CISCO SECURE | Gartner Peer Insights™

Cybersecurity for Industrial Operations

Operational technology (OT) is essential to efficient and sustainable industrial processes. Industrial organizations benefit greatly from digital transformation and the addition of Internet of Things (IoT) devices and monitoring systems. However, this increased digital nature opens the industry to potentially devastating cyberattacks.

Gartner Peer Insights and Cisco surveyed 100 IT, engineering, and security professionals who are involved in managing and/or securing industrial networks for industrial organizations to understand their approach to OT cybersecurity.

Data collection: June 20 - September 5, 2022

Respondents: 100 IT/Eng/Infosec professionals

Visibility into industrial network risks is a key motivator for tech leaders as they work toward OT network maturity

Overall, the need to assess risks (69%) and mitigate the use of shadow IT solutions (52%) are the primary factors driving the need for industrial network visibility.

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

Unsurprisingly, tech leaders' first step for securing their industrial operations are to gain comprehensive visibility on OT devices and industrial networks (58%). Segmenting the industrial network and securing remote accesses are also top of mind (43% and 42% respectively).

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

- 58% Gain comprehensive visibility on OT devices and industrial networks
- 49% Train OT staff on cybersecurity risks
- 43% Segment the industrial network
- 42% Implement secure remote access to OT environment
- 38% Patch OT vulnerabilities

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%**

While nearly two-thirds of respondents (66%) say they are in the implementation or advancing stages of their OT security deployment, none said they had completed a full integration of their OT/IT security tools.

What stage of your operational technology (OT) security journey are you in right now?

- 11% **Getting started** – Building Industrial Demilitarized Zone (IDMZ) to secure production sites
- 22% **Implementation** – Starting to deploy OT visibility solutions
- 44% **Advancing** – Scaling OT visibility across all sites and leveraging initial insights to fix some OT security issues
- 16% **Mostly there** – Leveraging OT visibility to segment industrial networks
- 7% **Converging** – Starting to feed OT asset details and events into IT security tools to ease policy creation, investigation, and remediation

0% **All Done** – Fully automated OT visibility, segmented industrial networks, and complete integration of OT/IT security tools

While tech leaders prefer SPAN and TAP for OT visibility, cost and complexity remain major obstacles

About two-thirds of respondents rely on data provided by engineering teams (65%) to gain visibility. Most that use automated methods use SPAN or TAP technologies (59%), but 48% use network scanners that may risk disrupting operations.

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

- 65% Work with OT engineering teams to get asset inventory from them
- 59% Mirror traffic from industrial switches using SPAN or TAP to a central OT visibility platform
- 50% Deploy industrial switches that have OT visibility capabilities to avoid the cost and complexity of a dedicated SPAN network
- 48% Use network scanners to poll OT devices

0% Other

And nearly three-quarters of respondents (74%) also say that the cost and complexity of building an out-of-band SPAN network or deploying network TAPs is the main obstacle for gaining comprehensive visibility on OT devices and industrial networks.

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

- 74% The cost and complexity of building an out-of-band SPAN network or deploying network TAPs
- 65% OT team's reluctance to modify the industrial network
- 50% Still have to demonstrate the value of gaining OT visibility
- 39% Lack of budget to upgrade industrial switches to gain this capability
- 31% We do not have access or permission to access switches within the industrial network

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

Visibility remains a key motivator across various business units

The primary value OT visibility provides for IT teams is the ability to know exactly what is connected to the industrial network (76%). A large majority also see value in starting to segment the network, and enable collaboration with the OT teams (58%).

What *value* does OT visibility provide to your team? Corporate IT (n = 33)

- Know exactly what OT devices we have and what they are doing 76%
- Assess efficacy of current industrial network topologies and plan for more network segmentation 58%
- Understand use of shadow IT solutions in industrial sites 58%
- Enable effective collaboration between OT and IT experts 58%
- Other 0%

For cybersecurity teams, OT visibility's primary value lies in gaining an accurate understanding of the industrial attack surface (77%) and having OT information to extend their IT security tools to the industrial domain (77%). Network segmentation is also a priority (73%).

What *value* does OT visibility provide to your team? Corporate Cybersecurity (n = 52)

- 77% Gain an accurate understanding of the industrial attack surface (assets, vulnerabilities, traffic patterns, topologies, etc.)
- 77% Enrich SOC with information on OT assets and events to support threat detection, investigation and remediation across both IT and OT networks
- 73% Plan more effective industrial network segmentation to prevent attacks from spreading
- 37% Enable effective monitoring of industrial networks at scale
- 25% Gain information for regulatory compliance

