



SECURITY PRIORITIES SURVEY

The evolving security landscape

Companies continue to grapple with a highly complex and active cybersecurity landscape. While AI promises to simplify and improve safeguards, it also opens doors to new risks.

Complexity remains the defining characteristic of the cybersecurity agenda as organizations grapple with accelerating threats and an expanding portfolio of specialized tools. While AI's rise presents an opportunity to simplify and solidify the cybersecurity landscape, there are growing concerns the technology will unleash new attack vectors, increasing vulnerabilities and amplifying risks.

Ransomware, insider threats, and supply-chain attacks continue to keep organizations in the crosshairs. The shift to cloud, and in turn, hybrid IT infrastructure, has magnified complexity and risk as the lack of visibility and cloud misconfigurations become a leading cause of data and system breaches.

As adversaries get more creative and aggressive, security organizations see value in AI as a means to quickly analyze massive datasets, allowing them to more easily pinpoint vulnerabilities and automate threat response. CSO's 2025 Security Priorities survey confirmed there is mounting interest in integrating AI into cybersecurity strategies. Thirty-eight percent of companies are accelerating the use of AI to improve security effectiveness, more prevalent among companies in the healthcare (44%) and technology (43%)

sectors. While roughly two-thirds of respondents (64%) said AI-enabled security technologies are on their radar screens or part of active pilots, only 18% have launched production-scale initiatives. This confirms that despite the interest, it is still relatively early in the maturity and adoption cycle of AI-powered cybersecurity tools.

Even as it gains traction, AI's role in the modern cybersecurity era is perceived as a doubled-edged sword. While automation and smarter insights lead to better safeguards, AI can also serve as a powerful weapon for adversaries aiming to continuously expand the attack surface and enable new and diverse threats. Survey respondents are particularly concerned about AI-enabled ransomware (38%), use of AI to facilitate attack automation (35%), and adversaries' ability to leverage AI to hunt for enterprise vulnerabilities


that can then be exploited by bad actors (33%). Companies in the APAC region were far more concerned about the possibilities of AI-enabled cyberattacks compared to their global counterparts.

CSO's 2025 Security Priorities study surveyed 641 IT security executives, managers, and professionals from around the globe to understand the state of cybersecurity within organizations as well as the expanding remit of key leaders. The research also explored the makeup of the increasingly complex tool portfolio along with the opportunities and challenges associated with AI capabilities as they become integrated into the cybersecurity landscape.

AI-enabled cybersecurity comes into focus

As enterprises dial up the volume on AI, many see potential for the technology to address longstanding challenges related to safeguarding critical data and mitigating cyber risks. Nearly three quarters (73%) of respondents said their firm was more likely to consider a solution that leveraged AI, higher among large companies with over 1,000 employees (78%).

Among those currently implementing AI in a cybersecurity capacity, threat detection (35%) and malware detection (35%) are most prevalent use cases



73%

say their organization is more likely to consider a security solution that leverages AI.

In organizations with 1,000+ employees, this increases to 78%.

followed by anomaly detection (33%). That's significantly higher than in the 2024 survey, where roughly a quarter of organizations were enlisting AI for malware detection (26%) and threat detection (24%). This year, large company respondents were more likely to harness AI technologies as part of their threat and malware detection toolkits (both at 41%), as were companies in the EMEA region, at 43% for threat detection and 46% for malware detection. Overall, companies were least likely to see a role for AI in tools and strategies related to authentication and audit and compliance (both at 22%).

As AI makes its way into cybersecurity strategies and tool sets, organizations are reporting a wide range of benefits. Given the fast-changing nature of the threat landscape, speed of response is critical, and companies view AI as a key lever for achieving those goals. Forty-four percent of respondents in this year's survey said they are able to identify unknown threats far

The no. 1 benefit seen from AI-enabled security technology is faster identification of unknown threats.

more quickly with use of AI while 42% said AI accelerates decision and response times.

