2024 State of Industrial Networking Report

A global view of the evolution of operational technology and its impact on security, IT, and future innovation.

Introduction

More than 1,000 respondents participated in the 2024 State of Industrial Networking Report.

This, the inaugural edition, reveals how firms operating in industrial sectors worldwide are designing and deploying their operational technology estate to improve security, increase efficiency and provide a platform for innovation. We spoke to decision-makers at firms in 17 countries, operating in more than 20 sectors including manufacturing, utilities, energy, and transportation.

The report aggregates findings from management to the C-suite at companies with annual revenues of over $100 million. We examine nuances by region and company size, and delve into respondents' most pressing concerns.

Cisco, in association with Sapio Research, commissioned this double-blind study to establish the highest business and technical priorities for industrial networks today: to reveal how global organizations are overcoming challenges, where the opportunities lie, and how to align resources for success.

Executive Summary

Cybersecurity is top concern

Cybersecurity is the biggest reported challenge in running and maintaining industrial networks. The requirements of Industry 4.0, a backlog of legacy systems and assets, an expanding attack surface, and an overstretched workforce are exacerbating the problem.

- Cybersecurity risks are the **#1 internal barrier to growth**
- **89% say cybersecurity compliance is very important** in their operational network
- **The #1 challenge when running industrial infrastructure** is mitigating against cyber threats

IT and OT teams must become more collaborative

The management of organizations' enterprise and industrial networks is increasingly overlapping. Executive leadership can see the benefits of a unified approach, but currently the two functions are still siloed; impacting efficiency and threatening the overall security posture.

- 41% of firms' IT and OT teams are **working independently on cybersecurity**
- Organizations believe the #1 outcome of **better collaboration** would be **improved cybersecurity**
- 92% of executive leaders and C-suite believe there is **significant value in having a unified cybersecurity solution**

AI is driving an infrastructure refresh cycle

There is a clear sense that AI will boost business growth for those who can successfully use it to run better industrial networks. Leaders will ensure their operational technology is capable of capturing the data required to fuel AI models.

- 48% believe AI is the emerging technology **likely to have the biggest impact** within the next five years
- AI is the #2 **spending priority** in the next two years (after cybersecurity)
- Almost half (49%) expect AI to **improve network management** across IT and OT

Table of Contents

Introduction Letter

I'm happy to introduce Cisco's inaugural 2024 State of Industrial Networking Report.

Operational technology, and specifically the network supporting industrial operations, has become a key differentiator for organizations globally, across a wide range of industries including manufacturing, utilities, and transportation. In short, the network has never been more important.

The 2024 State of Industrial Networking Report is unique in that it captures the views and insights from over 1,000 operational leaders, across 17 countries and 20 industries. While the potential of industrial transformation is clear, the report highlights some of the most critical networking challenges organizations face today, including cybersecurity, IT/OT collaboration, and the adoption of AI.

At Cisco, we've been delivering solutions for both IT and OT networks for decades, creating a unified solution that delivers operational simplicity and security at the scale needed for industrial networking.

Listening to our customers is the highest priority for Cisco, and this year's survey produced some deep insights on what's top of mind.

Our hope is that this report, summarizing feedback from such a broad and diverse set of industrial leaders, will provide you with context and benchmarks as you navigate your strategy, decision making, and partnerships in the coming year.

Together with our customers, we've witnessed exceptional business outcomes and competitive advantages delivered through operational network modernization.

We hope you find the report as valuable and informative as we have.

Vikas Butaney

Senior Vice President, General Manager
Cisco Networking – SD-WAN, Multicloud, and Industrial IoT

Section 1

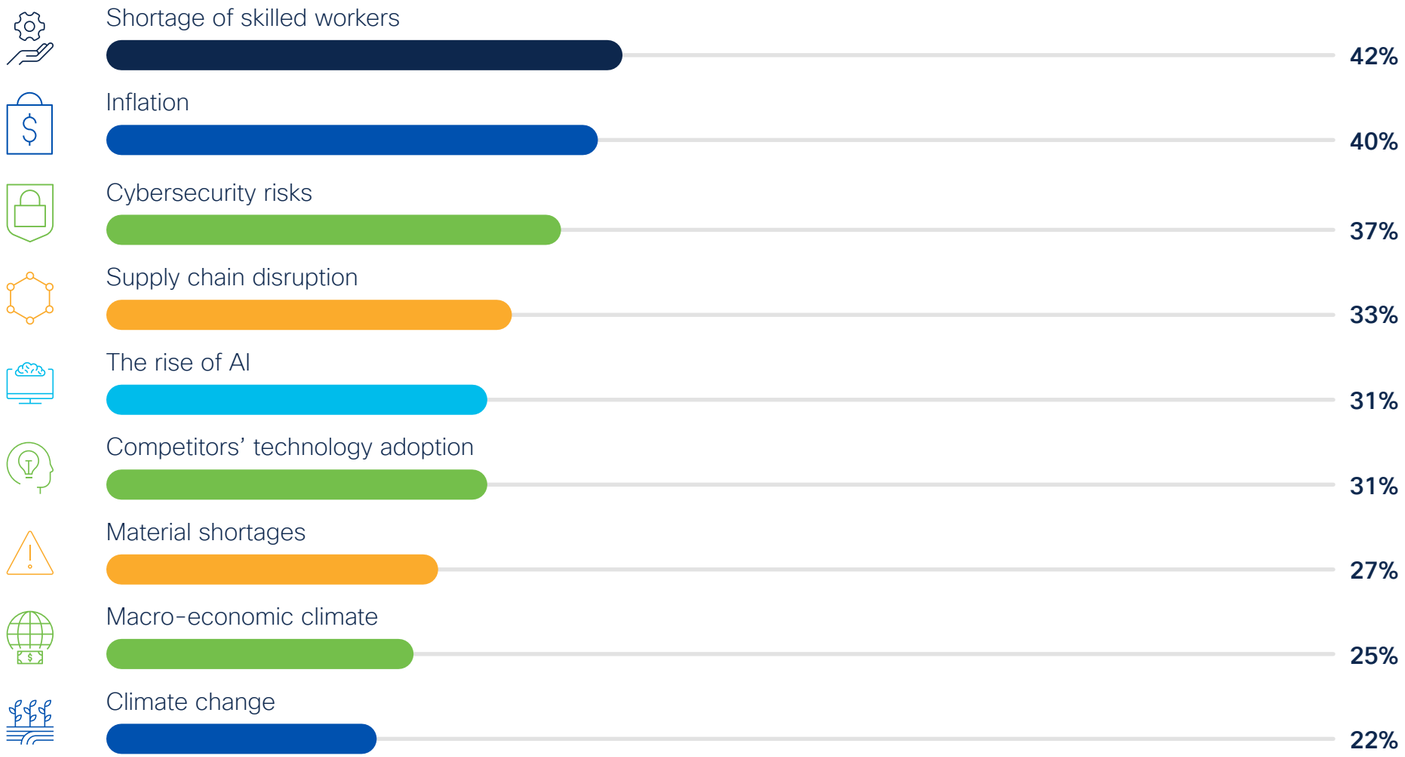
The current state of industrial networking

Skills shortages, the impact of inflation and cybersecurity risks are impacting firms' ability to grow. To overcome these barriers, organizations are doubling down on investment in operational technology, while prioritizing a focus on upskilling, improving collaboration, and introducing AI.

Industry obstacles to growth: external

Over the past few years, businesses worldwide have faced macro-level challenges ranging from supply chain issues to a global pandemic. But what are the top issues hampering growth in industrial sectors today?

The number one concern—cited by 42% of respondents—is a shortage of skilled workers, closely followed by inflation (40%) and cybersecurity risks (37%). These are global issues: our analysis uncovered minimal regional variations.



