

Secure Connectivity for the AI-Ready Enterprise

The Complete Story

Joe Rubino, Secure Routing, SASE SE

Antonio Hurtado, CISSP – Security SE – Southeast US



Reimagine networking with innovative SD-WAN

Simpler

Simplified networking that
is scalable and efficient

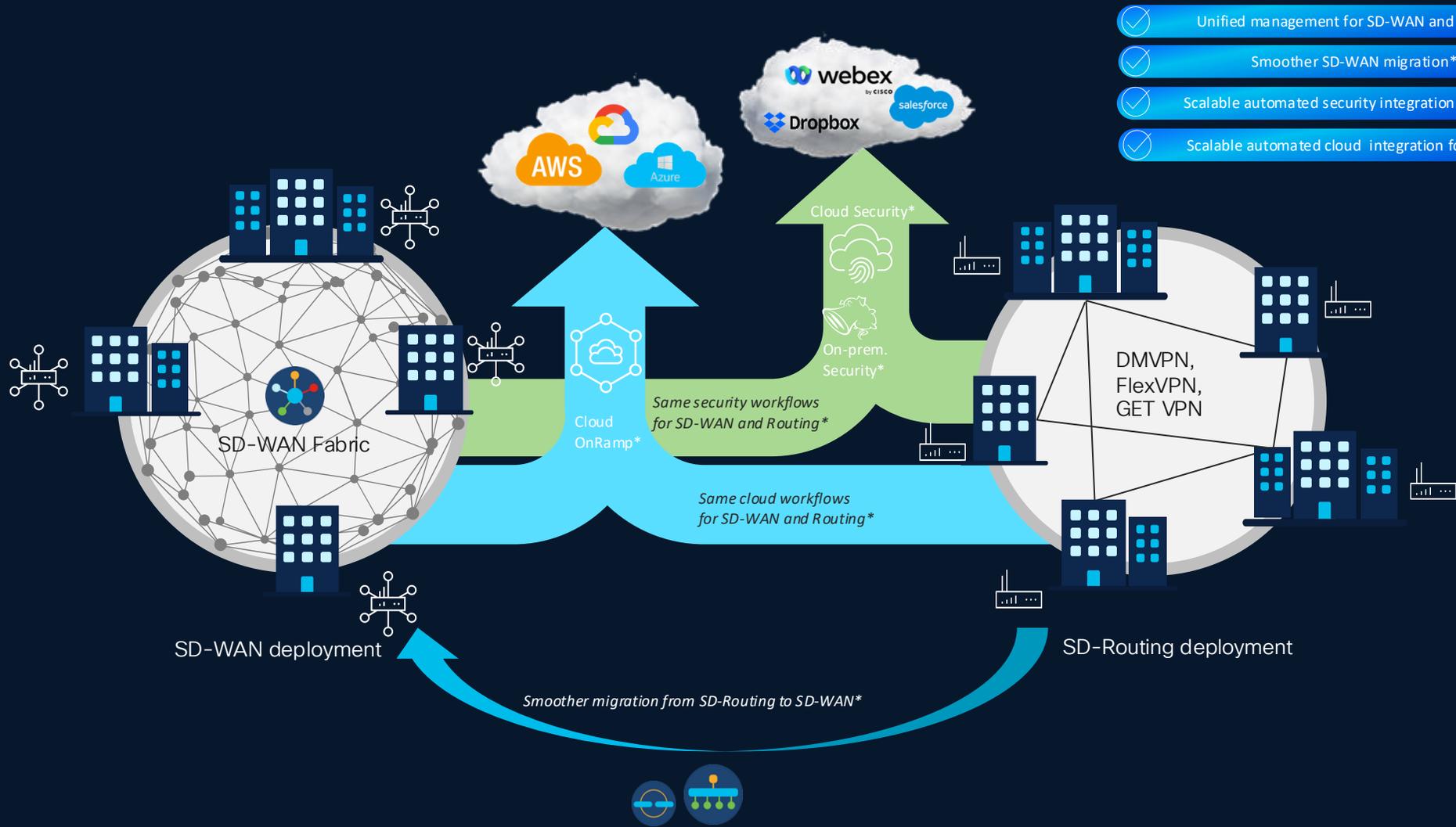
Smarter

AI powered capabilities that
power end-to-end visibility

Safer

Security integrations designed to
be SASE-ready and always-on

Unified Management: SD-WAN and SD-Routing



- ✓ Unified management for SD-WAN and Routing
- ✓ Smoother SD-WAN migration*
- ✓ Scalable automated security integration for Routing*
- ✓ Scalable automated cloud integration for Routing*

SD-WAN Manager (UI)

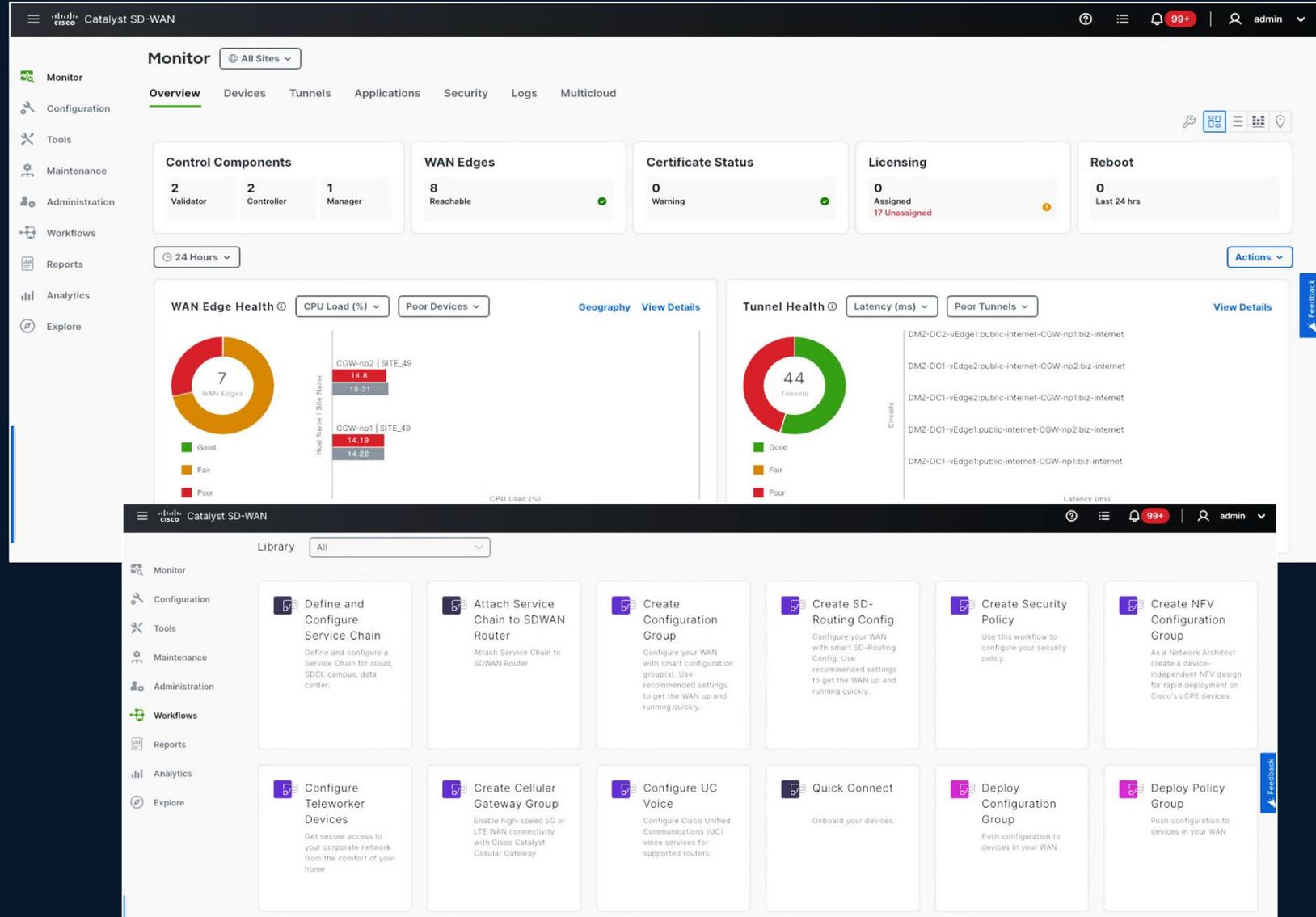
 **Enhanced UI**

 **Guided Workflow**

 **Simplified Configuration**

 **Granular Management**

 **Smart Troubleshooting**



The screenshot displays the Cisco Catalyst SD-WAN Manager interface, divided into two main sections: Monitor and Library.

Monitor Section:

- Control Components:** 2 Validator, 2 Controller, 1 Manager.
- WAN Edges:** 8 Reachable.
- Certificate Status:** 0 Warning.
- Licensing:** 0 Assigned, 17 Unassigned.
- Reboot:** 0 Last 24 hrs.
- WAN Edge Health:** 7 WAN Edges. Legend: Good (Green), Fair (Yellow), Poor (Red). Data table:

Host Name / Site Name	CPU Load (%)
CGW-np2 SITE_49	14.8
	15.31
CGW-np1 SITE_49	14.19
	14.22
- Tunnel Health:** 44 Tunnels. Legend: Good (Green), Fair (Yellow), Poor (Red). List of tunnels:
 - DMZ-DC2-vEdge1:public-internet-CGW-np1:biz-internet
 - DMZ-DC1-vEdge2:public-internet-CGW-np2:biz-internet
 - DMZ-DC1-vEdge2:public-internet-CGW-np1:biz-internet
 - DMZ-DC1-vEdge1:public-internet-CGW-np2:biz-internet
 - DMZ-DC1-vEdge1:public-internet-CGW-np1:biz-internet

