INTERN NOTES (delete before publishing)
Source: OT/ICS Network Monitoring Solution Brief, iDefender LLC, 2021. The brief predates FERC Order 907, which approved NERC CIP-015-1 in June 2025 and made internal network security monitoring mandatory for the North American electric sector. Section 6 covers that.

Product should confirm the protocol list and the APM description before this publishes, since both may have changed since 2021.

Source links are delivered separately and still need to be placed. Case study callouts and pillar pages are filled. Boxes marked GLOBAL MODULE are being built in-house.

OT CYBERSECURITY | NETWORK MONITORING | CRITICAL INFRASTRUCTURE

OT Network Monitoring: What It Sees, What It Misses, and Why Regulators Now Require It

A Practical Guide to Passive Monitoring, Asset Discovery, and Anomaly Detection on Industrial Networks

Industrial Defender Staff | [Publish Date] | [Reading time]

Executive Summary

OT teams work under a handful of frameworks that shape how they build and run critical infrastructure.

Engineers and security leaders use Industrial Defender's asset management and risk mitigation solutions to meet those requirements without adding to the daily workload.

Nearly all of those frameworks ask for network monitoring in some form. For years, it was also the first item cut when budgets got tight.

That changed in June 2025. FERC approved NERC CIP-015-1, which requires utilities to monitor traffic moving inside their electronic security perimeters, not only at the edge.

High and medium impact systems with external routable connectivity have until October 1, 2028, to comply, and the remaining systems have until 2030

The technical problem has been the same for years. You cannot run an IT scanner against a control network without risking the process it controls, so the safe way to learn what is on an OT network is to listen to it.

Passive monitoring does that. A sensor watches a copy of the traffic through a SPAN port, a mirror port, or a network tap, and builds a picture of the environment from what the devices are already saying to each other.

This guide covers how passive monitoring works, what a sensor can identify on its own, and where it needs help.

It also walks through the anomalies it catches and how that data maps to CIP-015.

It also covers the part vendors tend to skip. Network monitoring gives you a good view of traffic and a partial view of assets.

It does not tell you which patches are missing, which user accounts exist, or whether a firewall rule changed last Tuesday.

Those answers come from somewhere else, and most compliance frameworks ask for that information as well.

Table of Contents

[@designer: these should all link to the sections below]

1. Why OT Networks Need a Different Approach
2. How Passive Monitoring Works
3. Automatic Asset Discovery
4. Network Anomaly Detection
5. Traffic Visibility and NetFlow
6. CIP-015 and the New Compliance Driver
7. What Network Monitoring Cannot Tell You
8. Where the Sensors Go
9. Getting Started
10. Who We Serve
11. Frequently Asked Questions
12. Resources

[PLACEHOLDER: VIDEO FROM USER GROUP]
Embed the user group session on network monitoring deployment. Add a one-line caption: who is speaking, what they cover, runtime.

Link: _____

Why OT Networks Need a Different Approach

The volume and variety of devices on industrial control system networks keep growing, and most OT teams have no reliable way to keep up with what is actually connected.

Underneath that sit two separate problems: you don't have a current list of what is connected, and you wouldn't notice suspicious traffic if it appeared.

An IT team solves both with active scanning. They run a scanner, which probes every address and reports what it finds.

On a control network, that approach carries real risk. Older programmable logic controllers were built to talk to a small number of known systems on a predictable schedule.

An unexpected probe can knock one into a fault state, and a faulted PLC takes more than a help desk ticket to recover.

A faulted controller can stop a line or trip a safety system, and someone usually has to walk out and reset it by hand.

So OT teams either scan carefully during a maintenance window once or twice a year, or they don't scan at all. Both leave them working from an inventory that is out of date the moment it is finished.

Passive monitoring is the workaround the industry settled on, and it works by listening to the devices.

How Passive Monitoring Works

Industrial Defender monitors OT network traffic through a SPAN port, a mirror port, or a network tap placed inside the control network security perimeter.

All three do the same basic job, which is to hand the sensor a copy of the traffic without putting the sensor in the path of it.

