

# Cisco AI-Ready

Secure Network Architecture  
for Campus, Branch, and IloT



# Another massive technology disruption

Internet



Mobility



Cloud



AI



# AI is bringing changes and challenges

**1,000s**

AI Agents per  
enterprise expected

**#1 risk**

AI-enhanced  
malicious attacks

**64%**

of orgs face IT skills  
shortage by 2026

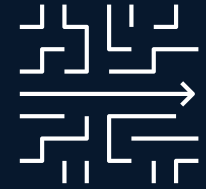
# Is your Campus Network AI ready?

For explosive traffic, for increased security risks, for more complexity



# Architecture for the AI-Ready secure network

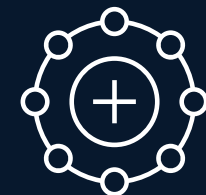
AgenticOps  
for operational simplicity



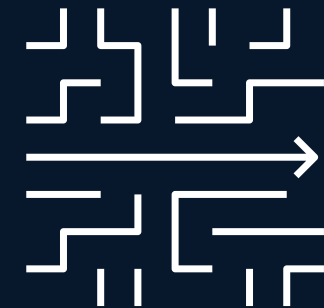
Security  
fused into the network



Scalable devices  
ready for AI



# AgenticOps for operational simplicity



# Unifying Catalyst & Meraki

## Catalyst

Catalyst Center

Catalyst License

Catalyst Hardware

MANAGEMENT

LICENSE

CISCO HARDWARE

## Meraki

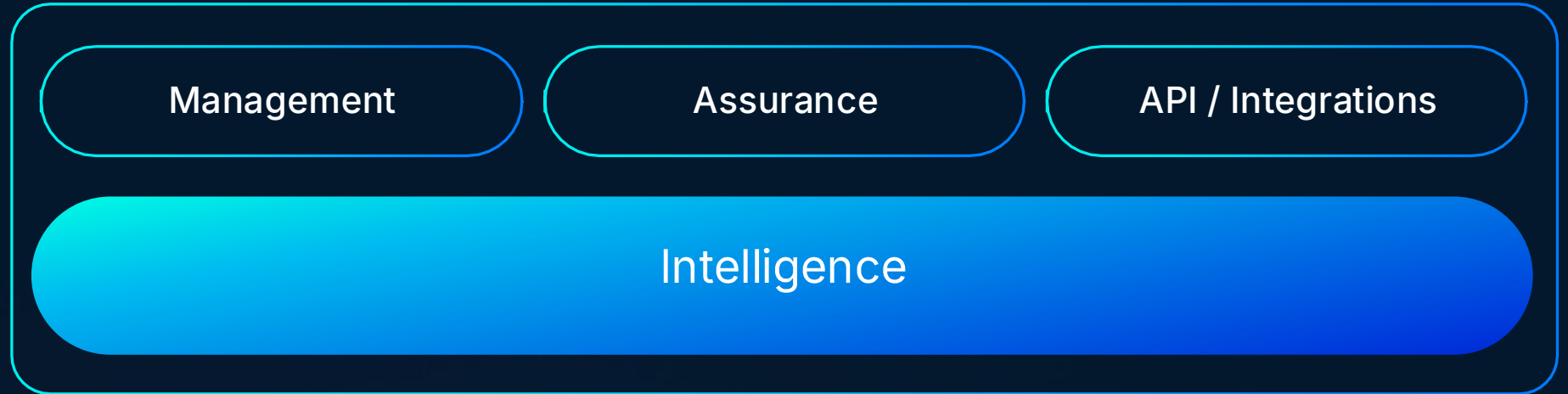
Meraki Dashboard

Meraki License

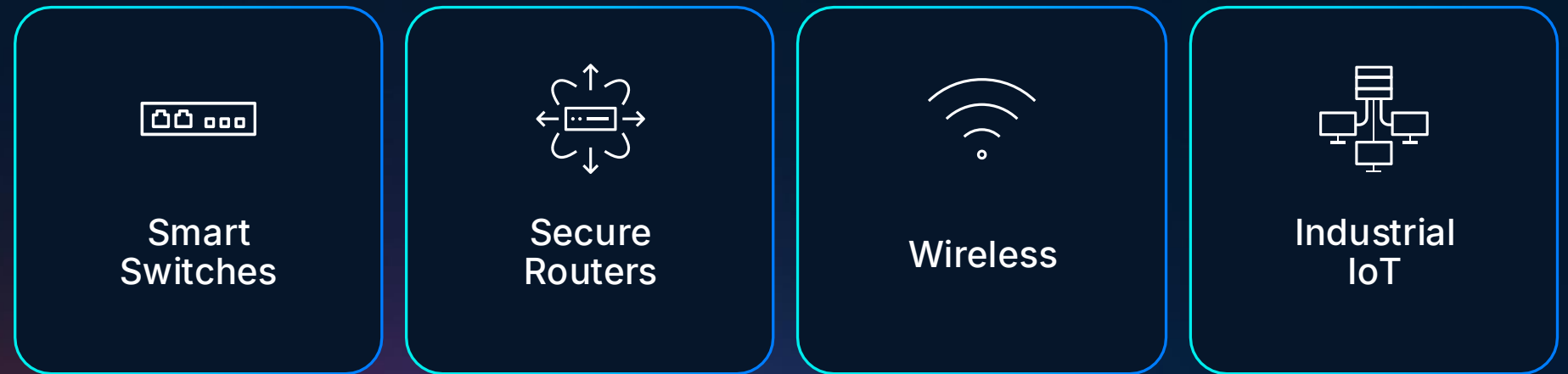
Meraki Hardware

# Our unified platform

PLATFORM



HARDWARE



# A unified OS for cloud and on-prem management

The foundation of operational simplicity

**Fast, consistent  
out-of-box  
provisioning**

Simple day 0 operations  
Simple, streamlined onboarding  
Automated port config  
Secure, fast onboarding of devices

