

FLEXCARE FACT

Did you know that Clip Training is part of FlexCare? Clip Training is an employee training and enablement tool. They have great videos around the entire M365 stack that you can leverage through your FlexCare agreement. Pricing begins at \$25/month for 50 users. If you are interested or want to learn more about Clip Training, please see your Account Rep.





Unified Security & Cloud Networking

Cisco Integration Strategies

Ben Sherwood – Security AE
US Commercial

Matt Ham, Solutions Engineer
US Commercial

November 14th, 2024





Security Agenda

- Investment and Innovation
- Secure Service Edge
- Cisco Extended Detection & Response (XDR)



Network Agenda

- The Meraki Platform
- Cisco XDR with Meraki
- Secure Connect

Cisco Secure

A modern approach to business resilience and employee satisfaction

Cisco Security Acquisitions since 2020



Application Security



Vulnerability Management



Cloud Network Security



Cloud Security



AI-powered Threat Detection



Identity Security



Cloud Security



Security Automation



Cisco Security Acquisitions – Growing and Evolving



Cloud Email Security and
ETD



Firewall Platform and Secure Endpoint



Cross-Platform Secure Malware Analytics



Umbrella SIG and Secure Access (SSE)



Network and Cloud Analytics - XDR



Umbrella SIG and Secure Access (SSE)



User Protection Suite

Simplifying Security

Security that Drives Business Outcomes

User Protection Suite



Cloud Security Suite



Breach Protection Suite



Simplifying Security

Security that Drives Business Outcomes

User Protection Suite

Cloud Security Suite

Breach Protection Suite

Future-Proofed Workplaces

AI-Ready Cloud and DC

Digital Resilience

Accelerate Zero Trust
Network Access

Identity | SSE

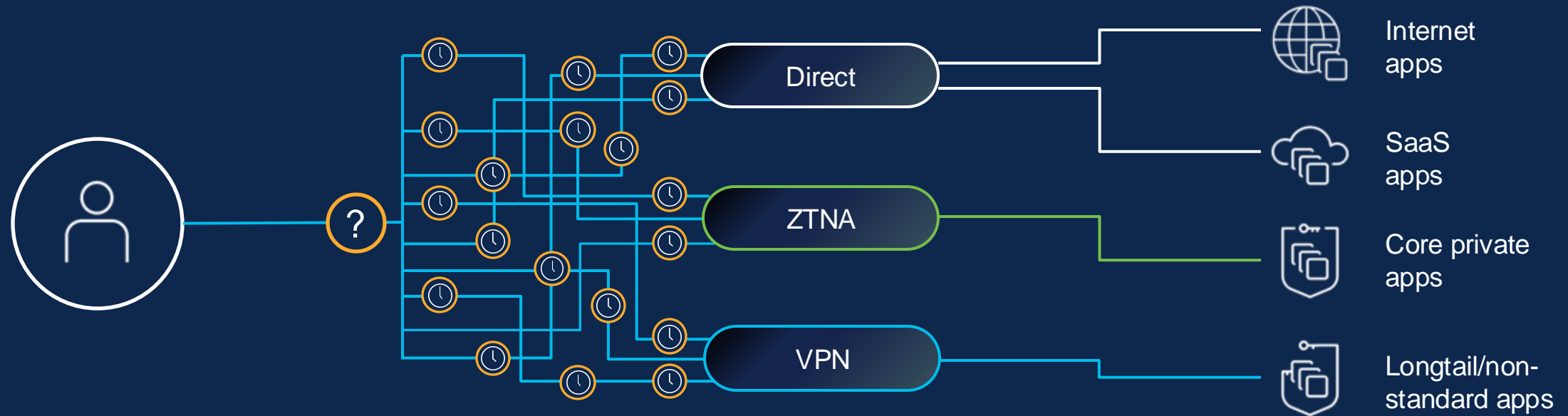
Secure Data Center and
Cloud

Segmentation | Unified Policy
Visibility

Power
Security Operations

XDR
SIEM | SOAR

Users experience fatigue, friction, repetition



- Many connection decisions
- Various processes
- Multiple steps
- Repetitive authentication tasks

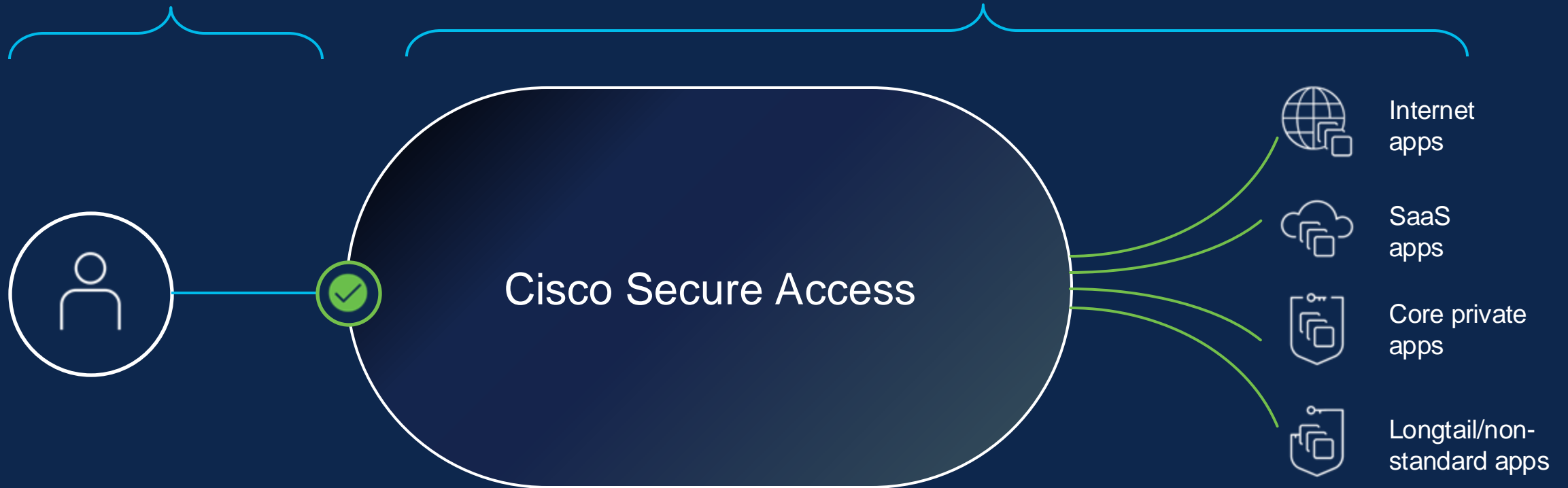
49% Employees frustrated with tech

26% Employees leaving job because of tech experience

Easy, frictionless user experience

1 Connect to a network

2 Get to work



Security Service Edge (SSE)

