


# Connecting & Securing Critical Infrastructure with Industrial Networking in an AI- Native World

Jack Reader- Industrial Internet of Things, Solutions Engineer

[jreader@cisco.com](mailto:jreader@cisco.com)



# Cisco powers how people and technology work together across the physical and digital worlds



AI-ready data centers



Future-proofed workplaces

Secure global connectivity



Digital resilience

Accelerated by Cisco AI

# Cisco Extends IT to the Physical World (OT)



Uniform network architecture  
Common OS and network management  
Consistent security policies

# Scalable Industrial Networks, Built for the AI Era



Industrial switches for  
**AI-driven operations**

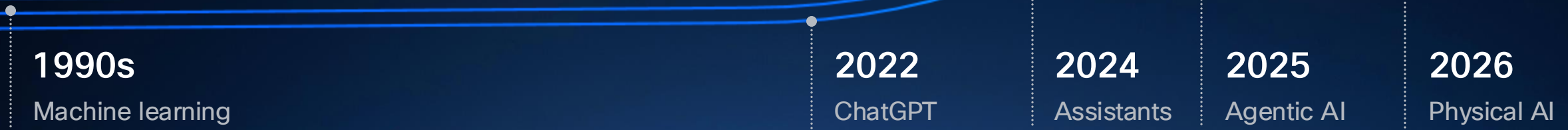


Redefining Wi-Fi to support  
**AI-driven industrial mobility**



# The AI Pace Is Staggering

When to jump in?

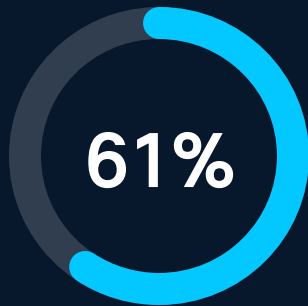


# AI Is Already Driving a Paradigm Shift for Industrial Networks

<https://www.cisco.com/site/us/en/solutions/networking/industrial-iot/industrial-networking-report/index.html>



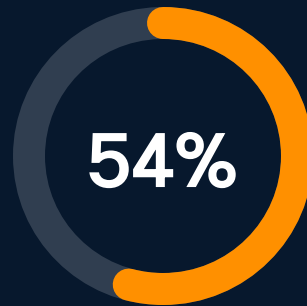
## “Active”



are actively deploying industrial AI

Q. Your organization's current stage of AI adoption in industrial operations?

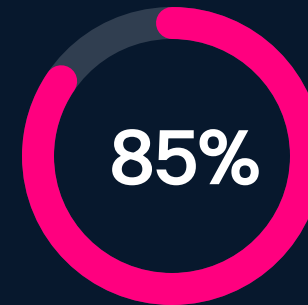
## “Payoff”



are already seeing payoffs from AI

Q. When do you expect to see these outcomes?

## “Security”



say AI will improve cybersecurity posture

Q. Will deploying AI impact your current cybersecurity posture?

# AI Is Transforming Critical Infrastructure (Industrial AI)



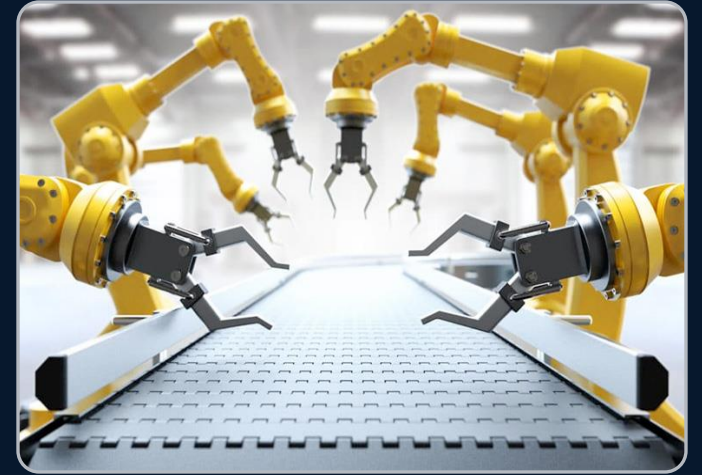
## Machine Vision

Quality inspection, Robot guidance, Packaging, Yield optimization, etc.



## Autonomous Vehicles

Automated guided vehicles (AGVs), Autonomous mobile robots (AMRs), Tele-remote operations, etc.



## Software Controls

Software-defined Industrial Automation, Virtual PLCs, etc.

To enable industrial AI use cases, a new network paradigm is required

# Vision Systems Needing Higher Wattage

e.g. 480W Power Over Ethernet Budgets



PTZ video surveillance for gunfire incidents

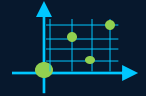


Cameras with heater/blower in extreme weather



Asset thermal monitoring to reduce maintenance costs

# Cisco Is Enabling AI at Every Networking Layer



AI Infra. Stacks

Vertical markets

## Industrial AI

### AI Tooling

How we use AI to make the life of our customers easier

### AI for Networking



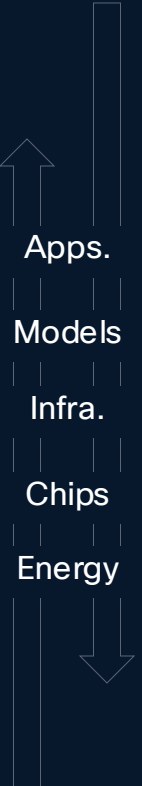
### AI Infrastructure

How do we enable our customer AI projects

### Networking for AI

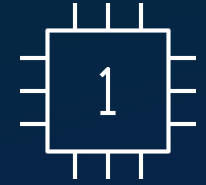
Pragmatic  
Task-level

Transformational  
Secure AI Factory



# To Enable Industrial AI, A New Network Paradigm Is Required

**Scalable network**  
ready for AI



**Operational simplicity**  
powered by AgenticOps

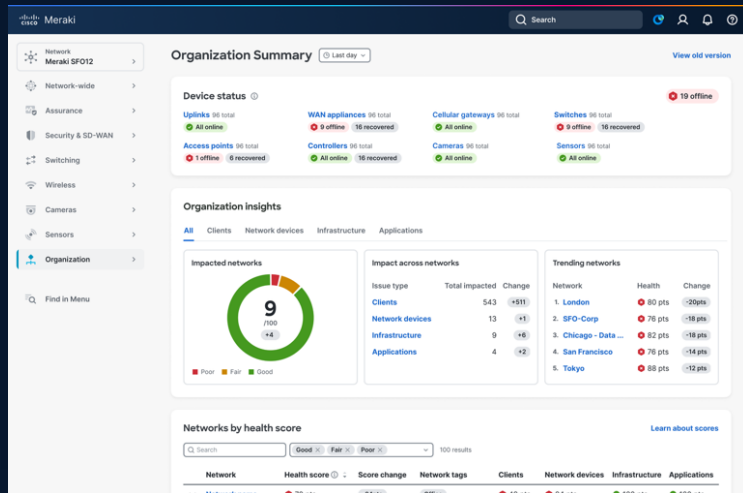


**Security**  
fused into the network



# New Pragmatic Innovations to Drive Operational Simplicity in OT

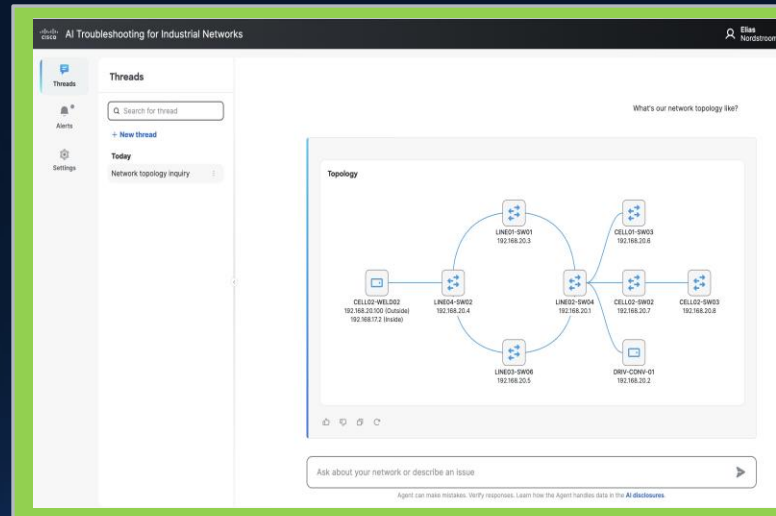
**NEW!**



## Cloud Management for Rugged Networks

Simplifying management across IT and rugged networks with the Meraki dashboard

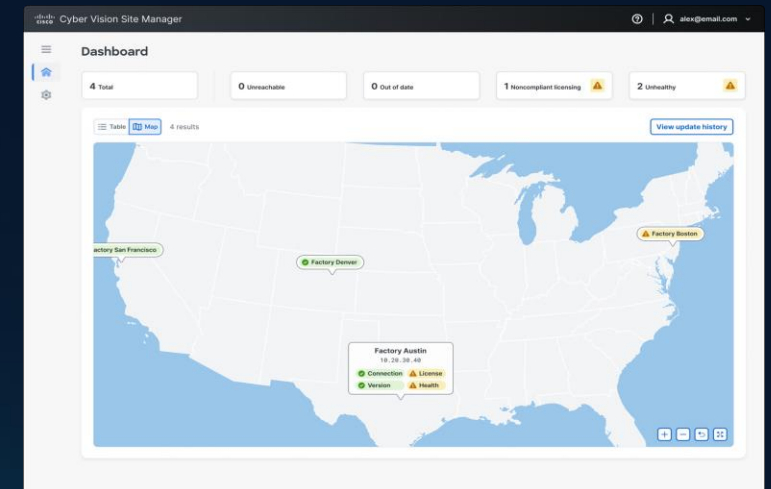
**NEW!**



## AgenticOps for Industrial Networks

Simplifying troubleshooting for OT teams to maximize network availability

**NEW!**



## Multi-site OT Threat Intelligence Distribution

Simplifying OT threat intel deployment and security infrastructure management

# Keeping Industrial Networks Running

Increased pressure on OT personnel to “do more with less” ensuring network availability