**Expanding IOS XE  
capabilities available  
in the cloud**

CLOUD MANAGEMENT AVAILABLE NOW

BETA



C9300L



C9300



C9300X



C9200L



C9500



C9200/CX



C9300LM



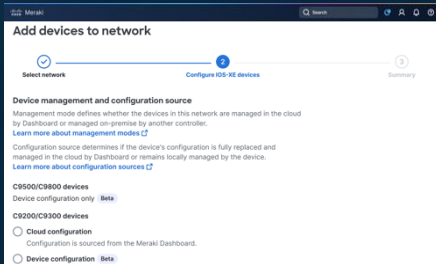
C9350



Modular

# Large campus cloud capabilities

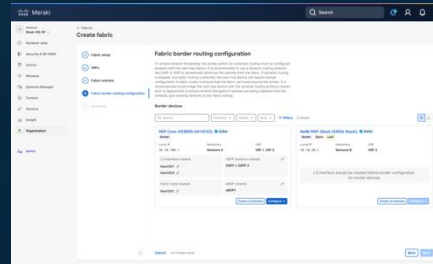
## Powerful Switching Capabilities



Support campus deployments with BGP, VRF, ISSU, and IOS XE stacking

AVAILABLE NOW

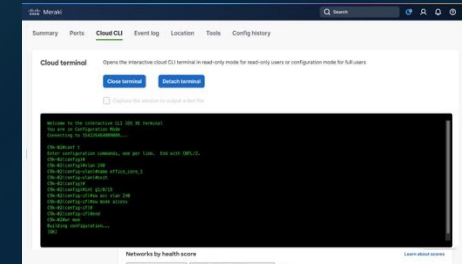
## Fabric for Secure Networking



Simplify NetOps with a secure fabric and micro/macro-segmentation

AVAILABLE NOW

## Cloud CLI for Flexibility



Simplify onboarding and flexibility with operating mode options and Cloud CLI

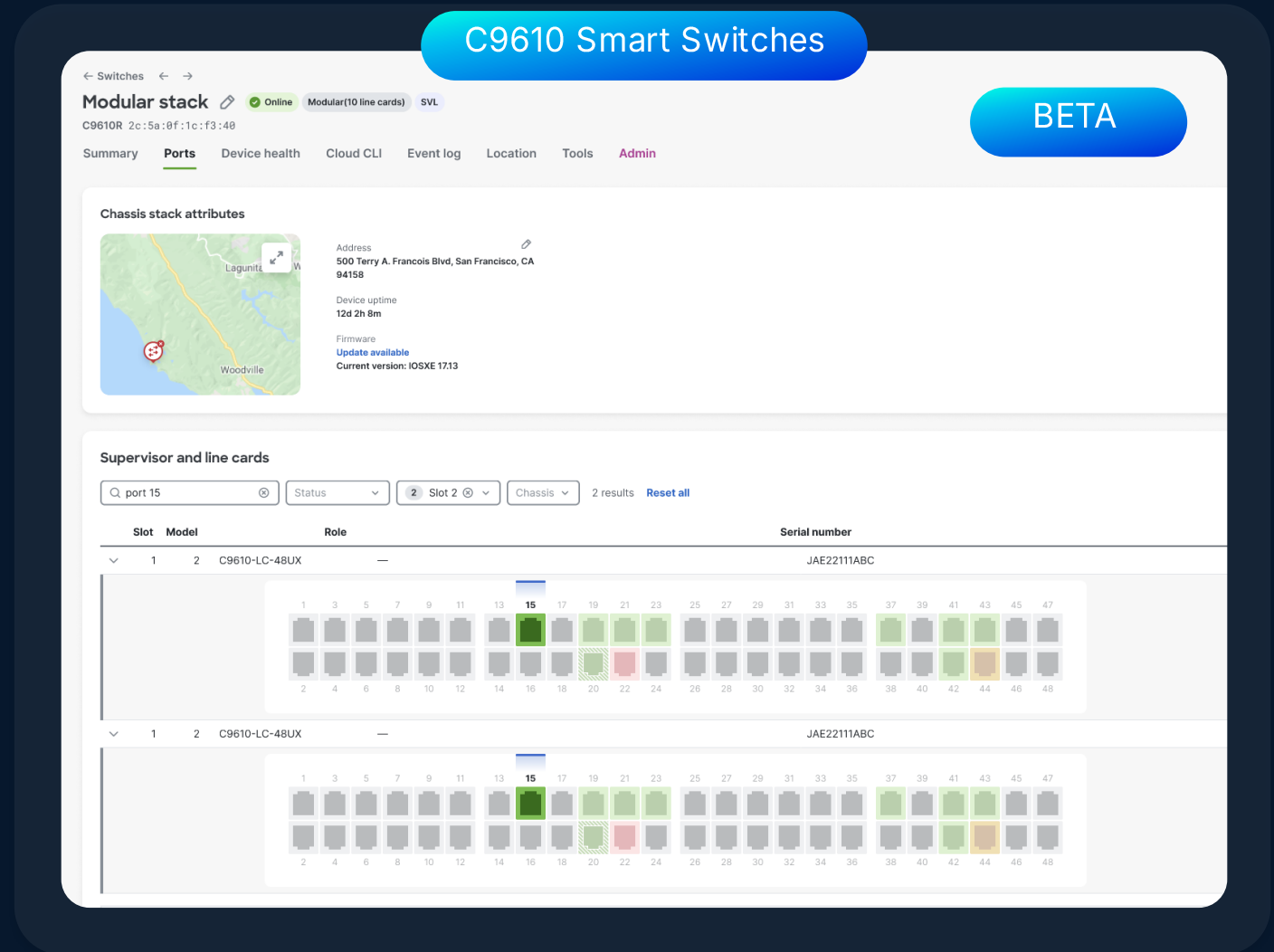
AVAILABLE NOW

# Cloud-managed switching

# Cloud management for modular switches

View stats, configs, and troubleshoot switches remotely

Manage and edit configs via Cloud CLI while retaining local SSH/console access.



AVAILABLE TODAY

## Agentic Workflows

# Accelerate cross-domain deployments with AI Assistant

Automate workflows across Meraki, Catalyst Center, Catalyst SD-WAN Manager, ISE, Nexus, and more

The screenshot displays the Cisco Meraki AI Assistant interface. On the left, a navigation sidebar includes sections for Global Overview, Organization (Ed lab), Network (Demo WiFi), Network-wide, Assurance, Wireless, Cameras (Learn more), Organization, and Automation. The main workspace is titled 'Workspace' and contains a list of workflows under the heading 'Workflows'. A search bar is present above the list. The AI Assistant chat window is open, showing a user query: 'I would like to run a workflow that conducts a compliance audit of all networks with the network Audit in all my organizations'. The AI Assistant responds: 'I found a workflow that can help you with this task: Compliance Audit on Multi-Organization Networks by Tag'. Below this, four recommended actions are listed: 'Create a table of all Organizations', 'Create Network List from Tagged Networks from all Organizations', 'Run Compliance Audit sub-workflows for each Network', and 'Generate the Audit Findings Report'. A confirmation prompt asks 'Please confirm if you want to proceed.' At the bottom of the chat, there is a text input field 'Ask the AI Assistant a question' and a note: 'Assistant can make mistakes. Verify responses. Cisco handles your data responsibly. See [Privacy Data Sheet](#)'. The footer of the interface shows 'Cisco Live, CDA-111' and two 'Validated' status indicators for Ed Novak.

Cut MTTR to near seconds with AI-driven root cause and resolution.

Catch critical issues early with AI that sees across the stack.

Operate at scale with lean teams and built-in AI expertise.

Troubleshoot faster together with shared context across teams.