Better connect and protect your business

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



XDR



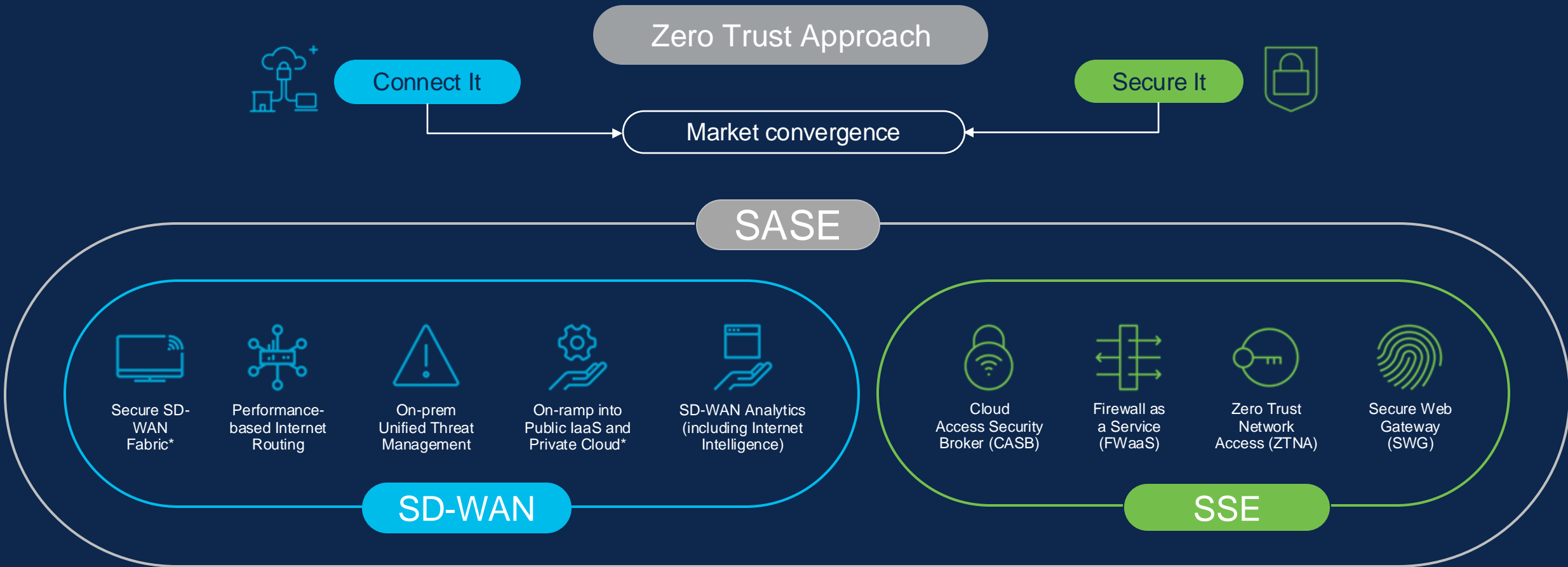
Duo MFA/SSO



CSPM

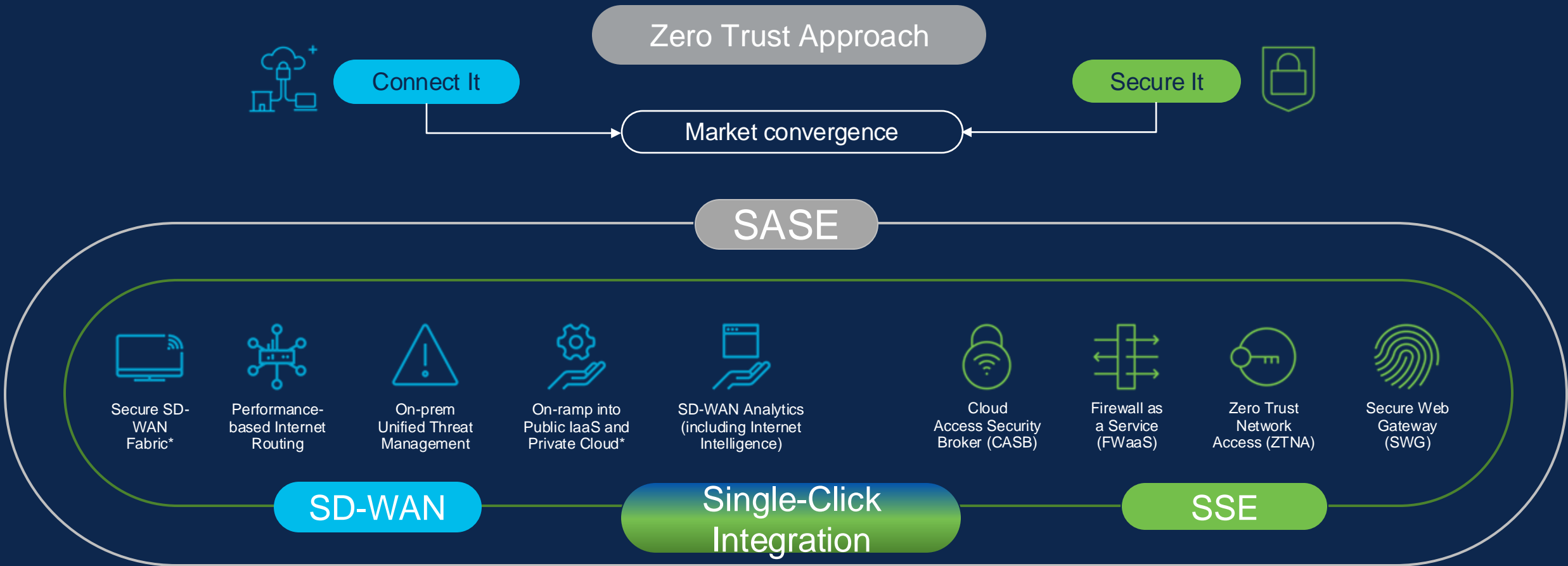
SASE/SSE approach is the technology foundation

