REPORT

2025 State of Operational Technology and Cybersecurity Report

FORTINET

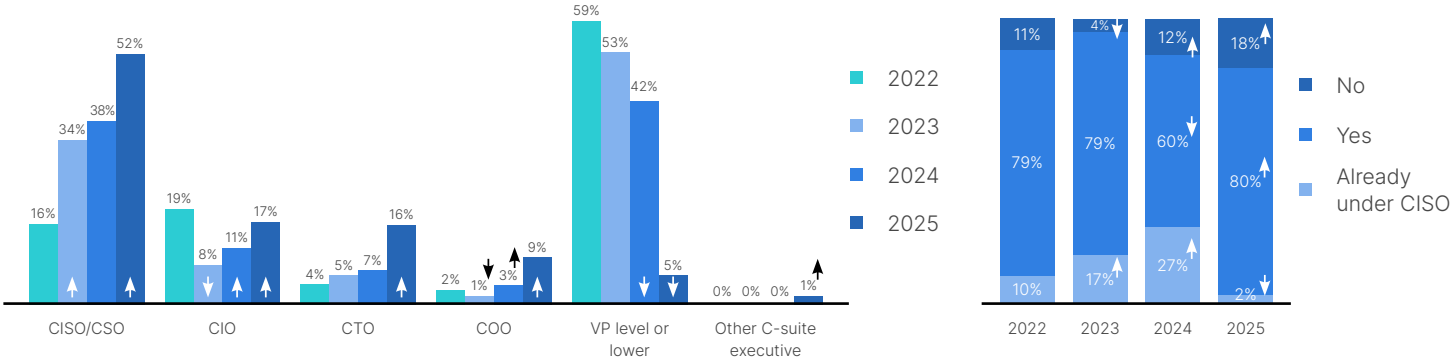
Table of Contents

Key Takeaways

People

An indication of increasing cybersecurity maturity is the global trend of corporations planning to integrate operational technology (OT) cybersecurity under the CISO, which increased again this year as part of an ongoing trend to consolidate OT responsibility within the C-suite. Now, more than half (52%) of organizations report that the CISO/CSO is responsible for OT, up from 18% in 2022.

According to the *Fortinet 2025 Threat Landscape Report*, nation-state actors continue actively using ransomware against manufacturing companies, the most targeted sector.[1] In this year's *State of Operational Technology and Cybersecurity Report*, increasing awareness of OT cyber risk within organizations continues to drive the assignment of that risk to an executive, most commonly the CISO. For four consecutive years, OT risk and assignment of the risk to C-suite continues to grow with the intention to move OT cybersecurity under CISO in the next 12 months, increasing from 60% to 80% in 2025.

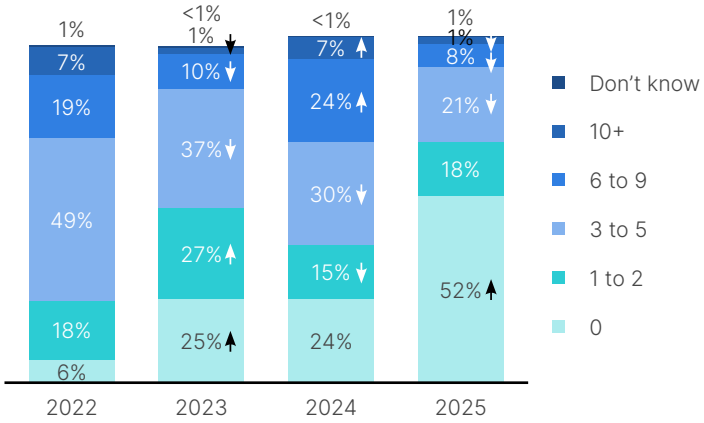


OT cybersecurity responsibility

Cybersecurity to be under CISO in the next 12 months

Cybersecurity incidents

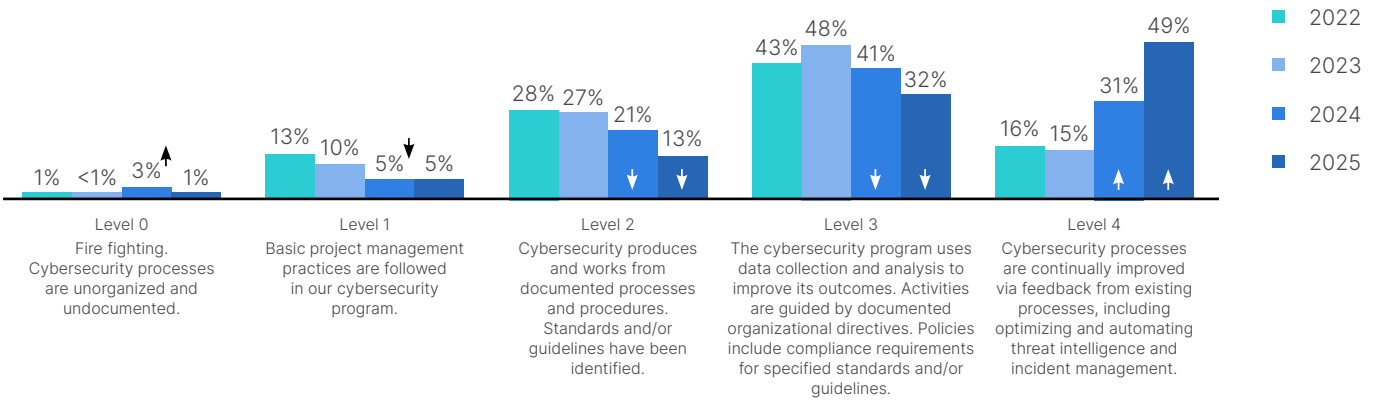
OT networks are quickly evolving as modernization and digitalization connect and enable the use of rich operational data to optimize operations. However, increasing connectivity also poses several risks. Criminal ransomware crews are targeting manufacturing as they monetize production interruptions and extract ransoms more effectively by preying upon a manufacturer's need to return to operations quickly. Additionally, well-funded, state-aligned, or state-sponsored threat actors are attempting to penetrate industry and critical infrastructure to lay the groundwork for future disruption or to cause immediate disruption as a political statement.