Q. What do you believe are the biggest external obstacles to your organization's growth? Select all that apply

> Even with some recent cooling, the labor market remains tight, and the resulting applicant gap may continue. This could impact the ability of manufacturers to fully capitalize on [the] recent growth in public and private investment.
>
> The net need for new employees in manufacturing could be around 3.8 million between 2024 and 2033. And, around half of these open jobs (1.9 million) could remain unfilled if manufacturers are not able to address the skills gap and the applicant gap.
>
> 'Taking charge: Manufacturers support growth with active workforce strategies,' **Deloitte**[1]

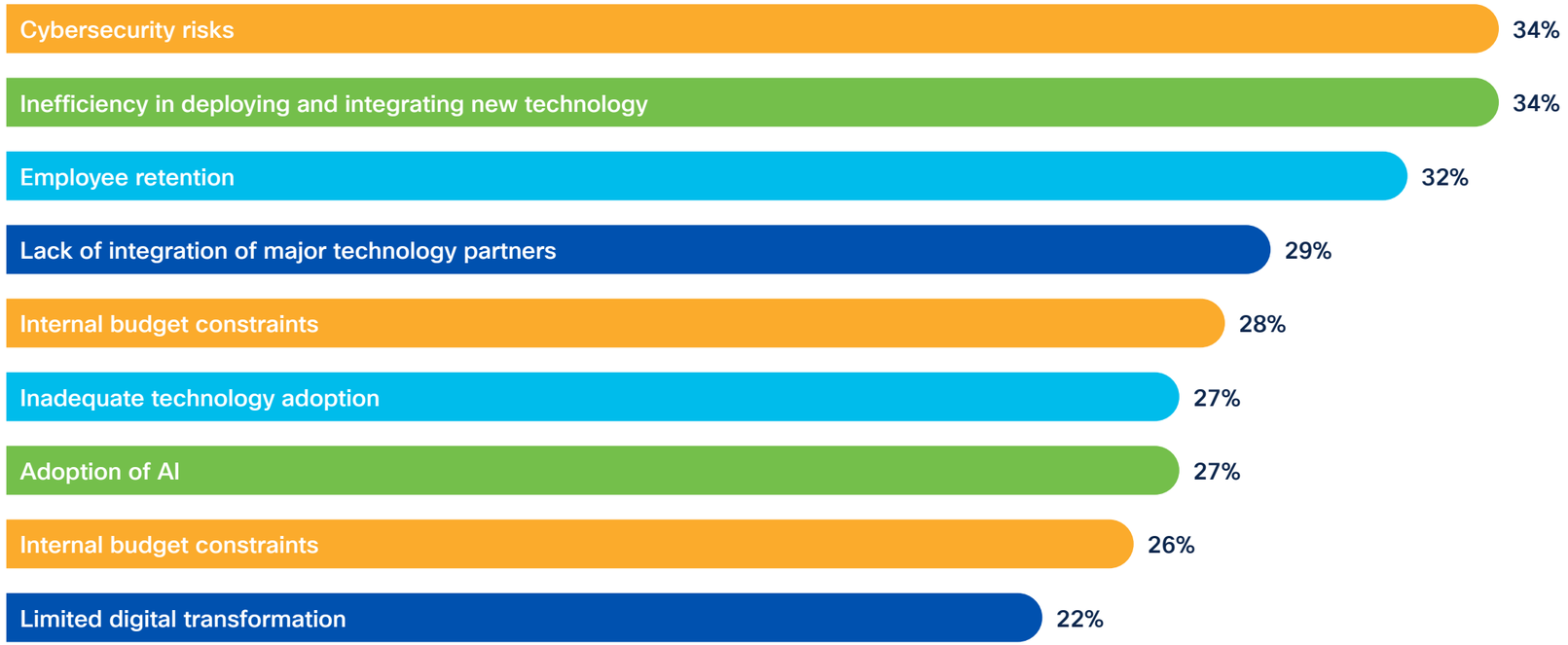
1 https://www2.deloitte.com/us/en/insights/industry/manufacturing/supporting-us-manufacturing-growth-amid-workforce-challenges.html

Industry obstacles to growth: internal

Compounding the external factors are issues within organizations which hamper progress. Again, we see businesses struggling with cybersecurity risks (#1) and workforce challenges–namely employee retention (#3); alongside a lack of efficiency when deploying new technology (#2).

These barriers are primarily operational, rather than technical: representing human factors such as resistance to change which can lead to difficulties upskilling and retaining a fit-for-purpose workforce.

Market maturity and distribution of skills impact regional results. Retaining employees is proving particularly hard for North American firms, who rated it their top internal obstacle; while inefficiency in deploying technology is the biggest problem for organizations in APAC.



In spite of the impact of inflation, **74% of businesses say growth is not being impacted by budget constraints;** suggesting a recognition that investment must be made in order to capture opportunities and remain competitive.

Q. What do you believe are the biggest internal obstacles to your organization's growth? Select all that apply

Training and collaboration mitigate risks

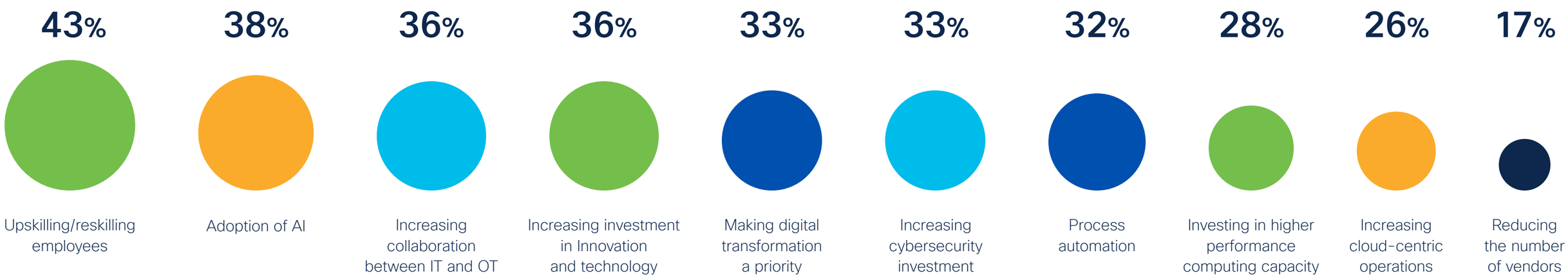
Technology is seen as an enabler of, rather than an alternative to, the workforce by firms operating in industrial sectors.

The top way these organizations are mitigating against the internal obstacles they face is through upskilling or reskilling their employees; followed by adopting AI, which can reduce manual tasks and speed up processes.

Importantly, **more than a third of respondents (36%) say they are increasing collaboration between information technology (IT) and operational technology (OT) teams.** Aligning potentially siloed functions will be crucial to overcome organizations' reported technology deployment inefficiencies and cybersecurity risks.

83%

have no plans to reduce the number of vendors they work with, indicating a preference to optimize existing technology rather than attempt to shed and consolidate platforms.



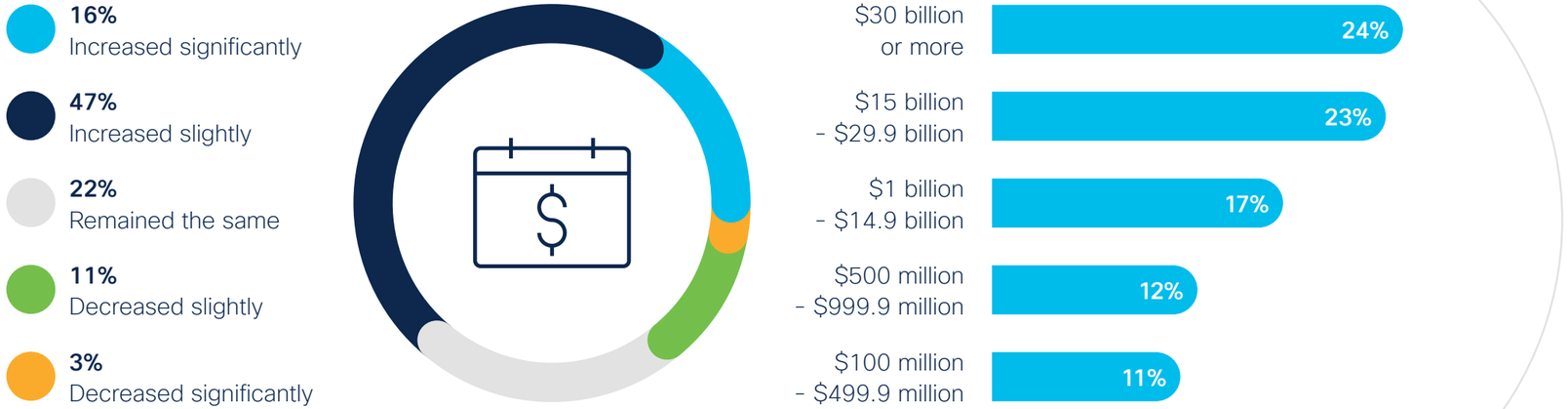
Q. How is your organization mitigating these internal obstacles? Select all that apply

Majority increase investment in OT

Organizations worldwide are recognizing the need to invest more in operational technology in order to capitalize on the opportunities offered by Industry 4.0.

