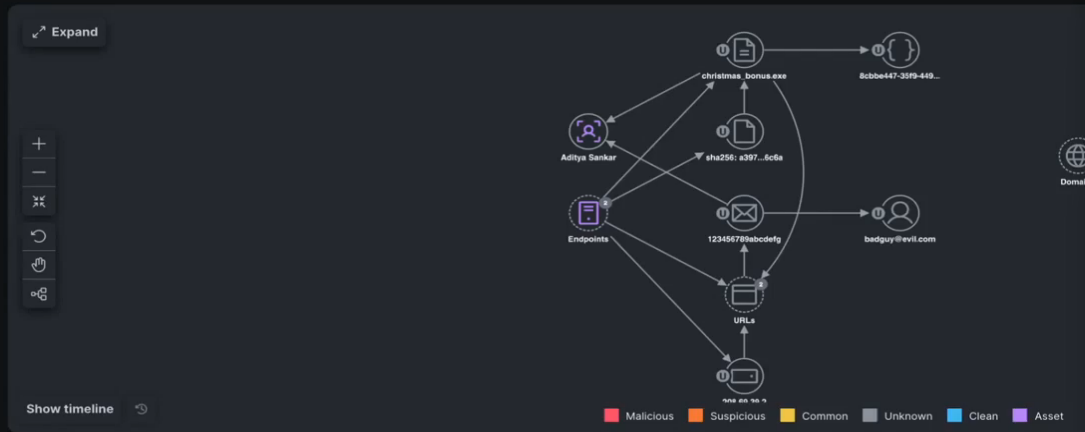
Malware Executed on MY-DEVICE-42 - Incident by Cisco XDR Automation

Reported by Cisco XDR Automation on 10, Oct 2024 @ 12:36 AM IST - 1 Linked Incident

[View detailed description](#)

Created by an Automation workflow.

Overview Detection Response Worklog Report



Show timeline

■ Malicious
 ■ Suspicious
 ■ Common
 ■ Unknown
 ■ Clean
 ■ Asset

3 Assets [View all](#)

TOP ACTIVE

- Endpoint
MY-DEVICE-42 2 events
- Person
Aditya Sankar 1 event
- Endpoint
c1-9300-2-g1-4-win10 1 event

10 Observables [View all](#)

TOP ACTIVE

- Unknown URL
http://www.internetbadguys.com 3 events
- Unknown File Name
christmas_bonus.exe 2 events
- Unknown SHA-256
a3973e2fca3fedb94964ef4c2bc4de3b52fd4e5473f1c705541de... 2 events
- Unknown Email
badguy@evil.com 1 event

Automatic incident assignment to current user and status update to Open successful.

AI Assistant

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.

- How do I respond to an incident?
- How are integrations used in XDR?
- How are incident priority scores calculated?
- How do I trigger an Automation workflow to run?

Ask the AI Assistant a question

[View User Guide to learn more.](#)

AI Assistant for Security Cloud Control



Gain end-to-end visibility from a single screen



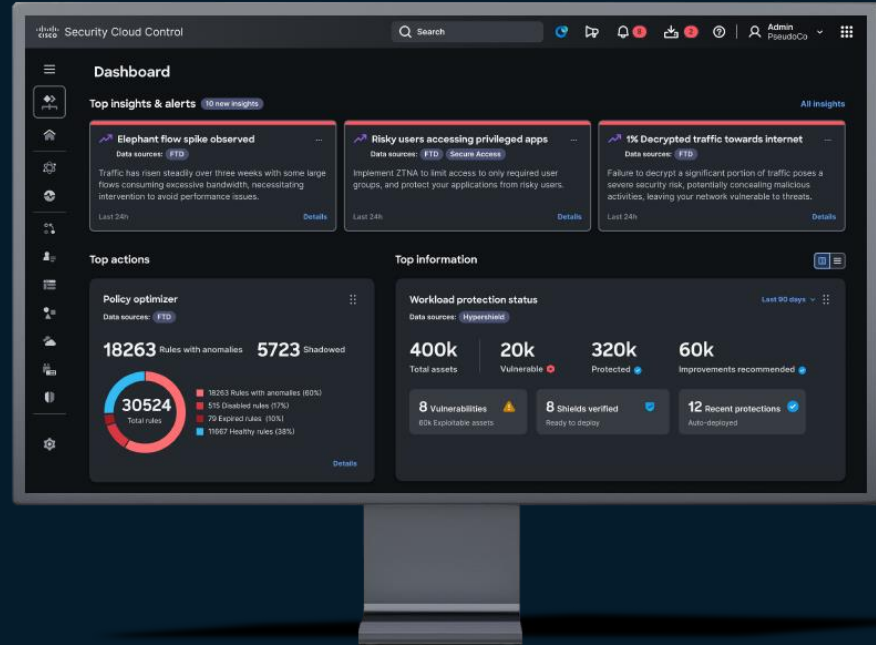
Access comprehensive insights across all security platforms.



Enable prompt issue resolution through a live view of network traffic and security events



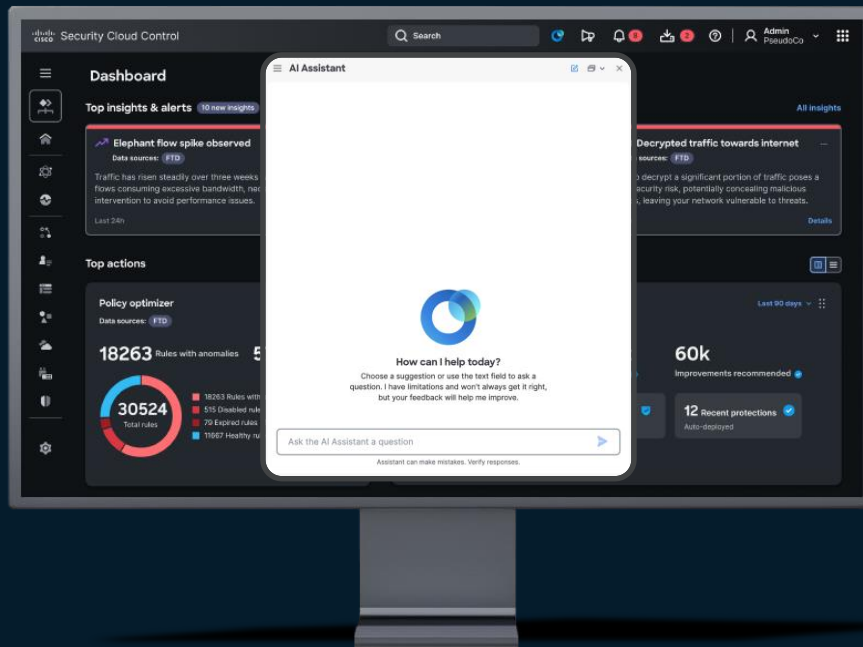
Empower informed decisions with operational insights from network data