That distinction has practical consequences. A device sitting in the traffic path is a device that can fail and take the process with it, which is not a risk a sensor reading a copy carries, since nothing on the control network waits for it to respond.

From that copied traffic, the sensor pulls two kinds of information. It identifies which devices are talking, then watches the content of those conversations for anything unusual.

The second half covers internally generated attacks as well as anything that slipped past your perimeter defenses, which is the case perimeter firewalls were never designed to handle.

Hybrid Monitoring: Agent, IDC & Passive Data Collection

Purely passive monitoring has one limitation worth understanding before you deploy it.

A sensor can only identify a device that is actually communicating, and some OT equipment goes quiet for long stretches by design.

Our Hybrid Monitoring (APM) engine handles that gap.

It sends small broadcast messages using native commands the devices already understand, which is enough to identify thousands of different OT device types without the load of a conventional scan.

The information APM collects feeds the same asset record as everything else, so a quiet device ends up with the same vulnerability coverage as a chatty one.

Packet Replay

The platform can also replay a captured packet file to simulate network behavior without putting that traffic back on the live network.

Teams use this for tuning detection rules and for training, and it is a safer way to test a detection than waiting for the real thing.

[GLOBAL MODULE: NERC CIP-015 GRAPHIC]

Awaiting global module. No copy needed here.

Automatic Asset Discovery

Every framework worth following starts with the same requirement, which is knowing what you have.

For devices actively communicating on the ICS network, Industrial Defender captures their communications from the traffic using deep packet inspection.

It reads the contents of the packets, not just the addresses on the outside, and uses what it finds to identify the device and onboard it into a baseline inventory.

New devices generate an alert as soon as they appear. Your team then decides whether it is an authorized addition or a rogue device that needs to come off the network.

The data the sensor collects on each device includes:

- Product name
- Model number
- Vendor
- Device type
- Firmware version
- Serial number

The firmware version is the one that earns its keep. It is the field that connects an asset to a known vulnerability, and it is also the field most manual inventories get wrong, because it changes during maintenance and the inventory rarely gets updated to match.

[CASE STUDY CALLOUTS]

Chemical Manufacturing (CFATS Compliance)
A Fortune 500 chemical producer needed a complete picture of hundreds of OT systems for CFATS audits, and got one while holding CPU impact under 1%. Read the case study **HERE>**

European Electric Utility
Serving 8 million customers across a distributed grid, this operator swapped manual asset tracking for automated discovery, patch monitoring, and file integrity checks. See what changed **HERE>**

Midwest Utility (NERC CIP)

A public utility with more than 500 assets and a thin IT bench cut its NERC CIP documentation prep by 80%. Read how **HERE>**

Network Anomaly Detection

Discovery tells you what is on the network, and detection tells you what those devices are doing with it.

Industrial Defender identifies malicious activity and invalid configurations using publicly available signatures and customer signatures, both updated continuously.

Teams can also insert their own signatures as new threats appear, which matters in OT because the threats that reach industrial environments often show up in a handful of sectors before anyone writes a public rule for them.

The sensors watch the conversation between SCADA systems and controllers.

That is where the interesting activity happens, and it is traffic that perimeter tooling never sees because it never crosses the perimeter.

Protocols Supported

Passive monitoring covers widely adopted industrial protocols:

- Siemens S7
- Profinet
- MODBUS
- BACnet
- DNP3

Others are supported as well. If you are running something unusual, ask, because protocol coverage is the first thing to check against your own environment.

What Gets Detected

Examples of activity the platform flags:

- Changes to controller firmware
- Logic downloads
- Protocol violations
- I/O force
- Invalid messages
- Device timeout or busy
- Information loss
- Mode change, including starts and stops
- Use of insecure protocols such as TELNET

Several of these are worth a second look, because they describe legitimate engineering work as well as an attack.

A logic download is how an engineer updates a controller. An I/O force is how a technician tests a circuit. Firmware changes happen during scheduled maintenance.

