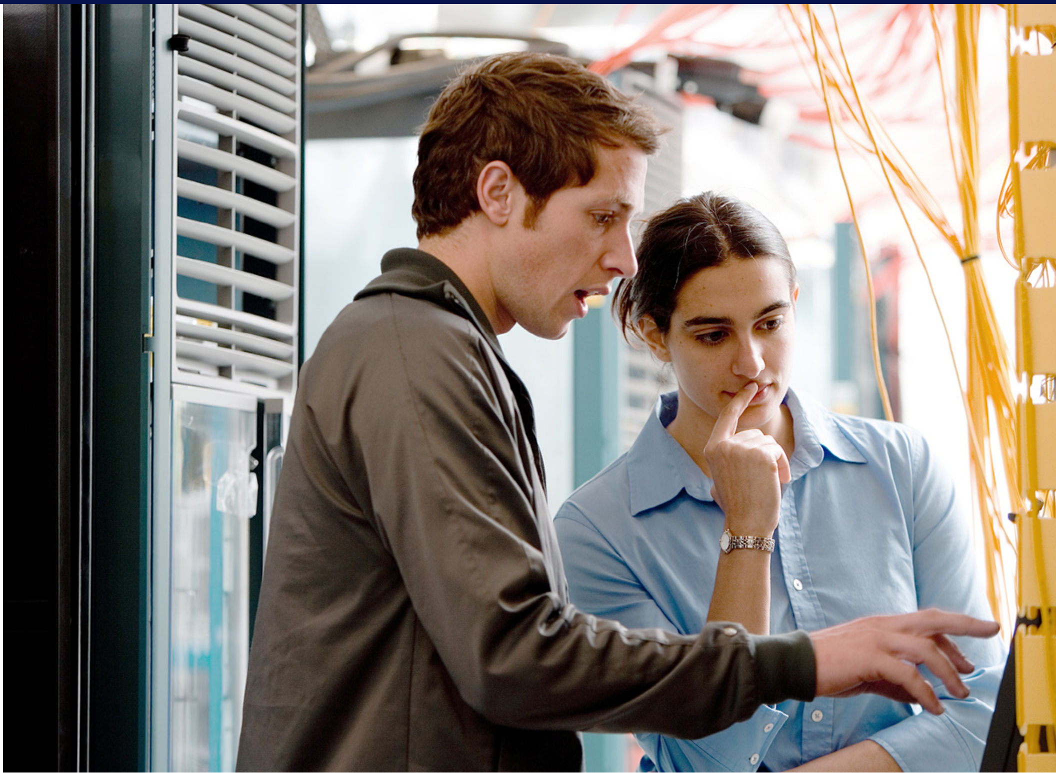
Malisko
ENGINEERING, INC.

The Malisko Guide to Securing and Managing Your Industrial Network

The Three Key Ingredients to Success



cisco Partner
Premier Advisor
Integrator Partner

A Malisko Strategy

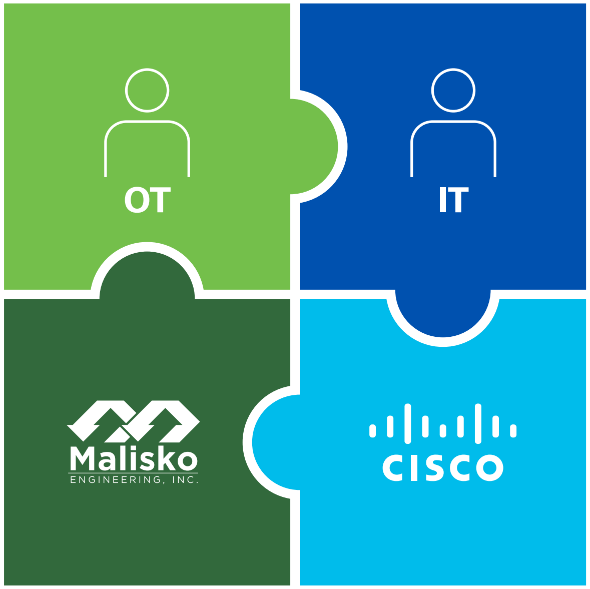
Malisko Engineering understands the challenges that industrial networks pose to your OT and IT teams, and has identified three key ingredients to success.

One: You need full visibility into all the points of connection between devices and infrastructure, so your OT personnel can confidently manage the access layer of the network.