*Available on site*

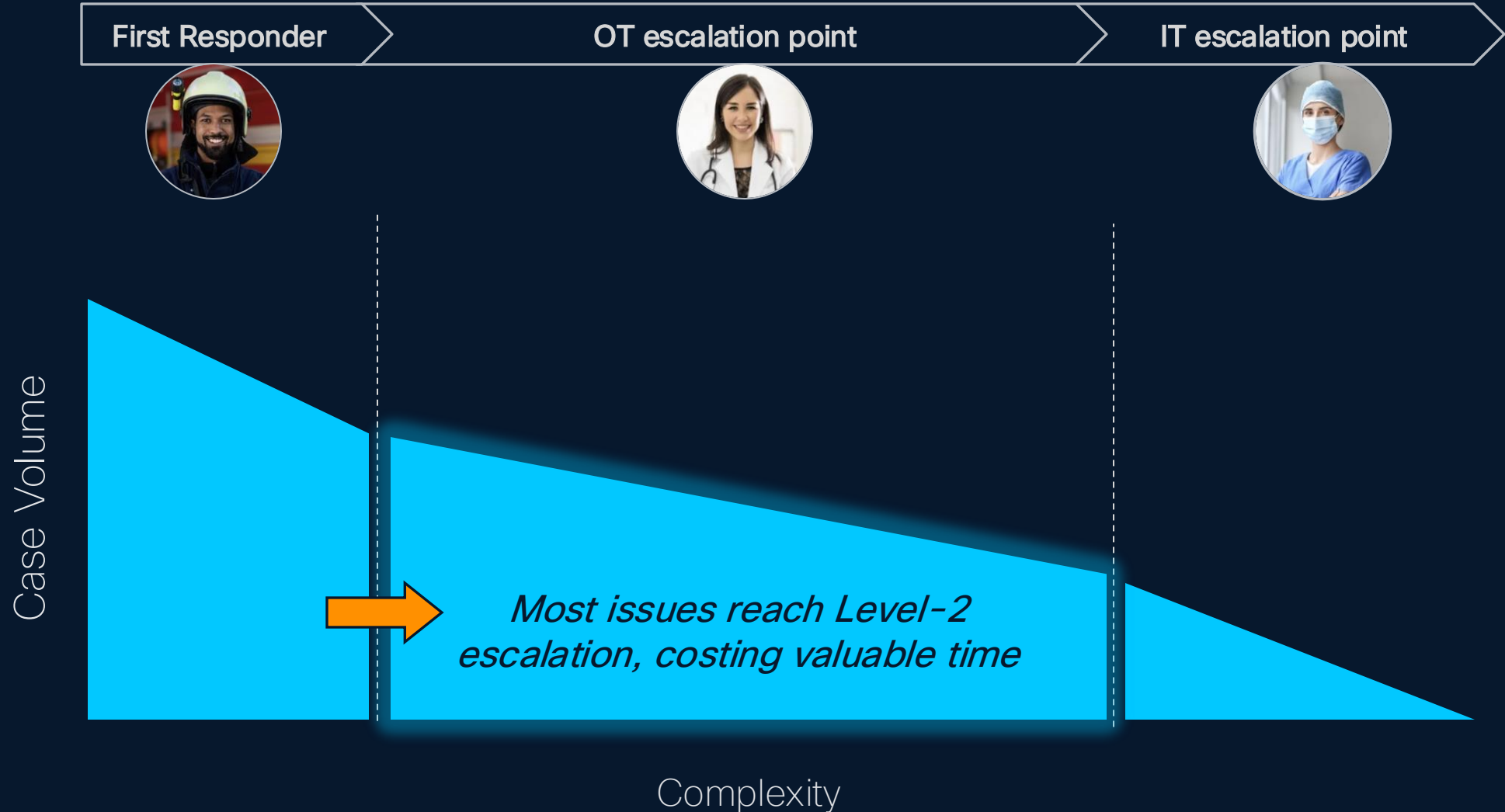
*Low IT skills*

*Not available on site*

*High IT skills*

# First Responders Lack Advanced Troubleshooting Skills

Before



# Introducing AgenticOps for Industrial Networks

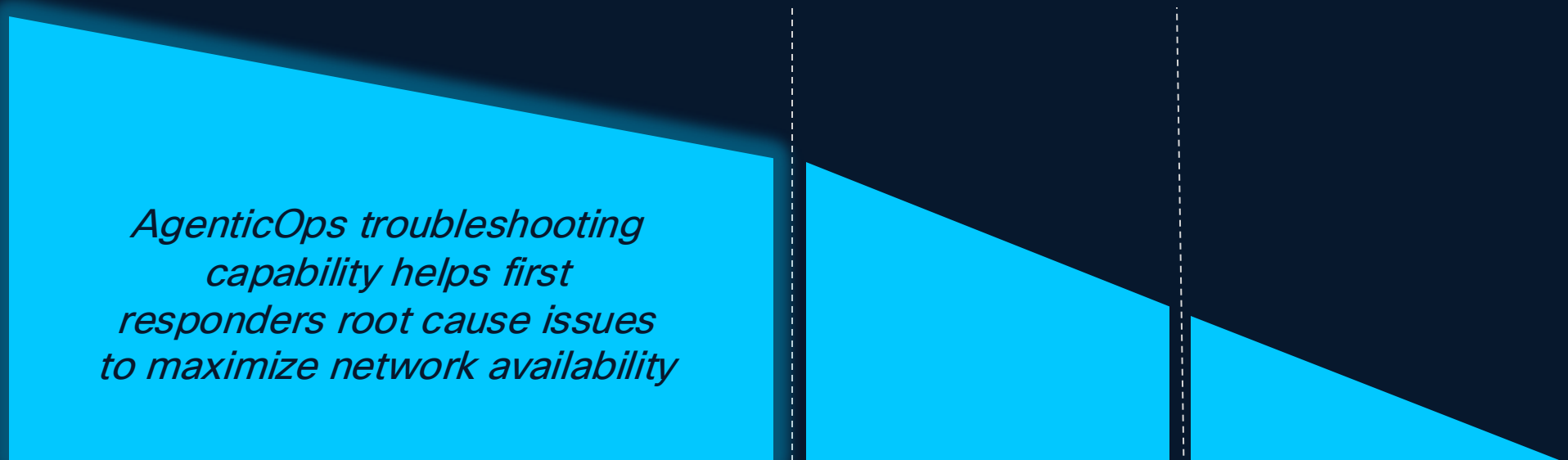
Today



With AgenticOps troubleshooting capability



Volume

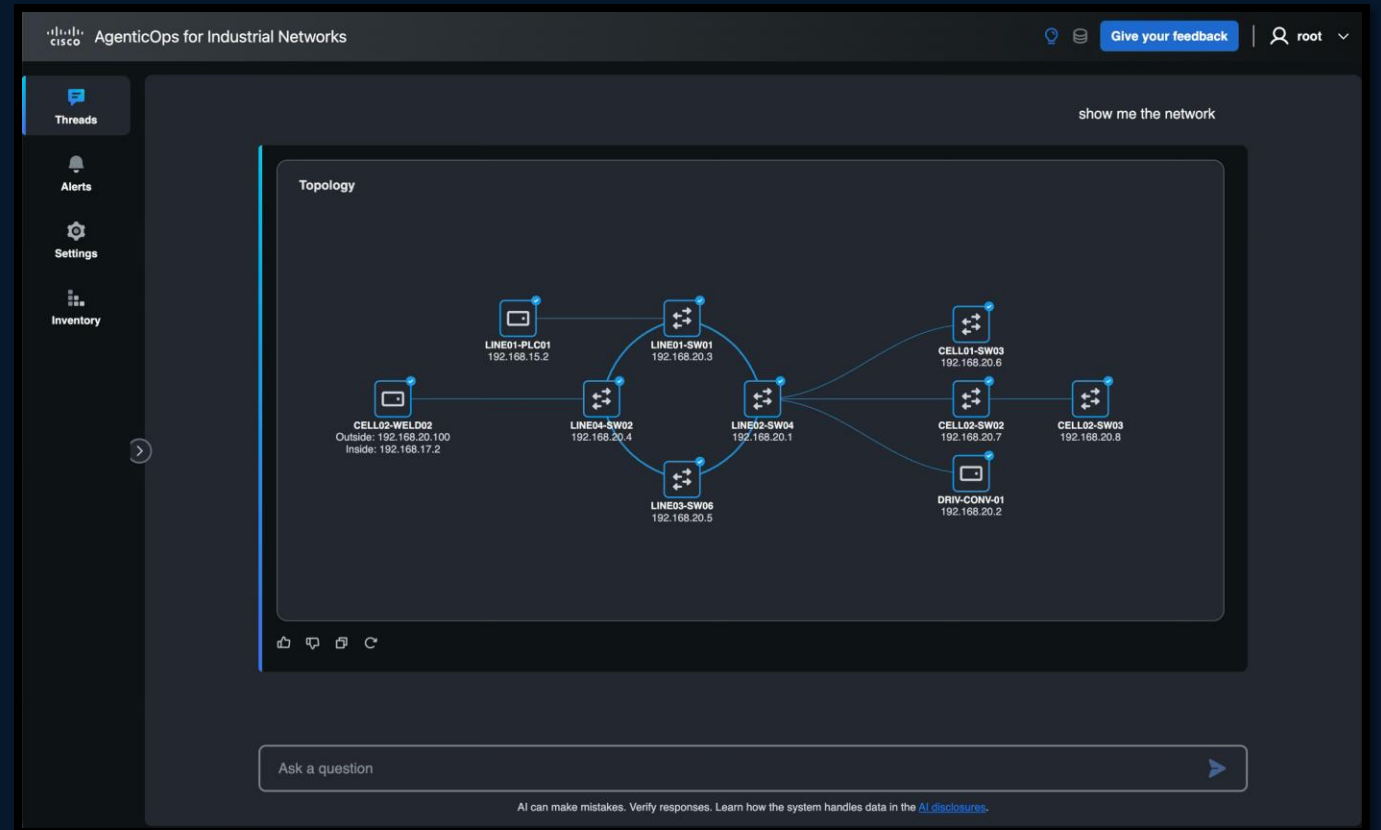


Complexity

# Introducing AI Troubleshooting for Industrial Networks

- An OT centric conversational interface for first responders to troubleshoot without escalation
- Proactively root cause issues in industrial networks to maximize availability
- Provides actionable guidance to enable OT teams to implement fixes quickly
- Agentic Engine deployed in Industrial Zone (Level 3)

Empowering OT teams to  
maximize network availability



# Empower OT Teams to Maximize Network Availability

## Key Features

Simple Network Questions

Troubleshooting (e.g. damaged cable)

Proactive Monitoring (e.g. duplicate IP)

## Deployment Mode

On-prem Agent + Cloud LLM

## Data Sources and Reasoning

SSH and Syslog

Curated runbooks

# Introducing AgenticOps for industrial Networks

*Now*

## Operational Issues

E.g. Faulty Cables,  
Duplex Mismatch

*Now*

## Misconfiguration Issues

E.g. Duplicate IP, VLAN Mismatch,  
NAT Misconfigurations

*Next*

## Prevent Production Impact

MCP Integrations with  
automation systems

# Example Use Cases

Case 1: damaged cable

Case 2: duplicate IP

# Access Layer Troubleshooting

The Agent leverages **tools** to troubleshoot top access layer issues.

