

AI Driven Operations and Self-Healing Cisco Secure Access

CISCO Live !

Esra Dumanli
Sr. Product Manager

Cisco Webex App

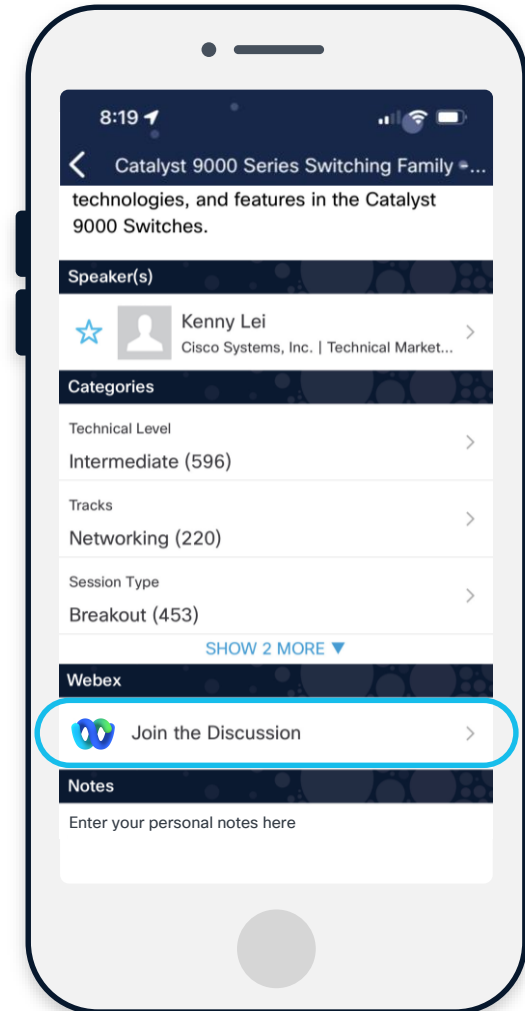
Questions?

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

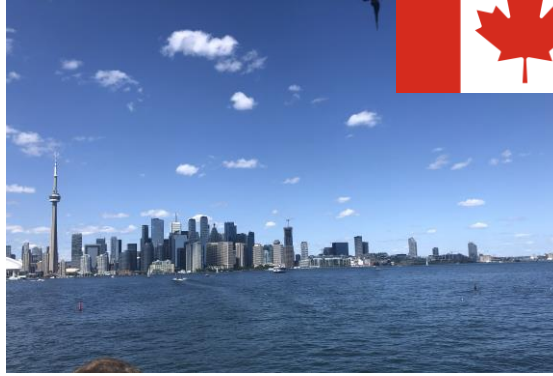
Webex spaces will be moderated by the speaker until June 13, 2025.



Agenda

- 01 Observability Challenges**
- 02 Cisco Secure Access Overview**
- 03 Experience Insights**
- 04 Agentic AI**
- 05 Self Healing Secure Access**

Introduction



20+ years of experience in technology development and management

User centered product development champion



Observability Challenges

It Is A New Era

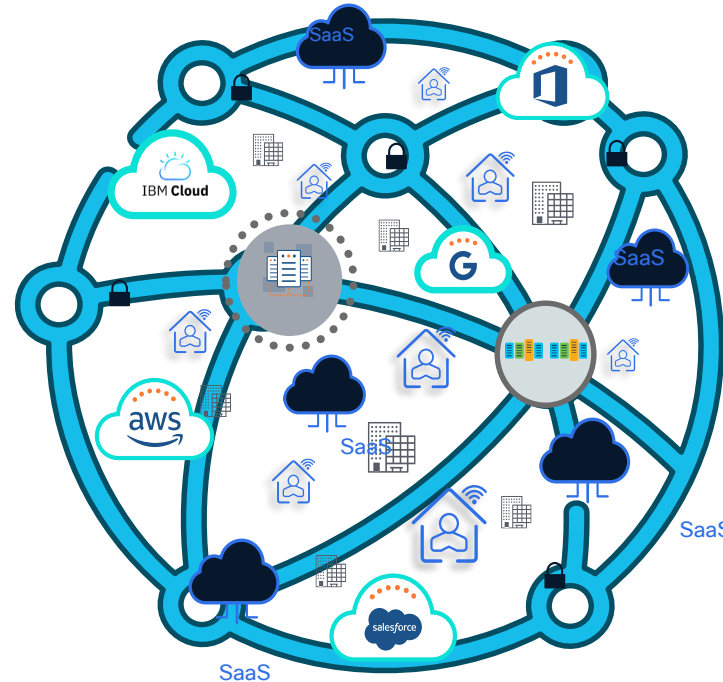
70% of organizations are planning to employ multiple clouds*

Applications

Users

Networks

All
distributed

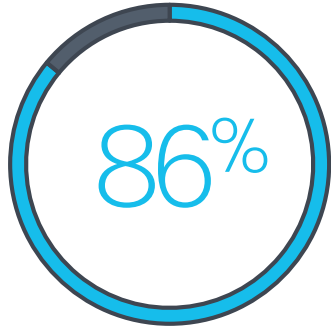


+ AI

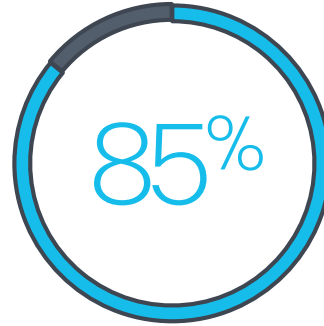
Enterprises don't own the end-to-end infrastructure.

*Source: IDC Future Enterprise Resiliency & Spending Survey Wave 5, IDC, June 2022, Worldwide n=832 weighted

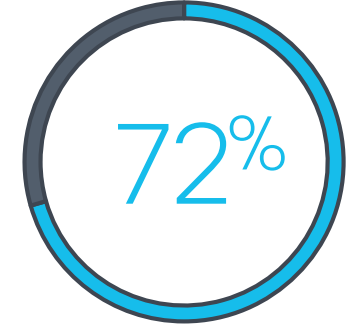
Service observability is top of mind for IT



See having a consistent **operational model** across on-prem, private cloud, public cloud, and SaaS as important



Say they value **simplicity** when it comes to **technology management**



Of users feel digital services should work perfectly

Business Impact of Poor Digital Experience

- 01 Uptime Institute: 2022
Outage Analysis
- 02 IHS: *The Cost of Server,
Application, and
Network Downtime*
- 03 Dun & Bradstreet:
*Assessing the Financial
Cost of Downtime*
- 04 IBM Global Services;
IDC: *DevOps and the
Cost of Downtime*

- Downtime cause loss of business and productivity
- Colocation, operators, providers can be source of major outages
- Frustrated users \$\$\$

\$700B

Annual Business
Loss ¹

Avg downtime
per week ²

1.6 hrs.

Outages ³

70%

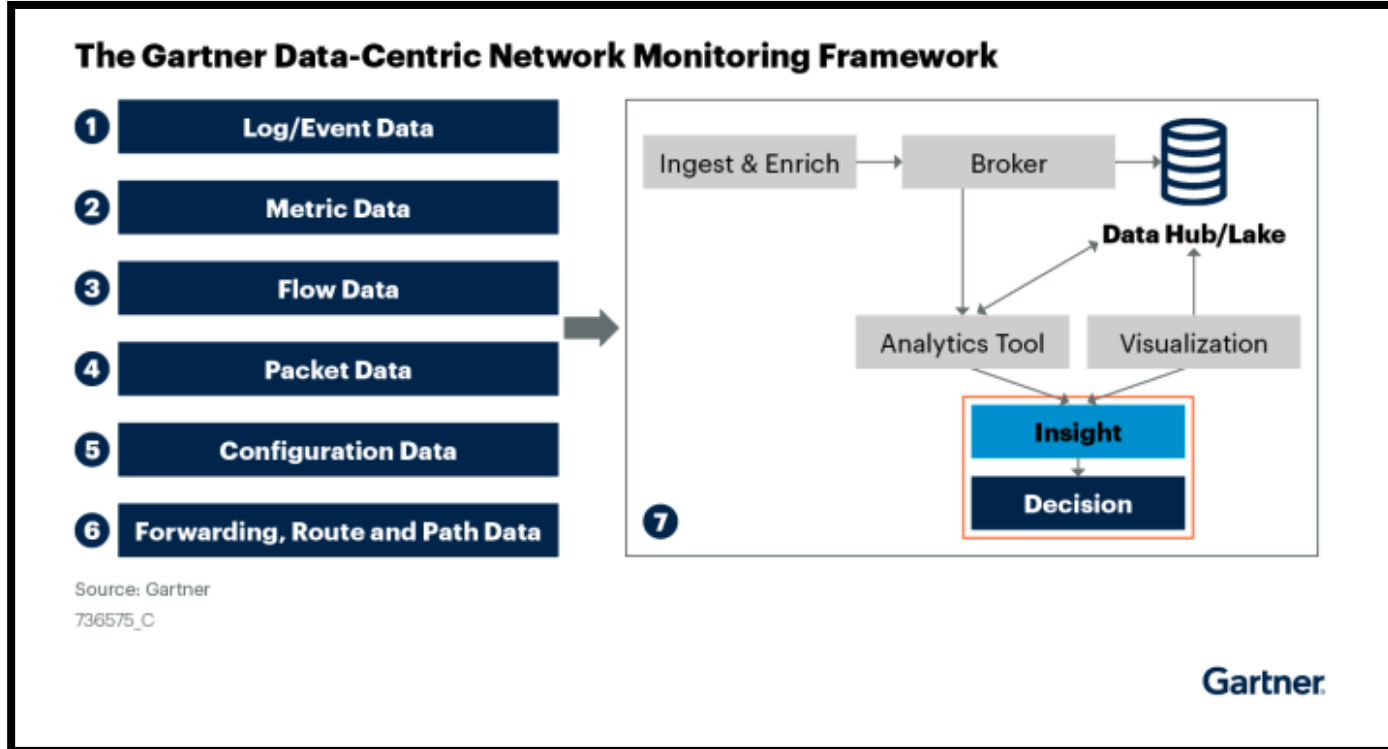
1hr of downtime
for critical app
costs ⁴

\$1M-5M+



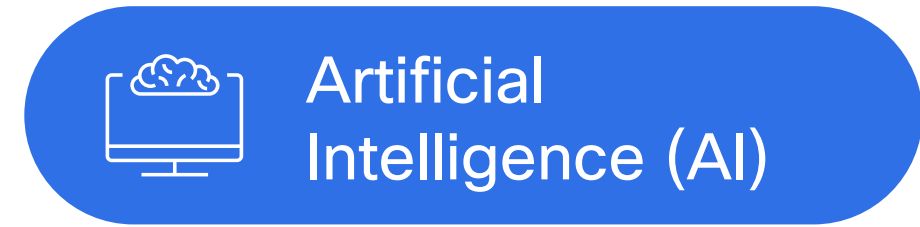
Intelligent Visibility and Control is Crucial

Data Centric Monitoring



- Focus on collection, analysis and visualization
- Collects vast amount of data and process to identify pattern, anomalies, issues
- Primarily reactive with human intervention
- Intelligent analysis with ML
- Can handle large volume of data

How Is AI Different From Regular Algorithms?



Cisco Secure Access Overview

Introducing Cisco Secure Access

Converged cloud-native security grounded in zero trust



Secure Access Service Edge (SASE) Components

Core SSE



Secure Web Gateway (SWG)



Cloud Access Security Broker (CASB) and DLP



Zero Trust Network Access (ZTNA)



Firewall as a Service (FWaaS) and IPS



Cisco delivers the core and more in a single subscription...



