CISCO
SECURE

Security Survey Report

Industrial Organizations Still Lack Visibility and Readiness to Defend Against OT/ICS Cyberattacks

CISCO The bridge to possible

Contents

Executive summary

Are industrial organizations prepared to defend their Operational Technology (OT) and Industrial Control System (ICS) environments in the event of a cyberattack?

That's what Cisco set out to answer in a Q3 2022 survey together with Gartner Peer Insights and Takepoint Research involving 100 IT, OT, engineering, and InfoSec professionals across the globe.

What we found was surprising: 77% of industrial organizations are still in the beginning stages of their OT security journey. And none of the respondents have yet to fully secure their OT/ICS environments.

This is worrying, considering the post-pandemic world in which we find ourselves today.

Much has changed over the last three years. The pandemic has significantly accelerated the digital transformation of OT, which has led most, if not all, of an organization's critical operations to be integrated with digital technologies. In turn, cyberattacks such as those suffered by the Colonial Pipeline and JBS in 2021 have become more prevalent as bad actors home in on the vulnerabilities of OT/ICS networks.

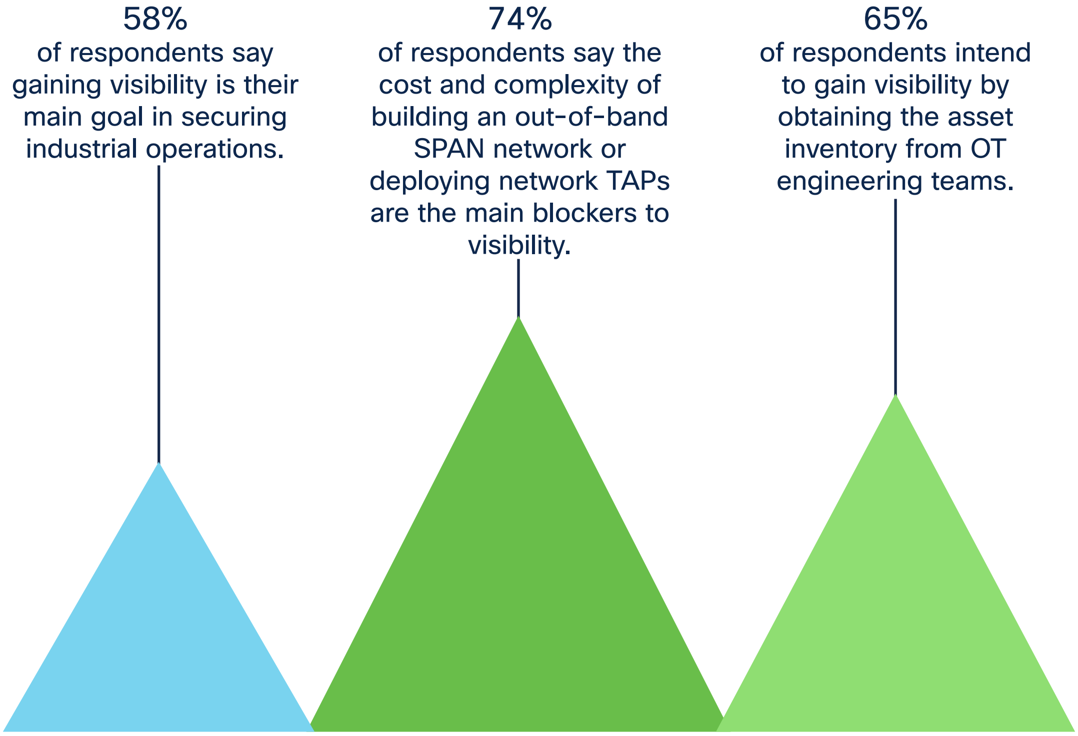
Behind closed doors, pressure is building in the boardroom, with business continuity concerns and security directives such as CISA's Shields Up no doubt contributing much of it. Our conversations with C-suite executives reveal that most organizations recognize that they're not prepared for a cyberattack and that many are just starting to prioritize OT security.

