2026 State of Operational Technology and Cybersecurity Report

FORTINET

Table of Contents

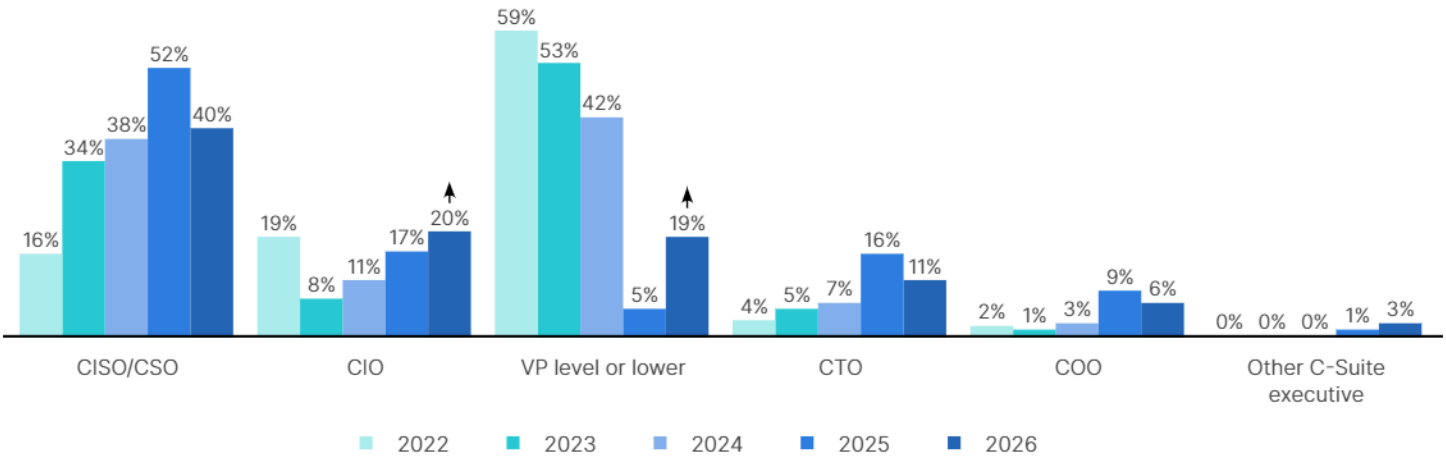
Key Takeaways	3
Executive Summary	7
Introduction	7
Critical Insights for OT Security	8
Best Practices	15
Conclusion	19

Key Takeaways

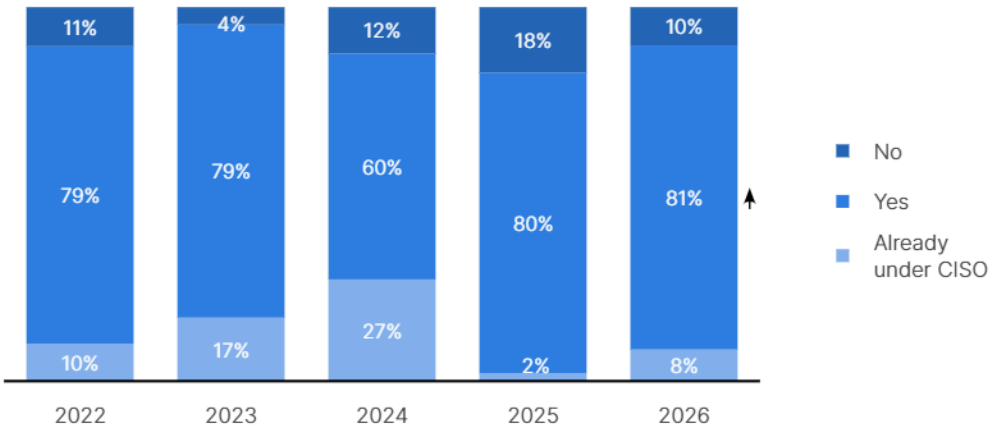
People

Over the past eight years, cybersecurity maturity has increased globally as organizations have integrated operational technology (OT) security under the chief information security officer (CISO) or other information security leadership roles such as the chief information officer (CIO). In 2026, 60% of respondents report that the CISO and CIO currently has ultimate responsibility for OT cybersecurity, down from 69% in 2025.

Signaling an increase in maturity, the C-suite has mitigated OT risk to the point of delegating OT cybersecurity responsibility back down to senior leadership roles. Those respondents who do not have elevated OT risk yet still need specialized knowledge and leadership to address the increasing number of sophisticated threats. For the fifth consecutive year, the number of respondents who intend to move OT cybersecurity under the CISO in the next 12 months increased from 80% in 2025 to 81% in 2026. These changes indicate a solidifying of the importance of OT risk ownership in the C-suite.



OT cybersecurity ownership



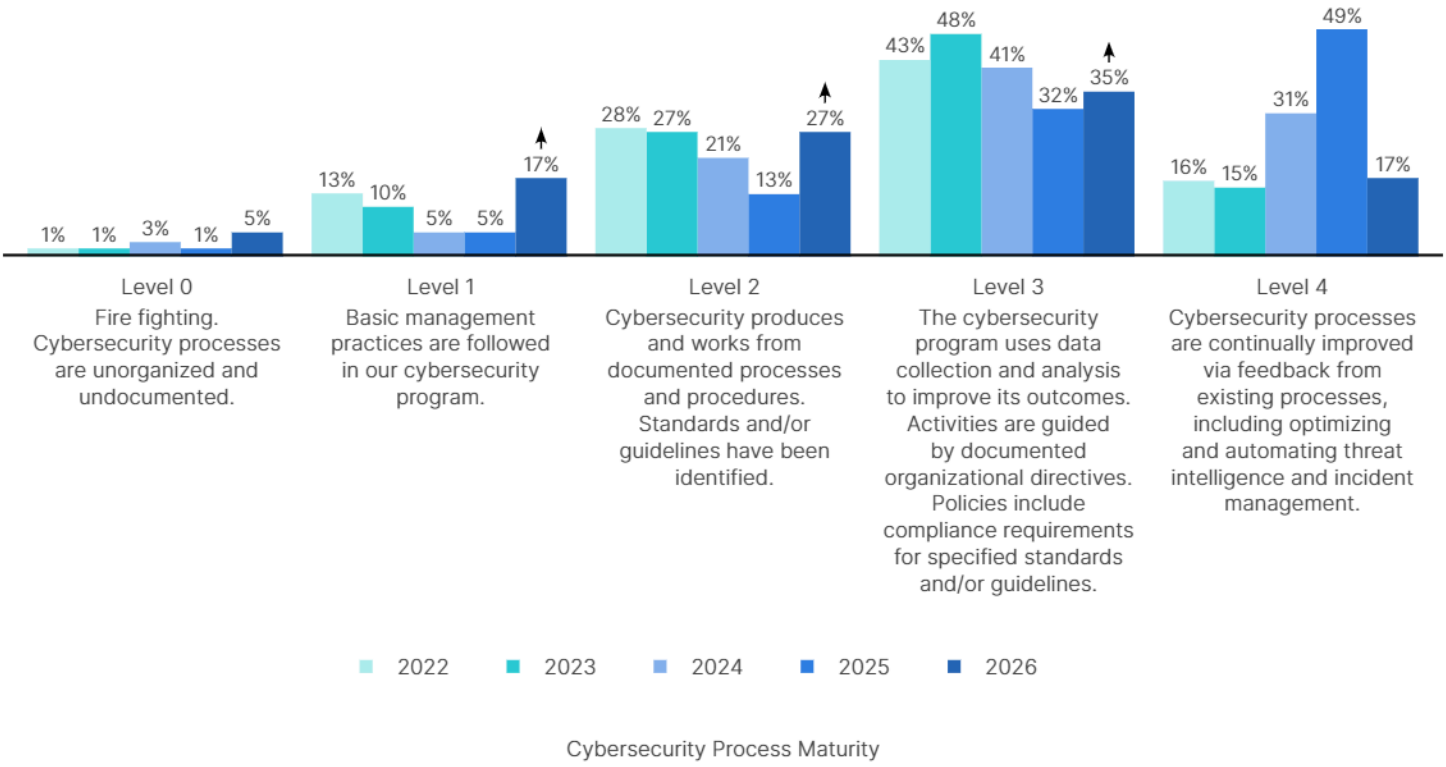
Planned CISO rollup

OT cybersecurity program, process, and solution maturity

In recent years, self-assessed program and process maturity was high with respondents reporting maturity levels of 3 and 4. Over time, as more resources and security solutions were introduced and IT teams and C-suite gained more oversight, it became apparent that the true maturity levels were actually much lower. Now the self-assessed process and security solution maturity levels have recalibrated as joint IT and OT security teams have received additional funding and deployed more solutions. Because of advanced OT security solutions, additional security experience, and more diverse teams, organizations have reevaluated their self-assessed levels. More OT security operators now realize where they are in terms of maturity and where their systems remain exposed, so they are implementing security basics such as improving asset visibility and access controls and implementing proper network segmentation.

