INDUSTRIAL DEFENDER®

RESEARCH REPORT

2022 State of Operational Technology (OT) Cybersecurity Survey

INDUSTRIALDEFENDER.COM

The rapid evolution of both threats and defenses inside the operational technology (OT) space creates a landscape that quickly—and continuously—changes. This survey and report are intended to be a snapshot of today's landscape, as well as a look forward to what might come next.

TABLE OF CONTENTS

A NOTE OF THANKS

We appreciate the time and attention of the OT experts and professionals who shared their expertise with us through the survey. Without their input this work wouldn't be possible.

SURVEY METHODOLOGY

This survey was conducted between October 2021 and May 2022 by Industrial Defender. A total of 101 participants completed the survey.

Big Takeaways

Overall, organizations are focused on solving very specific gaps and overlaps across OT security, while trying to better integrate with big picture IT security strategies and goals. The only way this happens is through the continued close cooperation on both sides of the OT perimeter. Our report suggests that, even with challenges coming from all directions, this critical collaboration is already shaping the future.

A NEED FOR FLEXIBILITY IN TOOLS AND GOVERNANCE

Organizations are persistent in finding ways to balance compliance and flexible operations. The unique constraints of OT environments demand multiple paths to both security and compliance.

- **The survey finds teams deploying multiple platforms and solutions to safeguard their control environments, layering agentless, active, passive and manual data collection tools with other solutions.**
- **We also saw a broad distribution of governance models, with organizations splitting nearly evenly between being led by IT, OT, or via shared responsibility.**

CONTINUING WORRIES ABOUT STAFF AND SKILLS SHORTAGES

When asked about barriers to success, people-adjacent challenges outpaced technology-centered problems. Organizations need both larger staff and additional capabilities.

- **When asked about barriers to OT security success, lack of in-house expertise came in second only to budget.**
- **Most respondents indicated they were growing their OT security headcount in 2022, with an ideal team size of between five and nine.**

A DELICATE BALANCE BETWEEN SECURITY AND COMPLIANCE

As compliance frameworks multiply and lawmakers begin to take OT threats more seriously, operational guidance is getting tighter. Teams are now trying to keep pace with both attackers and regulators.

- **When we asked about what was driving risk strategy, concern over meeting government regulation barely topped fear of an attack.**
- **Reporting and compliance remain popular areas for 2022 OT budget investments.**

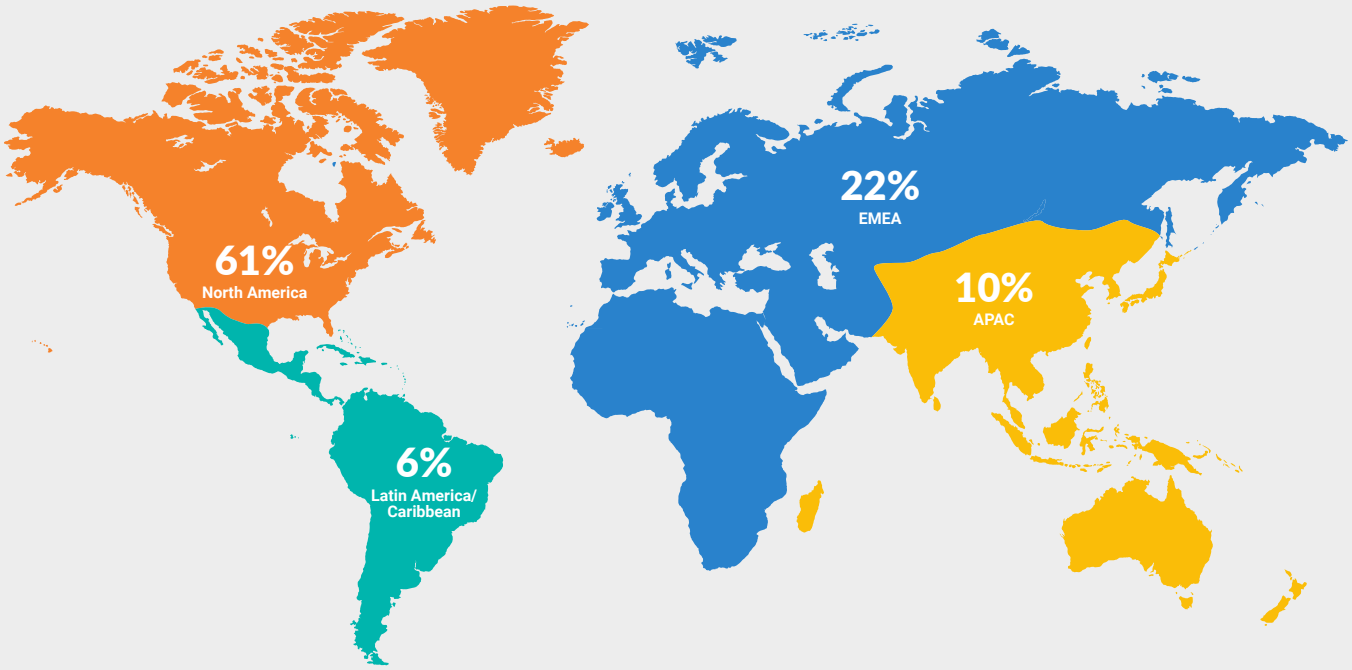
About Survey Respondents

GLOBAL REACH, DIVERSE INDUSTRY AND ROLE PARTICIPATION

We reached out broadly to OT professionals across diverse roles, regions, and industries. Our goal was to capture the depth and breadth of opinion and insight inside a rapidly—and continuously—evolving industry.

Their Regions

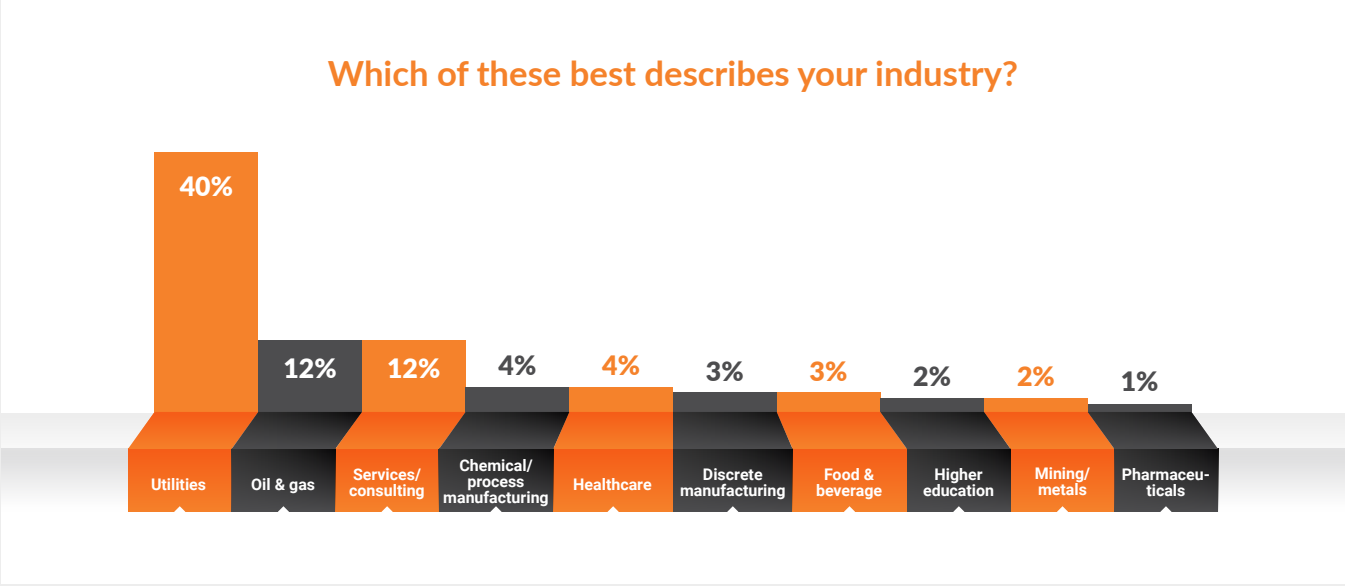
The vast majority of respondents (61%) currently work in North America, followed by 22% currently working in Europe, Africa, or the Middle East. Almost 10% work in the countries of the Asian Pacific, and finally almost 6% of respondents work in Latin America or the Caribbean.