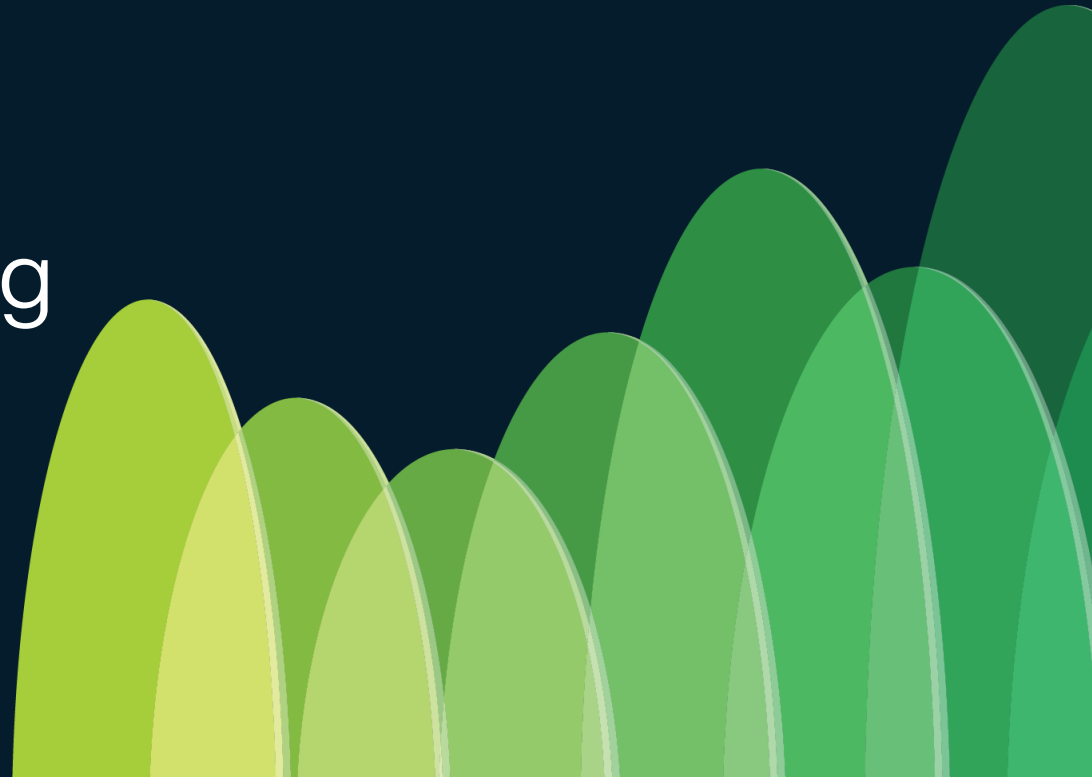
One Security Assistant

SCC AI Assistant interfaces to individual Assistants on various platform.

Seamless integration with Firewall, Secure Access, and Hypershield AI Assistants (more to come)

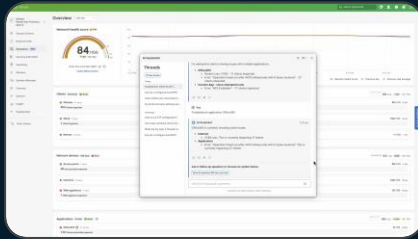


AI Assistants for Cisco Networking



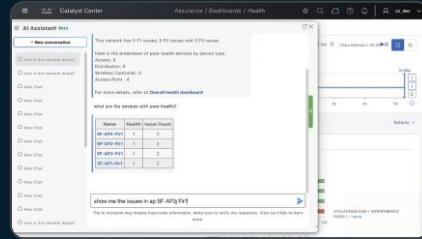
Cisco Networking's Suite of AI Assistants

Meraki



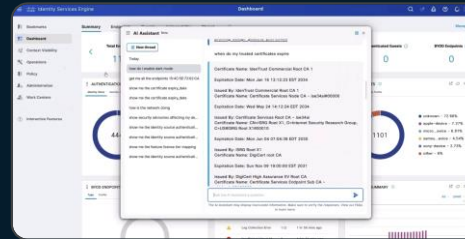
Cloud-managed networking with security, visibility, and device control.

Catalyst Center



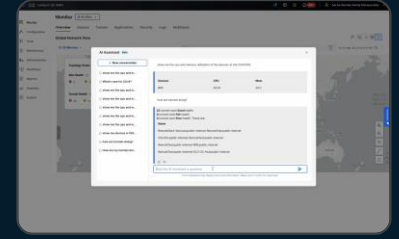
On-prem network management for automation, policy, security & assurance.

Identity Service Engine



Enforces identity-based access policies, ensuring secure network access and compliance

SD-WAN



Optimizes WAN traffic and security across remote sites.

Cisco Networking AI Assistant Skills

Documentation Summarization

Summarize key documentation and best practices for quick guidance.

Troubleshooting

Diagnose issues and recommend solutions based on network data.

Impact Analysis & Optimization

Assess impacts of changes and optimize for efficiency.



Networking

Network Visibility

Monitor real-time and historical network health and performance.

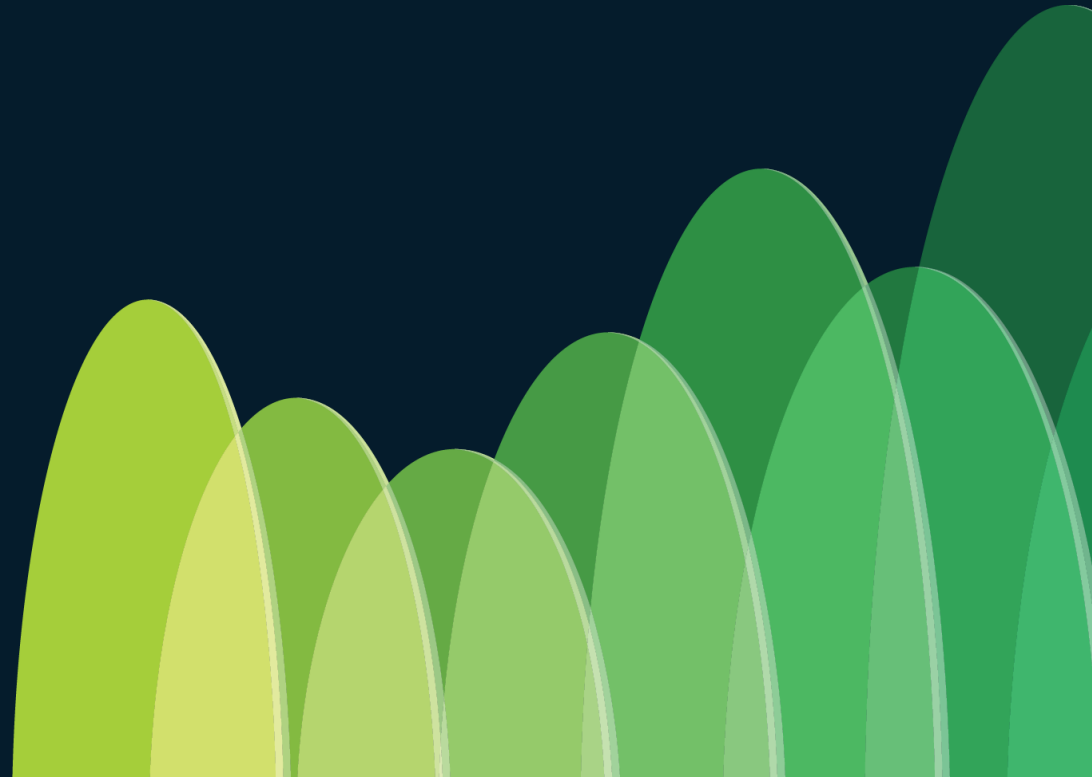
Configuration & Migration

Assist with feature setup and migration readiness.