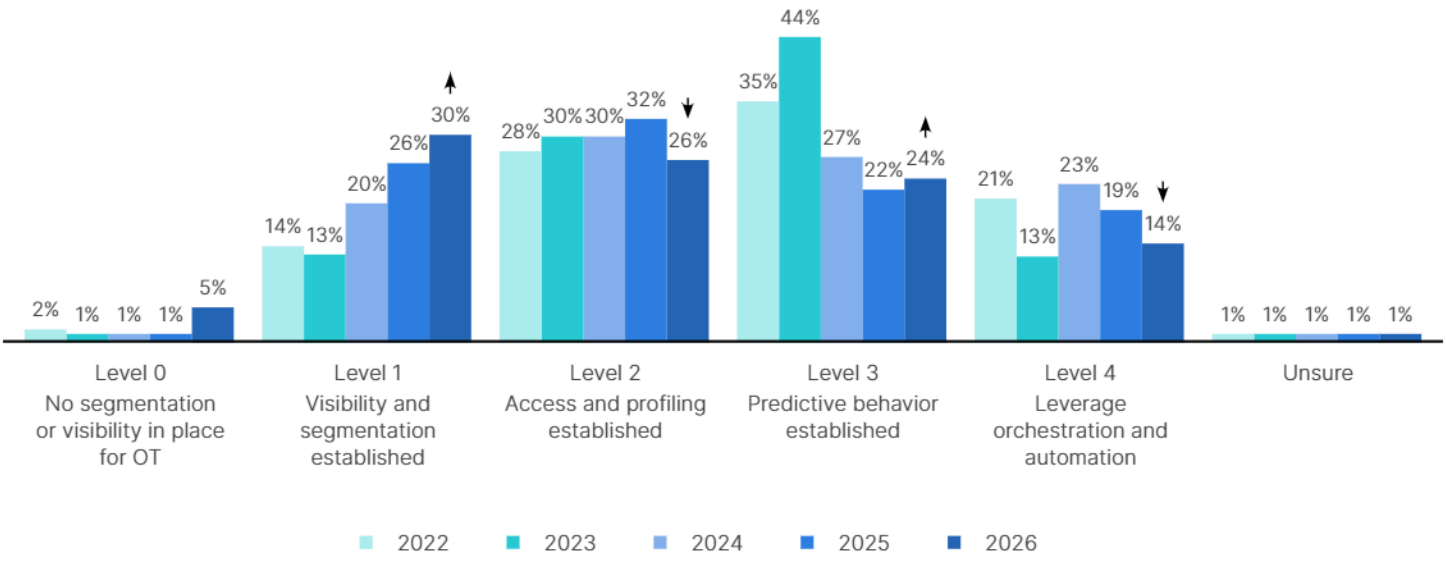
Regarding Process Maturity, many respondents in levels 1 and 2 report they are still in firefighting mode. Only a minority of respondents are at level 4 and truly mature in their security approaches. Respondents at level 0 struggle with a lack of documentation and core processes, increasing from 1% in 2025 to 5% in 2026. The level 1 and level 2 figures also increased sharply this year over 2025, from 5% to 17%, and 13% to 27%, respectively.

Level 3 respondents are relatively sophisticated, increasing modestly year-over-year (YoY). Advanced enterprises at level 4 declined sharply from 49% to 17%. This reassessment is a positive sign, signaling that OT security teams are more diverse, more experienced, better funded, and have implemented new security solutions that have revealed previously unknown security gaps.



Cybersecurity Process Maturity

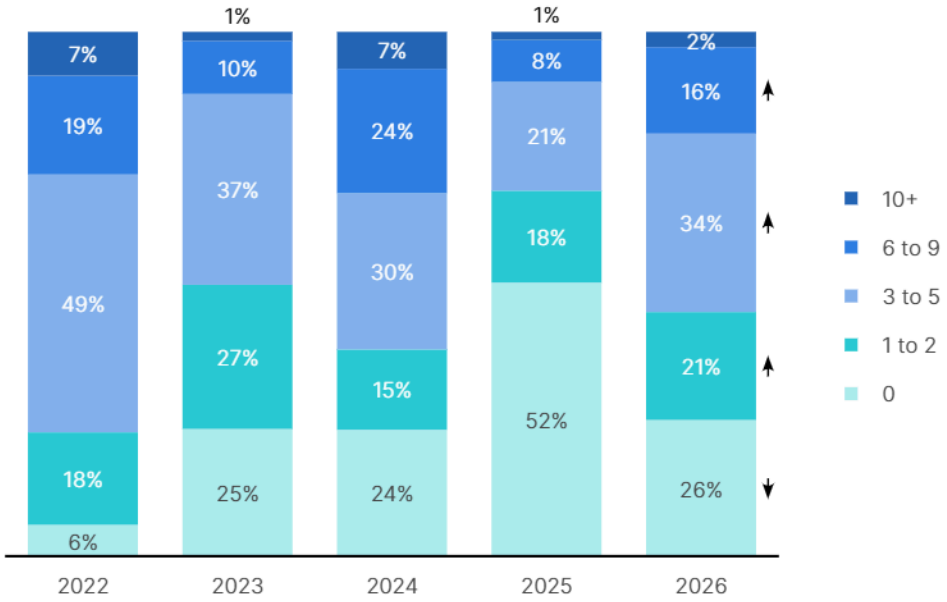
Solution maturity presents a similar picture. Level 4 respondents decreased YoY (19% to 14%), although level 3 was up slightly at 24% versus 22% in 2025. Level 0 and level 1 categories were up notably from 1 to 5% and 26 to 30%, respectively. These less mature companies are exposed and must move quickly to avoid falling victim to new and emerging threats.



Change title to read OT cybersecurity Solution maturity

Cybersecurity incidents

A positive indicator of increasing cybersecurity maturity is that teams are now reporting greater visibility of intrusions as opposed to reporting none. In this year's report, the declining numbers of respondents saying they had detected zero intrusions may point to a greater ability to detect intrusions rather than a real decline in the volume of successful attacks. At the top end, organizations that have had more than 10 intrusions in the year stayed steady at just 2%. However, the numbers of respondents reporting multiple attacks (one to nine incidents) have increased from previous years totaling 71%, up from 47%.



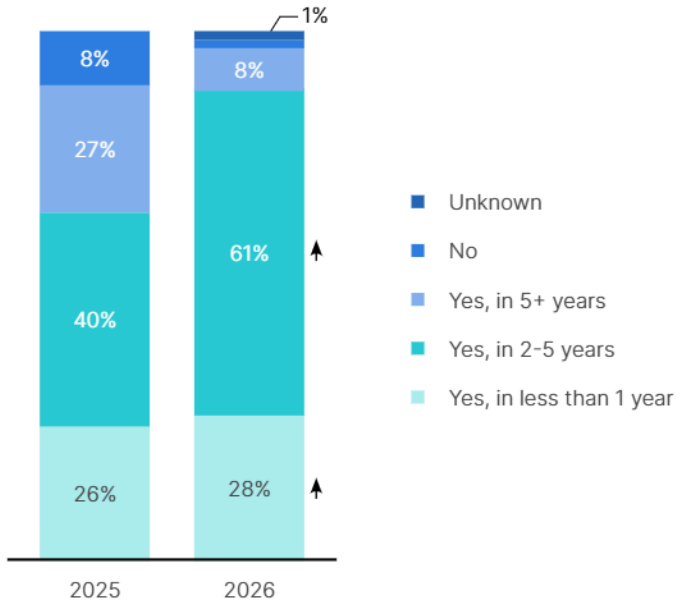
Number of intrusions

More regulations are expected sooner

Laws, regulations, and compliance mandates continue to be challenges for IT and OT leaders. Increasingly, these leaders want to get ahead of governance cycles and learn about potential pending rule changes that may impact data protection, cybersecurity, health, safety, and other factors.

Last year, some respondents expected new regulations in a few years, but now the vast majority of respondents predict new regulations will be coming soon. These new regulations will increase cybersecurity demands but also will improve network reliability and resilience.

In 2026, almost nine out of 10 respondents (89%) expect increased regulation in five years or less. This number is up sharply from 66% in 2025. Regarding timing, there was a 20-point shift in respondents now anticipating new regulations in two to five years as opposed to five+ years, suggesting that respondents want to prepare for IT and OT regulatory compliance challenges as they relate to cybersecurity.



Anticipated regulations increase

Executive Summary

This year marks our eighth edition of the *Fortinet State of Operational Technology and Cybersecurity Report*. The 2026 study is based on comprehensive data from a global survey of more than 700 OT-related professionals conducted by a respected third-party research company.