Their Industry

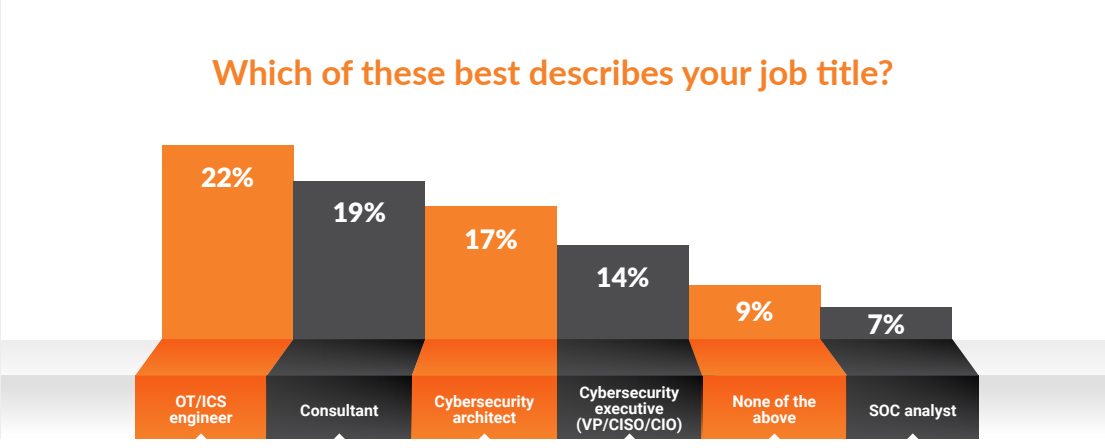
When asked in which industry they worked, we again saw a similar single dominant answer with well-distributed runners up. Not surprisingly, almost 40% of survey takers work in OT inside the utilities space.

After that, we saw strong response (12%) from the oil and gas industry and professional services firms (12%), who continue to play a larger role in OT modernization. Also showing up with consistency are manufacturing, food and beverage, healthcare, and finally higher education and mining.



Their Role

Our respondents' range of roles gives us a fairly representative perspective from both the dev and ops sides of OT—and both sides of the perimeter-- from front line practitioners up through to the C-suite. OT and engineers were our largest role sampled (22%), followed closely by consultants (19%) and cybersecurity architects (17%). After that, we saw cybersecurity executives (14%) and finally SOC analysts (7%).



OT Budgets and Resources

INSIGHTS INTO SHARED RESOURCE DECISION-MAKING

There's perhaps even more evidence of a growing collaborative control over OT security budget decisions. This is reflected in both who controls funds and also some of the decisions being made.

Who sets the budget?

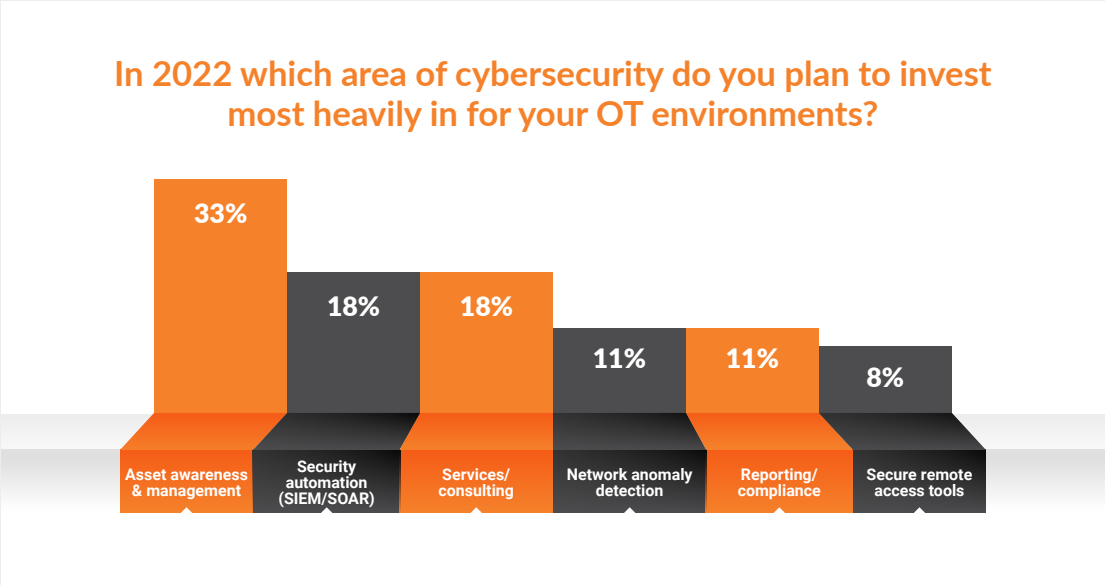
We asked respondents about who controlled the OT cybersecurity budget for their organization. Their answers indicated a close balance of control between IT and OT when it comes to identifying and prioritizing operational technology security needs and resource priorities.

38% of respondents indicated that either IT or the CISO team controlled OT security budget decisions. We then see a virtual tie for second place between control by the OT team (29%) or shared control by both sides of the organization (28%).

Where are teams adding solutions and capabilities?

When we asked about where security budget was being applied, the answers reflect a heavy focus on both OT and IT fundamentals. On the OT side, organizations are heavily investing in illuminating endpoints with asset-focused awareness and management solutions (33%). We next see organizations investing in both big picture automation through SOAR/SIEM (18%) and consulting help (18%).

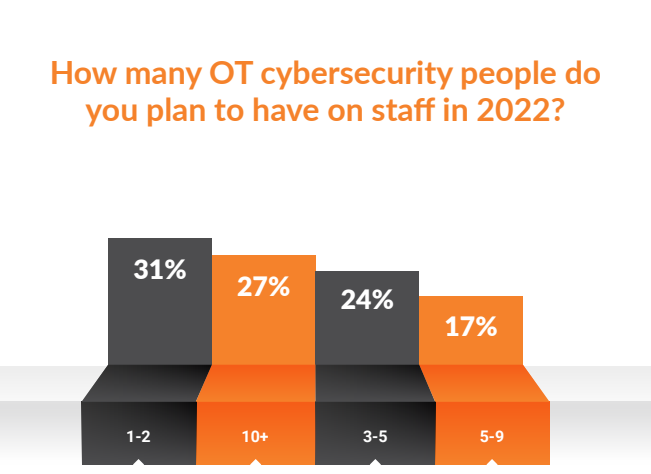
The internal and external pressures on OT teams shows up in their investment decisions, too, as they're acquiring new network anomaly detection tools (18%) and additional reporting and compliance capabilities (18%). Organizations are still buying secure remote access solutions, but it's a lower priority than other needs.