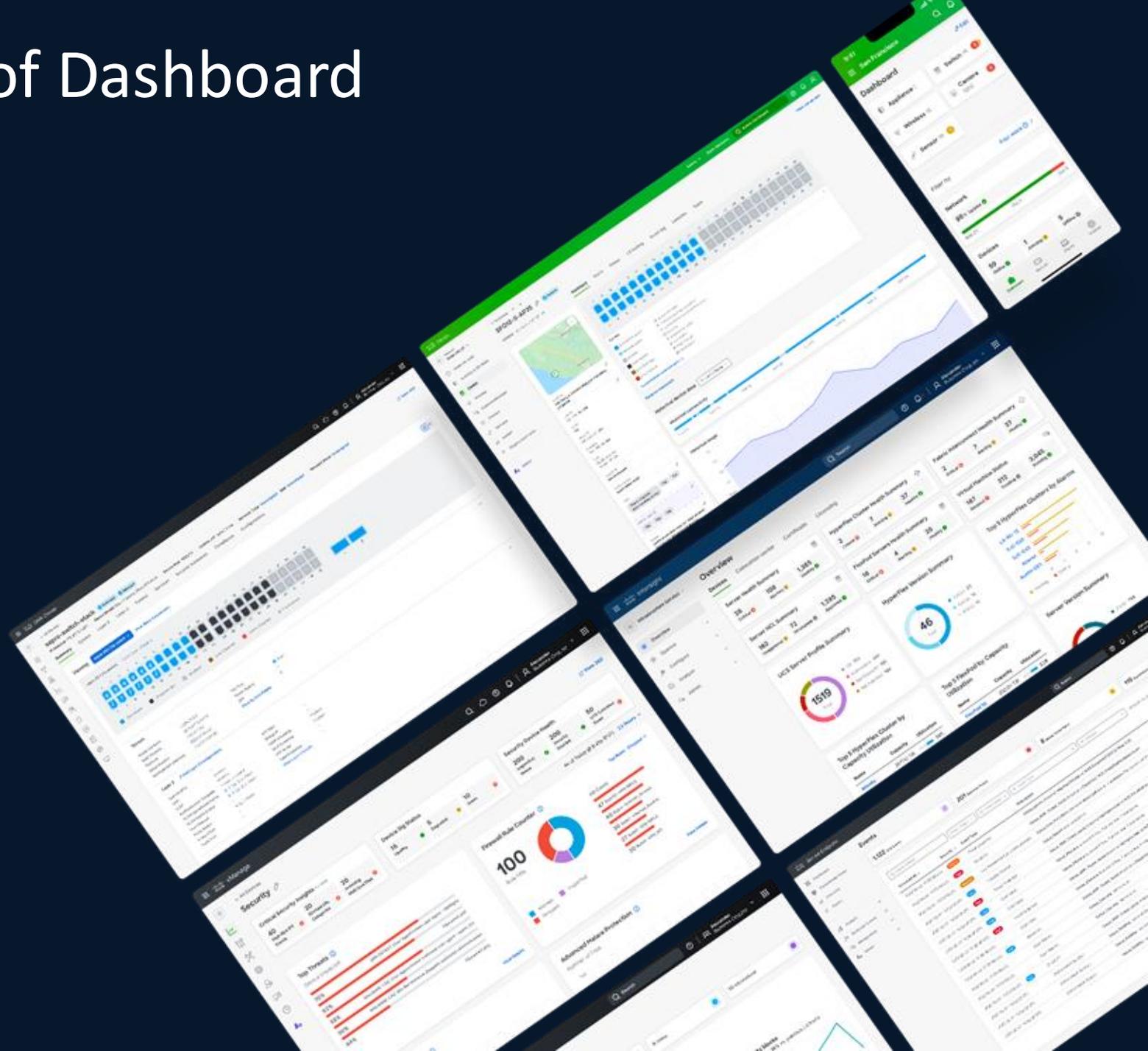
Library Section:

- Define and Configure Service Chain:** Define and configure a Service Chain for cloud, SD-CI, campus, data center.
- Attach Service Chain to SDWAN Router:** Attach Service Chain to SDWAN Router.
- Create Configuration Group:** Configure your WAN with smart configuration group(s). Use recommended settings to get the WAN up and running quickly.
- Create SD-Routing Config:** Configure your WAN with smart SD-Routing Config. Use recommended settings to get the WAN up and running quickly.
- Create Security Policy:** Use this workflow to configure your security policy.
- Create NFV Configuration Group:** As a Network Architect create a device-independent NFV design for rapid deployment on Cisco's uCPE devices.
- Configure Teleworker Devices:** Get secure access to your corporate network from the comfort of your home.
- Create Cellular Gateway Group:** Enable high-speed 5G or LTE WAN connectivity with Cisco Catalyst Cellular Gateway.
- Configure UC Voice:** Configure Cisco Unified Communications (UC) voice services for supported routers.
- Quick Connect:** Onboard your devices.
- Deploy Configuration Group:** Push configuration to devices in your WAN.
- Deploy Policy Group:** Push configuration to devices in your WAN.

Common Look and Feel of Dashboard

Unified experience across Networking and Security dashboard

- Catalyst Center
- Catalyst SD WAN
- Cisco Security Cloud
- Meraki
- Spaces
- ISE
- Intersight



Simplifying WAN management for the complex, distributed enterprise



Multi-Region
Fabric (MRF)



Multi-tenant
Edge



Cloud
On-ramp

What does it do?

Simplify and segment large-scale, geographically distributed networks with a central core

Securely and efficiently manage multiple tenants on a shared SD-WAN infrastructure

Simplifies and automates secure, optimized connectivity between on-premises and cloud environments

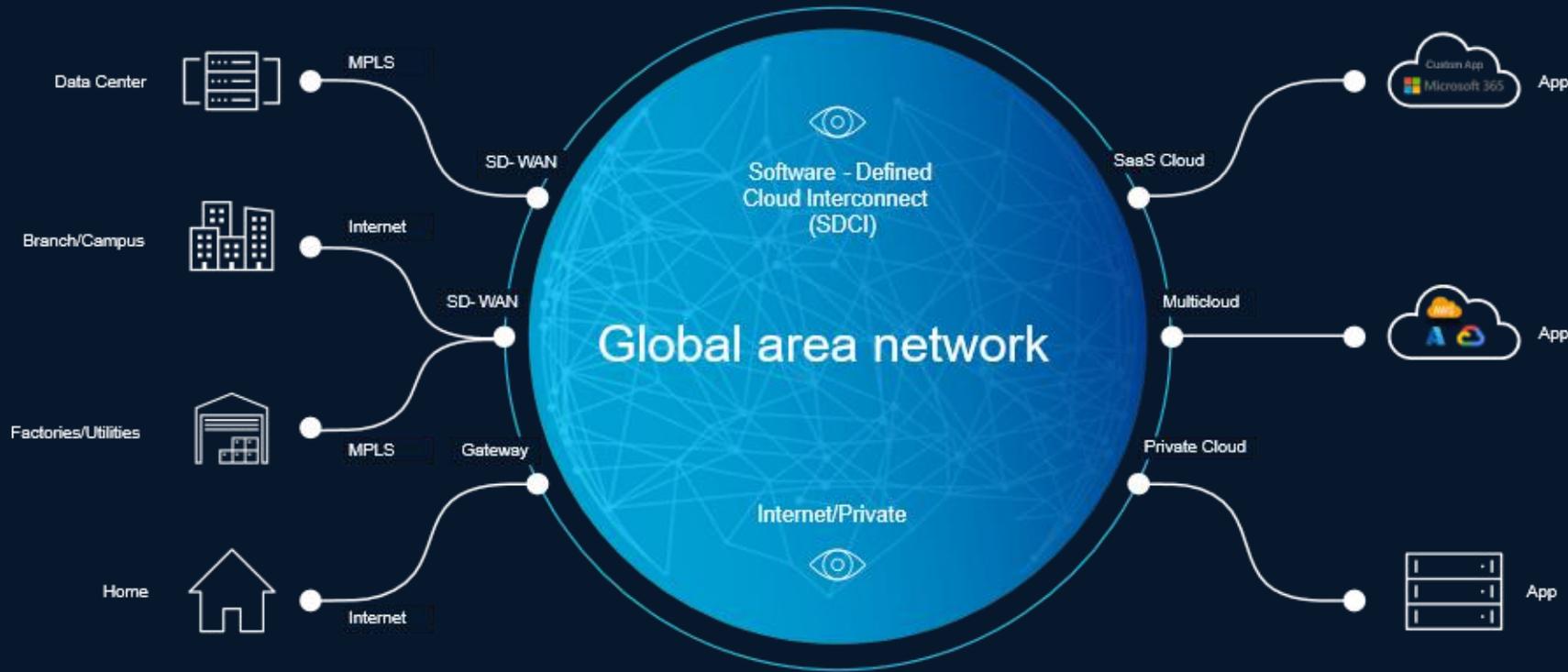
What is the value?

Operational simplification, enhanced security, scalability, and improved performance across multiple regions

Reduces costs, improves operational efficiency, and provides tenant-specific control and visibility for multi-customer environments

Accelerates multicloud connectivity made easy for better user experiences, simplified operations, and strengthened security across hybrid environments

Cloud OnRamp: Making cloud easy for the hybrid world



- Optimized SaaS experience
- Simple, automated SD-WAN extension to the cloud
- Integrated middle-mile backbones
- Built-in, cloud-based security

Automated connectivity, discovery, and optimization for any cloud

Reimagine networking with innovative SD-WAN

Simpler

Simplified networking that is scalable and efficient

Smarter

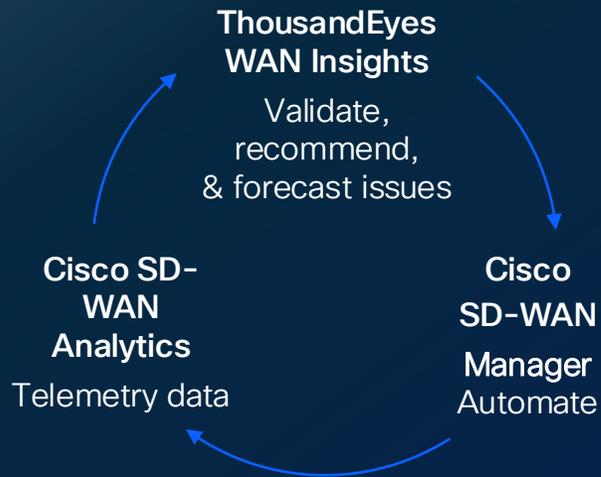
AI powered capabilities that power end-to-end visibility

Safer

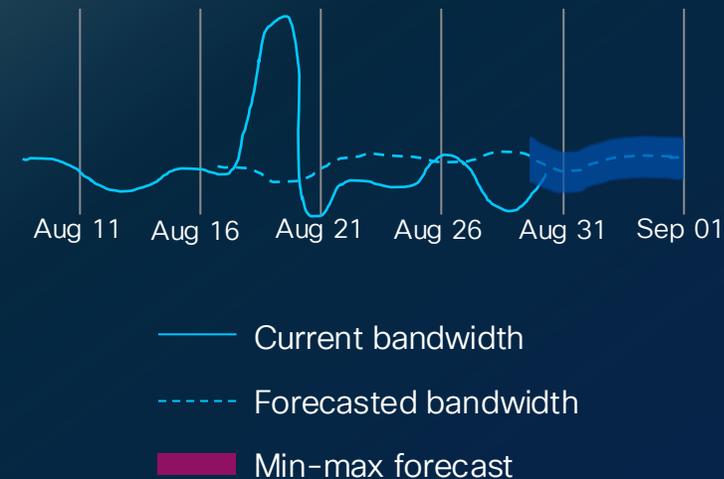
Security integrations designed to be SASE-ready and always-on