This year's report indicates that in 2026, organizations are taking OT security seriously, but they still have work to do. A minority of survey respondents have ensured they have the processes and tools in place to address the wave of cybersecurity attacks, threatening to bring their operations to a halt.

Many other respondents are taking sensible steps to meet regulations and repel attackers. They are responsibly documenting and reporting their actions and have senior people involved in strategic decisions to defend their operations. But security gaps remain, and a number of respondents admit that they are still in reactive, fire-fighting mode.

Organizations with the highest security maturity have implemented the best practices, suggested at the end of this report and consolidated vendors to manage complexity and costs. Many of these organizations have taken an integrated platform approach to OT cybersecurity with centralized management, threat intelligence, and security orchestration.

These organizations often turn to the C-suite for leadership rather than relying on specialists alone. This year, responsibility continues to move to the CISO and other executives as risk is better understood, funded, and redistributed. We've also seen a level of OT security maturity for certain organizations where OT risk is being mitigated and delegated to the VP level.

Those OT organizations with higher security maturity also are likely to experience fewer incidents in 2026. Enterprises are increasingly taking the opportunity to modernize their industrial control systems (ICS), which will improve their defenses. Organizations employing integrated OT security platforms for greater holistic defense also are likely to have fewer incidents.

The always-on nature of many OT organizations has created a rapid increase in connected devices, applications, and users that need to be secured. One of the greatest challenges in OT security is understanding the complex nature of business and operational systems that can impact production or reliability of critical infrastructure.

Introduction

Attacks on OT systems can slow down or topple core industrial processes, equipment, and critical infrastructure, potentially leading to human health and safety risks. Attacks also can lead to brand damage, penalties, reduced income, and loss of intellectual property (IP). As malicious actors increasingly target key operational sites and critical infrastructure, industry and governments worldwide are working to strengthen cybersecurity regulations, resilience requirements, and incident reporting rules for OT and ICS.

However, many OT systems are decades old, and the environments they were designed for were never meant to be connected to the Internet. Today, as organizations continue to digitize and transform their operations, OT and IT threats are inextricably linked. Connecting OT, IT, and cloud systems to align operations, infrastructure, and analytics can introduce serious cybersecurity challenges.

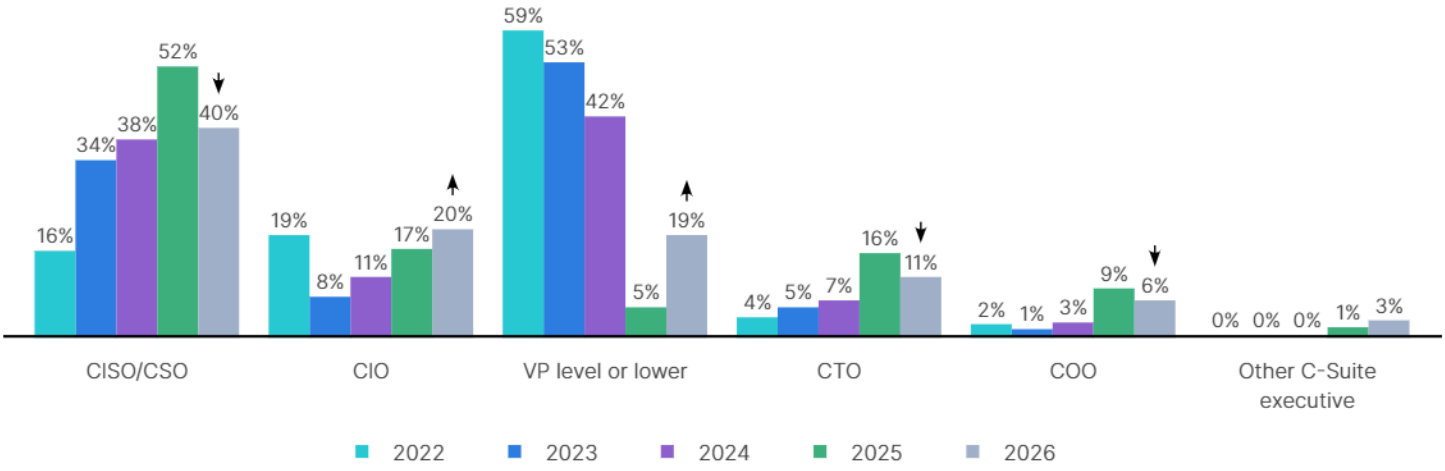
Securing OT networks isn't easy and today's rapidly evolving threat landscape requires vigilance. However, as this year's *State of Operational Technology and Cybersecurity Report* shows, organizations are tackling multiple challenges and improving their overall security posture by re-evaluating and appropriately assessing OT cybersecurity process and solution maturity.

Cybersecurity attacks are increasing and attackers continue to expand their capabilities. And now because of increased nation-state conflicts and geopolitics, OT systems are an appealing target for attackers seeking to disrupt operations to make a political statement or contribute to military operations. Protecting OT systems requires modern tools, diligent monitoring, and appropriate budgeting and resource allocation.

Critical Insights for OT Security

Critical insight #1: Responsibility for OT security remains in the C-suite

Cybersecurity is a board-level issue spanning virtually all industries, but OT security is equally important. The role of the CISO has become more visible in recent years, but in 2026, cybersecurity responsibility often extends to non-technical VP and C-suite executives.

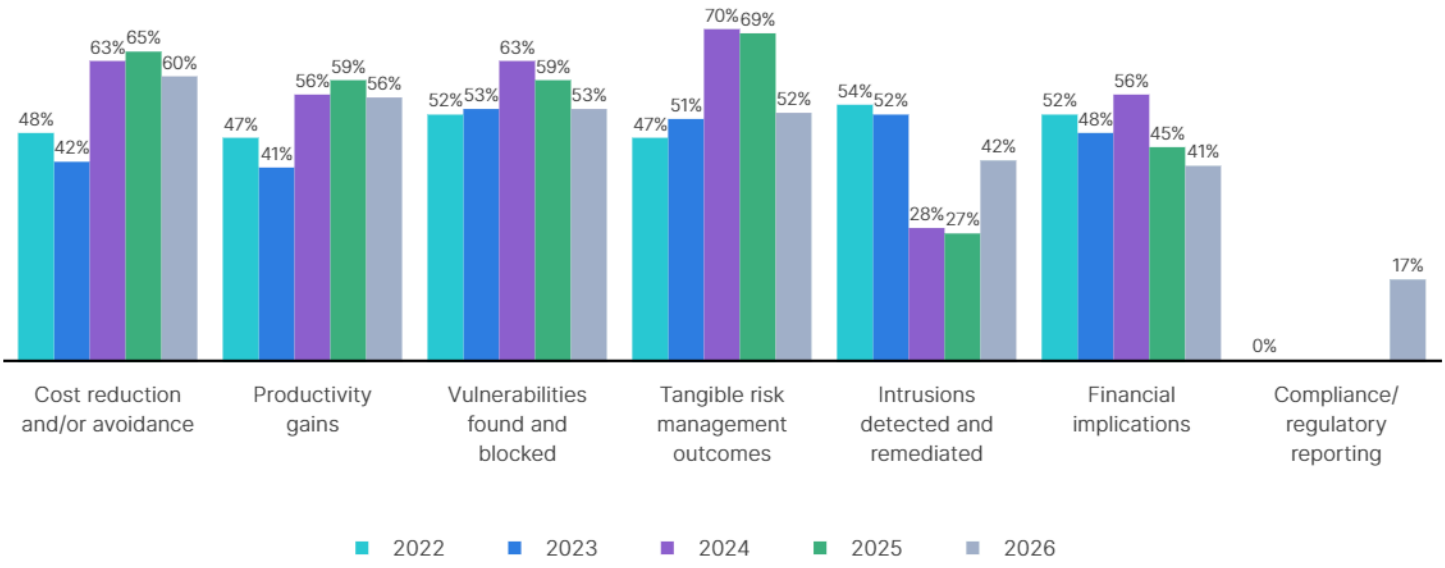


OT cybersecurity ownership

Critical insight #2: Buyers are focusing on cost constraints

The 2026 report suggests that buyers are tightening their belts. Although value is important, the need to keep operations secure and performing well when cybersecurity risks are high remains critical.

Cost reduction and avoidance was the number one cybersecurity measurement tracked and reported for 2026, rising from second place last year. More organization expect new regulations, leading to an increase in Compliance/Regulatory Reporting (17%).

