Research

TPR Survey Report

The State of Industrial Secure Remote Access

Sponsored by Cyolo

Executive Summary

Securing remote access and building an overall cybersecurity strategy should be approached like any other business decision. Advantages and associated risks must be reviewed. There are also many challenges, people, technologies, and processes to consider, which vary between and within industries. Despite these differing factors, all organizations should identify their operational objectives and risk appetite to develop an appropriate strategy. A diverse, multidisciplinary approach will help organizations align with various stakeholders and expectations while successfully deploying and securing remote access to industrial environments.

Remote Access is Essential to Most Industrial Operations

Many complex and specialized systems operate in industrial OT/ICS environments. These systems require installation, maintenance, and support from product vendors and numerous third-party technicians, operators, and contractors who can provide product/system support and maintenance due to their expert skill sets and in-depth knowledge. Most industrial enterprises are unable to operate without this cadre of support and rely on 24/7 external assistance.

Equally essential is the need to provide remote access to OT assets and operations. Remote access is now a universal and fundamental requirement for most industrial enterprises. However, the challenge that remains is to ensure that all access is safe and secure and cannot be exploited or abused by malicious actors, whether external or internal. As a result, Industrial Secure Remote Access (I-SRA) strategies have become a critical building block for every OT environment. Thankfully, there are ever-advancing technologies to handle the complexities of OT environments and the unique threats they face.

TPR conducted an industry survey of OT, IT, engineering, and cybersecurity professionals to better understand the challenges of successfully enabling and securing remote access to industrial environments

---

Key Findings

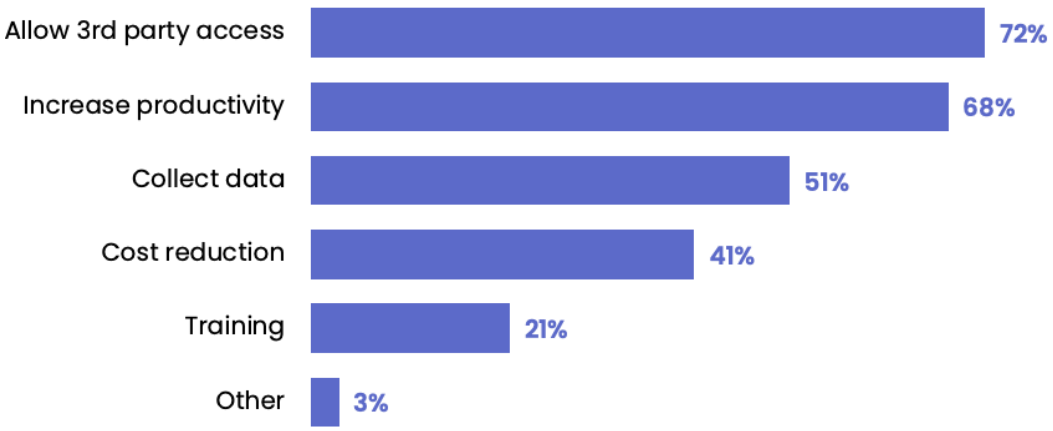
- Allowing third-party access is the primary factor for needing remote access according to 72% of survey participants. 68% also mentioned improved productivity as a key priority.
- Threats to operational safety (75%), Advanced Persistent Threats (APTs) (67%), and misconfigurations or unintended consequences (59%) were identified as the primary risks associated with remote access to industrial environments.
- 48% of larger companies (10,000+ employees) have over 50 remote users connecting to their industrial environment daily; however, securing remote access is not a challenge exclusive to big organizations.
- Companies of all sizes share concerns about the risks associated with remote access, with an average score of 8.61 on a scale of 1 to 10, indicating a high level of concern.
- Regardless of company size or industry/vertical, there is a substantial gap between the level of concern about remote access risk and the level of confidence in existing solutions.
- The top three areas of deficiency cited by respondents were lack of visibility (55%), insufficient user education and training (54%), and weak access control (53%).

Survey Findings

What are the main reasons for connecting?

According to survey respondents, the top reason for enabling secure remote access (SRA) is to **enable third-party access (72%),** closely followed by **increased productivity (68%)** and the need to **collect data (51%)** came in third place.

Reasons for connecting



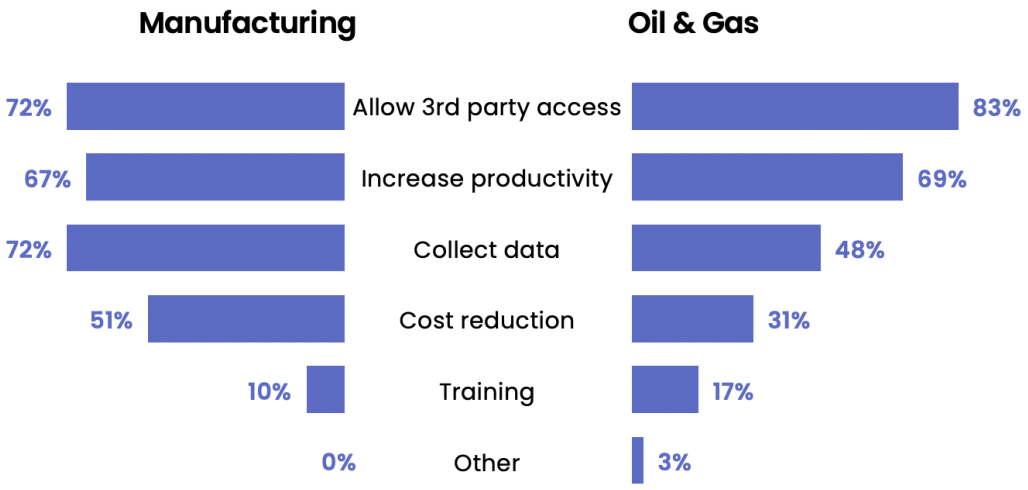
Not all industry verticals are the same

All operational asset owners and operators focus on core values such as safety, reliability, and availability. However, certain verticals/industries may have specific regulations to follow. For example, The North American Electric Reliability Corporation Critical Infrastructure Protection (NERC-CIP) is a set of standards designed to regulate, enforce, monitor, and manage the security of the Bulk Electric System (BES) in North America. The NERC-CIP calls out several areas of securing remote access, including identity, secure communications, access management, monitoring, and accountability that organizations in this space must adhere to.