Fundamental to your security strategy for a hyper-distributed world



SASE/SSE approach is the technology foundation

Fundamental to your security strategy for a hyper-distributed world



Cisco shines
where security
meets the network





AI-powered security is the future.
But to have good AI you need good data,
and to have good data you need deep
integration with the network



AI-Powered Security
with Cisco XDR

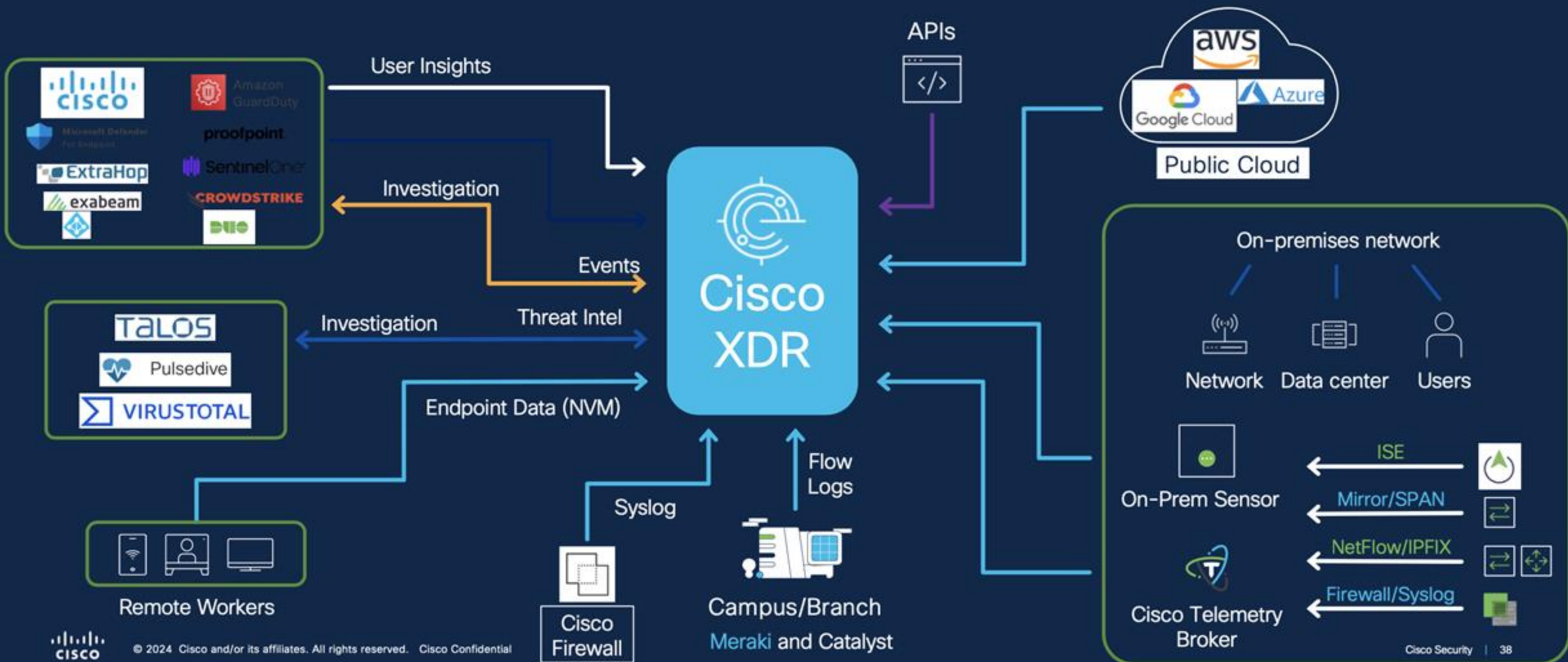


16 trillion flows of traffic
per week across 2+M MX
firewalls deployed

Extended context

Telemetry sources for Cisco XDR

Flexible integration for existing infrastructure



Cisco Meraki

Enterprise Cloud Networking Platform

The screenshot displays the Cisco Meraki dashboard for a switch named 'CORE 1'. The interface includes a sidebar with navigation options such as 'Network-wide', 'Security & SD-WAN', 'Switch', 'Wireless', 'Systems Manager', 'Cameras', 'Environmental', 'Insight', and 'Organization'. The main content area features a search bar, a map of the switch location, and several monitoring panels:

- Ports:** A grid showing the status of various ports on the switch.
- Historical data:** A line graph showing connectivity over time for the last day.
- Client usage:** A line graph showing client usage over time.
- Clients:** A table listing clients connected to the switch.