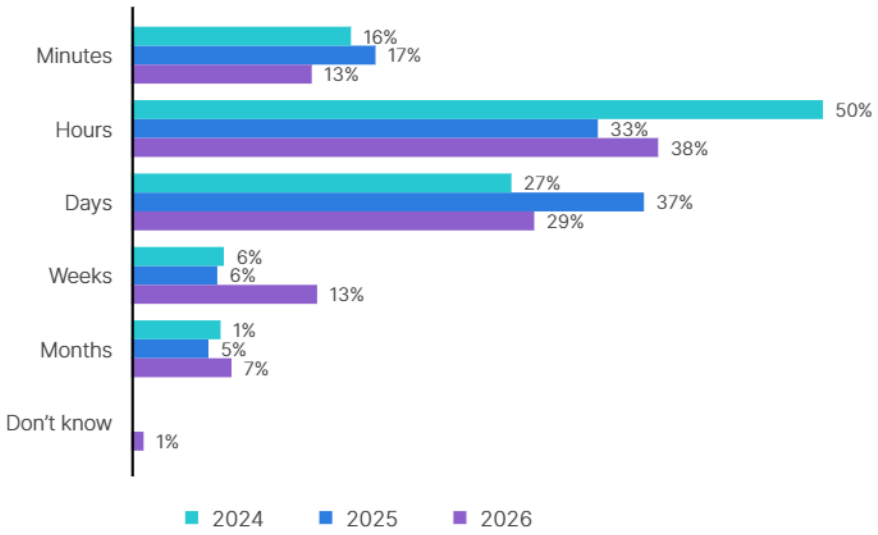


Cybersecurity metrics

Critical Insight #3: Dwell time numbers are up

Attacker dwell time measures how long attackers spend undetected. This critical key performance indicator (KPI) also often reflects how much damage attackers can inflict because it's easier for attackers to perform malicious tasks before they're detected.

Our survey suggests that although there is some flattening of dwell times of minutes, hours or days, attacks with longer dwell times of weeks, or even months, have increased. These long dwell times leave enterprises open to surveillance, loss of IP, and increase the risk of a ransom event or physical disruption.



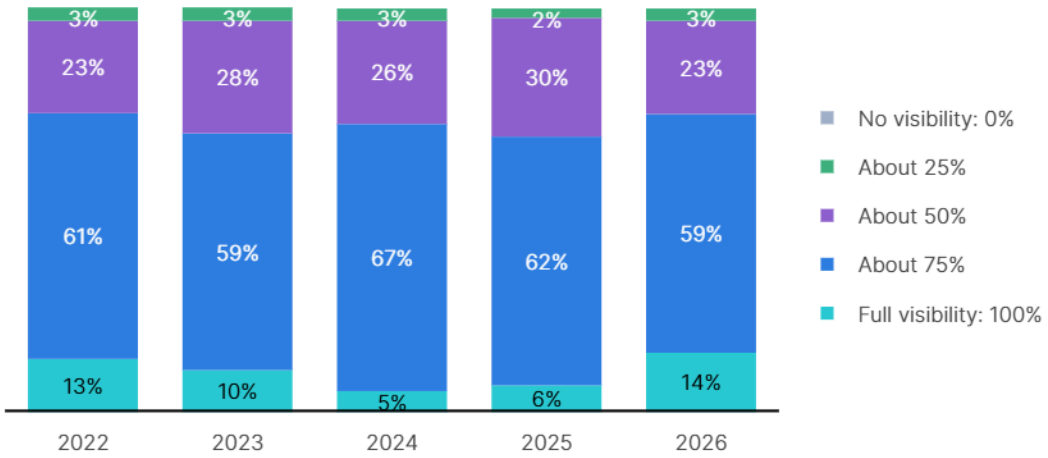
Anticipated regulations increase

A Deep Dive into the 2026 Survey

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

Although most OT environments are visible to security teams, 23% of respondents say they only have visibility into about half of their network, potentially leading to vulnerabilities related to siloed information, lack of awareness, monitoring challenges.

Notably in 2026, the number of respondents reporting that they have 100% visibility into OT systems has grown from 5% in 2025 to 14%, signaling growing confidence in comprehensive network visibility.

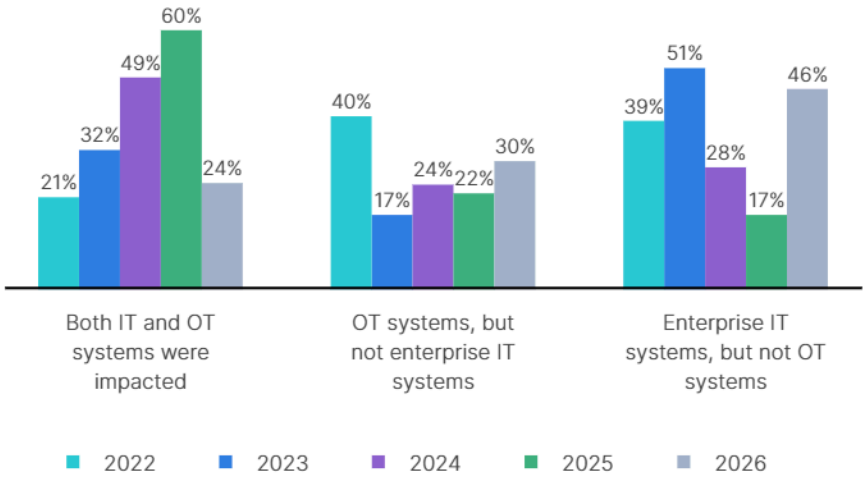


OT systems visibility

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, but respondents may be becoming better able to address the impact of intrusions.

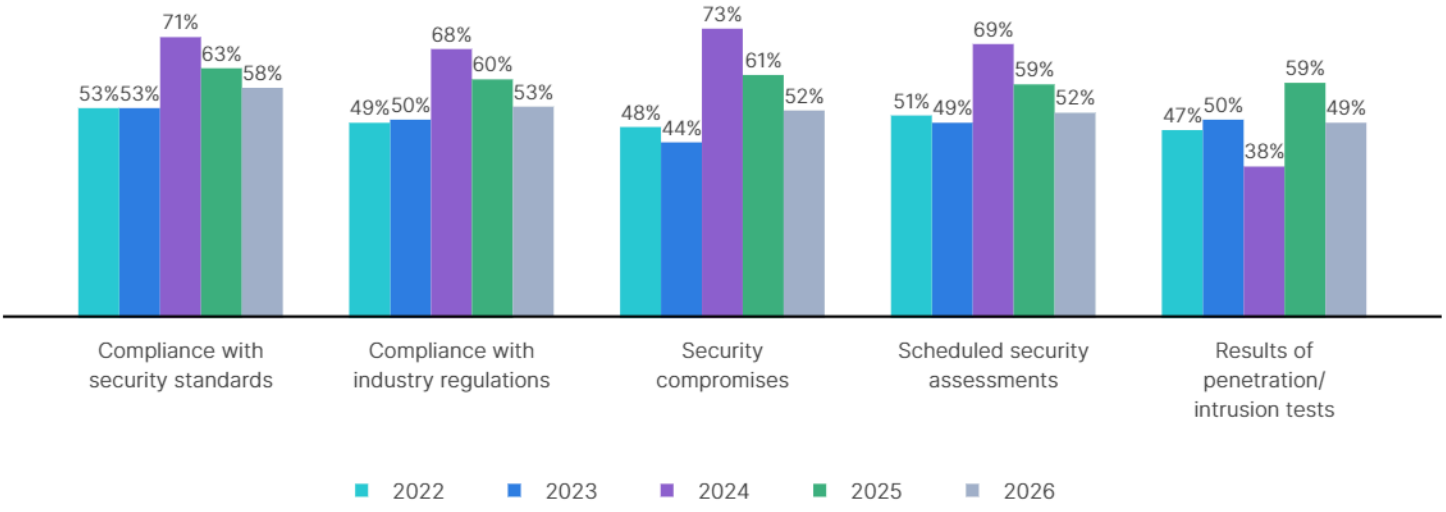
It's likely that segmentation between IT and OT systems is being deployed because less than a quarter of respondents (24%) said both OT and IT systems were affected by intrusions, a significant drop from 2025 (60%) and the lowest figure since 2022.



Impacted environments

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

Reporting routine cybersecurity events to senior leadership is performed by about half of respondents, but 53% fail to refer reports on compliance with current or pending regulations, a drop from 60% in 2025.