# AgenticOps

## The New Standard for IT Operations

### Workflows (GA)

AVAILABLE NOW



**CISCO**  
**AI Assistant**

### AI Assistant

Accelerate network operations

ALPHA



### AI Canvas

Cross-domain collaborative troubleshooting



Powered by Deep Network Model



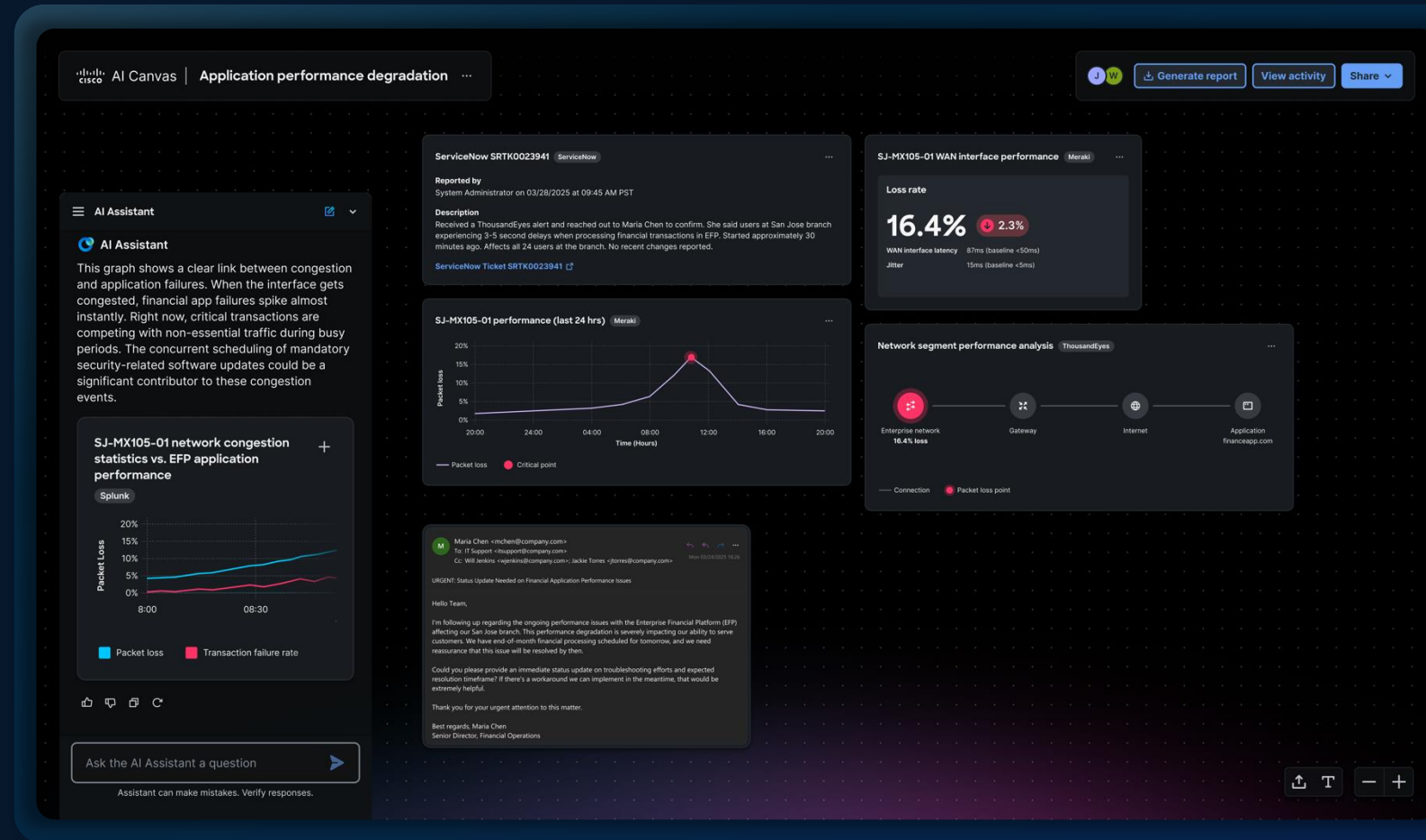


# AI Canvas

Troubleshooting and execution across multiple domains

Collaboration across multiple users (NetOps, SecOps and execs)

