

New England South MA, RI, CT

Account Team



Eric Shain
SMB Territory Manager
eshain@cisco.com
312 636 4494



Dario Loriato
Sales Acceleration
Manager
daloriat@cisco.com
678 352 2722



Michael Megless
Cisco Capital
mmegless@cisco.com

Security



Mustafa Megahed
Cloud Security Specialist
mmegahed@cisco.com



Megan Toune
Security Renewals
Specialist
mejarvis@cisco.com
984 216 4035

Meraki



Keith Giagnorio
Meraki Specialist
kgiagnor@cisco.com
408 894 7171
Boston Metro



Amy Allen
Meraki Specialist
amycalle@cisco.com
408 902 1790
MA, RI, Eastern CT

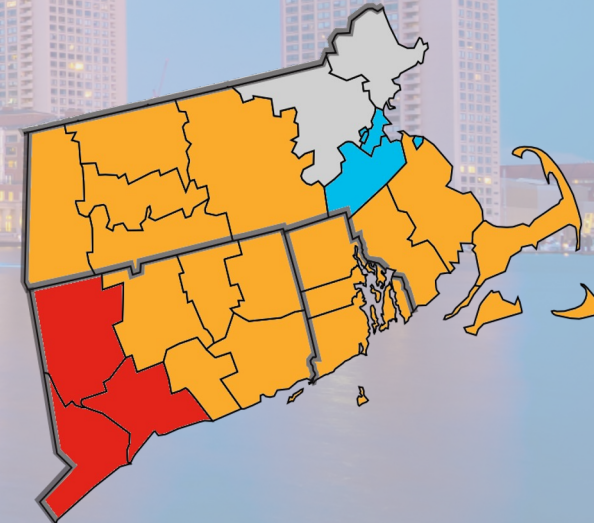


Monique Edmond
Meraki Specialist
medmond@cisco.com
415 865 3338
Western CT

Webex

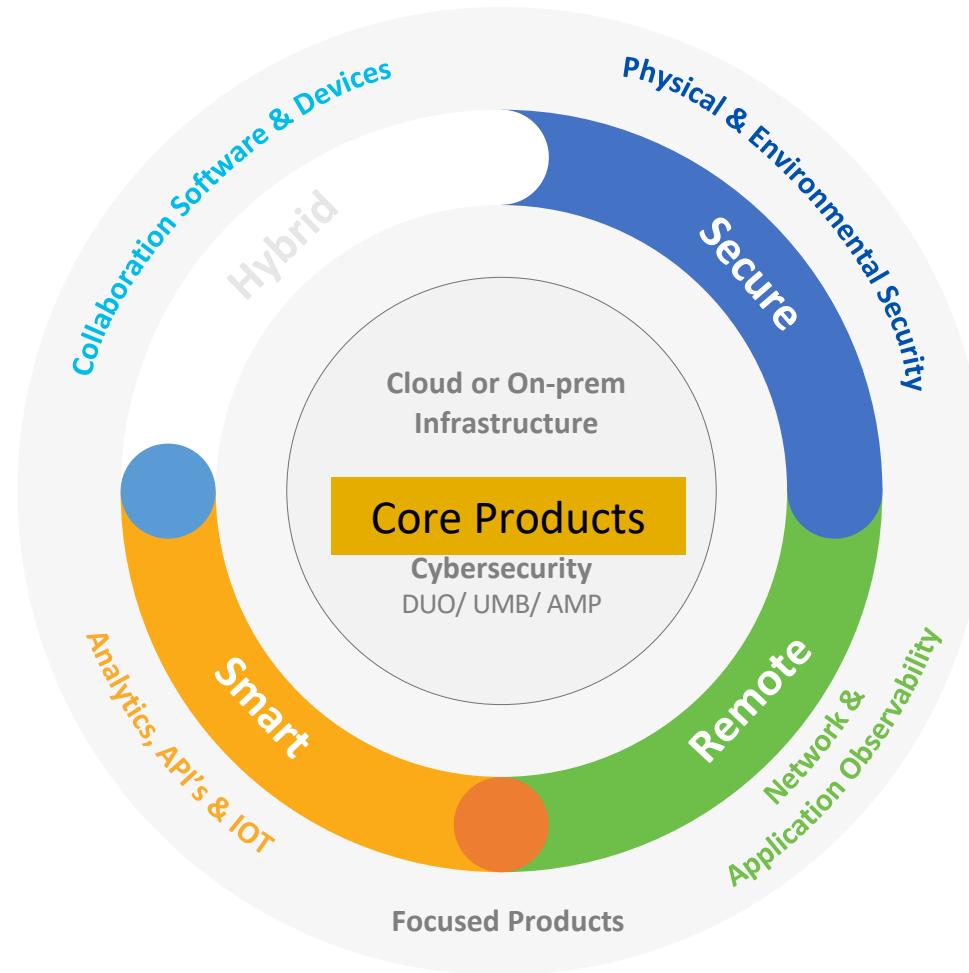


Ryan Robillard
Collaboration Specialist
ryrobill@cisco.com
508 939 5867



CISCO's SMB EXPERIENCES OUTCOMES

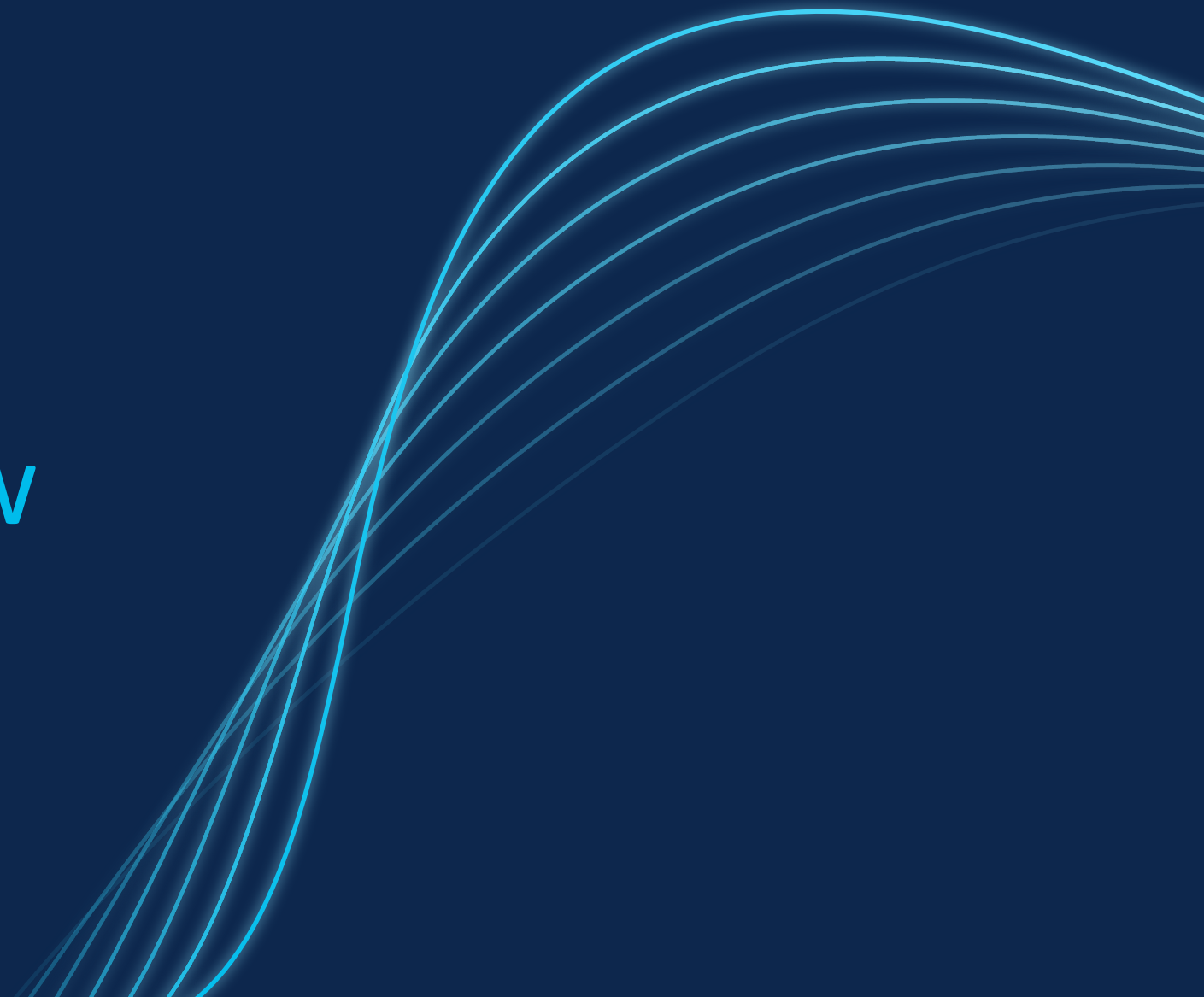
Empowered through combination of products from the Cisco SMB Portfolio