DNS Security



Multimode DLP



Advanced Malware protection



Sandbox



Talos Threat Intelligence



VPN as a Service



Digital Experience Monitoring



Remote Browser Isolation

Add-on solutions



SD-WAN



XDR



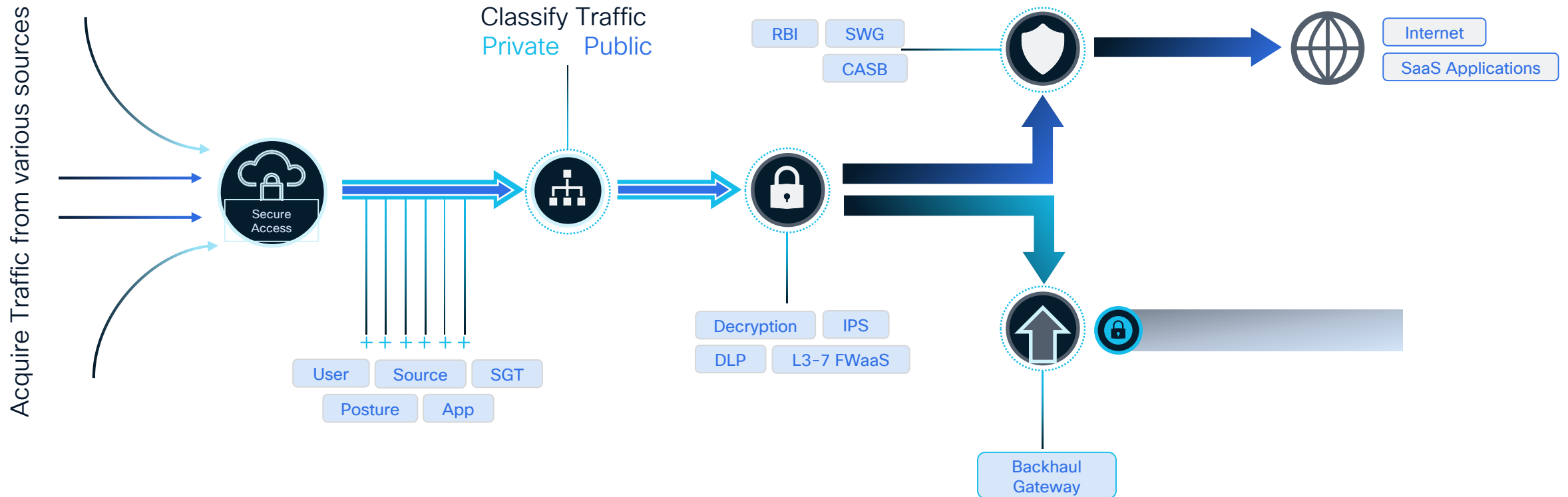
Duo MFA/SSO



CSPM

Unified Cloud Architecture

Universal Traffic Acquisition & Single Data Path

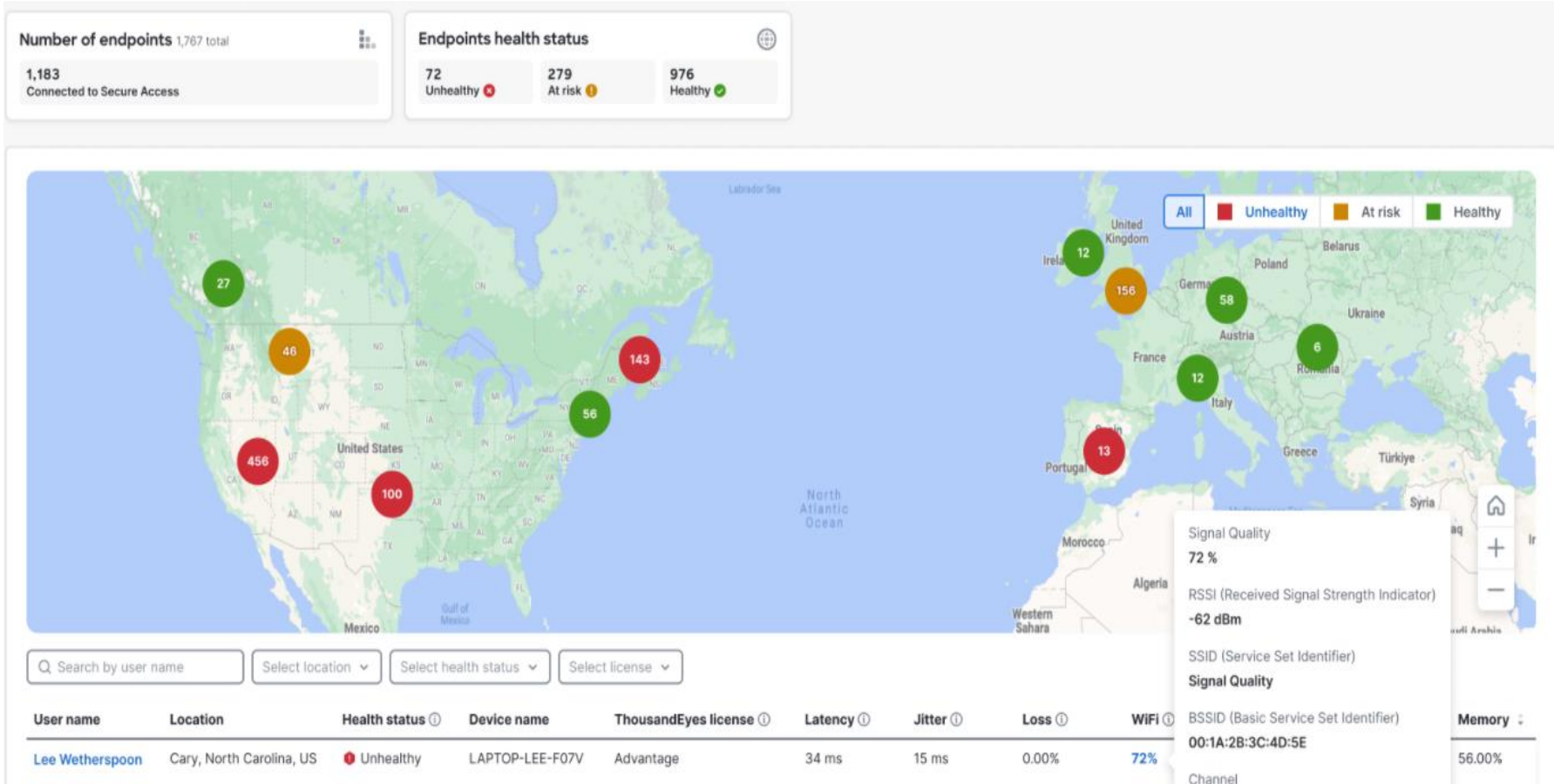


Experience Insights

Digital Experience Monitoring for Secure Access

Secure Access Experience Insights

Monitor digital experience with single agent and management portal



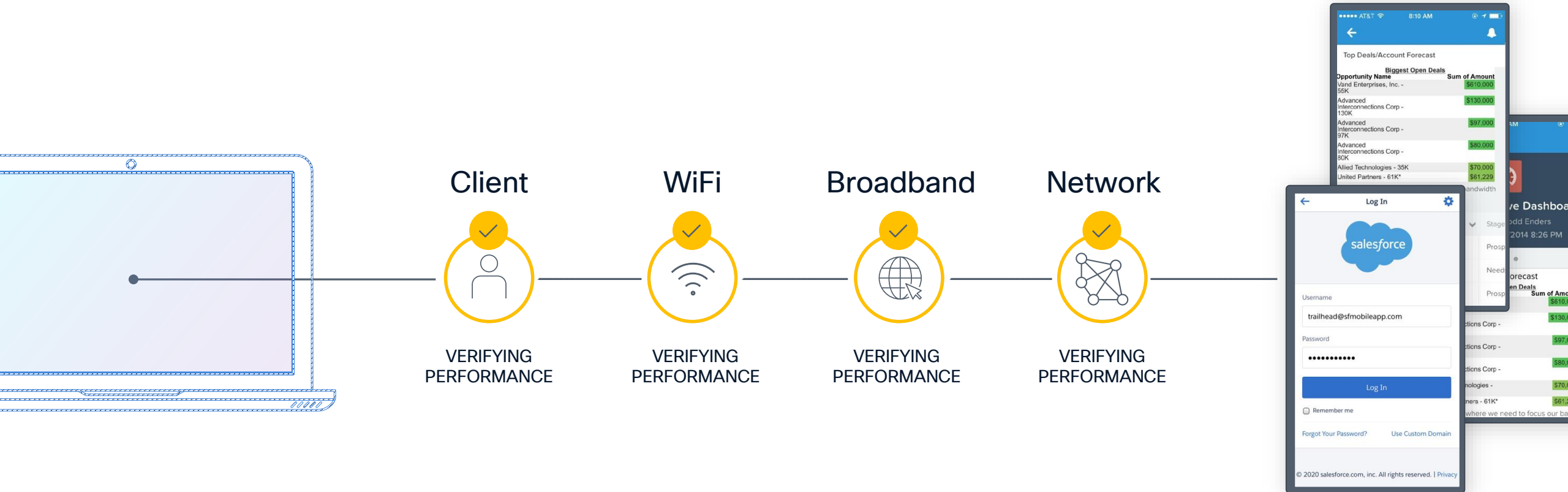
Local Device

Internet and Network Path

Collaboration Application

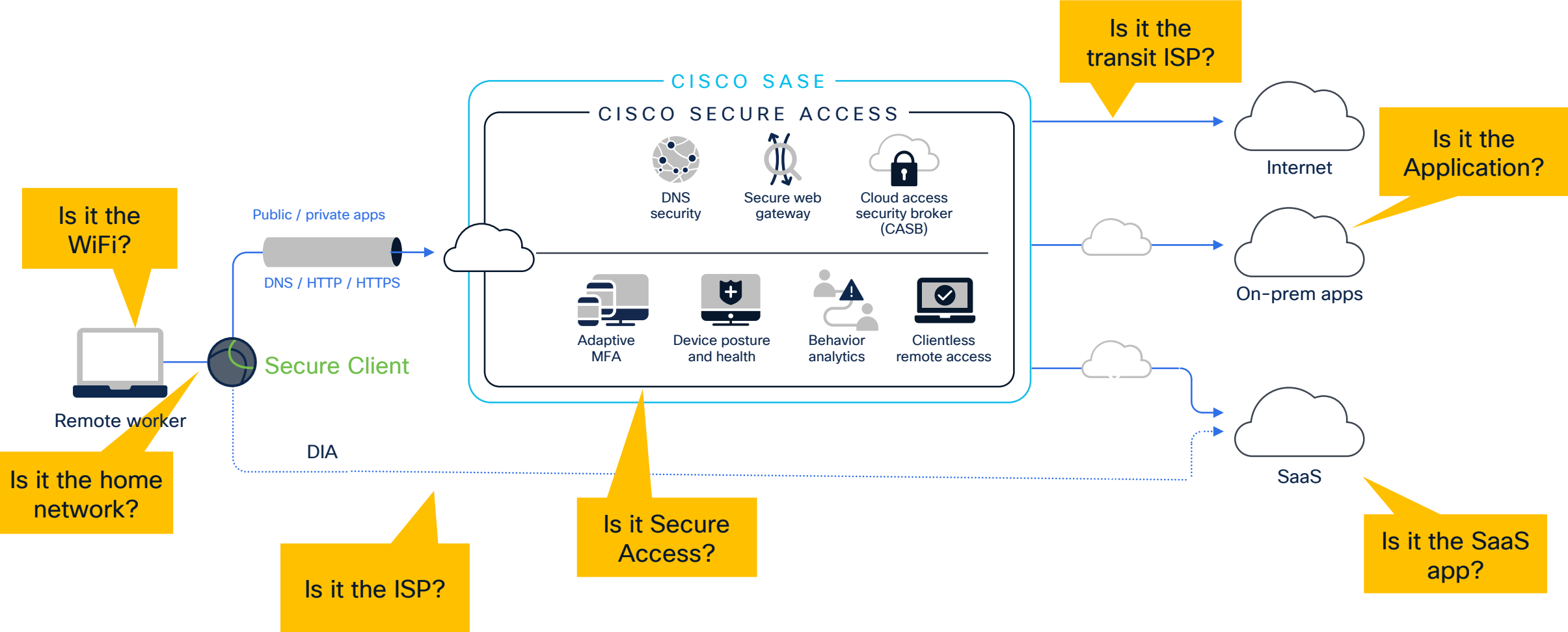
SaaS Performance

End-to-end visibility with Digital Experience Monitoring

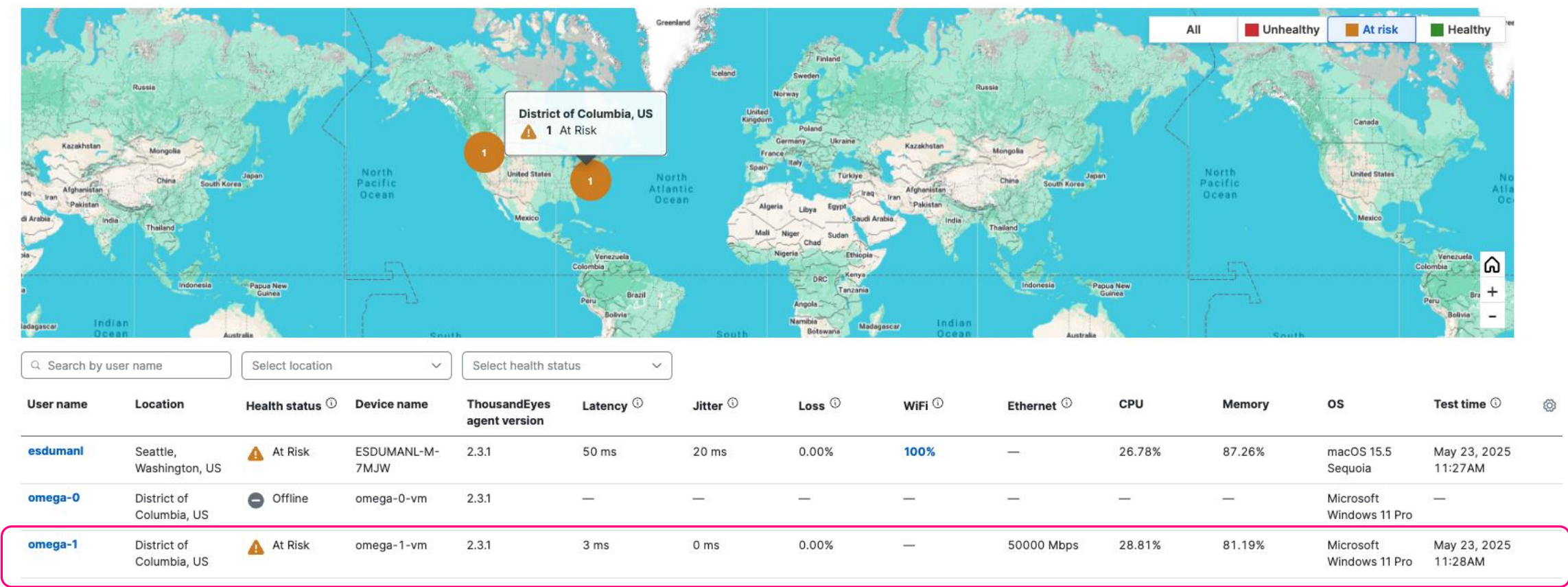


Historical performance and recommendations

Remote Worker Use Case



Start Troubleshooting on the Map



Detailed User/Device Information

← Experience Insights

Omega 1

Explore device performance metrics, connection quality to application cloud and collaboration tools. Monitor real-time CPU, memory, Wi-Fi strength, and view summarized security and application events for user safety.[Help](#)

Last updated May 23, 2025, 11:30

Summary

User Details

Email	avasilko+omegaurer1@cisco.com
Identity Provider	okta
Hostname	omega-1-vm
Groups	—
Devices	1 connected 0 disconnected

Device Details

Operating system	Microsoft Windows 11 Pro	Client-based Zero Trust Access	Enrolled
Public IP address	172.191.203.3	Certificate status	Enrolled (Expires in 32 days)