AI-native Network operations

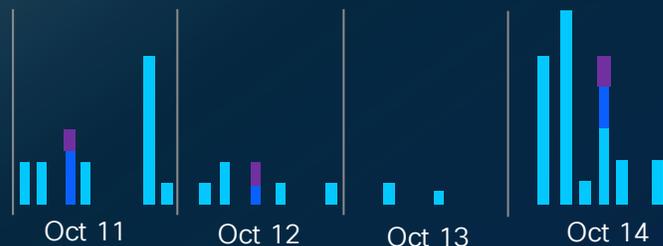
Predictive Path Recommendations



Bandwidth Forecasting

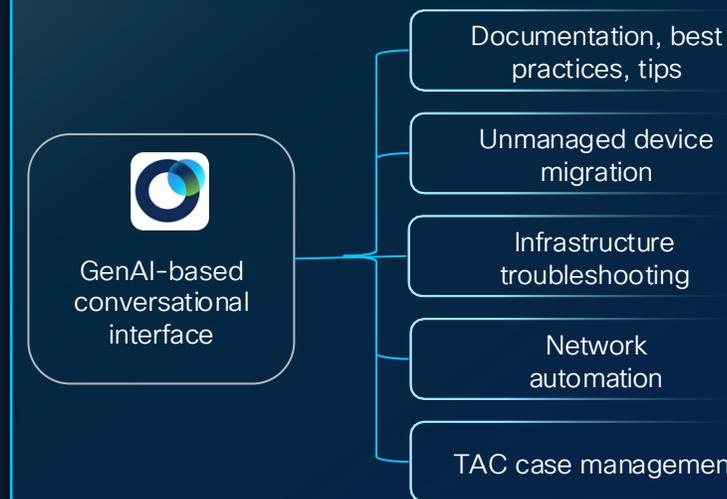


Anomaly detection



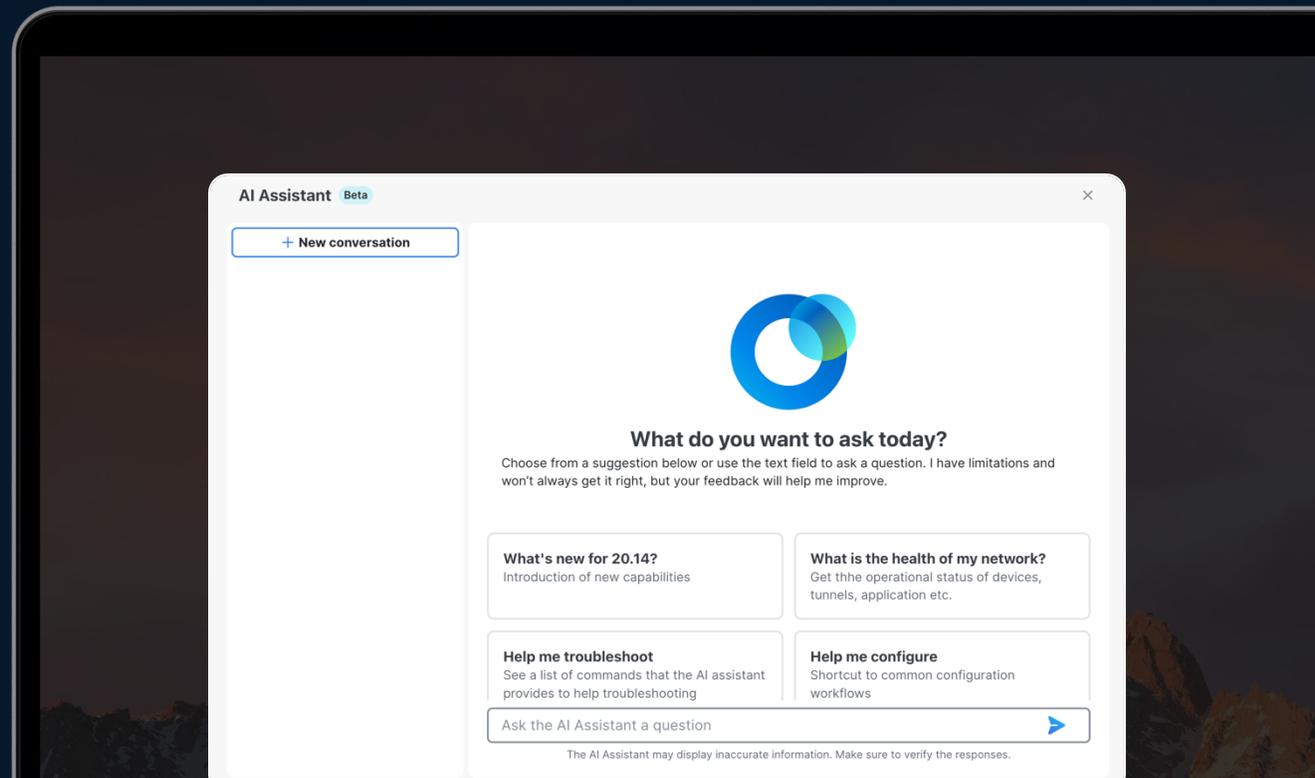
KPI	Detected	Rate	# sites
Loss	28	2.34	7
Latency	0	0	0
Jitter	0	0	0

Cisco AI Assistant



Using AIOps to streamline day-2 operations

Proactively optimize network and application performance to achieve higher operational efficiency

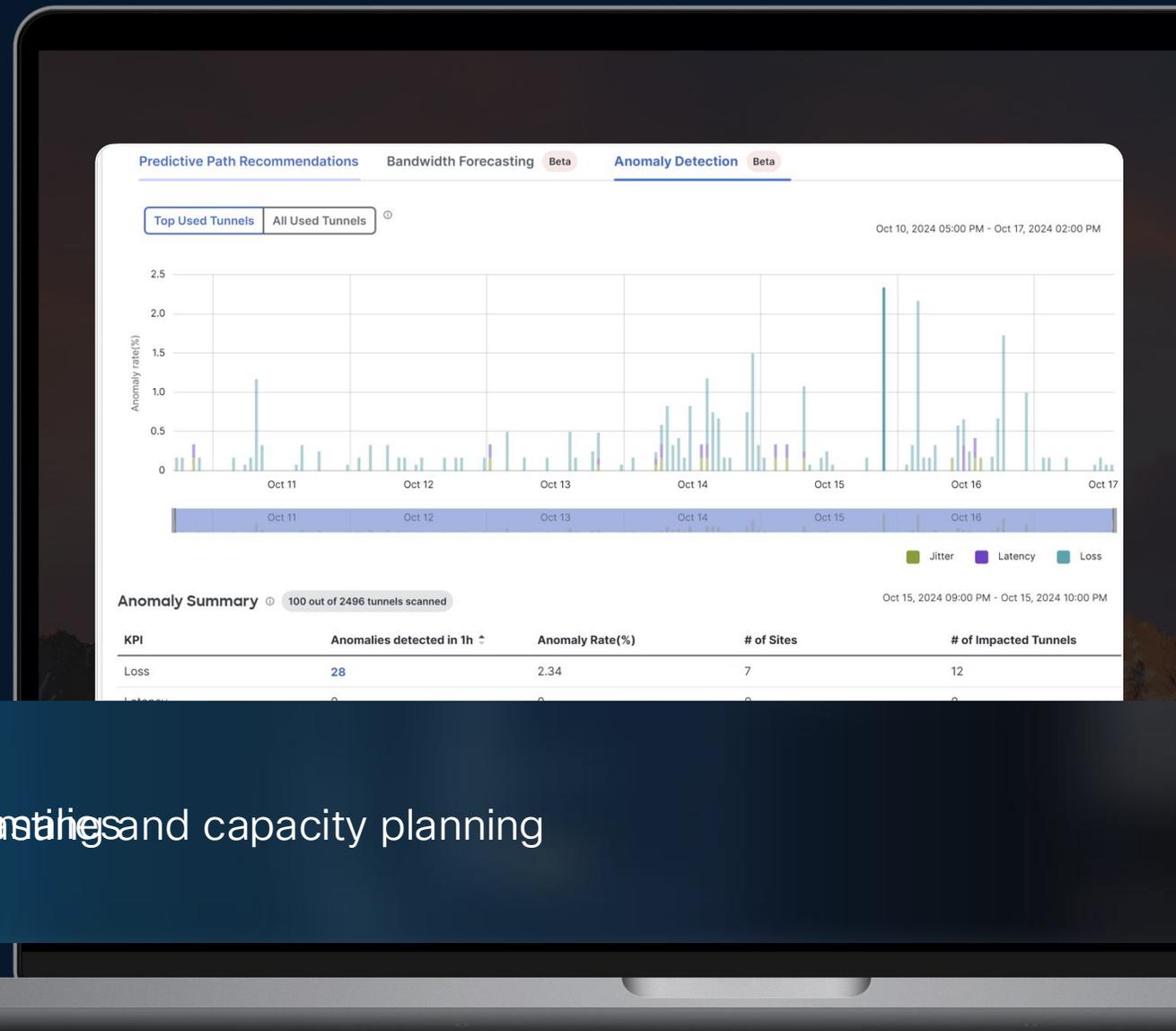


Predictive Path
AI Assistant
Recommendations

Proactive network and application performance monitoring and optimization using AI Assistant (Gen AI)

Using AIOps to streamline day-2 operations

Mitigate issues **before** they impact performance along with root cause analysis to reduce MTTR



Bandwidth
Forecasting

AI/ML based forecasting and capacity planning

Proactively stay ahead of threats

Actionable insights on **Security Advisories** and **Field Notices** applicable to your SD-WAN fabric

The screenshot displays a Cisco SD-WAN security dashboard. A modal window is open, showing details for advisory ID **C8K-2CA9CB26-5E57-1D1E-14ED-101F49488C00**. The modal includes a search bar, a 'Download' button, and a table of affected advisories. The background dashboard shows a list of advisories with columns for 'Affected advisory', 'Potentially affected ad', and 'Last scanned'.

Advisory ID	Advisory title	CVSS score	Severity
cisco-sa-caf-3dXM8exv	Cisco IOx Application Framework Arbitrary File Creation Vulnerability	8.1	High
cisco-sa-c9300-spi-ace-yejYgnNQ	Cisco IOS XE Software for Cisco Catalyst 9300 Series Switches Secure Boot Bypass Vulnerability	6.1	High
cisco-sa-ratenat-pYVLA7wM	Cisco IOS XE Software Rate Limiting Network Address Translation Denial of Service Vulnerability	8.6	High