0% Other

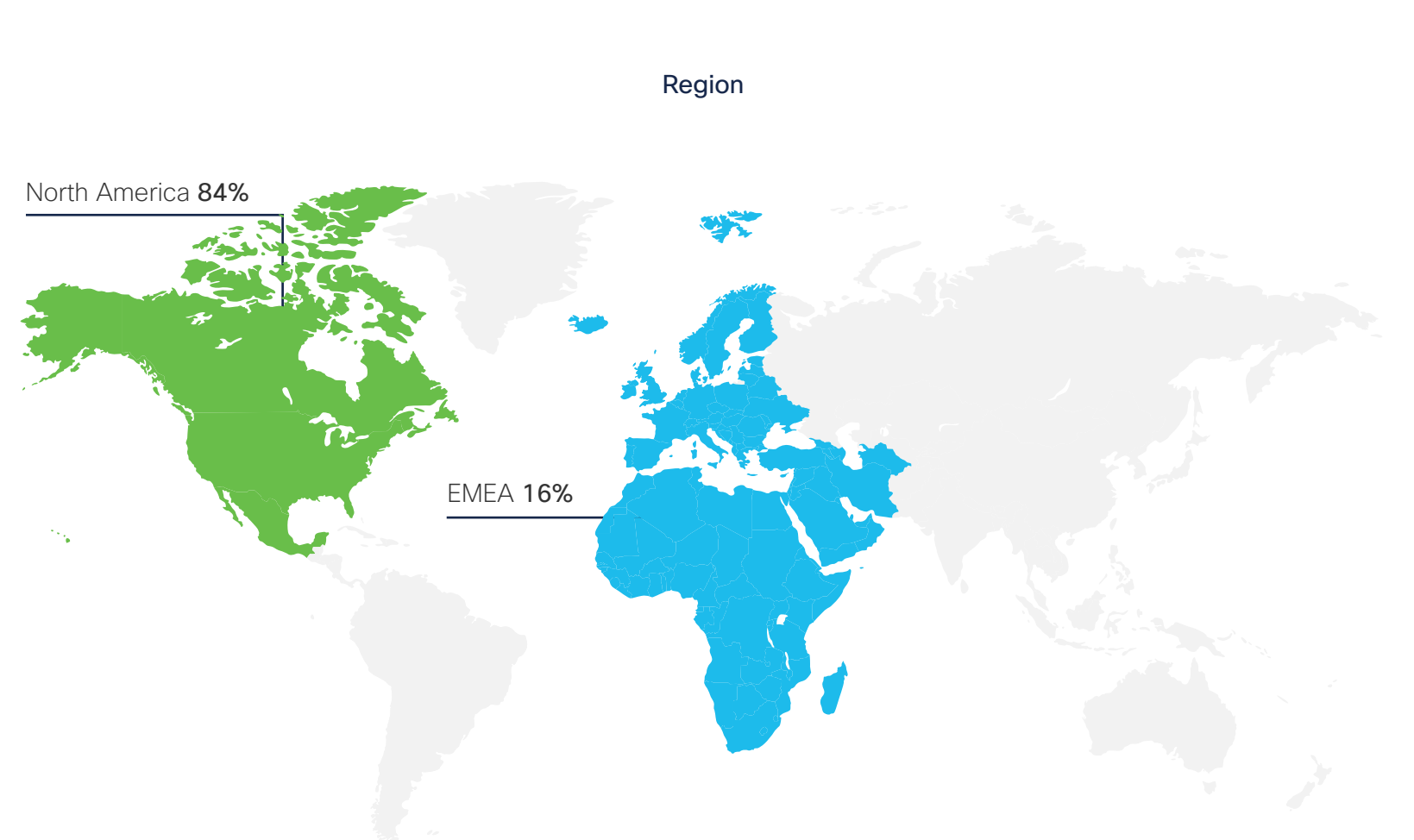
What are the biggest challenges that OT visibility can help your team address?

> "Our biggest challenge is to ensure data collection without putting the industrial control network at risk of outages."
>
> – Director, manufacturing industry, 10,000+ employees

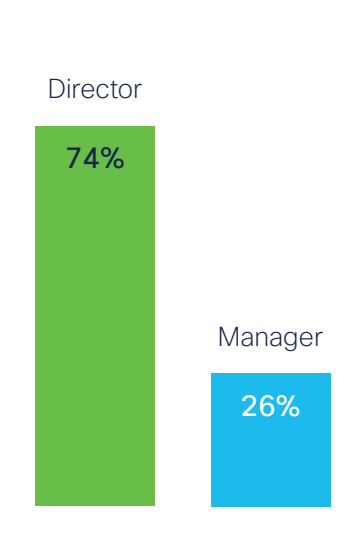
> "We're struggling securing remote locations and making sure it's to the standard and to the code."
>
> – Director, Electric Power Transmission & Distribution, 1,001 - 5,000 employees

Respondent breakdown

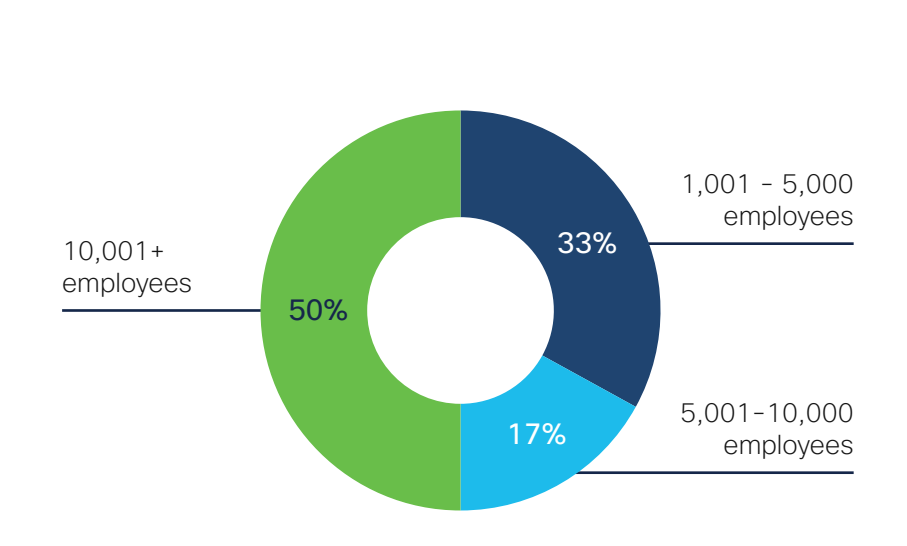
Region



Title



Company Size



Gartner

Source: Gartner Peer Insights, Cybersecurity in Operational Technology survey