Secure Client version	5.1.9	Last certificate issue	May 20, 2025 12:55:39
Last connected	May 23, 2025 11:20:50	ZTA module version	5.1.9.1200
Last location	District of Columbia, US	Last configuration sync	May 23, 2025 11:22:57
ThousandEyes Endpoint License	Advantage		

Endpoint posture ⓘ

Client-based Zero Trust Access

Unenroll device

Certificate status	Device firewall
Enrolled (Expires in 30 days)	Running platform-native firewall
Last certificate issue	Disk encryption
Mar 14 2023 09:14:35	Not running (Posture profile requires any disk encryption product on the endpoint)
ZTA module version	System password
5.5.01023	Set
Last connected	Endpoint security agent
Mar 14 2023 09:14:35	Running CrowdStrike Falcon Sensor 4.25.8705.0
Last configuration sync	
Mar 14 2023 09:14:35	

Security ⓘ

Last 24 hours

User-associated rules

Search

Action

2 rules

#	Rule name	Action	Hits
1	Access TestTitans private app	Allowed	10
3	For all private access	Blocked	33

1-2 of 2

<

1

>

Blocked Events 33 ↗ 100% from last 24 hours

View all

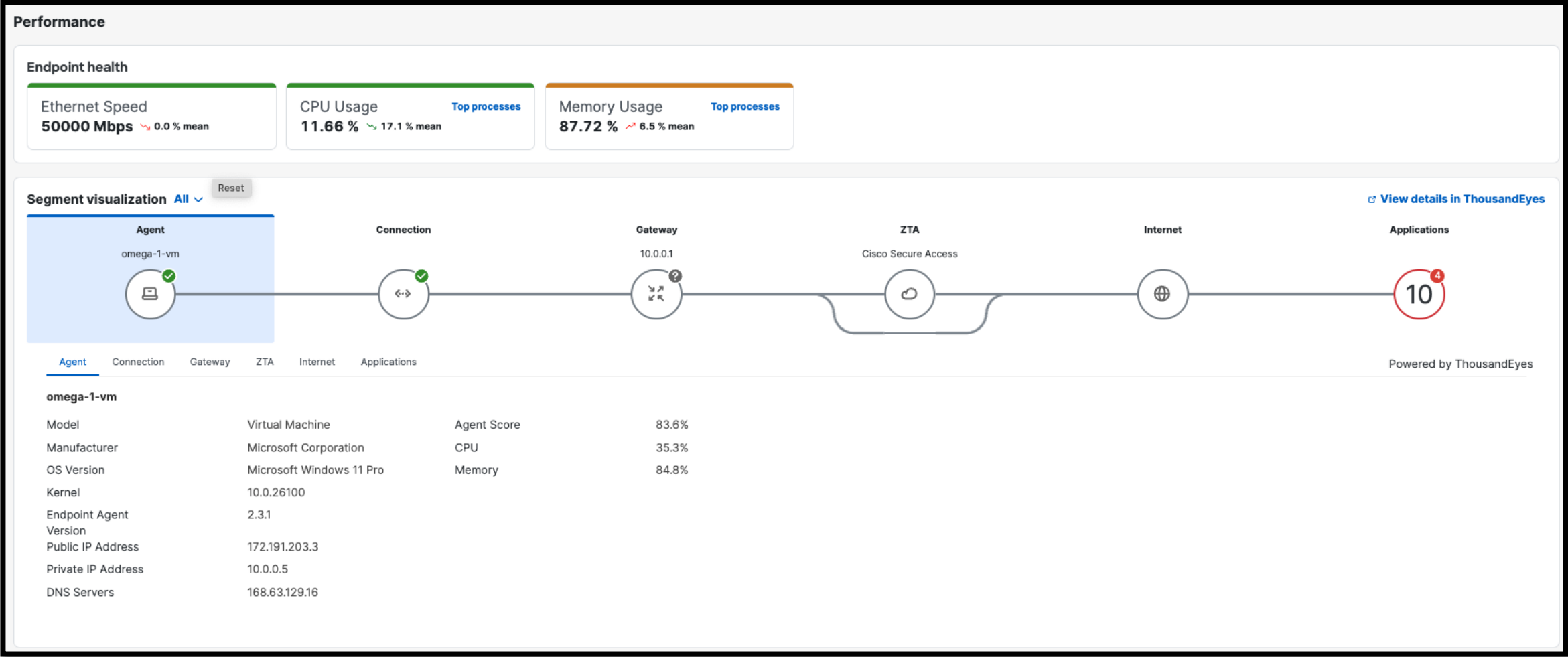


Allowed Events 10 ↗ 100% from last 24 hours

View all

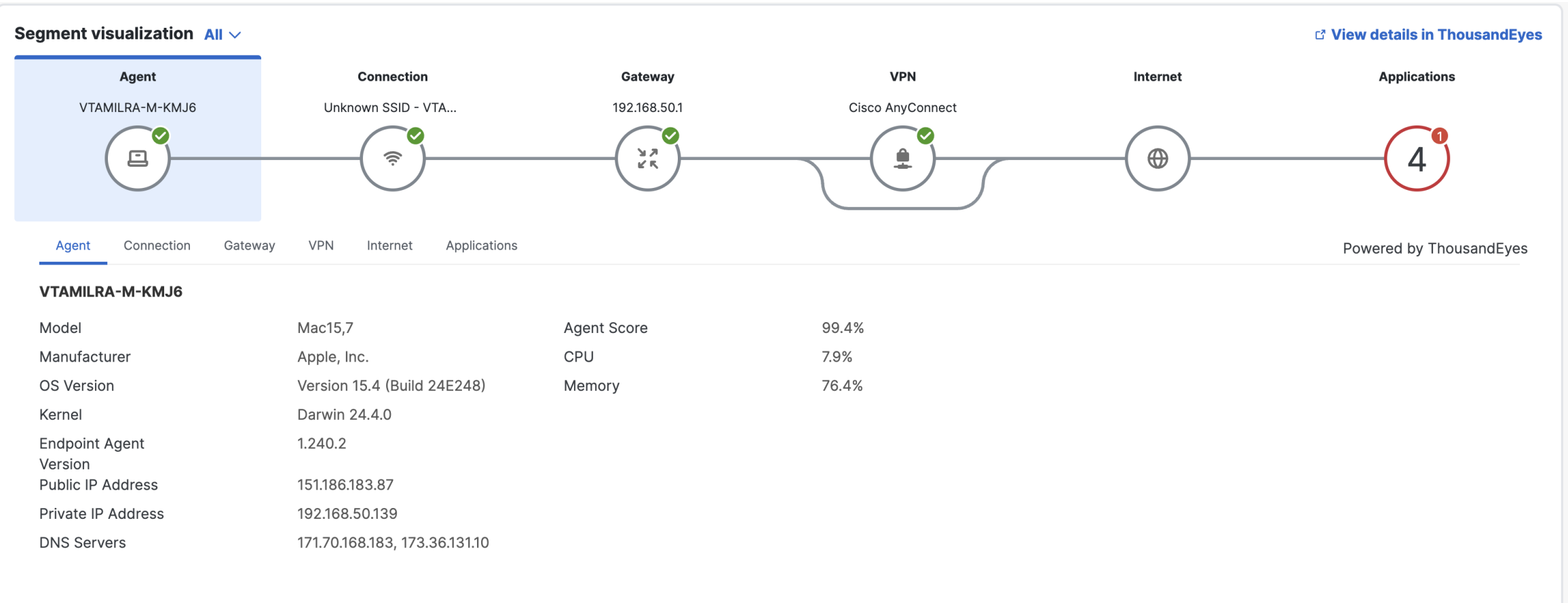


Endpoint Health and Network Segment



Network Segment Visualized

End to End Visibility



Create Synthetic Tests

Endpoint tests

Powered by  ThousandEyes

Simulate the user path to sites and applications using real traffic to gain insights into performance issues.

[Help](#)

Endpoint license usage

The number of endpoint tests you can run is based on your ThousandEyes license. For tips to increase test capacity, see [Help](#).