Almost two-thirds (63%) of respondents have ramped up spend on industrial infrastructure over the past year.

Of these, **16% spent significantly more than last year—with that figure rising to nearly a quarter (24%) of the largest businesses in our survey:** those with revenues of over $30bn.



Q. How did your industrial / OT infrastructure spend change in the past year? Select one

LATAM (72%) and APAC (67%) saw the highest investment increases of the four regions in our survey.

The presence here of emerging markets could account for the larger increases, as firms attempt to close the gap to more developed markets, and to benefit from the investment opportunities these regions represent. However, no region is exempt from investment increases, with 59% of firms in North America and 60% of those in EMEA spending more than last year. **The highest proportion of those who say the increase is 'significant' (22%) are from North America.**

Firms bolster cybersecurity and AI capabilties

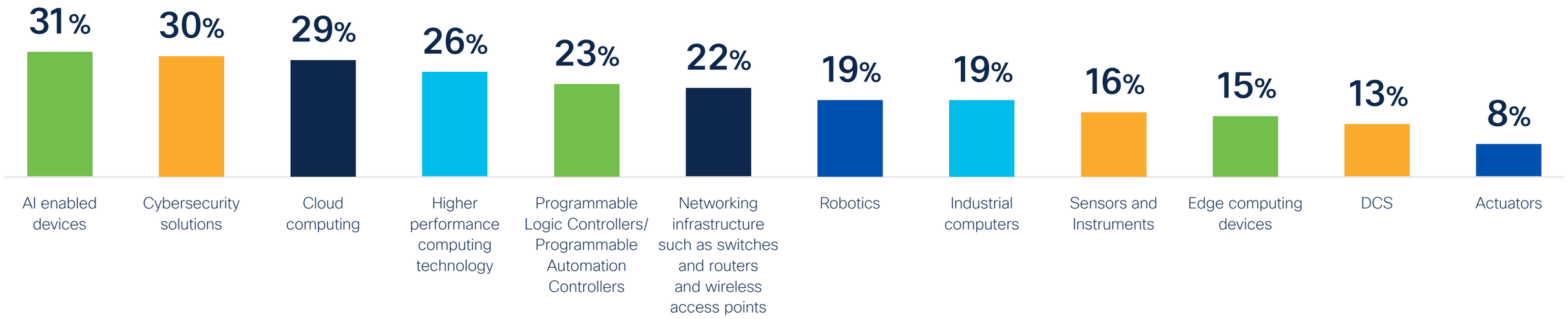
"With recent technology developments, cybersecurity is crucial to an organization's success. Realizing this, companies have been gradually increasing cybersecurity investments. Thus, in 2024, the cybersecurity budget worldwide was forecast to increase to nearly 283 billion U.S. dollars."

Distribution of cyberattacks across worldwide industries in 2023, **Statista**[2]

Industrial organizations are fully aware of their risk from cybercriminals—after all, manufacturing firms suffered the highest share of cyberattacks in 2023[3].

Industrial networking offers a large attack surface via Industrial Internet of Things (IIoT) connected assets. Our findings underline the drive to address this vulnerability, with **cybersecurity reported as the second-highest OT investment area, after AI-enabled devices.**

AI devices may themselves be seen as a double-edged sword. While AI offers OT benefits such as process optimization and threat detection, bad actors are also using adversarial AI techniques to turn the technology against firms.



Q. Which types of industrial/OT infrastructure are receiving the most investment in your organization currently? Select up to three

2 https://www.statista.com/statistics/1315805/cyber-attacks-top-industries-worldwide/
3 https://www.statista.com/statistics/1315805/cyber-attacks-top-industries-worldwide/

Section 2

Challenges & opportunities

The threat posed by cyberattacks in the industrial sector is driving intense focus on identifying and addressing vulnerabilities in operational technology. A closer collaboration between IT and OT teams is sought by those pursuing not only better security, but greater efficiency and competitive advantage.

Firms struggle to keep infrastructure secure

The top challenge for organizations trying to run and maintain industrial infrastructure is cybersecurity: cited by 39% of respondents.

This figure rises to 50% of companies whose revenues exceed $30 billion, suggesting the task of defending against cyberattacks increases as businesses get larger and more complex.

After cybersecurity, the next biggest stumbling blocks all relate to alignment and integration. Firms struggle with a lack of standardization (37%), disparate vendors and partners (36%), and a lack of collaboration with IT colleagues (33%).

1# 39%
Implementing robust cybersecurity measures and mitigating cyber threats

2# 37%
Lack of standardization across industrial infrastructure

3# 36%
Managing multiple vendors, including strategic partners and point solutions

4# 33%
Lack of collaboration and efficiencies with IT

5# 31%
Meeting regulatory compliance requirements

6# 28%
Addressing equipment maintenance and aging infrastructure

7# 25%
Lack of visibility and inventory of connected assets

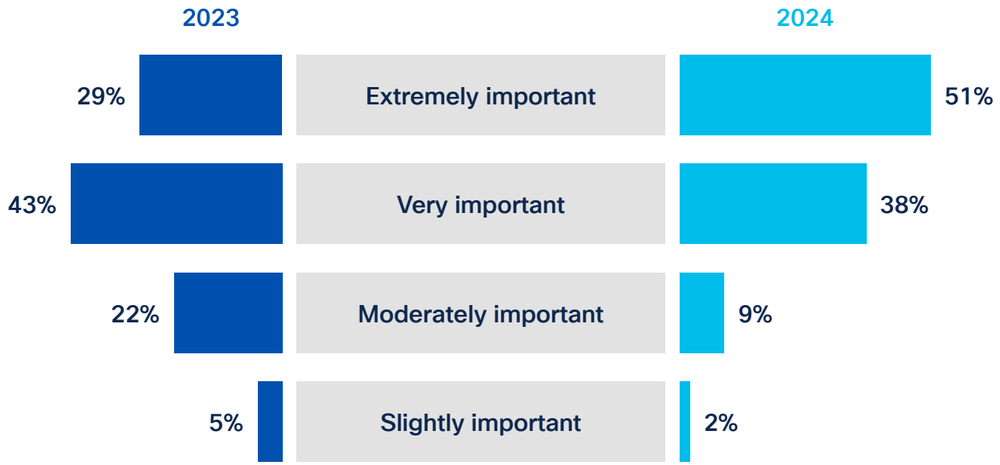
Q. What are the biggest challenges your company faces in the optimal running and maintenance of its industrial infrastructure? Select all that apply

A leap in cybersecurity importance

We've seen elsewhere in this report that cybersecurity is top of mind for those managing operational technology; it features in both the top three internal and external risks, and is the biggest challenge when running industrial infrastructure.

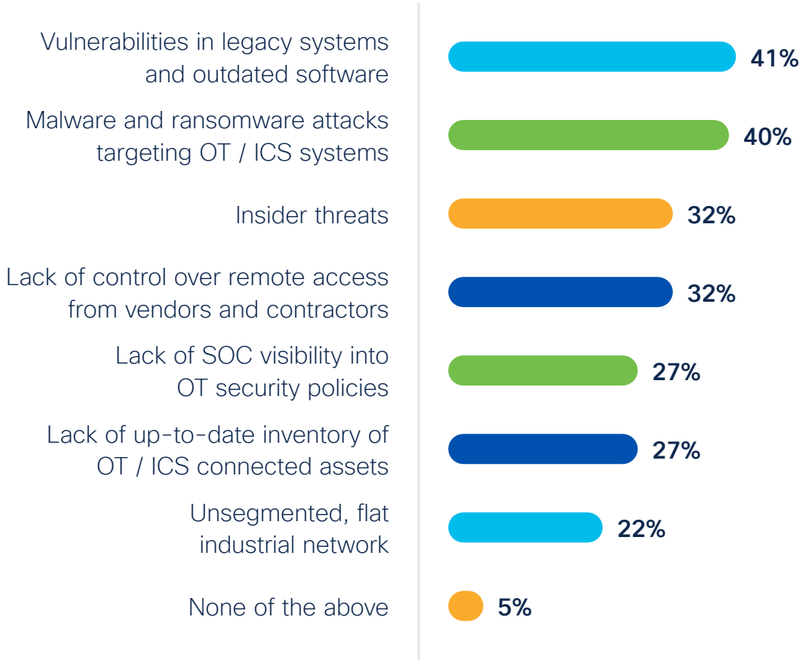
As firms grapple with this problem, the sense of urgency is growing: **22% more firms felt cybersecurity compliance was extremely important in their operational network this year, compared to 2023.**

Overall, 89% of organizations feel cybersecurity compliance is very or extremely important in OT.