Security Overview

January 30, 2024





Lookout

COALFIRE

red canary

passbase

Prove

CHECKPOINT

FusionAuth

clearswi

proofpoint

sophos

ping Identity

deepwatch

KnowBe4

U410

hackerone

axio

paloalto

CROWDSTRIKE

HUNTRESS

GoGuardian

NowSecure

VARONIS

DARKTRACE

RAPID7

Multiple clouds makes tool sprawl worse

Software as a Service

Applications



Platform as a Service

Services



Infrastructure as a Service

Security

Network

Compute

Storage

Other Services

AZURE

AWS

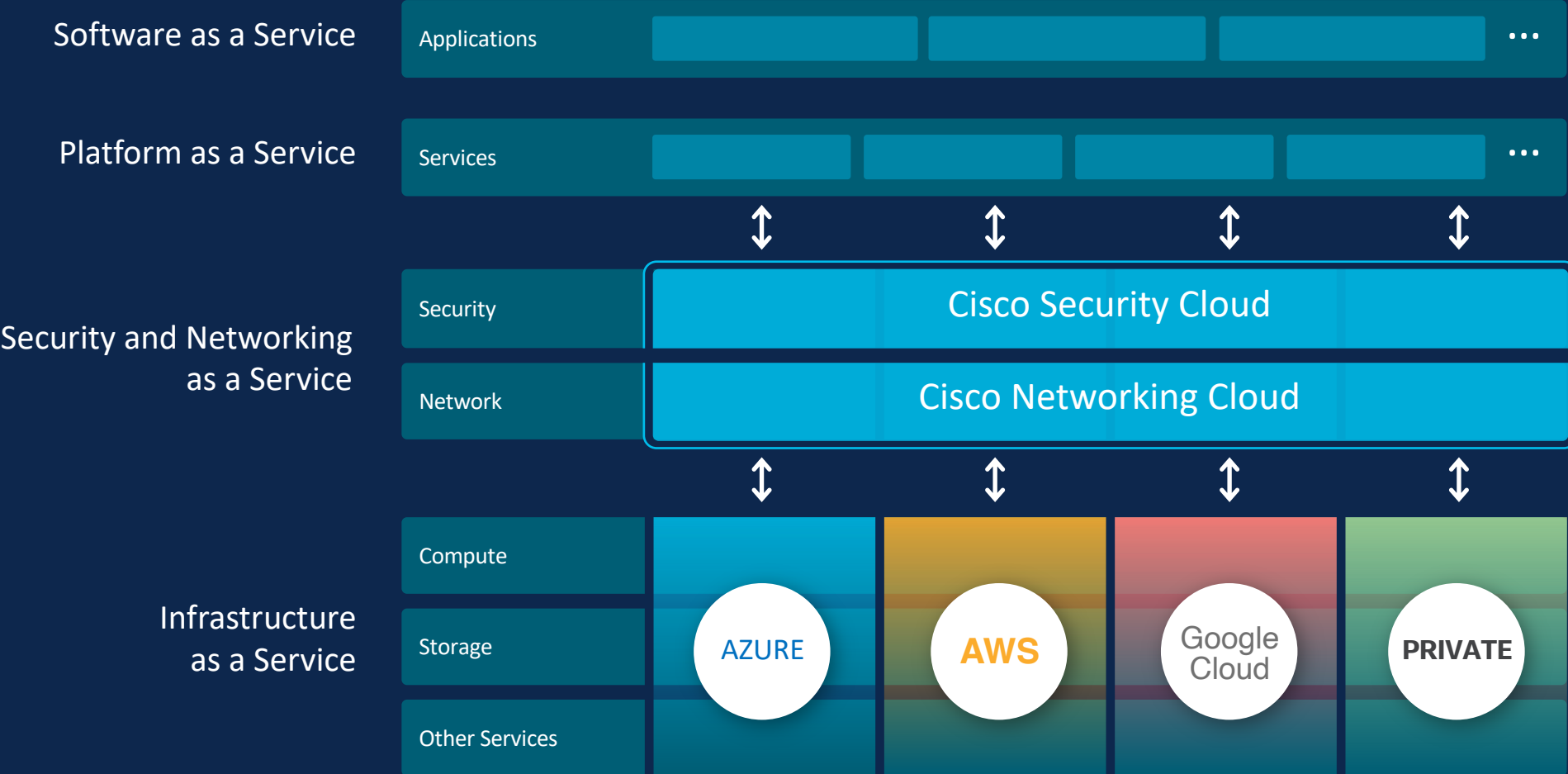
Google
Cloud