Number of intrusions in the past year

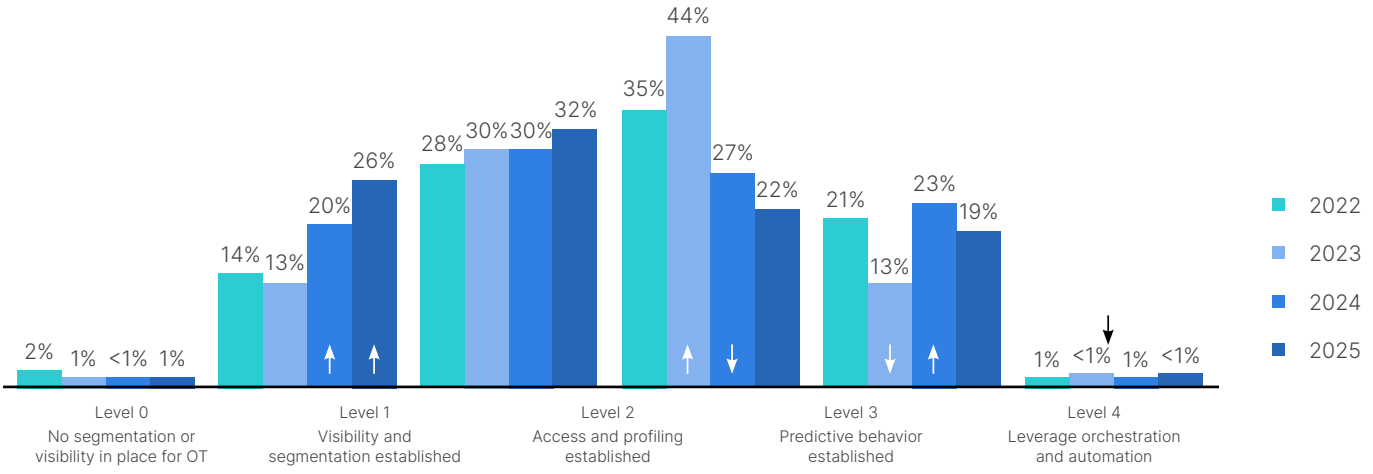
Growing maturity in OT cybersecurity processes and solutions

OT cybersecurity maturity shows signs of progress in both process and solution maturity. As process maturity is less intrusive and more administrative, it is quicker to mature, and nearly half of organizations (49%) state that their cybersecurity program's maturity is at Level 4, where processes are continuously improved through feedback on existing processes, including the incorporation of threat intelligence and incident management.



Maturity of cybersecurity program

Solution maturity involves solution selection and often proofs of concepts (POCs), so the maturation timeline is longer, but there are indications of solution maturity. After a few years of settling out and being properly recalibrated, solution maturity is progressing from Level 1 to 2. Companies are maturing past visibility and segmentation to incorporate user profiling and access management further. Although it shows promise, Level 2 is still the high point of solution maturity, with Levels 3 and 4 awaiting further investment.

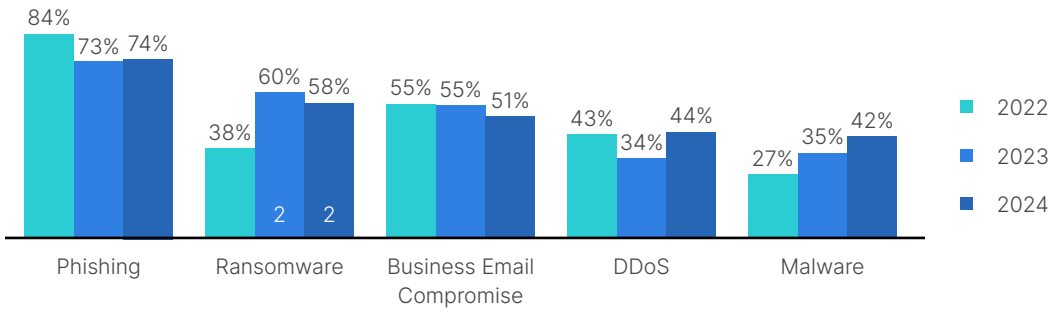


Maturity of OT security posture

As a positive sign of increasing maturity, organizations that had more than three intrusions declined and incidents seem to be decreasing overall. However, attacks are difficult to fully defend as 50% of survey respondents still experienced one or more incidents. Higher self-assessed maturity levels correlate to reduced intrusions, which suggests that security maturity is increasing and the adoption of robust OT security solutions is working, particularly for those organizations at the highest maturity levels.

The impact of intrusions

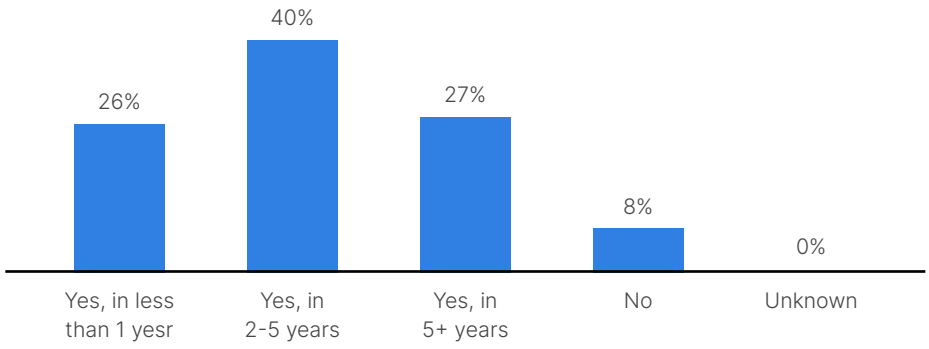
As organizations advance in their maturity level and adopt more advanced solutions, we see declines in most intrusion types. Compared to previous years, intrusions improved significantly, from 6% reporting no intrusions in 2022 to 52% in 2025. In fact, 65% of companies at maturity Level 4 reported zero intrusions compared to 46% within Levels 0–2. Those companies reporting a lower maturity level (0–2) experienced more phishing attacks, while ransomware and malware affected Level 3 and 4 organizations more frequently.



Intrusions experienced

How OT factors into cybersecurity

As organizations increase their maturity and take OT security more seriously, they are doing more to plan for changes in regulations and compliance. In 2025, the majority (66%) expect increased regulation in five years or less, with 40% of respondents expecting an increase in regulations and compliance requirements within two to five years and 26% anticipating it in less than one year.



Anticipated increase in regulation and compliance

Executive Summary

This year marks our seventh edition of the *Fortinet State of Operational Technology and Cybersecurity Report*. The 2025 study is based on comprehensive data from a global survey of more than 550 OT professionals conducted by a respected third-party research company.

This year's report indicates that in 2025, organizations are taking security more seriously, with 81% self-assessing their cybersecurity maturity level as 3 or 4. At this level, security activities and guidelines are documented, and at the highest level, security processes and tactics are also being improved through iterative feedback.

More mature organizations have implemented many of the best practices outlined in this report and are also working to consolidate vendors to reduce complexity and costs. Organizations at the highest levels often take a platform approach to OT cybersecurity with centralized management, threat intelligence, and security orchestration. This year, there has been a notable increase in the assignment of responsibility for OT risk to the C-suite, another indication that the importance of OT security to the organization is being elevated.

Those OT organizations with higher security maturity are also experiencing fewer incidents in 2025. There's a correlation between self-assessed maturity level and the ability to detect OT malware and other advanced threats. Most organizations continue to support a wide range of older OT devices and face security challenges because of the lack of patches. However, more mature organizations are taking advantage of advanced cybersecurity features such as threat intelligence feeds and virtual patching to mitigate some of the issues with older devices.

Introduction

Attacks on OT systems can compromise industrial processes, equipment, and critical infrastructure and potentially cause dire health and safety consequences. As bad actors increasingly target critical infrastructure, governments worldwide are working to strengthen cybersecurity regulations for OT and industrial control systems (ICS). These changes include stricter security directives, incident reporting requirements, and a focus on building resilience against cyber incidents.