Built on the foundation of the Deep Network Model



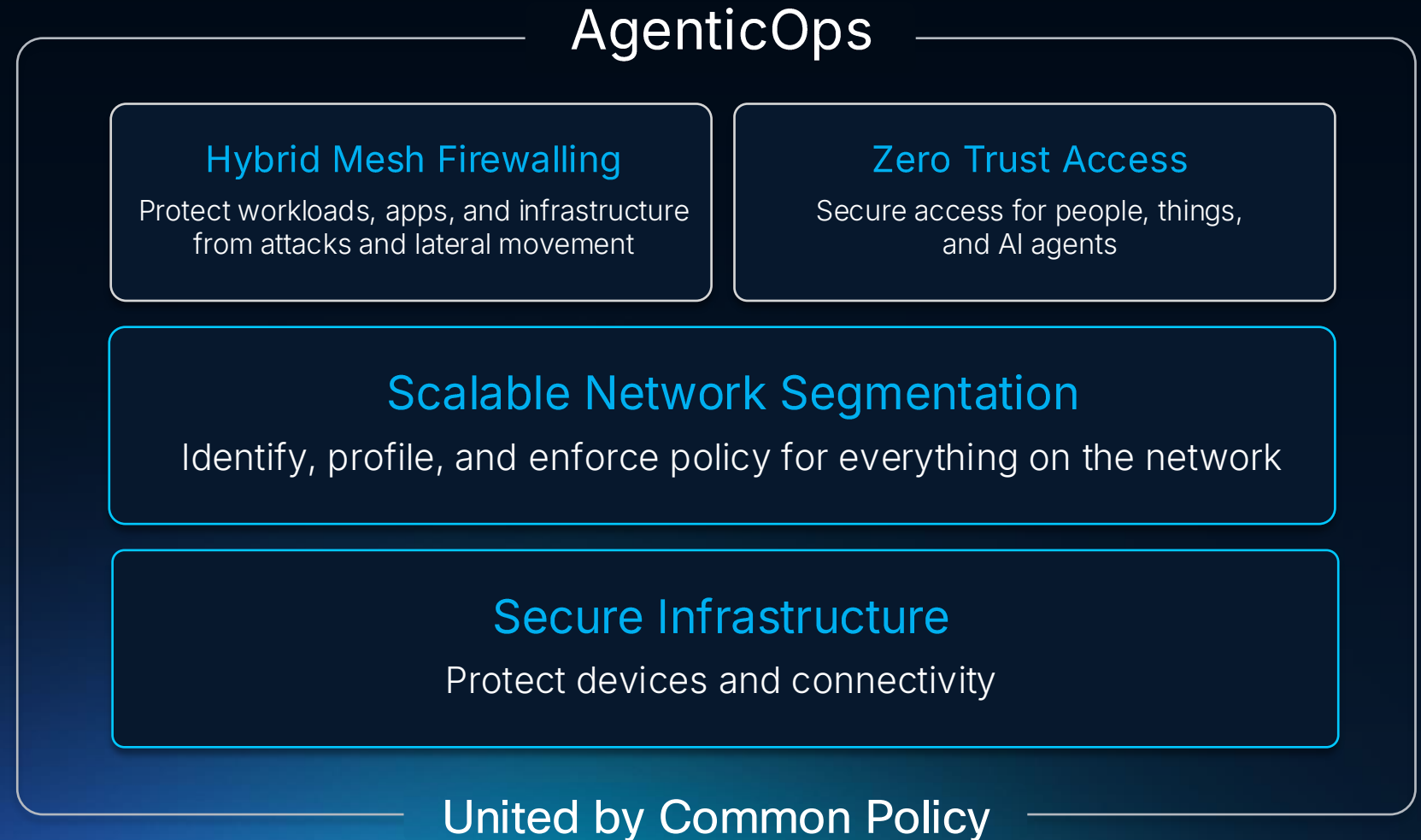
# Security fused into the Network



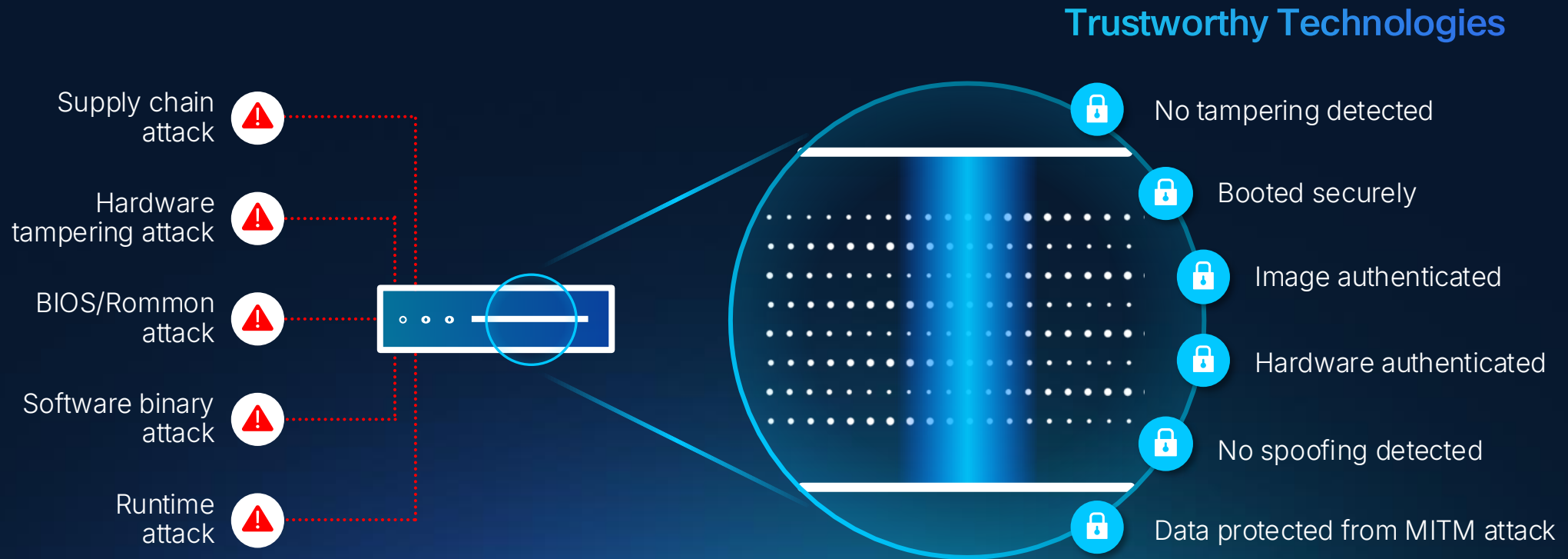
# Introducing Cisco's approach to secure networking

Security infused  
into everywhere the  
network extends

- Identity-first
- Continuously verified
- Enterprise-wide policies
- Comprehensive threat intel
- Distributed enforcement



# The strength of the network depends on the foundation it is built on



# Ensuring long term data privacy with quantum-ready encryption

Protect today's data from tomorrow's threats with built-in cryptographic agility with support for post-quantum algorithms.

## Network Traffic

MANAGED

UNMANAGED

IoT/OT



## Encryption Protocols

IPSec

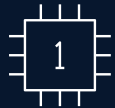