PRIVATE

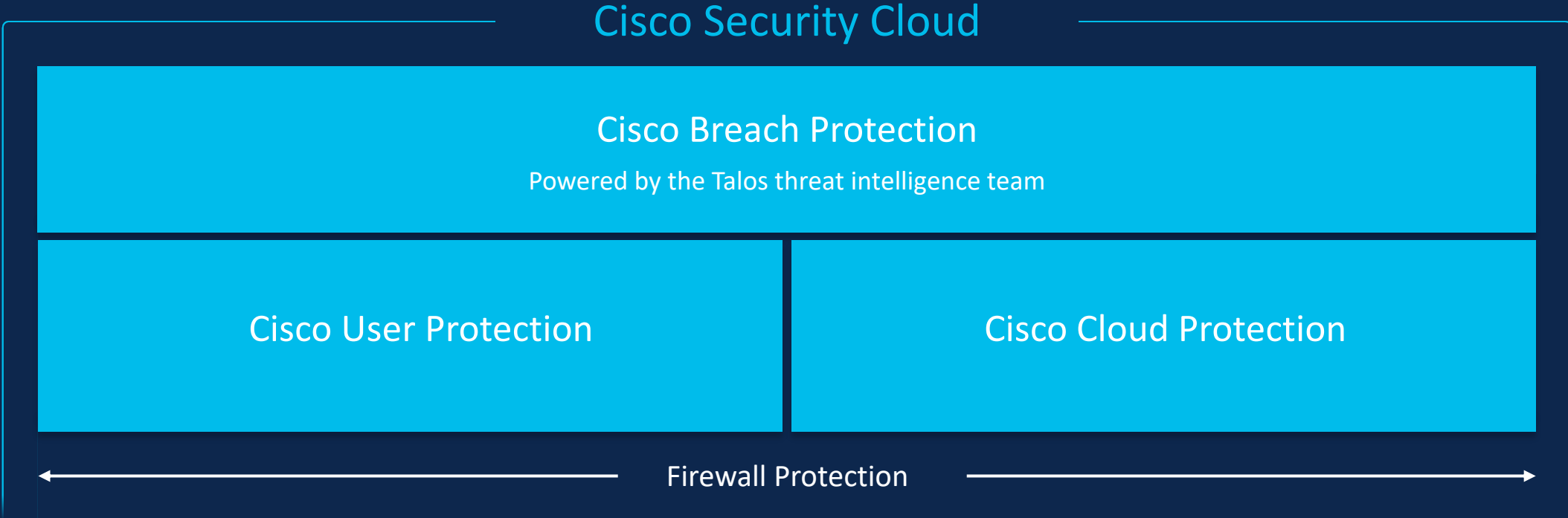


Different platforms, different controls

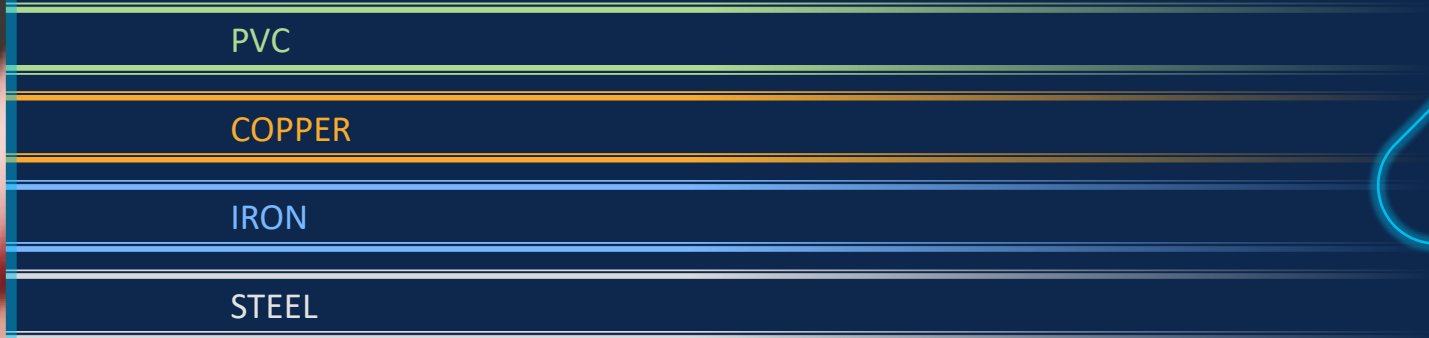
Cisco Security Cloud

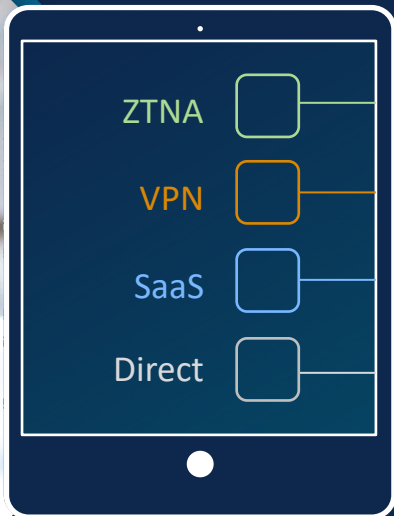


Security that only Cisco can deliver



User Protection





Private apps

Traditional apps

SaaS apps

Internet apps

STEP 1
Authenticate

STEP 2
Go to Work



- ZTNA
- VPN
- SaaS
- Direct

We handle the
plumbing

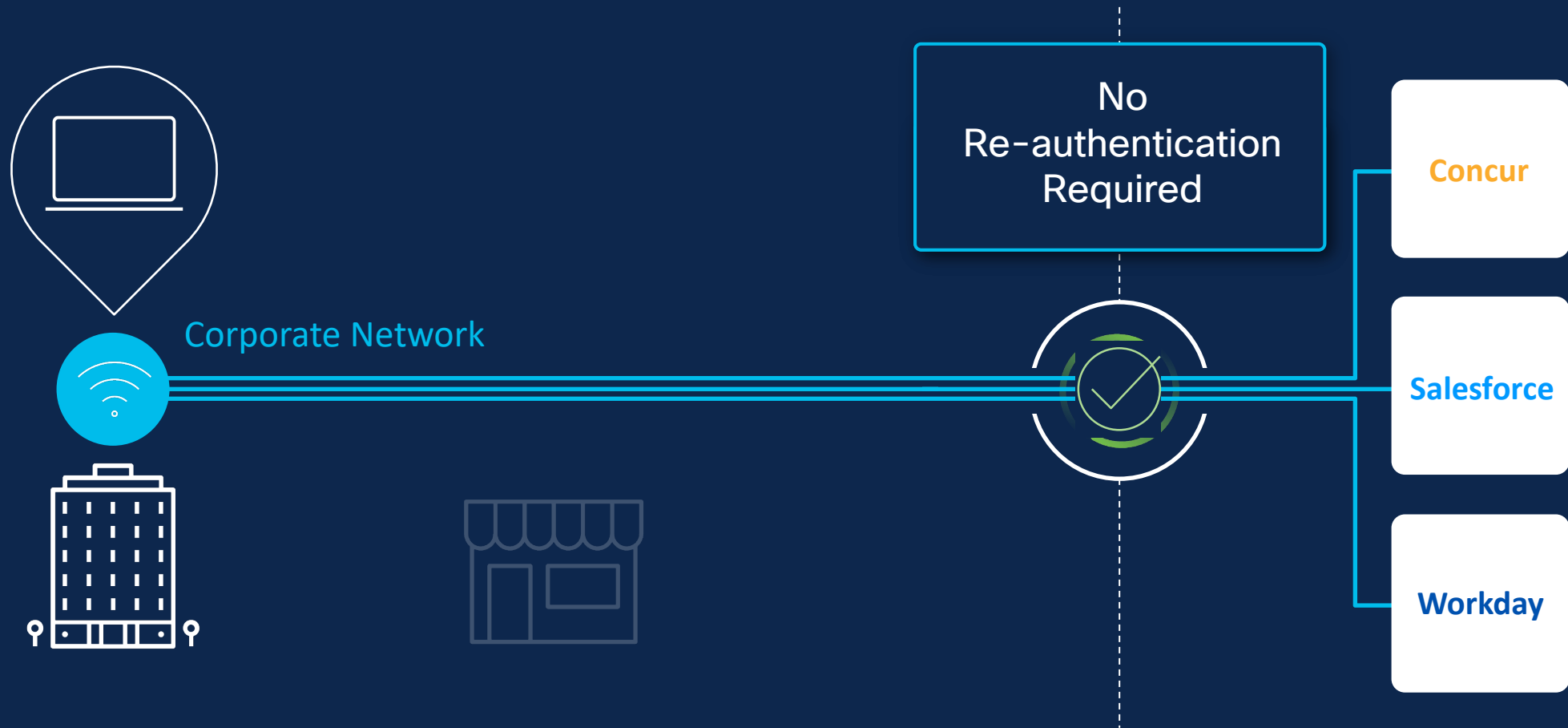
Private apps

Traditional apps

SaaS apps

Internet apps

Smooth and easy intelligent access