Unfortunately, many sensitive OT systems are decades old and were originally designed to work in relative isolation. But now, as organizations continue to digitize their operations, the diminishing "air gap" between OT and corporate IT networks means OT infrastructure is subject to many of the threats that IT systems have traditionally faced. Many OT disruptions occur because of attacks on linked IT systems, such as ERP or procurement, that spread and exploit connected OT networks. At the extreme, several industrial companies in the midst of a cyberattack have halted production or operations out of an abundance of caution citing safety concerns.

Securing OT systems is a complex task, but as the *2025 State of Operational Technology and Cybersecurity Report* shows, organizations investing in cybersecurity are realizing tangible benefits.

Continuing risks to OT systems

Cybersecurity attacks are rising, and OT systems continue to be attractive targets for attackers. Effective protection requires constant vigilance and resource allocation. According to the World Economic Forum, escalating geopolitical tensions and the reliance on complex supply chains are leading to a challenging risk landscape.[2]

As organizations continue to digitize and adopt new technology, risks increase correspondingly. OT organizations also face new regulations, compliance burdens, and increasingly sophisticated threats as cybercriminals adopt new techniques that incorporate technology such as artificial intelligence (AI). The most recent *Fortinet Threat Landscape Report* states that AI-powered cybercrime is scaling rapidly. Threat actors are harnessing AI to enhance phishing realism and evading traditional security controls, making cyberattacks more effective and difficult to detect.[3]

The *Fortinet Threat Landscape Report* also notes that industries such as manufacturing, healthcare, and financial services are experiencing a surge in tailored cyberattacks, with adversaries deploying sector-specific exploitations. In fact, in 2024, the most targeted sector was manufacturing at 17% as both nation-state actors and Ransomware-as-a-Service (RaaS) cybercriminals continue to capitalize on vulnerabilities. FortiGuard Labs observed billions of attempts each month, revealing an intensified focus on mapping exposed services and OT/IoT protocols such as Modbus TCP.[4]

Protecting OT systems remains critical

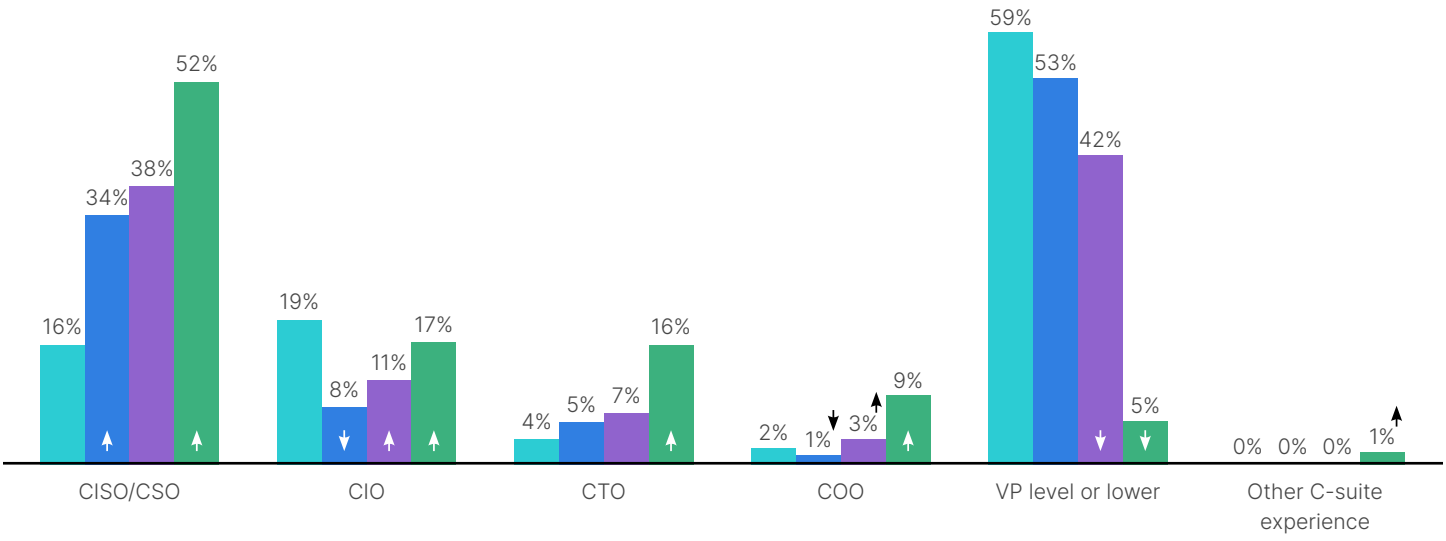
This year's *State of Operational Technology and Cybersecurity Report* indicates that those organizations that have invested in cybersecurity are making progress toward better protecting their sensitive OT systems. However, there is still more work to be done, and many organizations face significant risks from attacks such as phishing that can be relatively simple to curtail through basic cybersecurity hygiene and training.

The following critical insights, deep-dive trend analysis, and best practice recommendations can serve as a guide for making meaningful improvements to OT protections over the coming year.

Critical Insights for OT Security

Critical insight #1: Responsibility for OT security is elevating

There has been a significant increase in the global trend of corporations planning to integrate cybersecurity under the CISO. As accountability continues to shift into executive leadership, OT security is elevated to a high-profile issue at the board level. The top internal leaders that influence OT cybersecurity decisions are now most likely to be the CISO or CSO by an increasingly wide margin.



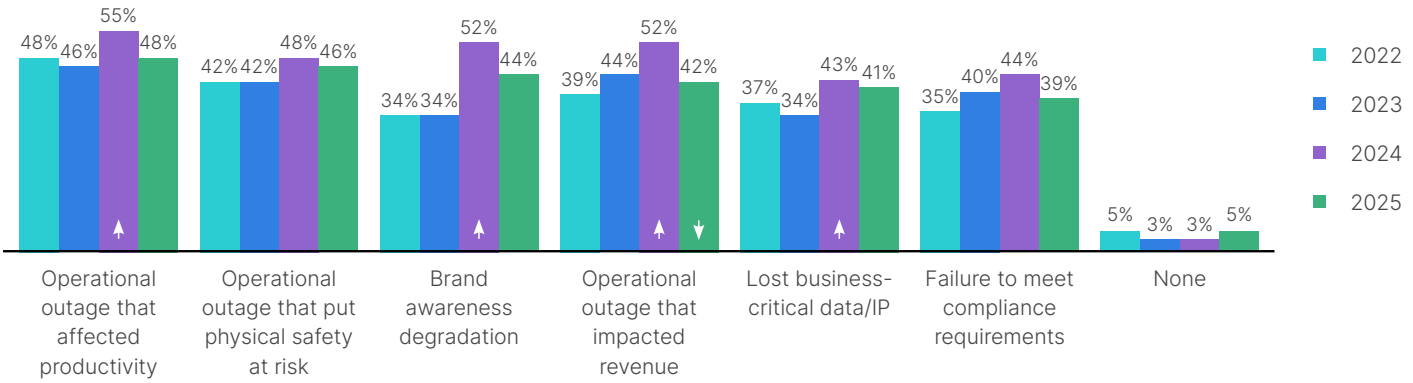
OT cybersecurity responsibility

Critical insight #2: OT cybersecurity is maturing

Self-reported OT security maturity has made notable progress this year. At the most basic level, 26% of organizations report establishing visibility and implementing segmentation, up from 20% in the previous year. Additionally, visibility and segmentation have increased compared to 2024. The largest number of organizations state their security maturity is at the access and profiling phase.