These actions aren't forbidden. The point is that you find out they happened and can check them against the change calendar

Traffic Visibility and NetFlow

The NetFlow application shows the shape of communication across your environment using data from Industrial Defender Collectors:

- Top services
- Source IPs
- Destinations
- Conversations

- Inbound external communicators
- Outbound external communicators

The last two deserve attention during any review. An OT device talking to something outside the environment should map to a documented integration. When it doesn't, that is worth running down

From the summary view, you can drill into individual conversations, which is where most investigations actually begin.

[GLOBAL MODULE: SOLUTION BRIEF CALLOUTS]

Awaiting global module. No copy needed here.

CIP-015 and the New Compliance Driver

For North American utilities, internal network monitoring stopped being optional.

FERC issued Order 907 on June 26, 2025, approving NERC Reliability Standard CIP-015-1. The standard took effect on September 2, 2025, and requires internal network security monitoring for traffic inside electronic security perimeters.

CIP-015-1 has three requirements:

- R1 Collect, detect, and analyze network activity, using a risk-based rationale to decide where the data feeds go and what counts as anomalous
- R2 Retain the monitoring data tied to anomalous activity long enough to support investigation and response
- R3 Protect collected and retained data from unauthorized modification or deletion

Compliance arrives in two waves. High-impact BES Cyber Systems and medium-impact systems with external routable connectivity have until October 1, 2028.

The remainder has until October 1, 2030.

FERC also directed NERC to extend the requirements to electronic access control and monitoring systems and physical access control systems that sit outside the perimeter.

That work became CIP-015-2, which passed the final ballot in March 2026.

If you own high or medium-impact systems, the useful way to read the 2028 date is as a procurement and architecture deadline rather than an installation one.

Sensor placement, data retention design, and the question of who reviews the alerts all take

longer to settle than the deployment itself.

What Network Monitoring Cannot Tell You

Network visibility alone is not enough, and this is the point where a lot of OT security programs stall.

Many asset inventory tools in this space stop at identifying devices on the network. They will tell you a device exists, what type it is, and who made it. Then they stop.

What they do not give you is the configuration detail that determines whether that device is actually secure:

- Which software versions are installed and which patches are missing
- Which user accounts exist on the device and when they were last used
- What the firewall rules are and whether they changed
- Which ports and services are running
- The position of a PLC key switch

None of that travels across the wire in a form a passive sensor can read.

A controller does not announce its patch level on the network, and a workstation does not broadcast its local account list.

Industrial Defender combines network monitoring with endpoint collection for this reason. The network sensor finds the device and watches its traffic.

The endpoint side fills in what the traffic cannot say.

When you evaluate any monitoring product, the question to press on is what it knows about a device beyond its presence on the network.

[PLACEHOLDER: TWO VIDEOS]
Suggested: (1) demo of network monitoring and asset discovery in the platform, (2) short explainer on passive versus active collection in OT. One-line caption each.

Video 1: _____ | Link: _____

Video 2: _____ | Link: _____

Where the Sensors Go

Industrial Defender Collectors sit at each network layer of a typical control architecture, and the

Industrial Defender Central Manager aggregates what they gather.

A common layout looks like this:

- **Level 1, Control Network.** PLCs and RTUs, with a collector on the local switch
- **Level 2, Supervisory Network.** HMIs, PLCs, RTUs, and the DCS or SCADA server, with its own collector
- **Level 3, Operations and Control.** Workstations, domain controllers, and historians, again with a collector
- **Level 4, Corporate Network.** The Central Manager, alongside the SIEM, Active Directory or LDAP, IT asset management, and threat intelligence feeds

Putting a collector at each level is what produces east-west visibility, meaning traffic between devices at the same layer.

That is exactly the traffic CIP-015 is written about, and it is invisible to anything watching only the boundary between OT and IT.

The Central Manager sitting at Level 4 is what lets the data reach your existing security stack without anyone on the corporate side needing access into the control network.

[GLOBAL MODULE: DEPLOYMENT PAGE]

Awaiting global module. No copy needed here.

Getting Started

Most teams begin in one of two places, depending on what is driving the project.

If a compliance deadline is driving it, start by mapping your electronic security perimeters and working out which systems fall in scope for CIP-015.

Sensor placement follows from that, and the retention and data protection requirements shape the architecture more than people expect.

If visibility is driving it, start with your busiest control network segment.

