NETWITNESS

Whitepaper

IT/OT Convergence Limitations: Solving the Visibility Divide

Executive Summary

The convergence of IT and OT networks has eliminated the air gaps that once kept industrial control systems safe. Security teams can monitor corporate infrastructure. They cannot see the production floor. This is not a tooling problem it is a structural failure. OT environments run on legacy protocols, decades-old hardware, and systems that were never designed with security in mind. Standard IT monitoring cannot be dropped into these environments without introducing new risk, which is precisely why fewer than 10% of OT environments have meaningful monitoring in place today.

The attack path is consistent: phishing or stolen credentials, lateral movement through corporate systems, then a pivot across a bridging point into OT. Once inside, adversaries operate in near-total darkness from the defender's perspective. Detection platforms have matured, but detection alone is not sufficient. In 2025, every ransomware incident monitored by leading OT platforms still resulted in an operational shutdown because a 45-minute gap exists between identifying a threat and being able to stop it. The real divide is not visibility. It is the gap between seeing a threat and stopping it.

Closing that gap requires a sequenced approach: foundational passive monitoring first, then unified cross-domain visibility, then inline prevention architecture that sits in the traffic path rather than beside it. Organizations that followed this sequence have achieved zero-intrusion rates of 52%, up from 6% in 2022. With NIS2 and NERC CIP 15-1 demanding comprehensive OT visibility, the window for treating this as optional is closing fast.

Table of Contents

What Are You Missing When IT and OT Converge?

There's a version of the IT/OT convergence story that gets told at conferences. It's about digital transformation, connected assets, and smarter operations. What gets skipped over is the security consequence of tearing down the walls between corporate networks and production floors: nobody can actually see what's happening anymore.

Not fully, anyway.

Security teams can monitor email servers, endpoints, and cloud workloads. They have dashboards, alerts, and SIEMs running 24/7. But the moment a threat crosses into operational technology, it's like watching someone walk into a fog bank. The tracking stops. The visibility ends. And the production floor, with all its PLCs, historians, and engineering workstations, carries on completely opaque to the people whose job it is to protect it.

This isn't a small problem to patch around the edges. It's a structural flaw in how most organizations have approached convergence.

How Bad Is It?

The numbers are clarifying. 81% of assessed manufacturing environments have poor IT/OT network segmentation. 46% share Active Directory domains across both environments. What this means in practice is that an attacker who compromises a corporate credential doesn't just get access to email. They potentially get a path directly into production systems.

And when that happens, they disappear from view. Security tools don't follow them. Alerts don't fire. The intrusion continues.

Fortinet's 2025 report found that 60% of organizations that experienced an intrusion saw impact on both IT and OT systems. That figure was 21% in 2022. The attack surface isn't just growing. It's growing fast, and the defenders aren't keeping up.

Fewer than 10% of OT environments have meaningful monitoring in place. The reason isn't that tools don't exist. It's that deploying visibility into live production environments is genuinely risky. These networks carry traffic that controls physical processes: valve positions, conveyor speeds, temperature setpoints. Plug in the wrong monitoring tool without understanding the operational context, and you can disrupt the very process you're trying to protect.

That tension sits at the heart of every IT/OT security conversation, and it doesn't get resolved by pretending it isn't there.

Why Standard Security Tools Simply Don't Work?

Industrial protocols are a foreign language to IT tools

OT devices speak Modbus, OPC UA, DNP3. These protocols were built for reliability and real-time control, not security. They were never designed to be inspected by a SIEM or flagged by a firewall rule. Standard IT security tools can't interpret them, which means security teams literally cannot distinguish a legitimate command from a malicious one. If an attacker sends a rogue command to a PLC, it looks the same as a normal operational instruction to anyone watching through an IT lens.

Network segmentation is not the same as security

The Purdue model, which organizes industrial networks into levels from field devices up through the enterprise zone, gives organizations a framework for thinking about segmentation. That's genuinely useful. But segmentation alone doesn't tell you what's actually moving between those levels. Without visibility inside and between Purdue levels, you can't verify that segmentation rules are being enforced. You can't detect lateral movement. You can't see which IT identities are reaching into OT. The architecture gives you a map. It doesn't show you what's walking around on it.

OT systems were never built for security maintenance

These systems are designed to run. Continuously. For years, sometimes decades, without interruption. Many depend on legacy operating systems that haven't seen a patch in years, and you can't just install an agent or run a vulnerability scan the same way you would on a corporate laptop. A few hours of unplanned downtime on a production line can cost millions. Security teams know this, and it makes them cautious about touching anything. That caution is rational, but it means security debt compounds quietly in the background.

Remote assets are harder still

Utility substations, unmanned manufacturing lines, remote pipeline infrastructure. These assets rely on legacy devices with limited compute capacity. They often connect via low-bandwidth links. Third-party vendors access them through VPN or RDP. Each of these conditions limits what centralized monitoring can see and adds to the overall attack surface.