Smooth and easy intelligent access



Cisco ensures a great user experience



ThousandEyes



Client



WiFi



Broadband



Network



Application

Built into Cisco
SD-WAN

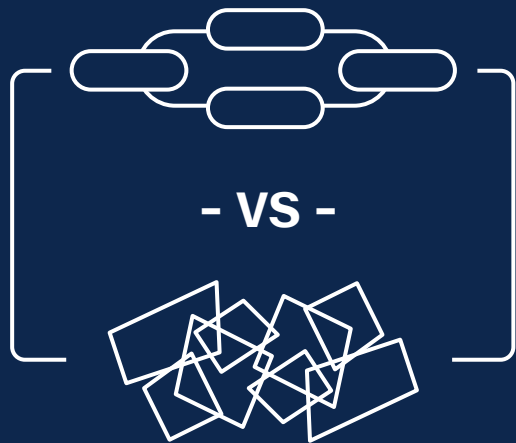
Robust, fault tolerant
global network

Target latency of ~40ms or
less for 99% of users

Built on industry leading
QUIC protocol

Less complexity, more visibility and control

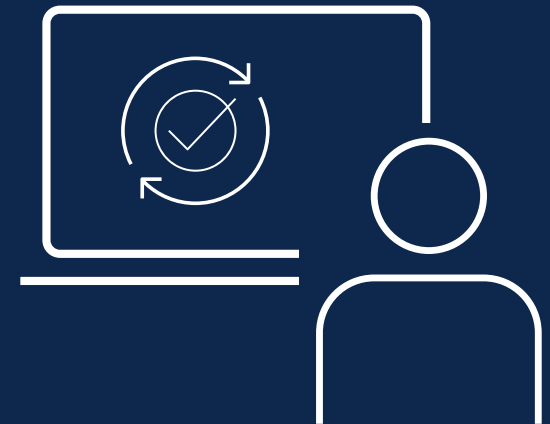
System vs. point solutions



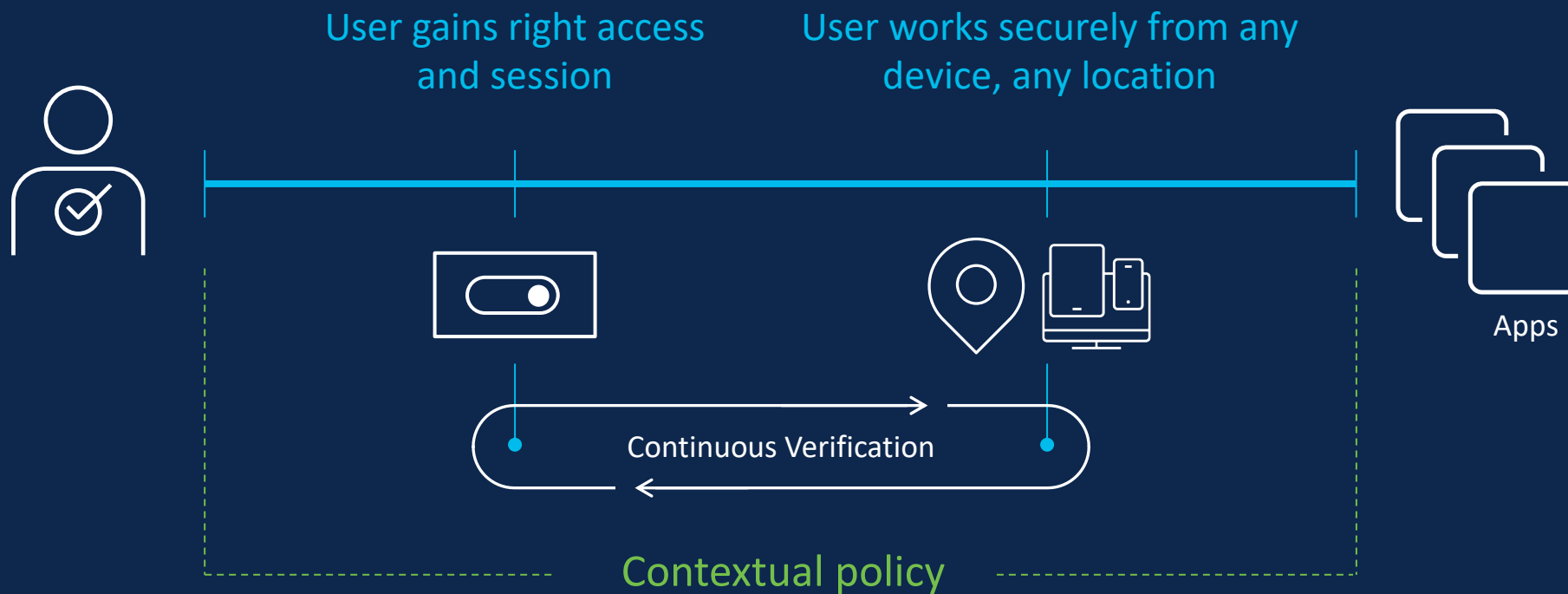
Unified dashboard and unified agent for SSE