Knows how to detect... ...using

Damaged cable    Interface errors and TDR test

VLAN mismatch    Switch VLAN configurations

Duplex mismatch    Interface speeds

Layer 2 NAT Misconfiguration    Layer 2 NAT instances

where is plc01 on line01 connected to?

PLC01 on LINE01 is connected to the following devices: LINE04-SW02 (IP: 192.168.20.4) via port Gi1/10, LINE02-SW04 (IP: 192.168.20.1) via port Gi1/3, and itself (IP: 192.168.15.2) via Vlan500.

Port Diagram

Port 1/7 - LINE01-PLC01  
IP: 192.168.15.2

can you run a cable test on LINE01-PLC01?

**Problem**

Cable diagnostic test on interface Gi1/7 of device LINE01-PLC01 (192.168.15.2) shows Pair A with a 'Short' status and Pair B as 'Open', indicating significant connectivity issues. Recommend replacing the faulty cable.

**Recommendation**

1. Inspect and replace the cable connected to interface Gi1/7 on LINE01-PLC01 (192.168.15.2).
2. After replacing the cable, rerun the TDR test to ensure that both Pair A and Pair B are functioning correctly.
3. Document the changes and monitor the interface for any further connectivity issues.

**Analysis**

The cable test results indicate that there are critical issues with the cabling connected to interface Gi1/7. Pair A's 'Short' status suggests a physical fault, while Pair B being 'Open' indicates a break in the connection. This could lead to network disruptions and should be addressed promptly.

**How this was determined** ^

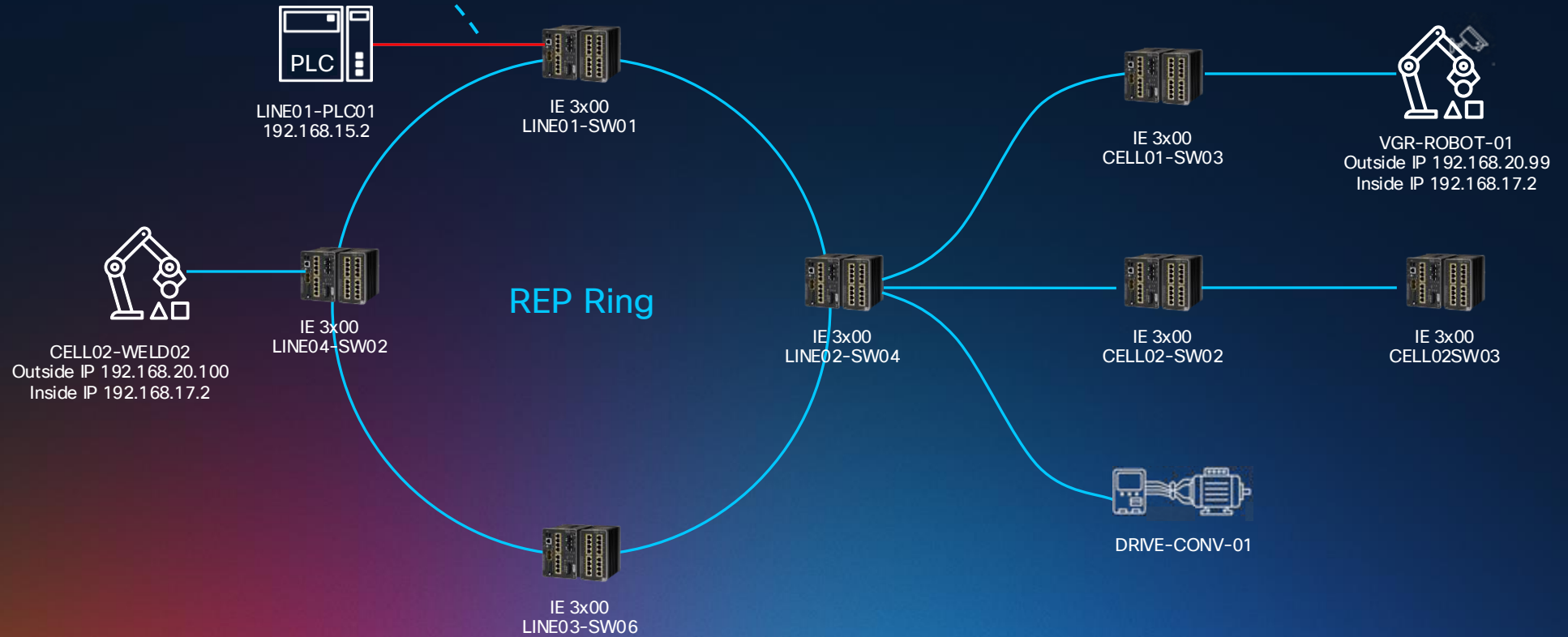
- 1) Check if interface name provided by user  
less than a minute ago
- 2) Gather Topology Information  
less than a minute ago
- 3) Identify Device IP  
less than a minute ago

# Demo Case 1

## Damaged cable




- Identify the device by asset name
- Retrieve topology
- Ping test
- Check parent switch port status