License type	Tests per endpoint	Active/total licenses	Usage
Embedded	2 tests	0 / 25	0%
Essentials	4 tests	0 / 5	0%
Advantage	10 tests	3 / 5	60%

8 Endpoint tests

8 Running

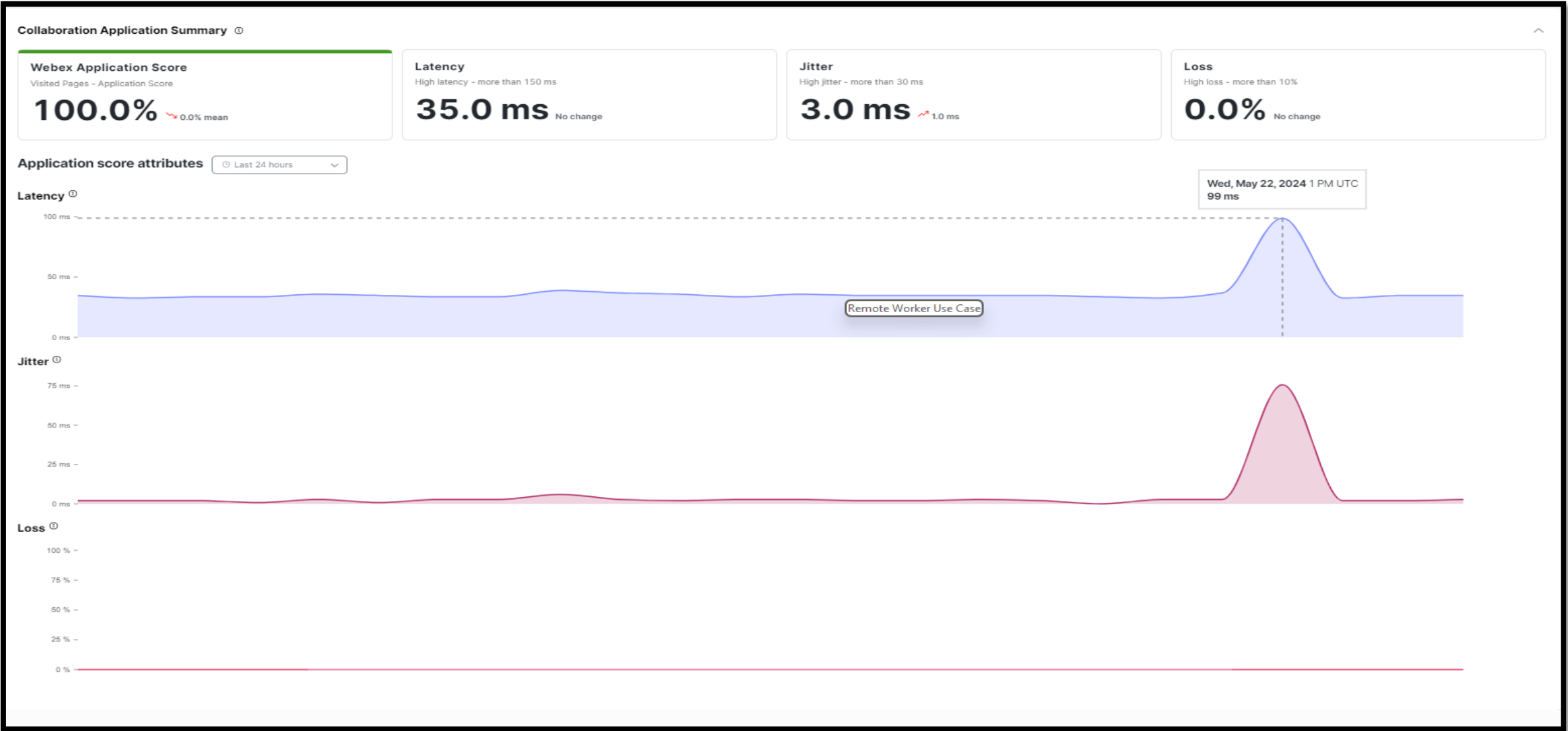
0 Disabled

Add new

☐	Status	Test name	Test type	Target	Running endpoints	Last modified	
☐	 Running	Facebook	Scheduled HTTP	http://www.facebook.com	All	2025-05-14T22:57:21Z	
☐	 Running	Google	Scheduled network	google.com	All	2025-01-06T13:42:41Z	
☐	 Running	MyPrivateApp	Scheduled HTTP	http://10.207.47.60	All	2025-01-06T13:45:24Z	
☐	 Running	Web App Test	Scheduled HTTP	https://www.facebook.com	All	2024-11-21T22:51:43Z	
☐	 Running	Webex	Scheduled network	webex.com	1 agents	2025-05-14T18:18:13Z	

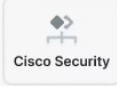
Collaboration Application Performance

How is the Webex experience?



AI Insights

 Secure Access

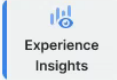
 Cisco Security

 Home

 Connect

 Resources

 Secure

 Experience Insights

 Monitor

 Admin

 Workflows

Experience Insights

Powered by **ThousandEyes**

Experience Insights brings together employee digital experience data so you can understand their journey to Secure Access and corporate resources. Get a comprehensive view into their device and network behavior to identify and resolve issues faster and make informed decisions on how to improve those interactions. [Help](#)

Last updated Jun 01, 2024 08:33

Summary

AI Insights

AI Generated Action Center

Latency Alert Summary

Our analysis has identified significant latency issues across multiple endpoints. Immediate action is recommended to prevent further degradation of network performance.

109 devices

70 devices (90 ms to 100 ms latency)

22 devices (75 ms to 90 ms latency)

17 devices (68 ms to 90 ms latency)

[Investigate latency issues](#)

Unhealthy Regions Detected

1850/4500

Our analysis indicates that the following regions have more than 76% unhealthy endpoints, suggesting significant regional issues that need immediate attention.

Region	Count
United Kingdom	800
Germany	500
San Jose, CA	290
Brazil	260

[Review unhealthy region](#)

Worst Performing SaaS Applications

Our analysis identifies the following SaaS applications with the worst performance, significantly impacting user productivity.

SaaS Application	Count
Monday.com	230
SharePoint	198
DocuSign	101

[View detailed performance](#)

The AI Assistant may display inaccurate information. Make sure to verify the responses. View our [FAQs](#) to learn more.

© 2024 Cisco Systems, Inc.

[Privacy policy](#) [Terms of service](#)



Unleashing the Power of Agentic AI: Transforming IT Operations

Simple LM vs Agentic AI

Simple LM

Reactive
Rely on Queries

Based on predefined
queries

Simpler tasks

Customer Support
Content Creation

Autonomy

Data Retrieval

Complexity

Use Cases

Agentic AI

Autonomous
With no instructions

Dynamically decide
what, when and how

Complex, dynamic
tasks

Autonomous vehicles
Robotics Automation

Characteristics of Agents



Autonomy



Reactivity



Proactive Behaviour



Learning and Adaptability



Reasoning



Communication

Characteristics of Agents

AUTONOMY

The ability to operate independently and make decisions without constant human oversight.



Autonomy



Reactivity



Proactive Behaviour



Learning and Adaptability



Reasoning



Communication

Characteristics of Agents

REACTIVITY

The capacity to perceive changes in the environment and respond appropriately in real-time.



Autonomy



Reactivity



Proactive Behaviour



Learning and Adaptability



Reasoning



Communication

Characteristics of Agents

PROACTIVE BEHAVIOR

(Goal-Orientation): The ability to take initiative and work towards specific objectives.



Autonomy



Reactivity



Proactive Behavior



Learning and Adaptability



Reasoning



Communication

Characteristics of Agents

LEARNING AND ADAPTABILITY

The capability to learn from experience and improve performance over time.



Autonomy



Reactivity



Proactive Behaviour



Learning and Adaptability



Reasoning



Communication

Characteristics of Agents

REASONING

The ability to process information, draw inferences, and make informed decisions.



Autonomy



Reactivity



Proactive Behaviour



Learning and Adaptability



Reasoning



Communication

Characteristics of Agents

COMMUNICATION

(Sociability): The capacity to interact with other agents or humans.



Autonomy



Reactivity



Proactive Behaviour



Learning and Adaptability

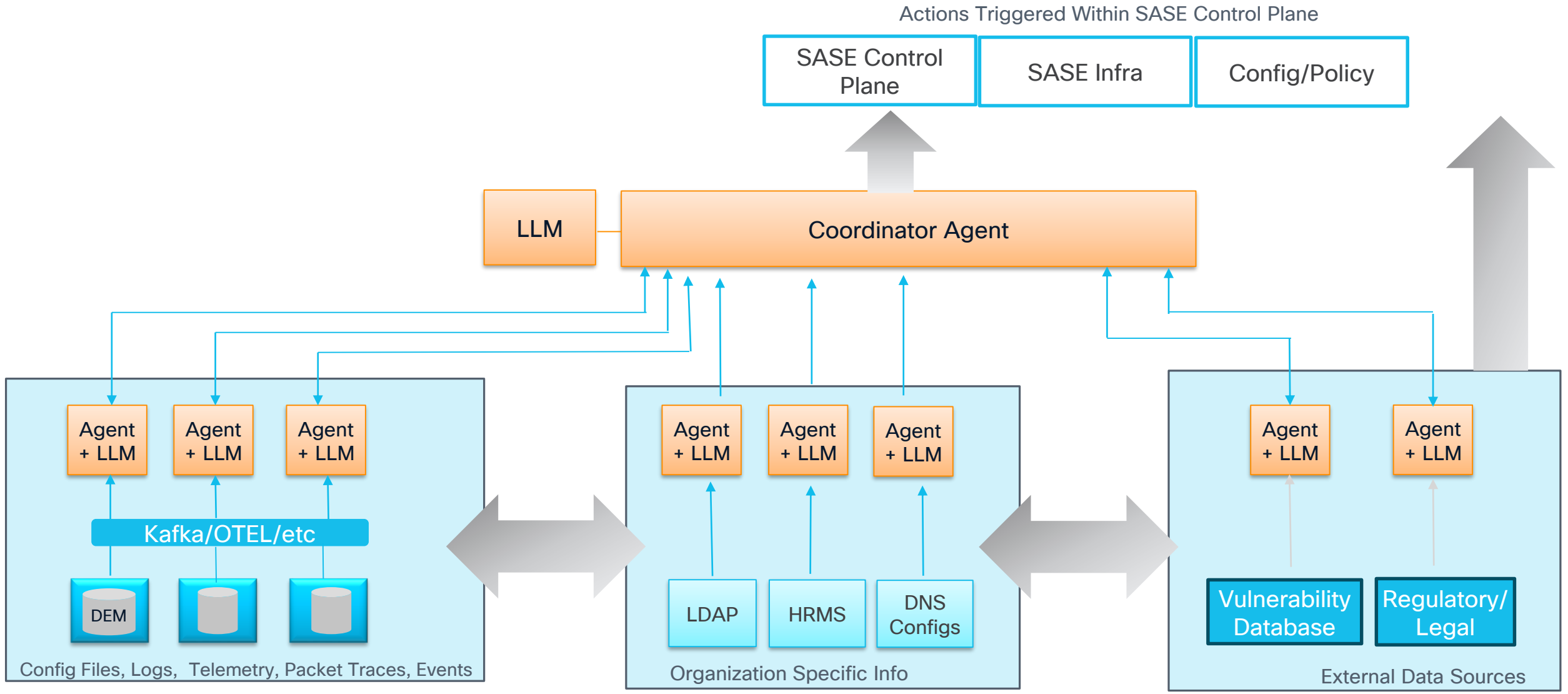


Reasoning



Communication

Agentic AI Conceptual Architecture



Key Focus Areas for AI Agents in SASE Networks

Cross-Domain Correlation & Decisioning

Integrate real-time data across security, networking, and apps for unified decisions that boost threat detection and performance.

Autonomous Configuration & Policy Management

Leverage AI to auto-generate, validate, and deploy network configs and policies, cutting errors and speeding compliance.