Automation & self-service / self-remediation for user authentication



Never assume trust, continuously verify



The Cisco Advantage



Cisco Secure Access incorporates all pertinent security modules in one system delivering a more powerful outcome



Automation, self-service and self-remediation reduce IT burden



Only solution with continuous verification for all applications

Global General Availability Coming Soon

Enhance visibility and control

13X

less time to administer with Duo vs. other authentication solutions

90%

of authentication related cases to the help desk eliminated

Cisco User Protection Suite

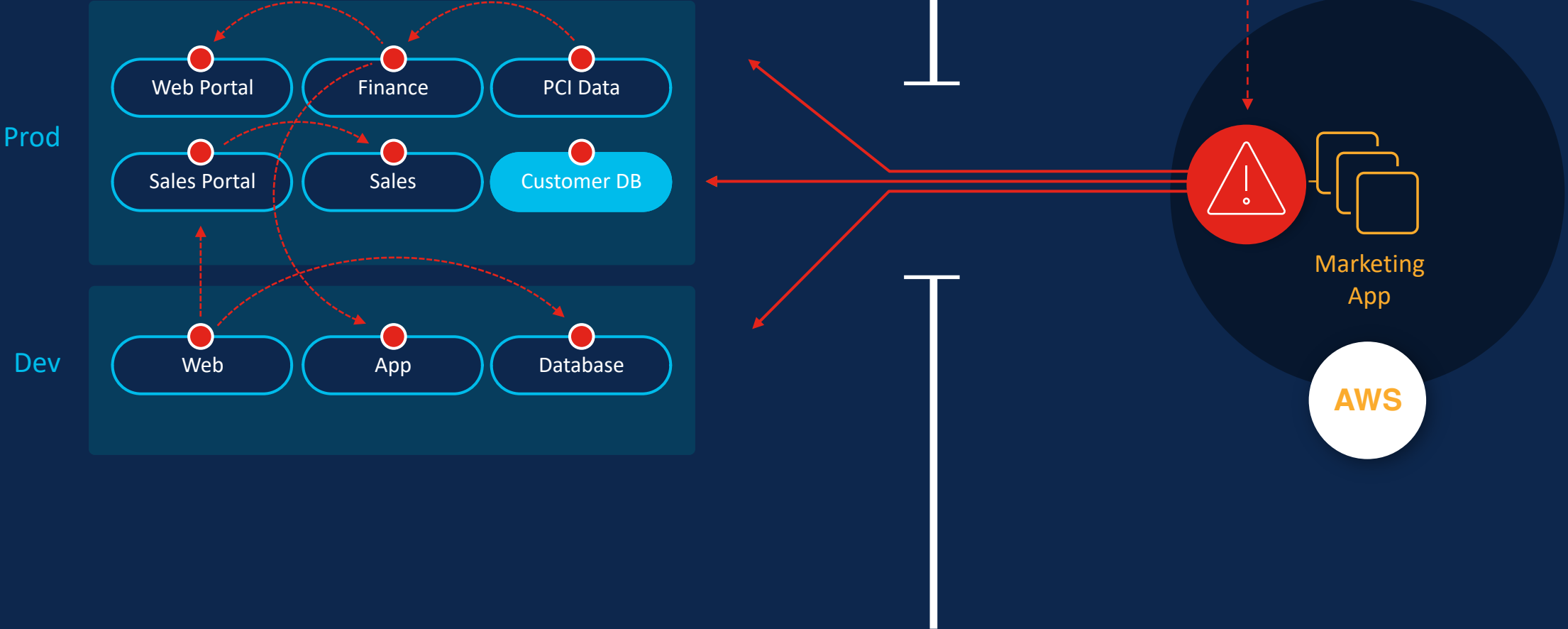


* Global General Availability Coming Soon

Cloud Protection



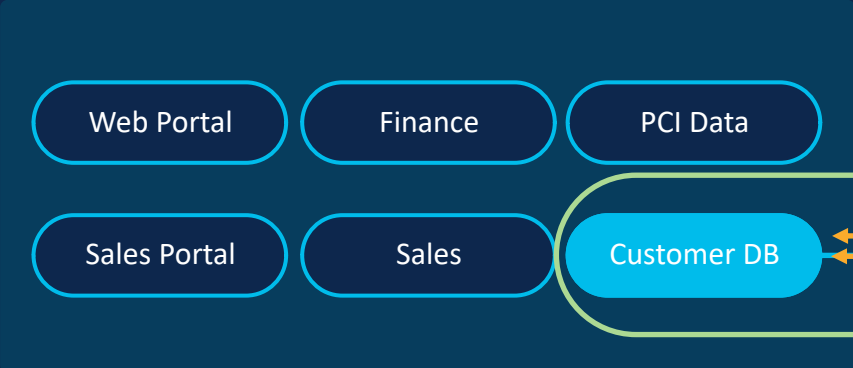
Private Cloud



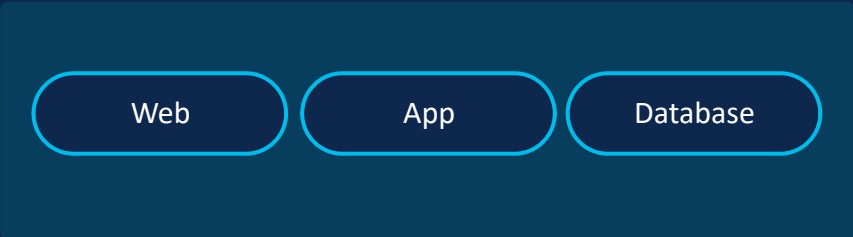
Private Cloud

Cisco
Understands

Prod



Dev



Zero Trust

Authorized Access Only

Marketing App

Google Cloud



AI help for creating and optimizing security policies

Policy Assistant

- Reduces security policy complexity
- Optimizes policy for efficacy & efficiency