Reimagine networking with innovative SD-WAN

Simpler

Simplified networking that is scalable and efficient

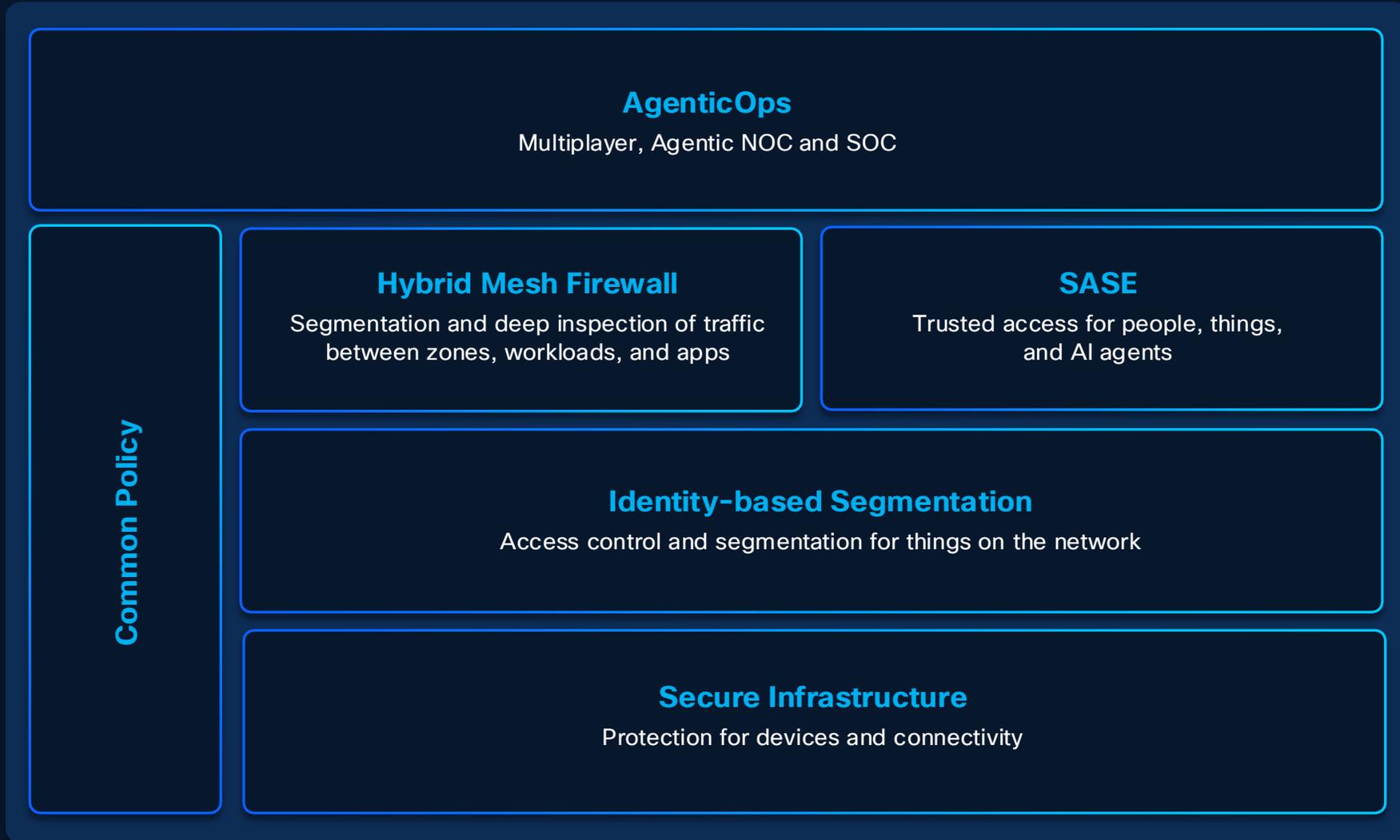
Smarter

AI powered capabilities that power end-to-end visibility

Safer

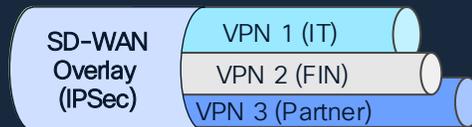
Security integrations designed to be SASE-ready and always-on

Reference design for fusing security into the network



Granular Network and/or Security Segmentation (802.1x / ISE)

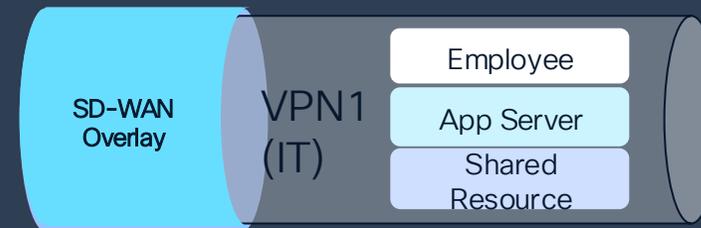
Macro Segmentation



VPN (VRF) Level Segmentation

- IT VPN
- Finance VPN
- Partner VPN

Micro Segmentation

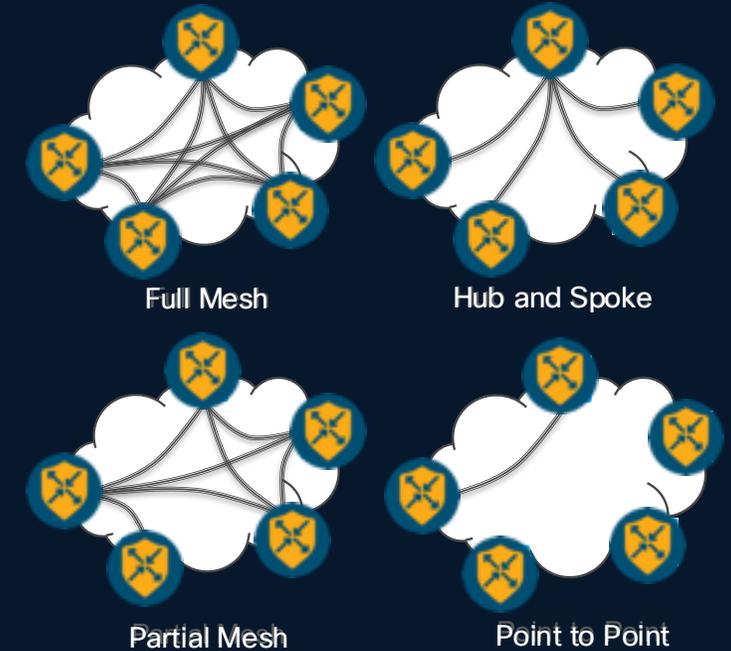
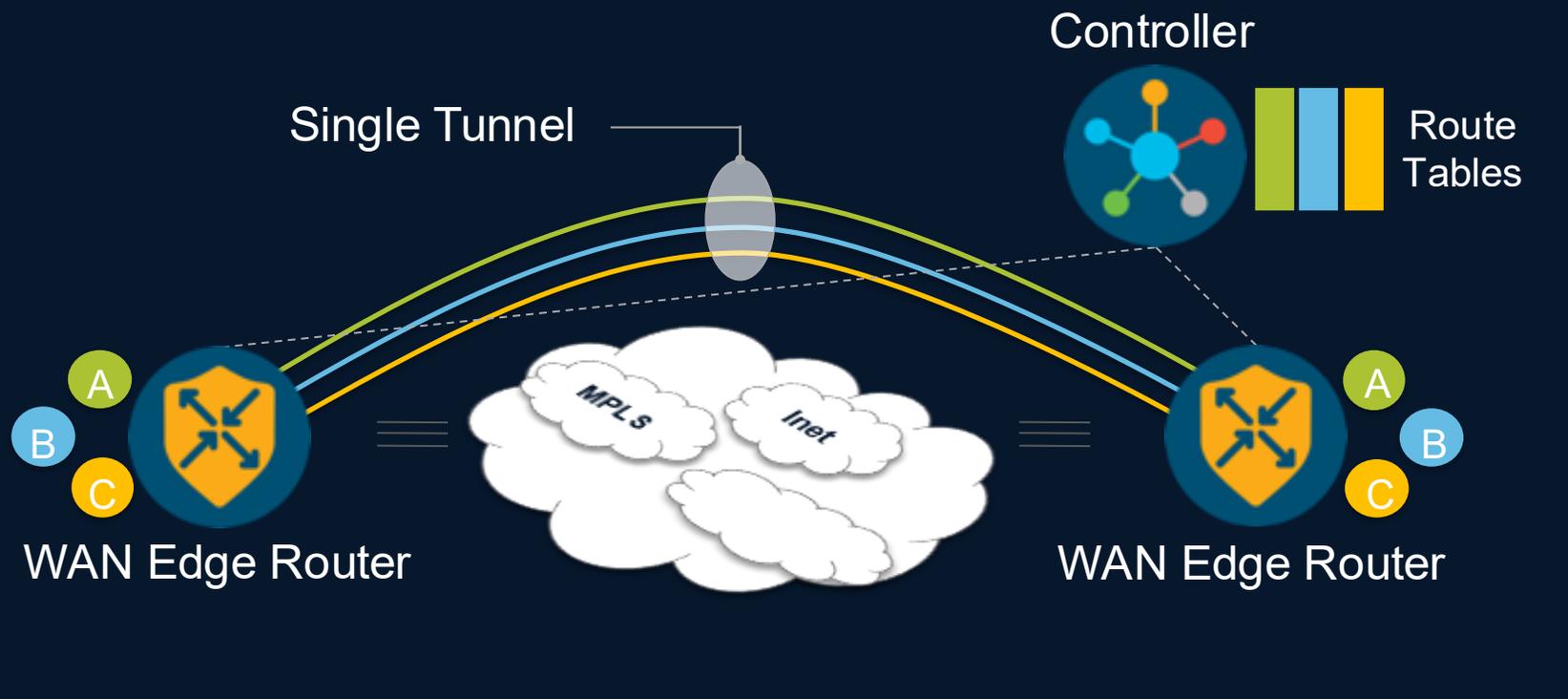


Group Level Segmentation (SGT)

Example: IT VPN

- Employee
- App Servers
- Printers

End-to-End Segmentation with Multi-VRF Topology



Segment connectivity across the SD-WAN fabric without reliance on underlay transport

WAN Edge routers maintain per-VPN routing table for complete control plane separation

Core Security Capabilities



SD-WAN Manager



SCC



Splunk

Cisco Secure Router's Built-in NGFW



L3 - L7 FW

Manage traffic
traversing the branch



IPS/IDPS

Protect assets from
bad actors



AMP

Protect against
malware



Sandboxing

File Analysis using
Threat Grid



URL-F

Filter Internet traffic



TLS Decryption

Inspect encrypted
traffic



EVE*

Protect against
Encrypted threats
without full decryption



Snort ML*
Protects from Zero
day threats



Cisco SSE Ecosystem



Auto Tunnel + HA

Automatic IPsec
tunnels to SSE - 8/ 8
Standby



Traffic Steering

App based traffic
inspection and
redirection to SSE



CASB

Govern access to
cloud applications



FWaaS

Manage traffic to the
internet



DLP

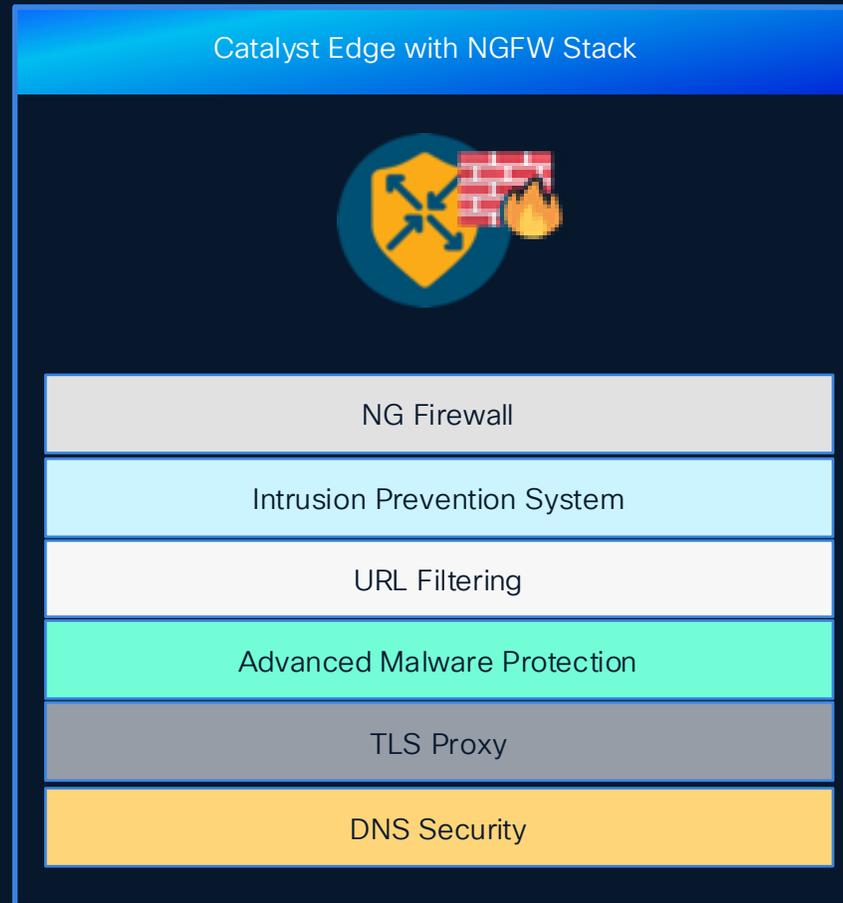
Protect sensitive data
from unauthorized
access