#	Description	VLAN #	VLAN name	IP address	VLAN	Port
1	...	None	76	57
2	...	None	76	57
3	...	100	100	10
4	...	100	100	25
5	...	100	100	30
6	...	100	100	10
7	...	100	100	10
8	...	100	100	10
9	...	100	100	10
10	...	100	100	10
11	...	100	100	10

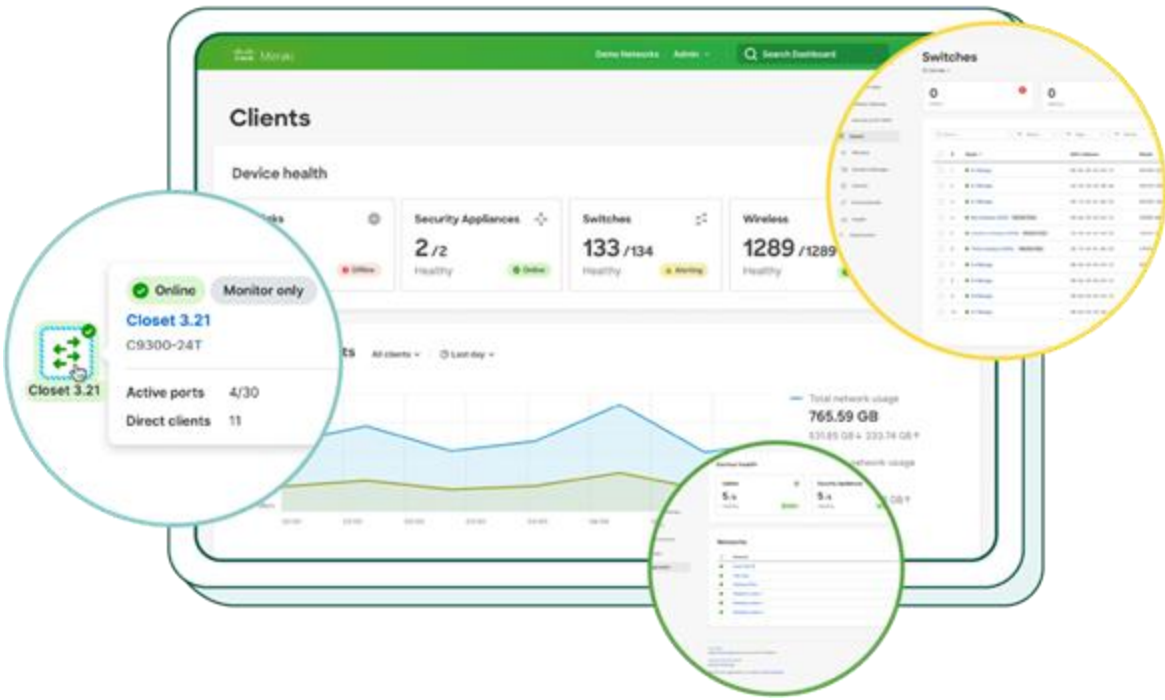


Cisco Meraki at-a-glance

Connecting passionate people to their mission by simplifying the digital workplace.



- 2006**
Invented cloud networking
- 2012**
Acquired by Cisco
- 2021**
Meraki powers 10M active devices
- Today**
18+ years designing scalable and secure cloud architecture



Cisco Meraki

Enterprise Cloud Networking Platform

75% of Fortune 500 companies trust Meraki for reliable operations at scale.