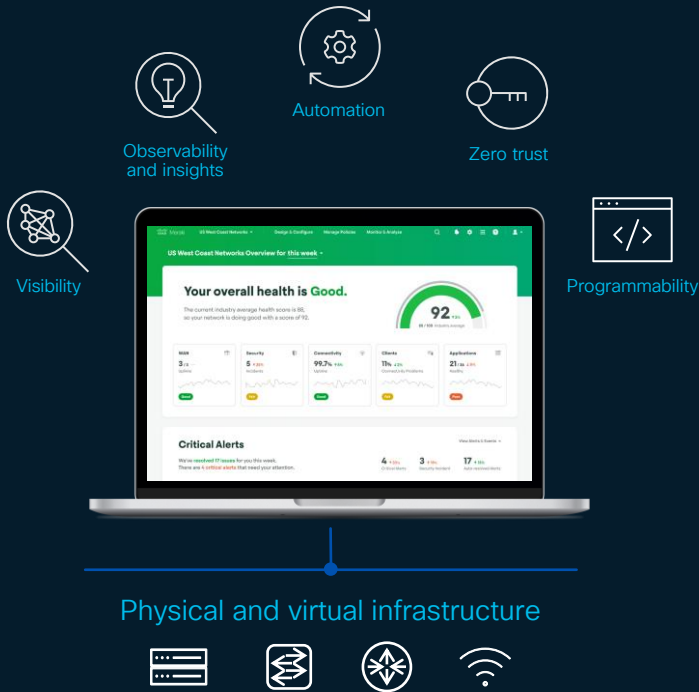
Support & Case Management

Streamline TAC support and automate case management tasks.

AI Assistant for Meraki



Cisco Meraki use cases and personas



NetOps Automation and workflows to streamline and simplify complex or repetitive tasks

AIOps AI/ML to ensure consistent performance and optimal user experience

SecOps Complete zero trust solution for flexible segmentation and policy enforcement including AI-driven device identification

DevOps APIs combined with playbooks for managing networks at scale and numerous out-of-the-box integrations

- Network Meraki San Francisco SFO12
- Secure Connect
- Network-wide
- Assurance **New**
- Security & SD-WAN
- Switching
- Wireless
- Systems Manager
- Cameras
- Sensors
- Insight
- Organization
- Find in Menu

Overview Last day

Your network health score is **Fair** 📉
 Some end clients are unable to access their applications and have moderate interruption from the network.



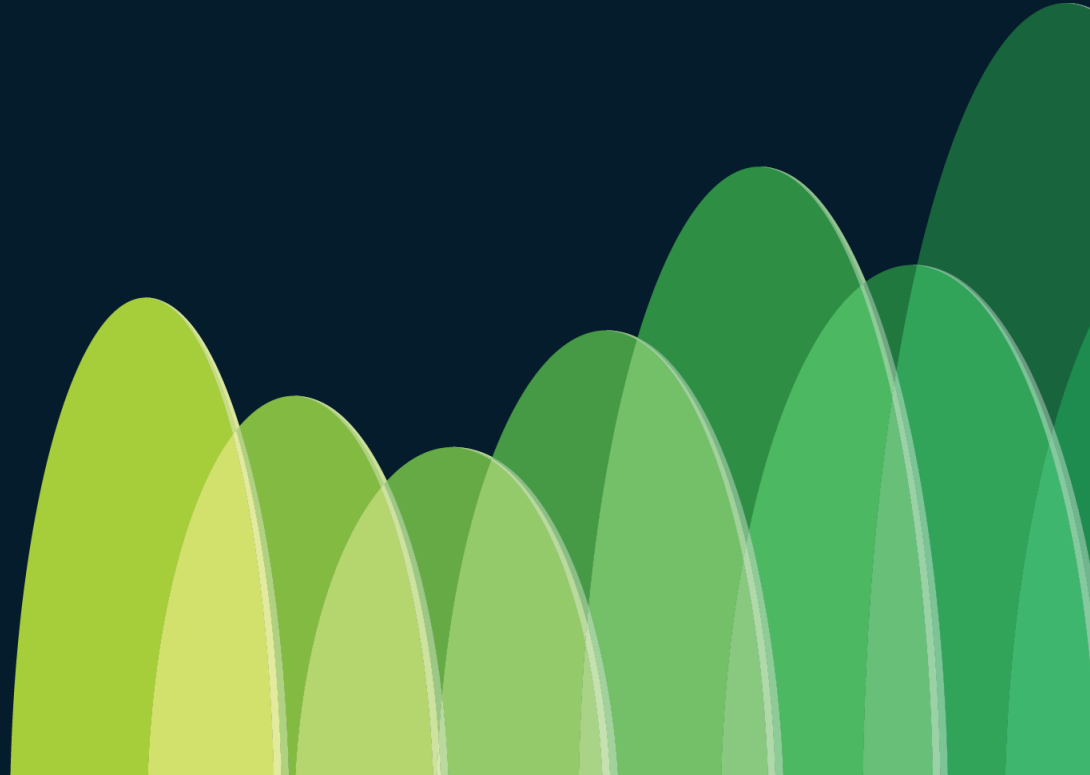
Clients 2029 total Fair 86/100 -1 pts last day

Wireless 6 issues	86/100 -8 pts
540 Clients impacted	
Remote 0 issues	—/100 — pts
Wired 2 issues	100/100 +0 pts
24 Clients impacted	

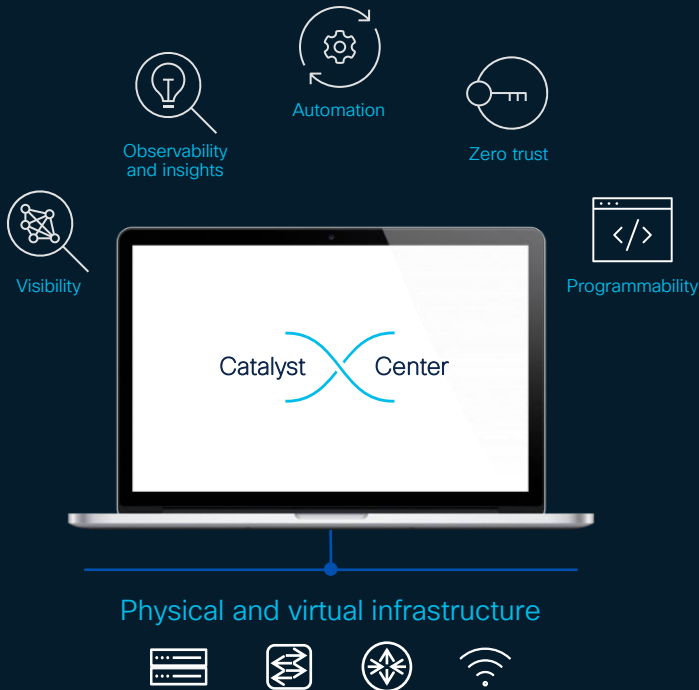
Applications 11 total Good 99/100 0 pts last day

Salesforce - meraki	98/100 +0 pts
meraki.enterprise.slack.com	98/100 +0 pts
Webex - cisco	99/100 +0 pts

AI Assistant for Catalyst Center



Catalyst Center use cases and personas



NetOps

Automation and workflows to streamline and simplify complex or repetitive tasks

AIOps

AI/ML to ensure consistent performance and optimal user experience

SecOps

Complete zero trust solution for flexible segmentation and policy enforcement including AI-driven device identification

DevOps

APIs combined with playbooks for managing networks at scale and numerous out-of-the-box integrations



AI Assistant Beta



+ New conversation

05/31/24, 12:56 AM

New Chat

how is the network doing?