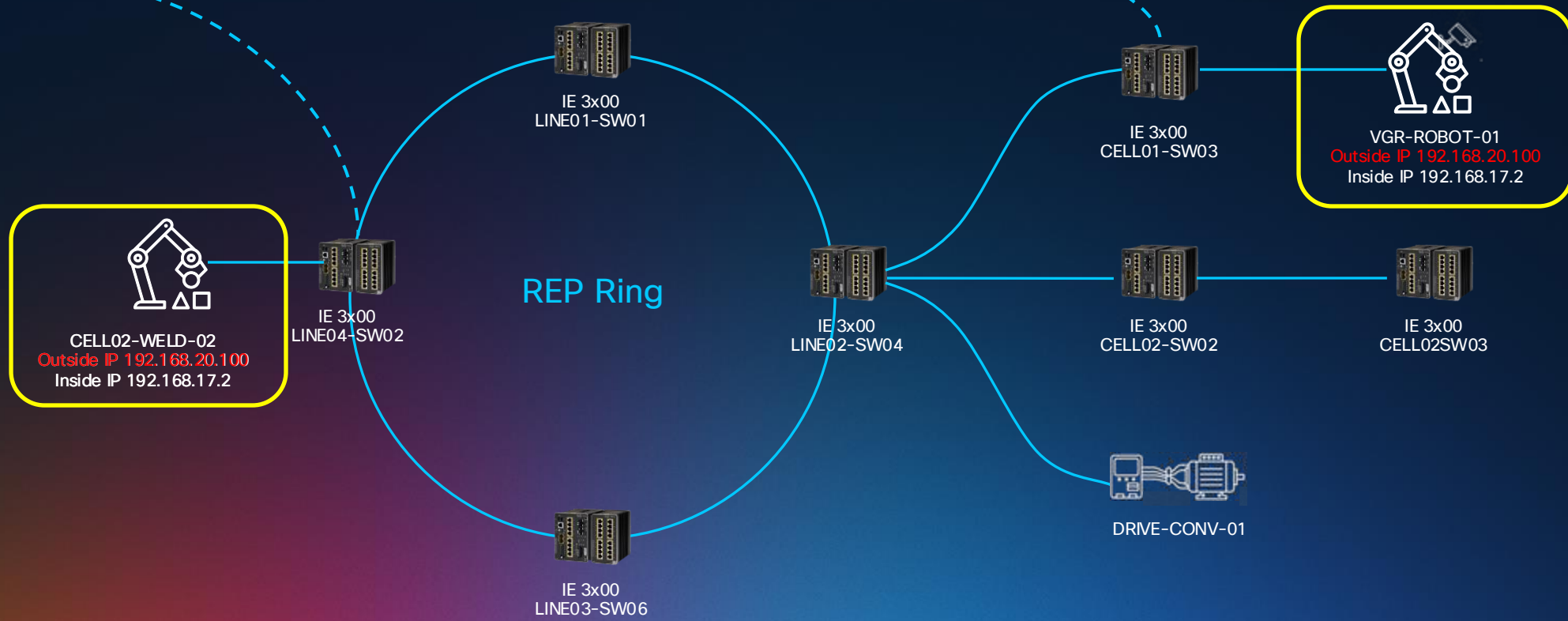


# Demo Case 2

## Duplicate IP addresses

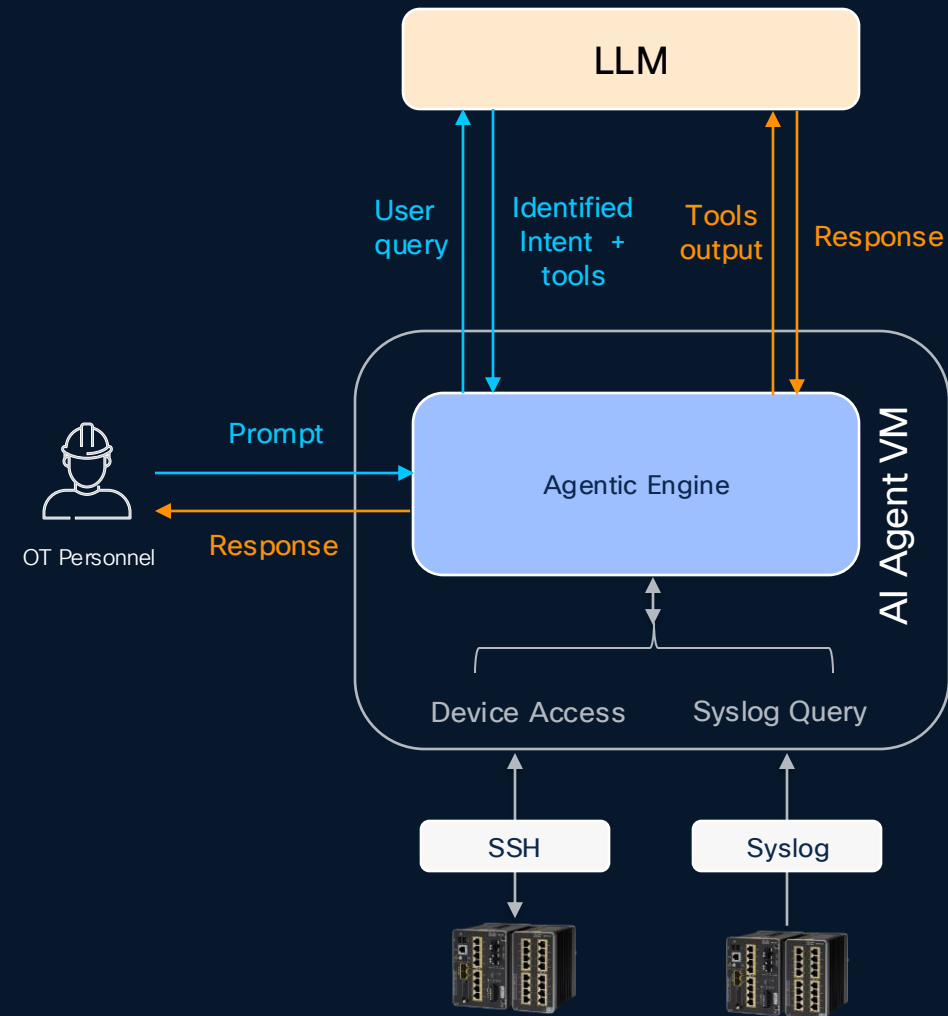
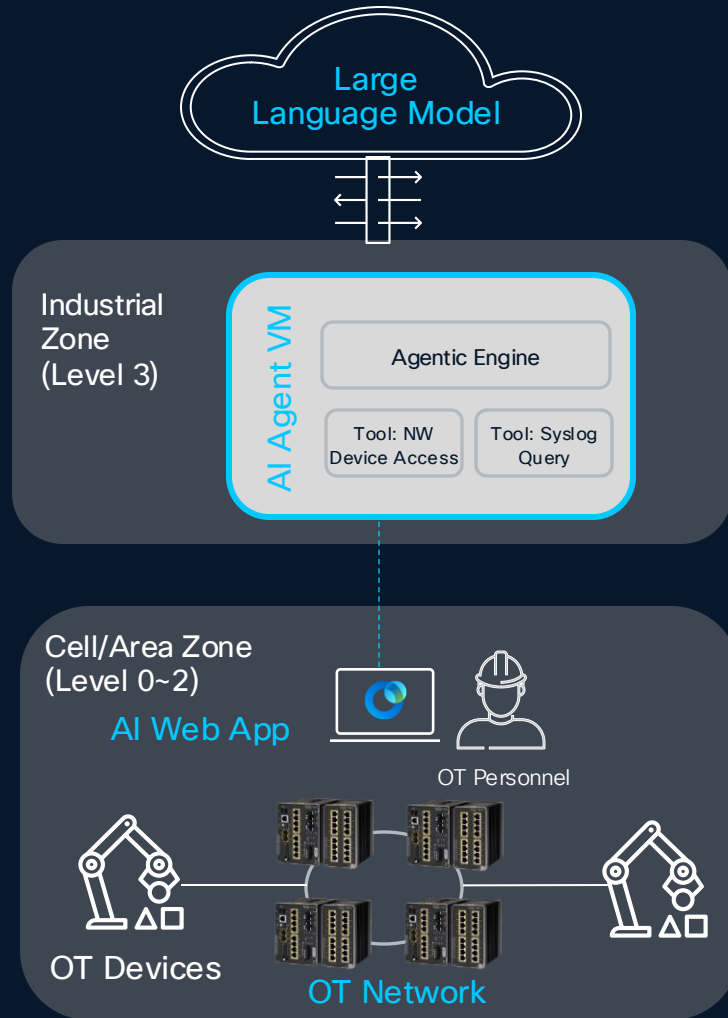
 **AgenticOps**

- Detect L2NAT config
- SSH to switch and diagnose
- Finds Duplicate IP
- Recommends config fix



# How the Agent Is Deployed and How It Works

Alpha



# Customer Journey

- 1 Discover
- 2 Download
- 3 Install
- 4 Setup
- 5 Use
- 6 Monitor
- 7 Upgrade

OT Architect

OT Maintainer

Discover AI Agent URL in product UIs:

Web UI / CLI

Download VM image (ESXi, HyperV)

Cisco Software Central

Install Agent as VM

12 CPU Cores, 24 GB RAM (Alpha)

Agent discovers devices

1. First switch as seed
2. Traverse the network LLDP
3. Use ARP and MAC tables for endpoints

Access agent via URL

<https://ciscootagent.custom-er.com> (example)

Provide API for monitoring (GA)

Running time / version / status / skills

Agent update/upgrade:

Human download / Agent pull from Cisco Cloud platform



# Invitation to Alpha Engagement (GA Late 2026)

AI Troubleshooting for Industrial Networks

## Ideal Profile:

- Manufacturing, switching
- Primarily Cisco IE switches as the install base
- Flexible for Cloud AI connectivity
- Innovative and forward looking, willing to test engineering prototype and provide feedback
- English speaking and preferably US based

Cisco AI Troubleshooting for industrial networks Alpha interest form



## Customer Feedback

“It helps sequence the logical steps during troubleshooting because often the little things are forgotten”

“This will help me sleep more at night - it'll reduce often escalations during ride testing and bring up”

# AI-Driven Semantic Search & Summarization

[Neelesh Pateriya](#)

November 18, 2024

<https://blogs.cisco.com/developer/new-ai-driven-semantic-search-and-summarization>



**Cisco Blogs** Executive Platform AI Networking Data Center Security More ▾

Cisco Blogs / Developer / New AI-Driven Semantic Search and Summarization

November 18, 2024 3 Comments

Developer  
**New AI-Driven Semantic Search and Summarization**  
5 min read  
[Neelesh Pateriya](#)

In today's fast-paced digital landscape, finding precise and relevant information is crucial. At DevNet, we continuously innovate to enhance the user experience and streamline how our users interact with our platform. Today, in collaboration with the Meraki API team, we are excited to announce the launch of our new AI-driven Semantic Search and Summarization beta feature for [Meraki API documentation](#). This powerful new tool leverages advanced Artificial Intelligence (AI) and Large Language Models (LLMs) to revolutionize how users search and retrieve information, making it more accurate, efficient, and intuitive.

This launch brings substantial improvements and benefits, showcasing the capabilities of the platform built by the DevNet group. The Meraki API team conducted an extensive user survey, highlighting several challenges and enhancements requested by users for API searches. These inputs have been integrated into the new UX improvements and semantic search feature development. Users will now enjoy support for natural language queries, enabling more intuitive and conversational interactions. Our search engine matches results based on the meaning and context of the queries, rather than just keywords, ensuring more relevant and precise results. Additionally, the feature includes summaries of search results, providing concise and actionable information at a glance, and an improved user experience with enhanced navigation and access to related resources.

In this blog post, we'll explore the features, benefits, and challenges that the new Semantic Search and Summarization feature addresses. We will delve into the technical details in follow-up blogs.

### What is Semantic Search?

Semantic search is a groundbreaking technology that goes beyond traditional keyword searches. It focuses on the meaning and context of search queries instead of just matching words. Unlike conventional searches, which return results based only on specific terms, semantic search interprets the intent behind the queries to deliver more relevant and accurate results.

Our semantic search engine uses advanced Artificial Intelligence (AI) and Large Language Models (LLMs). These tools help it understand complex queries and provide precise, contextually relevant answers. It leverages Natural Language Processing (NLP) and vector search techniques. This means it can understand the nuances of human language and find information based on meaning. Even if the exact keywords are not present, the search engine can still identify and retrieve relevant content by understanding the underlying meaning. This results in a more intuitive and effective search experience.

### Key Features of the New AI-Driven Semantic Search

Our new semantic search comes packed with several innovative features designed to enhance your search experience and address common challenges:

- **Contextual Understanding and Advanced Query Interpretation:** Our AI-driven semantic search engine interprets the meaning behind your queries by leveraging advanced algorithms and large language models (LLMs). This enables the search engine to grasp the nuanced intent behind your searches, ensuring that the results are contextually relevant. By understanding complex user queries and delivering the most pertinent information, this feature addresses the challenge of irrelevant search results, providing you with more precise answers.
- **Support for Natural Language Queries:** Users can now search using natural language, making interactions more intuitive and conversational. This feature allows you to ask questions in a more human-like manner, and the search engine will understand and process these queries effectively. When you search using natural language queries, our semantic search engine leverages contextual understanding and advanced query interpretation to match your queries against the indexed content. We index the content using similar techniques, ensuring that the search results are not just based on keywords but on the actual meaning and context of the queries. This is achieved through vector search, which finds results based on semantic similarity.

# Cisco MCP Basics

Shannon McFarland

March 12, 2025

<https://blogs.cisco.com/developer/mcp-usecases>



Cisco Blogs Executive Platform AI Networking Data Center Security More

Cisco Blogs / Developer / MCP for DevOps, NetOps, and SecOps: Real-World Use Cases and Future Insights

May 12, 2025 7 Comments

Developer  
MCP for DevOps, NetOps, and SecOps: Real-World Use Cases and Future Insights  
5 min read  
Shannon McFarland

MCP for DevOps, NetOps, and SecOps: Real-World Use Cases and Future Insights

In the previous post on MCP for DevOps: Architecture and Components, we discussed what MCP is and is not. We dove into a few architectural components and gently touched on use cases. Now, let's explore a few possible use cases for MCP in DevOps/NetOps/SecOps.