Access

- Wi-Fi
- Switching
- Mobile Device Management



Secure SD-WAN

- SD-WAN and Security
- Unified SASE
- Cellular gateways



IoT

- Smart cameras
- Sensors



APIs

- Meraki APIs
- Partner Ecosystem



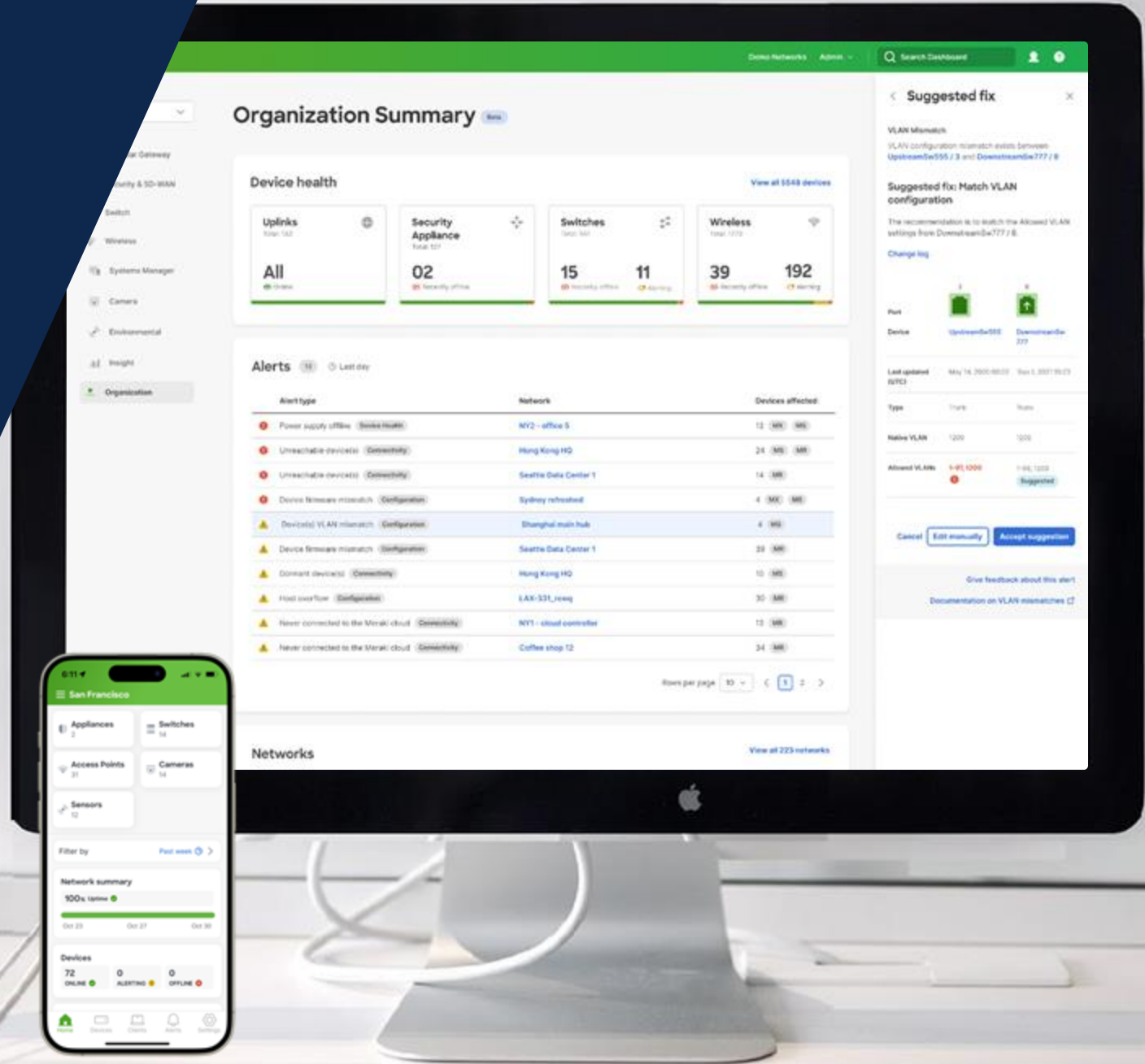
Cisco Security

- Secure Access
- Cisco Secure Endpoint
- Cisco Duo
- Cisco Secure Client

Meraki Dashboard: deliver operational excellence

- **Zero touch provisioning** at scale
- **Simple** UI accessible by anyone, reducing onsite support staff
- **Converge** networking and security
- **Improve** operational efficiency with energy usage reports and controls
- **Increase** productivity and lower MTTR with actionable insights

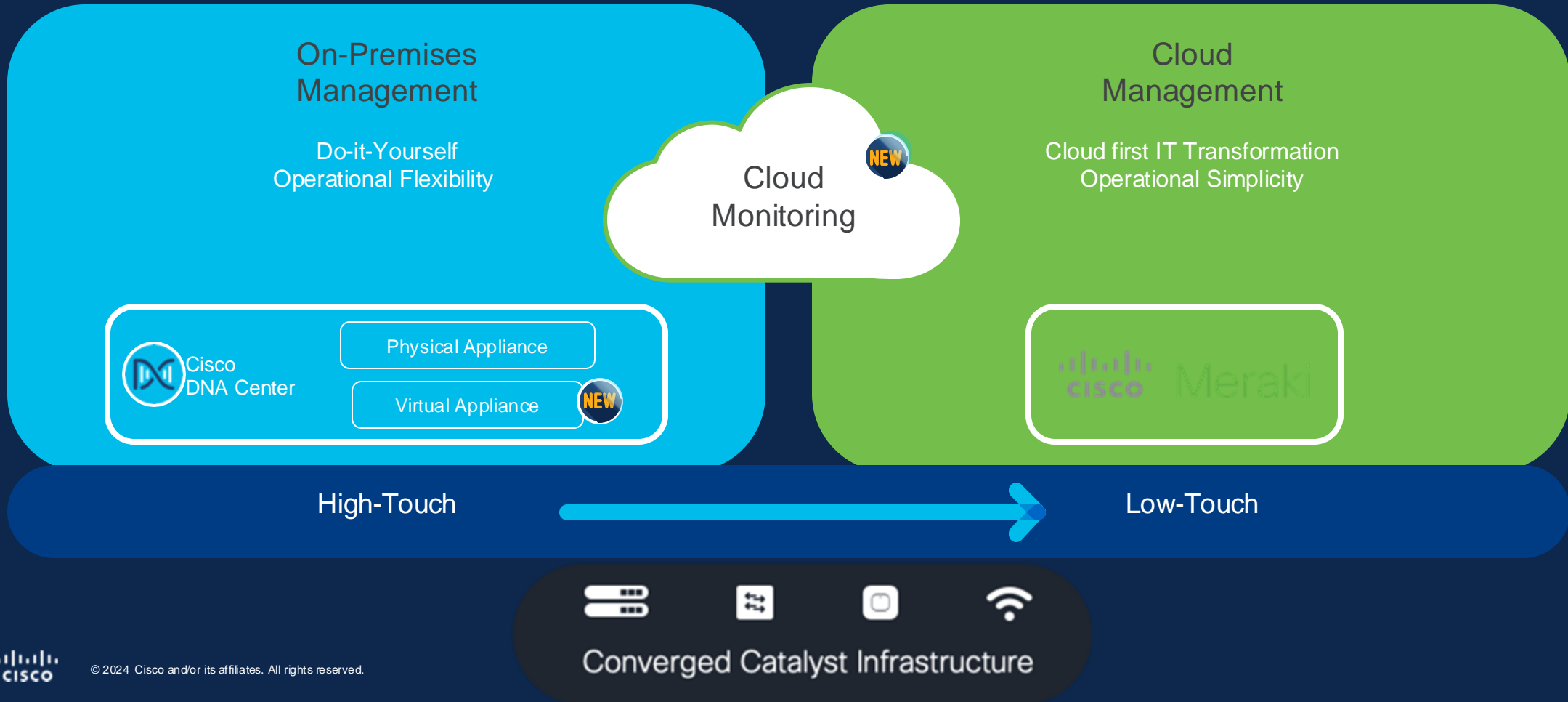
...plus **automate with APIs** for network automation and more



Converged Hardware

Your IT operating model, your way

Flexibility, choice, and simplicity



Supported Platforms and Software



Models

9200/L
9300/L/X
9500



Firmware

IOS-XE 17.3+



Licensing

DNA Advantage
DNA Essentials*



Models

CW916[x]
CW917[x]



Firmware

IOS-XE 17.9+



Licensing

DNA Advantage
DNA Essentials*

Accelerating momentum with Cisco Switching

CS17

Cloud Native IOS XE (Public Beta: Fall 2024)

2H FY25: Next Gen
Silicon One Switch

Troubleshooting CLI

Q3 FY25



MS150

Wi-Fi 7 ready

Up to 60W UPOE
5G mGig ports
4x 10G SFP+ uplinks
Layer 2+ stacking

Access

Orderability: 11/11/2024



CW917X

10G Port(s)
UWB
Directional Antenna (D1)

Access

Available Now



MS130(R)

Adaptive Policy
Layer 2
mGig + 10G options
R – Ruggedized

Access

Cisco GSX

Next-Gen High End MX650



1. 2 x 25Gbps (SFP28) interfaces (1 x WAN/LAN convertible)
2. 2 x 10Gbps SFP+ interfaces WAN/LAN convertible
3. 8 x 1Gbps SFP LAN only

2x Internal Redundant Hot-swappable 250W AC power supply

Dramatic Performance Improvements



25 Gbps VPN Throughput

2x increase over current generation maximum



18 Gbps Threat Protection Throughput

2x increase over current generation maximum



Concentrator Mode

First release will support Concentrator mode only.