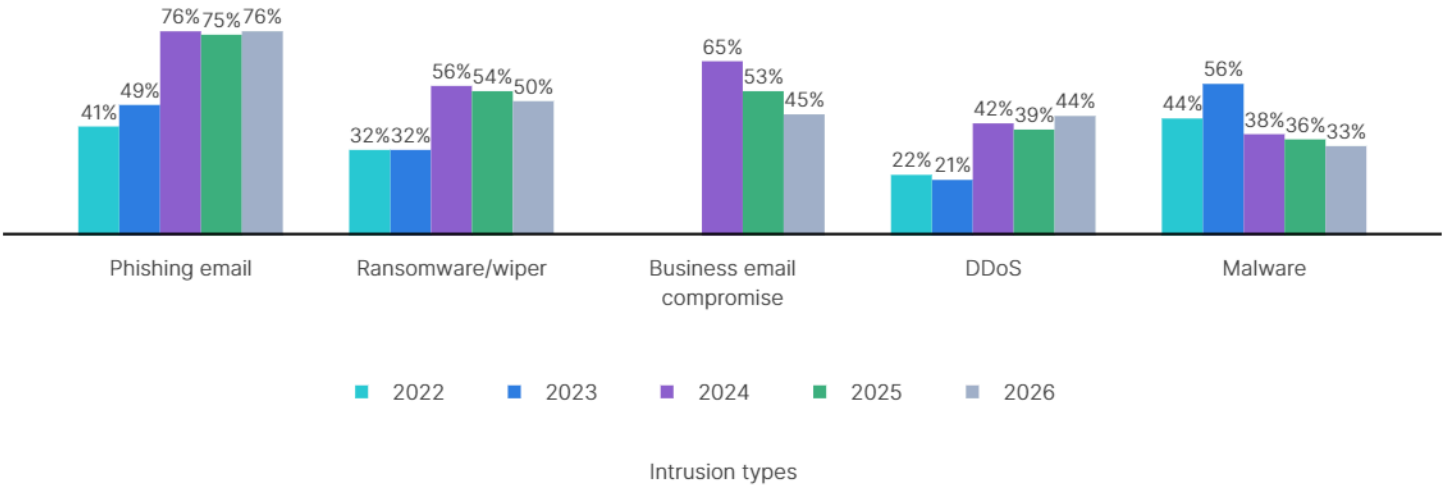
Escalated/reported issues

Q: What types of intrusions were experienced?

The types of intrusions respondents reported remained stable, with phishing emails at 76% and ransomware at 50%. Ransomware dropped marginally to 50% from 54% in 2025 but remains a major issue because of the potential for it to inflict significant damage.

As more enterprises digitize operations to better monitor and measure actions, OT networks are becoming more prevalent, strategic, and sophisticated. However, this increase in connectivity also raises the opportunities, scale, and seriousness of attacks.

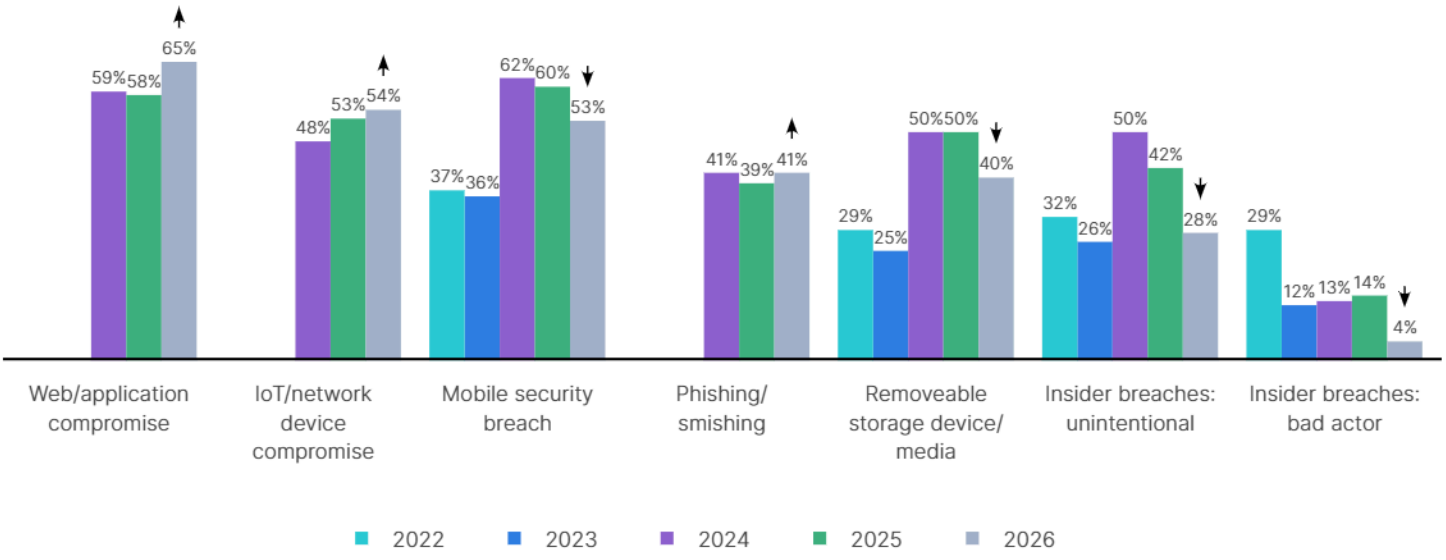
Ransomware attacks are often planned by highly organized groups, generally targeting the most sensitive enterprise vulnerabilities, which often include operations and OT systems. A disruption to performance and operations can be devastating, and state-sponsored actors represent another frightening challenge, given today's challenging geopolitics.



Intrusion types

Q: What techniques were involved in the intrusion?

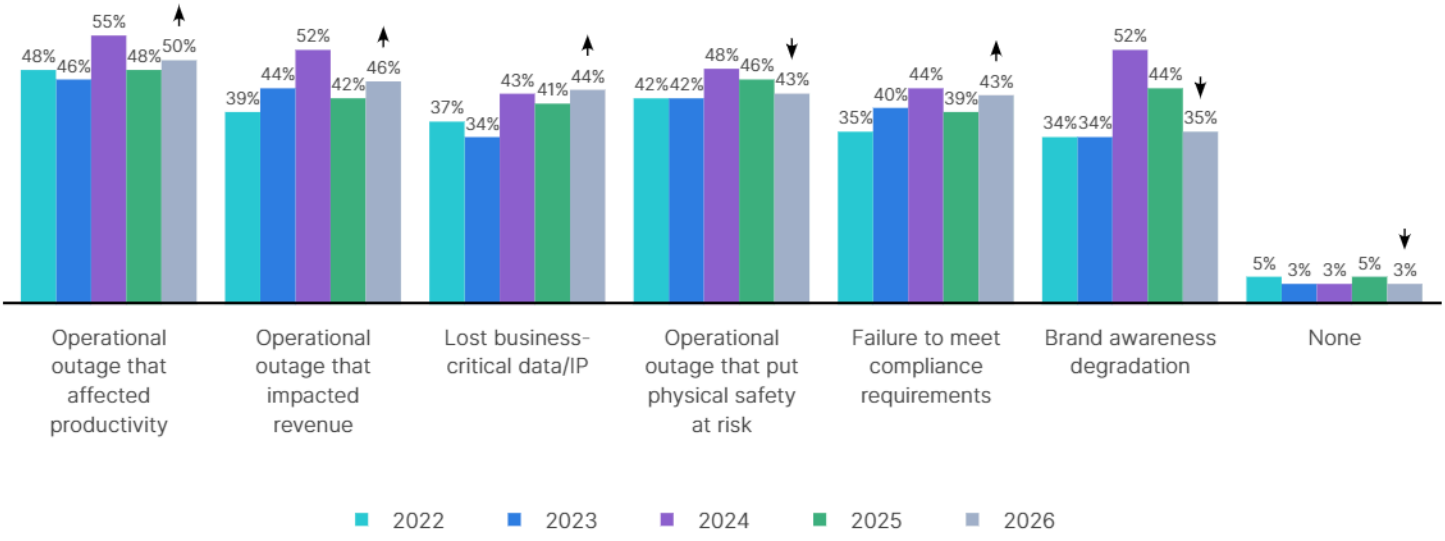
Intrusion techniques remained consistent between 2025 and 2026, but fewer unintentional and bad actor insider breach incidents were noted. This reduction may be related to better vetting, tighter controls, or more people remaining in the same job. Removable storage has trended down, but web application compromise rose in 2026.



Techniques involved

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

The impacts of intrusions remain consistent across the board, from lost intellectual property or trade secrets and factors that potentially have penalties attached, such as failure to meet compliance levels. Operational outages affecting revenue rose from 42% in 2025 to 46% in 2026. Lost critical data also increased from 41% to 44%, highlighting the risks to data. On a positive note, the impact to brand awareness decreased from 52% in 2024 down to 35% in 2026.