The Attack Path Everyone Should Understand

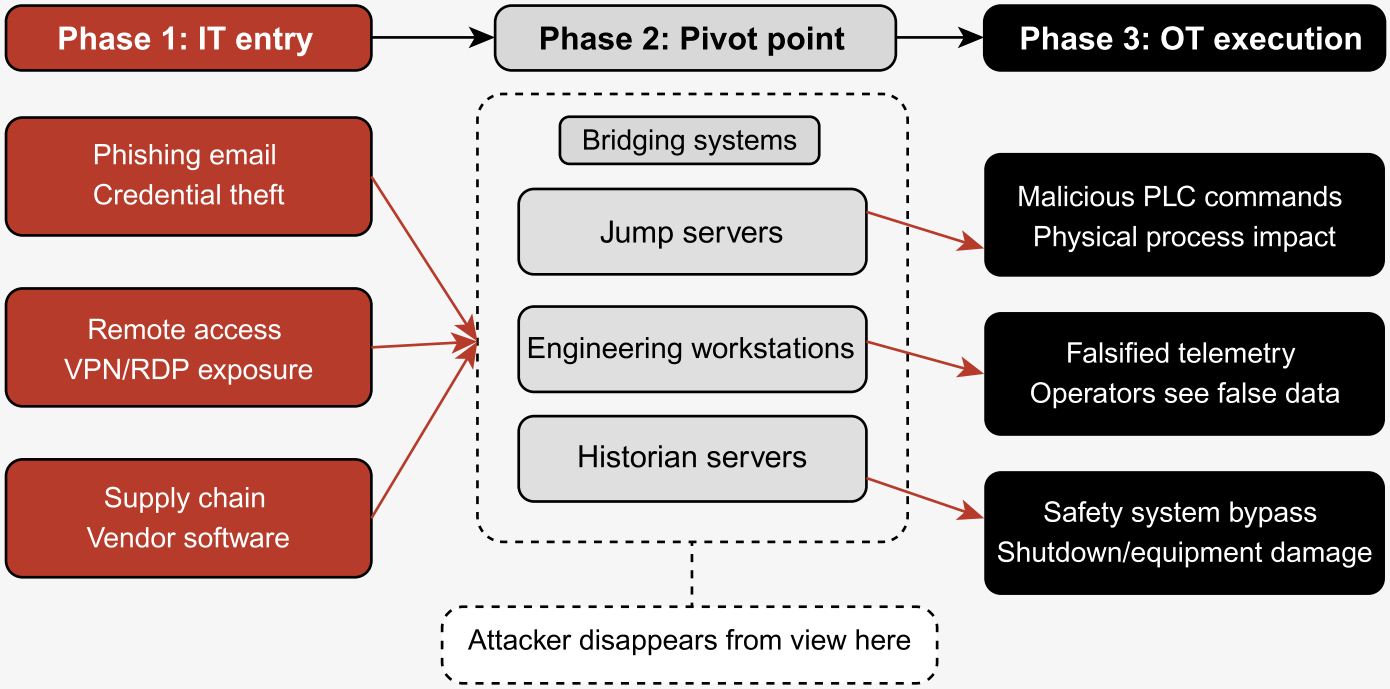
Modern OT attacks don't start at the PLC. They start with a phishing email, a stolen credential, or an exposed remote access gateway. From there, the attacker moves through corporate systems until they find a bridging point: a jump server, an engineering workstation, a historian that sits between IT and OT.

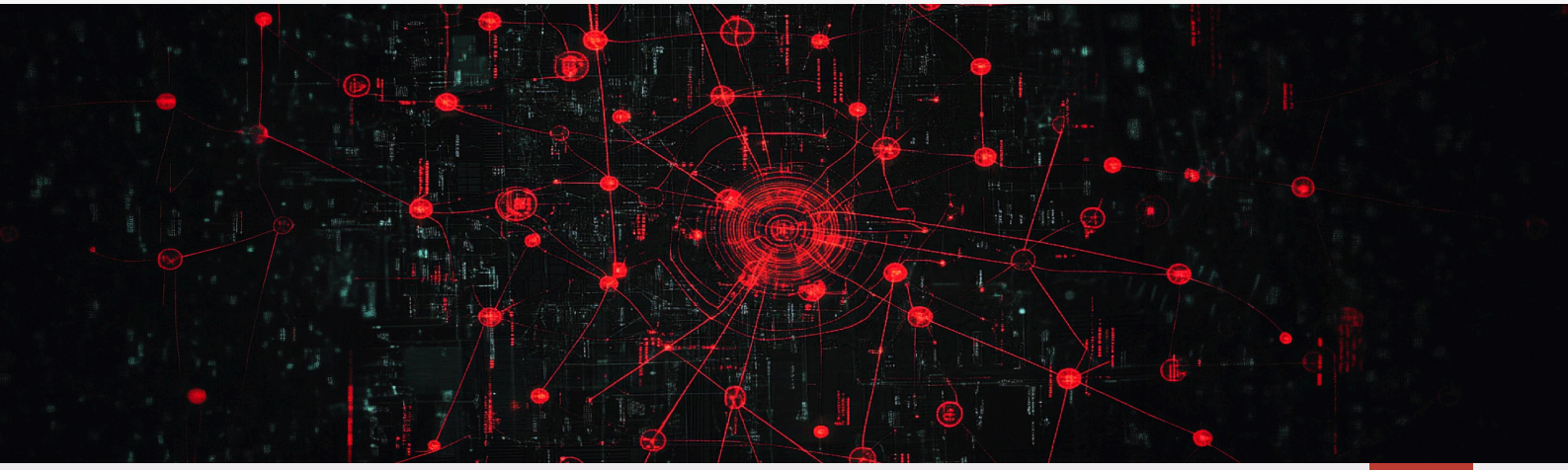
Once they reach that bridge, the rules change. They can enumerate OT assets, replay commands, and move laterally through systems that were assumed to be isolated. The OT environment, built on the assumption that everything inside it is trusted, doesn't question what it receives.