Interestingly, we see a correlation between maturity and attacks. Those organizations that report being more mature are seeing fewer attacks or indicate they can better handle lower-sophistication tactics, such as phishing. It's worth noting that some tactics, such as advanced persistent threats (APT) and OT malware, are difficult to detect, and less mature organizations may not have the security solutions in place to determine if they exist.

Overall, although nearly half of organizations experienced impacts, the impact of intrusions on organizations is declining, with a noteworthy reduction in operational outages that impacted revenue, which dropped from 52% to 42%.

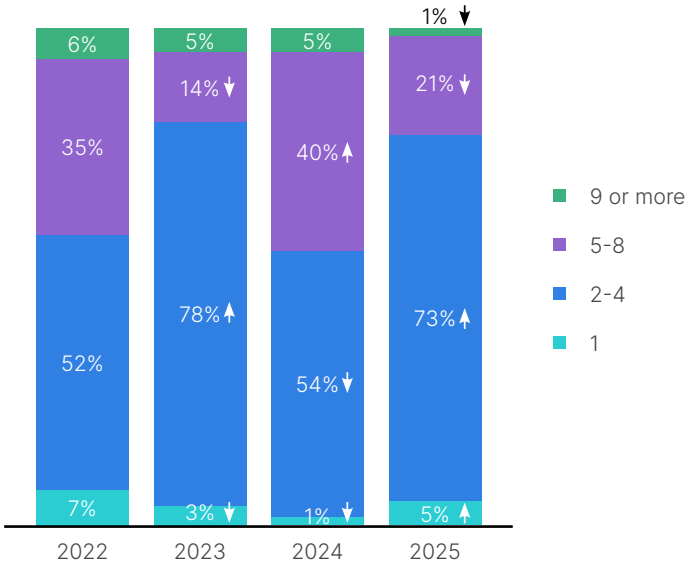


Impact on organization

Critical insight #3: Adopting cybersecurity best practices is having an impact

In addition to the maturity level affecting intrusions' impact, it appears that adopting best practices, such as implementing basic cyber hygiene and better training and awareness, is having a real impact, including a significant drop in business email compromise.

Other best practices include incorporating threat intelligence, which spiked (49%) since 2024, and a move to consolidate vendors. In 2025, we see a significant decrease in the number of OT device vendors, a sign of maturity and operational efficiency. More organizations (78%) are now using only one to four OT vendors, which indicates that many of these organizations are consolidating vendors as part of their best practices. Cybersecurity vendor consolidation is also a sign of maturity and corresponds to Fortinet customer experiences with our OT Security Platform. Unified networking and security at remote OT sites enhanced visibility and reduced cyber risks, leading to a 93% reduction in cyber incidents vs. a flat network. The simplified Fortinet solutions also led to a 7x improvement in performance through reductions in triage and setup.[5]

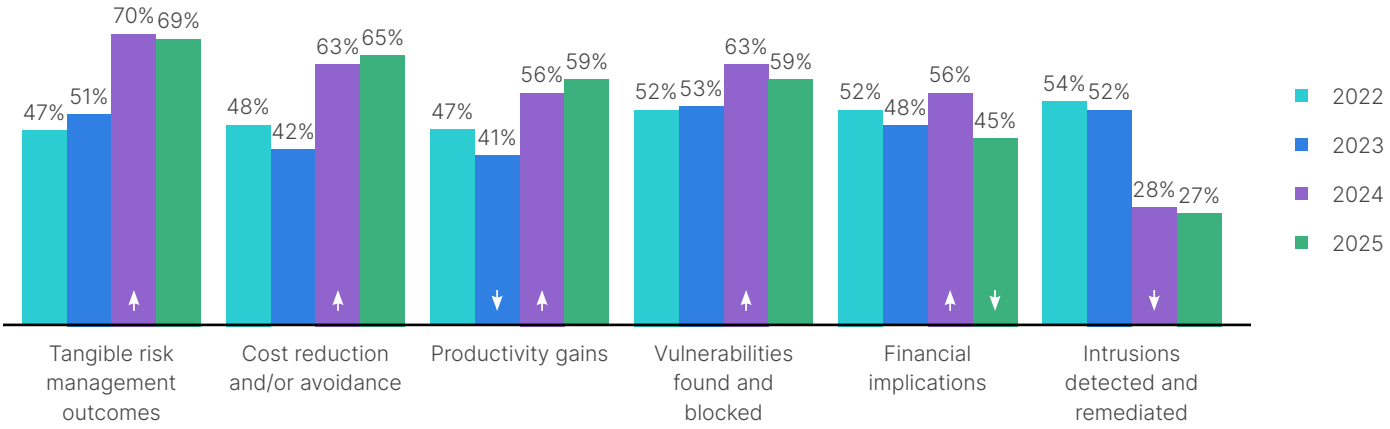


Vendors used for OT devices

A Deep Dive into the 2025 Survey

Q: What cybersecurity measurements do you track and report?

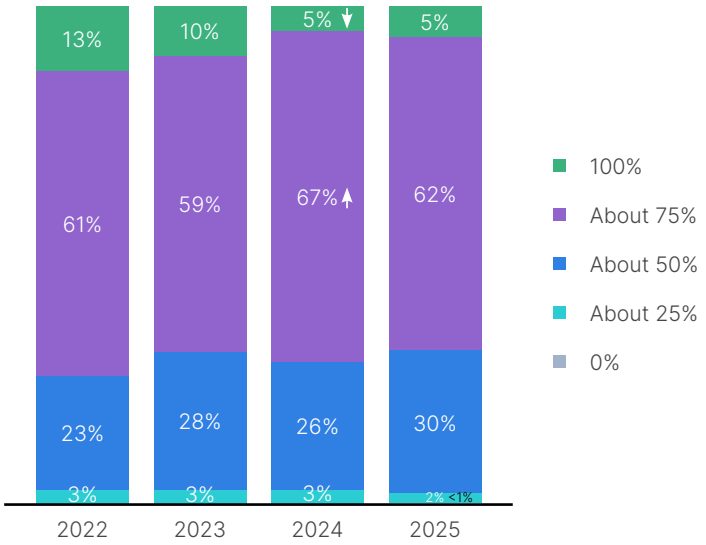
Cybersecurity metrics are mostly evenly tracked and reported by the survey respondents. Cost reduction and productivity gains have slightly increased from 2024, whereas financial implications had the only significant drop, from 56% to 45%. An overall increase in self-assessed maturity and adoption of more advanced OT security solutions appear to positively affect negative business impacts from intrusions. As OT teams conduct tabletop exercises and better understand operational contingencies to cyber events, along with proven restoration and recovery techniques, the impact of OT cyber events is mitigated.



Cybersecurity measurements tracked and reported

Q: What percentage of your OT systems are visible within your organization's central cybersecurity operations?