Q. How would you describe the importance of cybersecurity compliance in your operational network?

The main problems are **vulnerabilities in legacy systems and outdated software (41%) and malware or ransomware attacks specifically targeting operational technology (40%).**

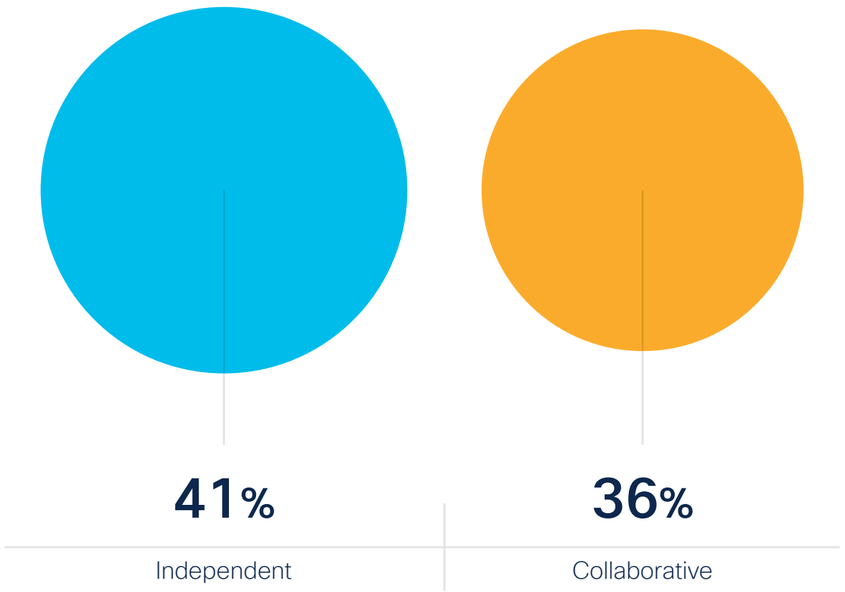


Q. How would you describe the importance of cybersecurity compliance in your operational network?

Collaboration presents cyber opportunities

Within many organizations, the greatest cybersecurity expertise sits within the IT team. Yet our research uncovered **a significant 41% of firms' IT and OT teams are working independently on cybersecurity.**

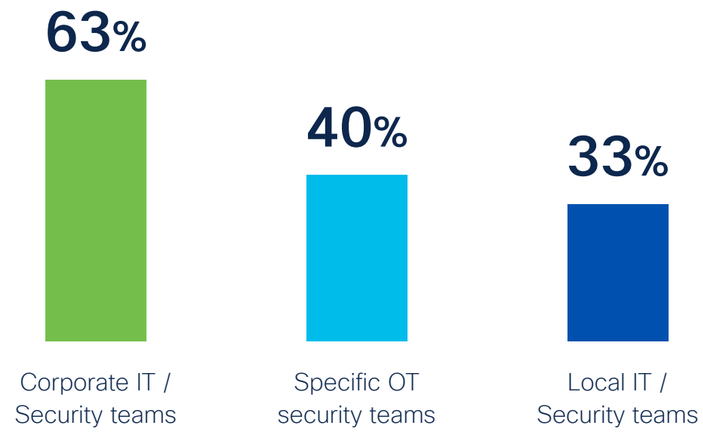
With collaboration paramount to protect quickly and effectively against cybersecurity threats, this represents an action opportunity for many businesses.



Q. How would you describe the importance of cybersecurity compliance in your operational network?

A similar finding emerges when we examine who is leading the industrial cybersecurity practice. While the majority report that corporate IT or security teams lead the way, there is evidence of decentralization in a third of firms. **The 33% whose cybersecurity practice is led by local teams risk inconsistent deployments, issues caused by skill disparities, and limited visibility across the OT estate.**

Organizations in APAC are most likely to have specific OT security teams, while cybersecurity leadership via local teams is more common in LATAM than other regions.



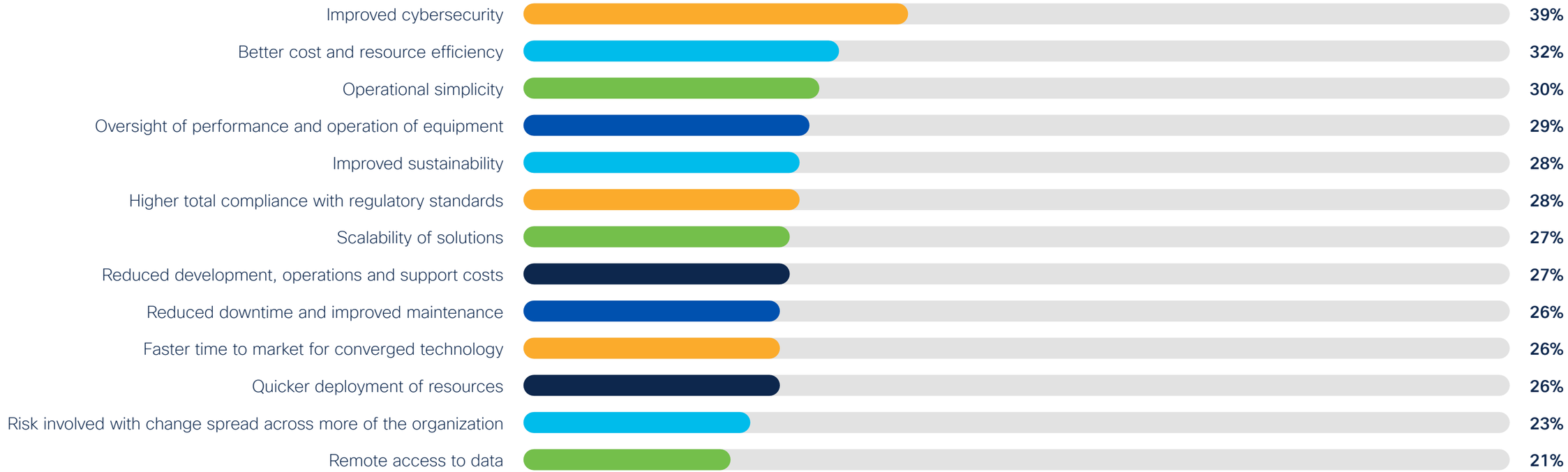
Q. How would you describe the importance of cybersecurity compliance in your operational network?

Firms target better IT/OT alignment

Despite the evidence of siloed working noted earlier in this report, respondents recognize that closer alignment between IT and OT teams would yield important benefits.

Firms believe the #1 outcome of better collaboration would be improved cybersecurity.

Almost a third say it would also bring benefits in terms of cost-effectiveness and efficiency (32%) and simplification of operations (30%).



Q. What do you think are the main benefits of IT and OT collaboration? Select all that apply

C-Suite values a more unified approach

OT decision makers, particularly executive leadership, believe there will be significant value in a consolidated cybersecurity approach right across the business, from the boardroom to the factory floor.

87%

of respondents agreed with the statement, "In the next 2 years, there will be significant value in having a unified cybersecurity solution for both enterprise and industrial networks". This rises to 92% among executive leadership and C-suite.

There is also appreciation of the value IT leadership brings across the business.

84%

of decision-makers (rising to 91% of the C-suite) **agreed that there is growing influence of IT leadership in the decision-making process around operational networking and cybersecurity solutions.**

A recent Ponemon Institute study found that most surveyed organizations lack a unified strategy and sufficient collaboration between IT and OT teams. Though the skill sets of these teams have some overlap, they specialize in unique technologies, and their activities focus on different requirements.[4]

'IT, OT, and ZT: Implementing Zero Trust in Industrial Control Systems,' **Software Engineering Institute, Carnegie Mellon University**

4 https://insights.sei.cmu.edu/blog/it-ot-and-zt-implementing-zero-trust-in-industrial-control-systems/