In addition, factors such as productivity and efficiency will also play a role depending on the industry, as results can vary dramatically depending on the industry vertical. For example, in the two biggest verticals, manufacturing and Oil & Gas (O&G), there are distinct differences between the forces driving connectivity.

For instance, if we look at manufacturing, the main reasons to connect are **allowing third-party access** and **data collection,** which are equal at 26% each. Meanwhile, the top reason for O&G is **allowing third-party access** (33%), with **increased productivity** coming in second (28%). While there are some strong similarities between these two verticals/industries, there are also substantial differences.

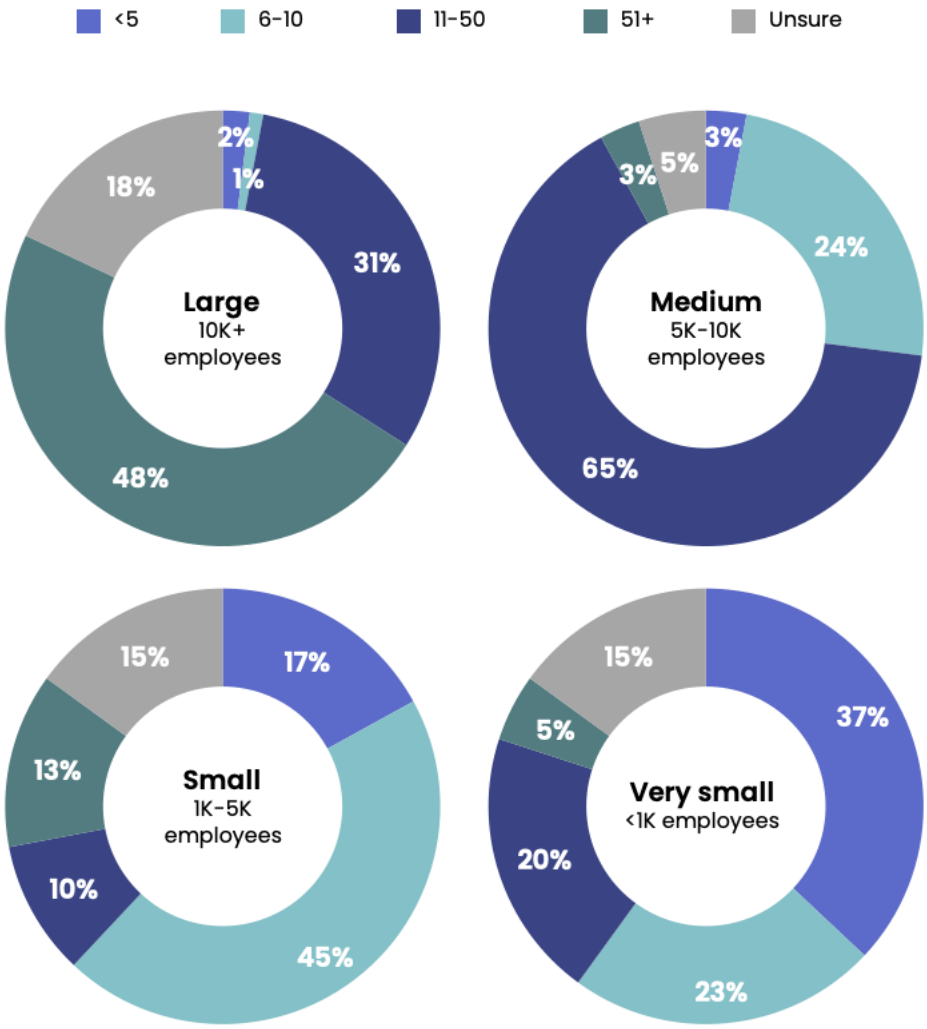
Such differences include each organization's business context, as well as various industrial, regional, and company-specific factors. Factors that influence operations include regulations, labor availability/cost, and the utilization of operational data for productivity and safety enhancement.



How many people are remotely connecting to OT environments?

We asked respondents to gauge how active the remote workforce is. The number of remote users (employees and contractors) is proportional to the company's size. In general, the larger the company, the more people who connect. However, regardless of company size, it is clear that there is a need to connect.

No. of users connect to your OT/ICS environment per day

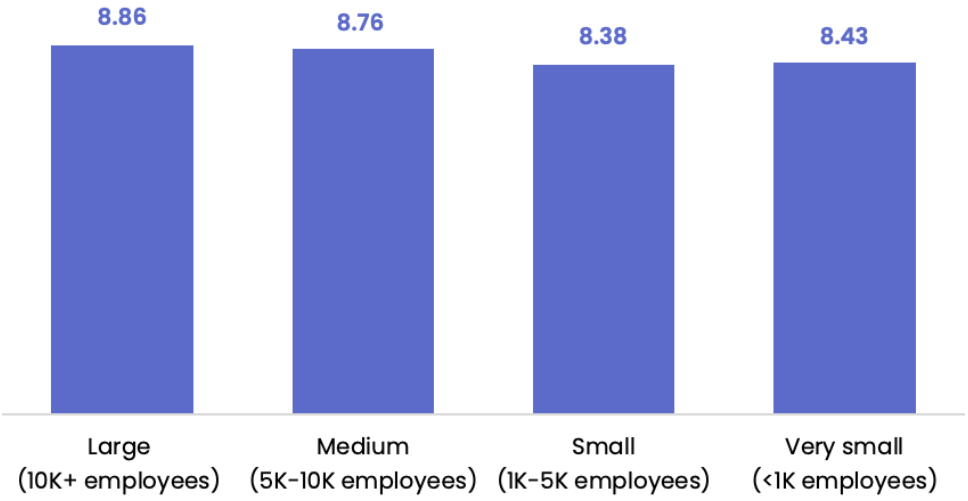


Secure remote access is not just a big company problem

It is apparent that there is a somewhat linear relationship between the company size and the number of remote connections. These numbers can mislead readers into thinking that the need for secure remote access solutions is only a big company issue. However, further analysis reveals that the level of concern

regarding threats associated with remote access is surprisingly consistent from the smallest (8.43) to the largest companies (8.86).

