Manufacturing security: Bridging the gap between IT and OT

cisco

For manufacturers, every new connection point is an opportunity.

And a risk.

The state of IT/OT security in manufacturing

On the plant floor, as connectivity increases, so does complexity—and so do security concerns.

Every new asset you put on the network is another security consideration, and another risk that requires monitoring.

In many plants, the increasing number of assets is making it difficult to see security context and truly understand the network at any given moment. Organizations lack the ability to identify what even just normal network activity looks like. When abnormal conditions arise, that means they have no baseline for comparison—making it difficult to identify threats.

Why can't they see the network? Since industrial control system (ICS) environments consist of many types of equipment operating with many different Industrial Internet of Things (IIoT) protocols, getting a centralized view is difficult, if not impossible. The greater scope of asset types and ages presents challenges that traditional IT environments don't encounter.

At the same time, the manufacturing industry is becoming an increasingly alluring target for cybercriminals. Again, because of all those assets. Each one is a potential entry point. With so many devices at their disposal, cybercriminals are using ransomware to extract money from manufacturing organizations.

Plus, many manufacturers are operating with aging assets and equipment. Having originated in a time far removed from today's threats, this equipment wasn't designed to guard against complex, high-tech cyberattacks. And that leaves the IT/OT staff to pick up the slack.

To prevent issues, OT needs to take ownership of cybersecurity.

But IT holds the keys and expertise.

Today's cybersecurity challenges for OT

Manufacturing operations are changing and becoming more and more connected. It's unlocking new levels of productivity and profit for the industry.

Since OT professionals are expected to be the experts about what makes plants run, they must change too. And, indeed, OT teams are becoming more skilled at networking and plant connectivity. But many OT professionals do not have sufficient training or education in cybersecurity necessary to manage the nuances and pitfalls of combatting advanced ransomware or other kinds of evolving threats.

Thus, plants find themselves in an awkward position: one where OT teams depend on IT staff that may not be local to the facility to ensure security and manage connected operations. Even though many IT teams often aren't familiar with the complexities of plant operations and manufacturing technologies.

Because of disparate systems–and compounded by the physical or virtual gap–OT teams often have limited visibility into IT security policies. As OT teams make control system changes, they can accidentally violate IT security policies, potentially leading to an attack or to unplanned downtime.

What does OT need?

When it comes to ensuring continuous operations, OT teams need to be more self-reliant. And that includes security. Without visibility into the network, they can't understand activity or identify anomalies. And without the ability to manage and apply security policies, they're too dependent on IT–slowing down responses, creating confusion, and impacting productivity.

Of course, IT teams need to stay in control too. They're the cybersecurity center of expertise for most organizations–but in manufacturing, they can't do their job effectively without OT's help.

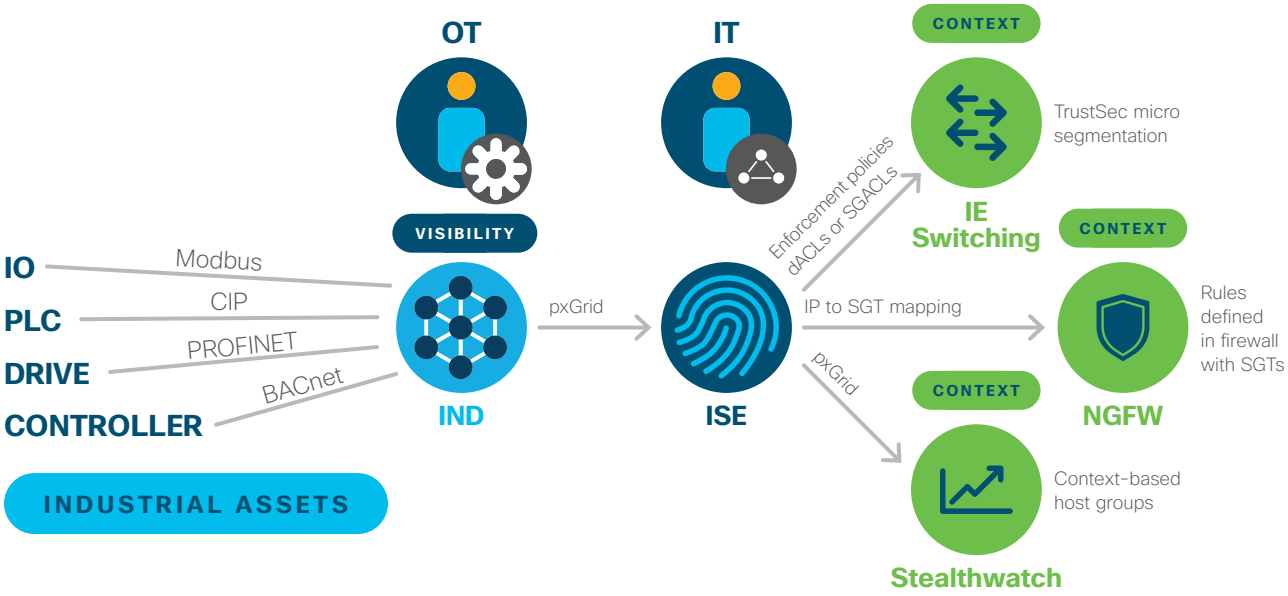
With Cisco manufacturing security solutions, IT stays in control.