Section 3

The future of industrial networking

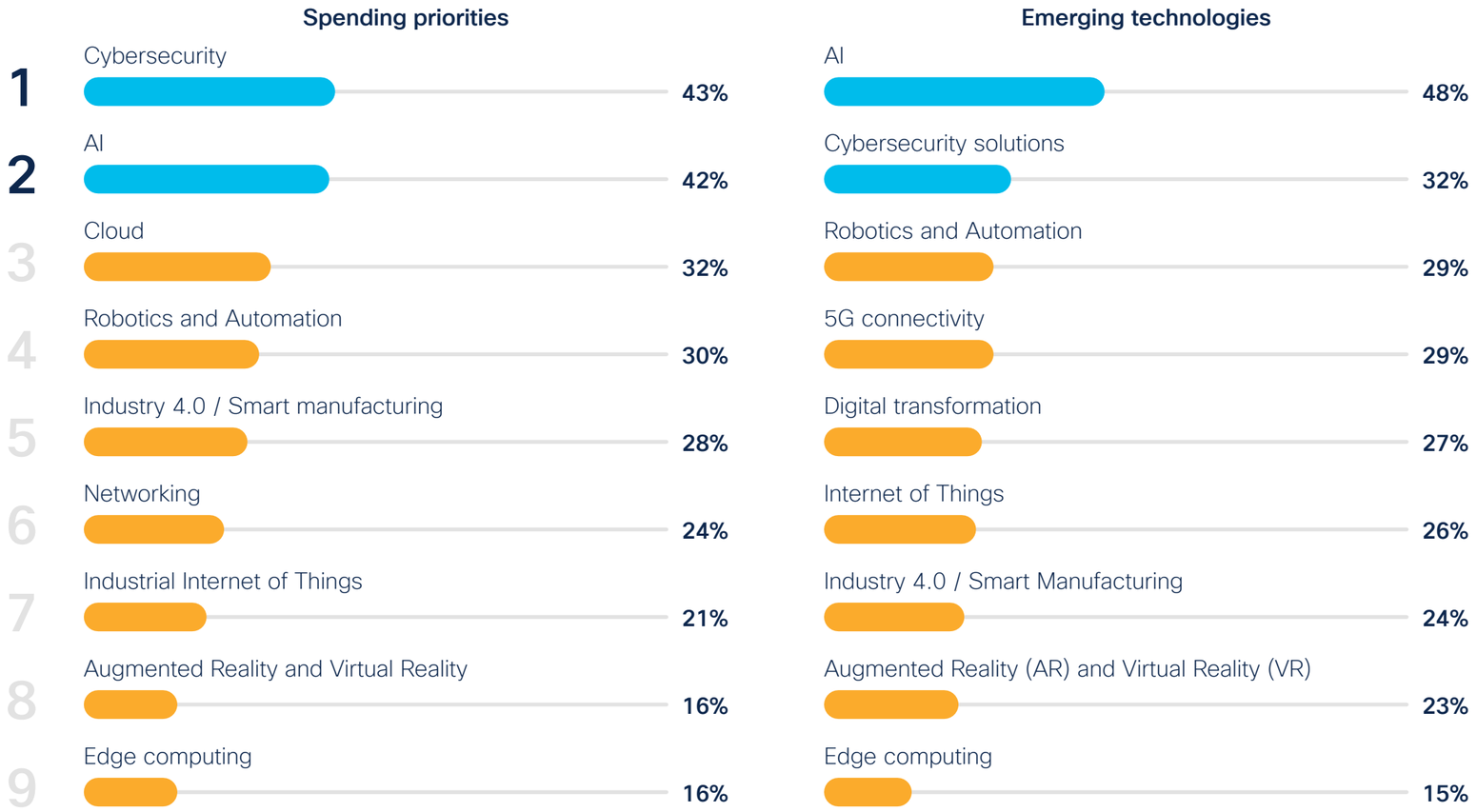
Both AI and cybersecurity are top of mind as operational technology leaders look to the future. Ensuring their infrastructure is futureproofed will be vital for organizations keen to maximize technology investments; as will collecting and analyzing OT data to improve business performance.

Investments planned in AI and security

We've seen that cybersecurity is top of mind for those operating industrial networks today. As we look toward the future, the other topic preoccupying decision-makers is AI.

Almost half (48%) believe AI is the emerging technology likely to have the biggest impact within the next five years, while around a third (32%) cited cybersecurity solutions.

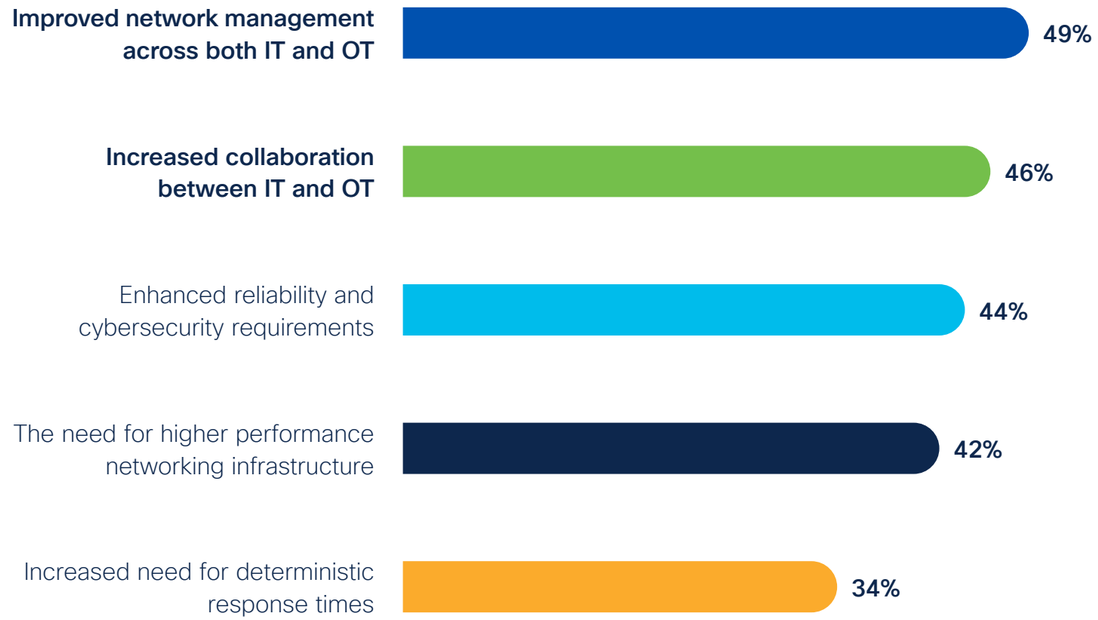
In order to capitalize on the potential of these technologies, firms have also named them the top two spending priorities over the coming two years.



Q. What are your organization's main technology spending priorities for the next 12-24 months? Select up to three
Q. What emerging technologies do you believe will have the most significant impact on industrial networking over the next 5 years? Select up to three

AI expected to improve IT/OT integration

The reasons for planned investment in AI become clear when we understand the expected benefits.



Q. What impact, if any, do you think the deployment of AI will have on industrial networking within your organization? Select all that apply

Not only do around half (49%) anticipate better network management across both IT and OT; a further 46% expect AI to improve collaboration between the two teams.

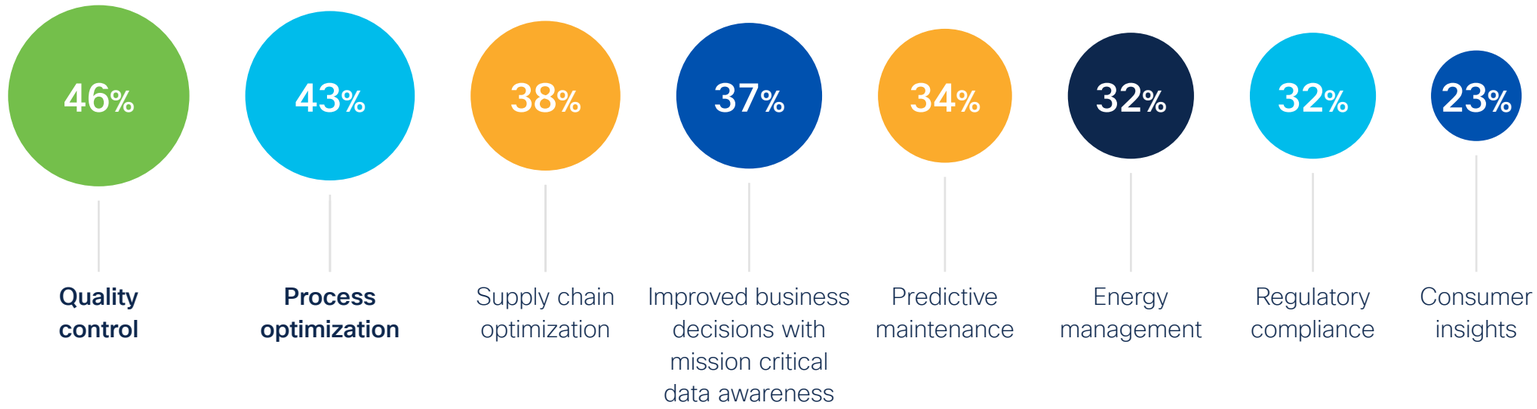
OT data fuels quality and optimization

Integrating OT data with IT systems, such as enterprise resource planning (ERP) and manufacturing execution systems (MES), can create a comprehensive view of the production process.