I have cherry-picked a few customer and partner use cases I've personally worked with and found appropriate for our discussion. My list will not be exhaustive, but it should give you a solid view of practical uses for MCP. Let your mind ponder the possibilities in your environment. 🍷

In the YouTube series on MCP for DevOps, we will leverage some use cases to build a working implementation with MCP, tools, and Cisco products.

Recap - Model Context Protocol (MCP)

If you didn't catch part 1 in this blog series on MCP for DevOps: Architecture and Components, check it out. But for now, here's a quick level-set on MCP. As illustrated in Figure 1, the Model Context Protocol (MCP) provides a uniform way to integrate an AI model into tools and services.

Figure 1. MCP with LLMs and Tools

LLM

MCP Hosts (AI Application)

Tools / Data Sources

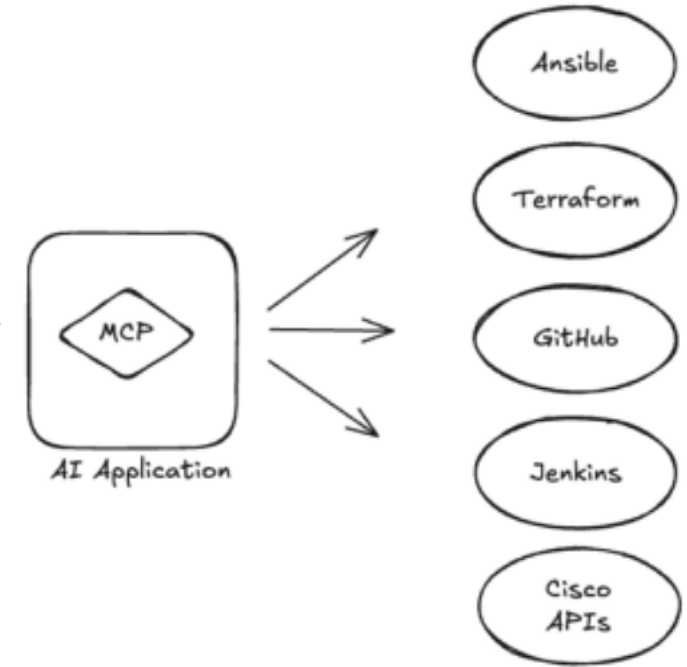
API, webservers

Files, DBs

It is:

- A lightweight communication protocol designed specifically for AI agents and applications.
- Built to connect those agents to tools, APIs, databases, and file systems.
- Structured as a client/server architecture—simple and predictable.
- Plumbing

Figure 2. MCP with Tools, Services, Platforms



# MCP Today – Enabling Tool Integration

MCP (Model Context Protocol) released in November 2024 is now a broadly adopted open-source standard created by Anthropic that allows AI models to securely connect with external data, software tools, and databases. It acts as a "universal translator" or connector, enabling AI assistants to read files, query databases, and use software, turning them into active, functional agents. Think of MCP as a universal language that AI models and tools can use to collaborate.

[MCP tutorial](#)

Click:

[Cisco DevNet for AI](#)

This is a demonstration project showcasing MCP server implementations for network management.

Intended for educational purposes, testing, and development environments.

Docker-based MCP server suite for AIOps – enabling AI-driven network operations through:

- Cisco Meraki
- Catalyst Center
- **IOS XE**
- ISE
- ThousandEyes
- Splunk
- NetBox & GitLab integration
- AI-ready with LibreChat, Cursor, and other MCP clients for intelligent network management, automated troubleshooting, CI/CD orchestration, and operational insights.

# Launch of DevNet Content Search MCP Server

Neelesh Pateriya

March 12, 2026

<https://blogs.cisco.com/developer/devnet-content-search-mcp-server>



Cisco Blogs / Developer / Launch of DevNet Content Search MCP Server

March 12, 2026 [Leave a Comment](#)

Developer  
Launch of DevNet Content Search MCP Server  
3 min read  
Neelesh Pateriya

From Search on the Web to Search in the IDE

Last year we launched [AI-driven semantic search](#) for Meraki API docs on [developer.cisco.com](#)—but developers live in their IDEs, not the browser. Without the right context, AI assistants in the IDE fall back to outdated or generic knowledge when it generates code.

The [DevNet Content Search MCP server](#) is the next step in that evolution: it takes the same semantic search that powers [developer.cisco.com](#) and puts it inside **your IDE**, where your AI assistant can use it in real time. MCP (Model Context Protocol) is a standard that lets IDE AI assistants call live tools—in this case, searching Cisco API documentation—so you get accurate, current context without switching windows. One click to install, nothing to configure, and your IDE can now ground its code suggestions in **official Cisco API specs** instead of outdated or generic knowledge.

Today the server supports **Meraki** and **Catalyst Center** API documentation; we’re expanding to more Cisco products and DevNet content. Want your product’s APIs included? [Create an issue](#) to request it.

### One-Click Install, Live API Search

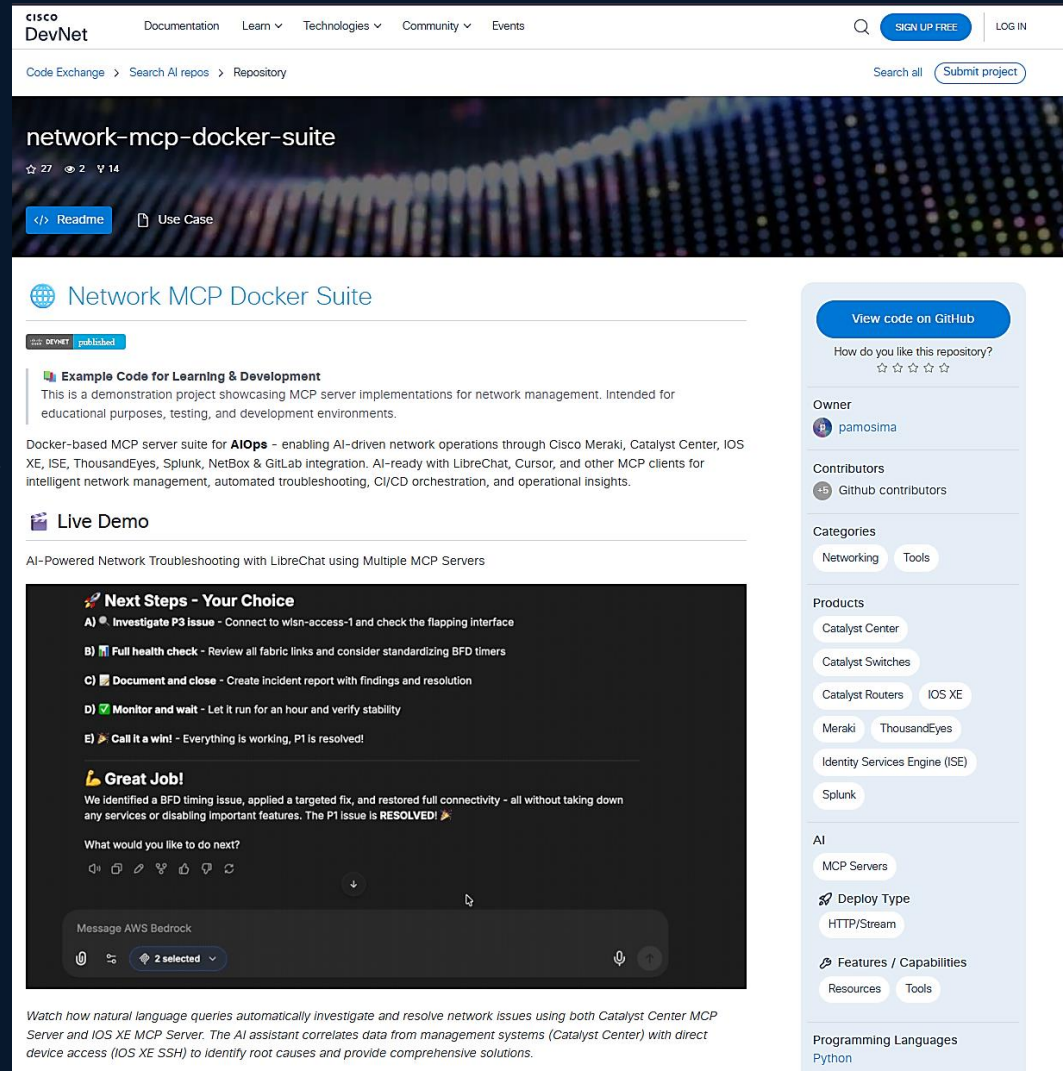
The DevNet Content Search MCP server has one-click install for [VS Code](#) or [Cursor](#)—your environment is ready, nothing to configure. The server doesn’t replace the browser; it brings the right slice of DevNet into the flow of coding.

Once installed, try a query from your IDE chat panel—for example, “*Find Meraki L3 firewall API endpoints for configuring traffic rules*” or “*Find Catalyst Center APIs for device inventory management*”—and see the AI assistant pull live documentation and use it in its response.

```
CONFIGURATION
Name: devnet-content-search
Type: MCP
URL: https://devnet.cisco.com/...

Chat
MERAKI API FOR L3 FIREWALL MX UPDATE
Find Meraki API for L3 Firewall MX update
Searched Meraki API documentation for L3 Firewall.
Run Meraki[API]DocSearch - devnet-content-search (MCP Server)
Here is the Meraki API for updating L3 Firewall rules on an MX network:
Update Network Appliance Firewall L3 Firewall Rules
Method: PUT
Path: /networks/{networkId}/app/lansec/firewall/l3fw/firewallRules
Operation ID: updateNetworkApplianceFirewallL3FirewallRules
```

# Docker-Based MCP Server Suite for AIOps



The screenshot shows the Cisco DevNet repository page for 'network-mcp-docker-suite'. The page includes a navigation bar with 'Documentation', 'Learn', 'Technologies', 'Community', and 'Events'. The repository title is 'network-mcp-docker-suite' with 27 stars, 2 forks, and 14 clones. A 'Readme' button is visible. The main content area features a 'Network MCP Docker Suite' header, a 'published' status, and an 'Example Code for Learning & Development' section. A 'Live Demo' section is also present, featuring a video player with a 'Next Steps - Your Choice' list and a 'Great Job!' message. The right sidebar contains a 'View code on GitHub' button, a 'How do you like this repository?' rating, and various filters for 'Owner', 'Contributors', 'Categories', 'Products', 'AI', 'Deploy Type', 'Features / Capabilities', and 'Programming Languages'.