Concern about remote access threats to OT/ICS systems



If anything, larger companies often have more resources and skilled professionals focused on cybersecurity. Meanwhile, smaller companies that may struggle with budget and experience actually need more external assistance due to this very lack of skills internally.

What are the main objectives for Securing Industrial Remote Access?

For decades, control system asset owners/operators acquired their security from a very small set of people who knew how to build, manage, or manipulate various OT/ICS systems. Overall, the knowledge needed to cause real damage to such systems was limited. What has changed in more recent years is that system vulnerabilities and documentation are now easily accessible in the public domain, and critical systems are more frequently coming under attack.

As a result, the main objective for securing remote access is to **lower the risk that such access poses to the effectiveness of the operational systems.** However, in many industries, the teams responsible for security are unaware of all the internal and external remote users or backdoors in place for access. Likewise, the lack of session monitoring or recording solutions means that unauthorized users or malicious insiders can manipulate the OT systems from within.

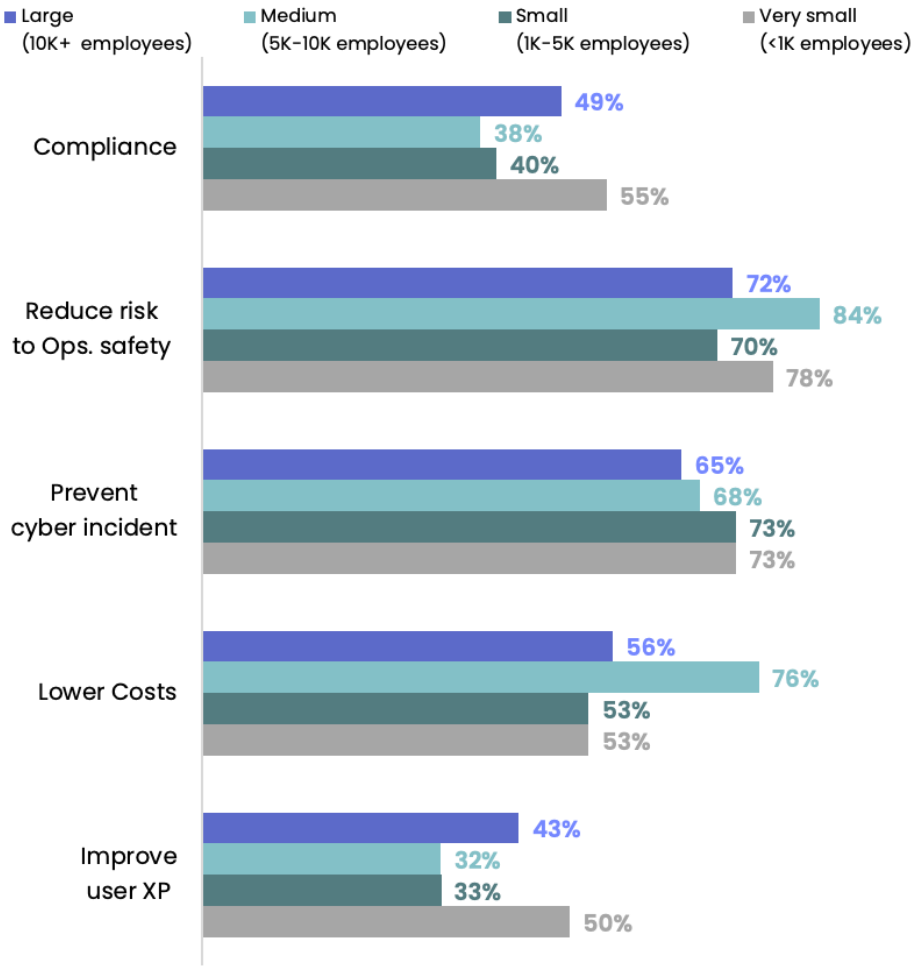
According to the MITRE ATT&CK knowledge base, adversaries have several ways to gain access using remote methods. For example, they can exploit software vulnerabilities in public-facing applications and remote services, as well as

internet-accessible devices that do not have adequate protection. They can also impersonate users and systems by capturing valid credentials and using them freely. Once inside, adversaries can leverage remote services to move between OT assets and network segments, just like authorized operators and vendors do.

Following the lowering of risk, the second most common objective for using SRA is to **prevent cyber incidents and the proliferation of ransomware.** In cases where devices are directly accessible to the internet, this is a valid concern, as ransomware is one of the most common causes of service/production interruption.

The third objective is to **lower the cost of maintenance and support.** While this is more associated with efficiency than security, it is nonetheless a valid concern, as remote access means less need for costly travel and more skills available to remote sites, etc.