Anomaly Detection & Response

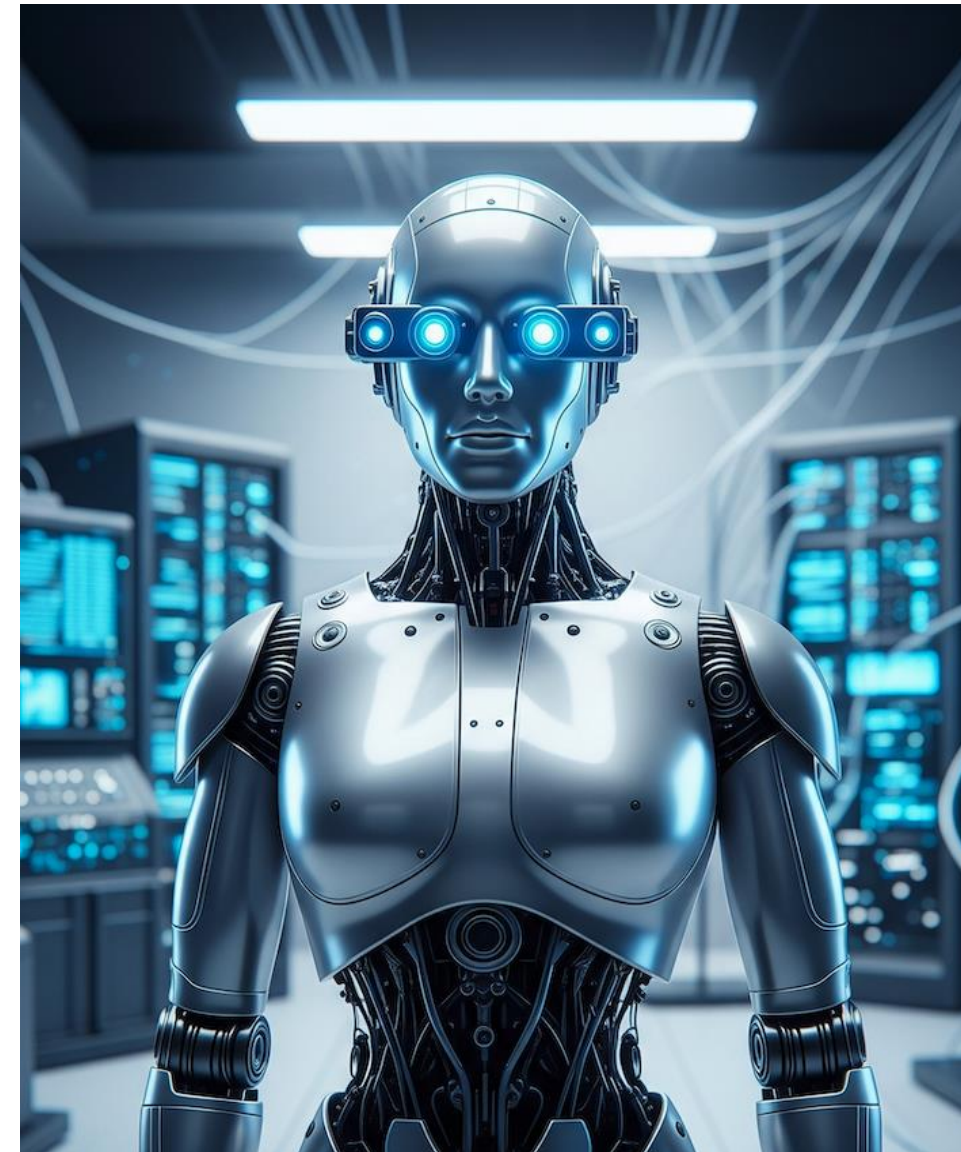
Apply machine learning to spot unusual patterns fast, triggering quick containment and keeping networks healthy.

Incident Management & Response

Use smart monitoring to quickly detect, prioritize, and automate threat remediation, reducing downtime.

Self-Healing Networks

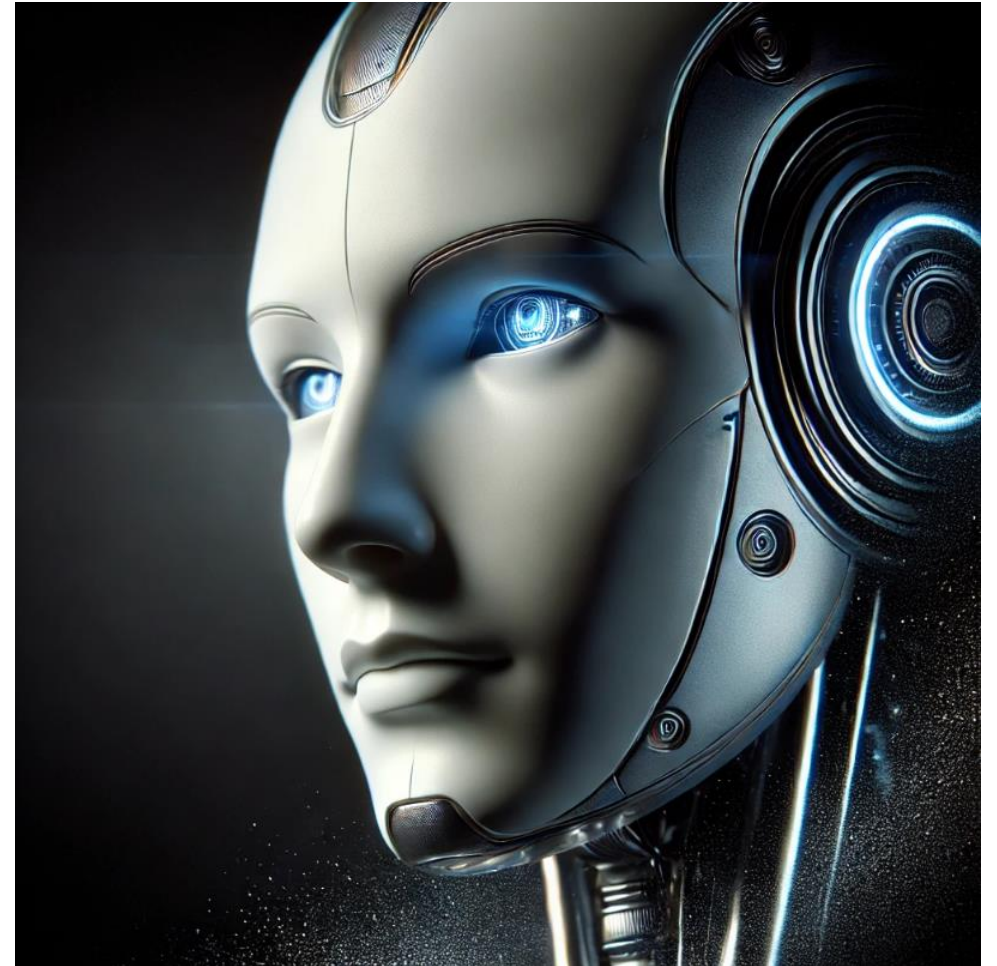
Perform real-time health checks with autonomous fixes to detect anomalies, optimize traffic, and maintain seamless service.





Cisco AI Assistant

Generative AI-Powered conversational interface
for increasing productivity



Policy Creation Skill

- Convert natural language prompts into security policies
- Create single or multiple rules at a time
- Assistant can infer the type of access needed
- The rule is disabled by default
- Simplify and speed up rule creation by 70%

The image displays the Cisco AI Assistant interface for creating security policies. The main window shows a prompt: "Let the Cisco Assistant help you! Just type your request and let the Assistant simplify your work!". Below this are buttons for "Create a single rule" and "Create multiple rules". A search bar at the bottom says "Add a rule or ask the AI Assistant a question".

Two example rules are shown on the right:

- Rule 1:** "Block Finance from Gambling".
 - Access: Internet
 - Action: Block
 - Sources: Finance
 - Destinations: Gambling
- Rule 2:** "Block Finance from Gambling and Allow Engineering access to Jira".
 - Access: Private
 - Action: Allow
 - Sources: engineering
 - Destinations: jira
 - Endpoint Requirements: (expanded)

Three blue speech bubbles at the bottom provide natural language prompts for the rules:

- "Allow Lee access to Jira"
- "Block Finance access to Gambling sites"
- "Allow HR access to Workday and Block Engineering access to Streaming Video"

Policy Optimization Skill

Optimize your Access Policy

- Identify **duplicate** and **shadow** rules
- Remove unnecessary and ineffective rules

The screenshot shows the Cisco Secure Access dashboard with the 'Access Policy' section selected. A modal window titled 'Cisco AI Assistant' is open, displaying the results of an access policy optimization scan. The scan has completed and identified 11 duplicate rules. The modal shows a list of rules, including rule 13 (Engineering, Finance, HR access Private App 1, Private App) and rule 14 (Sales, Finance, HR access Private App 1, Private App 2). Rule 13 has 1 of 2 duplicate rules, and rule 14 has 5 duplicate rules. The modal also shows a list of sources and destinations for the rules. At the bottom of the modal, there is a text input field for adding a rule or asking a question, and a disclaimer that the AI Assistant may make mistakes.

AI Powered Private Resource Discovery



- Shadow IT Visibility
- Insight-Driven Decisions
- Proactive Security Management

☰

Home

Connect

Resources

Secure

Experience Insights

Monitor

Admin

Workflows

Private Resource Discovery

Suggestions to define Private Resources based on resource usage data on your network so you can understand what resources users use most and make informed decisions on how to improve the end-user experience and maintain robust security standards for those resources.

Suggestions

Last 30 days

Private Resource suggestions are derived from existing network traffic based on VPN usage data. <Help>

83 Not Reviewed

?

Search by host address

Protocol

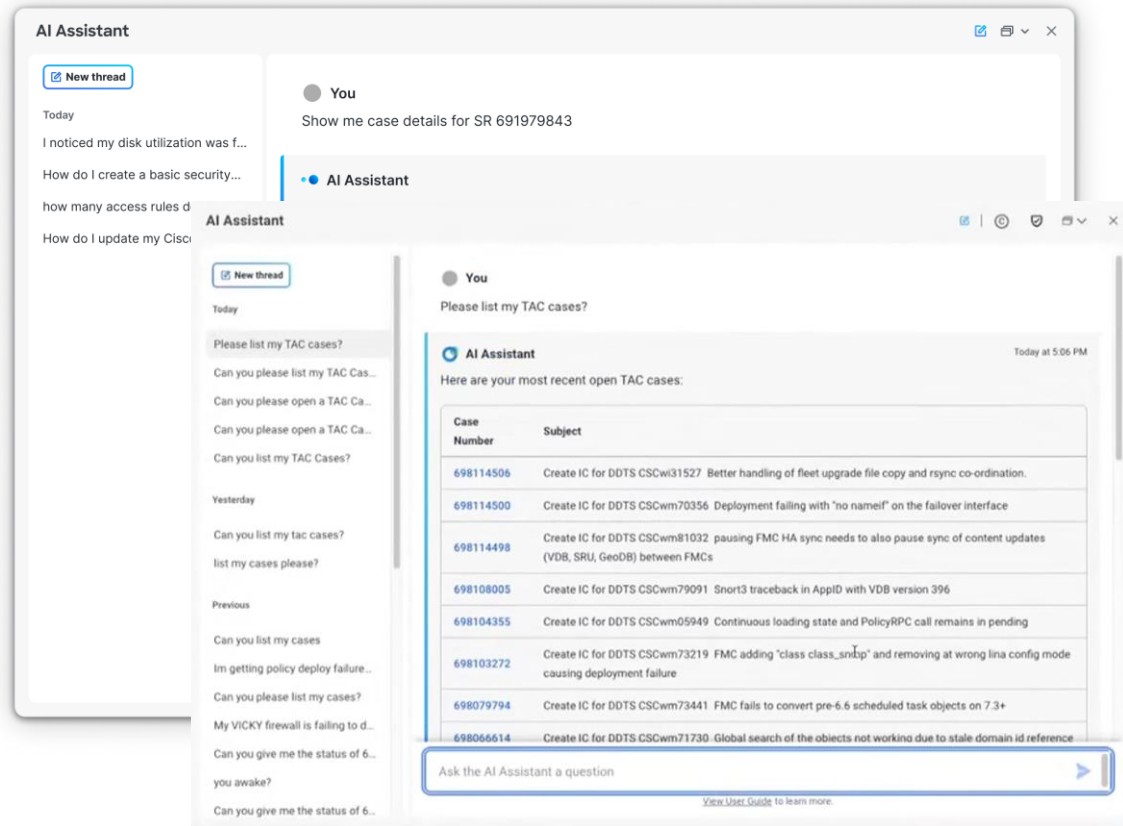
Label

83 Suggestions

Network Address ⓘ				# Users ⓘ	Total Hits ⓘ
☐	Host Address	Port	Protocol ⌵		
☐	> global.sqlserver.acme.com	8443	TCP > HTTPS	4345	45,231
☐	> external.deel.acme.com	8080	TCP > HTTPS	4154	34,275
☐	192.168.10.52	53	UDP > DNS	3589	24,138
☐	> acme-dev.atlassian.net	8443	TCP > HTTPS	4345	19,231
☐	192.168.10.54	3360	TCP	2487	16,634
☐	> printpool.us.acme.com	8443	TCP > HTTP	1587	14,259
☐	192.168.10.52	8443	TCP	1569	8256
☐	> remoteserver.proxy.acm...	8443	SSH	874	7644
☐	192.138.1.32	8443	TCP	633	7087
☐	> certman.acme.com	8443	TCP > HTTPS	458	458

In-Product Support/Escalation Skill

File TAC cases without leaving Secure Access



- Create TAC Cases by conversing in Natural Language
- Ask for details about specific TAC Cases

Troubleshooting Skill



AI Assistant11:08 am

Event analysis:
Based on the information provided, here are the possible reasons why **Lee Meadows** cannot access **Jira2**:

- A ZTA block event occurred for **Lee Meadows**
- A **Resource Connector 2** connection was issue for **Lee Meadows**

Note that these are possible reasons only, and further investigation may be required to determine the exact cause.