Two: You need the ability to map and manage all the traffic patterns between those devices, so you can identify and address security vulnerabilities and threats.

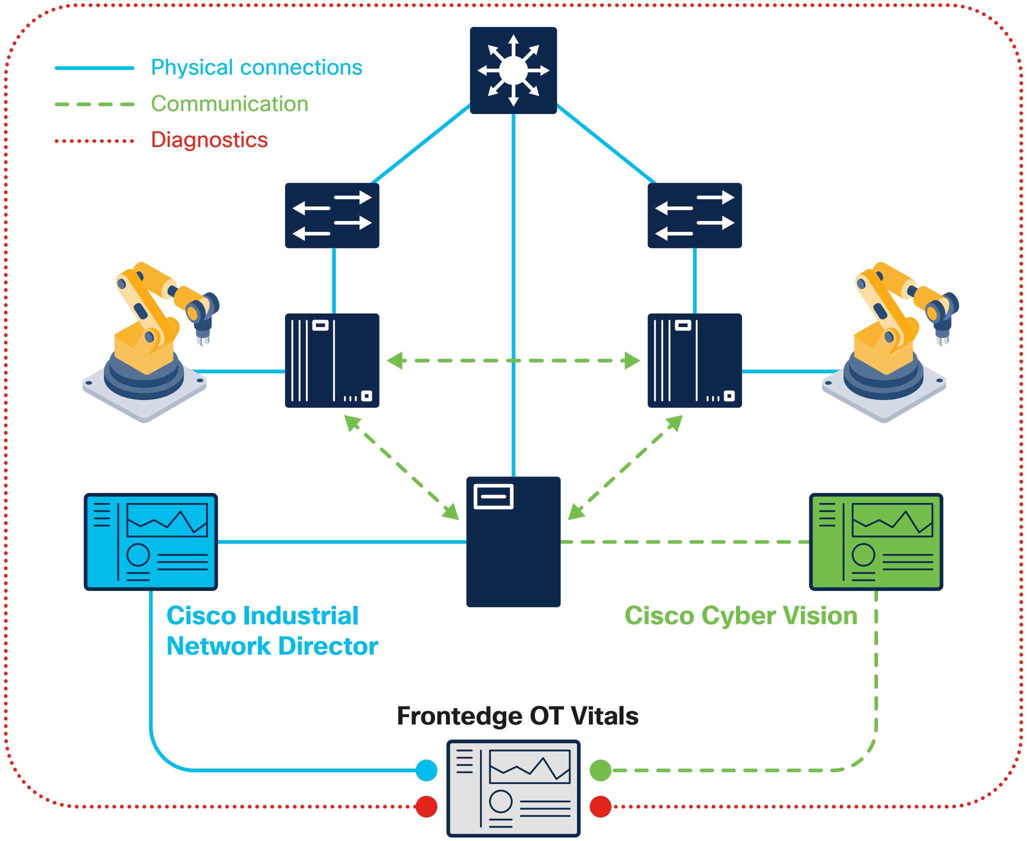
Three: You need a way to pull all that information together, along with other system health information to fill in the gaps—all on a single pane of glass—so you can get on top of the data, anticipate the problems, and achieve the productivity you're aiming for.

In this guide, we'll show you how.



Everything you need to know. When you need it, at your fingertips.

Today, both your OT and your IT teams can have full access to the visibility they need. Shared, unified, and real-time visibility into everything that's happening on the industrial network. System status. Health diagnostics. Security vulnerabilities. All on a single pane of glass—so they can fix problems as they arise.



Here's how it all adds up:

With **Cisco Industrial Network Director (IND)**, your people can monitor industrial infrastructure devices on the network, see how they're connected to endpoints, browse topology maps, and perform routine network management tasks.

With **Cisco Cyber Vision**, you'll solidify your security posture by monitoring and analyzing the communication patterns on your network to immediately detect anomalous traffic and report security vulnerabilities.

With **Frontedge OT Vitals**, you'll complete the picture. You'll aggregate health and diagnostic information from many data sources—including IND and Cyber Vision—to get a single-pane-of-glass view of the health status of your overall industrial IT environment.

Next, let's look at each of the solutions, and the difference they can make for your operations.