Primary objectives to achieve from securing the access



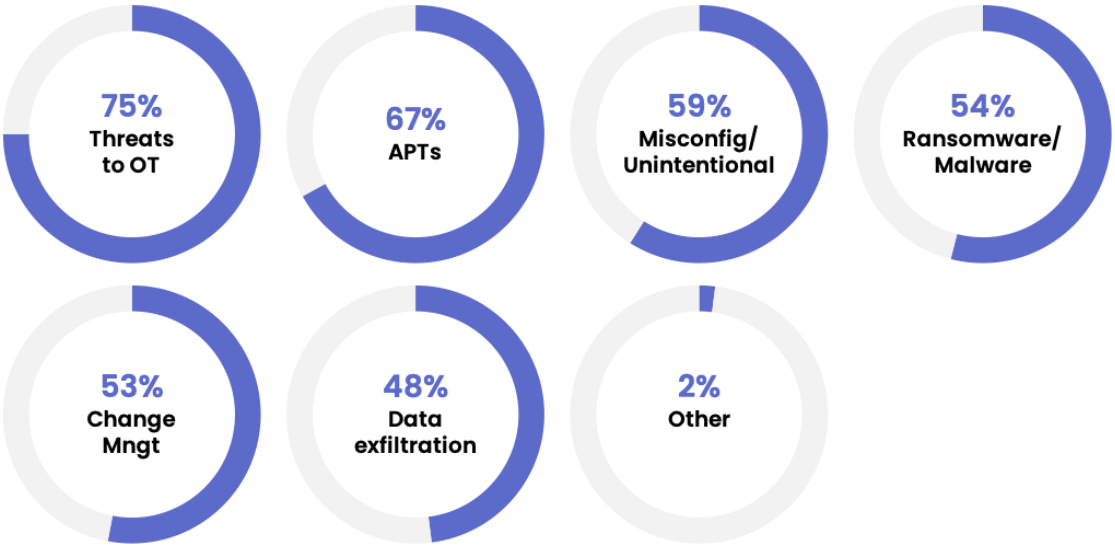
When we take a closer look at the primary objectives for wanting to strengthen secure remote access, they are similar across the board, for both smaller and

larger companies (with the exception of compliance). It is important to note that larger companies often have to adhere to specific regulations or need to self-regulate, which does not always apply to smaller companies.

What are the "biggest risks" associated with remote access?

Despite the relative consistency across company size, it is evident once again that the objectives and risks associated with remote access vary over both verticals and geographies. For example, the concerns of a water and waste facility in North America may be very different from that of a pharma manufacturer in Europe.

The Biggest Risks



What are companies doing today to minimize these risks?

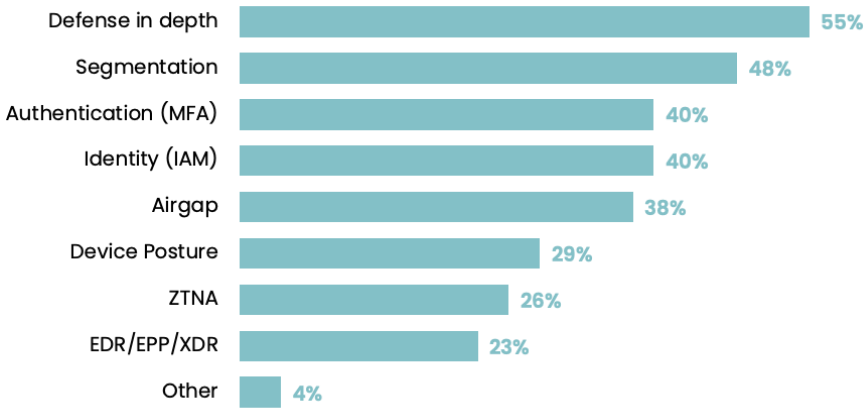
According to survey respondents, the top two implemented solutions are **defense in depth** and **network segmentation,** respectively. Meanwhile, some IT-originating solutions are also popular, with **multi-factor authentication (MFA)** leading this sub-category and coming in third place overall. It is worth noting that MFA is in fact a very effective method for blocking unauthorized access; however, many of the legacy systems that characterize OT environments do not have the modern infrastructure required to support MFA, limiting its ability to help enhance secure access if accommodations cannot be made.

Interestingly, traditional **airgrapping** comes further down the list; perhaps this is because accelerating IT/OT convergence has opened many environments that were previously airgapped or otherwise isolated. And, according to our research,

zero trust appears to be seen as both an "overlay" to enhance the maturity of existing methods as well as a complete new approach to I-SRA.

Finally, more **IT-type endpoint solutions** come in last, which is not too surprising considering the difficulty of deploying and updating these types of solutions in the industrial environment.