Analyzing huge swaths of data is another requirement for an effective cybersecurity campaign, and here too, AI delivers. Forty-two percent of respondents said AI capabilities make it easier to sift through large amounts of data faster than previous solutions. The same percentage also called out the advantages of AI for automating security functions to reduce employee workload and for helping security organizations be more proactive.

Top security priorities and challenges

Outside of establishing a roadmap for effective AI use, security organizations are juggling the usual long list of priorities as threats multiply and the need to protect the business intensifies. Strengthening the protection of confidential and sensitive data remains at the top of the list, cited by nearly half (48%) of this year's respondents and significantly higher than the 40% reported


in 2024. While that number remained pretty consistent across company size and industry sector, respondents in the APAC region were more entrenched in this aspect of cybersecurity, at 53%, compared to any of their global counterparts.

Securing cloud data and systems remains a top mandate for security organizations, cited by 45% of this year's respondents, followed by the desire to simplify IT security infrastructure, at 39%. Enhancing security awareness through end-user training is a higher priority since the last survey, cited by 34% of this year's respondents compared to 31% in 2024.

Over the next 12 months, spending on cybersecurity will be driven by an array of core business objectives. Among them: increasing cybersecurity protections (42%), increasing operational efficiency (37%), and accelerating AI-driven innovation

Business priorities driving security spending

- Improving cybersecurity protections **(42%)**
- Increasing operational efficiency **(37%)**
- Accelerating AI-driven innovation and applications **(31%)**



76%

of security decision-makers say that understanding which security tools and solutions fit best within their company is becoming more complex.

and applications (31%). Companies are also funding security programs as part of efforts to transform existing business processes through automation and integration (30%) and to improve profitability (30%). Cybersecurity's connection to robust business health was reflected in the two top-ranked business priorities fueling investments this year: increasing cyber security protections followed by increasing profitability.

As always, there are numerous challenges that threaten to circumvent cybersecurity goals, not the least of which is growing complexity. Multiple standalone tools continue to complicate implementation and day-to-day tool management while making it more difficult to detect and respond to threats. Over half (57%) of respondents in this year's survey said their organization struggles to find the root cause of security incidents they've experienced over the prior 12 months, higher among those in the technology (64%) and financial services (63%) fields.

The plethora of diverse tools also makes it difficult to determine which tool is the best fit for the job. More than three quarters (76%) of this year's survey respondents struggle to understand which security solutions make sense for their company and its specific security needs. This is on par with the 2024 findings, indicating there has been marginal progress reducing complexity and simplifying tool choices. As a result, 70% of this year's respondents favor a consolidated security platform to streamline the cybersecurity landscape, higher among companies in the technology sector (78%) and in North America (72%).

Other obstacles are hampering cybersecurity success. According to the survey, employee awareness and training issues remain a central hurdle, cited by 31% of respondents. Budget constraints (30%) and the need to address the risks introduced by disruptive technologies like AI and machine learning (28%) present additional challenges. There is a perennial struggle to recruit and retain quality security employees, cited by 28% of respondents.

Security leaders embrace their expanding remit

With digital capabilities a central cog of modern business, companies are expanding the responsibilities of security leaders while adding more senior security-related roles to their executive rosters. This

year’s respondents report a pretty even split between top security roles with 48% led by a CSO and 46% by a CISO. The majority of security leaders report into the CEO (57%), higher among manufacturing companies (67%) and larger companies with over 1,000 employees (61%). Companies in the APAC region were far more likely to have a direct reporting line between their security lead and the CEO, at 72%.

95% of top IT security executives have engagement with their Board of Directors. Up from 85% in 2023.