MACSec

WAN MACSec



New with IOS XE 26.1.1

# Future-proofing devices, achieving PQC compliance



## Trust the System

**Management Plane:** PQC-compliant secure management access to protect admin access and control planes



## Data Confidentiality at Layer 3

**PQC VPN:** Support IKEv2 IPsec, DMVPN, FlexVPN, and IKEv2 CLB, protecting encrypted tunnels



## Data Confidentiality at Layer 2

**MACsec and WAN MACsec:** First to support key NIST-approved algorithms to protect data in transit across LAN and WAN



## Trust the Device

**PQC Secure Boot:** NIST-approved PQC algorithms (LMS) for secure boot processes

# Eliminating lateral movement and securing network access

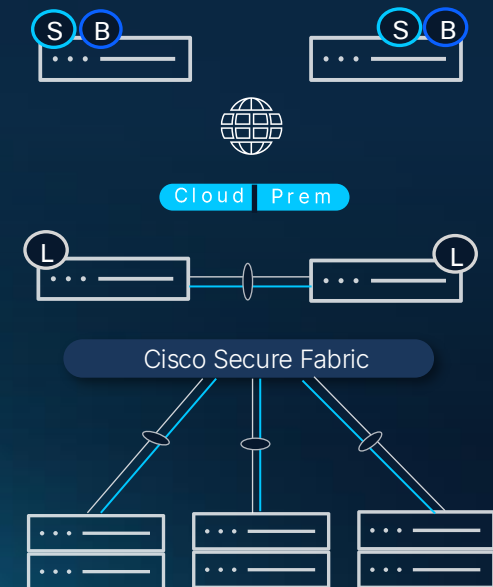
## Native segmentation features VRF, VLAN, SGT, VPN