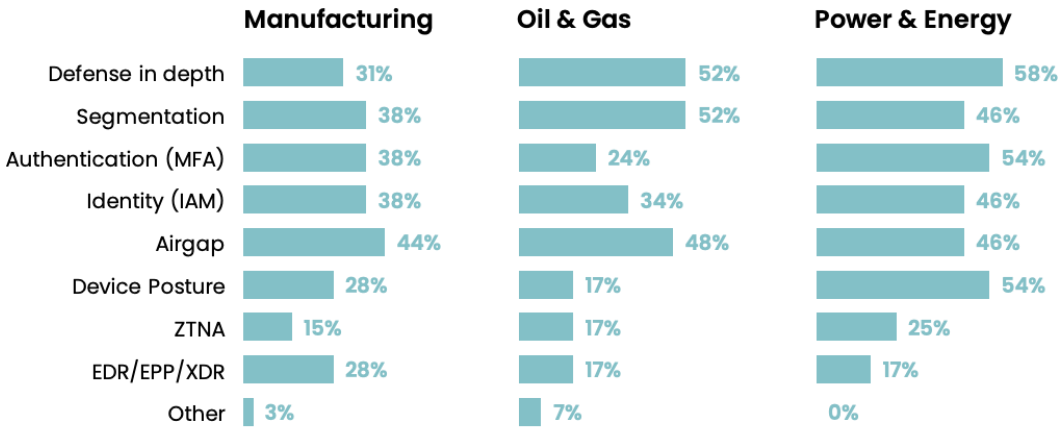
Solutions implemented

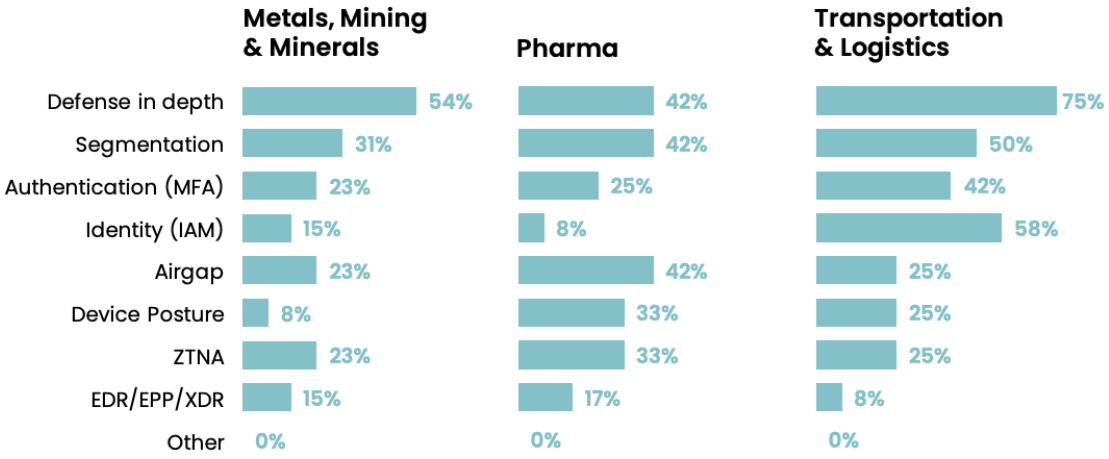


Once again, it is interesting to see and compare the breakdown of solutions implemented by both vertical and geography. For example, **while defense in depth** is common across geographies, **zero-trust** adoption varies significantly across regions, as it is a relatively new concept in the OT environment.

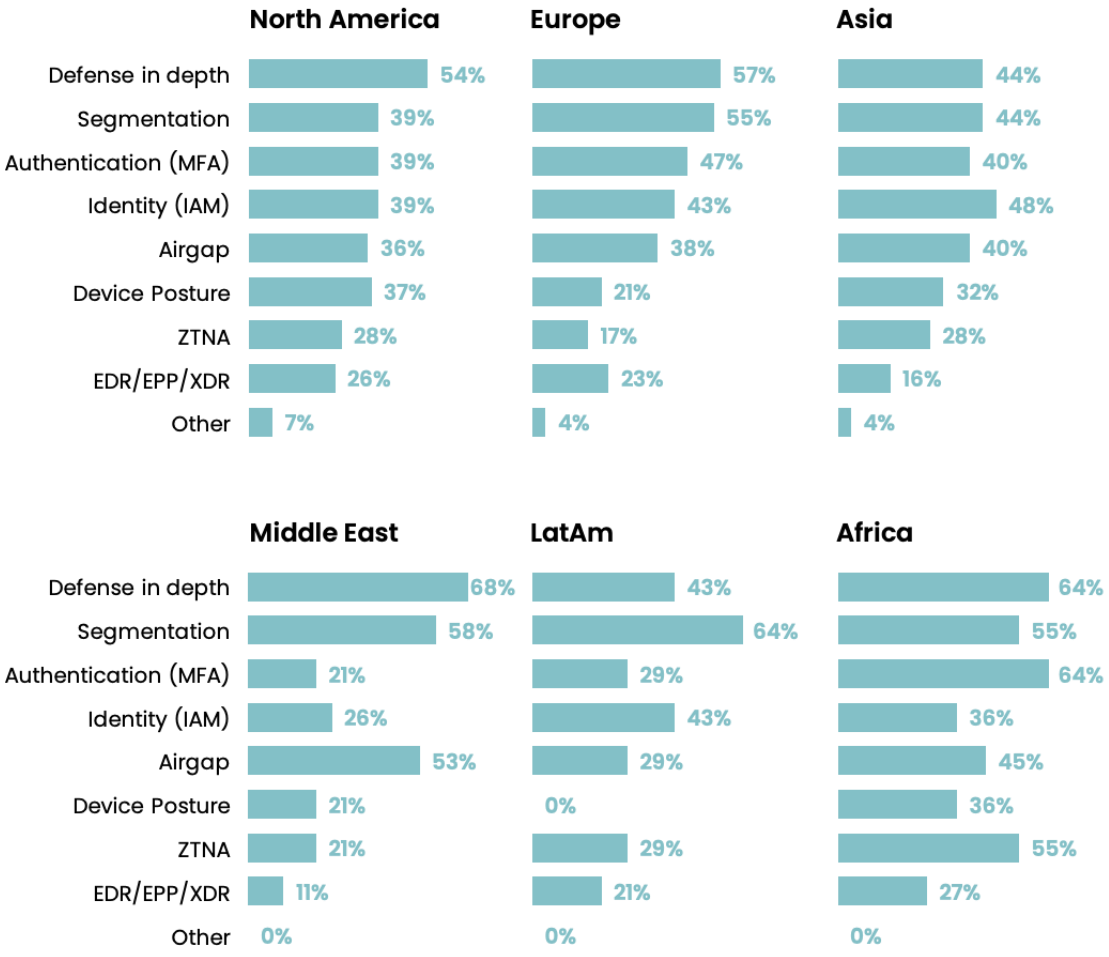
Similarly, **network segmentation** is common across most verticals, but endpoint detection and response (**EDR**) is less so. With that being said, **EDR** achieved its greatest popularity at 30% in the healthcare and life sciences sector. This is possibly due to the closer interaction between IT/OT/IoT in such environments.

By Vertical: (Top 6 verticals)