The screenshot displays the Cisco Defense Orchestrator (DO) interface for configuring an Access Control Policy (ACP) in a production environment. The breadcrumb trail shows: Packets → Prefilter Rules → Decryption → Security Intelligence → Identity → Access Control → More. The page title is 'ACP - Production'. A search bar is present with 'Total 9 rules' and buttons for 'Add Category' and 'Add Rule'. A table lists the rules under the 'Default (1-9)' section:

Name	Action	Source				Destination				Applicability
		Zones	Networks	Ports	Dynamic Attributes	Zones	Networks	Ports		
Mandatory										
There are no rules in this section. Add Rule or Add Category										
Default (1-9)										
<input type="checkbox"/> 1 External	Block	Any	any-ipv4	~1 more	Any	Any	Any	Any	TCP_47001	Any
<input type="checkbox"/> 2 Internal	Allow	Any	any	~1 more	Any	Any	Any	Any	TCP_8302	Cisco
<input type="checkbox"/> 3 Block Malwares	Block	Any	any-ipv4	~1 more	Any	Any	Any	Any	Any	Tiny
<input type="checkbox"/> 4 Block Torrent	Block	Any	Germany	~8 more	Any	Any	Any	Any	Bit-torrent	Torre

Default Action: [Intrusion Prevention: Balanced Security and Con...](#)

The AI Assistant chat window on the right contains the following text:

AI Assistant

I'm trying to determine what rules are poorly written by analyzing the number of hits. Can you show me the rules with the least number of hits in the last 30 days?

AI Assistant 8:12 AM

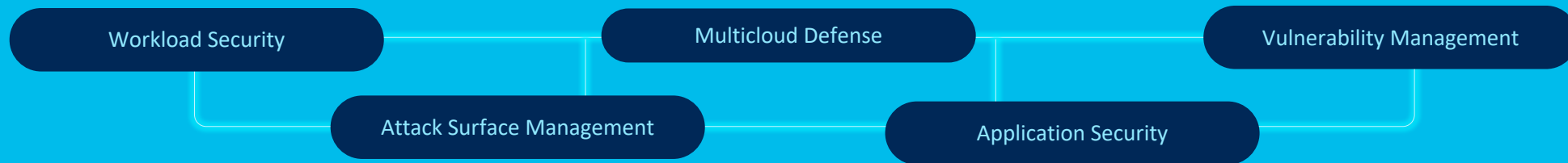
There are five access control rules with low hit counts in the last 30 days.

[View details](#)

[Regenerate](#)