New Chat

New Chat

New Chat

New Chat

New Chat

New Chat

New Chat

New Chat

New Chat

New Chat

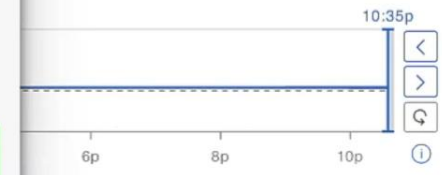
how is the network doing?

Ask the AIAssistant a question



The AI Assistant may display inaccurate information. Make sure to verify the responses. View our FAQs to learn more.

5 PM | Data Refresh in 05:00

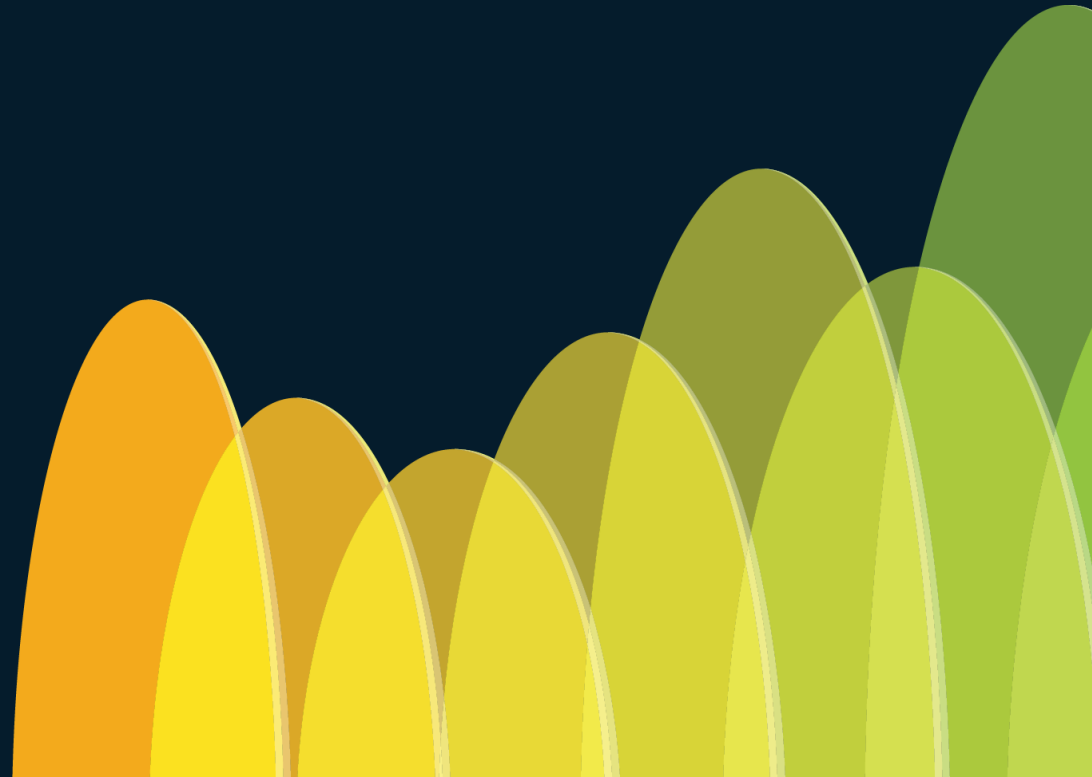


Actions

UTILIZATION FAIR | INTERFERENCE POOR | 1 more

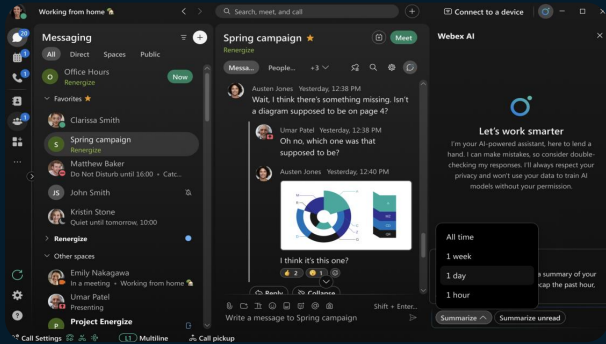
100

AI Assistant for Collaboration

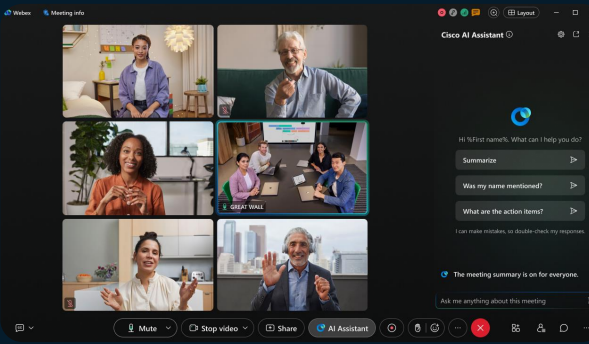


Cisco Webex's Suite of AI Assistants

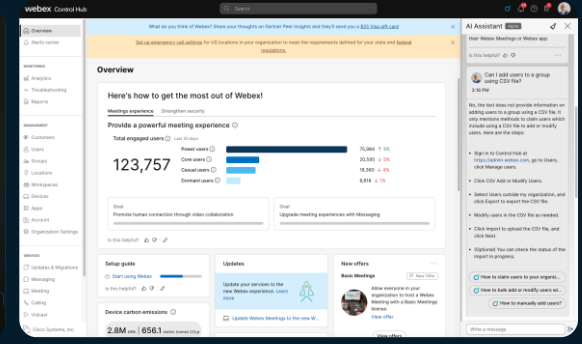
Teams



Meetings



Control Hub



Collaboration workspace with chat, file sharing, and video meetings

High-quality video conferencing for virtual meetings and webinars.

Centralized management for Webex services, users, and security

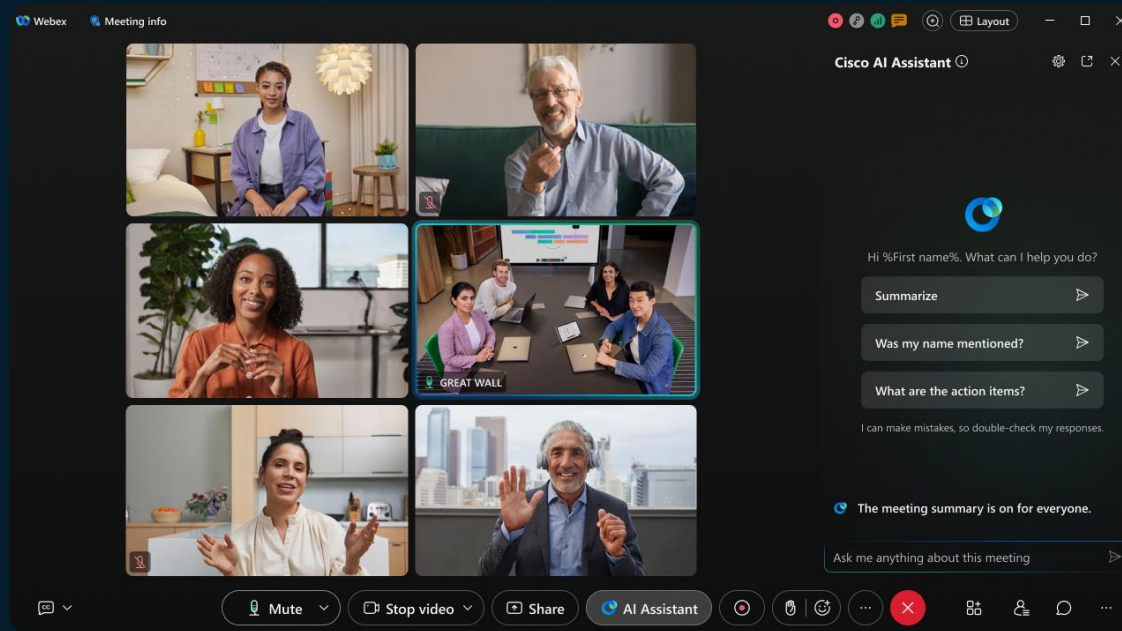
Conversation Catch up & Summary

- AI summarizes entire spaces, threads and messages for you.
- Get to the point and stay productive