Routed mode release date TBD.



New VPP based OS architecture

A new 'Software ASIC' driven architecture which is highly performant and highly efficient.

Meraki MX Integration in Cisco XDR

NEW!

Gain enhanced network security

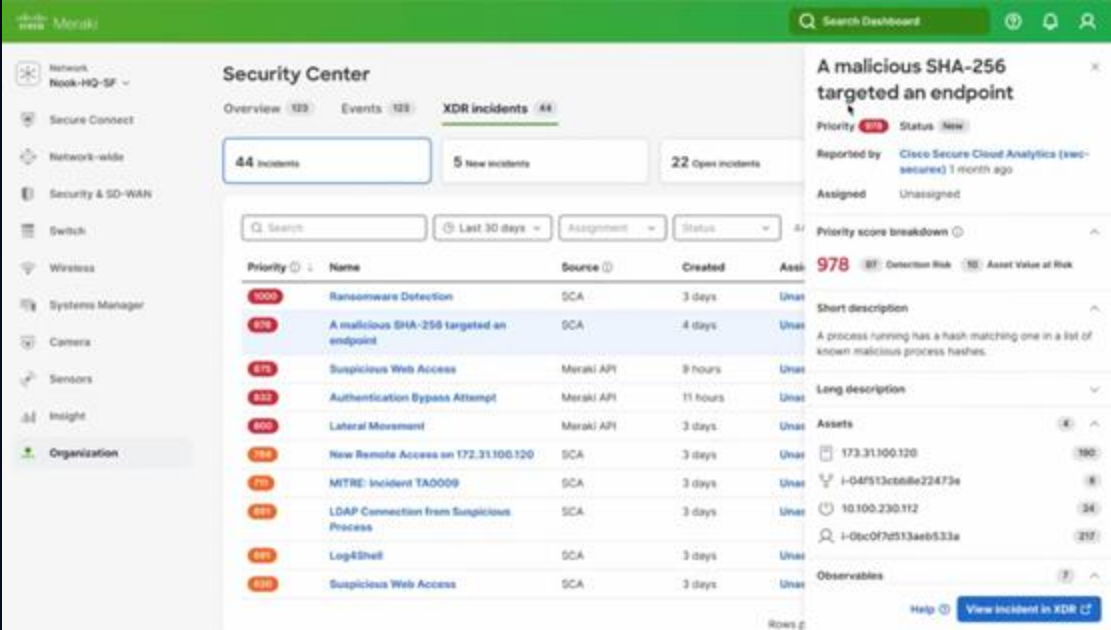
- Optimized network and security operations using native integration
- Network-first analytics enhances security coverage
- Faster threat response with a seamless user experience
- Enhanced threat detection by identifying network threats missed by EDR-focused tools

The screenshot displays the Cisco Meraki Security Center interface. The top navigation bar includes the Meraki logo, a search bar, and user profile icons. The left sidebar lists various network management categories: Network (Nook-HQ-SF), Secure Connect, Network-wide, Security & SD-WAN, Switch, Wireless, Systems Manager, Camera, Sensors, Insight, and Organization. The main content area is titled 'Security Center' and shows an overview of 44 incidents, 5 new incidents, 22 open incidents, and 41 unassigned incidents. Below this, there is a search bar and filters for 'Last 30 days', 'Assignment', and 'Status'. A table lists the incidents with columns for Priority, Name, Source, Created, Assigned, and Status.

Priority	Name	Source	Created	Assigned	Status
1000	Ransomware Detection	SCA	3 days	Unassigned	New
978	A malicious SHA-256 targeted an endpoint	SCA	4 days	Unassigned	New
875	Suspicious Web Access	Meraki API	9 hours	Unassigned	New
832	Authentication Bypass Attempt	Meraki API	11 hours	Unassigned	New
800	Lateral Movement	Meraki API	3 days	Unassigned	New
784	New Remote Access on 172.31.100.120	SCA	3 days	Unassigned	Open
711	MITRE: Incident TA0009	SCA	3 days	Unassigned	Open
691	LDAP Connection from Suspicious Process	SCA	3 days	Unassigned	Closed