Where are teams adding staff and expertise?

Many organizations are still struggling to close technology and talent gaps simultaneously. The two are obviously linked. New needs drive new tools, which require more team hours and additional expertise. As a result, OT teams are trending larger.

When we analyzed responses around current vs. hopeful future team size, we saw a move towards consistent hiring at all sizes. While one or two member OT teams are still the most prevalent, the biggest gain was those planning to staff at between five to nine dedicated OT professionals.



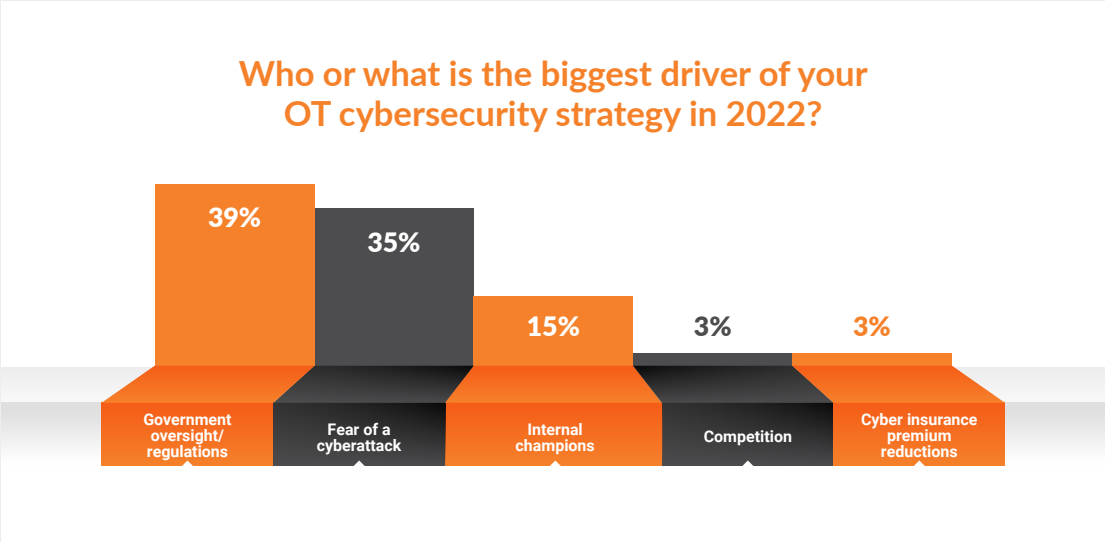
OT Strategies and Barriers

PROBING STRATEGIC DRIVERS AND BARRIERS

As organizations look at modernizing and strengthening their OT security, they face big choices and challenges. Even as the threat and regulatory landscape keep changing, internal decision dynamics also shape OT planning and readiness. Unfortunately, for all the talk about proactivity, many organizations still find themselves primarily reactive.

What's driving strategic thinking?

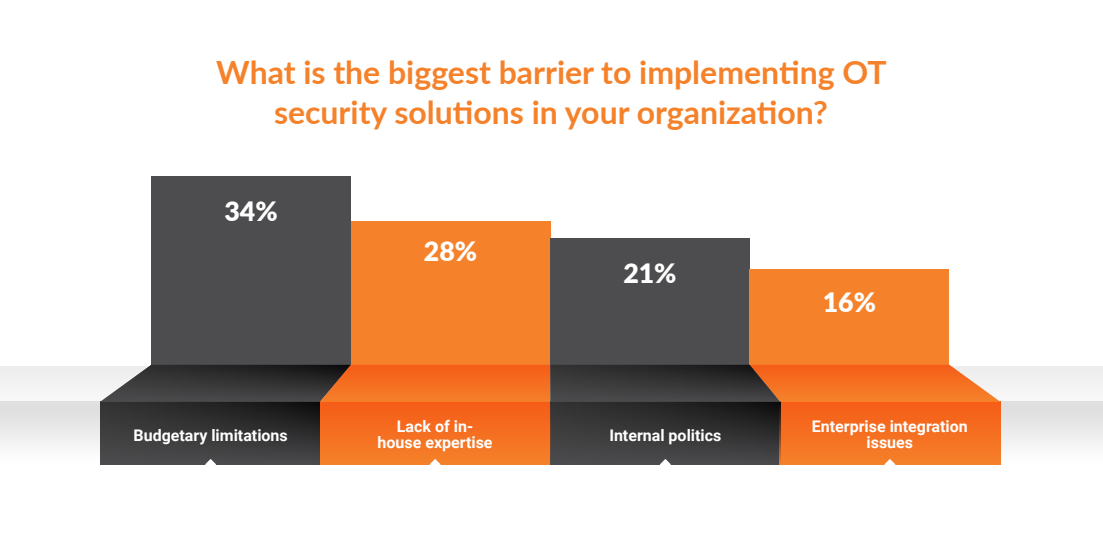
While external events frequently drive internal change, we wanted to know what else was driving OT strategy decisions. What were the prime drivers of security investment and innovation? Were organizations being proactive, or still mostly reacting to real or perceived risk?



The top drivers of strategy were still overwhelmingly external. Most respondents (39%) were focused on meeting government regulations, while only 35% were motivated by fear of the attacks themselves. Internally, champions for better OT were seen as prime movers by 15% of our survey. Competitive concerns and attempts to reduce cyber insurance both captured about 3% of the answer.

What are the barriers to doing a better job?

When we asked about barriers to OT security implementation, budget limitations unsurprisingly showed up at the top of the list with 34%. These money concerns were followed by a lack of in-house expertise (28%), internal politics (21%) and finally enterprise integration issues (16%).



Setting the obvious impact of money on everything aside, only one answer (enterprise integration issues) is focused on tech. This might reveal that much of the remaining work to be done around OT security isn't about technology, but rather solving adjacent gaps and overlaps around talent, process, and governance.

OT Incidents and Detection

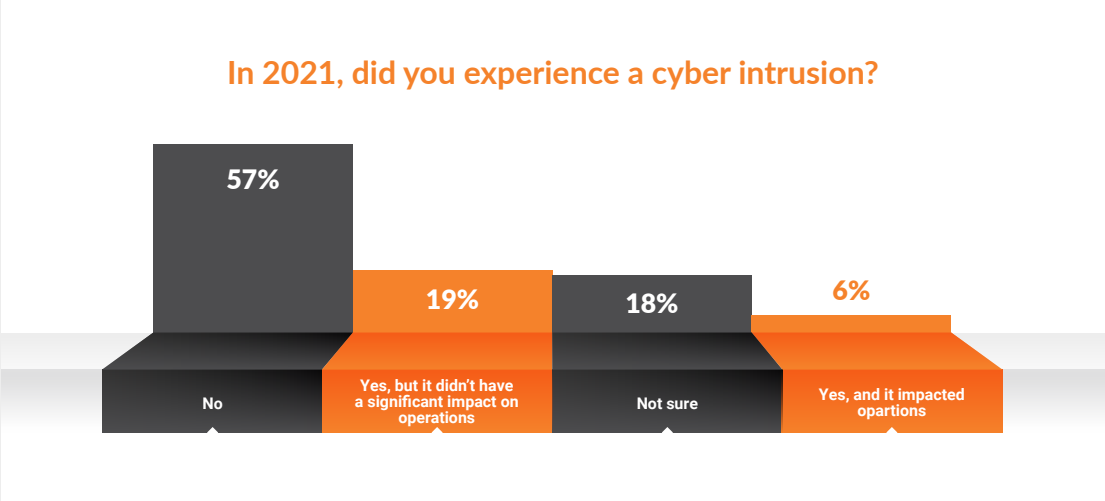
OT INCIDENTS AND DETECTION

The intense focus on OT vulnerabilities has increased vigilance around internal and external risk. But the actual impact of incidents might be less dramatic.