Those companies who successfully capture and analyze the data from industrial networking will gain a competitive advantage: **46% plan to use OT data to improve quality, while 43% will optimize their processes.**

Rising energy prices have impacted organizations' profitability over the past couple of years. Data gathered from OT provides opportunities to save energy—but not all are harnessing the benefits.

42% of larger companies (more than $30bn revenue) use data for better energy management (42%), compared to fewer than a quarter (25%) of $100 million–$499.9 million revenue companies.

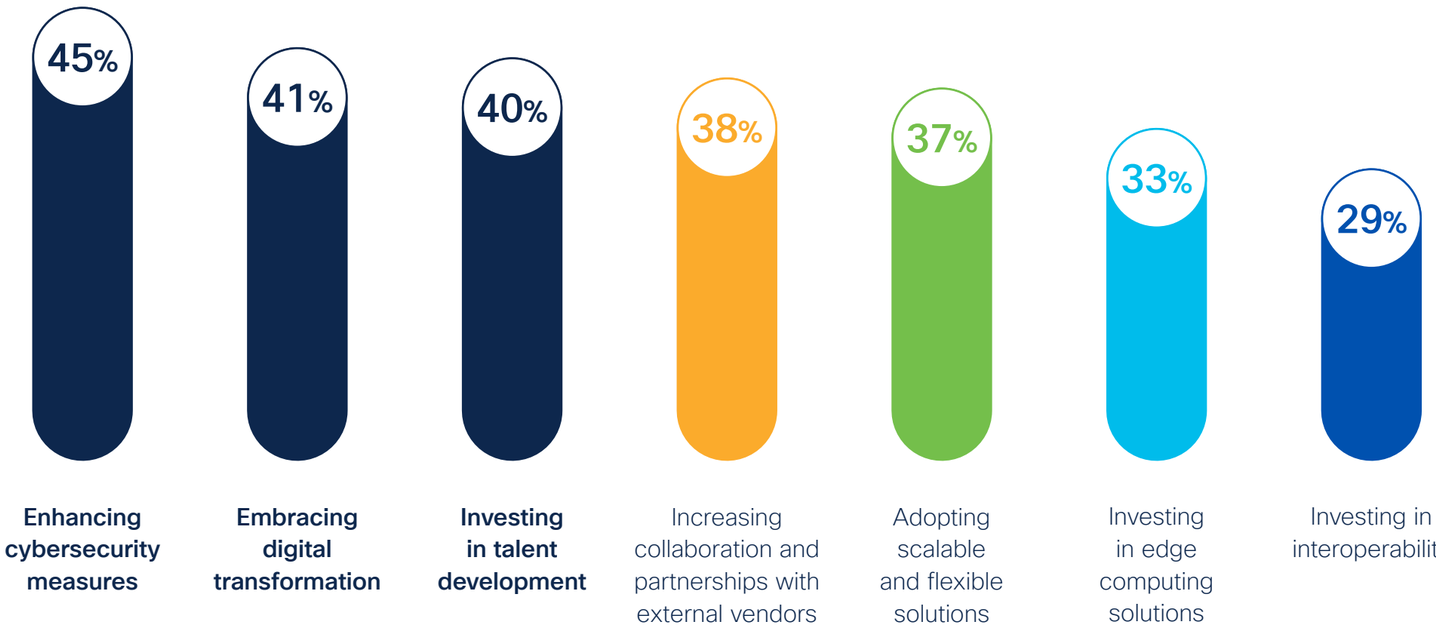


Q. How is your organization leveraging or planning to leverage the data obtained from operational technology (OT)? Select all that apply

Futureproofing through people and tech

In any economic environment—but particularly during a slowdown—investments in new technology must be planned with longevity in mind.

Organizations worldwide are designing measures to **futureproof their OT infrastructure, including enhanced cybersecurity (45%), increased digital transformation (41%), and investment in talent development (40%).**



Q. How is your organization leveraging or planning to leverage the data obtained from operational technology (OT)? Select all that apply

> The world has changed for manufacturers. Preparation for uncertainty has become an industry norm, with executives expecting the impact of disruption—whether from geopolitical tensions, climate change effects, technology breakthroughs, or supply chain vulnerabilities—to increase by 15 to 25 percent over the next five years.[5]
>
> 'Adopting AI at speed and scale: The 4IR push to stay competitive,' **McKinsey & Company**

5 https://www.mckinsey.com/capabilities/operations/our-insights/adopting-ai-at-speed-and-scale-the-4ir-push-to-stay-competitive

Section 4

Conclusion

Key takeaways and partner considerations.

Key takeaways

The industrial operational networking landscape is a place of enormous change and opportunity for those who can overcome its inherent challenges.

1 Prioritize cybersecurity in your OT plans

Organizations who fail to prioritize cybersecurity considerations in their industrial networking strategy will find energy, time, and money absorbed in mitigating against attacks—resources which could be otherwise invested in designing OT as a platform for innovation and growth.

2 Introduce measures to encourage IT/OT collaboration

IT and OT can no longer work in isolation as their skills and domains increasingly overlap. A combination of human and organizational factors, alongside unified technological solutions, will be required to optimize and protect data and assets.

3 Harness AI for competitive advantage

Innovative OT leaders are embracing AI to differentiate their firms; delivering higher quality products quicker. Organizations who fail to refresh their industrial networking infrastructure for AI in order to optimize efficiency, harness data for AI models, support over-stretched employees, and defend against damaging cyberattacks, will struggle to compete.

Industrial networking partner considerations

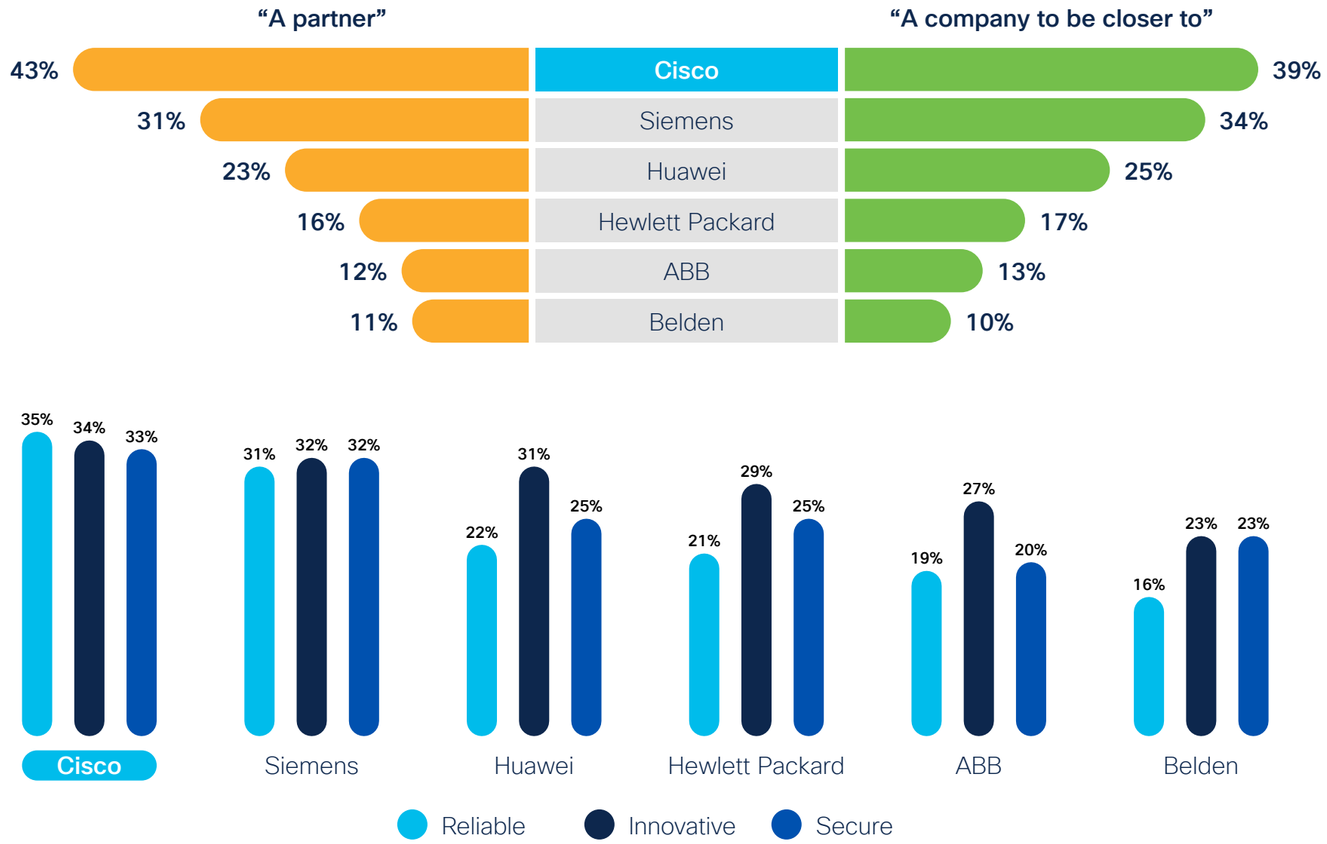
As you outline your industrial networking strategy and select a partner to support you on that journey, consider four important factors.