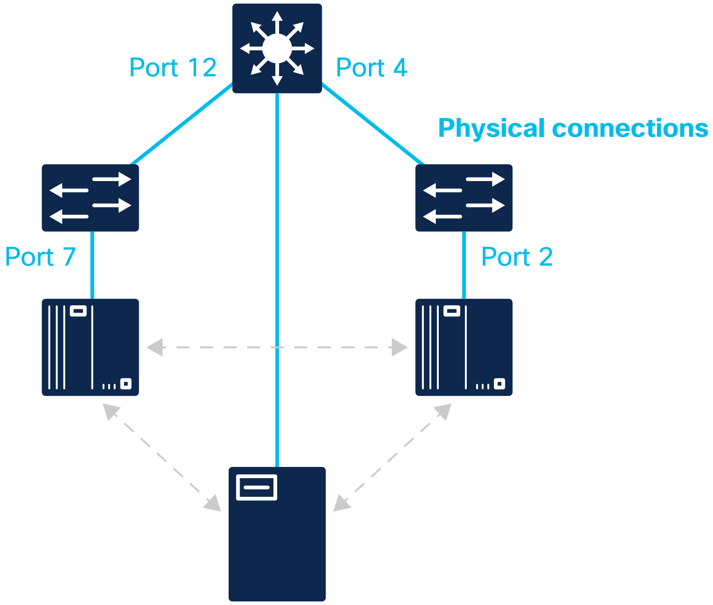
Map and manage the industrial network

Cisco Industrial Network Director (IND) non-intrusively scans the entire industrial network, then generates topology maps that reveal the interconnectivity of the network infrastructure and its endpoints.

IND features an intuitive and easy-to-use GUI interface for management, configuration, and zero-touch commissioning of Cisco Industrial Ethernet and Allen-Bradley Stratix switches, eliminating the need for CLI (command line interface) knowledge for frontline technicians and control system engineers.

This means your OT personnel can manage the access layer of the network closest to the equipment they're responsible for, liberating their IT counterparts from getting involved in routine OT network tasks, such as adds, moves, and changes.

With IND, your OT team will also have the confidence and ability to undertake the replacement of unmanaged switches—which are so prevalent in legacy OT environments—so they can achieve greater network visibility, performance, and reliability.



A Malisko Customer Story

For several years, the OT maintenance manager of a mid-sized pharmaceutical company resisted the deployment of managed switches in his company's industrial network because unmanaged just worked "off the shelf." He was concerned about introducing complexity into an already fragile production environment, and about his staff's lack of familiarity with networking concepts and command line interface (CLI) tools.

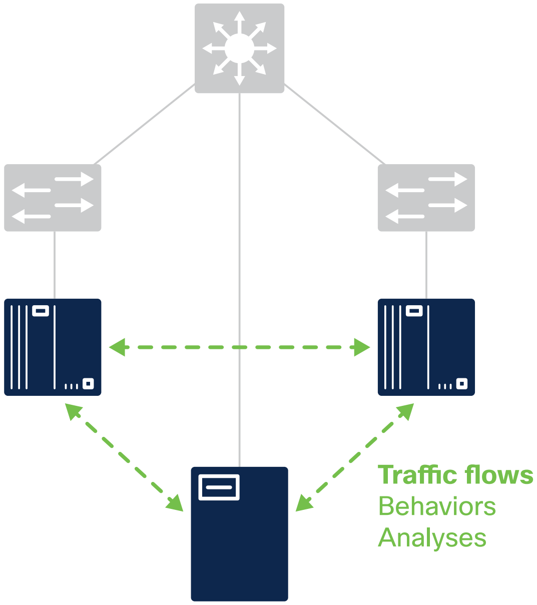
After being introduced to Cisco IND at a trade show, he installed a free trial. Today, he's an IND ambassador, having used it to map out his ICS network, and he has deployed a half dozen Cisco Industrial Ethernet switches to replace unmanaged ones. He attributes his newfound confidence to IND's point-and-click interface, management capabilities, and network discovery features.

Achieve OT security with ICS network visibility, operational insights, and threat detection

Cisco Cyber Vision delivers a powerful array of cybersecurity features to protect your OT network from security threats.

Whereas IND discovers and visualizes the connectivity of your industrial network devices, Cyber Vision maps and visualizes the traffic patterns between those devices (including the processing of native OT protocols). System baselines define normal network behavior and configuration, and when a deviation occurs, alerts are generated immediately, allowing quick mitigation of potential threats.