The screenshot displays the Microsoft Teams interface. On the left, the 'Messaging' sidebar shows a list of spaces, including 'Office Hours', 'Spring campaign', and 'Project Energize'. The main window shows a conversation in the 'Spring campaign' space. The conversation history includes a message from Austen Jones asking about a missing diagram and a response from Umar Patel pointing to a specific diagram. Below the messages, there is a 'Summarize' button and a dropdown menu with options for 'All time', '1 week', '1 day', and '1 hour'. The 'Webex AI' panel on the right provides a brief introduction to the AI assistant.

AI Assistant in Meetings

- Ask AI about this meeting!
- Catch up on what you missed or if your name was mentioned.
- Save the summary without having to record and more!



Control Hub

A single-pane-of-glass management

Webex Control Hub



Webex Contact Center



Webex Suite



Cisco Devices



Meetings



Messaging



Calling



Webinars



Events



Whiteboarding



Polling



Video Messaging

Cisco Control Hub AI Assistant Skills

Setup and Configure

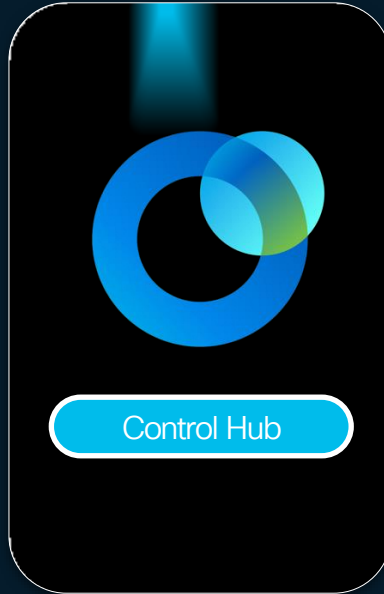
Easily configure settings and manage setups. Ask “How do I...?” or request, “Do it for me.”

Troubleshooting

Receive proactive notifications of issues, along with root cause analysis.

Contextual Q&A with Recall

Get answers with context-based memory for accurate, relevant responses.



Analytics and Insights

Query your data for valuable insights and metrics to enhance decision-making.

Converse with Reports

Engage with your reports seamlessly for enhanced, conversational insights.

Smart Search with AI

Leverage AI-driven search for faster, smarter information retrieval.



Hi there.

I'm Cisco AI Assistant. I can guide you through Control Hub and help with admin tasks. I can make mistakes, so consider double-checking my responses. I'll always respect your privacy and won't use your data to train AI models without your permission.

How do I add new users?

What are the benefits of SSO?

How do I enable transcription?

Write a message to the Cisco AI Assistant



AI assistant may provide inaccurate information. Please verify answers and check sources.

Cisco Unified AI Assistant

CISCO *Live!*



AI Assistants Integrated Across Cisco



Security

Firewall, Secure Access, XDR, Hypershield, Duo



Networking

Meraki, Catalyst Center, ISE, Catalyst SD-WAN



Observability

Splunk Enterprise Security, Splunk Observability, Splunk Enterprise



Collaboration

Webex Meeting, Webex Teams, Webex Control Hub

Unified AI Assistant Increases Productivity

Documentation
Summarization

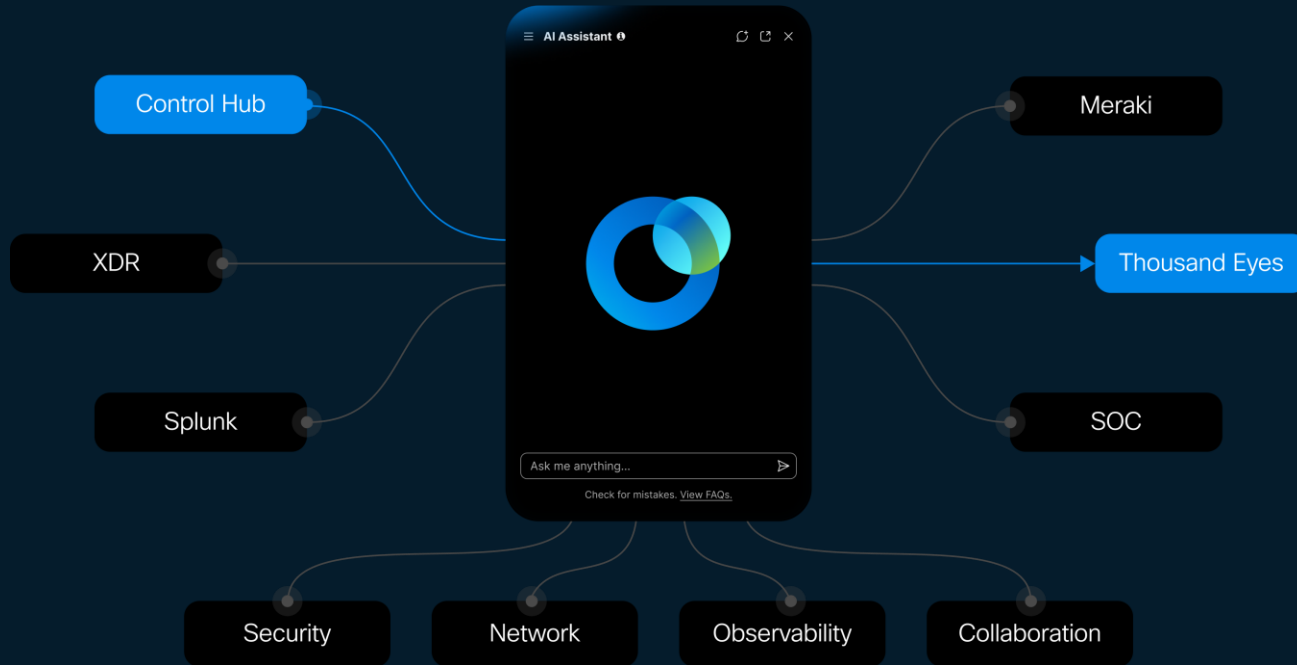
Troubleshooting
& Visibility

Configuration

Recommendation
& Optimization

Unifying Cisco AI Assistants

Bring “Skills” from across Cisco to 10x customer experience



Unified AI Assistant introduces “Composite” Skills

Simple Skills

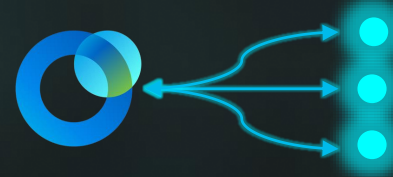
- **Definition:** Insights and actions taken for a single platform at a time.
- **Example:** Checking the client's health on Meraki.