But OT teams get what they need, too.

By combining Cisco Industrial Network Director (IND), Cisco Identity Services Engine (ISE), and Cisco Stealthwatch, Cisco delivers comprehensive security solutions that are built for the needs of both IT and OT teams.

These solutions do two critical things that help bridge the gap between IT and OT:

1. Deliver visibility into assets on the network and give the OT team a centralized view of network activity, so they have a better idea of both normal and abnormal activity.
2. Enable IT to pre-define security policies and dynamically assign them based on input and intent from the OT team.



Cisco Industrial Network Director (IND)

- Provides OT with a user-friendly network monitoring solution
- Allows OT staff to call down security policies by signaling the intent of what they're trying to do

Cisco Identity Services Engine (ISE)

- Enables full IT control of access to critical assets
- Empowers IT to create security policies that are dynamically applied to plant floor assets based on signaled OT needs

Cisco Stealthwatch

- Monitors and analyzes network traffic to assist in policy creation
- Helps speed threat detection and remediation

Connected via pxGrid connector

Cisco Industrial Network Director is a network management solution that's built for OT departments.

Cisco IND provides operations teams with an easily integrated system for user-friendly network monitoring. It enables OT teams to see a full view of their network topology so they better understand what's normal and what is cause for concern.

Users of Cisco IND gain full visibility and control of the industrial Ethernet infrastructure in the context of connected devices and network infrastructure. Cisco IND can automatically discover devices that use common industrial protocols such as CIP and PROFINET to enable a dynamic, integrated view of connected devices and network infrastructure.

Connection with Cisco ISE via Cisco Platform Exchange Grid

As OT workers go about their day and manage asset connectivity, Cisco IND interfaces with Cisco ISE. OT staff can input their intent—such as connecting a device to a remote vendor—and Cisco ISE dynamically applies the correct security policies for the scenario, based on previous IT policy definition. It's all enabled by Cisco Platform Exchange Grid (pxGrid), our open and scalable platform that enables multiple security solutions to seamlessly share data and work together.