DNS/SWG

Protect web servers /
applications

Catalyst SDWAN with L7 NGFW



ISE/AD Integration for Identity based FW rules

LAUNCHED JUNE 2025

Cisco 8000 Series Secure Routers for every size location



Small Branch: 8100

4 Variants

IPsec:
Up to 1.5 Gbps

Threat Protection:
Up to 1 Gbps

Ports:
1 GE

2 NEW
SKUs



Medium Branch: 8200

4 Variants

IPsec:
Up to 5 Gbps

Threat Protection:
Up to 2.5 Gbps

Ports:
2.5 GE, 2 x 10 GE



Large Branch: 8300

2 Variants

IPsec:
Up to 20 Gbps

Threat Protection:
Up to 7 Gbps

Ports:
5 GE, 4 x 10 GE



Campus: 8400

2 Variants

IPsec:
Up to 45 Gbps

Threat Protection:
Up to 11 Gbps

Ports:
25 GE



Data Center: 8500

2 Variants

IPsec:
Up to 60 Gbps

Route Scale up to 8M

Ports:
40/100 GE

Secure Networking Processor

Purpose built for the Future AI Workloads

C8400, C8300, C8200, C8100 Series Secure Routers are powered by 'secure networking processor'



- Inline Crypto
- PQC capable crypto engine
- Cisco Secure Firewall acceleration
- Built-in AI/ML inferencing engine



- Integrated hardware accelerators
- Various Ethernet standards- 2.5mGig, 5mGig, 10GE, 25GE
- Performance defined Power - 30%+ power saving
- Programmable uCode - feature parity

Key Takeaways

Secure networking processor

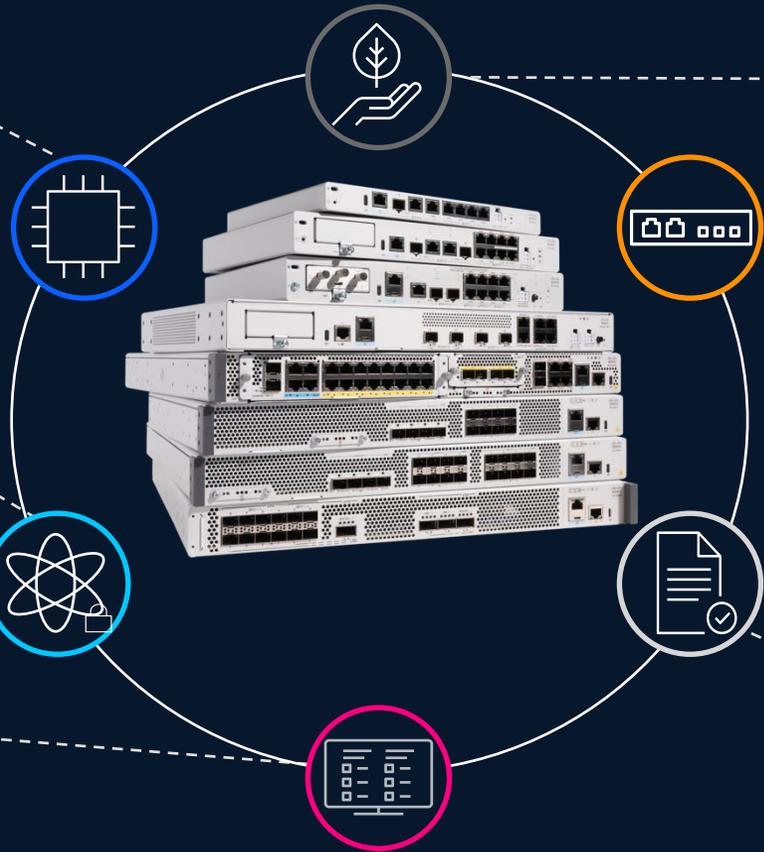
- Integrated hardware accelerators
- Inline crypto processing
- Increased performance, uncompromised security

Post-Quantum Crypto Capable

- Prepare the network for quantum attacks
- NIST compliance for IPsec & MACsec
- Post Quantum Safe secure boot (future)

Management

- Catalyst SD-WAN Manager
- Catalyst Center
- Meraki Dashboard (future – mid 2026)



Sustainability

- Fan-less medium branch 8200-G2
- Fan-less large branch 8355-G2
- Energy star certified: C8400,8500-G2

Port Density

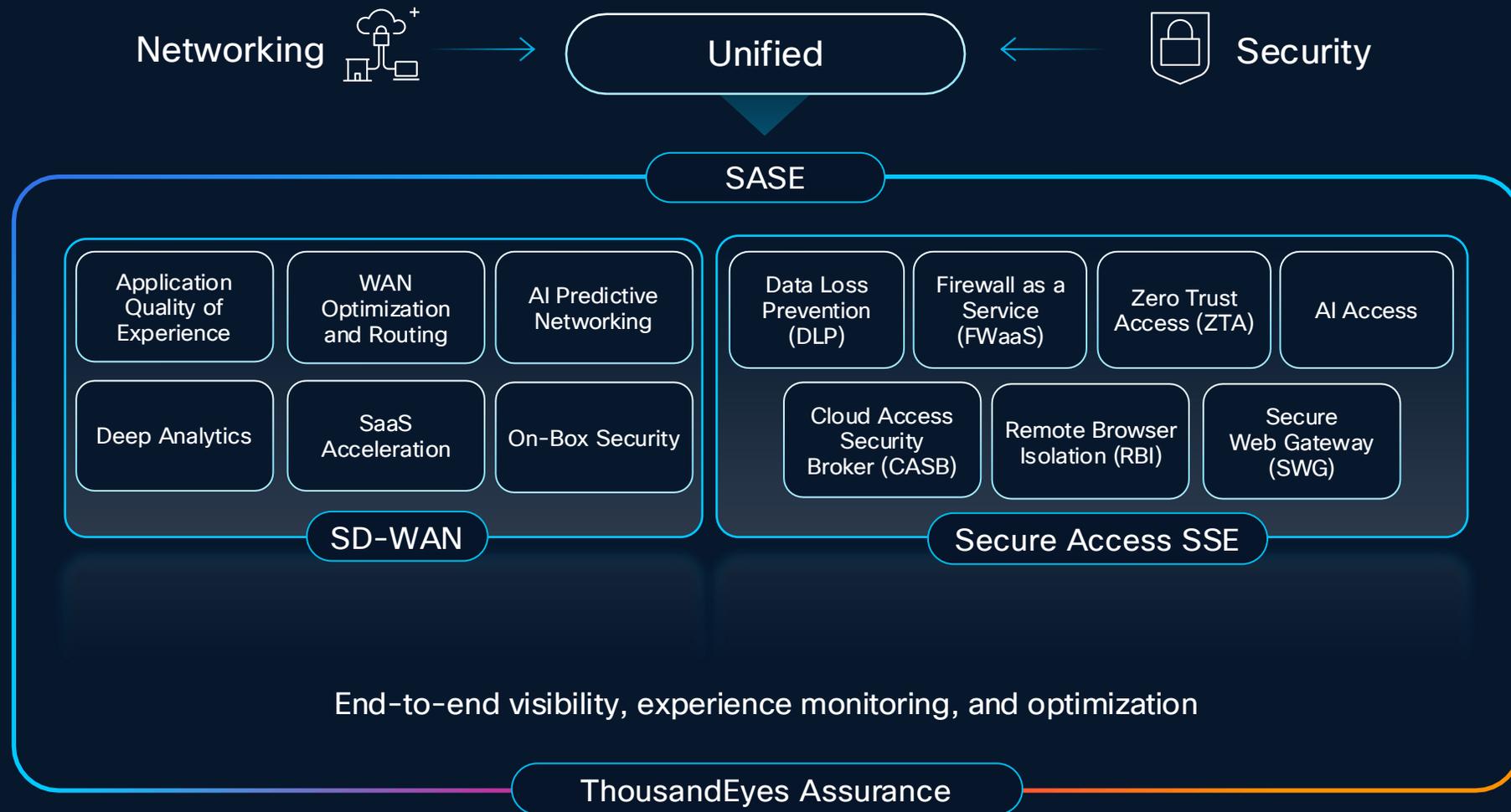
- Flexible L2/L3 ports
- 2x 10G port medium branch
- 4x 25G port campus router

Documentation & More

- Individual TDMs, mechanical drawings, cheat sheets, sustainability
- Datasheets, HIG, SCG, FAQs, RFP Boilerplate
- CCAPP, Router Selector, Power Calc.

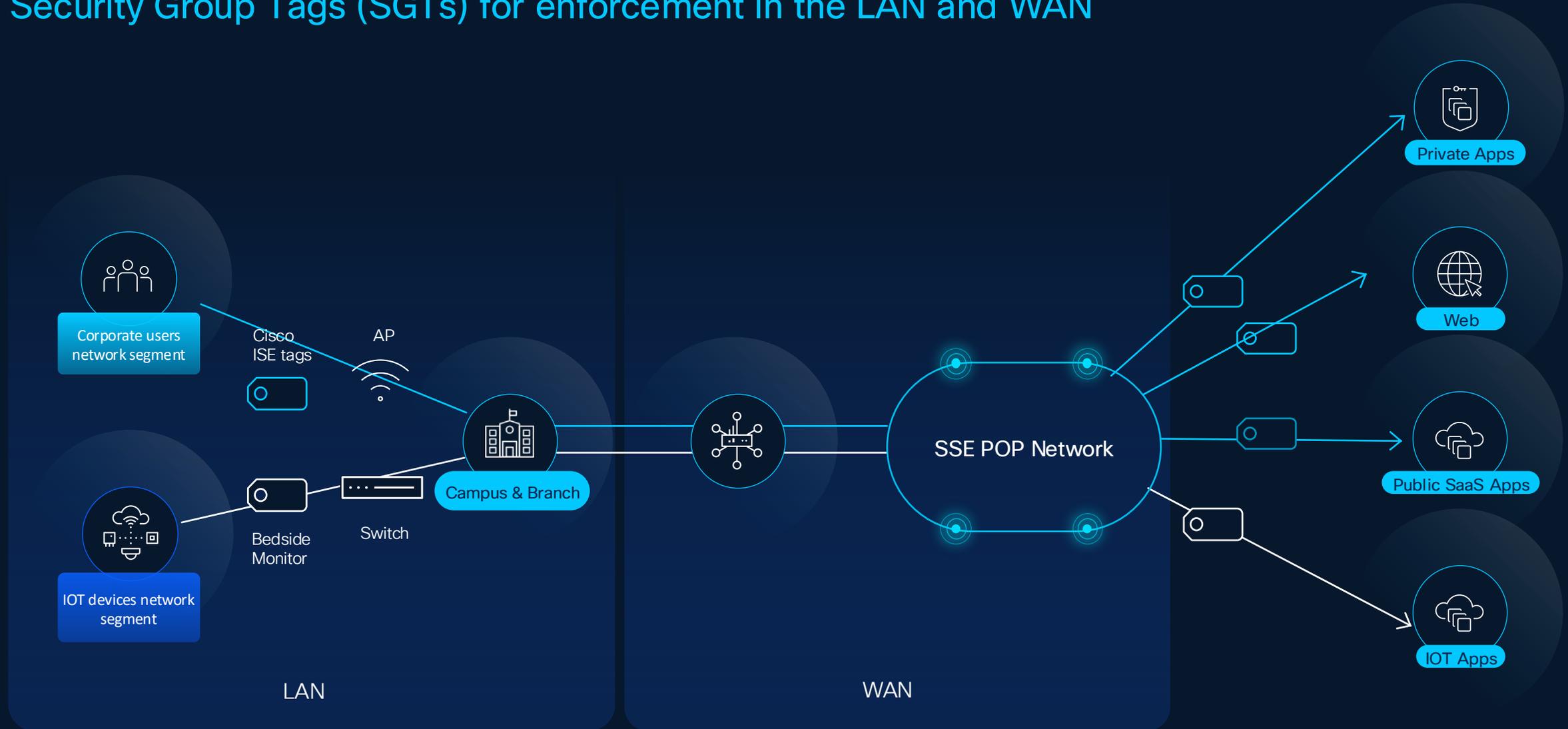
Cisco Secure Access Service Edge (SASE)

Performance, reliability, and security. Unified.