Cyber Vision allows OT personnel to group assets, providing the foundation of OT network segmentation. It also shares industrial asset context with other Cisco security solutions, giving your IT team unparalleled visibility into the OT environment.



Additionally, Cyber Vision provides insights into your OT security posture, risk scoring, device vulnerabilities, signature-based intrusion detection systems (IDS), and operational activities like configuration changes and control system events.

Cyber Vision deep packet inspection sensors are built into industrial-compute-capable Cisco switches, routers, and other network elements, lowering total cost of ownership (TCO).

Cisco Cyber Vision integrates with

- Cisco Identity Services Engine (ISE)
- Cisco Firepower Next-Generation Firewalls
- Cisco Stealthwatch
- Cisco DNA Center

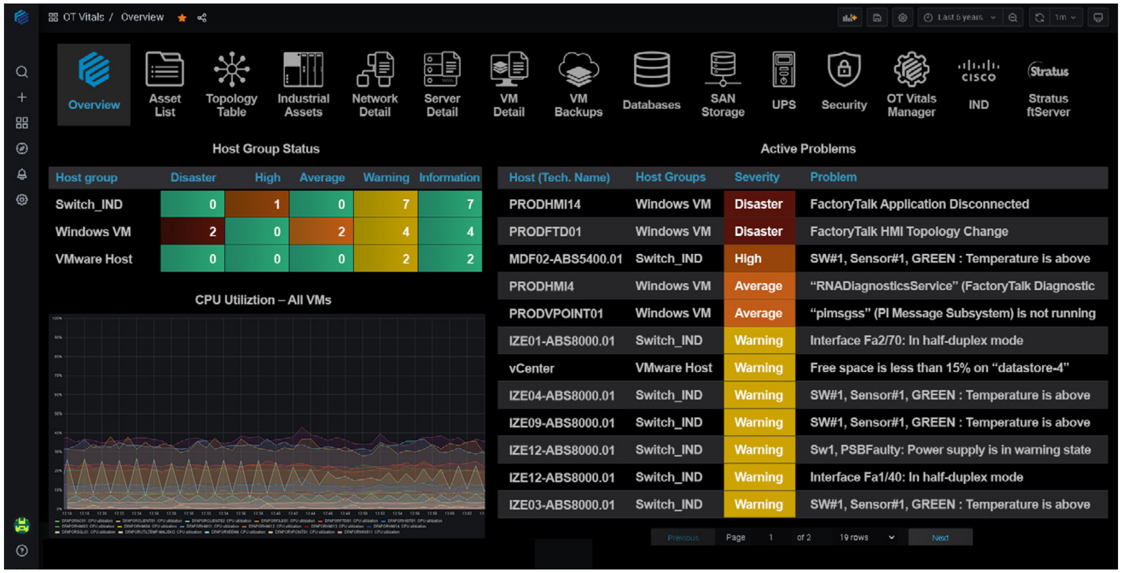
A Malisko Customer Story

Using Cisco Cyber Vision, a manufacturer discovered several non-domain-joined Windows machines communicating with PLCs throughout its plant. The suspect machines turned out to be dual-homed laptops–connected via ethernet to its ICS and via Wi-Fi to its Internet-enabled guest network. While intended for on-demand remote access for OEMs and Systems Integrators, this vulnerable connection could allow bad actors to directly access the production network from anywhere in the world.

This discovery served as a catalyst for the company to implement deeper segmentation and access policies, including an Industrial Demilitarized Zone (IDMZ). They used Cyber Vision to group OT devices by functional area, and pushed contextual information to Cisco Identity Services Engine (ISE) to develop and enforce security policy for the industrial zone.

Fill in the gaps with one comprehensive view

Frontedge OT Vitals delivers the vital signs of critical industrial infrastructure, endpoints, and applications with intuitive and visual dashboards, all on a single pane of glass.