Ask a question or request, or type "/" for suggestions

Cloud Protection Suite

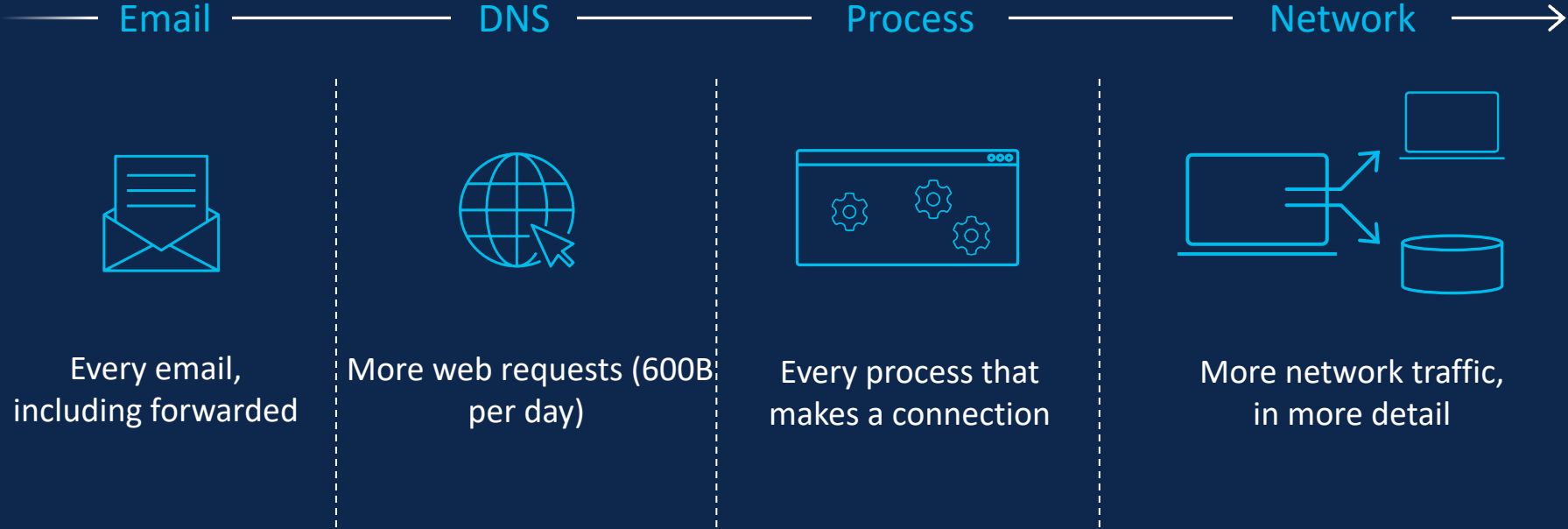


Breach Protection



Cisco XDR has the broadest native telemetry

Central data warehouse, analytics, and management in the Security Cloud



Talos powers the Cisco portfolio with intelligence

TALOS



500
threat researchers

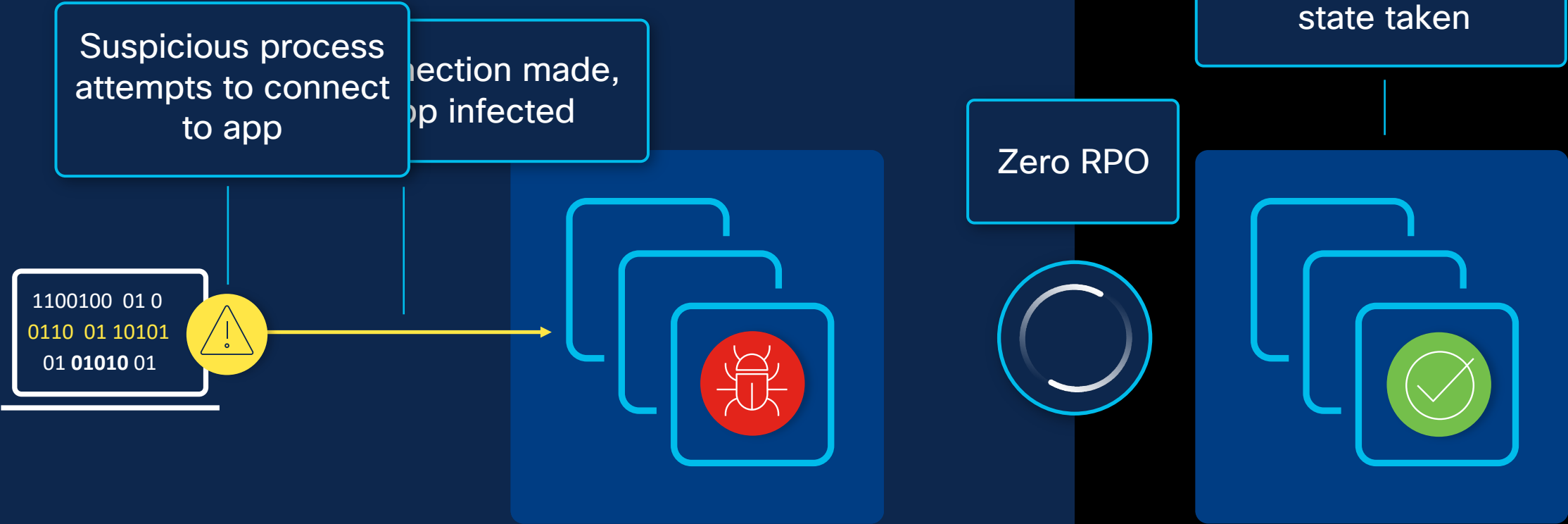


AI
powered algorithms



550B
security events observed daily

Accelerating ransomware recovery



AI help for the SOC analyst

SOC AI Assistant

- Summarizes incidents across domains
- Optimizes remediation tactics

The screenshot displays the Cisco XDR interface with an AI Assistant chat window on the left and incident details on the right.

AI Assistant Chat:

- Input: "this malicious file?"
- AI Assistant 8:30 AM: "Who are the owners associated with these endpoints?"
- User 8:30 AM: "What endpoints were affected by this malicious file?"
- AI Assistant 8:30 AM: "The following endpoints are associated with 4 user accounts that this malicious file was emailed to, and all contain multiple events."
- Endpoints listed: E2E-DataLake-Internet1, DESKTOP-2ER967Q, E2E-Win10-x64-G, Desktop-Win53.
- Remediation question: "How do you want to address this incident?"
- AI Assistant suggestion: "Quarantine the compromised systems."

Incident Details:

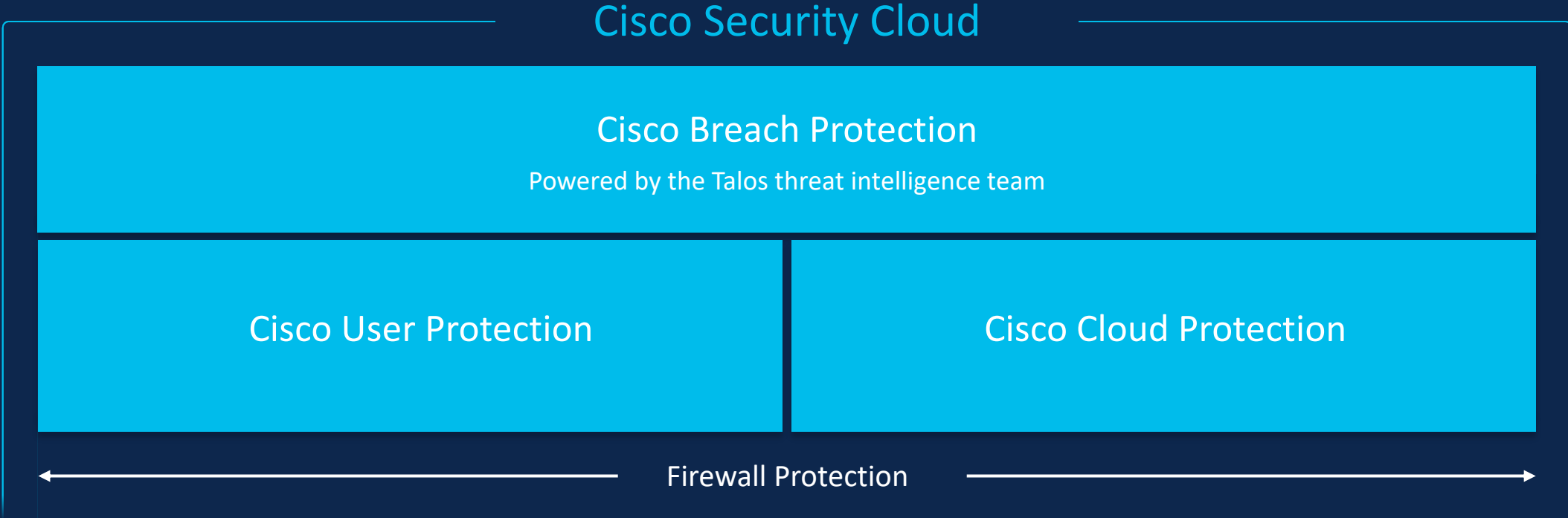
- Incident: Malicious Email Sent to Multiple Users (990)
- Reported by: Umbrella 2m ago - Linked Incidents
- Description: A device is involved in excessive malicious Command and Control communication, which is already flagged and blocked by Umbrella.
- Overview tabs: Overview, Detection, Response, Worklog
- Duration of the attack: 1d, 20h, 33m, 42s
- Graph showing relationships between endpoints, files, and assets.
- 50 Assets (TOP ACTIVE): E2E-DataLake-Internet1 (10 events), DESKTOP-2ER967Q (10 events), E2E-Win10-x64-G (10 events), Desktop-Win53 (10 events).
- 20 Observables (TOP ACTIVE): 263efd9cd65b9c2e9... (65 events), bfd9cd626359c2e9e... (65 events), 99.196.187.4 (23 events), 99.196.187.4 (12 events).