Looking ahead, we see the perfect OT security storm headed our way. Most industrial organizations are expected to have converged security functions across both IT and OT environments in the next three years, which will greatly expand their attack surfaces. And attacks on OT/ICS environments will continue to intensify to the point that lives will be harmed or lost, likely within the decade.

Industrial organizations must accelerate their OT security efforts now to safeguard business continuity.

Key findings

Our survey revealed that comprehensive visibility of OT devices and industrial networks is the main goal—and challenge—to securing industrial operations. While this is not a surprise, considering the stage that most organizations are at in their OT cybersecurity journeys, their approaches and challenges to achieving this goal are interesting to note.



58%
of respondents say gaining visibility is their main goal in securing industrial operations.

74%
of respondents say the cost and complexity of building an out-of-band SPAN network or deploying network TAPs are the main blockers to visibility.

65%
of respondents intend to gain visibility by obtaining the asset inventory from OT engineering teams.

Why is visibility the foundation of industrial security?

To understand what it takes to secure OT/ICS environments in a fast-changing digital environment, one has only to look at the evolution of IT security over the last 20 years.

Before, security efforts focused on the perimeter and sensitive systems were isolated. Internal network visibility was deemed unimportant because it was assumed that anyone with access was a legitimate agent. That all changed with phishing and zero-day attacks.

Now, with zero-trust and defense-in-depth approaches, the focus has shifted to maintaining full visibility and network segmentation to limit the effects of a breach. We see this in the proliferation of Network Detection and Response (NDR) systems and round-the-clock Security Operations Centers (SOCs).

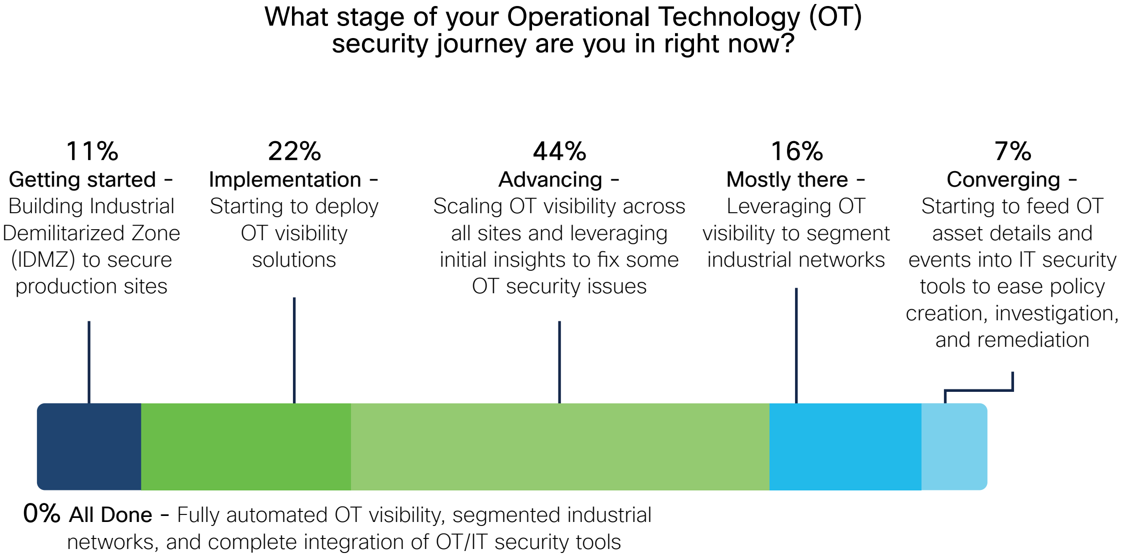
Prevention is still a big part of security, but so is rapid containment and remediation.

When it comes to securing their OT/ICS environments, many organizations have followed the same playbook—wall off the network and isolate critical systems—but as we've seen, this won't work for long.

Organizations simply have to establish full visibility into their IT and OT networks before any remedial or preventive measures can be taken.

Current status and goals

Most organizations are just beginning their OT security journey



While no organization surveyed has yet to reach full OT security maturity, the good news is that the data reflects a level of self-awareness and urgency in improving the situation.