Host Group Status

Host group	Disaster	High	Average	Warning	Information
Switch_IND	0	1	0	7	7
Windows VM	2	0	2	4	4
VMware Host	0	0	0	2	2

CPU Utiliztion – All VMs

Active Problems

Host (Tech. Name)	Host Groups	Severity	Problem
PRODHMI14	Windows VM	Disaster	FactoryTalk Application Disconnected
PRODFTD01	Windows VM	Disaster	FactoryTalk HMI Topology Change
MDF02-ABS5400.01	Switch_IND	High	SW#1, Sensor#1, GREEN : Temperature is above
PRODHMI4	Windows VM	Average	"RNADiagnosticsService" (FactoryTalk Diagnostic
PRODVPOINT01	Windows VM	Average	"pimsgss" (PI Message Subsystem) is not running
IZE01-ABS8000.01	Switch_IND	Warning	Interface Fa2/70: In half-duplex mode
vCenter	VMware Host	Warning	Free space is less than 15% on "datastore-4"
IZE04-ABS8000.01	Switch_IND	Warning	SW#1, Sensor#1, GREEN : Temperature is above
IZE09-ABS8000.01	Switch_IND	Warning	SW#1, Sensor#1, GREEN : Temperature is above
IZE12-ABS8000.01	Switch_IND	Warning	Sw1, PSBFaulty: Power supply is in warning state
IZE12-ABS8000.01	Switch_IND	Warning	Interface Fa1/40: In half-duplex mode
IZE03-ABS8000.01	Switch_IND	Warning	SW#1, Sensor#1, GREEN : Temperature is above

IND and Cyber Vision serve specific purposes on the network itself, but there is so much more in the industrial IT and ICS environment to keep tabs on. OT Vitals fills in the gaps.

Drawing from IND's device inventory as a starting point, OT Vitals provides a wide array of infrastructure and endpoint health metrics, including the display of vulnerabilities and risk scoring from Cyber Vision.

If thresholds are crossed or critical diagnostic events are detected, alerts are pushed to Webex Teams, enabling your OT and IT personnel to collaborate quickly and efficiently. They can even push comments and acknowledgements back to OT Vitals.

OT Vitals also enables integration of custom data sources for unique customer applications and devices.

OT Vitals fills in the gaps

- Sortable device list per switch
- Server host, virtual machine, and network component CPU, memory, and storage utilization
- SNMP alerts from infrastructure devices
- Device liveness (ICMP ping)
- ICS application logs
- Microsoft Windows services state
- Virtual machine backup status
- Custom Data Sources

A Malisko Customer Story

At a contract manufacturer's mixing and blending plant, all the HMI screens monitoring and controlling its production equipment intermittently froze, requiring system reboots and causing significant downtime.

Using Frontedge OT Vitals, the company identified trends showing intermittent spikes in CPU on all the plant's virtual machines. They were able to correlate the CPU spikes with application-level HMI errors indicating a communication loss. By reviewing server host diagnostics in OT Vitals, they were able to identify an intermittent hardware failure and replaced the faulty part.

We'll be there every step of the way

Now that we've introduced you to each of the three ingredients for securing and managing your industrial network, let's talk about how the right team of experts can help you bring them all together.

The Malisko Step-by-Step Roadmap

1 Introductory call to learn about your infrastructure, pain points, and where you sit in the Factory Floor Convergence Maturity Model

2 Preliminary asset visibility study

- Implement Cisco IND: Discover network topology—what is *connected* to what—and provide a means to manage the industrial network.
- Implement Cisco Cyber Vision: Discover assets and communication mapping—what is *talking* to what—and detect security vulnerabilities in the environment.
- Implement Frontedge OT Vitals: View comprehensive infrastructure and ICS health and alerting on a single pane of glass.

3 Industrial Network Advisory Report

- Identify connected devices and highlight security issues and prioritize risks.

4 Remediation planning

- Identify the steps you'll need to take when you're ready to modernize your network.

5 Design and commission converged IT/OT infrastructure solutions.

6 With a solid foundation for your IoT and ICS devices, we can then help gain the full value of your investment through digital initiatives that drive business outcomes.

Malisko ENGINEERING, INC.

Who is Malisko Engineering?

- An award-winning manufacturing automation and industrial IT systems integrator
- A Cisco Digital Solutions Integrator (DSI) partner
- We implement industrial IT, IoT, and ICS technologies and practical solutions that bring business value
- Our foundation in Industrial Control Systems brings practical OT experience and perspectives to Digital Transformation and Industry 4.0 initiatives

Our Goal

Malisko aims to be part of your team as a trusted industrial IT and automation advisor and advocate to accelerate your digital initiatives.

Next Steps

At Cisco and Malisko Engineering, we’re ready to help you start your journey towards securing and managing your industrial network. To get started, contact your Cisco sales representative.

https://www.malisko.com >

https://frontedge.malisko.com/otvitals >

https://www.cisco.com/c/en/us/solutions/internet-of-things/iot-network-connectivity.html >