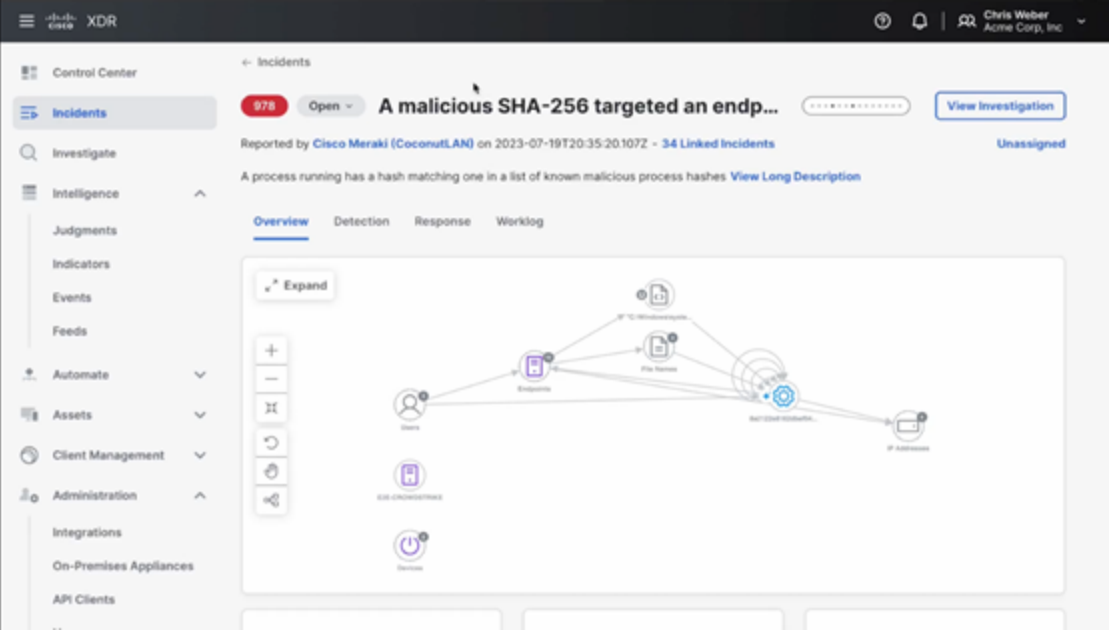
Meraki MX Integration in Cisco XDR

Leverage high-fidelity security incidents



MERAKI MX DASHBOARD

High-fidelity alerts are prioritized inside Meraki dashboard

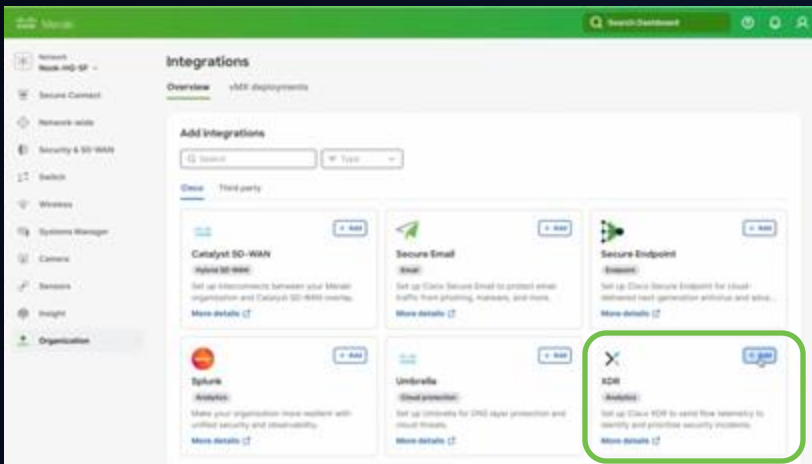


CISCO XDR DASHBOARD

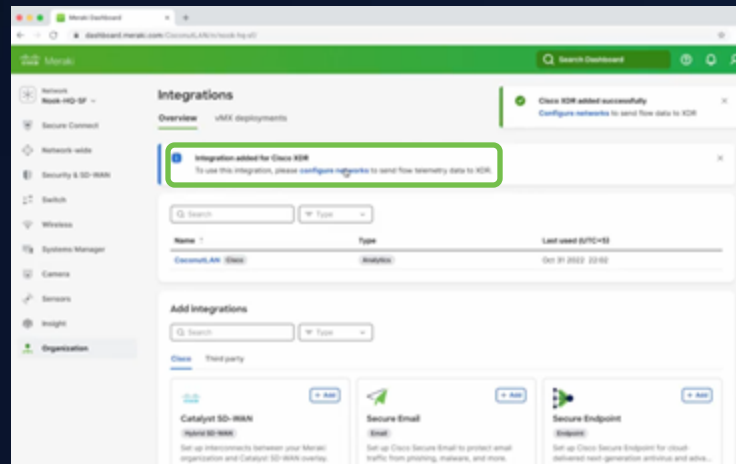
Network insights enriches Cisco XDR telemetry

Meraki MX Integration in Cisco XDR

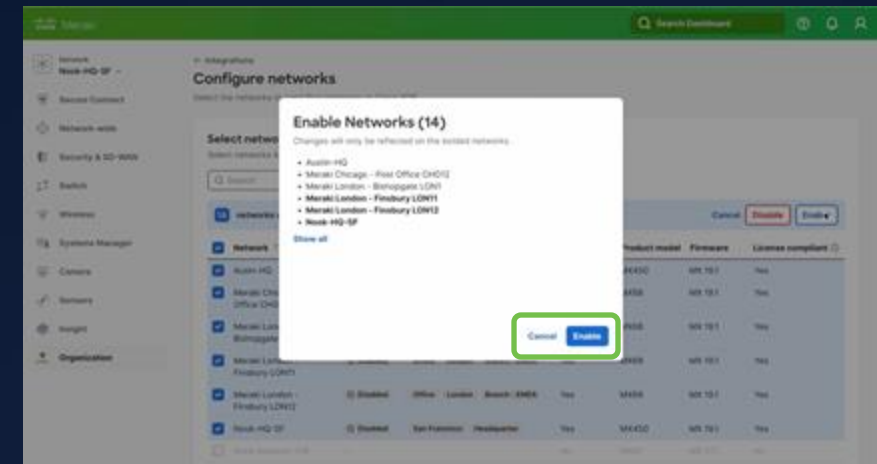
Set up in a few simple clicks



1 Add the Cisco XDR integration



2 Select networks to configure



3 Enable networks

ThousandEyes Assurance Integration



Assurance Overview Dashboard

Applications Fair 10 82/100 -2%

- Microsoft365** 1 issue 63/100 -21% last day
12 Estimated clients impacted
- Sharepoint** 100/100 No change
- Asana** 100/100 No change
- Salesforce** 100/100 No change
- Box** 100/100 No change

Microsoft365 12 est. clients impacted

- Internet** 12 est. impacted clients
- Application** No impacted clients

Applications enhanced by ThousandEyes

Accessed by this client only (in the past 2 hours)

- Microsoft365.com
- Salesforce.com
- Slack.acme.com
- Jira.acme.com
- Googlecloud.com