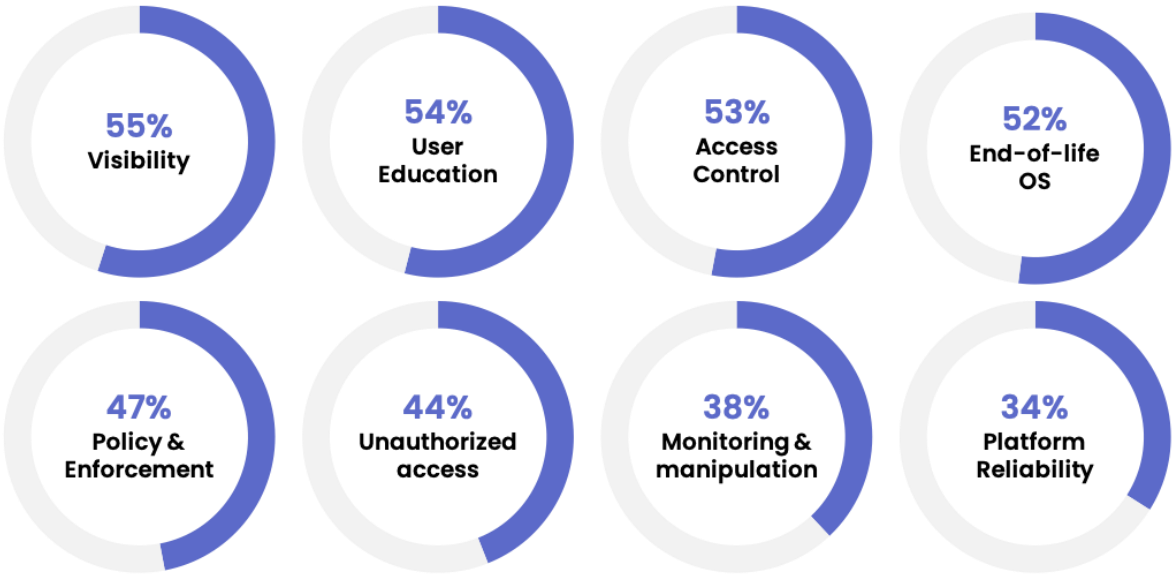


By Region:



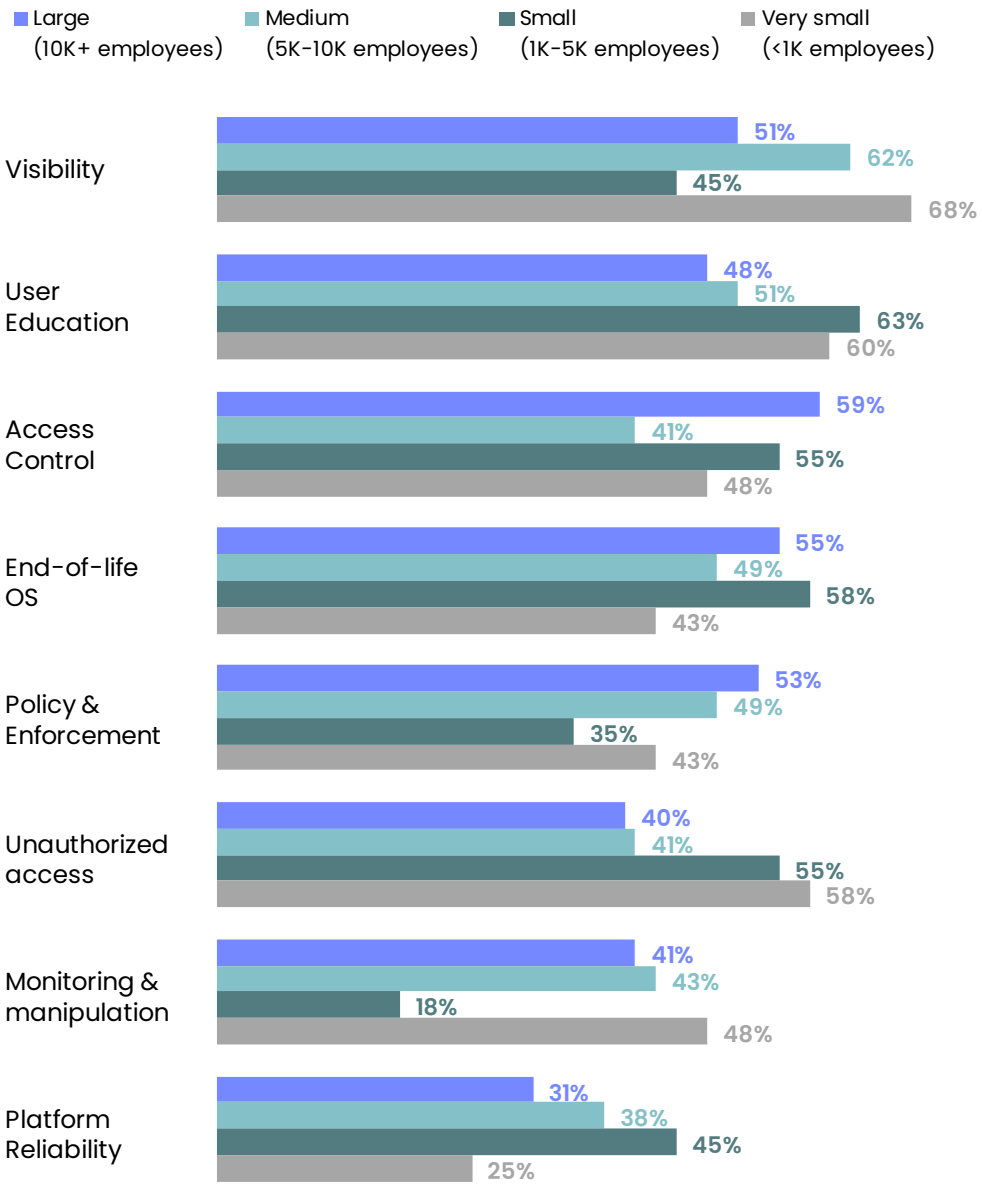
Some concerns remain:

Exposure concerns



The top four concerns all received more than 50%, with first and second place being **lack of visibility** and **insufficient user education,** respectively — both of which are to be expected. Third and fourth are the **weak access control** and **outdated operating systems,** respectively which both point towards more systemic and cross-domain concerns. It is also encouraging to see that operational concerns relating to people and processes are being addressed, rather than just relying on technology fixes.