Individual AI Assistant Skills for One Platform

Composite Skills

- **Definition:** Combines intelligence across multiple products for enriched insights to accelerate RCA action.
- **Example:** Correlating a poor-performing Meraki client with XDR, Firewall, & ThousandEyes data for cross-domain context.

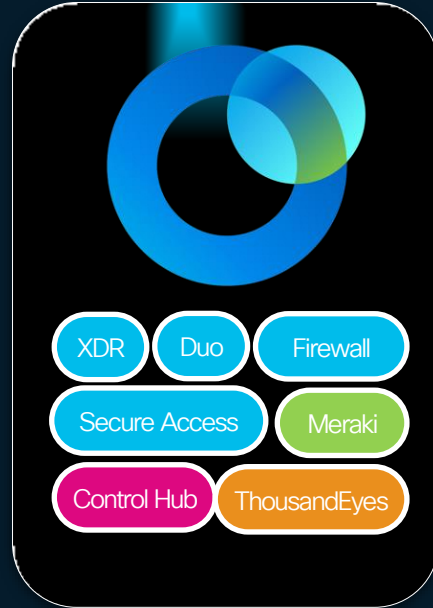


Unified AI Assistant Skills for Many Platforms

Key Composite Skill Use Cases

**Multi-Source Docs
Summarization**
All Platforms

**Cross-Platform Correlation
for Threat Investigation**
XDR + Any Other Platform

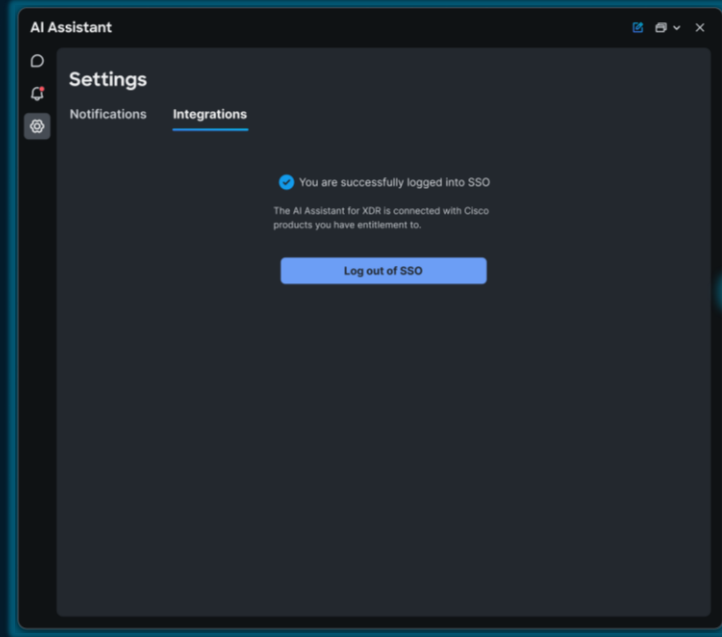


**Cross-Platform Correlation
for Troubleshooting**
Any Platform + Any Other Platform

**Cross-Platform Correlation
for Threat Mitigation**
XDR + Any Other Platform

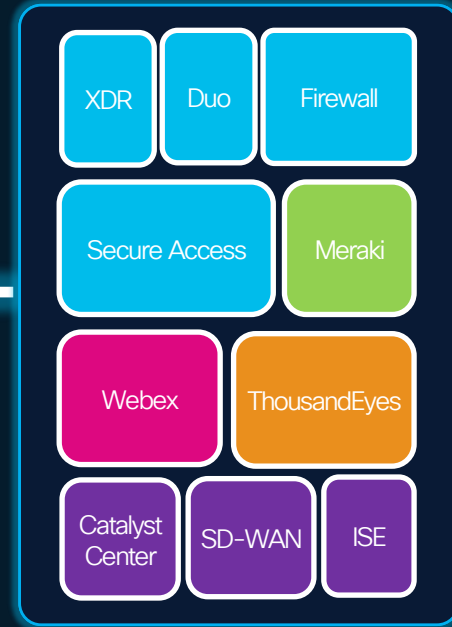
Connect Cisco's AI Assistant to All Platforms