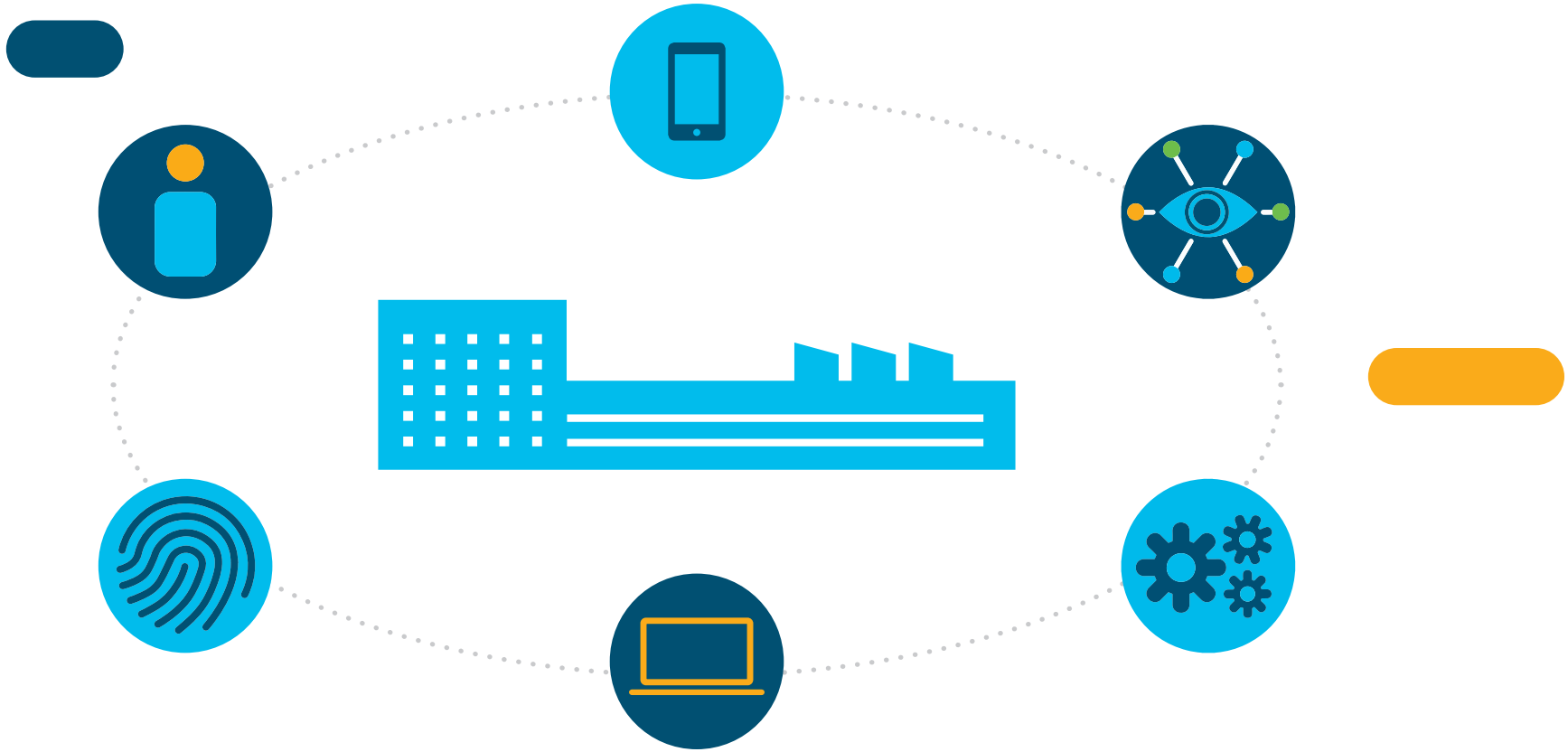
BENEFITS

- **Enable operations to dynamically assign IT-defined security policies as needed:** Simply group and tag assets as needed and signal intent over pxGrid to pull down predefined policies from Cisco ISE
- **See industrial network activity:** Helps operations teams gain full visibility of network and industrial assets with real-time monitoring
- **Simplify integration and discovery:** Unifies industrial endpoints such as programmable logic controllers, IO, HMI, drives, and more into a single view; rich APIs enable connection to other systems as well
- **Apply enterprise security techniques to the plant floor:** Enables Cisco security capabilities such as TrustSec micro segmentation, context-based host groups, and Security Group Tag-based firewall rules to be used on the industrial network

Cisco ISE is a powerful tool for controlling access to connected plant floor assets.

Cisco ISE gives your IT department the ability to set and enforce access policies for your entire network topology. As operation teams work, Cisco ISE works in conjunction with Cisco IND to allow them to assign pre-set security policies for industrial assets, based on definitions previously made by the IT team.

It does far more than that, too. Cisco ISE allows IT to control access for remote experts or vendors, so they can get the information they need without risking security. Segmentation, containment, and remediation functionality ensures a rapid, accurate, and effective response to network threats.



Cisco Stealthwatch is a scalable visibility and analytics solution.

To set effective security policies, the IT department needs to be able to understand what both an average day on their network looks like and what a very unaverage day looks like.

Cisco Stealthwatch provides the deep network visibility and analytics that IT teams need to build the best possible security policy strategy and to keep up to date on network activity.

Plus, Cisco Stealthwatch provides up-to-the-second threat intel, faster threat detection, and enhanced threat forensics.

When anomalous traffic is detected, IT teams can quickly get to the bottom of the issue by leveraging audit histories and threat forensics. Integrated segmentation features allow for safer network designs and can help prevent infections from spreading.

Use cases

Empower OT while keeping IT in control of security

WHAT YOU CAN DO: Allow IT to define security policies that dynamically apply themselves based on OT's intentions and input.

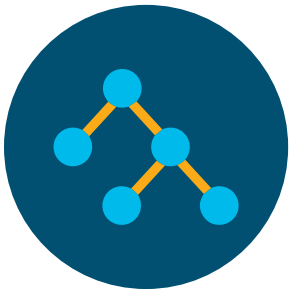
WHY IT'S IMPORTANT: OT needs to be able to take ownership of security to ensure continuous operations, but requires IT expertise to do so.

Provide a full view of industrial network topology for OT

WHAT YOU CAN DO: Create a centralized network view so that OT can stay abreast of conditions and deep dive into individual assets.

WHY IT'S IMPORTANT: OT needs better context around security to successfully enforce it.

Segment networks



WHAT YOU CAN DO: Create discrete network zones within your overall topology that restrict access and prevent infection.

WHY IT'S IMPORTANT: Cybercriminals are looking for any entrance point they can find. For example, one case of the WannaCry ransomware attack in May 2017 started from a single workstation that was connected to the network at large. Segmentation helps to prevent infections from spreading too far.

Enable remote access

WHAT YOU CAN DO: Enable secure, remote access to securely bring in remote expertise such as contractors and vendors to help solve issues, apply patches, and more—without needing to involve IT in every incident.

WHY IT'S IMPORTANT: Allowing OT to enable access to select assets for third-party organizations helps increase agility and ensure continuous operations.

It's time to give OT teams the tools they need.

Cisco manufacturing security solutions enable manufacturing organizations to empower OT with the ability to apply security policies and understand security context–while IT remains in ultimate control.

Combining Cisco ISE, Cisco IND, and Cisco Stealthwatch, our solutions enable a real-time view of your entire network topology, with alerting, segmentation, and more. So both IT and OT stay informed of what they need to know to ensure continuous operations.

It's all built on technologies that are familiar to those in the enterprise IT world–increasing usability and preventing the need for a multivendor security solution.

Learn more today at cisco.com/go/ind