Incidents and their impact

The good news is that most survey respondents (57%) reported no OT incidents in 2021. 19% indicated a breach with no real effect on operations, and only 6% of organizations said they experienced an incident that brought a significant impact.

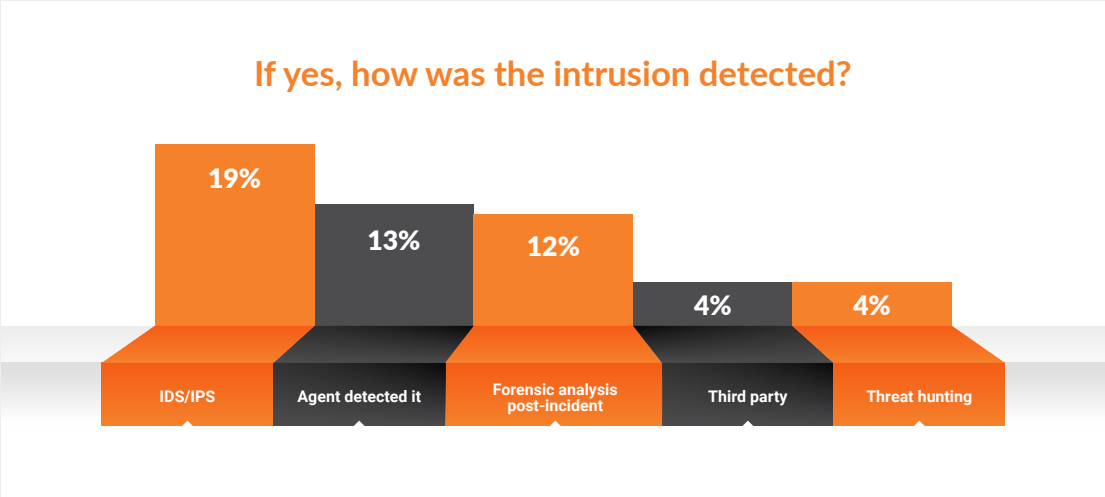
At the same time, the large percentage (18%) of respondents answering “Not Sure” could potentially point to a troublesome lack of visibility inside organizations, or simply be a byproduct of incomplete and inconsistent communications.



How incidents get detected

Probing on how incidents get detected shows us a rapidly maturing OT security stack. Collaborating on both sides of the perimeter, IT and OT (with the help of third-party partners) are relying on both passive and active solutions for detecting incidents, either in real-time or review, across networks and at the endpoint.

Either IDS or IPS solutions were the most frequent (19%) path to incident detection, followed by agents (13%) and forensic detection after the fact (12%). Finally, respondents said both third party partners and active threat hunting detected incidents 4% of the time.



OT Operations 1 – Risk Assessment

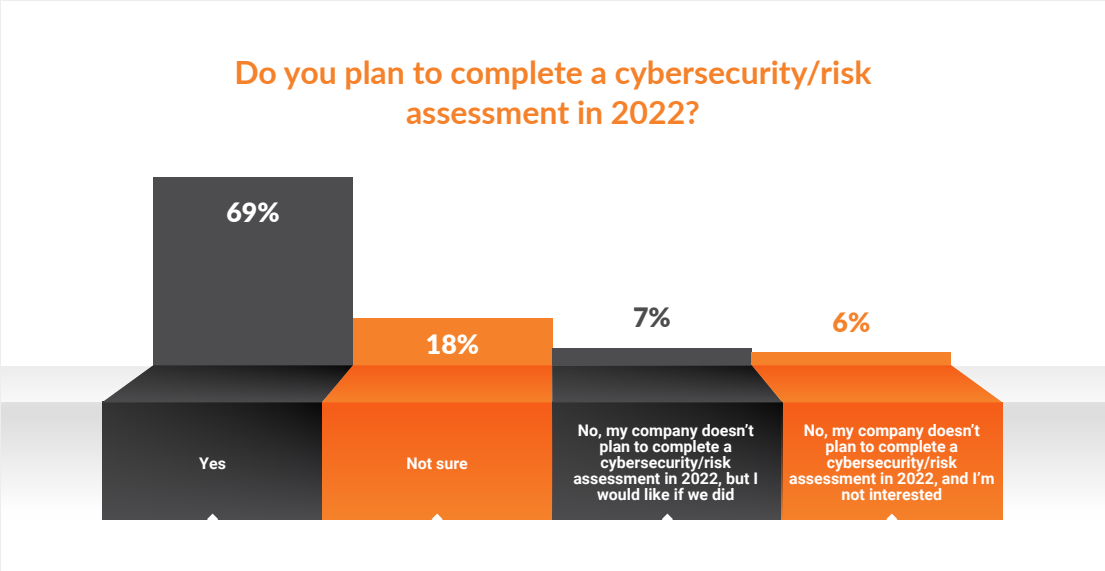
WATCHING FOR RISK

While environment-wide risk assessments are fundamental to general cybersecurity good governance, they take on special significance inside OT. Formal risk assessments, built around OT-focused vulnerabilities and threat indicators can help organizations better understand potential problems and deficiencies.

Formal Risk Assessments

When we asked if organizations had plans for a formal risk assessment in 2022, an impressive 69% indicated they intended to complete one, but 18% weren't sure. Remaining respondents were split:

- 7% said they would prefer an assessment but don't have one planned
- 6% expressed neither a plan nor an interest in an assessment

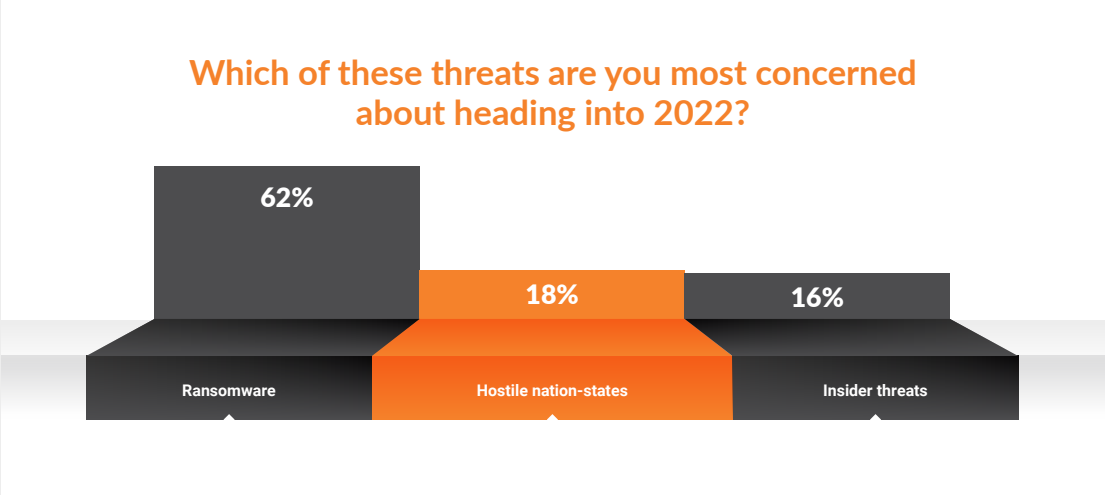


Where are the risks coming from?