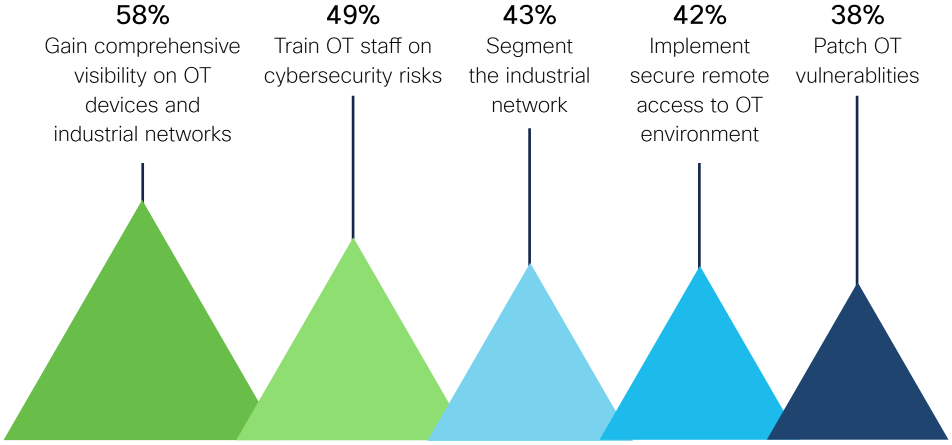
11% of respondents have started their journeys with industrial demilitarized zones (IDMZ) to secure production sites, 22% have started implementing OT visibility solutions, and 44% are scaling OT visibility across all sites and leveraging initial insights to fix some OT security issues.

However, only 23% of respondents have scaled their OT visibility deployments, and even fewer are leveraging these tools in an advanced security strategy: 16% have segmented their industrial networks, and only 7% have started feeding OT asset details and events into IT security tools to ease policy creation, investigation, and remediation.

Overall, we find that security leaders are seeing the benefits of OT visibility solutions and view them as a mature technology to be deployed at scale.

Visibility, training, and segmentation are top priorities

What are your main goals for securing your industrial operations over the next 12-24 months?



Introduce OT/IT response and remediation playbooks **27%**,
Integrate OT alerts into the security operations center (SOC) **25%**,
Implement intrusion detection (IDS) on the industrial network **21%**,
Create cross-domain (OT/IT) functional teams **6%**, Other **0%**

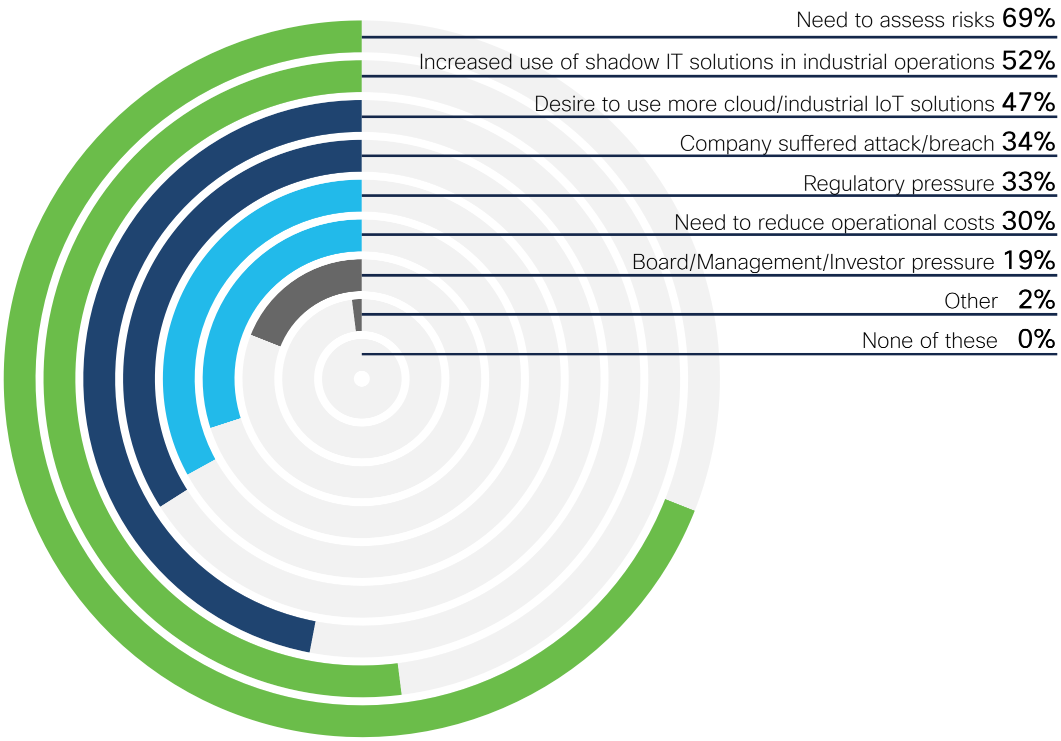
When it comes to goals, 58% of respondents say they intend to gain comprehensive visibility into their industrial network within 24 months and 49% indicated that they're prioritizing cybersecurity training, while 43% aim to segment their industrial network.