1#
A major vendor solution, designed for both IT and OT, can support better collaboration between these two teams (while, conversely, siloed point solutions can have the opposite effect).

2#
In order to maximize AI potential via fit-for-purpose infrastructure, it's important to partner with a provider such as Cisco, that is consistently named a networking leader by analysts including Gartner and Forrester

3#
A strong, open relationship with a partner naturally leads to more successful deployments. Respondents to our global survey were more likely to describe Cisco as a 'partner' (43%) or a company they were 'closer to' (39%) than five other named providers.

4#
Reputation matters when it comes to choosing the right partner. Against five other named providers, Cisco was named top by survey respondents for reliability, innovation and security.



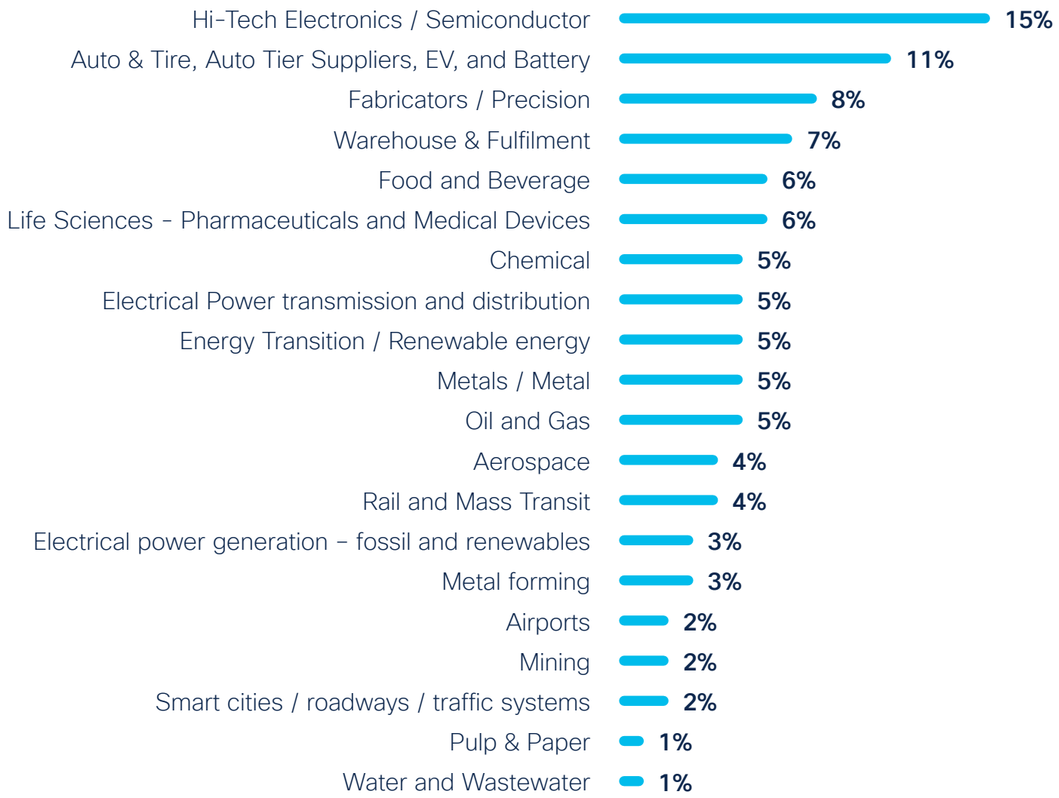
Q. Of the following suppliers, which do you consider to be a partner/closer to? Select all that apply
Q. Which of these attributes do you associate most with each of these suppliers? Select all that apply

