EDGE TEAM
TECHNOLOGY

WHITE PAPER

Securing what IT doesn't manage

A practical guide to OT and IoT security for organizations running both.

For: IT and security leaders at organizations with operational technology, connected devices, or both, and a security team sized for neither.

Reading time: ~12 minutes · May 2026

Executive summary

Every organization now runs technology its IT team never bought, never inventoried, and cannot patch. Building controls, factory equipment, medical devices, security cameras, badge readers, and the long tail of connected sensors sit on the same networks as laptops and servers. They are invisible to the tools built to defend laptops and servers, and that blind spot is where a growing share of breaches now begin.

This paper is for the organization that has operational technology (OT), connected devices (IoT), or both, and a security program that was never scoped for either. It explains why these environments are uniquely hard to defend, what the threats actually look like, and a practical framework for closing the gap without ripping out equipment or hiring a specialist who is nearly impossible to find.

The thesis is simple. You cannot protect what you cannot see, and you cannot see OT and IoT with the tools you already own. Closing the gap starts with visibility, moves to segmentation, and ends with a clear decision about which work stays in-house and which gets delegated to a partner.

What you will leave with

- A working definition of OT and IoT, and why both are invisible to traditional security tooling.
- The six reasons these environments are harder to secure than standard IT.
- A four-step framework: discover, segment, monitor, respond.
- A decision guide for what to own and what to delegate.

1. The visibility gap

Two categories of technology have quietly become the largest unmanaged surface on most networks.

Operational technology (OT)

OT is the hardware and software that monitors and controls physical processes. Programmable logic controllers on a production line, the SCADA systems behind a water utility, the building management system running HVAC and access control, the equipment on a hospital floor. OT keeps the physical world running, and until recently it ran on networks that had little or nothing to do with corporate IT.

The Internet of Things (IoT)

IoT is the broad category of connected devices that are not traditional computers. Cameras, badge readers, environmental sensors, smart displays, printers, point-of-sale terminals, and the steady stream of new devices that arrive with a network port and a default password. Individually they look harmless. Collectively they are a large, unmonitored population living on the same network as everything that matters.

Why both are invisible

Traditional security tools were designed for managed computers. Endpoint detection needs an agent installed on the device. Vulnerability scanners expect to log in and inspect. OT and IoT devices accept neither. They cannot run an agent, they often speak proprietary protocols, and many were built years before security was a design consideration. The result is that most organizations underestimate how many connected devices they have, frequently by a wide margin. The first time a team runs a proper discovery pass, the device count is routinely several times higher than anyone expected.

> **IN PRACTICE**
> A mid-size manufacturer believed it had roughly 400 connected devices. A passive discovery pass found over 1,300, including controllers, cameras, and sensors that no one in IT had ever inventoried. You cannot write a security policy for devices you do not know exist.

2. Why OT and IoT are uniquely hard

Securing these environments is not just standard IT security applied to more devices. Six structural differences make the work genuinely harder.

1. IT and OT have already converged

The air gap is mostly a memory. OT now connects to IT for telemetry, remote maintenance, and operational efficiency. That connection delivers real value, and it is also the path an attacker uses to cross from a compromised laptop into the systems that run physical operations.

2. You cannot just patch

A controller running a production line or a device keeping a patient monitored cannot be taken offline for patching on a Tuesday afternoon. Downtime is measured in lost revenue or, in some settings, physical risk. Worse, a large share of OT runs operating systems that reached end of life years ago and will never receive another patch.

3. The protocols were never built for security

Many OT protocols were designed for reliability and determinism, with security simply out of scope at the time. Several carry no authentication and no encryption by default. A device on the same network segment can often issue commands without proving who it is.

4. Safety and availability outrank confidentiality

In corporate IT, the instinct during an incident is to isolate or shut down the affected system. In OT, stopping the wrong system can halt production or create a safety hazard. Any control introduced into an OT environment has to be non-intrusive, because a security tool that risks tripping a turbine or a ventilator is worse than the threat it guards against.

5. There is nowhere to install an agent

You cannot put software on a sensor or a controller. That removes the entire foundation of modern endpoint security. Visibility and detection have to happen passively, observed from the network rather than reported by the device.

6. Ownership is ambiguous

OT is frequently owned by facilities, operations, or a plant manager rather than IT. IoT is often bought by whichever department needed it. When no one clearly owns the security of these devices, no one is accountable for it, and it falls through the gap between teams.

3. The threat reality

The risk is not theoretical, and it does not require a sophisticated nation-state actor. The most common scenarios are mundane and effective.