While practical concerns like staff and budget are persistent headaches, OT leaders are also working to stay out in front of a rapidly changing threat landscape. The survey period, from October 2021 to May 2022, saw an industry still absorbing the impact of Colonial Pipeline even as worries about Russia and Ukraine grew.

When we asked respondents to rate the largest current driver of security strategy, their top concern, ransomware, was way out front at 62%.

And while ransomware attacks continue to generate big headlines and even bigger revenue, other threats are also keeping OT professionals up at night. Worries about hostile nation states (18%) and insider threats (16%) also inform decision-making.



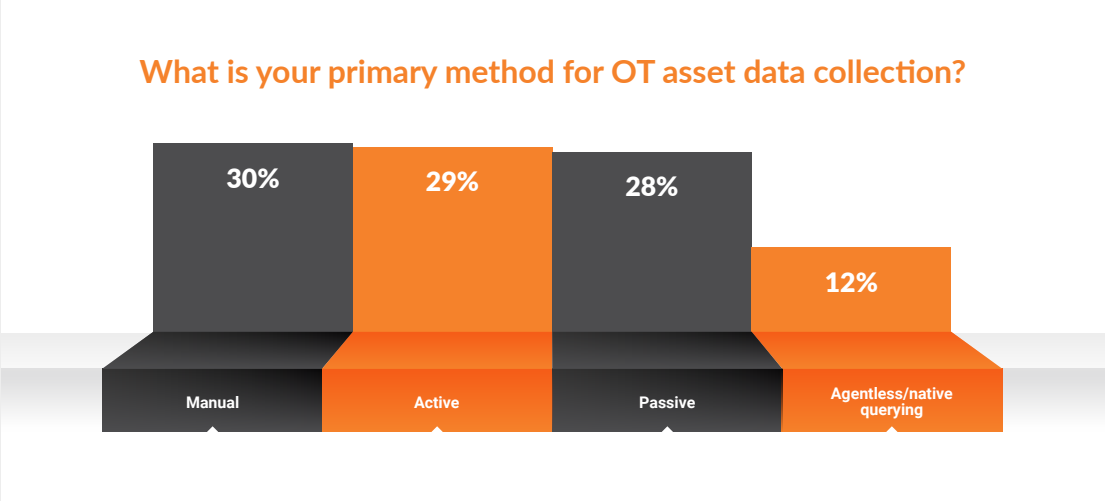
OT Operations 2 – Data Collection

UNDERSTANDING OT DATA COLLECTION

The challenge of monitoring OT networks has seen organizations deploy varied active and passive methods of collecting the data required to monitor environments with maximum visibility and minimal impact on performance or reliability. While most organizations are committed to moving away from manual processes where possible, the ability to mix active and passive remains important to effective OT security.

Data collection, current state

When we asked about primary current method of data collection, responses were almost evenly split among traditional manual processes (30%), various active methods (29%) and passive solutions (28%). Finally, 12% of organizations were relying on agentless methods to collect data.

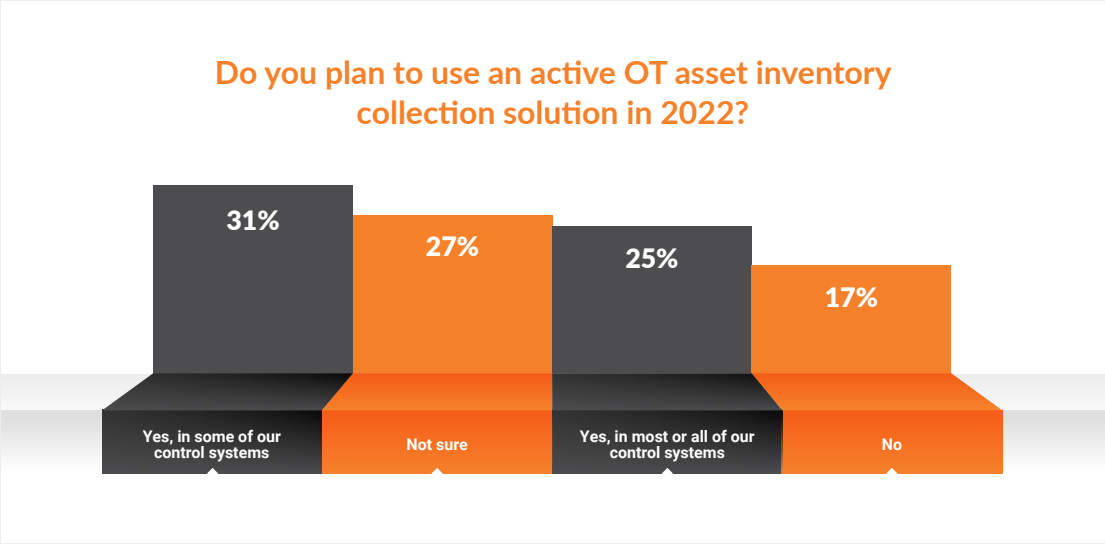


Data collection, future state

When we asked respondents about future data collection plans, it's clear that both passive and active solutions have a role to play.

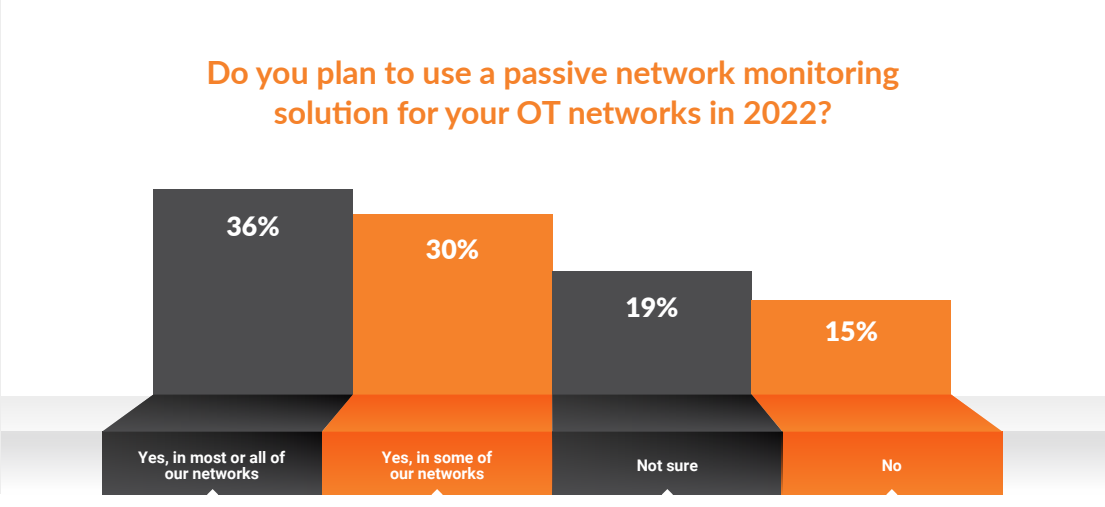
When we asked about active data collection:

- 25% of respondents planned to use it for all systems, and 31% said they'd use it for some.
- 17% said they wouldn't use active data solutions at all, and 27% weren't sure.