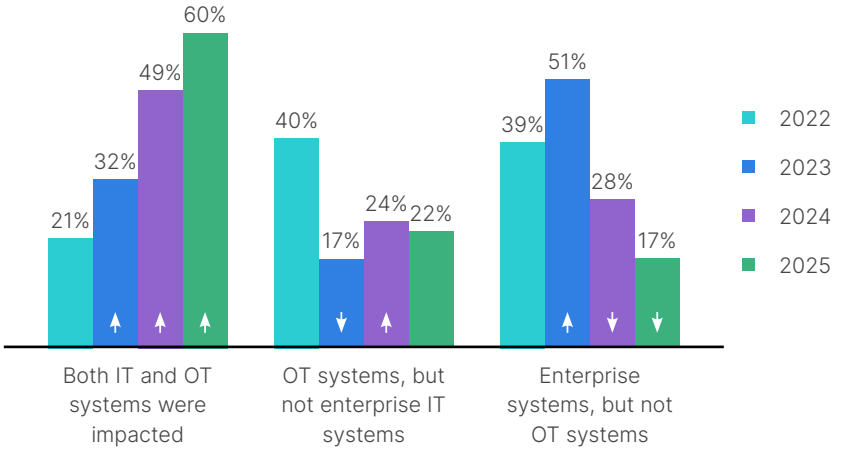
Since 2022, there has been a decrease in the proportion of OT teams claiming to have 100% visibility. As more security solutions are applied and combined IT and OT teams collaborate, there is also a decline in those identifying 75% visibility within the organization's central cybersecurity operations. This data indicates that as an organization advances in OT security maturity, it becomes more aware of blind spots in its asset visibility.



% of OT systems centrally visible

Q: Which of your environments have been impacted by cybersecurity intrusions in the past year?

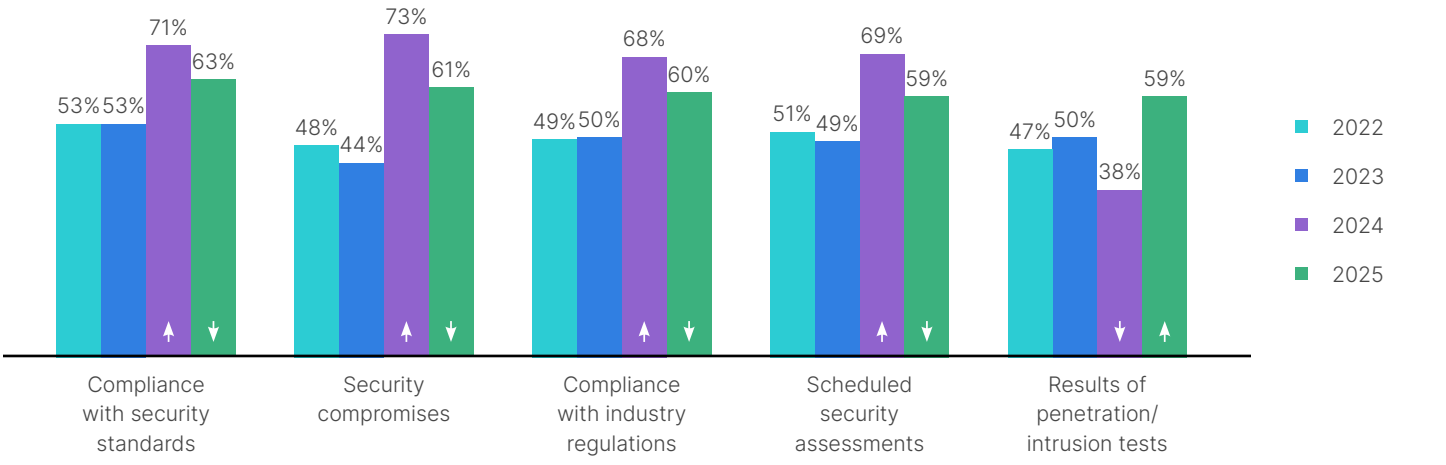
Intrusions are having a growing impact on both IT and OT systems. The trend of intrusions affecting OT systems in some way continues to rise. In 2024, 49% of respondents who experienced an intrusion saw impacts on both IT and OT systems, but this year, 60% of organizations reported that both were impacted. We also saw a slight decrease in intrusions that affected only OT systems (from 24% to 22%). Note that impacts on OT systems may be due to IT systems or connections being offline rather than an infection within the OT environment itself.



Environments impacted

Q: What OT cybersecurity issues are reported to senior and executive leadership?

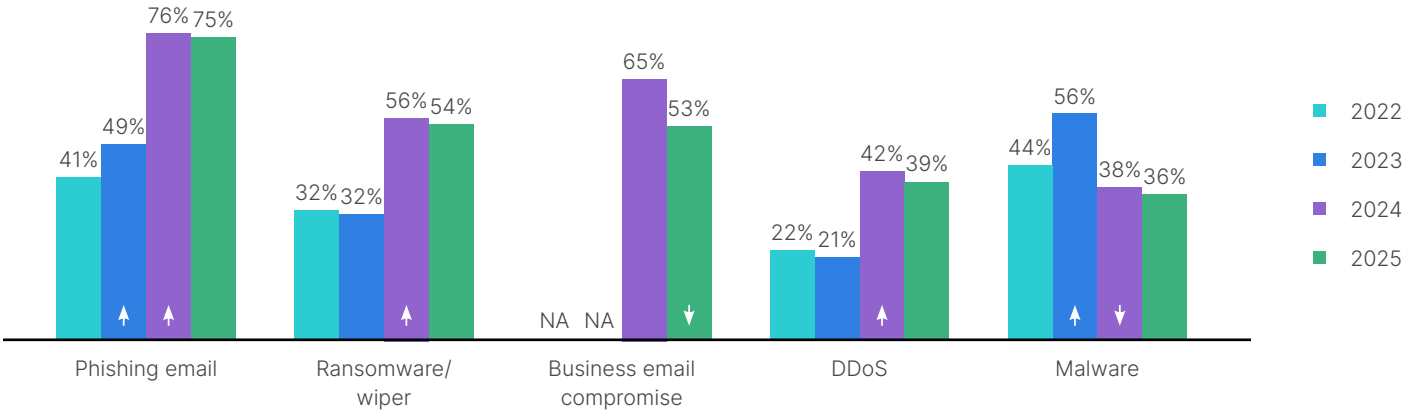
Aligning with the general finding of increasing maturity, reporting basic and routine cybersecurity events to senior leadership has declined compared to 2024. However, organizations increasingly report penetration and intrusion test results to senior leadership. This shift from reporting and compliance to more advanced penetration testing may reflect an increasing adoption of these advanced assessment capabilities.



Reported OT cybersecurity issues

Q: What types of intrusions were experienced?