Ransomware that crosses the boundary

The typical OT incident does not begin in OT. An attacker compromises a standard IT system through phishing or a stolen credential, moves laterally, and either reaches the OT network or forces operations to shut down OT systems out of caution to contain the spread. In several of the most disruptive incidents on record, the production stoppage was a precautionary IT decision, not a direct OT compromise. The blast radius reached operations regardless.

The connected device as a foothold

A camera or sensor with a default password is a quiet entry point onto the network. These devices are rarely monitored, rarely updated, and rarely missed. An attacker who lands on one can sit undetected and use it as a base to study the environment and move toward higher-value targets.

Conscripted into a botnet

Unsecured IoT devices are routinely absorbed into botnets and used to launch denial-of-service attacks against others. Your unmonitored cameras can become someone else’s weapon, consuming your bandwidth and your reputation along the way.

> **THE PATTERN**
> In nearly every case, the device that lets an attacker stay hidden is the device nobody was watching. Visibility is not a nice-to-have. It is the precondition for everything else.

EDGE TEAM
TECHNOLOGY

4. A framework: discover, segment, monitor, respond

Closing the OT and IoT gap follows four steps, in order. Skipping the first makes the rest impossible.

Step 1: Discover

Build a complete, continuously updated inventory of every connected device, what it is, what it communicates with, and what normal behavior looks like for it. Because agents are not an option, this is done by passively observing network traffic and identifying devices by how they behave. This is step zero, and most organizations have never completed it. Everything downstream depends on knowing what is actually on the network.

Step 2: Segment

Once you know what is present, separate it. OT should not share a flat network with corporate IT. IoT should be isolated from production and from sensitive systems. Segmentation, and finer-grained microsegmentation where it fits, limits how far an attacker can move after gaining a foothold. If a compromised camera can only talk to the few systems it legitimately needs, it is a far smaller problem.

Step 3: Monitor

Watch OT and IoT traffic continuously for anomalies. Since detection cannot rely on an agent, it happens at the network layer. Establish a baseline of normal communication for each device, then alert when behavior deviates: a sensor suddenly scanning the network, a controller talking to a system it has never contacted, traffic leaving for an unexpected destination.

Step 4: Respond

Build a response plan that respects how OT actually works. You cannot reimage a controller the way you would a laptop, and you cannot always pull a device offline without operational consequences. Effective OT response is a coordinated decision among security, operations, and safety, agreed in advance and rehearsed, so that the first time the plan is used is not during a live incident.

> **IN PRACTICE**
> A regional utility ran discovery, segmented its OT network away from corporate IT, and stood up passive monitoring. When a contractor laptop later introduced malware on the IT side, segmentation kept it from reaching OT, and monitoring flagged the lateral movement within minutes. The production environment never went down.

5. What to keep, what to delegate

A small security team cannot operate an OT and IoT security program alone, and it should not try to. The work splits cleanly into what only you can do and what is better delegated to a partner.

Keep in-house

- Policy decisions. What is allowed to talk to what, which devices can be taken offline, and what the acceptable risk is for each system.
- The relationship with operations and facilities. Security of these devices only works when IT, operations, and safety are aligned, and that alignment is yours to build.
- Business context. Only your team knows what a given device controls and what happens to the business if it stops.

Delegate to a partner

- The specialized platforms that discover, classify, and passively monitor OT and IoT devices.
- Around-the-clock monitoring of device traffic, which a team of one cannot staff.
- Incident response that requires OT-specific expertise during a live event.

This is the value-added reseller model. EdgeTeam designs the architecture, recommends the right discovery and monitoring platform for your environment without loyalty to any single vendor, and coordinates the managed partner who runs it. You keep the decisions that require knowing your business. We bring the specialists and the tooling for everything else.

Conclusion

The devices your security tools cannot see are multiplying, and they sit on the same networks as everything you are trying to protect. The good news is that the path forward is well understood and does not require a large team. Start with discovery and get a complete inventory. Segment what you find. Monitor it passively. Build a response plan that respects how OT operates. Do those four things in order and the gap closes.

The mistake is to wait until an incident forces the inventory. By then the device that let the attacker in was already on the network, unwatched, the whole time.

Next step

EdgeTeam's Security Posture Review can extend to OT and IoT discovery: a passive look at the connected devices on your network, what they talk to, and where the exposure sits. We will scope it to your environment on the first call.

Request a posture review: edgeteam.com/cybersecurity

Or call the bridge: 1.866.EDGETEAM, available 24/7.

About EdgeTeam Technology

EdgeTeam is a value-added reseller and architect of record for organizations across K-12, Higher Education, SMB, Enterprise, and Local Government. We design, recommend, and coordinate cybersecurity, infrastructure, and connectivity engagements with vendor-neutral partners. We do not run an in-house SOC. We pair our architecture team with the right managed partner for your environment.

edgeteam.com · sales@edgeteam.com · 1.866.EDGETEAM