When we asked about passive data collection:

- 36% of respondents planned to use it for all systems, and 30% said they'd use it for some.
- 15% said they wouldn't use passive data solution at all, and 19% weren't sure.



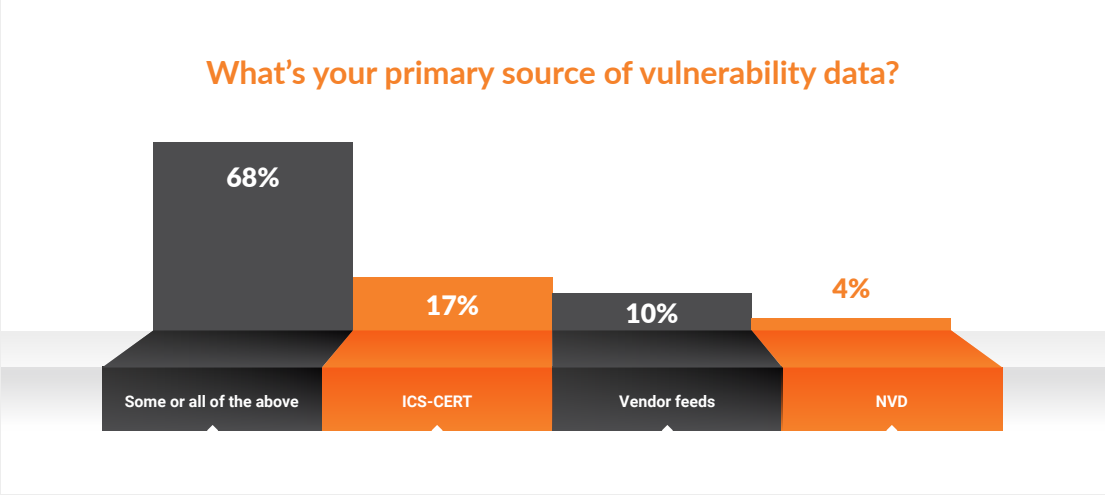
OT Operations 3- Vulnerability Management

UNDERSTANDING VULNERABILITY MANAGEMENT

The intense focus on third-party security, especially in OT, highlights the need for robust vulnerability management. Like their peers in IT, OT security teams need access to a globally managed, continuously refreshed set of known vulnerabilities to serve as inputs into internal monitoring and discovery as well as informing defenses and compliance controls.

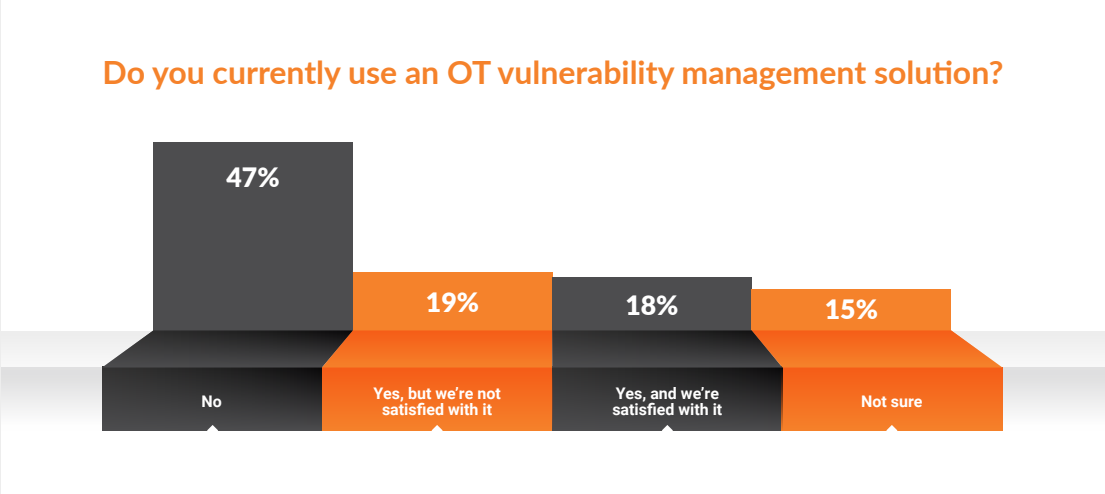
Preferred data sources

When asking for organizations' primary source of system vulnerabilities, we asked about the use of vendor feeds as well as the databases maintained at NIST's NVD and ICS-CERT. A wide majority (68%) said they used some or all of the sources in combination. For those preferring single feeds, ICS-CERT (17%) led both vendor feeds (10%) and the data from NIST's NVD (4%).



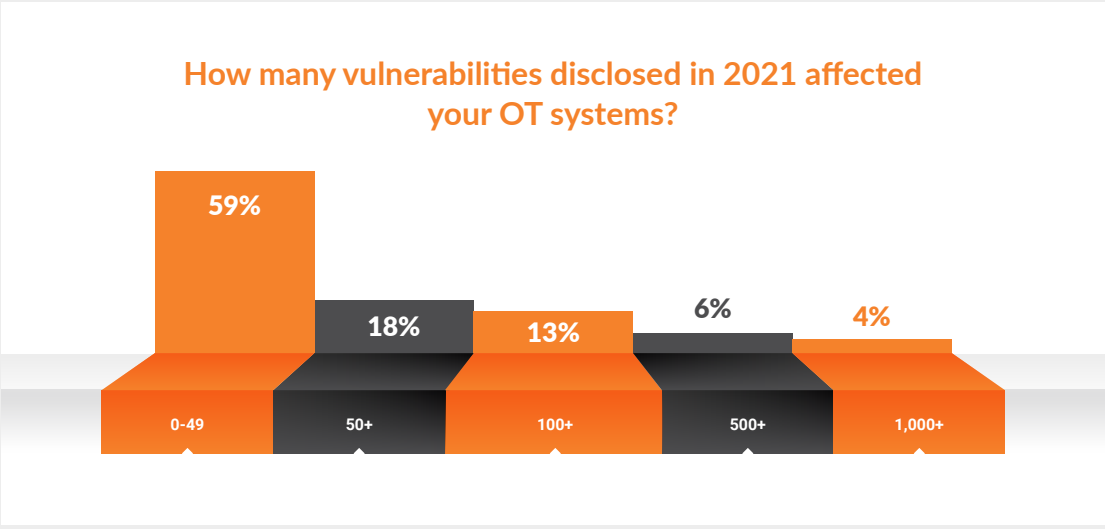
Solution satisfaction

There appears to be less confidence in formal vulnerability management systems, with many OT teams possibly falling back to manual processes they know and trust. Only 18% of respondents had a solution they liked, while another 19% had a solution they were not satisfied with. More importantly, 47% indicated using no system at all.