**Example Code for Learning & Development**  
This is a demonstration project showcasing MCP server implementations for network management. Intended for educational purposes, testing, and development environments.

Docker-based MCP server suite for **AIOps** - enabling AI-driven network operations through Cisco Meraki, Catalyst Center, IOS XE, ISE, ThousandEyes, Splunk, NetBox & GitLab integration. AI-ready with LibreChat, Cursor, and other MCP clients for intelligent network management, automated troubleshooting, CI/CD orchestration, and operational insights.

**Live Demo**  
AI-Powered Network Troubleshooting with LibreChat using Multiple MCP Servers

**Next Steps - Your Choice**

- A) Investigate P3 Issue - Connect to wsn-access-1 and check the flapping interface
- B) Full health check - Review all fabric links and consider standardizing BFD timers
- C) Document and close - Create incident report with findings and resolution
- D) Monitor and wait - Let it run for an hour and verify stability
- E) Call it a win! - Everything is working, P1 is resolved!

**Great Job!**  
We identified a BFD timing issue, applied a targeted fix, and restored full connectivity - all without taking down any services or disabling important features. The P1 issue is **RESOLVED!**

What would you like to do next?

Message AWS Bedrock

2 selected

Watch how natural language queries automatically investigate and resolve network issues using both Catalyst Center MCP Server and IOS XE MCP Server. The AI assistant correlates data from management systems (Catalyst Center) with direct device access (IOS XE SSH) to identify root causes and provide comprehensive solutions.



[Thousand Eyes MCP Tools tutorial](#)

<https://developer.cisco.com/codeexchange/github/repo/pamosima/network-mcp-docker-suite/>

# Industrial NetDevOps on IOS XE

Getting Started with Programmability & APIs on Cisco IoT Hardware



## Industrial NetDevOps: Getting Started with Programmability & APIs on Cisco IoT Hardware

Industrial NetDevOps is the combination of the tools and best practices from DevOps with network engineering and operations in industrial networks.

Instead of using SNMP and CLI, you configure, manage and monitor industrial network devices via **standardized network device APIs and software automation tools**. Industrial NetDevOps workflows use Open Source, standards and Python scripts alongside commercial devices and tools to deliver flexible and fast-responsive industrial networks.

This is a collection of scripts which will get you started on how NETCONF & RESTCONF works especially on Cisco IoT hardware. Also, some Ansible playbooks are here to get you started with Ansible.

- IOS XE on Cisco IR1101
- IOS XE on Cisco IE3200, IE3300, IE3400
- IOX XE on Cisco ESS3300



### Script Overview

For more information on how to use these scripts, definitely check out the learning labs at [DevNet Learning Labs](#).



Industrial Ethernet Switch 3500

configure, manage & monitor  
NETCONF/  
RESTCONF



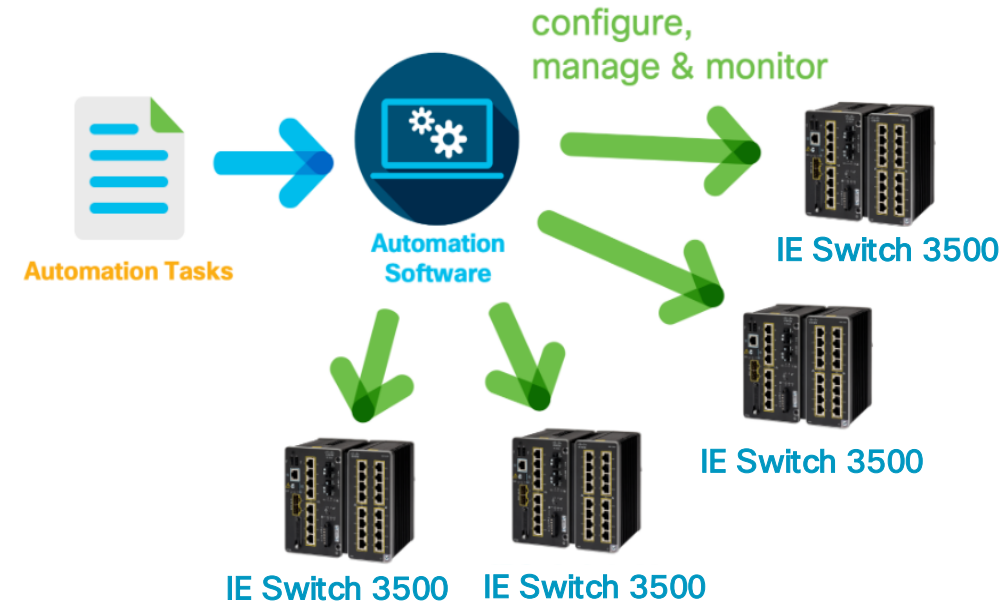
Any REST or NETCONF-capable Application

## Cisco Unified Edge



### Use-cases

#### Network Automation



MCP Server

<https://developer.cisco.com/codeexchange/github/repo/CiscoDevNet/industrial-netdevops/>

Files

main

Go to file

- .github
- .img
- catc-mcp-server
- clickhouse-mcp-server
- gitlab-mcp-server
- ios-xe-mcp-server
  - .dockerignore
  - Dockerfile
  - README.md
  - ios\_xe\_mcp\_server.py
  - pyproject.toml
- ise-mcp-server
- meraki-mcp-server
- netbox-mcp-server
- prometheus-mcp-server
- splunk-mcp-server
- thousandeyes-mcp-server
  - .env.example
  - .gitignore
  - CODE\_OF\_CONDUCT.md
  - CONTRIBUTING.md
  - LICENSE
  - NOTICE
  - README.md
  - SECURITY.md
  - USECASE.md
  - deploy.sh
  - docker-compose.override.yml.ex...
  - docker-compose.yml

network-mcp-docker-suite / ios-xe-mcp-server / README.md

pamosima feat(ios-xe): Add enable mode support for privilege escalation

9bf1302 · yesterday History

Preview Code Blame 415 lines (304 loc) · 12.8 KB

Raw, download, edit icons

# IOS XE MCP Server

A Model Context Protocol (MCP) server for managing Cisco IOS XE devices via SSH using Netmiko with enterprise-grade security.

## Overview

This MCP server provides secure SSH-based management capabilities for Cisco IOS XE devices, enabling:

- Device Configuration:** Send configuration commands to IOS XE devices
- Monitoring Commands:** Execute show commands for device monitoring
- Secure Authentication:** Environment-only credentials (no password parameters)
- Password Protection:** Comprehensive password masking and sanitization
- Enhanced Security:** SSH-based communication with timeout controls and error protection
- HTTP Transport:** Modern MCP transport for MCP clients (Cursor, LibreChat, etc.)

## Features

### Available Tools

- `show_command`: Execute any show command on an IOS XE device (credentials from environment only)
- `config_command`: Send configuration commands to an IOS XE device (only available when `IOS_XE_READ_ONLY=false`)

### Read-Only Mode

For monitoring and troubleshooting workflows, you can enable **read-only mode** which only exposes the `show_command` tool:

```
# In .env
IOS_XE_READ_ONLY=true # Only show commands available (recommended for AI troubleshooting)
IOS_XE_READ_ONLY=false # Both show and config commands (default)
```

Mode	IOS_XE_READ_ONLY	Available Tools
Read-Only	true	show_command only
Read-Write	false (default)	show_command + config_command

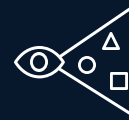
### Use Cases:

- netops-stack troubleshooting:** Set `IOS_XE_READ_ONLY=true` - AI can only run show commands

# Security Fused Into the Network

# Building Cyber-Resilient, AI-Ready Industrial Networks

Cisco Industrial Threat Defense



## Unified visibility across OT and IT

Insights to drive industrial security best practices and better detect threats traversing IT and OT domains



## Adaptive network segmentation

Protect industrial operations by streamlining network segmentation to prevent attacks from spreading