Log into SSO in AI Assistant Settings

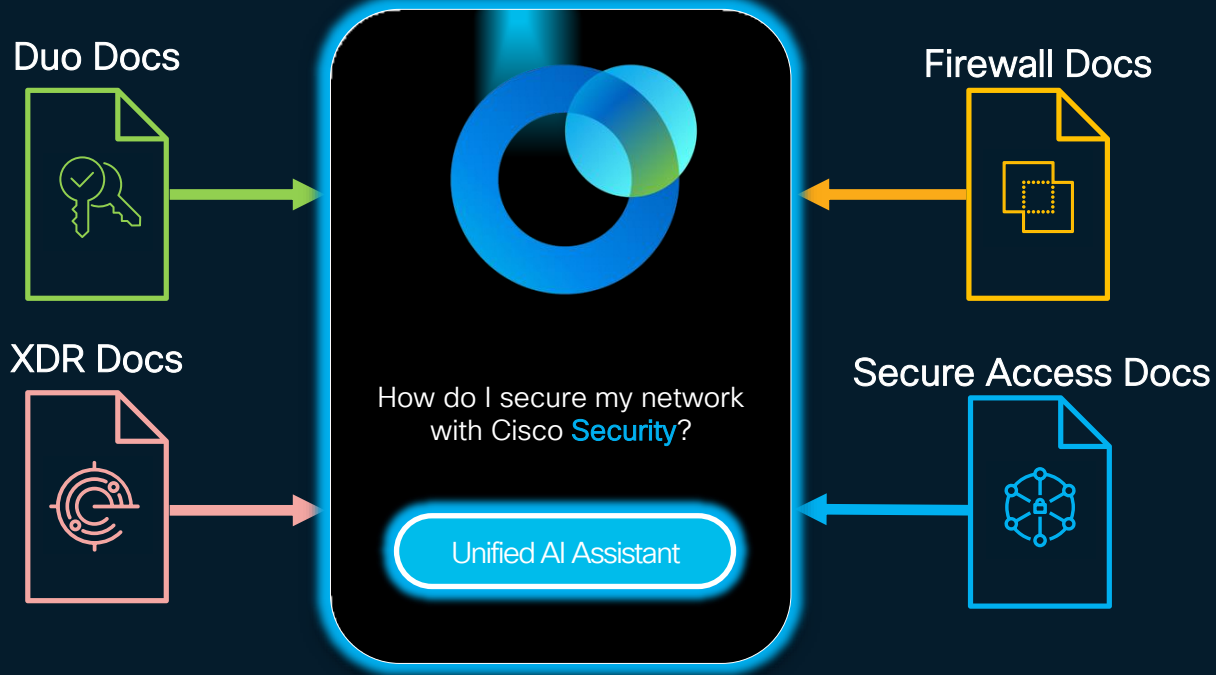


SSO

User's Platforms



Seamless Knowledge Access Across Cisco Products



Cross-Platform Troubleshooting is Complex



Integrations Are Seldom Comprehensive

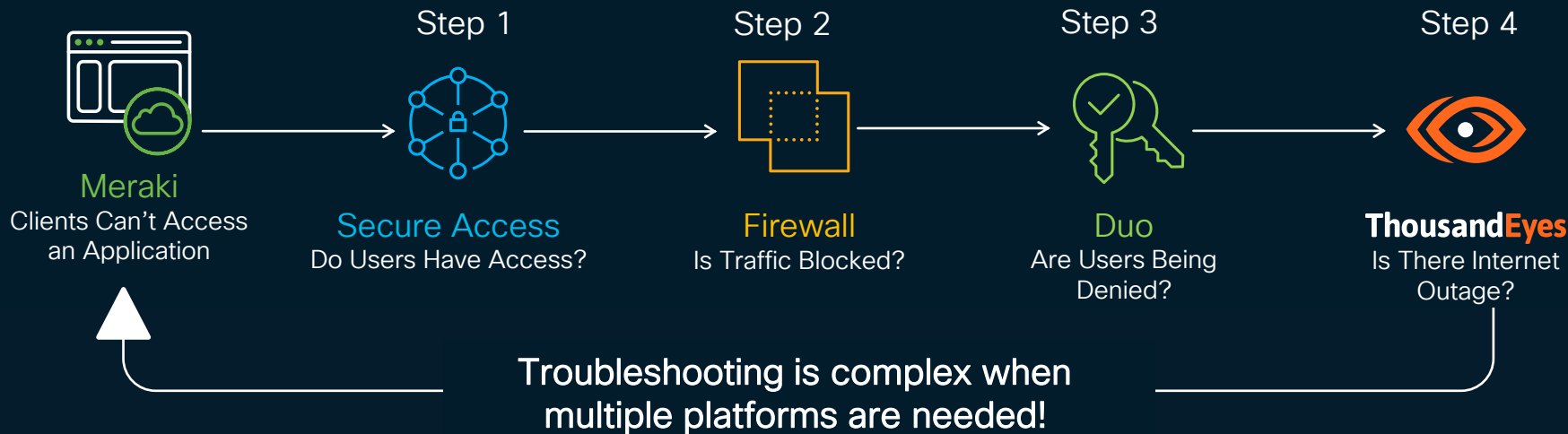
- Cisco platforms often only have basic integrations with each other.
- Users must manually correlate data across platforms for troubleshooting.



Troubleshooting is Time-consuming

- It can require multiple teams & tickets, hours to days to resolve.
- Example: Poor Webex experience could require Meraki, ThousandEyes, & Firewall teams.

Troubleshooting Clients, Devices, & Apps Often Requires Data From Multiple Platforms



Troubleshooting with the Unified AI Assistant

Issue Identified

AI Assistant 11:05 am
Severe warning
Degraded connectivity for user Chuck Robbins detected via **Snack Control Hub**.
Webex service status has been checked, and all statuses are up and running.

Would you like to raise a ticket?

You
Yes, raise ticket.

AI Assistant 11:06 am
Ticket #7078 has been raised.

View client network details via **Meraki**?

You
Yes, view client details.

Ask the AI Assistant a question

Assistant can make mistakes. Verify responses.

Network Assessed

AI Assistant 11:06 am
The following is your client's connection topology queried from **Meraki**.
No Wi-Fi nor switching issues have been detected.

Check Network (via Meraki) - WiFi (via Meraki) - Access Switch - Webx Appliance

Check WAN and Internet status via **ThousandEyes**?

You
Yes, check WAN and Internet status via **ThousandEyes**.

Ask the AI Assistant a question

Assistant can make mistakes. Verify responses.

WAN Analyzed

AI Assistant 11:07 am
ThousandEyes observes spikes in WAN latency and Webex app response time.

WAN Appliance - Webex Application

Run **Firewall** diagnostics via **Snack**?

You
Yes, run **Firewall** diagnostics via **Snack**.

Ask the AI Assistant a question

Assistant can make mistakes. Verify responses.

Issue Resolved!

AI Assistant 11:07 am
Snack ingested **Firewall** logs shows that policy "new-rule-block" is blocking the UDP port.
Updating the firewall policy will resolve this issue.

What would you like to do?

You
Update the firewall policy

AI Assistant 11:08 am
Policy "new-rule-block" has been adjusted to allow traffic through the UDP port.
The issue has been resolved!

Can I help you with anything else?

Ask the AI Assistant a question

Assistant can make mistakes. Verify responses.



Accelerate Troubleshooting with Cross-Platform Insights

Client has an issue accessing an app

The image shows two overlapping screenshots. On the left is the Meraki dashboard for 'Sam's MacBook Pro', displaying status (Online), user information, device type (Apple), and usage graphs. On the right is the 'AI Assistant' interface, which provides a cross-platform summary of data from Duo, Firewall, and XDR. The summary shows 3 XDR incidents (33 blocked), 100 Firewall events (5 denied), and 8 Duo MFA attempts (5 denied). A white arrow labeled 'Relevant Data' points from the AI Assistant interface towards the 'User's Platforms' box on the right.

Platform	Count	Details
XDR Incidents	3	33 Blocked
Firewall events	100	5 Denied
Duo MFA attempts	8	5 Denied

User's Platforms



Accelerate Threat Investigations with Cross-Platform Insights

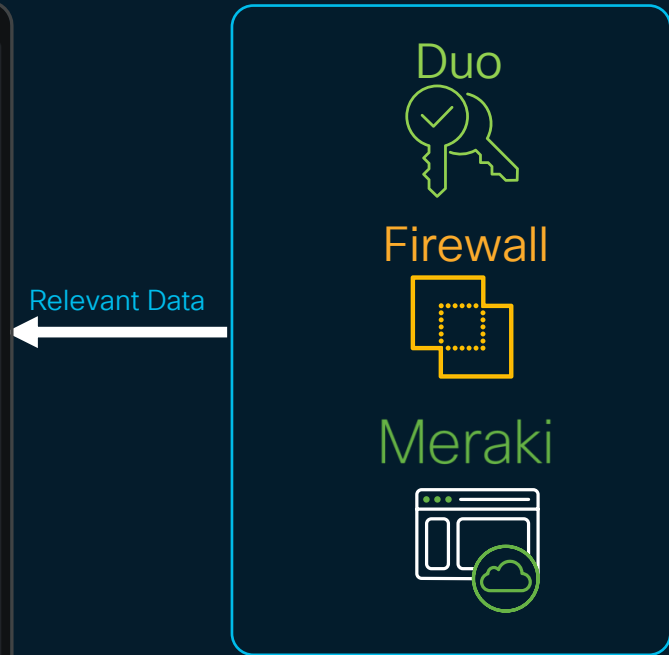
Compromised Client Discovered on XDR

User's Platforms

The screenshot shows the Cisco XDR interface with an incident titled "Ransomware Detected on Employee-Laptop-123". The AI Assistant window provides a "Severe warning" and a "Cross-platform summary" of suspicious activity. The summary includes data from Duo (8 MFA attempts, 5 suspicious), Firewall (100 events, 33 suspicious), and Meraki (Wireless connection, AP-03-THIRD-FLR, CorpNet SSID).