Impact on systems

Where both a data source and a solution are in place, we wanted to know how many vulnerabilities were being proactively identified across the environment. More than half (59%) reported finding less than 50 vulnerabilities. 18% of respondents identified more than 50, with 13% of organizations uncovering more than 100. The outliers were teams that found more than 500 (only 6%) and the 4% that identified more than 1,000 vulnerabilities.



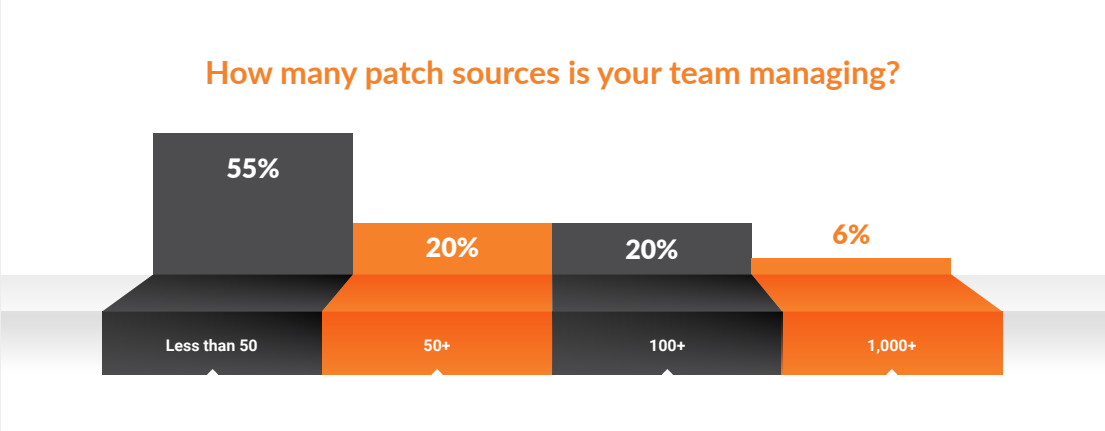
OT Operations 4 – Patching/Monitoring

MONITORING AND MANAGING OT SYSTEMS

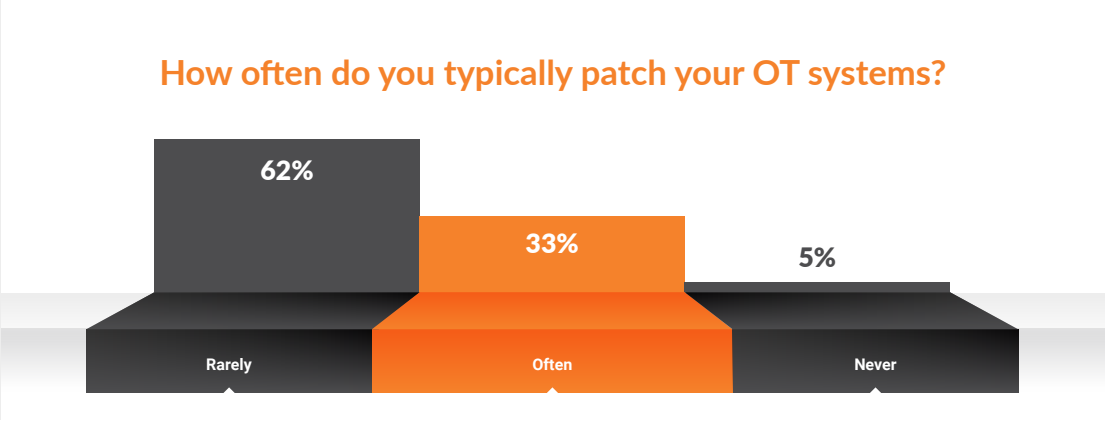
The application of patches and upgrades is one area where IT and OT priorities dramatically diverge. On the IT side, software updates can generally be frequent and designed for easy rollback, but the stakes on the OT side of the perimeter are much higher. The importance of continuous monitoring is similarly amplified.

Managing patches

We started by asking the number of patch sources teams managed. More than half (55%) of organizations said they were managing fewer than 50 sources. From there, we see that 20% said they used more than 50 sources, and the same number said they had to use more than 100 patch sources. An unfortunate 6% said they were working with over 1,000 patch sources.

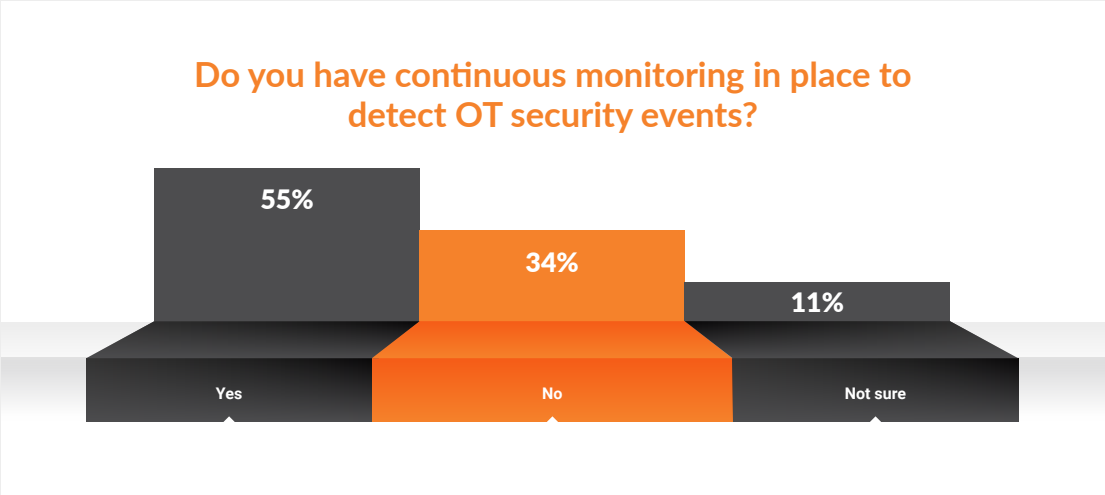


When we polled on the frequency of patch applications, another contrast with IT organizations becomes clear. 62% answered rarely, 33% often, 5% never.



Continuous monitoring

We also asked about another cybersecurity fundamental, continuous monitoring. More than half (55%) of organizations have it in place, with 34% indicating they don't have a formal continuous monitoring solution in place, and 11% aren't sure.



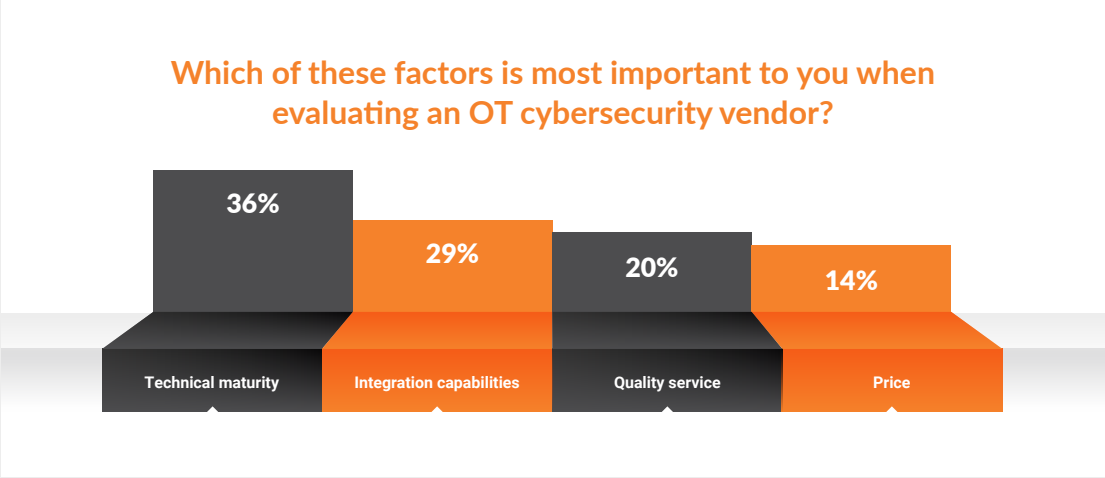
Solution/Vendor Selection

UNDERSTANDING PARTNER, SOLUTION, AND FRAMEWORK SELECTION

When organizations do reach out for help with modernization, how do they evaluate potential vendors and solutions? We asked about the decision-making process that takes place when bringing new tools or partners on board.