Run passive collection for a few weeks and compare what it finds against your existing asset list.

The gap between the two is usually the strongest argument you will have for funding the rest of the deployment.

Either way, decide early who reads the alerts. A monitoring platform that nobody watches

produces audit evidence and not much else, and that question tends to get answered late.

To see what passive collection would find in your environment, schedule a demo with one of our OT security architects.

[GLOBAL MODULE: NERC CIP-015 GRAPHIC]

Awaiting global module. No copy needed here.

(Insert 2 pillar pages)

Who We Serve

Power (Electric Utilities)

CIP-015 lands on utilities first, and substations spread across several states make sensor placement a real design problem. See how electric utilities approach OT visibility and compliance reporting **HERE>**

Oil & Gas

Pipelines, terminals, and offshore platforms run OT assets across long distances with limited bandwidth between them. Learn how oil and gas operators build network visibility under those constraints **HERE>**

Frequently Asked Questions

What is OT network monitoring?

OT network monitoring is the practice of watching traffic on an industrial control system network to identify the devices connected to it and detect suspicious or unusual activity. It is typically done passively, using a copy of the traffic, so that the monitoring itself cannot disrupt the process.

Why can't I just run a normal vulnerability scanner on my OT network?

Active scanners probe devices to identify them. Older industrial controllers were not designed for unexpected traffic and can fault when they receive it, which in a plant setting can mean a stopped process or a tripped safety system. Passive monitoring avoids that risk because it never sends anything to the devices it is identifying.

What is the difference between a SPAN port, a mirror port, and a network

tap?

All three deliver a copy of network traffic to a monitoring sensor. SPAN and mirror ports are switch features that copy traffic in software, while a tap is a separate piece of hardware placed on the link. Which one you use usually depends on what your switches support and how much traffic you need to copy.

What is Hybrid Passive Monitoring?

Hybrid Passive Monitoring sends small broadcast messages using commands the devices already recognize, so that equipment which rarely communicates can still be identified. It is used alongside passive collection to close the gap left by quiet devices.

Which industrial protocols does Industrial Defender monitor?

Passive monitoring supports widely adopted protocols including Siemens S7, Profinet, MODBUS, BACnet, and DNP3, among others. Protocol coverage is worth checking against your own environment before deployment.

What does NERC CIP-015 require?

CIP-015-1 requires internal network security monitoring inside electronic security perimeters. Its three requirements cover collecting and analyzing network activity, retaining data associated with anomalies, and protecting that data from unauthorized modification or deletion.

When do I have to comply with CIP-015?

High-impact BES Cyber Systems and medium-impact systems with external routable connectivity must comply by October 1, 2028. Remaining systems have until October 1, 2030. The standard itself took effect on September 2, 2025.

What is east-west traffic and why does it matter?

East-west traffic moves between devices inside the same network segment, as opposed to crossing the perimeter. It matters because an attacker who is already inside the environment generates east-west traffic, and perimeter defenses do not see any of it.

Can network monitoring alone satisfy my compliance requirements?

Not usually. Network monitoring identifies devices and detects traffic anomalies, but it cannot report patch levels, user accounts, firewall rule changes, or running services on a device. Most frameworks ask for that information as well, which requires endpoint collection alongside the network sensors.

Will passive monitoring slow down my control network?

No. A passive sensor receives a copy of the traffic and sends nothing back, so it adds no load to

the control network and cannot sit in the path of process communication.

Resources

[PLACEHOLDER: RESOURCE LINKS]
NERC CIP-015-1 standard page: _____
FERC Order 907: _____
NIST SP 800-82 Rev. 3: _____
OT Cybersecurity: The Ultimate Guide: _____
What Is NERC CIP: The Ultimate Guide: _____

Schedule a demo: _____

About Industrial Defender: Since 2006, Industrial Defender has been solving the challenge of safely collecting, monitoring, and managing OT asset data at scale, while giving cross-functional teams a single view of security. The platform is built for complex industrial control system environments by engineers with decades of hands-on OT experience.
1 (877) 943-3363 | info@industrialdefender.com | 225 Foxborough Blvd, Foxborough, MA 02035 | industrialdefender.com