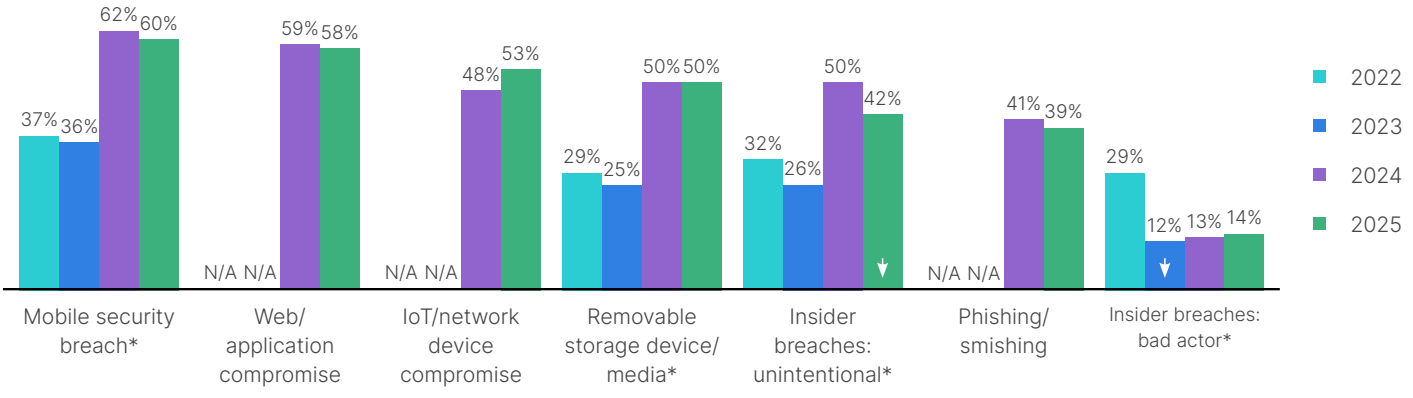
Unlike previous years, intrusions remained mostly stable, with a few small declines in tactics, such as phishing emails and DDoS attacks. Business email compromise was the only intrusion type with a sharp decline compared to 2024. It's encouraging that even with the increase in ransomware volume and the expansion of Ransomware-as-a-Service reported by FortiGuard Labs, ransomware and wipers remained steady.[6]



Intrusions experienced

Q: What techniques were involved in the intrusion?

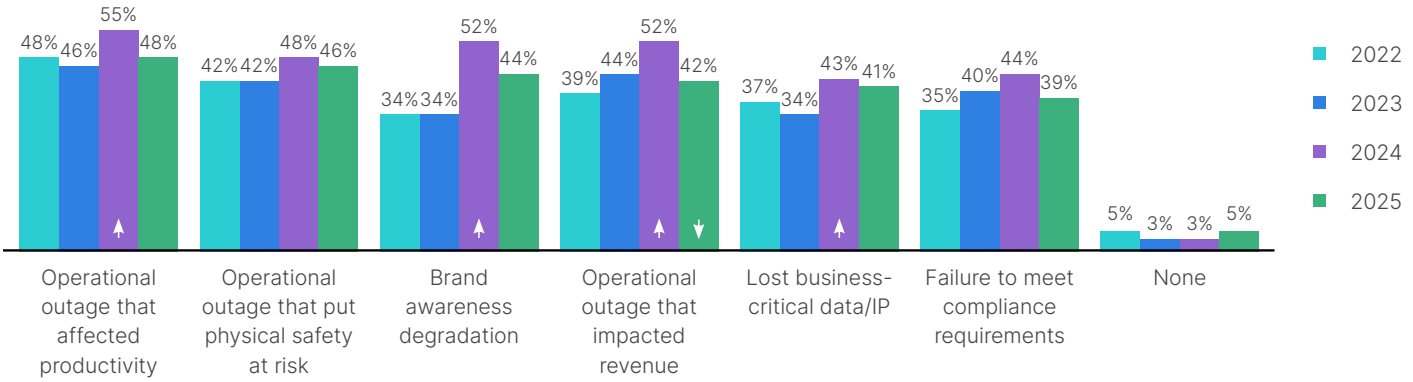
The overall involvement of the listed techniques has slightly decreased compared to last year, except for IoT and insider breaches. As of 2024, mobile security breaches and web compromises ranked highest, and the threat landscape is shifting toward mobile, web, IoT, and removable-media vectors. Although deliberate insider sabotage has receded over time, it is slowly creeping up again in 2025.



Techniques involved

Q: What impact did the intrusion(s) have on your organization?

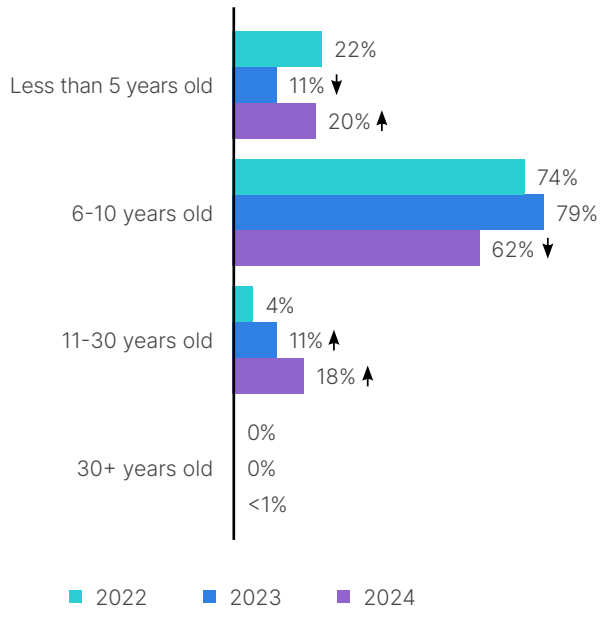
Although nearly half of organizations experienced impacts, the impact of intrusions on organizations is declining. The spikes we saw in 2024 in the degradation of brand awareness and operational outages that impacted revenue dropped significantly in 2025.



Impact on organization

Q: What is the age of your ICS system?

The number of ICS systems under five years old has increased, indicating a renewal of ICS systems. Although some systems would have moved into an older age bracket, the data indicates that organizations are working to refresh their systems as modernization continues. This investment in automation and refreshing technology is a positive trend. With that said, aging also continues, and most devices are at least six years old, so organizations need to turn to compensating controls and virtual patching as their systems continue to age.