Policy-based segmentation for secure IT, IoT and OT

Security Group Tags (SGTs) for enforcement in the LAN and WAN



SASE: Secure Access integrated with Cisco SD-WAN

Your security strategy for a hyper-distributed world

SASE

Secure
SD-WAN

Converged set of cloud networking

+

Secure
Services Edge / CSA

Converged set of cloud security

End-to-end Assurance with ThousandEyes

Cisco Zero Trust Access

Secure
SD-WAN

+

Secure
Services Edge

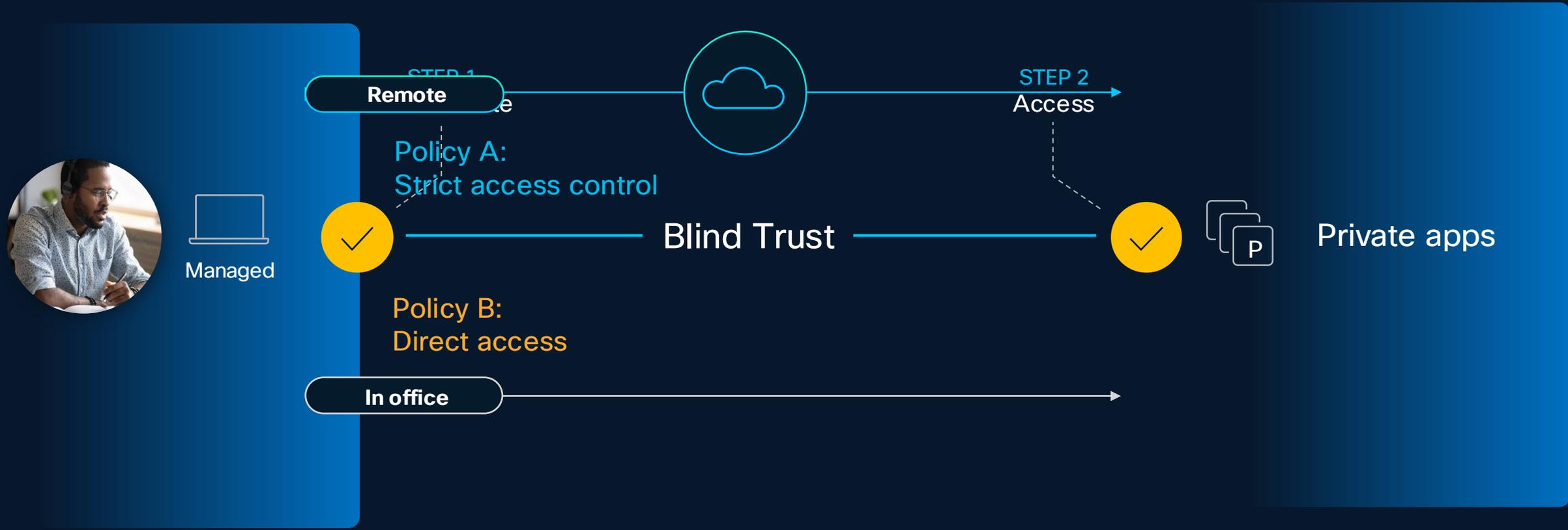
+

Trusted
Identity Edge

SINGLE VENDOR SASE

End-to-end Assurance with ThousandEyes

Traditional ZTA: Work from home solution



Managed devices,
private apps

Different policies
for home versus office

Blind trust between
authentication and access

Cisco Zero Trust Access



Every device, people, things,
agents everywhere

Cisco Zero Trust Access

We do the plumbing



Every device, people, things, agents everywhere

One policy, all apps, no hairpinning

Seamless user to app experience

No blind trust with Identity Intelligence

The background features a dark blue field with dynamic, glowing light streaks. These streaks are primarily blue, with some orange and pinkish hues, and they curve and flow across the frame, creating a sense of motion and energy. A dark blue rectangular box is positioned on the left side, containing the text.

Zero Friction

One client, multiple functions



Extending SDWAN Identity Context to Secure Access

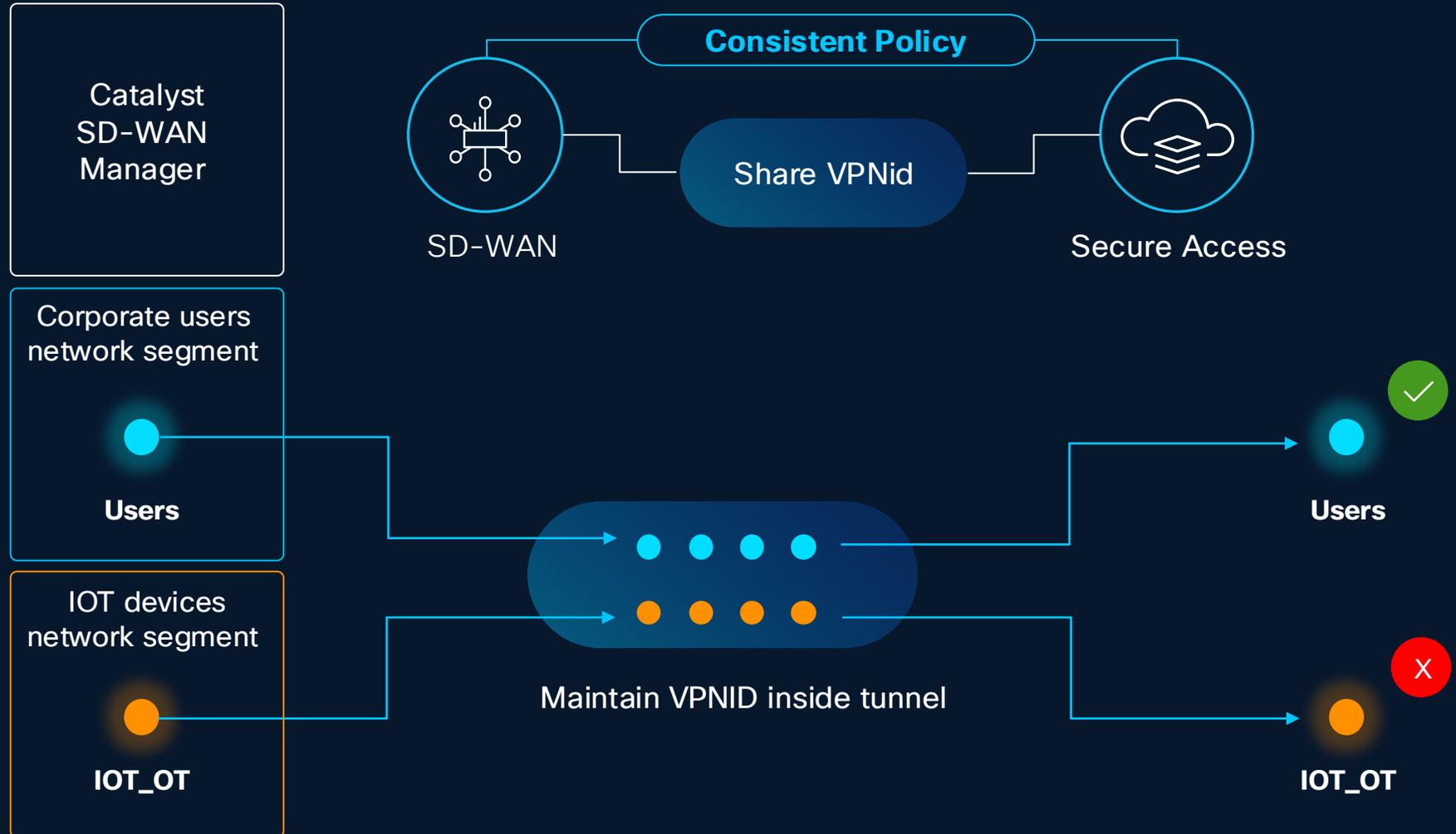
The screenshot displays the Cisco Catalyst SD-WAN interface. The top navigation bar (1) shows the 'Catalyst SD-WAN' title. The left sidebar contains navigation options like Monitor, Configuration, Analytics, Workflows, Tools, Reports, Maintenance, Administration, and Explore. The main content area is titled 'SSE Provider' and includes a 'Context Sharing' section with a 'VPN' toggle (2). Below this is a 'Tracker' section. The primary focus is on the 'Network Tunnel Groups' page (3), which shows a specific group: 'C8K-3D1A8960-6E76-532C-DA93-50626FC5797E'. The page includes a 'Summary' section with a 'Connected' status, 'Region' (US (Virginia)), and 'Routing Type' (NAT / Outbound Only). It also features 'Primary Hub' and 'Secondary Hub' sections, each with a 'Hub Up' status and 'Active Tunnels' count. At the bottom, a 'Network Tunnels' table lists the details for the primary and secondary tunnels.

Tunnels	Peer ID	Peer Device IP Address	Data Center Name	Data Center IP Address	Status	Last Status Update
Primary 1	65539	128.107.222.147	sse-use-1-1-1	44.217.195.188	Connected	May 20, 2025 10:45 AM
Secondary 1	131073	128.107.222.147	sse-use-1-1-0	35.171.214.188	Connected	May 20, 2025 10:44 AM

Catalyst SD-WAN

VPNid support for consistent segmentation

- VPNiD Based policy across both SDWAN & Secure Access
- Maintain segmentation in branch & in the cloud



Leveraging SGTs in Cloud based policy enforcement

The image displays two overlapping screenshots of the Cisco Secure Access web interface. The background screenshot shows the 'Security Group Tags' configuration page, with three red circles highlighting key elements: '1' on the 'Rule name' field, '2' on the 'Rule order' field, and '3' on the 'Specify Access' section. The foreground screenshot shows the 'Activity Search' page, which displays a table of search results and an 'Event Details' sidebar.