## Strengthened with NAC ISE and Access Manager

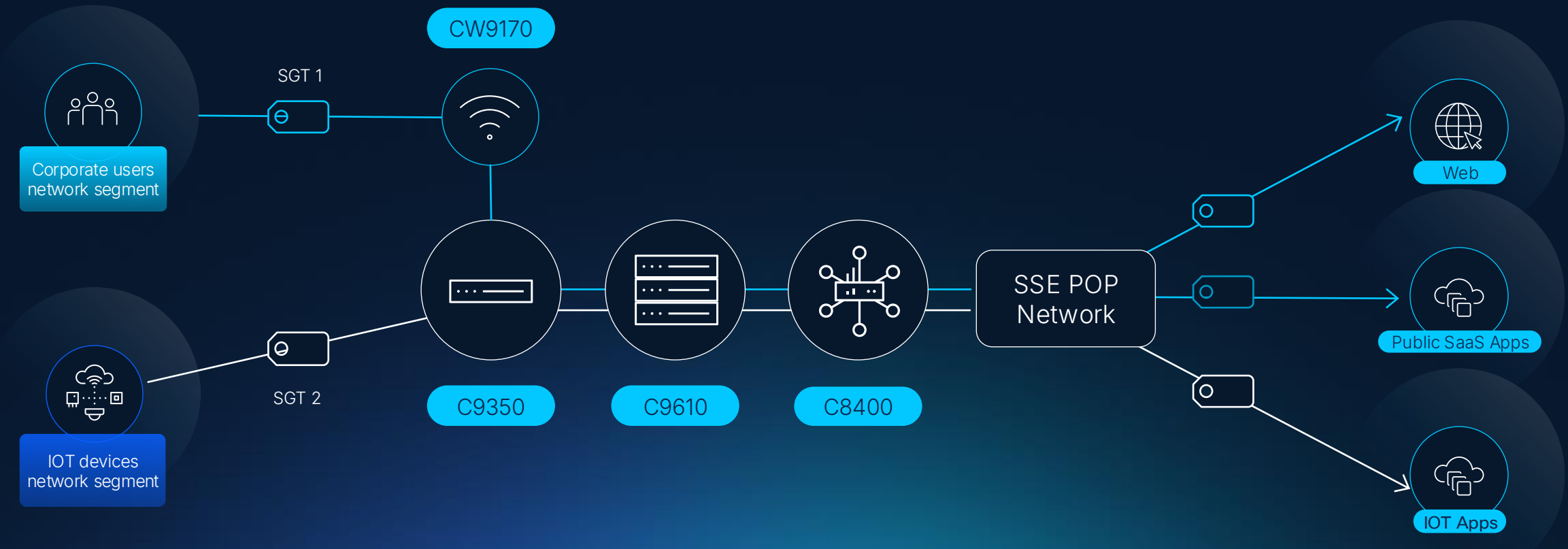


## Automated with secure fabric Cloud and On-Premise



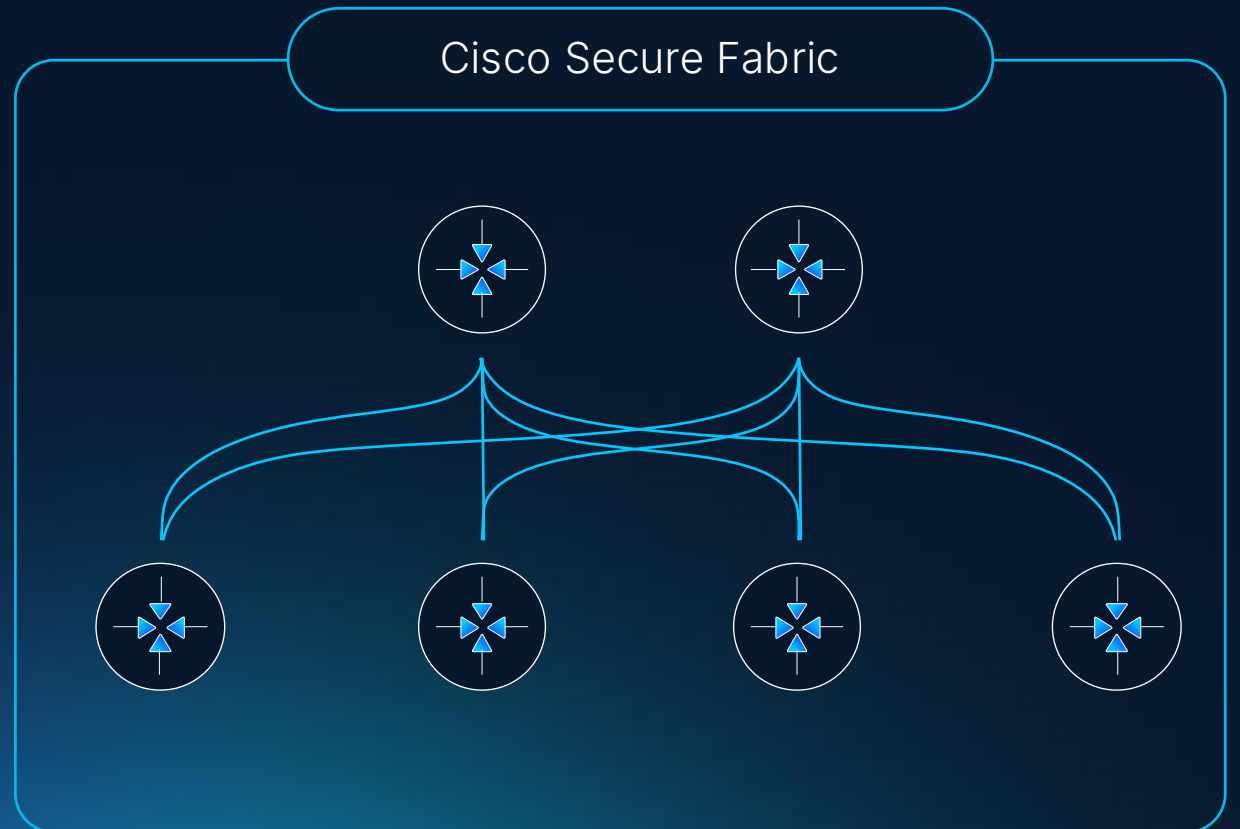
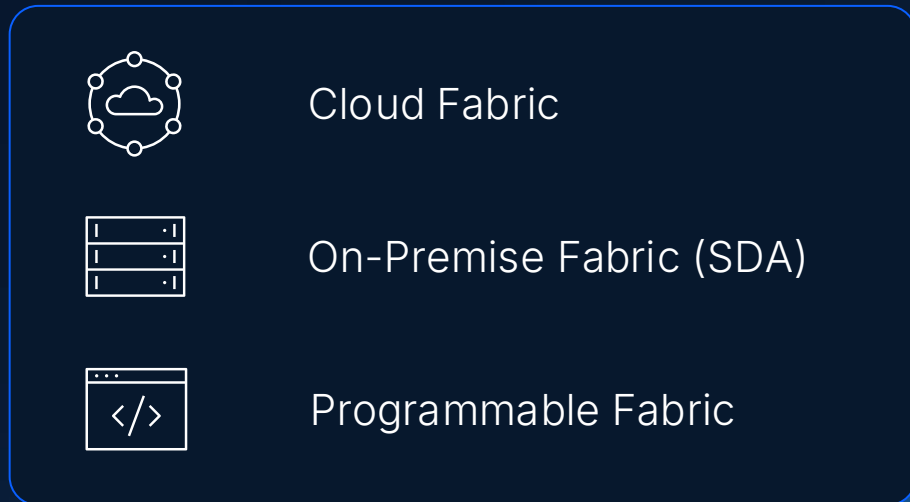
## Scalable Network Segmentation