Platform	Category	Count	Status
Duo	MFA attempts	8	5 Suspicious
Firewall	Firewall events	100	33 Suspicious

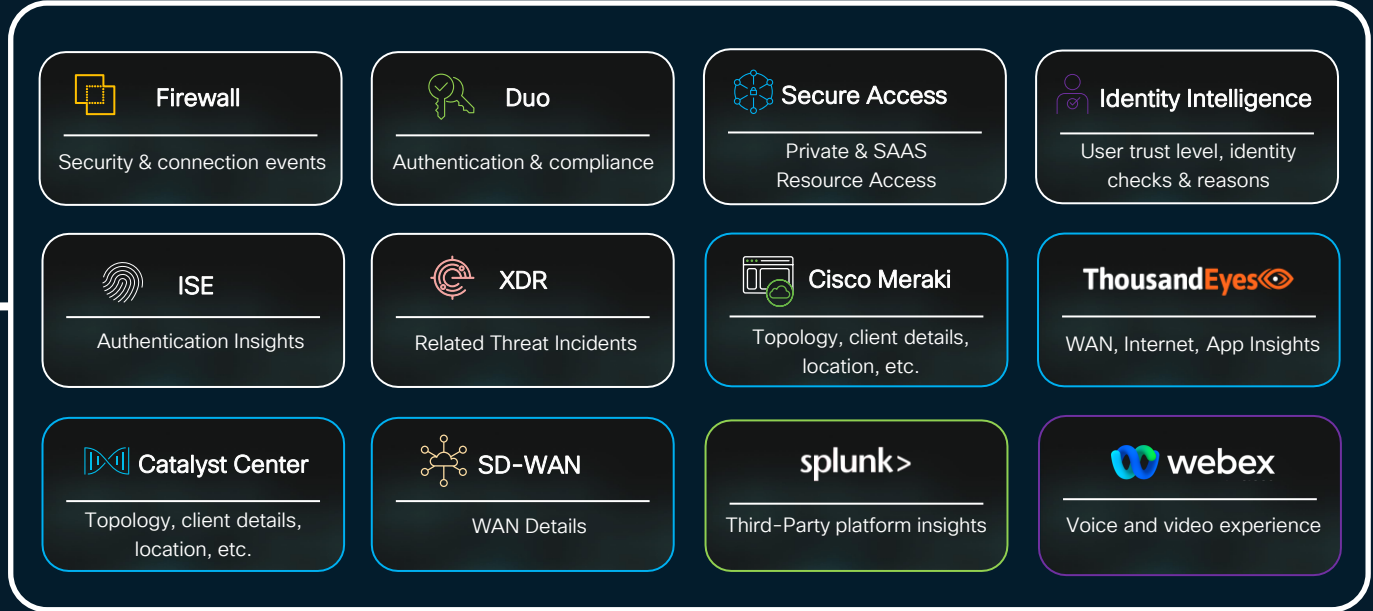
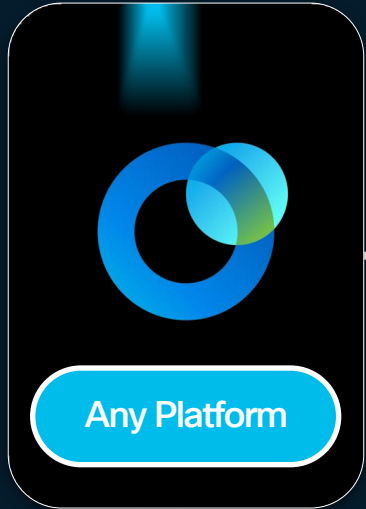
Meraki details include: Connection type: Wireless, Connected device: AP-03-THIRD-FLR, SSID: CorpNet.



Correlate Data Across All Platforms

All Platforms

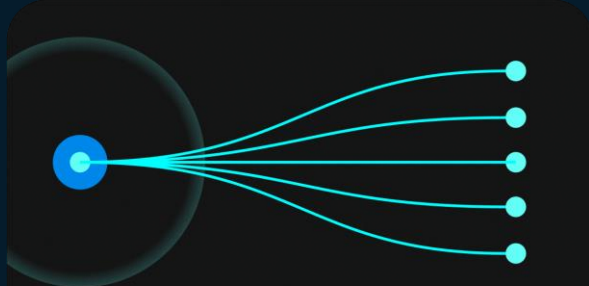
Originating Platform



Conclusion

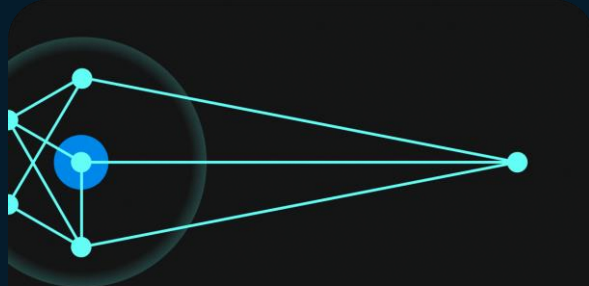


Benefits of the Unified AI Assistant




One assistant, many skills

Each Cisco product enhances the Unified AI Assistant with additional “simple” skills to troubleshoot issues.



Compounding value

Combines cross-platform ‘simple’ skills into ‘composite’ skills—more Cisco products mean exponentially richer context and smarter recommendations.



Accelerated resolution

Troubleshooting is consuming, but the AI Assistant enables RCA in minutes by correlating cross-domain insights!

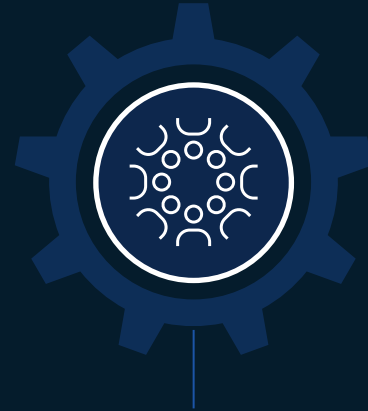
Better User Experience & Productivity



Security



Networking



Collaboration

Webex App

Questions?

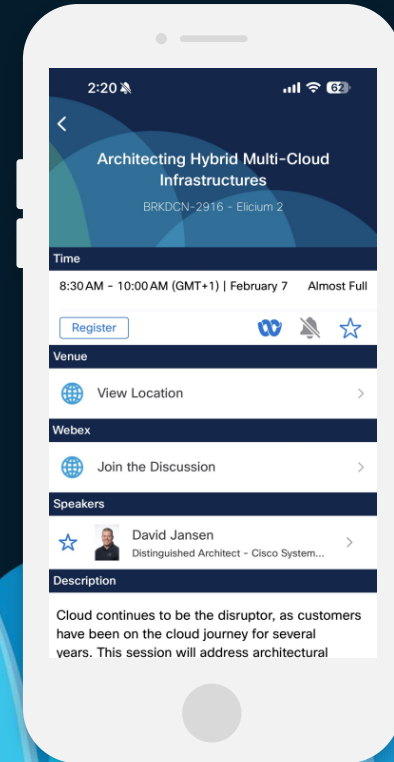
Use the Webex app to chat with the speaker after the session

How

- 1 Find this session in the Cisco Events 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 February 28, 2025.

CISCO *Live!*



Fill Out Your Session Surveys



Participants who fill out a minimum of 4 session surveys and the overall event survey will get a unique Cisco Live t-shirt.

(from 11:30 on Thursday, while supplies last)



All surveys can be taken in the Cisco Events mobile app or by logging in to the Session Catalog and clicking the 'Participant Dashboard'



Content Catalog

Continue your education

- Visit the Cisco Showcase for related demos
- Click the “join the discussion” button for this session on the Cisco Events Mobile app to ask any questions
- Visit the On-Demand Library for more sessions at ciscolive.com/on-demand. Sessions from this event will be available from March 3.



Thank you

CISCO *Live!*

CISCO *Live!*

GO BEYOND

A series of overlapping, vertically-oriented ovals in various shades of blue, ranging from light to dark, positioned on the right side of the image.