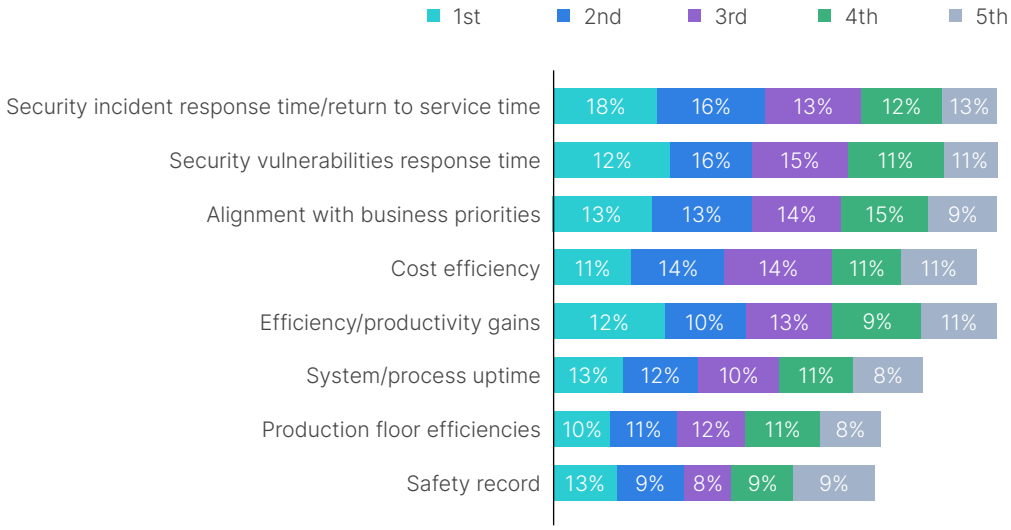


Average age of ICS systems

Global Impact

Q: How is your success measured? (rank up to five)

Organizations measure their success in several ways, but "response time to security incidents/return-to-service time" was the top answer overall, and nearly half (46%) of respondents ranked this as one of the top three success factors. It is the fourth year in a row that this response has ranked as one of the top three factors, and, notably, companies are measuring success based on recovery. It's also worth noting that security vulnerabilities response time is most commonly ranked number one (17%).



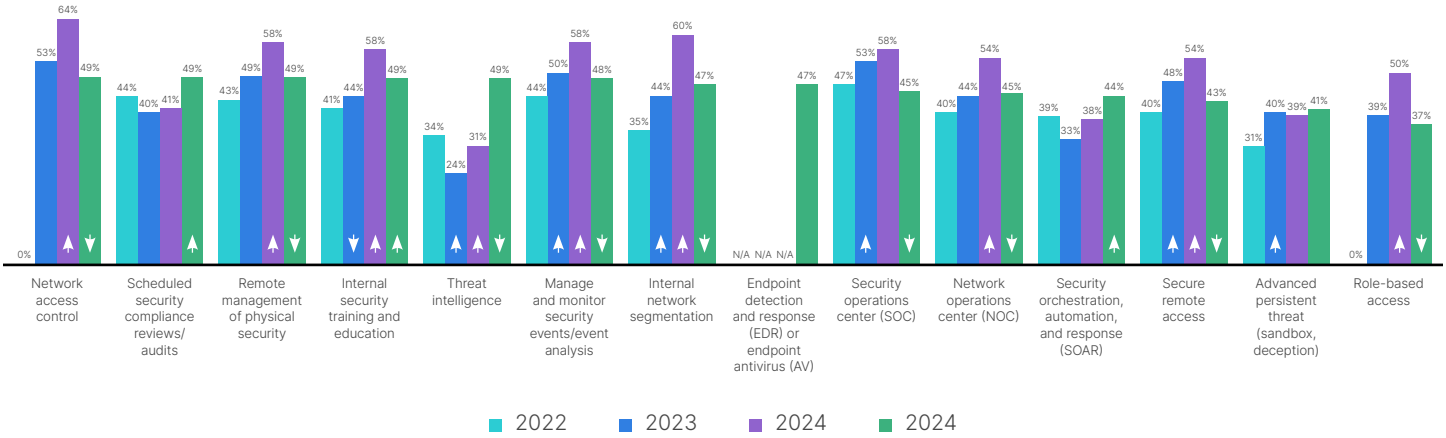
	2022	2023	2024	2025
Security incident response time/return to service time	35%	41%	46%	46%
Security vulnerabilities response time	33%	45% ↑	42%	43%
Alignment with business priorities	33%	36%	39%	42%
Cost efficiency	39%	35%	35%	41% ↑
Efficiency/productivity gains	43%	42%	40%	41%
System/process uptime	34%	36%	33%	34%
Production floor efficiencies	33%	31%	35%	27% ↓
Safety record	32%	27%	30%	25%

How success is measured (ranking)

Q: What cybersecurity and security features do you have in place today?

Although 2024 saw an increase in the cybersecurity measures and technologies in use, 2025 saw a year-over-year decrease in security features in a number of areas, such as network access control, internal network segmentation, and role-based access. It's possible that these decreases can be attributable to vendor and device consolidation by more mature organizations.

At the same time, threat intelligence has spiked (49%) since 2024, along with scheduled security audits and security orchestration. These shifts are another possible indication of increasing maturity levels. The spike in threat intelligence may be because it is generally incorporated into an OT security operations center. Security orchestration and sandboxing are also being prioritized, and they are other tools often used by more mature organizations. The increase in scheduled security audits from 41% to 49% indicates that organizations are getting more organized and prioritizing compliance.



Cybersecurity and security features in place

Best Practices

Based on this year's survey results, we've assembled the following best practices:

1. Deploy segmentation

Reducing intrusions requires a hardened OT environment with strong network policy controls at all access points. This kind of defensible OT architecture starts with creating network zones or segments. Standards such as ISA/IEC 62443 specifically call for segmentation to enforce controls between OT and IT networks and between OT systems.

Segmentation solutions also provide some visibility of key OT assets and network flows, allowing organizations to better understand and manage cyber risk in the newly established zones.

TIP: Implement a strategy for secure networking. By starting with segmentation, you initiate visibility of assets between zones that can support the need for asset inventory. Start with segmentation and then the basic steps of asset inventory. Next, consider more advanced controls such as OT threat protection and microsegmentation.

2. Enhance visibility and compensating controls for OT assets

Once segmentation and initial visibility are established, organizations can expand visibility within their OT networks to help quantify and manage OT cyber risk. Organizations can then take steps to protect key devices that may be vulnerable using compensating controls that are designed for sensitive OT devices. Capabilities such as protocol-aware network policies, system-to-system interaction analysis, and endpoint monitoring can detect and prevent compromise of vulnerable assets.

TIP: A combination of application-layer policies, OT vulnerability protections, and virtual patching can greatly reduce the exposure of vulnerable legacy systems.

3. Embrace OT-specific threat intelligence and security services

OT security depends on timely awareness and precise analytical insights about imminent risks. A platform-based security architecture should also apply threat intelligence for near-real-time protection against the latest threats, attack variants, and exposures. Organizations should ensure their threat intelligence and content sources include robust, OT-specific information in their feeds and services.

TIP: Your threat intelligence and security services should include specialized intrusion prevention system signatures designed to detect and block malicious traffic targeting OT applications and devices.

4. Integrate OT into security operations (SecOps) and incident response planning

Organizations should be maturing toward IT-OT SecOps. To get there, OT needs to be a specific consideration for SecOps and incident response plans, largely because of some of the distinctions between OT and IT environments, from unique device types to the broader consequences of an OT breach impacting critical operations.

One key step in this direction is to have playbooks that include your organization's OT environment. This kind of advanced preparation will foster better collaboration across IT, OT, and production teams to adequately assess cyber and production risks. It can also ensure that the CISO has proper awareness, prioritization, budget, and personnel allocations.

TIP: Security tools with effective machine learning capabilities can empower data aggregation and analysis to detect and respond more quickly to potential threats.