# A unified framework for managing security policies across diverse IT environments



## Scalable Network Segmentation

# Simplifying network segmentation through automation with campus fabric



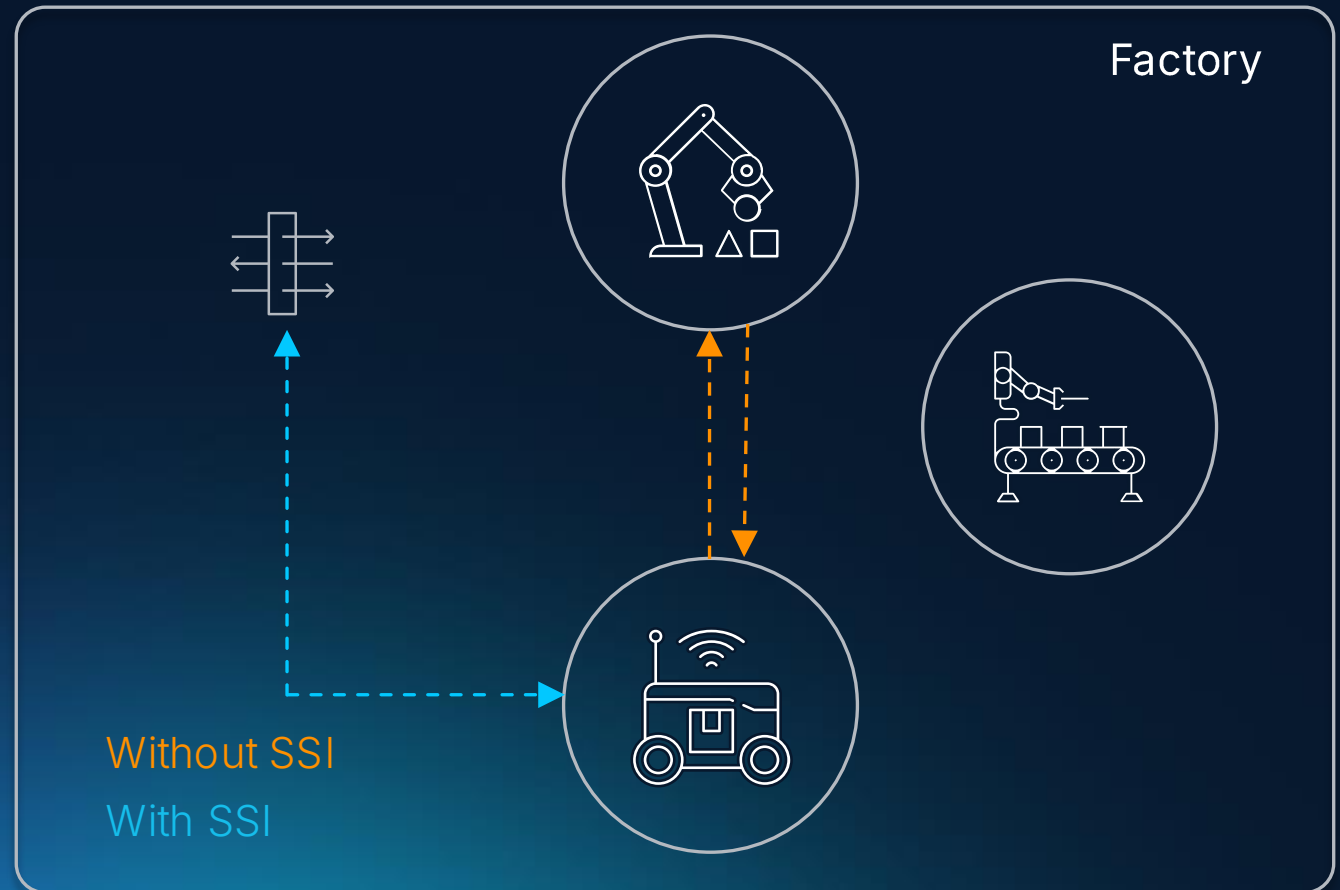
Scalable Network Segmentation

# Firewalling for any network flow, at scale

## Security Service Insertion

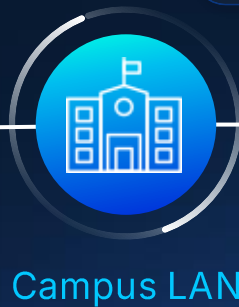
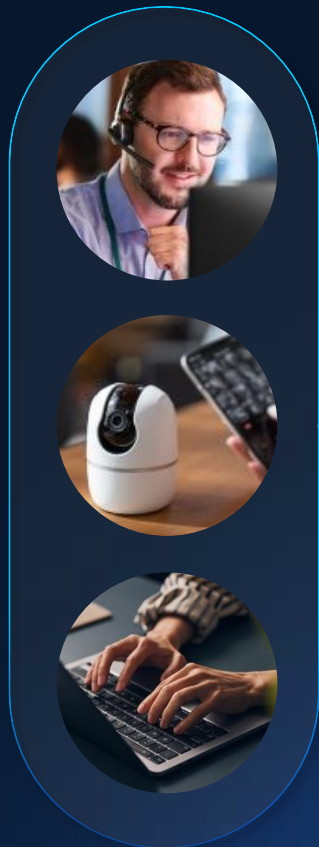
GA Mar 2026

- Logically insert Firewalling in any traffic flow
- Bring east-west traffic between micro-segments to existing Security infra, at scale
- Stateful steering for operational simplicity (manage the return flow automatically)
- Vendor agnostic, works with any firewall
- If using Cisco Firewall, can enforce policies directly by micro-segment (SGT-based)



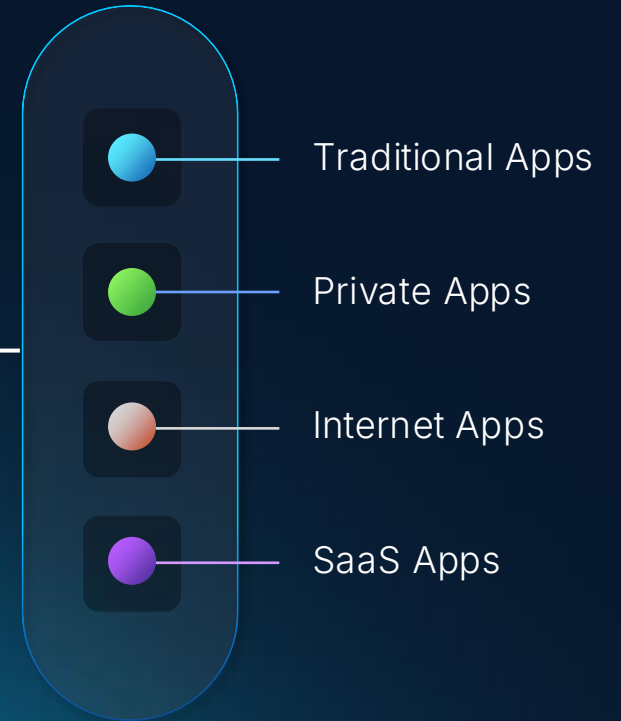
# Connecting and securing every corner of the network

Users, Devices, and Things



Data Loss Prevention (DLP)	WAN Optimization and Routing
Secure Web Gateway (SWG)	Firewall as a Service (FWaaS)
Cloud Access Security Broker	Remote Browser isolation (RBI)

Secure Application Access



Consistent WAN Security  
Security Service Edge + SD-WAN

Zero-Trust Network Access

# Segmentation and deep inspection of traffic between zones

SECURITY CLOUD CONTROL



Cisco  
Firewalls