On segmentation, it's worth noting that even though OT environments have become more connected over time, they have not been optimized for security. IDMZs, firewalls, and unidirectional gateways are broad security measures that may secure the perimeter, but they do not protect the OT environment from whoever makes their way in.

Many OT networks are still flat and unsegmented, and it is not uncommon for organizations not to have a full accounting of the whole network.

Risk management and shadow IT are driving the need for visibility

What are the primary factors driving the need for industrial network visibility and cybersecurity at your organization?



It’s interesting to note that the top two drivers for network visibility are the need to assess risks (69%) and the increased use of shadow IT solutions within industrial operations (52%).

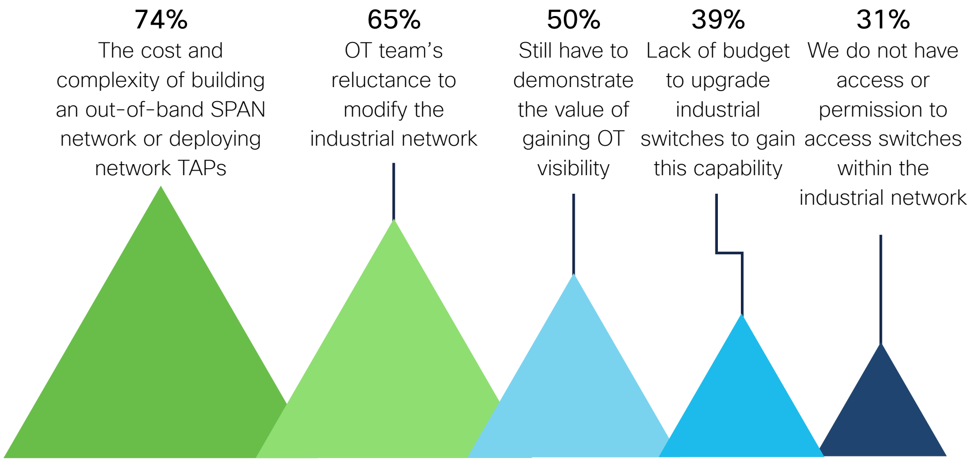
This reflects the fact that OT security issues are often much more serious than organizations realize and that, anecdotally, security leaders know that their organizations are vulnerable. For example, it is not uncommon to find various ports wide open or operating systems deployed with default credentials or OEMs assessing machines without supervision.

These vulnerabilities can be exposed and addressed only with comprehensive visibility into connected assets and network activities.

Challenges

Conventional solutions are costly and complex

What do you see as the main obstacles for gaining comprehensive visibility on OT devices and industrial networks?



None of these **2%**, Other **1%**

74% of respondents say that the cost and complexity of building a Switched Port Analyzer (SPAN) Network to capture and monitor industrial network traffic is the main blocker to visibility. This is not surprising, considering that this would entail building out a mirror network, which is simply not scalable.