5. Consider a platform approach to your overall security architecture

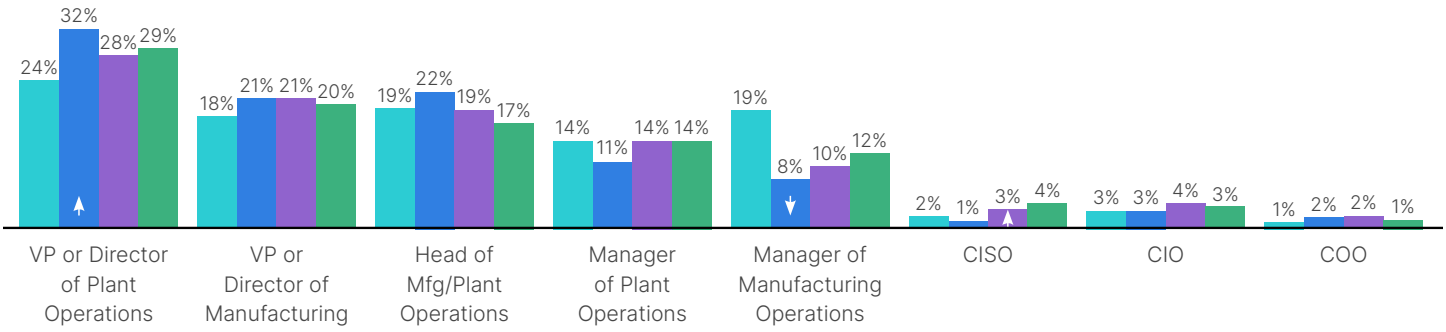
To address rapidly evolving OT threats and an expanding attack surface, many organizations have assembled a broad array of security solutions from different vendors. This has yielded an overly complex security architecture that inhibits visibility while placing an increased burden on limited security team resources.

A platform-based approach to security can help organizations consolidate vendors and simplify their architecture. A robust security platform with specific capabilities for both IT networks and OT environments can provide solution integration for improved security efficacy while enabling centralized management for enhanced efficiency. Integration can also provide a foundation for automated responses to threats.

TIP: Security platforms featuring context-aware generative AI capabilities can help organizations further strengthen their security posture and increase operational efficiency with automated tools like troubleshooting device vulnerabilities and threat hunting analysis.

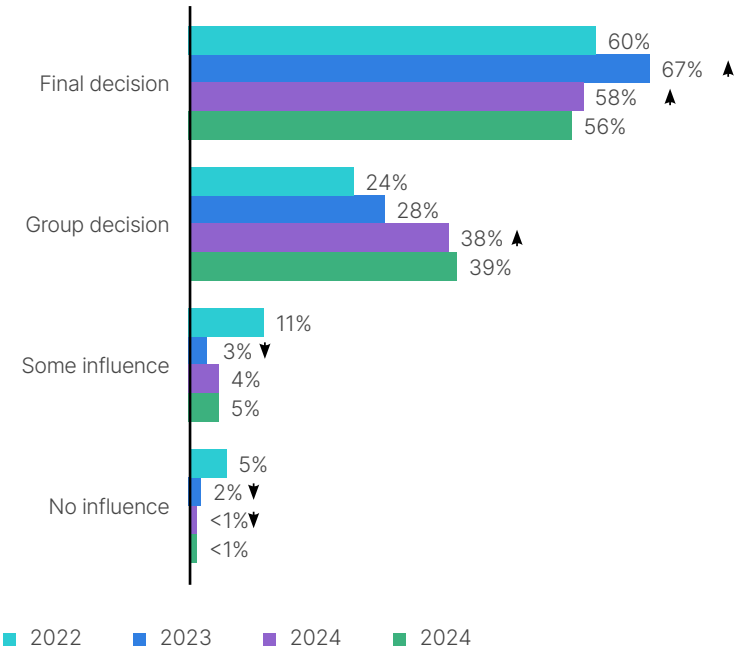
Methodology

Most survey respondents have “plant operations” or “manufacturing operations” titles, with more than one-quarter (29%) being vice presidents or directors of plant operations. No matter their title, most of those surveyed are deeply involved in cybersecurity purchase decisions.



Titles that best describe their roles

While more than half (56%) of these individuals still have the final say in OT purchase decisions, this year’s survey found that a rising number of organizations (39%, up from 28% in 2023) now make these decisions as a group.



OT purchase decision involvement

Study objectives

Fortinet retained InMoment, a third-party company with research expertise, to help us develop the persona of an OT professional. The survey they helped us create is intended to understand the following better:

- How the persona fits in organizations
- How security features are utilized
- How information is tracked and reported
- Influences and success factors

Approach

A panel sample was used to obtain 558 completes with the following respondent type:

- From a business in Energy/Utilities, Healthcare/Pharma, Transportation/Logistics, Manufacturing, Chemical/Petro-Chemical, Oil/Gas/Refining, or Water/Wastewater, with more than 1,000 employees
- Exception: More than 250 employees if in South Africa, UAE, Hong Kong, Singapore, Thailand, Philippines, Malaysia, Indonesia, Korea, or Israel

Other sample participation criteria included:

- Operations technology is within functional responsibility
- Has reporting responsibility for manufacturing or plant operations
- Involved in cybersecurity purchase decisions

Expanded to global reach since 2022

Survey respondents were from different locations around the world, including Australia, New Zealand, Argentina, Brazil, Canada, Mainland China, Colombia, Denmark, Egypt, France, Germany, Hong Kong, India, Indonesia, Israel, Italy, Japan, Malaysia, Mexico, Norway, Philippines, Poland, Portugal, Singapore, South Africa, South Korea, Spain, Sweden,* Taiwan, Thailand, UAE, UK, USA, Vietnam.

Year	2020	2021	2022	2023	2024	2025
Reach	NA	NA	Global	Global	Global	Global
Completes	100	100	520	570	558	558
Field Dates	4/14-4/16	2/24-2/25	3/14-3/18	2/28-3/1	3/7-3/13	3/3-3/4

Conclusion

OT is essential to businesses and governments around the world, including critical infrastructure, healthcare systems, and manufacturing operations. The indispensable nature of OT and ICS systems is precisely what puts them at elevated risk. Because many OT devices are 20 or even 30 years old, creating a secure OT environment has been extremely challenging for many organizations, but we're starting to see signs that more organizations are making progress, and their efforts are paying off.

As the *2025 State of Operational Technology and Cybersecurity Report* shows, more organizations are self-reporting higher security maturity levels compared to previous years, and intrusions have improved significantly. Although almost half of level 0–2 companies still see intrusions, more mature organizations are improving their numbers substantially. To continue this positive trend, everyone from the C-suite on down must commit to protecting sensitive OT systems and allocating the necessary resources to secure critical operations.

[1] Fortinet, 2025 Global Threat Landscape Report, May 1, 2025.

[2] World Economic Forum, Global Cybersecurity Outlook 2025, January 2025.

[3] Fortinet, 2025 Global Threat Landscape Report, May 1, 2025.

[4] Ibid.

[5] Fortinet, Fortinet OT Security Platform Customer Success Stories, November 5, 2024.

[6] Fortinet, 2025 Global Threat Landscape Report, May 1, 2025.

June 25, 2025 4:21 PM / MKTG-1383-0-0-EN