ZTA Access failure analysis1 Block

✓ Device Enrollment

✓ Access Policy

✓ Endpoint Posture

✓ User Authentication

✓ DNS

✓ IPS Profile

✗ Resource Connector 1 Block

You

Why can't Lee Meadows access Jira2?

AI Assistant11:05 am

I have identified the user **Lee Meadows** with email address **lmeadows@abc.com** and **Jira 2** (Office Productivity App) in our system. Verify settings in the event details section and then click Analyze events.

Event details

Sources:Lee Meadows (lmeadows@abc.com)

Destinations:Jira 2 (Office productivity app)

Connection Type:ZTNA

Device type:macOS

Devices:Lee-mac-C4605 (ZTNA)

Analyze event

- Private App Access Issues
- Multi Agent Collaboration
- Faster Time to Resolution

Prompts:

“Why can’t Lee Parker access Jira”

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

BRKSEC-2772

43

Documentation Summarization Skill



The screenshot shows the Cisco Secure Access dashboard with a sidebar containing navigation links: Home, Experience Insights, Connect, Resources, Secure, Monitor, Admin, and Workflows. The main content area displays the 'Overview' section. A modal window titled 'Cisco AI Assistant' is open, showing a conversation. The user asks, 'How do I deploy a resource connector in AWS?'. The AI Assistant responds with a high-level procedure and a list of prerequisites.

Cisco AI Assistant

You
How do I deploy a resource connector in AWS?

AI Assistant
Sure, I can help with that. Here's a high-level procedure to deploy a resource connector in Amazon Web Services (AWS).

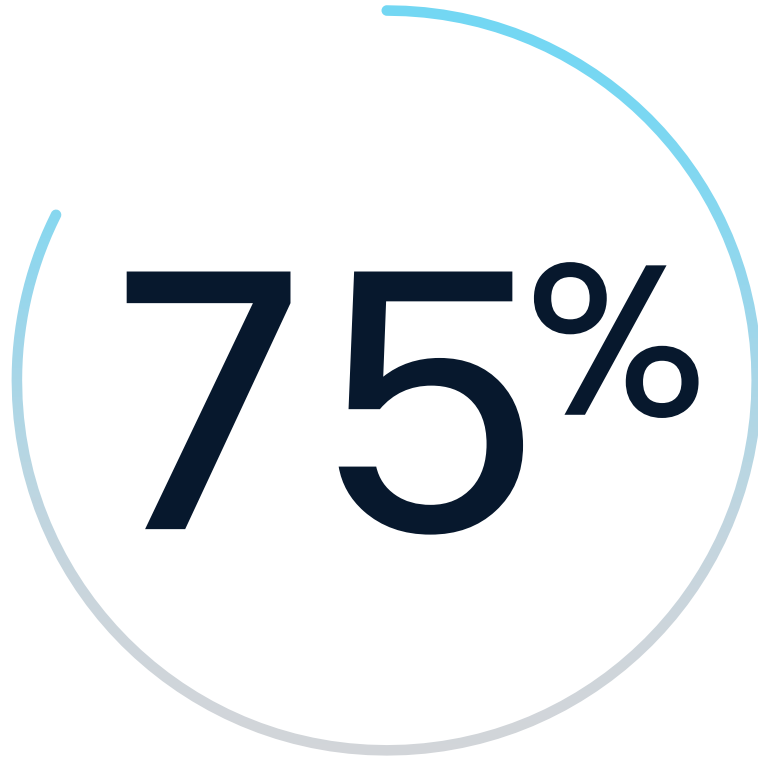
Prerequisites
Before you start, make sure you have:

- An AWS account.
- A supported architecture (Intel x86_64 or AMD64).
- The required instance type for deployments in production environments: C5.xlarge.
- Created the connector group in the region nearest to your geographical location.
- Obtained the connector image from the AWS marketplace.
- Copied the provisioning key for the specific connector group.

Add a rule or ask the AI Assistant a question

The AI Assistant may display inaccurate information. Make sure to verify the responses.

- Streamlined documentation experience
- Answers within the Secure Access Dashboard
- Linked citations

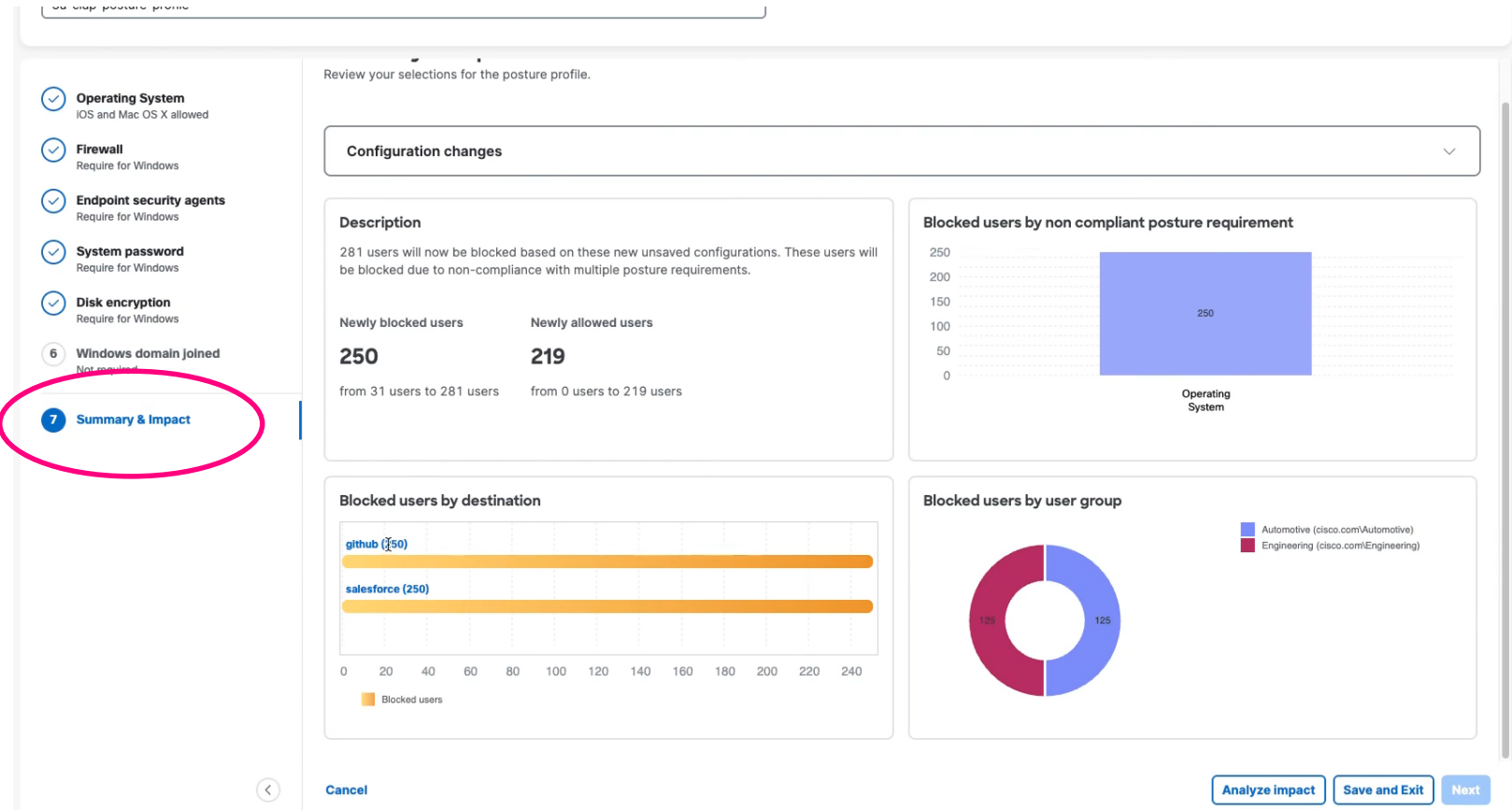


75%

of outages are from
misconfigurations

Gartner

Intelligent Policy Verification



Impact assessment before policy change

Use both analysis and synthetic data

Build intelligence to identify intended and unintended changes

Demo – Intelligent Policy Verification

Secure Access

?

Naman Tandon

☰

Home

Connect

Resources

Secure

Monitor

Admin

Workflows

Endpoint Posture Profiles

Posture profiles define requirements for user devices when accessing resources and the network. [Help](#)

Zero Trust Connection

VPN Connection

Zero Trust Connection

Define posture profiles for user devices that connect to resources on the network without using VPN. If the SSE client is not installed on an endpoint, the endpoint can connect only via browser, and few posture checks are possible. Access rules will associate posture profiles with specific resources. [Help](#)

Q Search

Posture type

Requirements

17 Posture profiles

Add posture profile

Posture profile name	Posture type	Requirements	Associated rules
System provided (Client-based) Default for client-based connection ⓘ	Client-based	Operating SystemFirewallEndpoint Security AgentDisk Encryption	2...
System provided (Browser-based) Default for browser-based connection ⓘ	Browser-based	Operating SystemBrowser	2...
test-bap-posture-profile-1	Browser-based	Operating SystemBrowser	0...
test-clap-posture-profile-1	Client-based	Operating SystemFirewallEndpoint Security AgentSystem passwordDisk EncryptionWindows domain joined	0...
test-3a-clap-profile-change	Client-based	Operating System	0...
test-3a-bap-profile-change	Browser-based	Operating SystemBrowser	0...
dummy	Client-based	Operating System	0...
Prasook Test ⓘ Unsaved changes	Client-based	Operating SystemFirewallSystem passwordDisk EncryptionWindows domain joined	1...
test j2n profile	Client-based	Operating System	0...

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

BRKSEC-2772

47

CISCO

Self-Healing Secure Access

How does Self-Healing Secure Access solve the same problem?