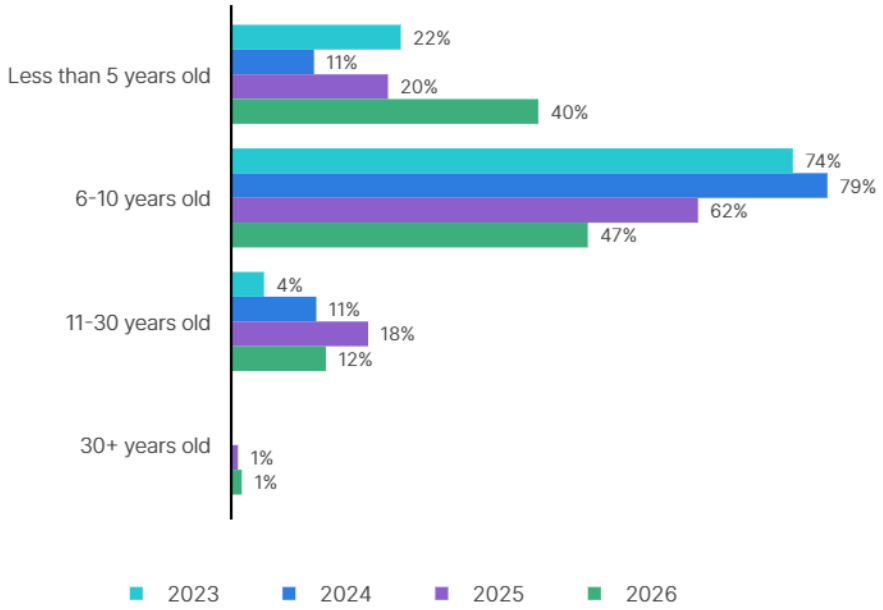


Intrusion impacts

Q: What is the age of your ICS system?

Respondents appear to be refreshing their ICS systems with 40% reporting that their systems are under five years old, a sharp increase from 2025 (20%) and previous years. This rise points to a healthy attitude toward the benefits of modernization and transformation.

Those organizations with aging 11-year-old or older systems should upgrade soon, or if refreshing the systems isn't feasible, they should adhere to a strict patching and monitoring schedule.

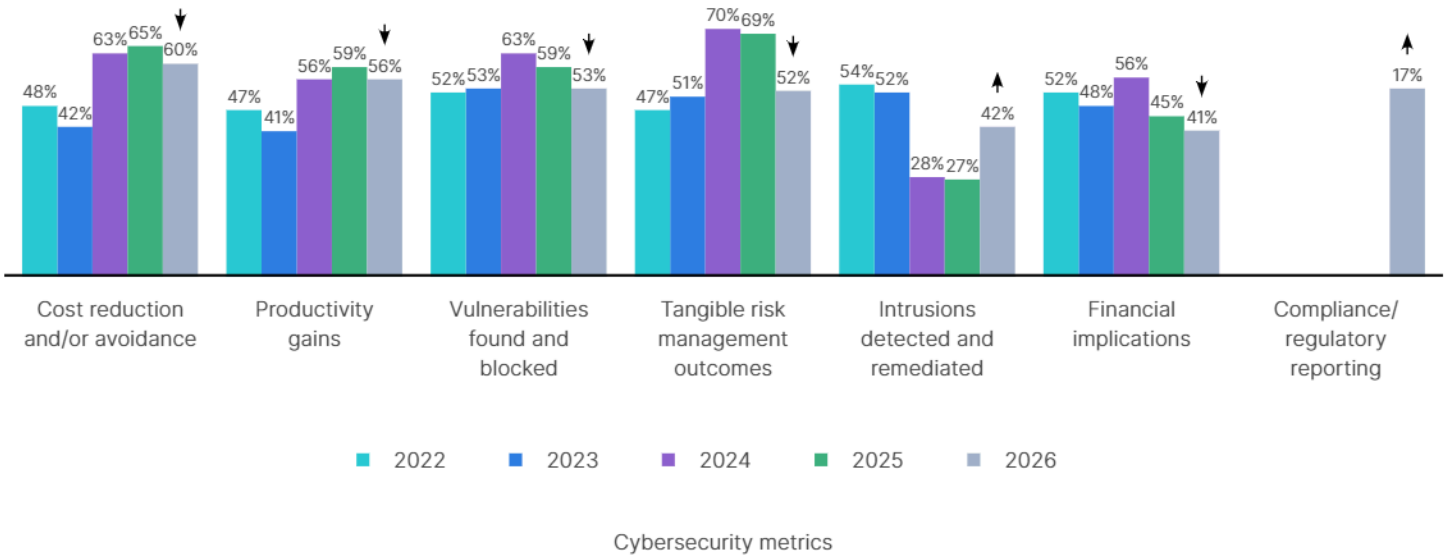


ICS systems age

Global Impact

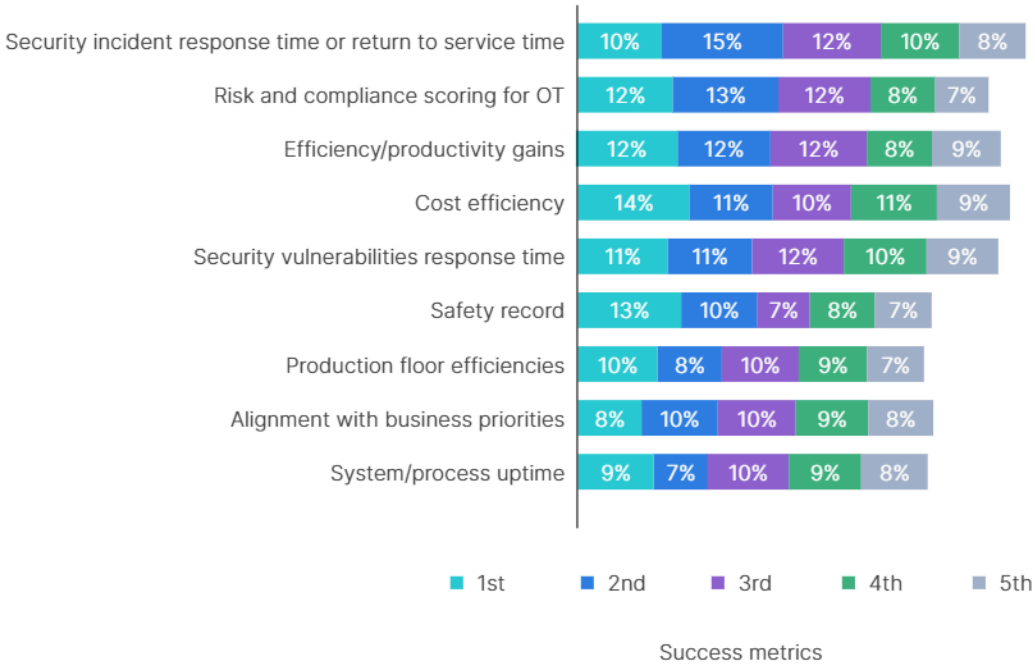
Q: What cybersecurity measurements do you track and report?

Because of tightening budgets, cost reduction and/or avoidance is the highest metric being tracked and reported by survey respondents, followed closely by productivity gains. The value placed on tangible risk management outcomes decreased in 2026.



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

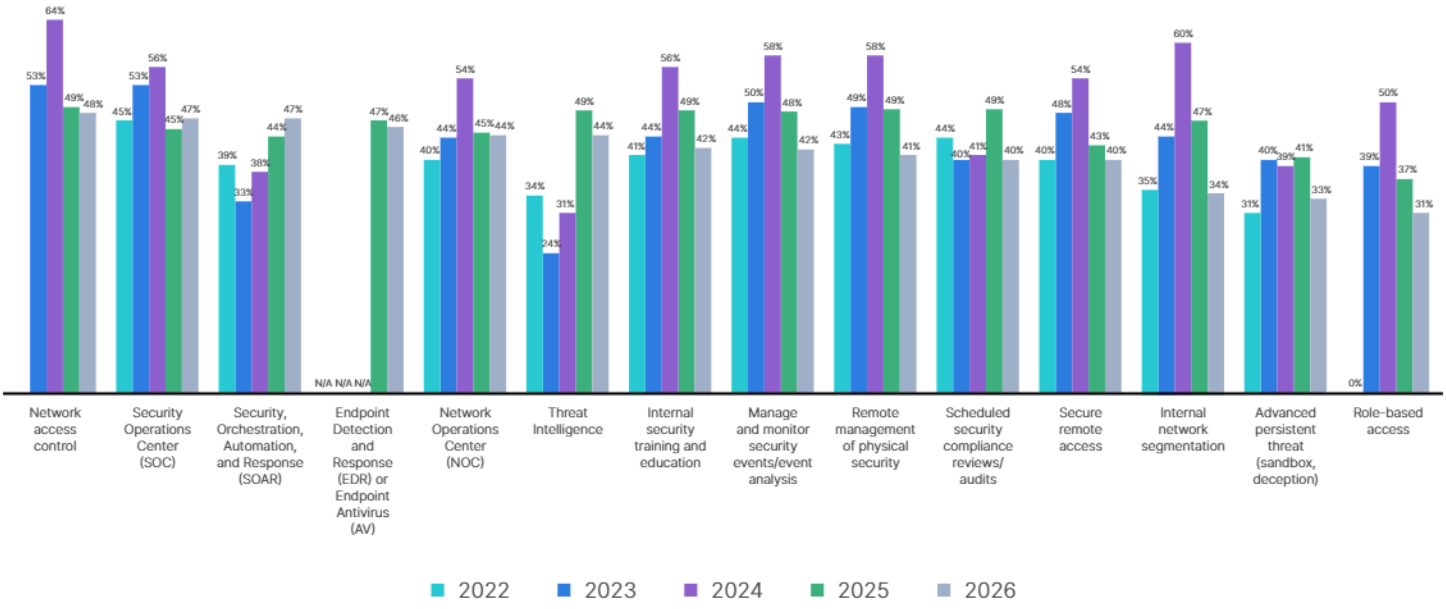
As noted, we are seeing a shift toward cost efficiency and productivity value, which is reflected in the success metrics. In 2026, the highest number of respondents cited cost efficiency (14%) as their top measure of success, up from 11% in 2025 (not shown). Security incident response time, which was a top success measurement in the past has dropped from 18% in 2025 (not shown) to 10% this year.