Activity Search Filters:

- Search by domain, identity, or URL
- Advanced
- CLEAR
- Filters: IDENTITY TYPE Security Group Tags
- Search filters
- 1,304,977 Total
- Viewing activity from May 1, 2025 12:00 AM to May 30, 2025 10:03 PM
- Page: 1
- Results per page: 50
- 1 - 50
- SAVE SEARCH

Activity Search Results Table:

Request	Source	Rule Identity	Destination IP	Destination Country	Internal IP	External IP	Action	Category
FW	*IOT_OT (VPN-154)	*IOT_OT (VPN-154)	108.139.3.127	United States	192.168.25.3		Allowed	Uncat
FW	*IOT_OT (VPN-154)	*IOT_OT (VPN-154)	108.139.3.127	United States	192.168.25.3		Allowed	Uncat
FW	*IOT_OT (VPN-154)	*IOT_OT (VPN-154)	151.101.195.5	United States	192.168.25.2		Allowed	Uncat
FW	*IOT_OT (VPN-154)	*IOT_OT (VPN-154)	151.101.195.5	United States	192.168.25.2		Allowed	Uncat
FW	*IOT_OT (VPN-154)	*IOT_OT (VPN-154)	108.139.3.127	United States	192.168.25.3		Allowed	Uncat
FW	*IOT_OT (VPN-154)	*IOT_OT (VPN-154)	108.139.3.127	United States	192.168.25.3		Allowed	Uncat
FW	*IOT_OT (VPN-154)	*IOT_OT (VPN-154)	151.101.195.5	United States	192.168.25.2		Allowed	Uncat
FW	*IOT_OT (VPN-154)	*IOT_OT (VPN-154)	151.101.195.5	United States	192.168.25.2		Allowed	Uncat
FW	*IOT_OT (VPN-154)	*IOT_OT (VPN-154)	108.139.3.127	United States	192.168.25.3		Allowed	Uncat

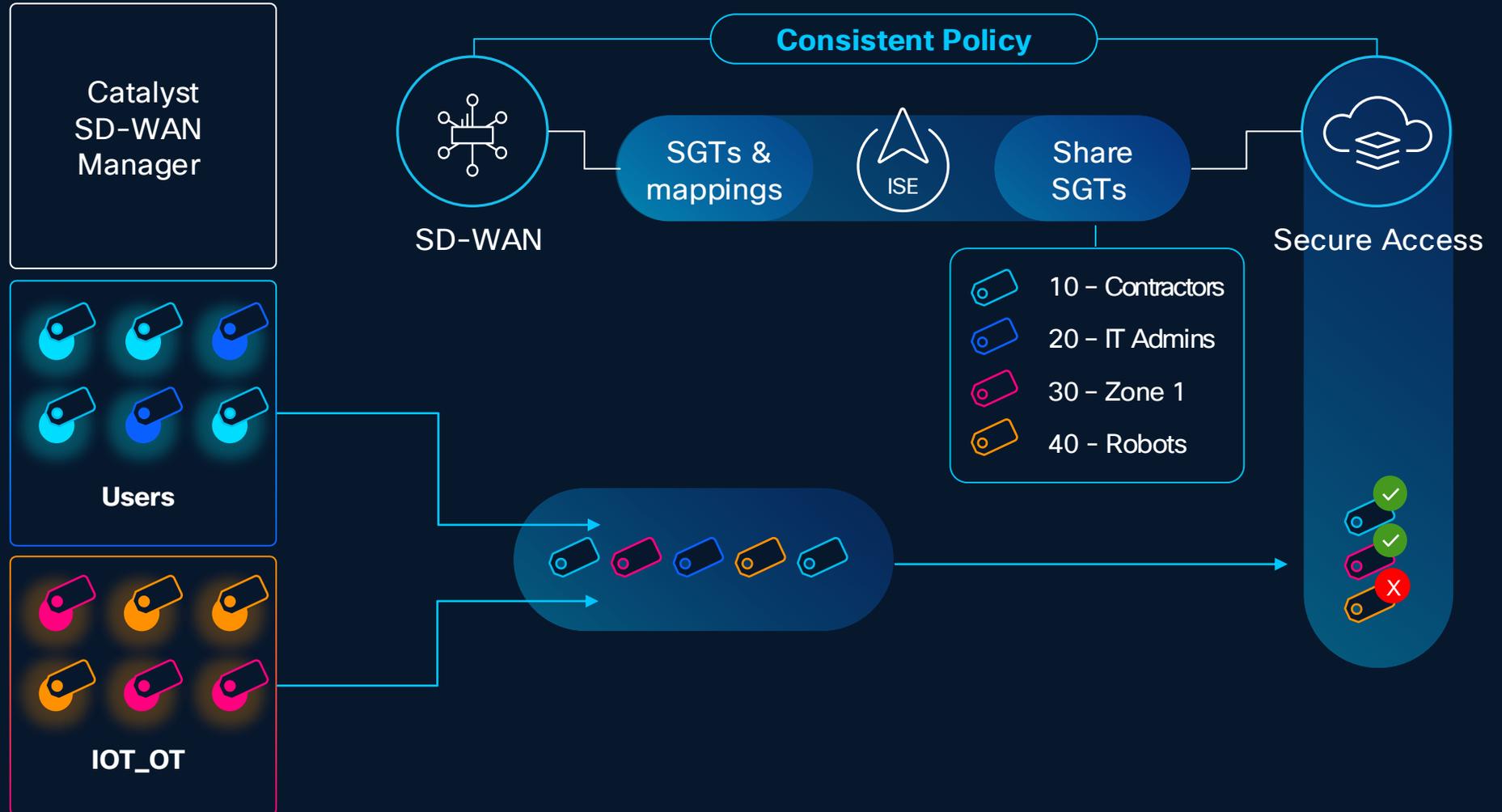
Event Details:

- Action: Allowed
- Time: May 30, 2025 10:03 PM
- Rule Name: IOT branch (952085)
- Source: *IOT_OT (VPN-154)
- Cell1 (SGT-28)
- Source IP: 192.168.25.3
- Destination IP: 108.139.3.127

Identity Services Engine (ISE)

Leverage SGTs for granular access control

- SGT Based Policy across network & Cloud
- Maintain micro segmentation through Secure Access
- Uniquely identify devices and traffic based on context from ISE
- Apply policy to SGT Based identity



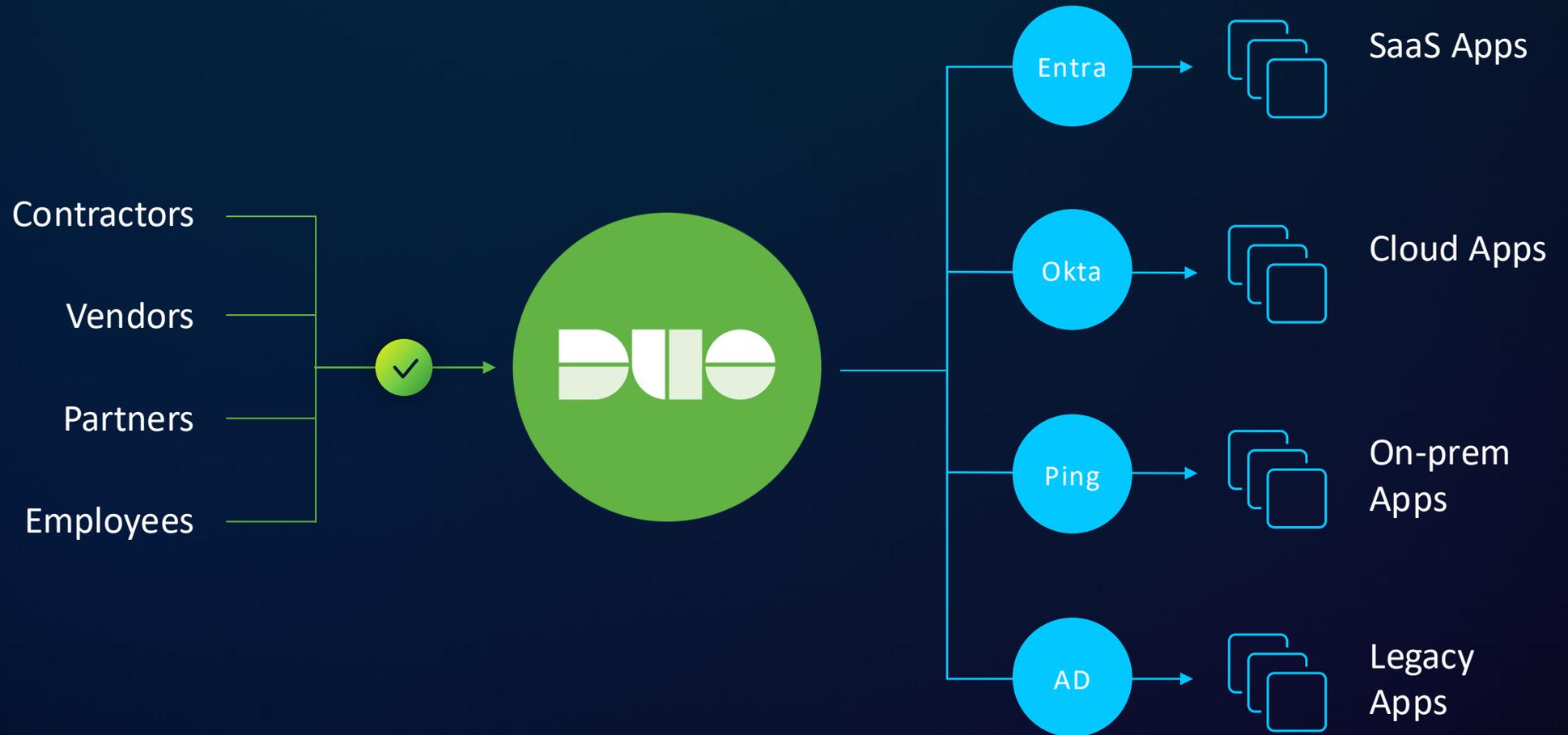
Duo Identity & Access Management (IAM)