Autonomous Remediation



Predictive Optimization



Continuous Monitoring

Autonomous Secure Access

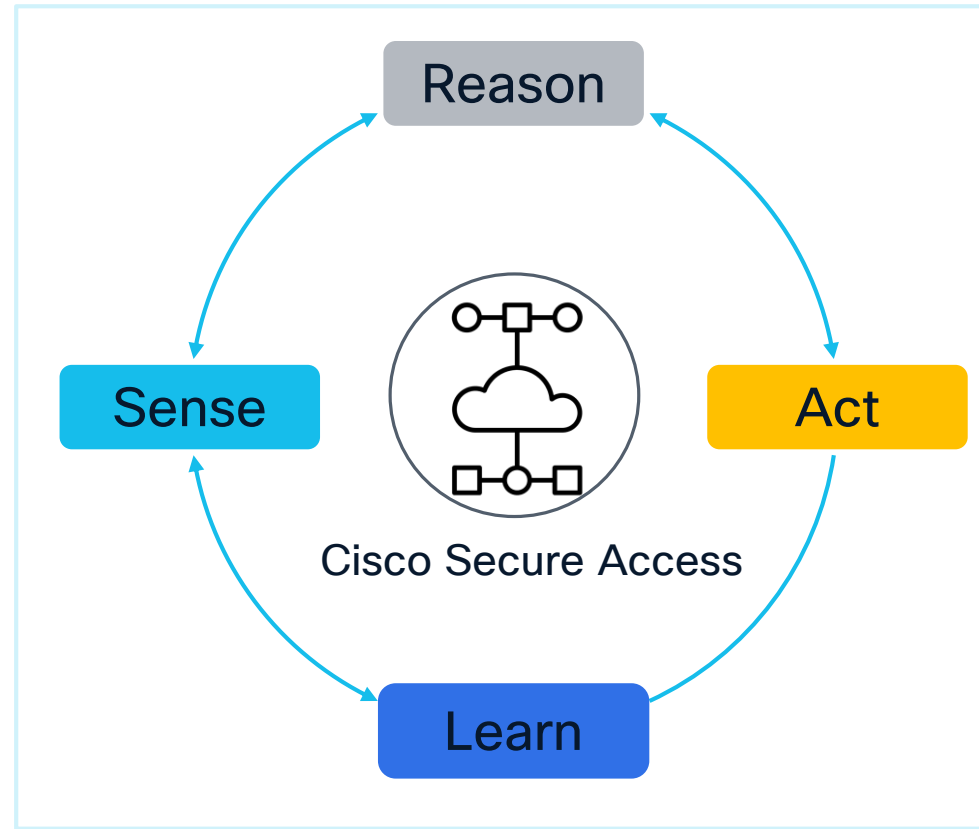
Sense from multiple sources

Reason and decide on actions

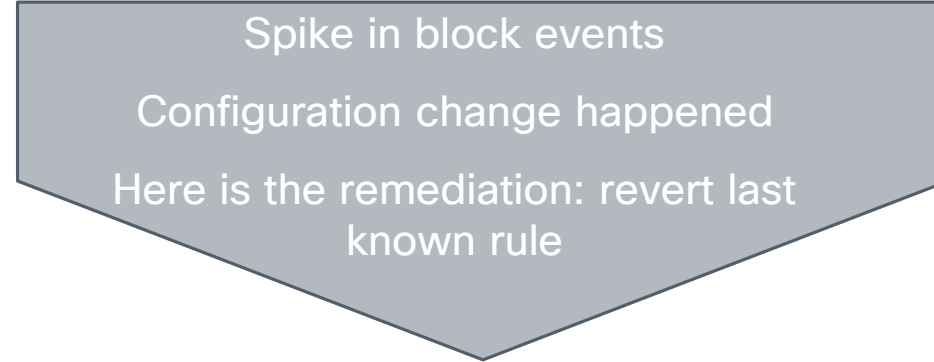
Act on the decision

Learn and proactively predict

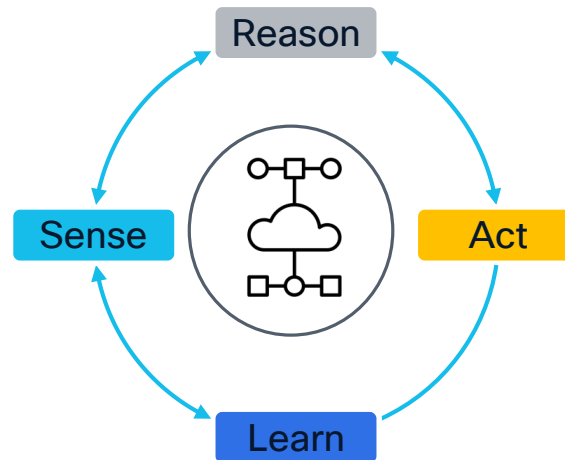
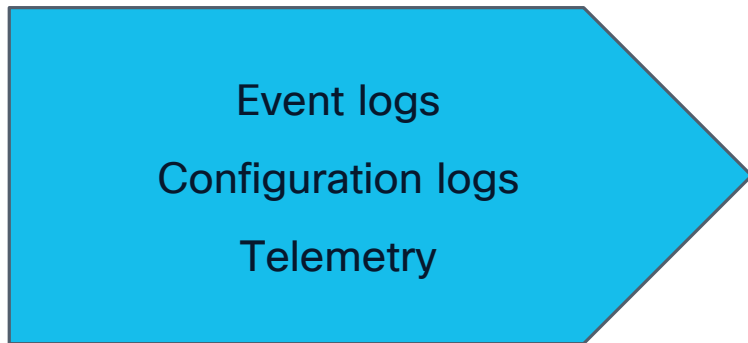
Drives smooth SASE operations



Self- Healing Secure Access – Configuration Assurance



Intentional ?
Unintentional?



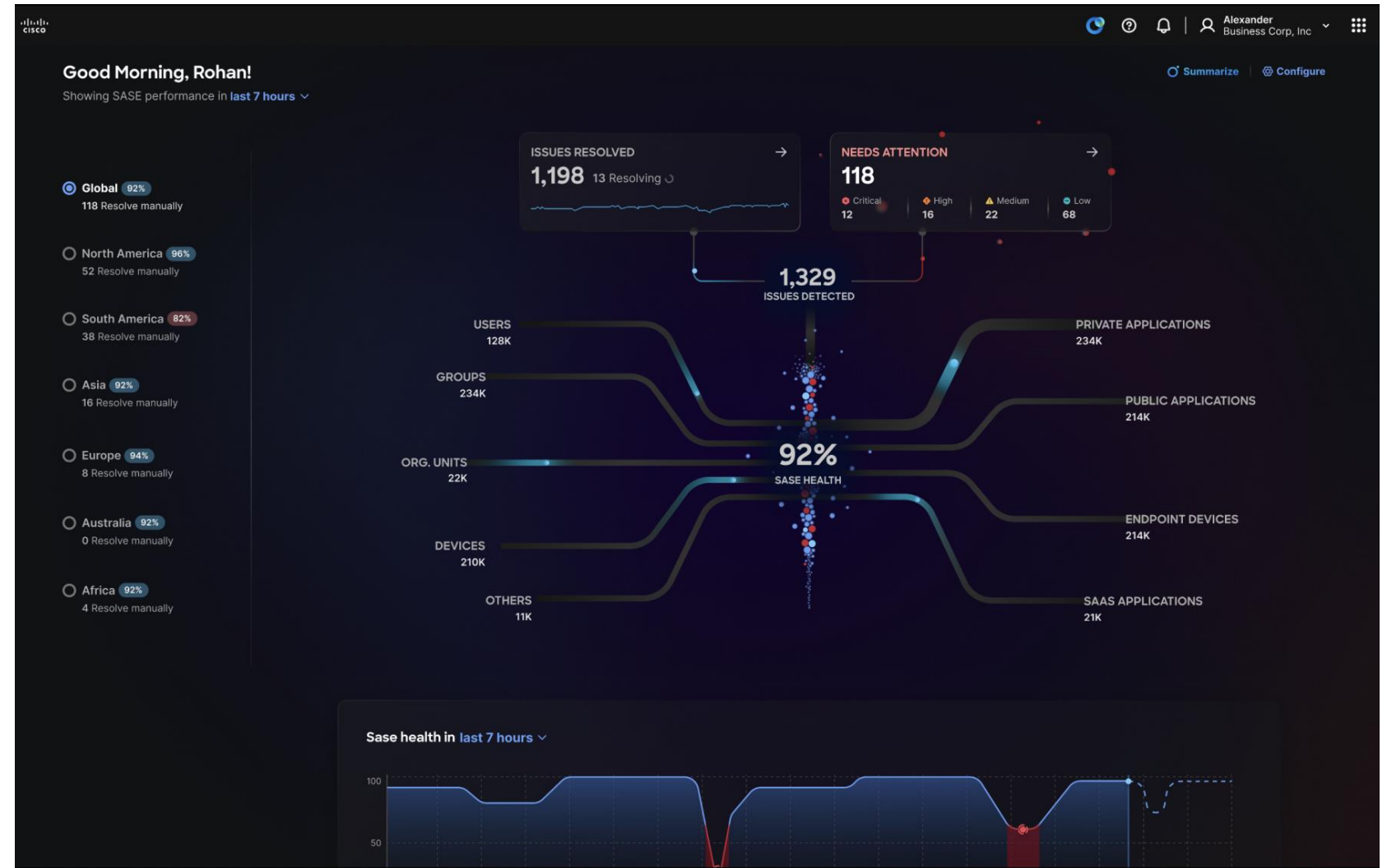
Self-Healing Secure Access- System Health

What is the intent and goal?

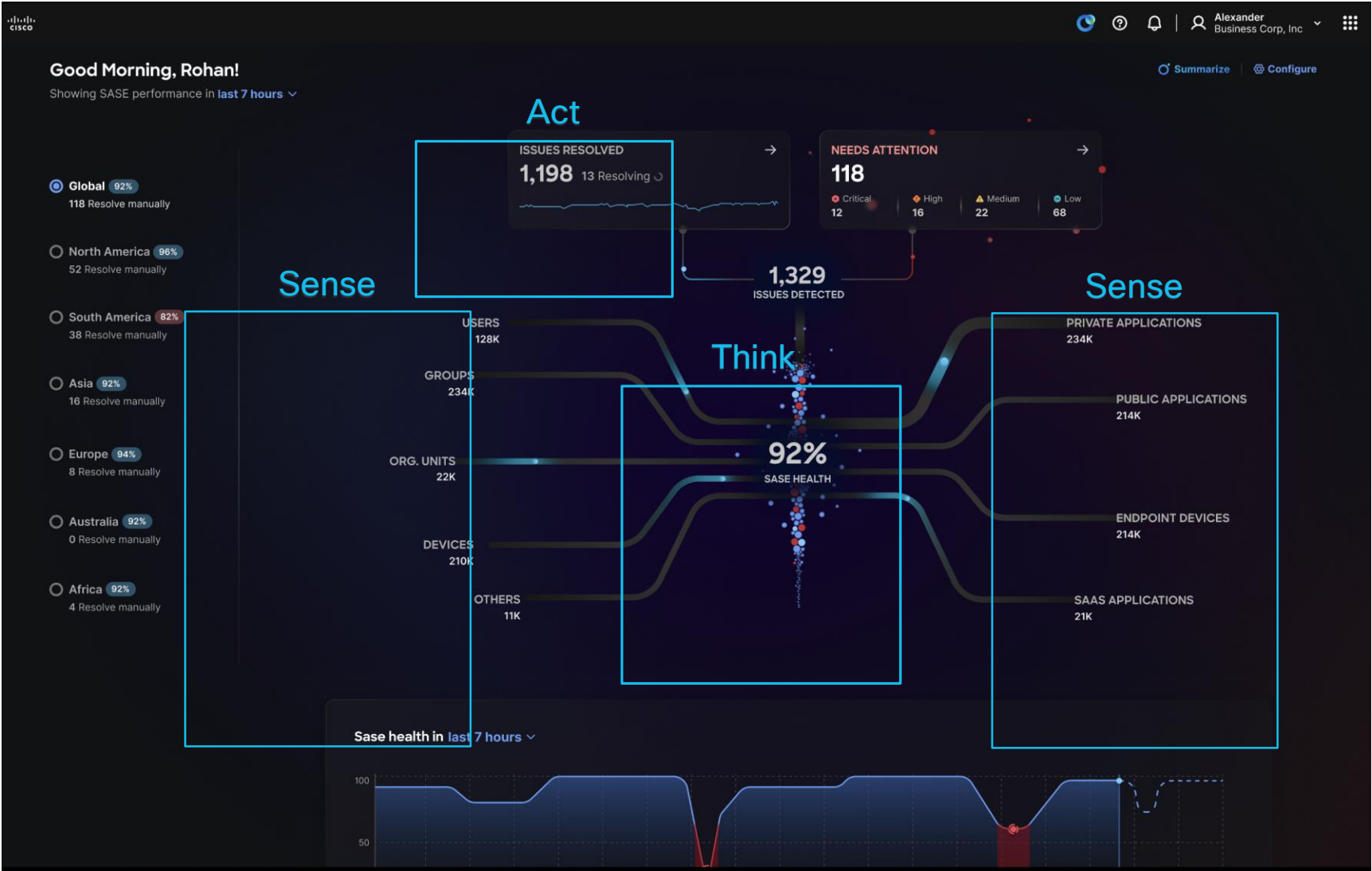
What is the definition of healthy system?