	In Top 3				
	2022	2023	2024	2025	2026
Security incident response time or return to service time	35%	41%	46%	46%	38%
Risk and compliance scoring for OT	N/A	N/A	N/A	N/A	37%
Efficiency/productivity gains	43%	42%	40%	41%	36%
Cost efficiency	39%	35%	35%	41%	34%
Security vulnerabilities response time	33%	45%	42%	43%	33%
Safety record	32%	27%	30%	25%	29%
Production floor efficiencies	33%	31%	35%	27%	28%
Alignment with business priorities	33%	36%	39%	42%	27%
System/process uptime	34%	36%	33%	34%	26%

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

In 2024, there was an increase in the number of cybersecurity approaches and technologies deployed, but 2025 saw a YoY decrease in security features in a number of areas. In 2026, this downward trend continues with drops in features related to basic cybersecurity controls, deployment, and effective defenses. However, advanced controls such as SOC and SOAR are on the upswing. This investment in more advanced technology is consistent with the cybersecurity maturity journey.



Existing cybersecurity features

Best Practices

Based on the 2026 survey results and feedback, we've assembled the following best practices:

1. Segment and microsegment IT and OT networks to limit the impact of attacks

IT attacks can cripple or disable OT operations, and attacks that damage both IT and OT are common. A defensible OT cybersecurity program begins with intentional segmentation and microsegmentation across both IT and OT networks. Leaders who prioritize this architectural foundation gain two critical advantages: greater visibility into assets and communication flows, and reduced impact when intrusions occur. As the report shows, organizations that have advanced beyond basic visibility and segmentation experience fewer and less severe incidents because segmentation limits lateral movement, isolates high-risk systems, and enables the precise monitoring needed to detect abnormal behavior early.

In OT environments, legacy devices, flat networks, and limited patching options are common, so segmentation is not just a best practice, it is a compensating control that materially reduces operational risk. Microsegmentation further reduces risk by enforcing granular, policy-driven communication paths between systems, so teams can better understand exactly who and what is communicating across the environment. This clarity accelerates asset inventory, supports compliance, and lays the groundwork for advanced capabilities such as virtual patching, protocol-aware monitoring, and automated responses.

TIP: Champion segmentation as a strategic investment, not a tactical project. By embedding segmentation and microsegmentation into modernization roadmaps, IT and OT teams can jointly increase their security maturity, simplify operations, and build a resilient architecture that is capable of withstanding today's targeted OT threats.

2. Employ secure remote access

Organizations with OT networks should implement secure remote access (SRA) to shield against cyber-physical attacks. The use of SRA allows third-party vendors to perform critical remote maintenance efficiently without the security risks of traditional VPNs. SRA solutions enforce zero-trust principles, granting granular, temporary access that strictly prevents attackers from moving laterally through the network. SRA also provides continuous monitoring, session logging, and the strict access controls required to satisfy rigorous industrial compliance standards.

TIP: Many SRA solutions exist, so look for advanced features that are OT-aware and consider the key use cases relevant to your organization.

3. Integrate OT into security operations and incident response planning

In the years we have been compiling this report, we have seen two major trends relating to overall OT security responsibility. First, CISOs are taking more responsibility for OT security, and the C-suite is getting more involved. This rise in decision-maker seniority is welcome and positive, but it also indicates that many organizations are still working out how to address OT cybersecurity.

A critical maturity step is developing incident response playbooks that fully incorporate OT systems, production processes, and plant-level roles. This preparation strengthens collaboration across IT, OT, and production teams, enabling them to jointly evaluate cyber risk and operational impact during an event. It also ensures the CISO has clear visibility into OT-specific priorities, resource needs, and budget requirements. By embedding OT into security operations (SecOps) planning, leaders can develop more coordinated, resilient responses that take both cybersecurity and production continuity into account.

TIP: As organizations advance toward a unified IT-OT SecOps model, it's essential to treat OT as a key component of security operations and incident response. OT environments differ fundamentally from IT. OT environments often include specialized device types and a disruption can have far-reaching operational and safety consequences, so security processes must explicitly account for these distinctions.

4. Invest in OT-specific threat intelligence

Effective OT security relies on timely visibility and accurate analysis of emerging risks. A modern, platform-based security architecture should continuously apply threat intelligence to deliver near-real-time protection against new threats, evolving attack variants, and emerging exposures. To be effective, organizations must ensure their intelligence sources include deep, OT-specific insights that cover industrial protocols, asset behaviors, and sector-relevant threat activity. Armed with this information, security teams can detect issues earlier and respond with greater precision.

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

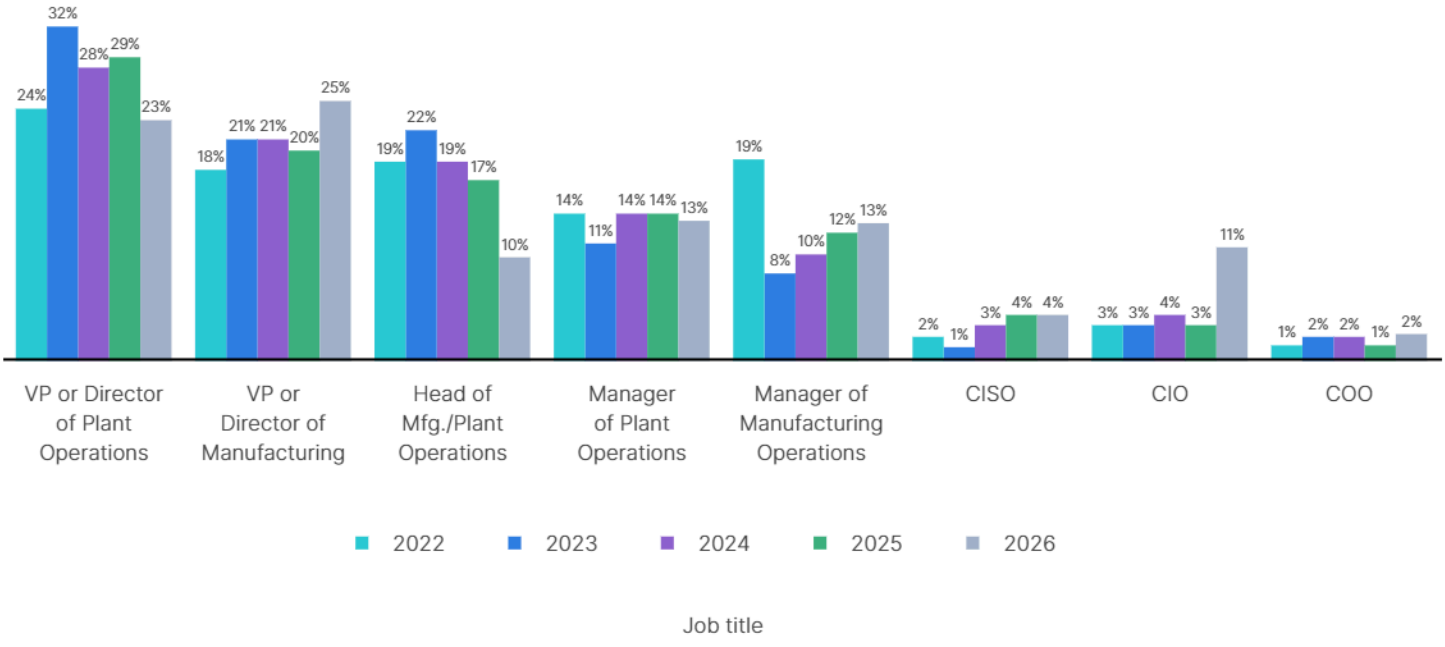
5. Consider a platform approach for overall security architecture

To address rapidly evolving OT threats and an expanding attack surface, many organizations have assembled a broad array of security solutions from different vendors. Taking this multiple vendor and product-based approach often leads to overly complex security architectures that inhibit visibility and places an increased burden on limited security team resources. By taking a platform-based approach to security, organizations can consolidate vendors and simplify their architecture. A robust security platform that includes specific capabilities for both IT networks and OT environments offers solution integration for improved security efficacy while enabling centralized management for enhanced efficiency. Integration can also provide a foundation for automated responses to threats.