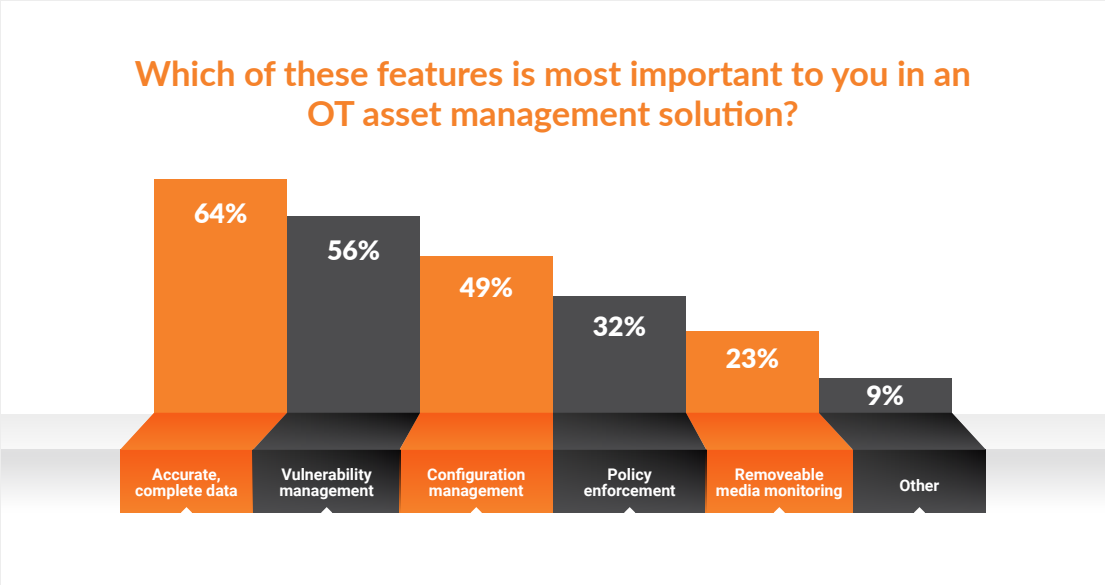
Selecting vendors

A narrow majority of respondents (36%) prioritized technical maturity over system integration capabilities (29%). The quality of service was seen as the next highest priority at 20%, with price being the prime decision-making factor for only 14% of organizations.



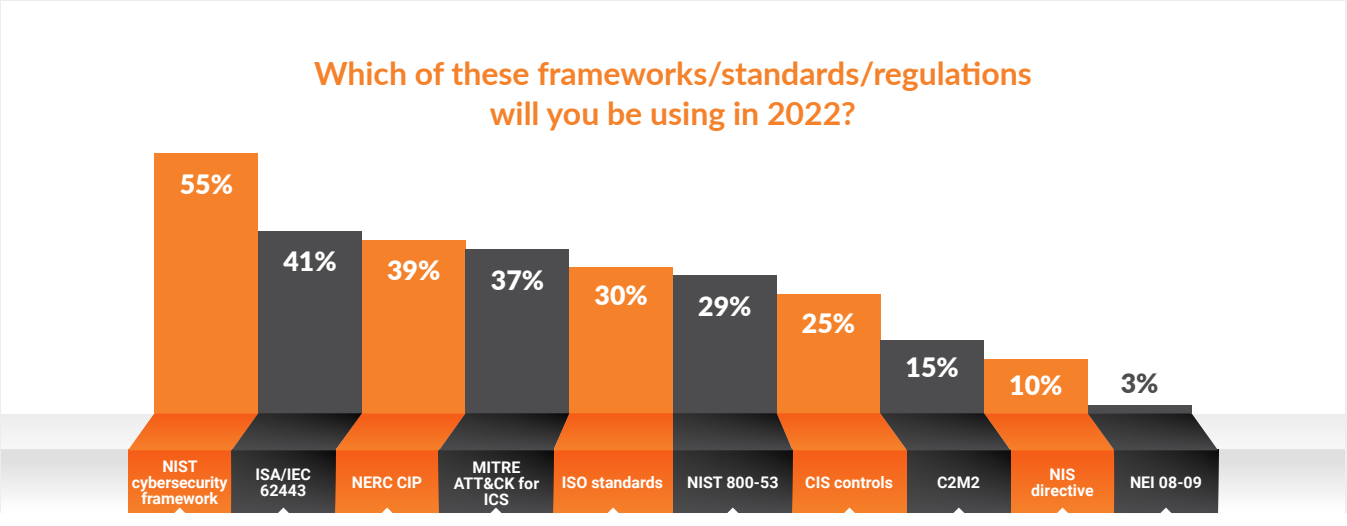
Prioritizing solution features

Answers to the question about 'most important feature' are similarly varied, revealing diverse critical areas of OT concern. Accurate complete data came out first (64%), ahead of formal vulnerability management capacities (56%) and configuration management (49%). Other respondents indicated policy enforcement (32%) and removable media monitoring (23%) were their most important features.



Which framework works best?

The last survey question also captured the wide variety of OT environments. When we ask organizations about which frameworks they will apply in their security operations for 2022, of the ten possible answers, the NIST Cybersecurity Framework (55%) led NERC CIP (39%) and MITRE ATT&CK for ICS (37%) at the top. The only framework that showed up in fewer than 10% of respondents was NEI 08-09 (3%).



Meeting a Collective Threat

Achieving OT cyber resilience inside today's heavily digital and hyperconnected organizations requires a new commitment to collaborative visibility, detection, and control on both sides of the perimeter.

In practice, this means IT and OT teams working together to link and layer defenses, bringing diverse tools to the fight. Where priorities align, so should tactics. It also sees security experts working together to strategically address the tech and talent gaps that stand in the way of meaningful modernization.

THE INDUSTRIAL DEFENDER DIFFERENCE

Industrial Defender protects the world's critical infrastructure from cyberattacks. As a leader in OT cybersecurity innovation, the company's scalable platform is used by organizations around the world to empower security stakeholders with actionable data from their OT and IIoT infrastructure, enabling them to make informed risk management decisions in a concise, single vendor dashboard. Learn more at **www.industrialdefender.com**.

Planning an OT Security Project?

Schedule a demo

FOR MORE INFORMATION

1 (877) 943-3363 • (617) 675-4206 • info@industrialdefender.com
225 Foxborough Blvd, Foxborough, MA 02035
industrialdefender.com