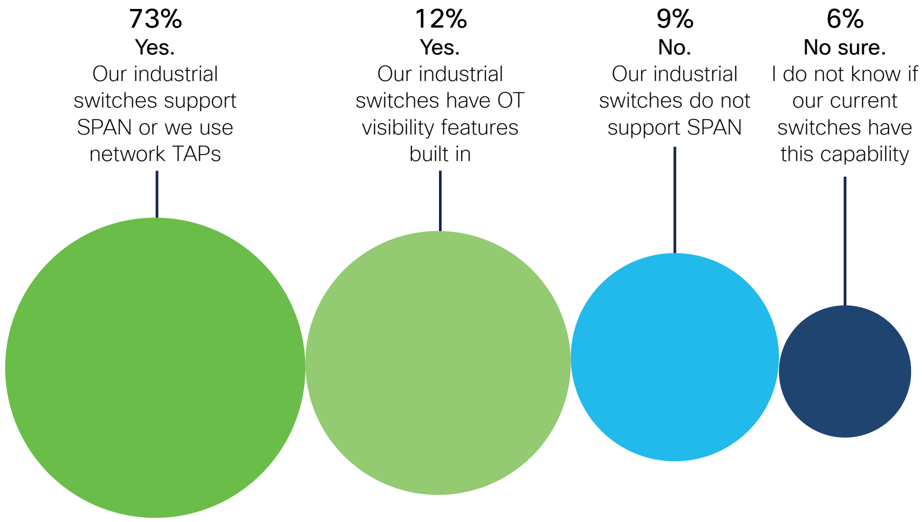
65% say that OT teams are reluctant to modify the network. Again, this is not surprising considering OT's priority to keep the lights on. Adjacent to that, 50% say demonstrating the value of gaining OT visibility is a challenge.

Moving on, 39% of respondents say they lack the budget to upgrade industrial switches, which further supports the fact that cost is the main constraint. And 31% say they do not have permission to access switches within the industrial network.

In our experience, only when IT builds trust with OT and can demonstrate the value of visibility in improving operational reliability will the business increase its investments in network upgrades. Until then, IT has to work around these constraints.

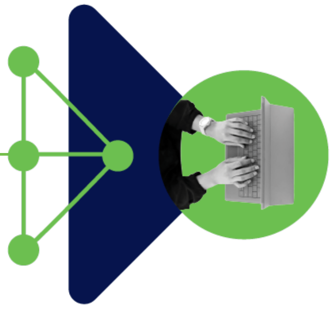
Scalability remains a challenge

Is your industrial network ready to give you visibility on OT devices and communications?



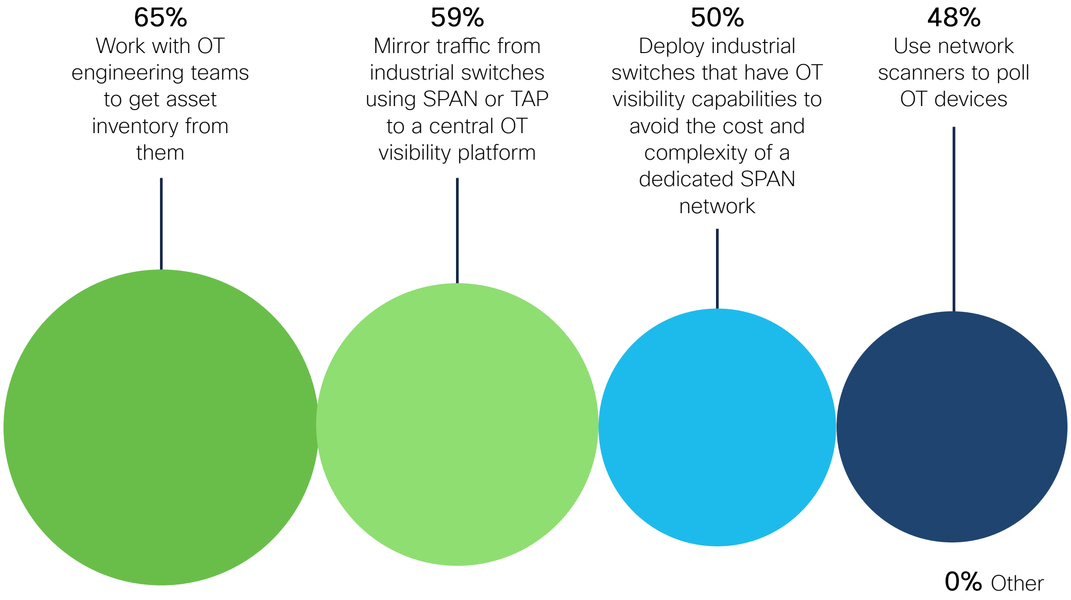
When quizzed on their network's readiness to provide visibility, 73% of respondents said that their switches were SPAN or Traffic Access Point (TAP) ready. This might explain the fixation on SPAN or network TAPs as a monitoring solution, even though 74% of respondents say such a deployment would be too costly and complex.