Show 3 more

All monitored for the entire network

Per-Application Health with active probing

Visibility beyond the WAN

Differentiate internet or application server issue

Integration with both network & single-client workflows

Single Client Dashboard

Current client connections

DONVO-M-9RGV — 6 — SFO12-S-AP21 — 18 — SFO12-WIFI32 — 8 — CORE1 — 7 — SFO12-MX1 — 16 — 88 — Applications

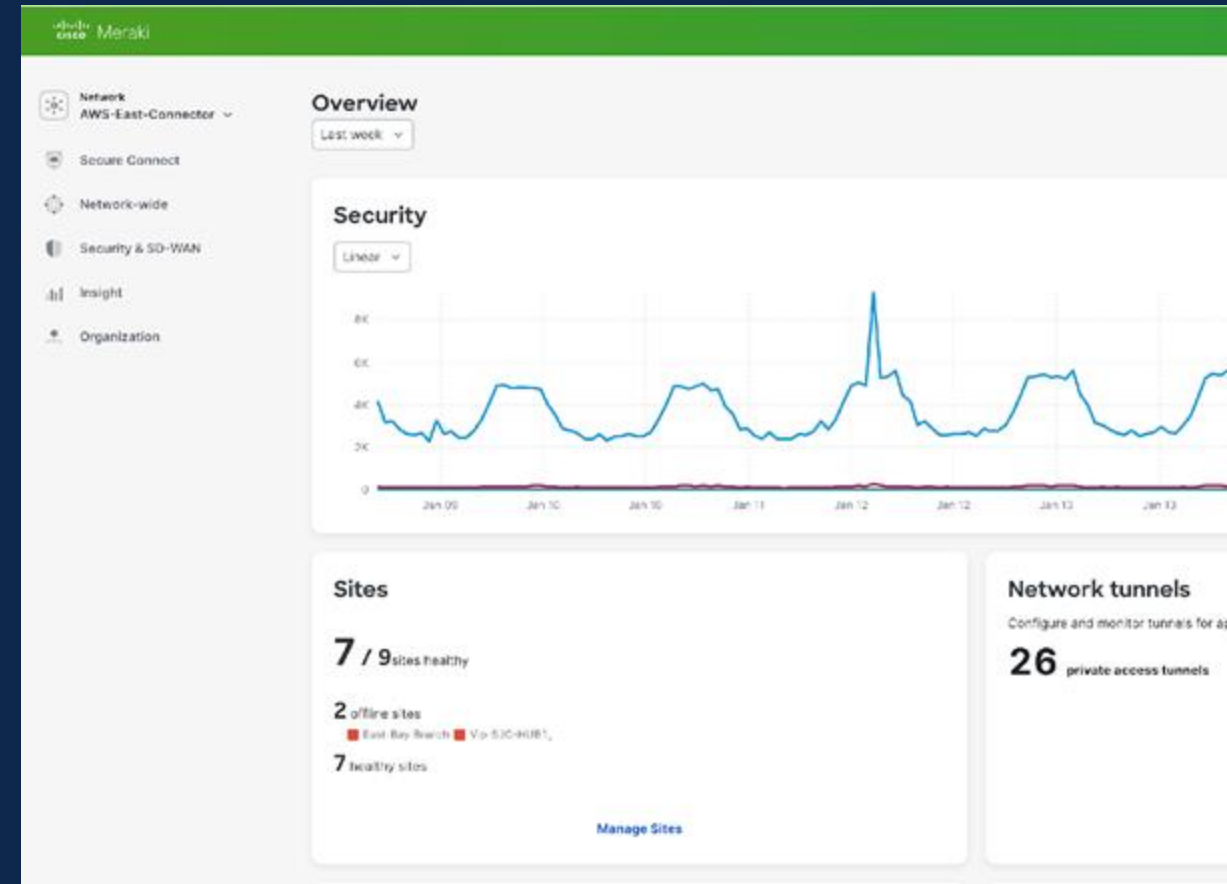


Centralized management for everything SASE

Simplified operations through consistent user experience

- SD-WAN management
- Site and remote user (new!) connectivity management
- Org-wide firewall policy management (new!)
- Posture management
- ZTNA management
- User and identity
- Logging (new!)
- APIs (new!)

Everything in a single dashboard



Centralized Management, Distributed Enforcement



The screenshot shows the Meraki management console for Firewall Policies. The page title is "Organization-wide Layer 7 Firewall Policies". Below the title, there is a brief explanation: "Organization rules apply across sites and cloud networks, allowing you to enforce security policies more efficiently. Organization rules are processed after local network rules." A link for "Organization-wide firewall policy documentation" is provided.

The main content area is titled "Rules" and contains a search bar, a "Filters" dropdown showing "0 results", and a "+ Add rule" button. Below this is a table header with columns: #, Status, Rule name, Action, Protocol, Source, Src Port, Destination, Dst Port, and Enforcements. The table is currently empty, displaying a large blue information icon and the text "No rules yet".

At the bottom of the page, there is a "Last login" section indicating the user logged in "about 2 hours ago" from their current IP address. It also shows "Current session started about 2 hours ago" and "Data for this organization is hosted in North America". A "Give your feedback" button is located in the bottom right corner.



Fastest path to SASE with MX + Secure Connect

Core capabilities	MX (on-prem)	Secure Connect (cloud)
WAN optimization and core routing	✓	✓
Content delivery/caching	✓	✓
Quality of service	✓	✓
SaaS acceleration	✓	✓
Threat intelligence	✓	✓
IDS/IPS	✓	✓
Malware protection	✓	✓
URL filtering	✓	✓
Visibility	✓	✓
SSL decryption	✓	✓
Firewall	✓	✓
Unified firewall policy engine		✓
Firewall-as-a-Service		✓
Data loss prevention (DLP)		✓
Zero trust network access (ZTNA)		✓
Cloud access security broker (CASB)		✓
VPN-as-a-service		✓
Unified SASE fabric		✓
End-to-end visibility, experience monitoring, optimization		✓
Single management console for SD-WAN/SSE functions		✓

 CISCO SECURE