Physical | Virtual | Cloud | FWaaS



3rd Party  
Firewalls



Smart  
Switches

eBPF



Workload  
Agents

Define once, enforce everywhere

# Advancing network resilience with proactive security hardening



Reduce the attack  
surface



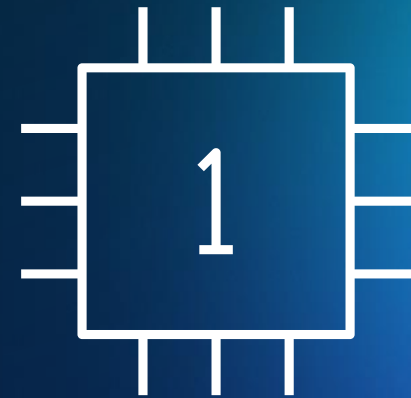
Protect sensitive  
data



Enable the  
defender

**Driving comprehensive improvements to our baseline security posture**

# Scalable devices ready for AI



# Scalable devices ready for AI

INTRODUCING

---



Smart Switches



Secure Routers



Campus Gateway



Secure Firewall



Large Venue Wi-Fi 7

Powered by

## Silicon One A100L & Silicon One K100L

Boosts hardware encryption post quantum security

Flexible and programmable for future AI and ML workloads

Intelligently adaptable to mitigate link failures, congestion, and bandwidth challenges

High-scale and low latency for time-sensitive applications

Efficient power performance



# Cisco Silicon One for Scale, Security, and Efficiency

# Cisco brings its IT expertise to rugged environments



Enterprise Grade

Best of IT innovations



Industrial Strength

Purpose built for harsh environments

Standardized equipment | Centralized management | Enterprise-wide security  
High-performance networking | One licensing model

**CISCO** Connect

Thank you