Top concerns by industry

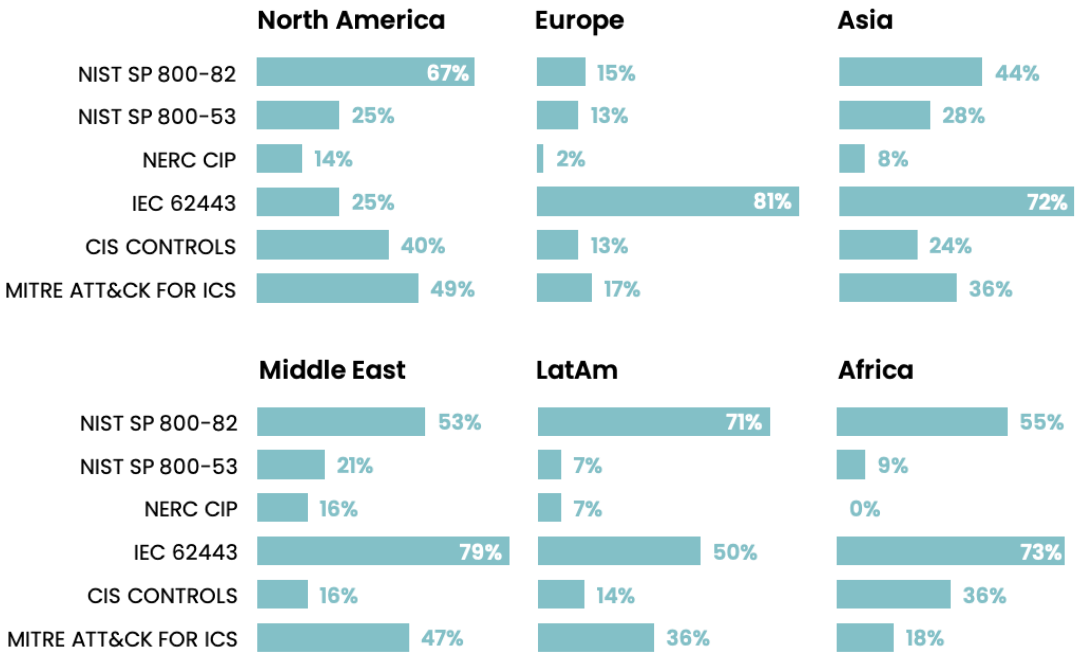


Interestingly, in this instance, concerns differ depending on the size of the company. For smaller companies, the main concerns are a **lack of visibility** and **insufficient user education.** Meanwhile, **weak access control** and **weak policy enforcement** top the list among larger companies. This could mean that by lacking the budget for the latest tools and solutions, smaller companies depend more on their users to maintain strong security hygiene to prevent threats.

Which cybersecurity standards/frameworks does your organization align with?

Regulated industries are required by governments to comply with specific cybersecurity and other regulations. Meanwhile, non-regulated industries are strongly advised to align their cybersecurity programs with industry standards or frameworks. While compliance is voluntary in the latter case, once adopted, the I-SRA project should follow suit and align with the framework requirements.

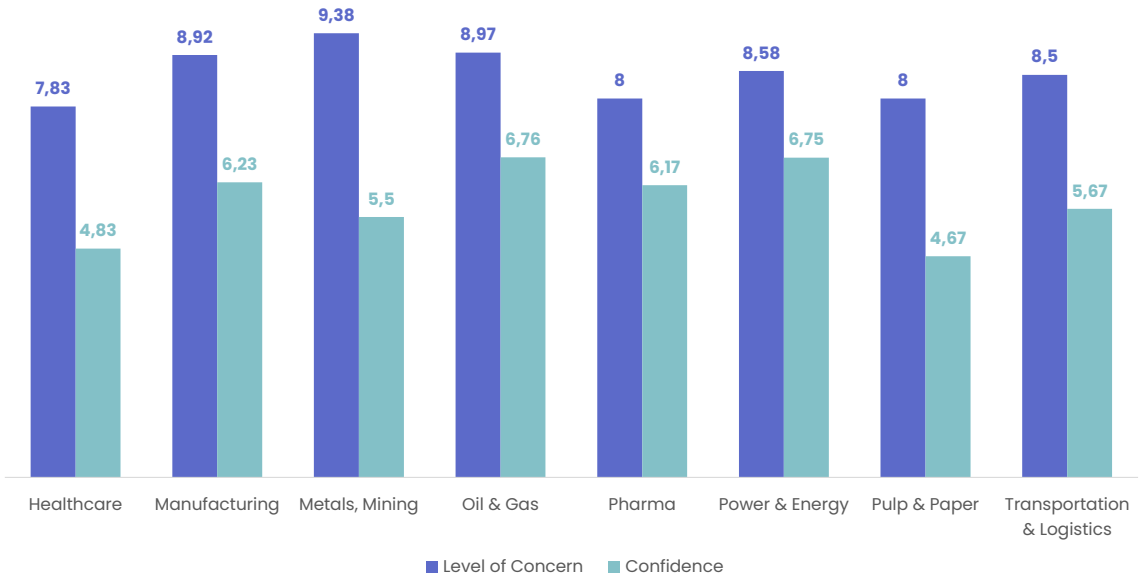
The adoption of standards and frameworks (both regulated and non-regulated) tend to be regional and typically consist of a choice between **NIST 800-82** or **IEC62443.** In addition, some cross-regions support **MITRE ATT&CK** and **CIS control.**



The reality of I-SRA in practice

One of the most significant findings of our survey is the lack of confidence many industries have in their current I-SRA solutions and their ability to minimize the risks associated with remote access.

As we can see in the graph below, there is a significant gap across the board between the **level of concern** vs. **the level of confidence in solutions.** This reveals that while more companies are focusing on improving their remote access security and have in many cases identified the risks, they are aware that more action is needed to further reduce such risks.



Conclusion: Industrial Secure Remote Access is a Journey

Remote access is essential for keeping OT environments around the world running, and this automatically creates a set of risks that must be mitigated, monitored, and managed. Industrial Secure Remote Access is a journey that will continue to present new obstacles and drive new technologies to overcome them. The lack of confidence respondents have in their current remote access solutions highlights the ongoing challenge and illustrates that many organizations may still be at the beginning of their journeys to ensure secure remote access. Equally clear is that new technologies and approaches, ideally ones that are purpose-built to meet the requirements of OT/ICS environments, are needed to establish stronger trust in I-SRA solutions and secure remote access overall.