Breach Protection Suite

Extended Detection & Response

Ransomware Recovery

Security that only Cisco can deliver



MS Update

NEW Meraki Switches! CAT9300-M & MS130

NEW

Introducing MS130

Power more possibilities with next-generation Meraki access switches

Public Announcement
September 26th

MS130 orderability/FCS
September 19th



8 and 8P

1 GbE



8X and 12X

mGig +10G uplinks



24/24P and 48/48P

1 GbE



24X and 48X

mGig + 10G uplinks

Versatile and compact desktop switches

Powerful and full-size rack-mount switches



Boost throughput with cost effective **mGig** options



Connect all your devices with **PoE/PoE+** options

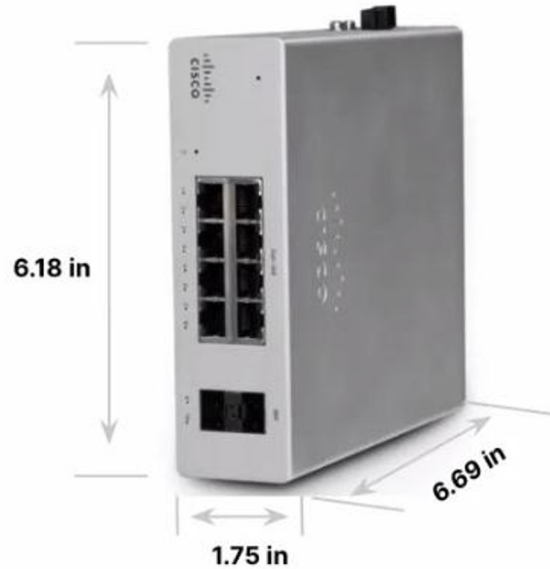


Manage it all in one **unified dashboard**

Extend the network with MS130R

MS130R orderability/FCS
FY24 Q2

Perfect for connecting outdoor access points, cameras, and other IoT devices in hot/cold/tight environments



Extend connectivity and power to wherever you need it

Power more use cases with 30 W PoE+, IP30 protection, and support from -40 °C to 70 °C.



Flexible mounting and power options

Mount via DIN rail, rack, or wall mount with multiple external power supply options.



One dashboard, any environment

Bring the powerful Meraki cloud-native platform to challenging environments.

Ideal for:



Drive-thru
menu boards



Parking
lots



Outdoor access
points and cameras



Hospitality and
entertainment



Outdoor
kiosks



Non-temperature
-controlled spaces



Pop-up
locations



Toll
booths

Please note: MS130 mGig (-X) models and MS130R are hardware-ready for the Adaptive Policy feature with a future firmware upgrade and advanced license.



Catalyst Meraki 9300 AT-A-GLANCE

When Simplification and Functionality Meet

It has never been easier to onboard and manage your Catalyst switch.

SIMPLE | SCALABLE | FLEXIBLE | SECURE



Simply powerful
Catalyst Meraki 9300



Catalyst Meraki 9300 gigabit

High-performing gigabit switches with optional modular uplinks/PoE/UPoE

Versatile switch designed for large campus networks.

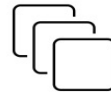


IMPROVED
Physical stacking

NEW
StackPower

Modular power supply

Get advanced networking without compromising operational efficiency and scalability



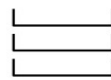
Modular uplinks

Get flexible hardware upgrades and easier management with hot-swappable uplink modules.



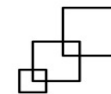
Wide range of mGig speeds

Address legacy infrastructure issues with PoE on all 24/48 ports, along with SFP and mGig.



StackPower

Create additional power capacity by pooling sources to power more PoE devices.



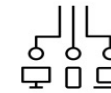
Improved physical stacking

Provide more throughput for Wi-Fi 6 and IoT, and get higher network resilience with up to 480 Gbps.



Adaptive Policy

Identify and enforce security policies of users, devices, and application with network based micro-segmentation.



60 W UPoE density

Power your smart space needs with UPoE and IEEE 802.3bt support.

Please note: Adaptive Policy feature requires Advanced licensing.

Catalyst Meraki 9300 multigigabit

High-performing UPoE mGig switch that enhances network performance for demanding enterprise environments

Unparalleled network performance and scalability for modern campuses, plus intent-based security with Adaptive Policy.



Meraki Subscription Licensing

Launched September 19, 2023!

What's launching

- Meraki Subscription Licensing
- Dashboard Management experience

Who's the target audience

New or renewing customers in the US and EU.

Note: Future releases will cover customers from other areas and that want to transition from their current Meraki license model.

The screenshot displays the Meraki Dashboard interface for a Corporate Subscription. The top navigation bar includes 'Demo Networks', 'Admin', and a search bar. The main content area is titled 'Subscriptions & License Info' and shows a 'Corporate Subscription' with an 'Active' status and a 'Modify' button. Below this, a 'Licenses' section provides a summary: Total 1,399, In Use 1,191 (85.2%), and Available 208 (14.8%). The dashboard is categorized into 'Security & SD-WAN', 'Switching', 'Wireless', 'Camera', and 'Environmental'. Three license categories are detailed: MS200 Large (115/120 in use, 5 available), MS300 Large (109/230 in use, 121 available), and MS300 Medium (50/100 in use, 50 available). A 'Details' sidebar on the right shows subscription ID, activation date (Jun 30, 2021), end date (Jun 30, 2028), and notes. A 'Networks' section lists three bound networks: New York HQ (34% / 473 Licenses), Philadelphia Office (29% / 408 Licenses), and Atlanta Office (22% / 310 Licenses). A 'Recent Changes' section lists three events: Environmental licenses added (Mar 4, 2022), Security licenses added (Mar 1, 2022), and Cloud Archive licenses added (Jan 30, 2022). The footer includes login information, copyright notice, and a 'Give your feedback' button.

Subscription Licensing: Simple and Flexible



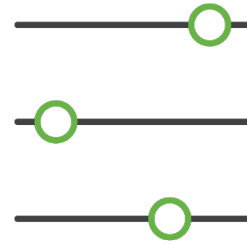
License management

Claiming is done only once in the lifecycle of a subscription



Simplified SKUs

More intuitive license options for streamlined deployments



Feature boundaries

Network-based licensing provides services where you need them most



Compliance

Only out of compliance devices affected

Licensing Model Feature Comparison

	Co-Term	Subscription
Common Expiration	Org	Org or Network
End Date	Dynamic	Fixed
Simplified SKUs	No	Yes
Multiple Feature Tier Support	No	Yes
Upgrades	Requires Loss of Time	Paid (Prorated)
License Key	Required for Origination, Additions and Renewals	Required for Origination Only
Payment Methods	Pre-Pay Only	Periodic or Pre-pay
Compliance	Org Shutdown	Network Mgmt Disabled <i>(License Expiration)</i> Device Mgmt Disabled <i>(Exceeding Limit)</i>



Subscriptions launch

- For new & renewing EU/US customers

What's Launching

- New subscription orderability
- Dashboard subscription experience
- Simplified SKUs
- Ability to cancel inline with Meraki's return policy

What's Launching

- Ability to grow size of subscription and add upgrades (ex: advanced tier features)

What's Launching

- Ability to migrate from Co-Term Licensing to a Subscription model mid-term
- Renewals & Extensions