What tools required to assess health?

What actions to take?

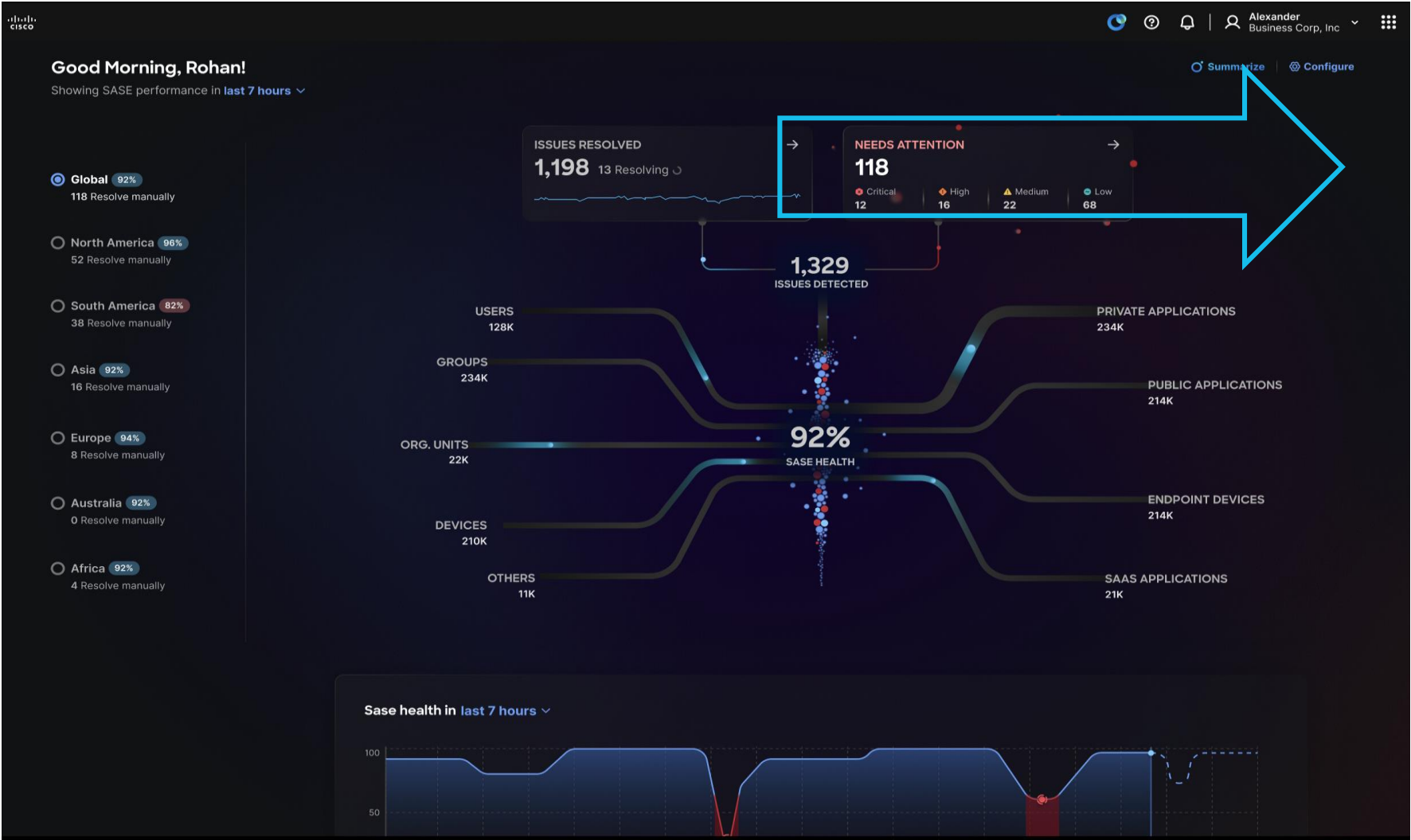


Self-Healing Secure Access- System Health

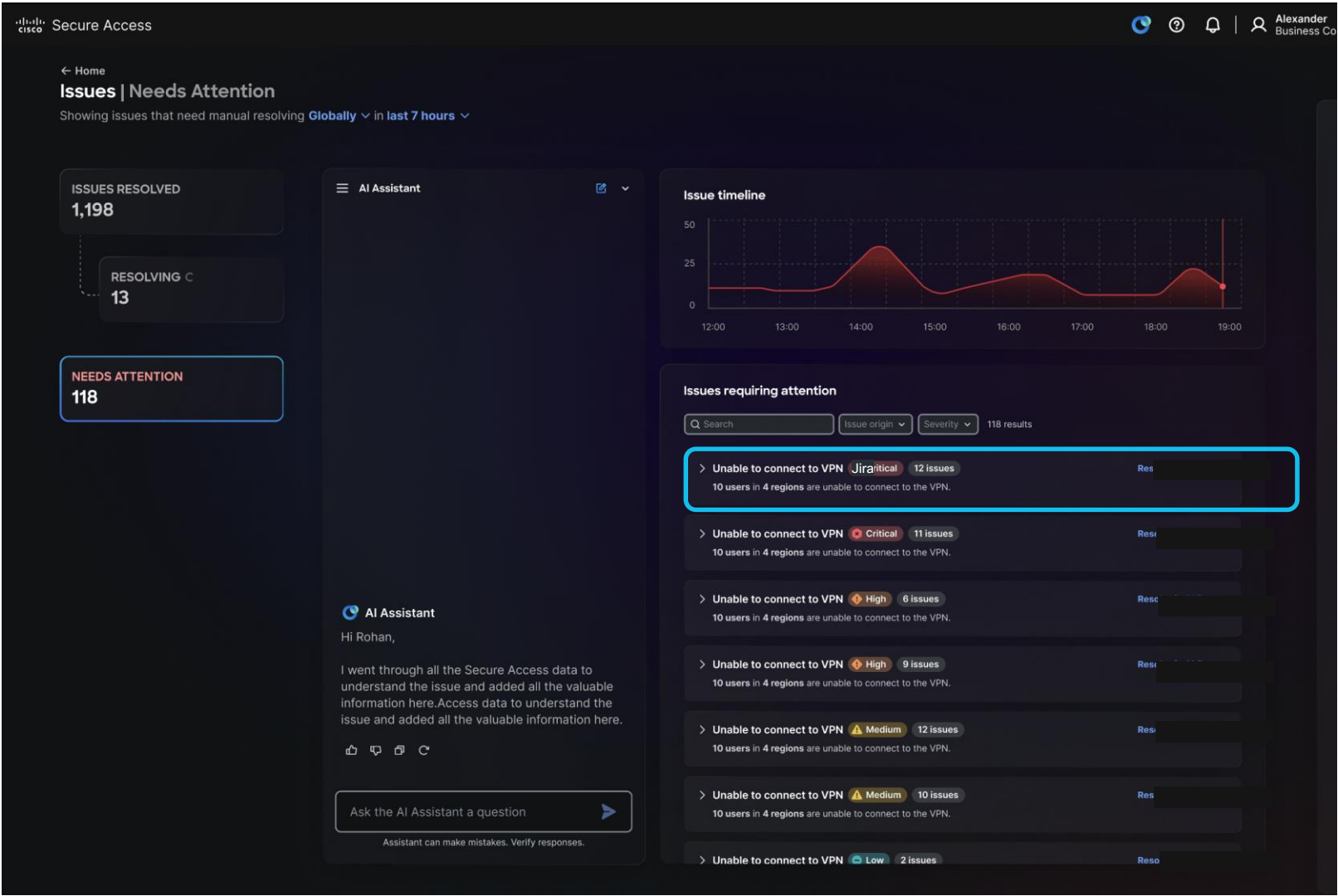


Self-Healing System Health

What needs attention?



Issues Need Attention



Continue Analysis with AI Assistant

Secure Access

Issues

Unable to connect to VPN

AI Assistant

You

Help me resolve this issue.

AI Assistant

Incident analysis flow

Recommendation provided

Recommended to bounce the AD node in United States to restore proper sync.

AI agent analysis

AI analysis between Firewall, Identity and Policy agent to find the cause and provide recommendation.

Issue detected

Several users are unexpectedly getting blocked

Based on our thinking, we are recommending the best way to solve this issue.

Recommendation

Bounce the AD node in United States to restore proper synchronization

Suggest another method

Accept

Ask the AI Assistant a question

Assistant can make mistakes. Verify responses.

Data flow overview

NORTH AMERICA

215 Endpoints

Incident Summary

Reported by

Firewall Agent

Description

Multiple users previously allowed are now being blocked by started occurring at 06/05/2025 17:20:00 UTC.

Severity

Critical

JIRA Ticket SRTK0023941

Blocked users

Users blocked

Time (Hours)

Packet loss

Critical point

Secure Access

Issues

Unable to connect to VPN

AI Assistant

Hi Rohan,

I went through all the Secure Access data to understand the issue and added all the valuable information here.Access data to understand the issue and added all the valuable information here.

You

Help me resolve this issue.

AI Assistant

Based on our thinking, we are recommending the best way to solve this issue.

Recommendation

Bounce the AD node in United States to restore proper synchronization

Suggest another method

Accept

Ask the AI Assistant a question

Assistant can make mistakes. Verify responses.

Data flow overview

NORTH AMERICA

215 Endpoints

Incident Summary

Reported by

Firewall Agent

Description

Multiple users previously allowed are now being blocked by the firewall in region XYZ. This started occurring at 06/05/2025 17:20:00 UTC.

Severity

Critical

JIRA Ticket SRTK0023941

Blocked users

Users blocked

Time (Hours)

Packet loss

Critical point

Impact

Users blocked

215

25%

Affected systems

Firewall cluster, AD Sync Service

Connectivity flow

Users

Connection

Gateway

VPN

215 users blocked

Internet

Applications

Connection

Point of issue

Incident analysis flow

Recommendation provided

Recommended to bounce the AD node in United States to restore proper sync.

AI agent analysis

Firewall Agent

Aha, that could be the issue. I have triggered an alert via Webex. Creating a Jira ticket. Recommending to bounce the AD node in United States.

Identity Agent

I notice that AD groups in region United States are out of sync. This started happening from 17:25.

Policy Agent

I don't see a policy change since 15:15

Firewall Agent

I am noticing that several users that were previously allowed are now getting blocked, starting 17:20. Are any of the other agents seeing anything that could have triggered this?

Issue detected

Several users are unexpectedly getting blocked

A Fundamental Shift In How We Work



Source: MIT Sloan Management Review and Boston Consulting Group Research

Autonomous Agents Working With Humans

- **Adaptive:**
Learns from data and environment.
- **Real-time Decision-Making:**
Adjusts based on evolving conditions.
- **Independent:**
Operates with minimal human intervention.

A woman with dark curly hair, wearing blue medical scrubs and a stethoscope, is looking down at a tablet computer she is holding. She is wearing a white smartwatch on her left wrist. In the background, another person is blurred, and there are blue and orange light bokeh effects, suggesting a hospital or clinical environment.

Human insights remains essential for smart decisions

Complete your session evaluations



Complete a minimum of 4 session surveys and the Overall Event Survey to be entered in a drawing to win 1 of 5 full conference passes to Cisco Live 2026.



Earn 100 points per survey completed and compete on the Cisco Live Challenge leaderboard.



Level up and earn exclusive prizes!



Complete your surveys in the Cisco Live mobile app.

Continue your education



Visit the Cisco Showcase for related demos



Book your one-on-one Meet the Engineer meeting



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



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

Contact me at: esdumanl@cisco.com

Thank you

CISCO Live !