It's also revealing that most respondents are not aware of other more cost-effective methods of monitoring network traffic, such as using industrial switches with built-in asset discovery and Deep Packet Inspection (DPI) capabilities. Only 12% say their industrial switches have OT visibility features built in.



Organizations must rethink visibility and scalability in OT

What methods do you favor for gaining visibility on OT devices and industrial networks?



65% of respondents say they would work with OT engineering to get an inventory, but this method is unreliable, as engineering inventories are generally incomplete and not updated in real time. The main issue is that such inventories don't provide visibility into actual communication activities and rogue devices connecting to the network. It also does not help detect threats and address the problem of shadow IT.

59% prefer mirroring traffic using a SPAN or TAP, likely from early successes or because they don't know of alternatives. This will be problematic at scale as the costs and complexity add up.

50% say they would use industrial switches with OT visibility capabilities. Of the three options, this solution has much going for it. It does not require building out a separate data collection network, nor does it require any modification of the OT network. This solution addresses the top two challenges discussed earlier.

48% say they would use network scanners. But this option, like getting an inventory from OT engineering, does not provide real-time visibility into assets or communications. Furthermore, although network scanners are widely used to detect IT devices in enterprise networks, they are inappropriate in industrial networks. Most OT devices are old and will quickly exhaust their limited CPU and memory resources. Network scans will likely bring them down and disrupt production. OT visibility solutions capable of querying assets using semantic technologies could be a viable alternative.

This challenge with network scanners is a good example of why organizations must look beyond standard IT best practices to find solutions, especially when it comes to OT challenges.

In-band vs. out-of-band: Which is best for your organization?

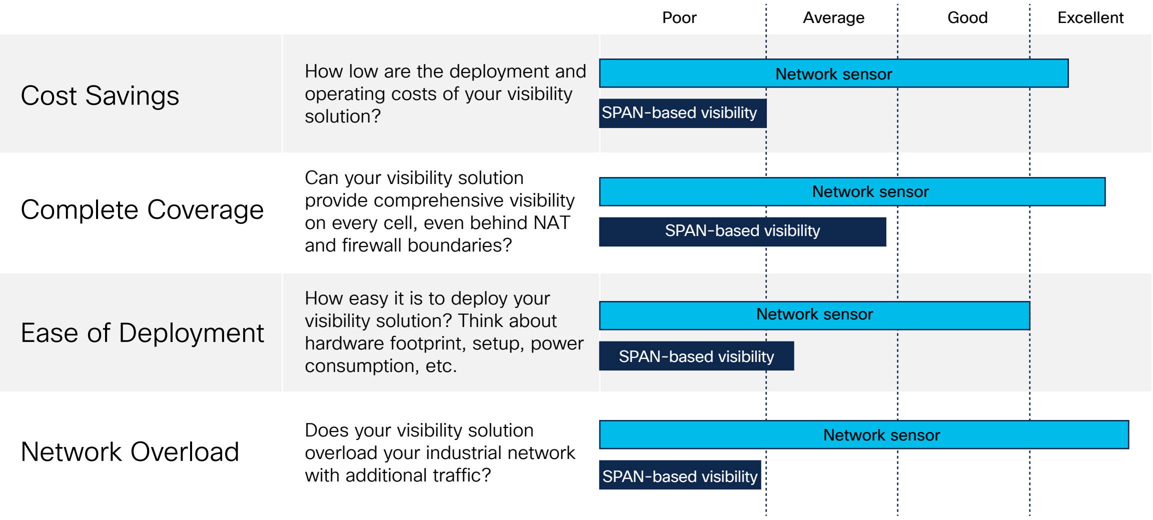
Let's compare the two most common ways of establishing visibility: building a SPAN network (out of band) or upgrading existing networking equipment (in-band) to devices with DPI capabilities.