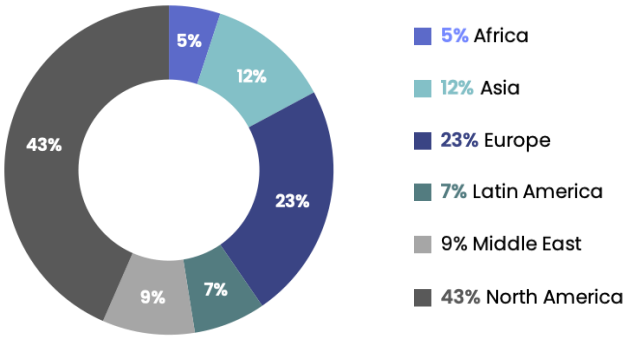
We must also keep in mind that the OT environment contains many devices with levels of security that are far below devices in the IT domain. Improving secure remote access implementation is a proven way to protect these minimally-secured assets from misuse or attack, and is vital to advancing overall cybersecurity posture.

Methodology

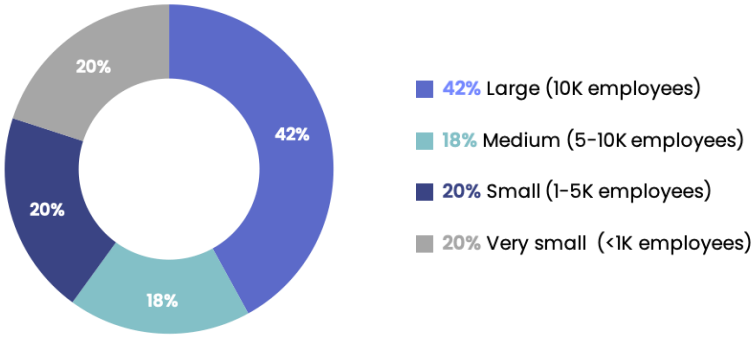
The findings in this report were derived from a Q1 2023 industry survey designed and conducted by TP Research 203 OT, engineering, cybersecurity, and IT professionals. The respondents come from a diverse range of geographies,

industries, and organizations — predominantly industrial asset owners and operators.

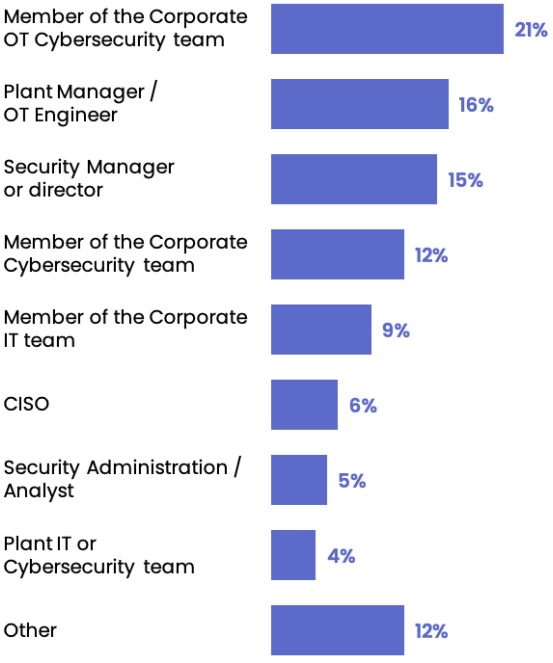
Regions

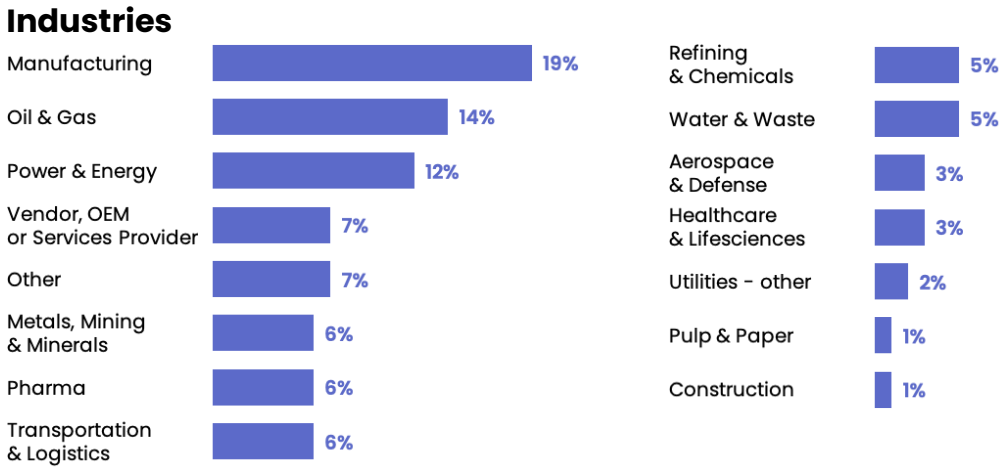


Org size



Roles





About TP Research

Takepoint Research (TPR) is a boutique industry analyst firm that provides focused research and actionable insight for industrial enterprises and those tasked with protecting them from cyber threats. TPR resources and analysis help them make informed decisions about evolving their industrial cybersecurity programs to meet the changing threat landscape. Collaboration is at the heart of our model and our mission is simply to deliver expert insight that has tangible value for your company.

About Cyolo

Too many critical assets and systems remain exposed because traditional secure access solutions are unable to protect the high-risk access scenarios and legacy applications that power modern business operations. Founded by a former manufacturing industry CISO and two ethical hackers, Cyolo was created to solve the challenge of securely connecting high-risk users, including remote workers and third-party contractors, to mission-critical applications within every kind of environment (on-premises, on IaaS platforms, and hybrid).

Cyolo is setting a new standard for secure remote access by providing the only trustless zero-trust access solution and giving organizations visibility and access control over the users who leave them most exposed to risk.

To learn more, visit cyolo.io or reach out to contact@cyolo.io.