Standalone IAM
when required

Identity broker for
existing IAM

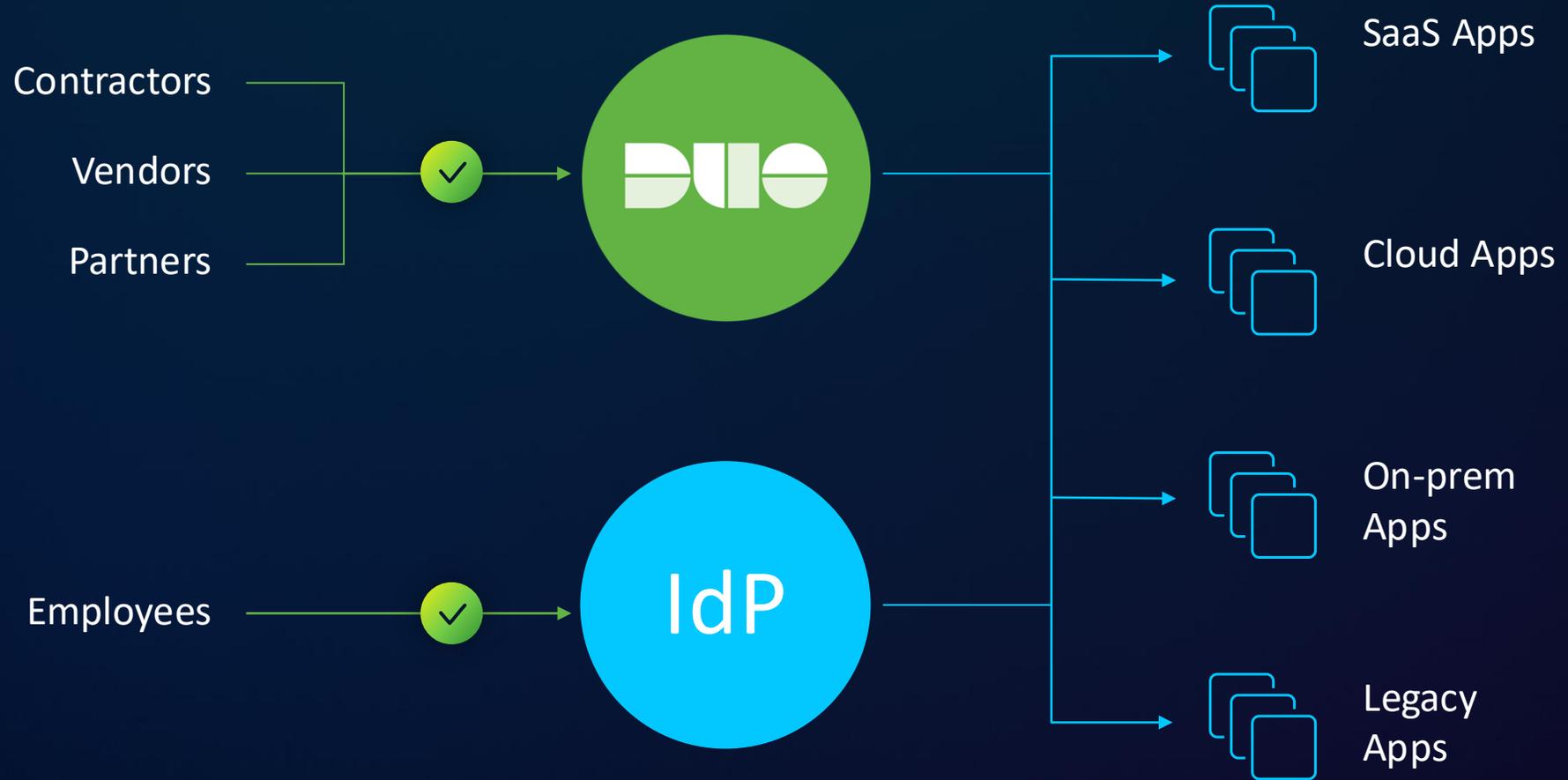
Alternate directory for
third-party users



Standalone IAM
when required

Identity broker for
existing IAM

Alternate directory for
third-party users

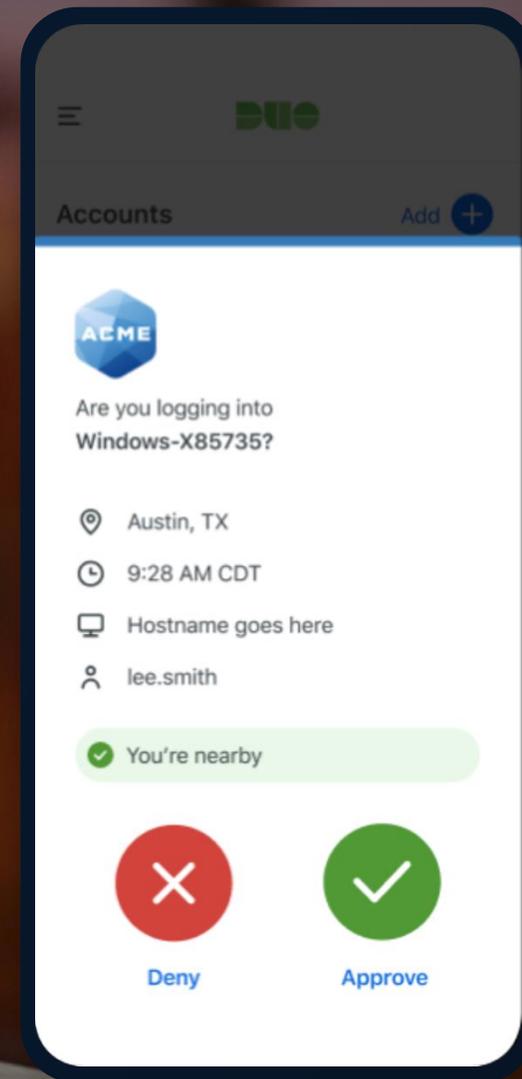




Proximity Verification

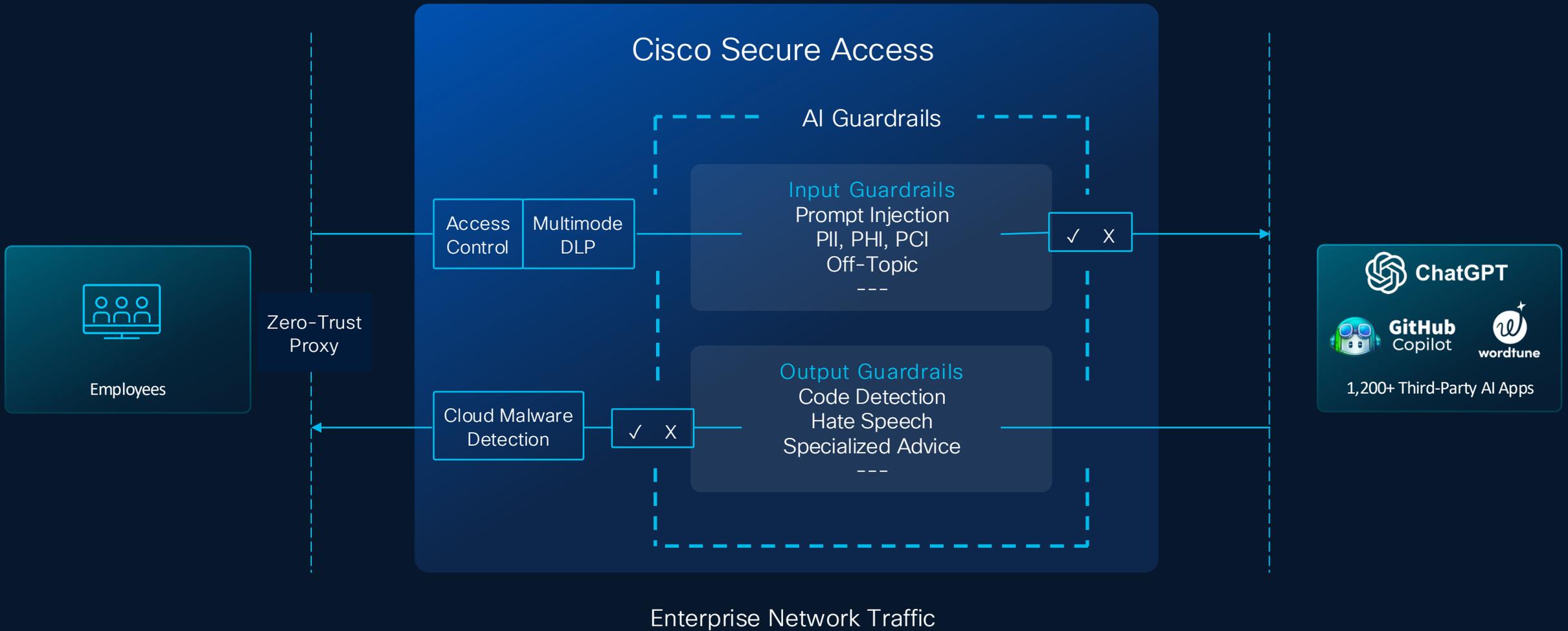


Bluetooth Low Energy (BLE)



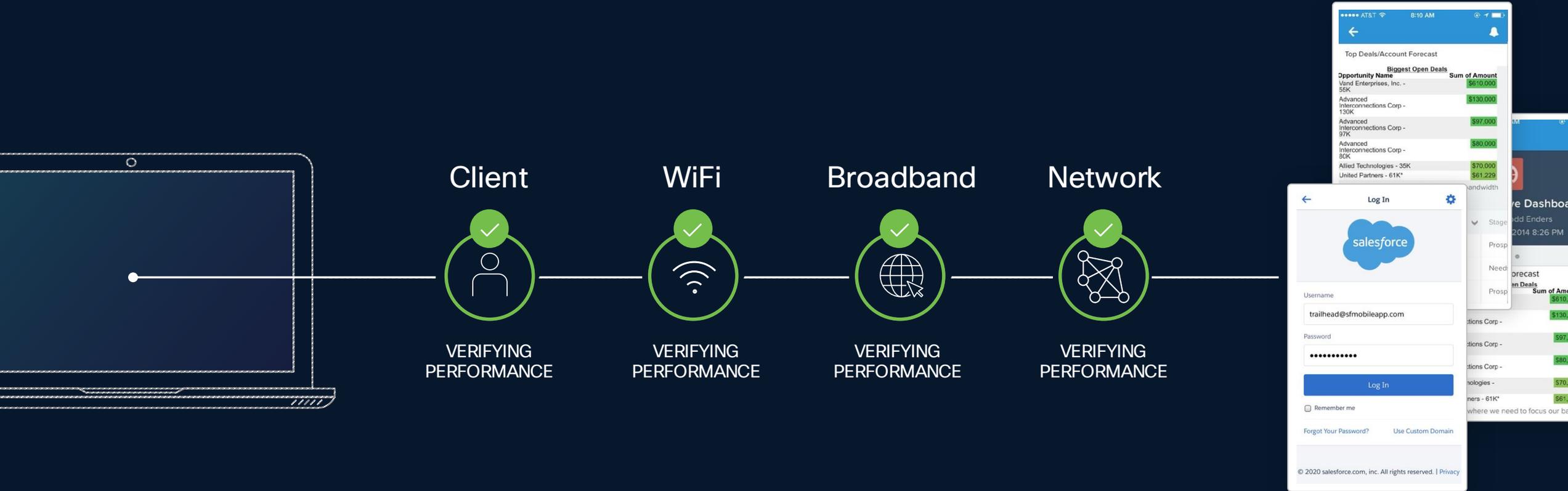
AI Access

Protecting usage of third-party AI apps



Shadow AI Security with Cisco Secure Access Demo

Fix issues fast with Digital Experience Monitoring



Historical performance and recommendations

The background features a dark blue field with vibrant, glowing light trails in shades of blue and orange. These trails are curved and dynamic, creating a sense of motion and energy. A dark blue rectangular box is positioned on the left side of the image, containing the text.

Flexible Management

Security Cloud Control

Define policy once and enforce anywhere

Secure Firewall
(FTD, ASA)

Hypershield

Multicloud
Defense

Secure
Workload

Secure Access

AI Defense

NEW

Secure Router

NEW

3rd party
firewalls

Security Cloud Control

Define policy once and enforce anywhere

Cisco Firewalling

AI Defense

3rd Party Firewalls

Secure Firewall

Secure Workload

Hypershield

Secure Access (FW as a service)

Secure Router NGFW



Unified AI Assistant:
Simplify policy administration **by up to 70%**

NEW

Security Cloud Control

Industry's first multi-vendor intent-based policy



Absorb and optimize
existing rules

Change enforcement
points, not policy

No rip and
replace

Cisco clears the path to zero trust



Control access across all users and things for tighter security



Protect identities with identity intelligence



Build resilience with optimized infrastructure and simplified IT

Thank you