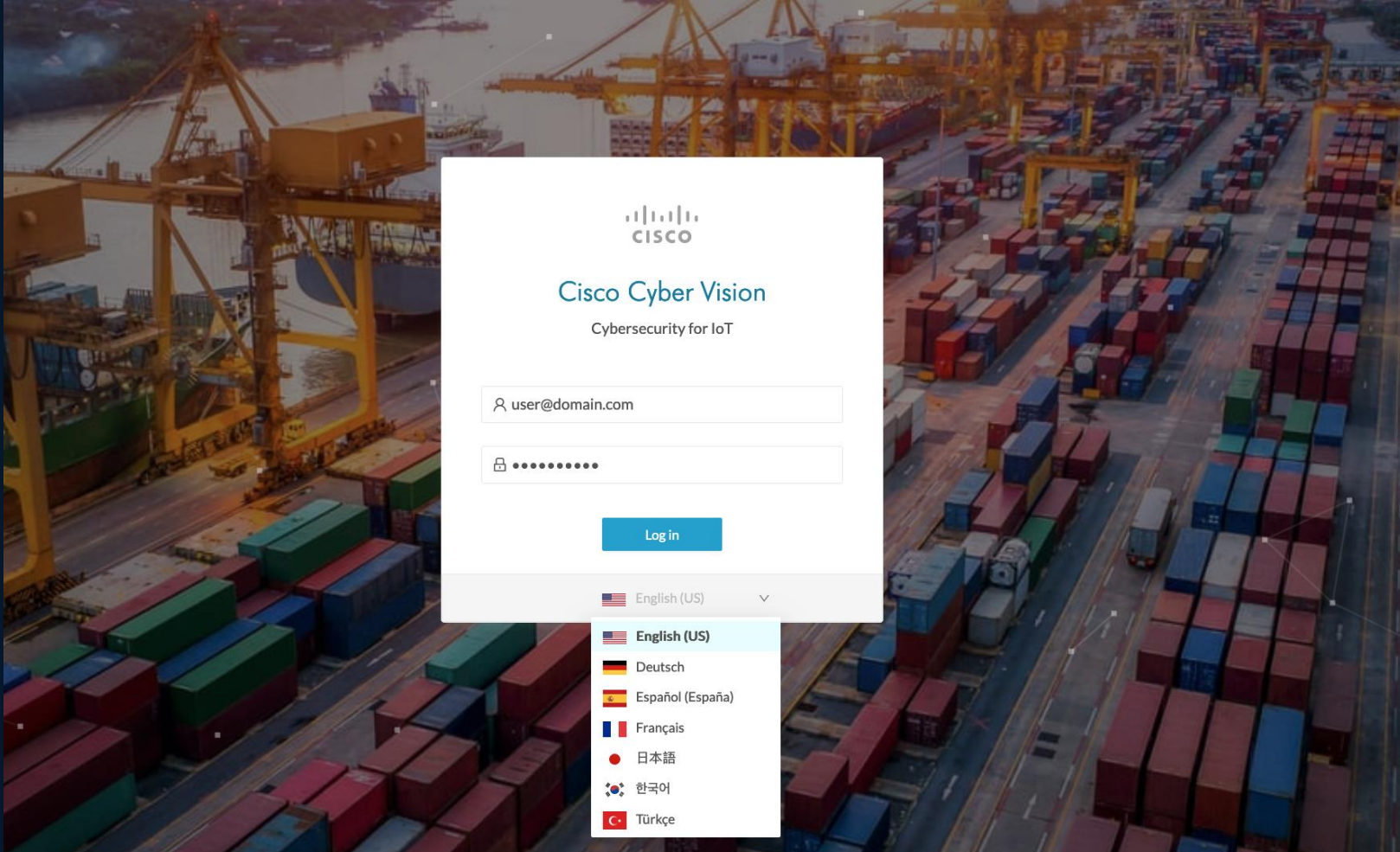
## Secure remote access

Get full control over remote access to industrial assets with a self-service ZTNA solution purpose-built for OT

Industrial security built into Cisco networking equipment to easily deploy at scale

# Cyber Vision UI

Multilingual support



User interface available in:

English

German

Spanish

French

Japanese

Korean

Turkish

# Cyber Vision



## Visibility

OT asset inventory  
Communication patterns



## Security Posture

Device vulnerabilities  
Risk scoring



## Zone Segmentation

Automate segmentation  
below the IDMZ to protect  
operations

The screenshot displays the Cisco Cyber Vision interface. At the top left, the Cisco logo and 'Cyber Vision' text are visible. The top right shows a user profile for 'Alexander alex@email.com'. A left-hand navigation menu includes 'Organization Global', 'Home', 'Alerts', 'Assets', 'Communications' (highlighted), 'Vulnerabilities', and 'Configuration'. The main content area is titled 'Communications' and shows a network diagram for 'Packaging Line 1'. The diagram features several nodes connected to a central hub. Nodes include 'SIEMENS', 'PANAC', 'SICK', and 'RA'. Each node is labeled with an IP address, such as '192.168.200.200' or '192.168.200.201'. A control panel on the left of the diagram allows filtering by 'OT Traffic', showing details, and sorting by volume. It also includes 'Map properties' (Time: Last 30 days) and 'Display options' (Asset identifier: IP address selected, Asset name unselected, Show volume unselected). At the bottom left of the diagram, it states 'Est total volume 45.7 MB'. At the bottom right, there are zoom and navigation icons. The top right of the main area indicates 'Assets here: 1286' and 'Edit filters'.

# Grouping Assets to Reflect Industrial Processes Is Challenging



Thousands of assets



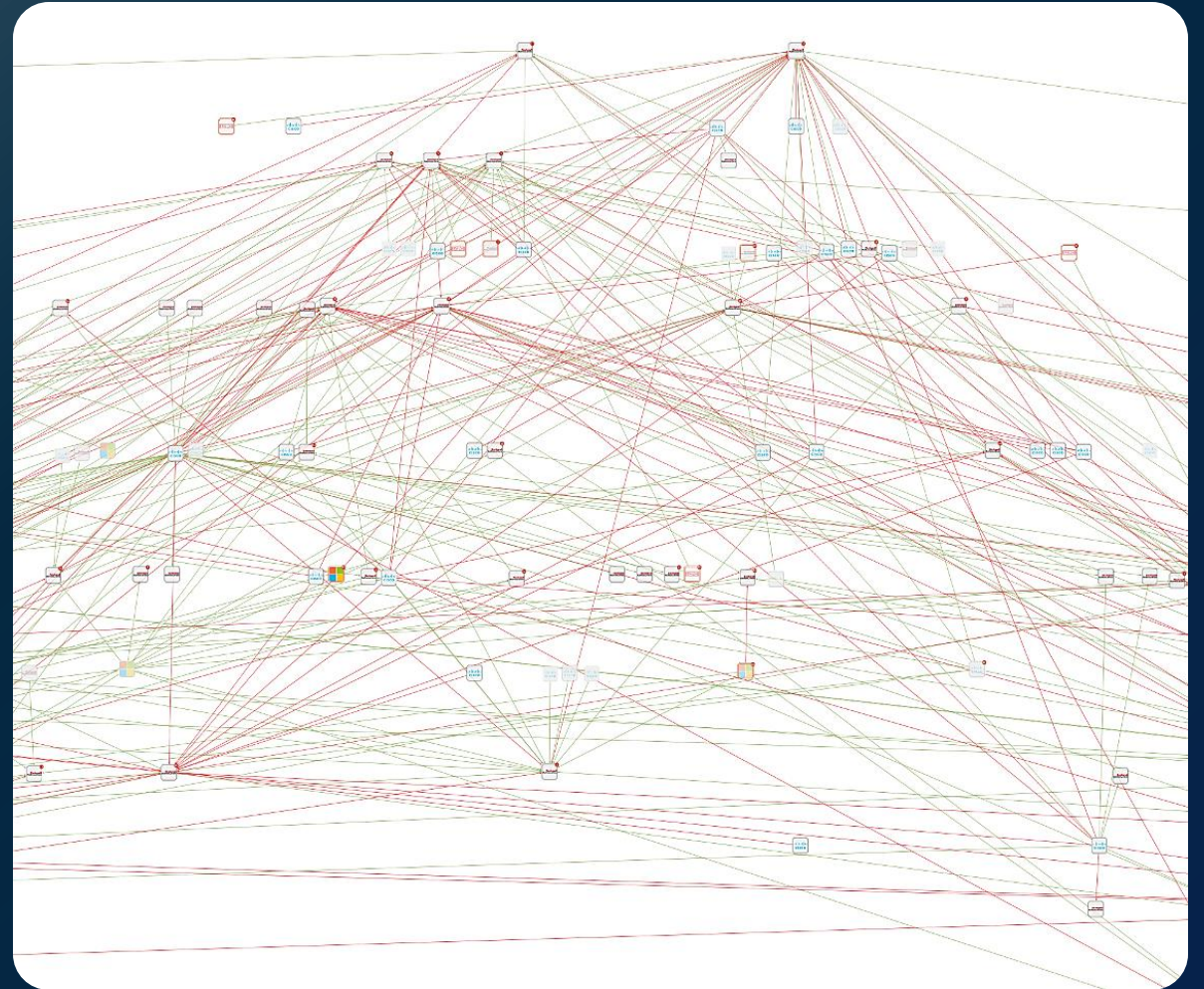
Millions of flows



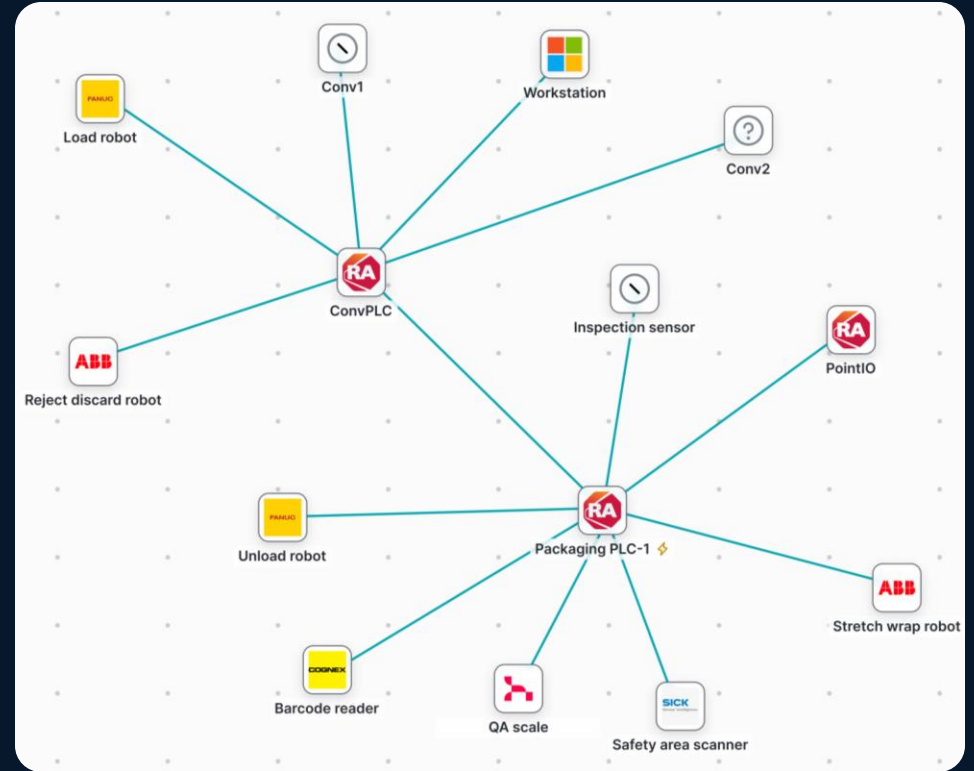
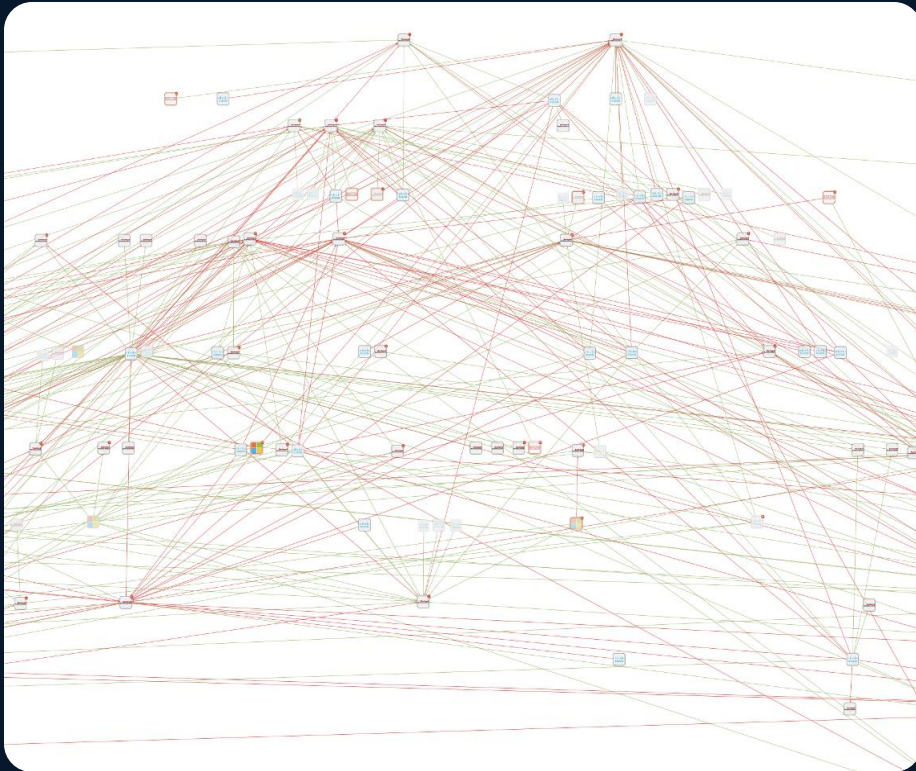
Broadcast, multicast traffic spreading across flat networks