Section 5

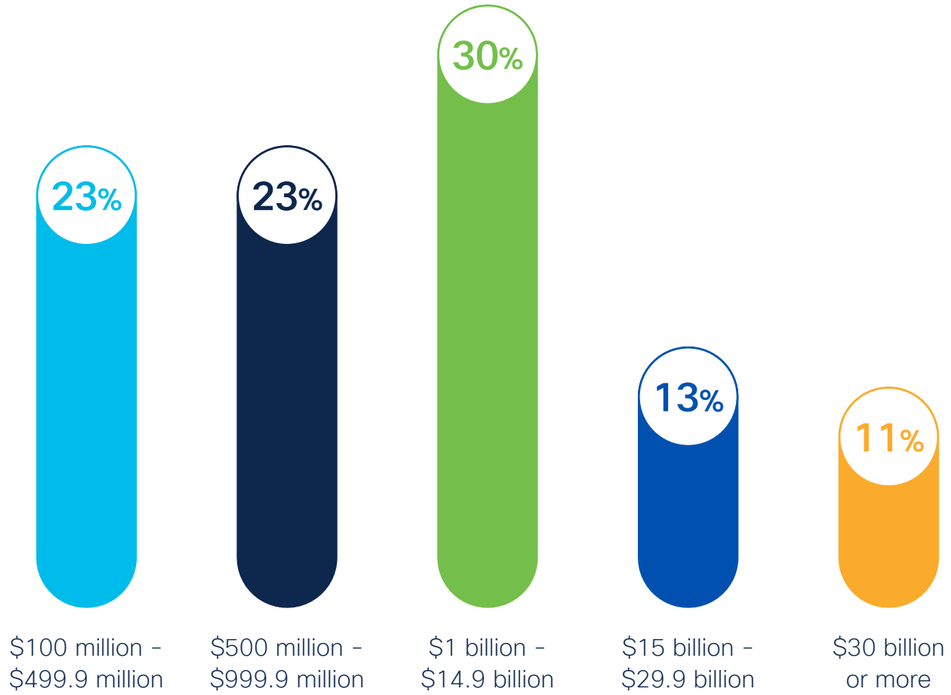
Demographics & firmographics

Demographics & firmographics

Industry

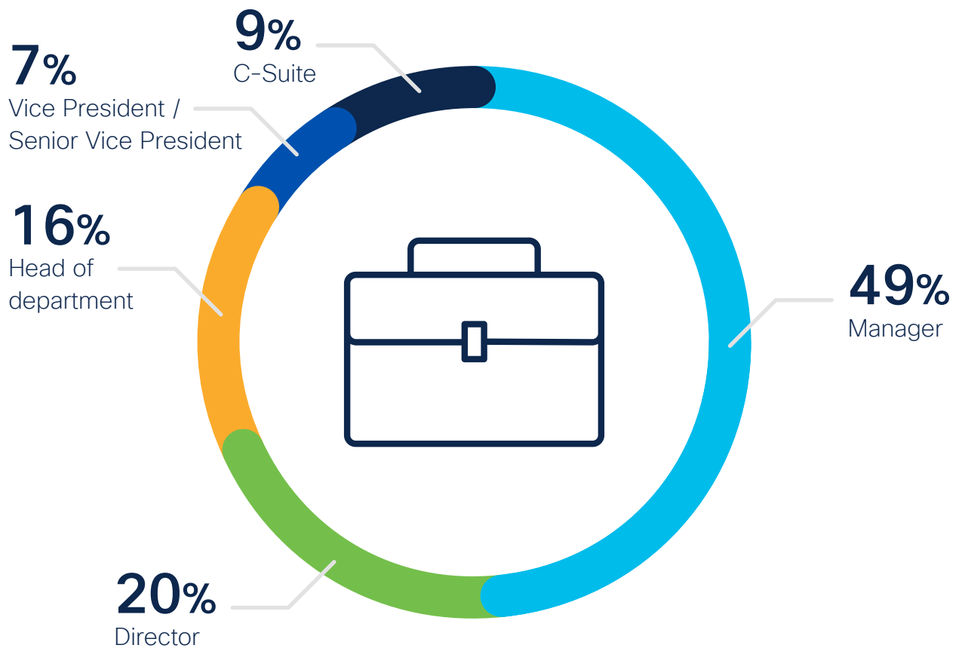


Annual revenue

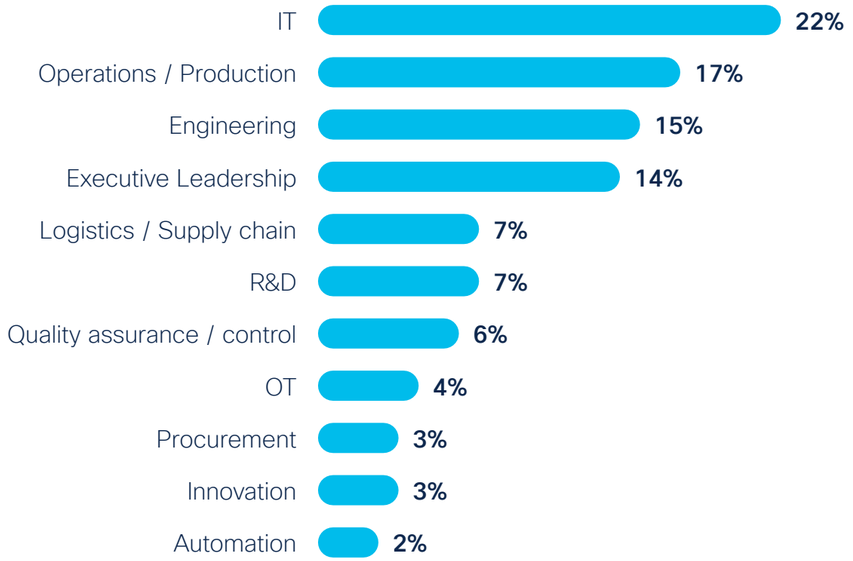


Demographics & firmographics

Job role

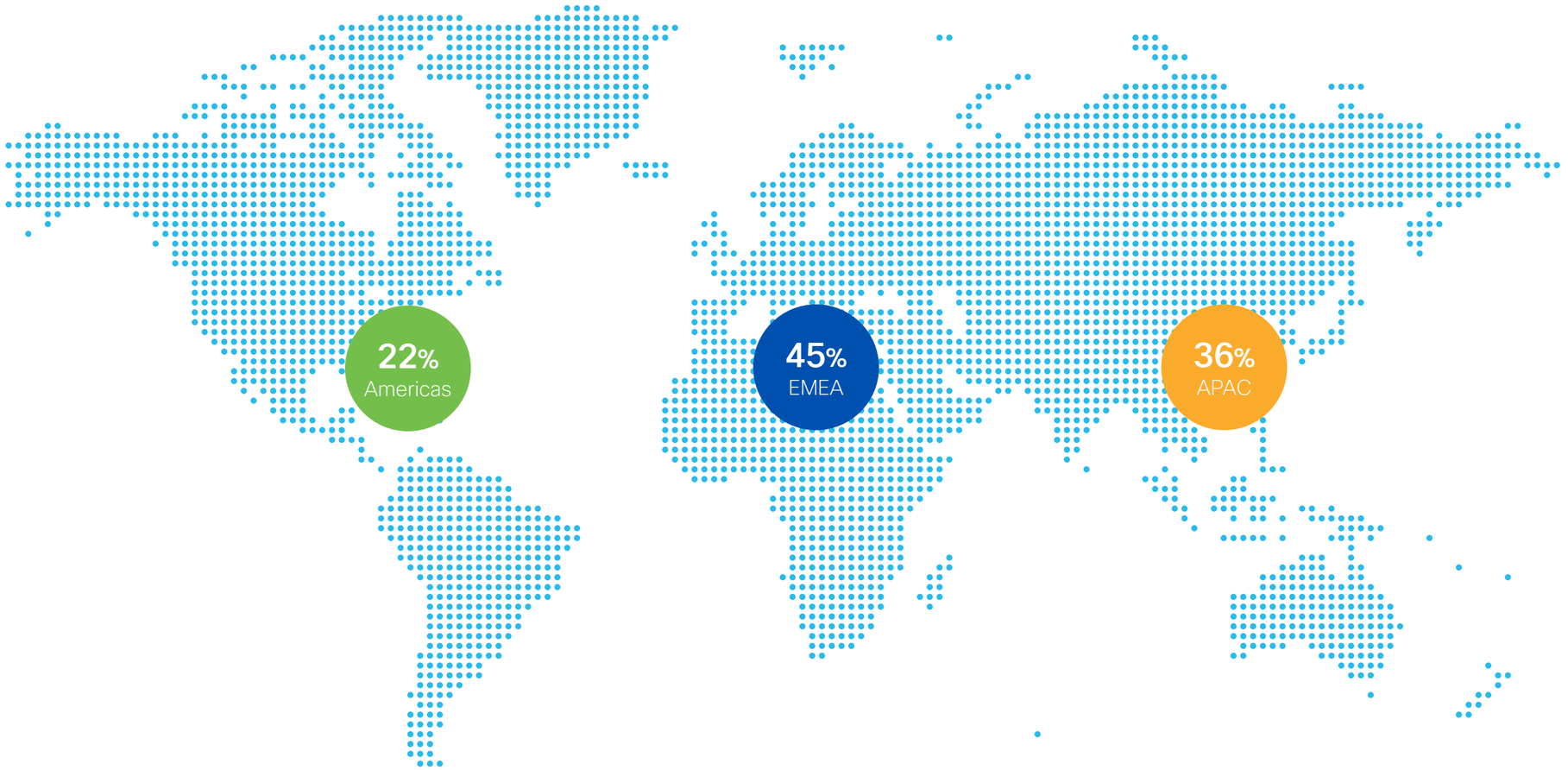


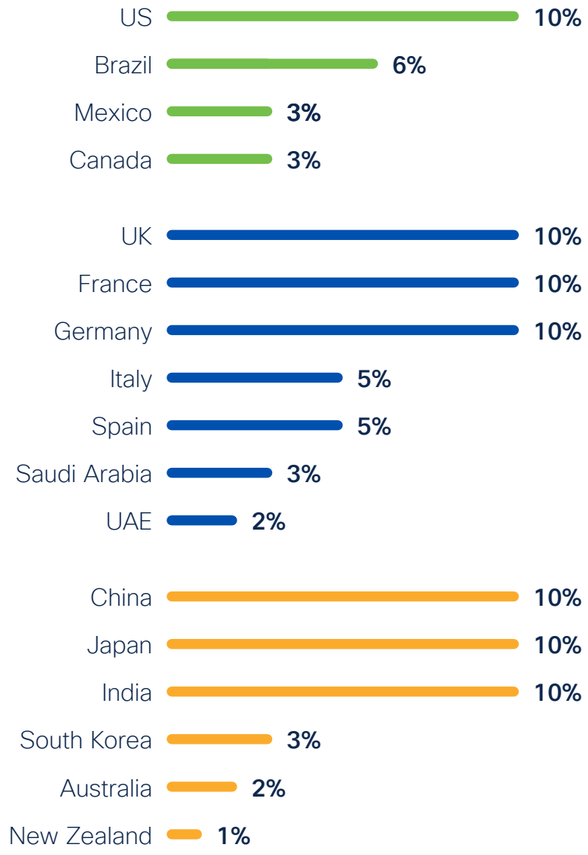
Department



Demographics & firmographics

Country





About Cisco

Cisco is the worldwide technology leader that securely connects everything to make anything possible. Our purpose is to power an inclusive future for all by helping our customers reimagine their applications, power hybrid work, secure their enterprise, transform their industrial infrastructure, and meet their sustainability goals.

About Sapio Research

Sapio Research is a full-service B2B and tech market research agency that helps businesses grow thanks to high quality, efficient and honest research solutions.

We deliver valuable insights to support our clients understand their audience, build powerful brands, cut through the noise with great content and headlines, and make vital business decisions relevant to their market. We're based in the UK and have access to over 149 million people across 130 countries, working with clients that range from top tech companies to global consultancies, Marketing/PR agencies and household name brands.

Our purpose-driven team of expert market researchers is passionate about providing data confidence for all and performing research that makes a difference. We're here to support our clients every step of the way in all areas of quantitative and qualitative research, so they can save time and thinking space, deliver with confidence, and unlock more value with their research.

sapioresearch.com

cisco

The bridge to possible