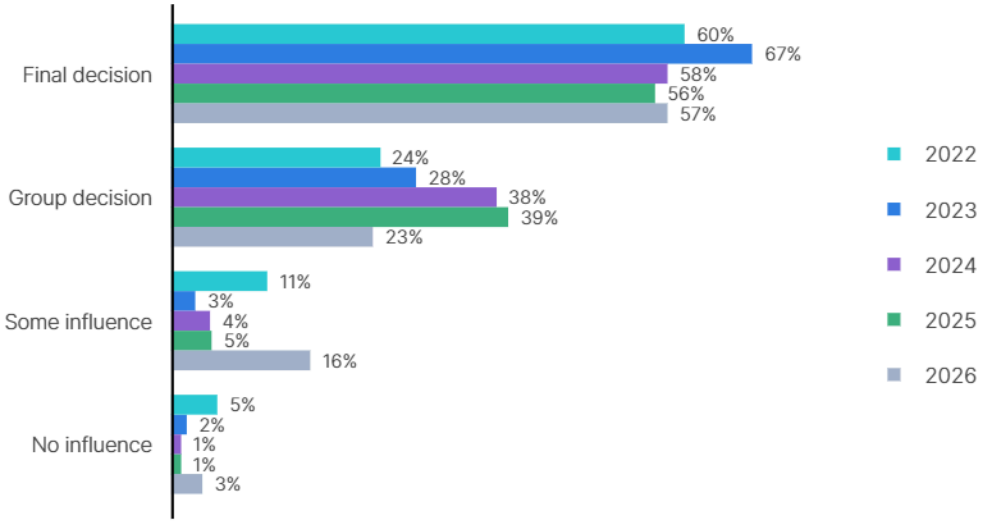
TIP: Security platforms enhanced with context-aware generative AI (GenAI) can significantly strengthen an organization's cyber resilience by automating tasks across both IT and OT environments. For industrial operations, these capabilities accelerate vulnerability troubleshooting, streamline threat-hunting workflows, and reveal insights that would otherwise remain hidden in complex, distributed systems. By applying AI to interpret OT-specific context, such as device roles, process criticality, and communication patterns leaders gain faster, more accurate decision support that improves protection and reduces operational burden on security teams.

Methodology

Most survey respondents have "plant operations" or "manufacturing operations" titles, with almost half (48%) being vice presidents. No matter their title, most of those surveyed are deeply involved in cybersecurity purchase decisions.



More than half of the respondents make the final decision on OT purchasing. As in previous years, many of the other organizations decide on OT purchases as part of a group.



OT purchase decision role

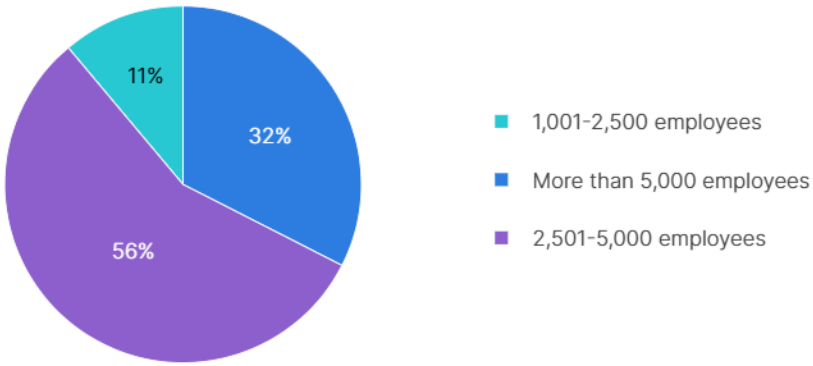
Study objectives

Fortinet retained Empanel Online, a third-party company, to analyze current OT security dynamics around the world and future outlook.

Results are based on an online survey of respondents in managerial and executive roles in companies with more than 1,000 staff members. The companies were primarily in the manufacturing and energy sectors across the world.

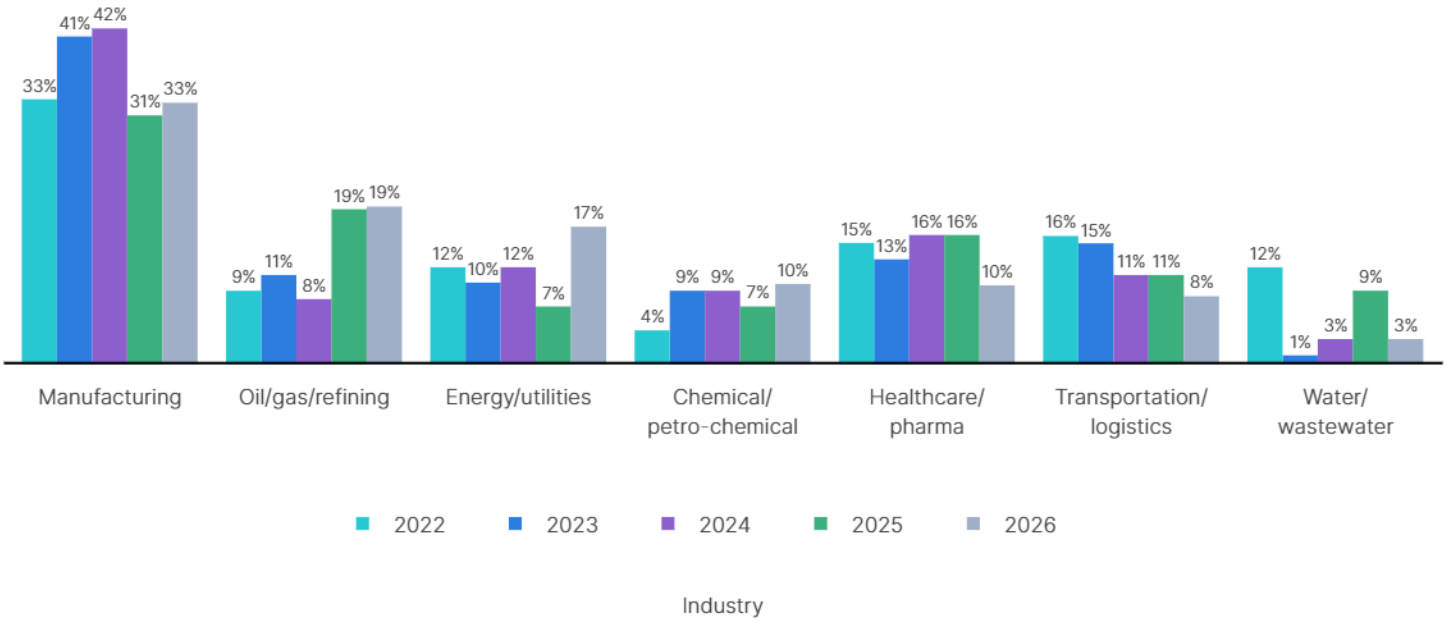
We specifically wanted to know about:

- OT security management
- Reporting and success metrics
- Purchase decision-making
- Factors, preferences, and priorities regarding product capabilities, features and functions
- The impact of cybersecurity on the careers of OT personnel
- OT cybersecurity intrusions, intrusion types, intrusion impacts, and actions taken
- The maturity levels of cybersecurity and OT security programs
- Monitoring and control mechanisms
- Future outlook



Company size breakdown

Sectors covered



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

*2022 and 2023 only

Conclusion

OT security is a critical aspect of the global economy. Only by defining and defending key operational assets and ensuring their performance can businesses compete in the global marketplace and governments protect their citizens. Although the convergence of IT and OT can be a powerful driver of innovation, it requires a strong commitment to implementing cybersecurity defenses, hiring, and strategic thinking.

Because many OT devices are more than 20 years old and unsecure by design, creating a secure OT environment is extremely challenging for many organizations. However, we see signs that more organizations are making progress and better assessing their OT security posture. These efforts are paying off in greater awareness of intrusions and a lower overall volume of intrusions.

As the *2026 State of Operational Technology and Cybersecurity Report* shows, companies with higher OT maturity security levels 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 allocate the necessary resources to secure critical operations.

Copyright © 2026 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's SVP Legal and above, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

June 11, 2026 10:02 AM / MKTG-3527-0-0-EN