In a SPAN-based solution, network traffic is collected from industrial switches and sent to a dedicated security appliance over an out-of-band network for analysis. An alternative solution is to use networking equipment that embeds visibility features such as passive DPI and active asset discovery.

These network elements will extract meaningful information and send only lightweight metadata to a central OT security platform for further analysis. As this metadata typically represents 3% to 5% of the original traffic, it can be transmitted in-band without the need to add additional network resources to the industrial environment.

Organizations should consider the following factors when choosing a solution:

- **Cost:** In-band solutions are relatively inexpensive because they do not require additional hardware or networking. Out-of-band solutions require sourcing, installing, and maintaining dedicated appliances, as well as a whole new network, including switches and cabling.
- **Scalability:** In-band solutions leverage existing network resources and can be implemented quickly. Out-of-band solutions require significant time and effort to build out a separate network.
- **Visibility:** Out-of-band solutions come at a cost, forcing most organizations to monitor traffic only from aggregation switches. This limits their visibility into north-south traffic and restricts their ability to discover assets sitting behind industrial firewalls or Network Address Translation (NAT) boundaries. With an in-band solution, visibility is built into every switch deployed in the environment.
- **Complexity:** In-band solutions do not require rethinking the network topology, just additional configuration. A SPAN network becomes more complex the bigger it becomes.
- **Bandwidth impact:** In-band solutions send lightweight metadata. Out-of-band solutions duplicate traffic and generally require building a separate network to avoid control loop congestions and jitter in the industrial network.



Cost Savings	How low are the deployment and operating costs of your visibility solution?
Complete Coverage	Can your visibility solution provide comprehensive visibility on every cell, even behind NAT and firewall boundaries?
Ease of Deployment	How easy it is to deploy your visibility solution? Think about hardware footprint, setup, power consumption, etc.
Network Overload	Does your visibility solution overload your industrial network with additional traffic?

For more details on gaining visibility by using an in-band or out-of-band architecture, refer to this technical brief.

Conclusion

The vulnerability of OT/ICS environments today cannot be overstated. Industrial organizations must accelerate their efforts to step up OT security.

Although most organizations are just beginning their OT security journey, it is encouraging to see them heading in the right direction. They have a fairly mature approach to security and understand the importance of visibility in enabling preventive and remedial measures.

Of course, visibility is just one part of the solution, but it is the foundational step on top of which everything else is built. Any viable solution must also be able to segment networks and be scaled across multiple sites cost-effectively.

Most importantly, organizations must look beyond standard IT best practices to find the best solution and improve the collaboration between IT, OT, and SecOps.

Cisco Industrial Threat Defense leverages your industrial network as a sensor and an enforcer to help you gain visibility at scale and adopt a step-by-step approach to implement a comprehensive OT security strategy. To learn more, visit cisco.com/go/iotsecurity.

Methodology

The findings in this report were derived from a Q3 2022 industry survey designed by TP Research and conducted by Gartner Peer Insights involving 100 IT, OT, engineering, and InfoSec professionals.

The respondents come from a diverse range of geographies, industries, and organizations:

- 84% of respondents are based in North America, and 16% in Europe, the Middle East, and Africa (EMEA).
- 74% of respondents are director level and above; 26% are managers.
- 50% of respondents come from enterprises with more than 10,000 employees; 17% come from organizations with 5,000 to 10,000 employees; 33% come from organizations with at least 1000 employees.