Stuxnet made this lesson visible more than a decade ago. If you can't validate protocol behavior and command integrity, industrial systems will blindly execute whatever they're told. That's the opposite of a secure posture, and it remains true today in most environments.

The convergence attack path

How attackers move from corporate network to industrial control systems





The Gap Between Seeing and Stopping

Here's where the conversation needs to move past the standard visibility narrative. Detection has genuinely improved. There are platforms that discover OT assets, monitor industrial protocols, and surface anomalies. That progress is real.

But in 2025, 100% of ransomware incidents monitored by leading OT security platforms still resulted in operational shutdowns. Detection wasn't the problem. The problem was that detection didn't lead to prevention fast enough.

Most OT security tools connect via SPAN ports. They observe passively, which is important for operational safety, but it means they're watching from the side. When they identify a threat, they have to hand off to a separate firewall or NAC solution. That coordination takes time. Roughly 45 minutes, based on observed incident data. In that window, ransomware encrypts, attackers move laterally, and malicious commands reach PLCs. By the time enforcement kicks in, the damage is done.

The real divide isn't just visibility. It's the gap between identifying a threat and actually stopping it. That's the architectural problem that hasn't been fully solved.

What Closing This Gap Actually Requires

Unified monitoring across both domains

Running separate IT and OT monitoring platforms guarantees blind spots. When a network issue causes quality control failures, IT sees nothing unusual while OT sees equipment errors. Hours get wasted in cross-team finger-pointing while the actual problem compounds. A single monitoring architecture that understands both traditional protocols like SNMP and WMI alongside industrial protocols like OPC UA and Modbus isn't a luxury. It's a baseline requirement.

Combining passive and active collection strategically

Passive monitoring remains the foundational approach for OT because it carries minimal operational risk. But passive-only monitoring has real limitations: assets that communicate infrequently, air-gapped segments, and legacy equipment that doesn't support port mirroring all fall through the cracks. Active collection, deployed during planned maintenance windows in collaboration with operations teams, fills those gaps without compromising safety. The key word is strategically. This isn't about running aggressive network scans. It's about enriching the asset picture deliberately and carefully.

Inline prevention architecture

Observation is necessary but not sufficient. Organizations need security infrastructure that sits in the traffic path, not beside it, and can act in real time. Combined with hardware bypass technology that ensures production continuity during security maintenance, inline deployment is the architectural shift that converts detection capability into actual protection. This is where the industry needs to go, and it's where the most mature industrial security programs are heading.

Cross-domain incident response that actually works

Security and operations teams speak different languages, prioritize different outcomes, and often work in organizational silos. Effective response to OT incidents requires playbooks and workflows built specifically for industrial environments, OT-native threat intelligence rather than repackaged IT threat feeds, and automated coordination that reduces the manual handoff time between detection and enforcement.

The Regulatory Clock Is Running

NIS2 in the EU and NERC CIP 15-1 in the US are both pushing toward mandatory, comprehensive OT visibility. Organizations that have been treating this as a future problem are running out of runway.

The organizations that have gotten ahead of this demonstrate what's possible. Those with strong, sequenced programs have achieved zero-intrusion rates of 52%, up from 6% in 2022. The sequence that worked: visibility first, introduced carefully and in collaboration with operations teams, then segmentation, then access controls, then governance layered on top. Skipping steps or compressing the timeline produces security theater, not actual resilience.

The Honest Conclusion

Deploying more IT security tools into OT environments doesn't solve this. It makes it worse, because it creates false confidence while introducing operational risk that erodes trust between security and operations teams.

What works is acknowledging that OT is different. Different constraints, different priorities, different failure modes. The path forward requires architecture built around those realities: unified visibility, thoughtful passive and active collection, inline prevention where operationally appropriate, and cross-domain response capability.

The goal is to move from detect-and-respond to verify-and-enforce. But you can't enforce what you can't see. Visibility isn't the finish line. It's the starting point.

Your OT Environment Is Already a Target

Talk to our experts and find out exactly where your visibility gaps are before an attacker does.

Talk to an Expert

Contact Information

Email for customer Service
info@netwitness.com

Website
www.netwitness.com

NETWITNESS