Hard for a human to group assets



# Introducing AI-Based Clustering for Segmentation



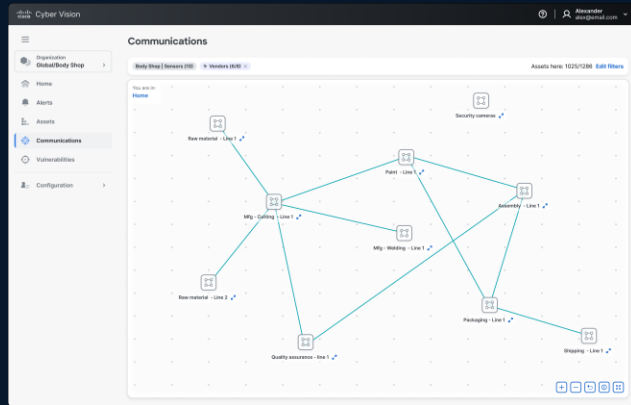
OT asset inventory projects highlight flat, unsegmented networks

Cyber Vision AI-driven auto-grouping automatically creates security zones to drive network segmentation using Firewalls or NAC

# Visibility Driven Segmentation with Identity Services Engine



Grouping assets  
in Cyber Vision



PxGrid

Drives TrustSec  
Auth policy in ISE

	Groups				
Groups	✗	✓	✗	✓	✓
	✓	✓	✗	✓	✗
	✗	✓	✓	✗	✗



RADIUS

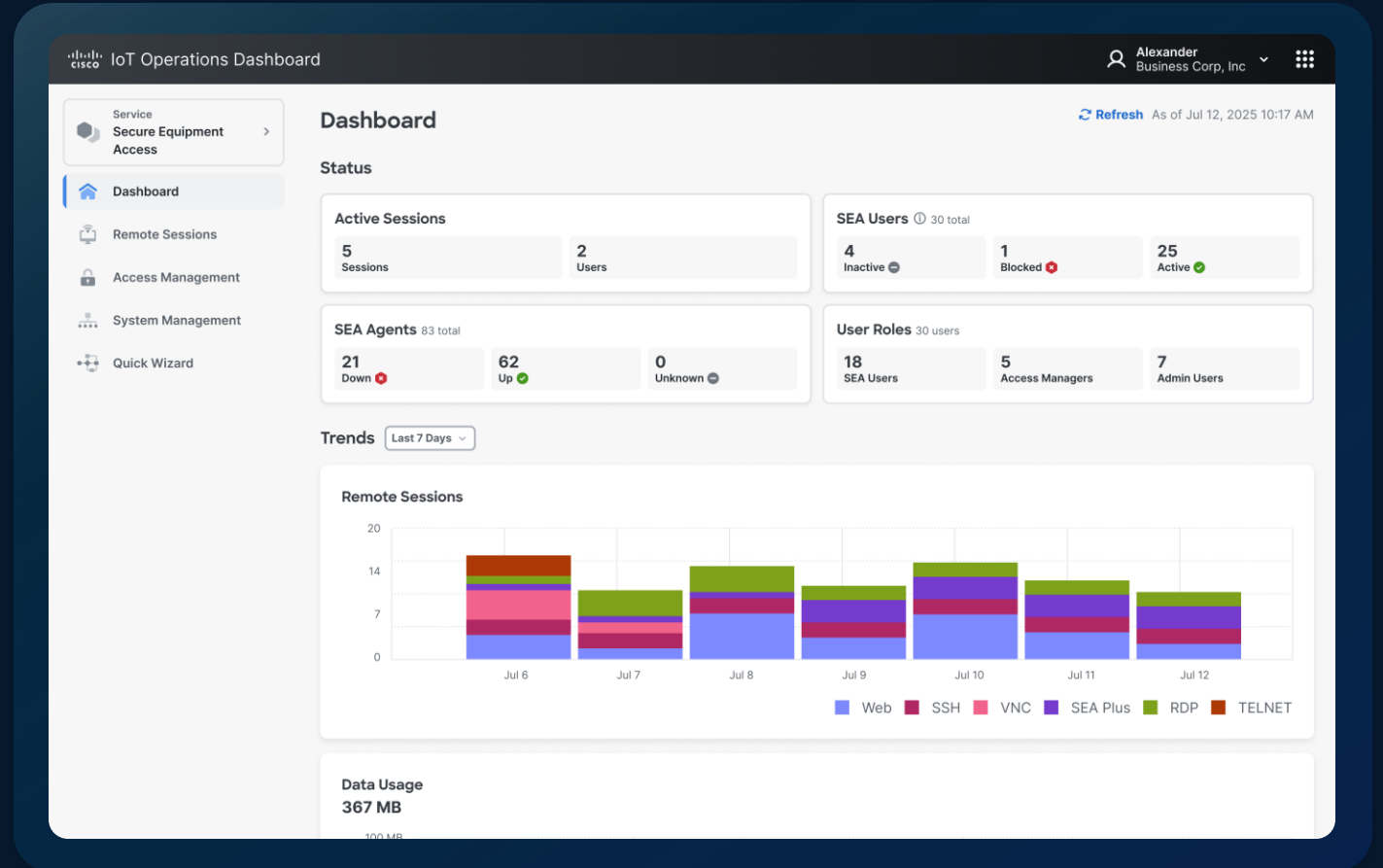
Segmentation enforced by  
switches and routers



Zero downtime with OT controlled **adaptive access policies**

# Secure Equipment Access

Network embedded **Zero Trust Remote Access** to your OT assets



# Remote User Identity Threat Detection

With the rise in remote access activities, remote user identity is becoming a significant attack vector in OT networks

We are delivering new capabilities in SEA to **detect threats related to remote user identity**

Login from unapproved geolocation

Login outside working hours

Auto deactivation of unused accounts

The image displays two screenshots of the Cisco IoT Operations Dashboard. The top screenshot shows an alert titled "Login From Prohibited Location" with a severity of "Critical". The alert summary states: "2 users have logged in from China 3 times: 1 access administrator, and 1 remote user." Below the summary, there is a section for "Active instances" with a search bar and a "Filters" button indicating 2 results. The bottom screenshot shows an alert titled "Login Outside of Working Hours" with a severity of "Medium". The alert summary states: "username@email.com logged in 2 times outside of approved working hours." Below the summary, there is a section for "Logins outside of approved hours" with a timeline for "PDT" showing "Thursday Dec 12, 2024" and "Tuesday Dec 10, 2024". The timeline includes a legend for "Designated working hours" (green), "Login with no sessions" (yellow), and "Login with sessions" (red). Below the timeline, there is a section for "Active instances" with a search bar and a "Settings" button. A table lists the active instances:

<input type="checkbox"/>	Login Time	Discrepancy	Alert Rules	Occurrences	Severity	Last Time Detected
<input type="checkbox"/>	Dec 12, 2024 10:31 PM	3 hr 1 min	1	1	Medium	Dec 12, 2024 10:31 PM
<input type="checkbox"/>	Dec 10, 2024 2:15 AM	4 hr 30 min	1	1	Medium	Dec 10, 2024 2:15 AM

# Introducing New Validated Designs for Manufacturing

- Seamless standardization
- Faster deployments
- Less risk
- Increased predictability
- End-to-end designs

Three vertical cards representing validated designs, each with a title, icons, and a brief description.

- AI MACHINE VISION**: BUILDING THE INDUSTRIAL NETWORK THAT MAKES IT HAPPEN. Icons include a document, a person, a document, a magnifying glass, a gear, a document, a document, and a document.
- INDUSTRIAL CONTROL VIRTUALIZATION**: DUAL FABRIC PLATFORM FOR VIRTUAL PLC, HMI, AND ROBOT CONTROL. Icons include a document, a document, a gear, a document, a key, and a document.
- INDUSTRIAL NETWORK MANAGEMENT**: DESIGN GUIDANCE TO EXTEND CATALYST CENTER TO THE OT SPACE WITH RBAC. Icons include a document, a document, a person, and a document.

[www.cisco.com/go/iotcvd](http://www.cisco.com/go/iotcvd)

Simplifying OT networks with proven technical blueprints and architectures

**CISCO** Connect

**Thank you**