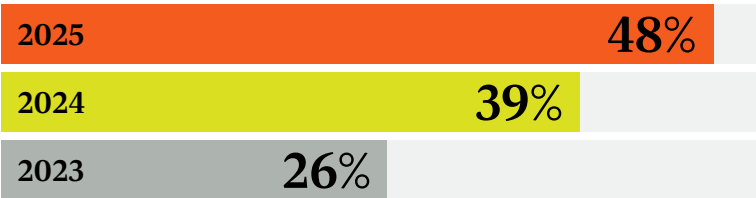
Most top security leaders (95%) regularly engage with the board of directors (BOD), at a cadence of multiple times a month (48%). Simultaneously, it’s become more common for board members to take

ownership and oversight of cyber risk management, a scenario cited by 70% of this year’s respondents compared to only 59% in 2024. Overall, respondents credit direct engagement with the BOD as a positive factor in advancing cybersecurity initiatives, cited by nearly three quarters of this year’s respondents (72%).

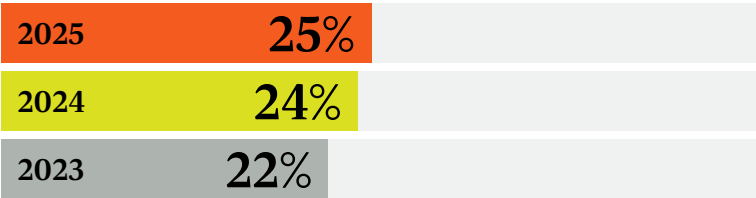
New reporting structures are also being designed to fortify board of director engagement. Thirty-one percent of this year’s respondents said the top security leader reports directly into the board of directors. Only one in five

Does your CSO, CISO, or top security executive have regular engagement with the Board of Directors?

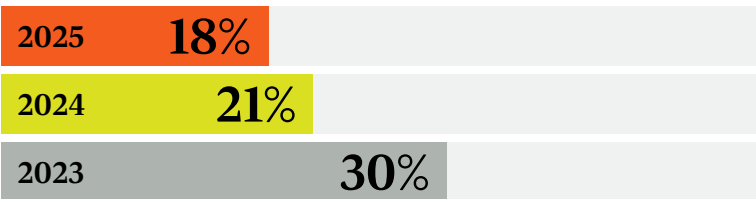
Yes, engages multiple times a month



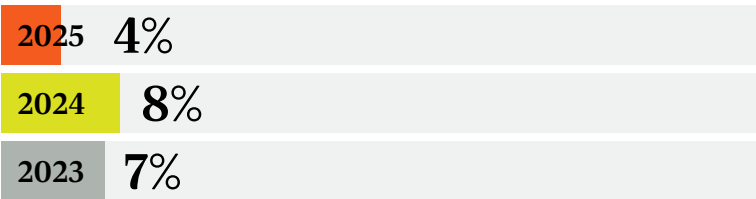
Yes, engages once a month



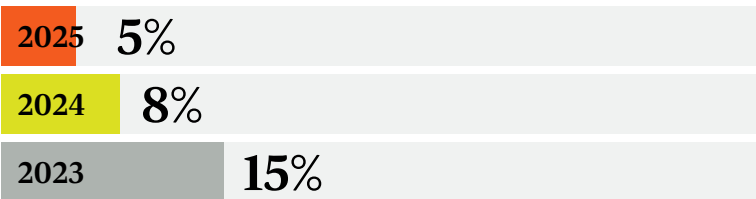
Yes, engages once a quarter



Yes, engages once a year



Has little to no engagement



AI-enabled tools see the greatest increase in spending

AI-enabled security technology

58%

Application development security

45%

Cloud data protection

44%

Cloud-based security services

43%

Cyber risk insurance

41%

respondents said their security chief reports into the corporate CIO, another sign that cybersecurity commands its own infrastructure and leadership outside of IT. There are also more layers being added to security leadership. Nearly two-thirds of respondents (64%) say there are one or more business information security officers (BISOs) reporting into CSOs and CISOs as part of the overall management hierarchy, higher among companies with over 1,000 employees (74%).

Looking ahead, security executives expect to have more personal involvement in

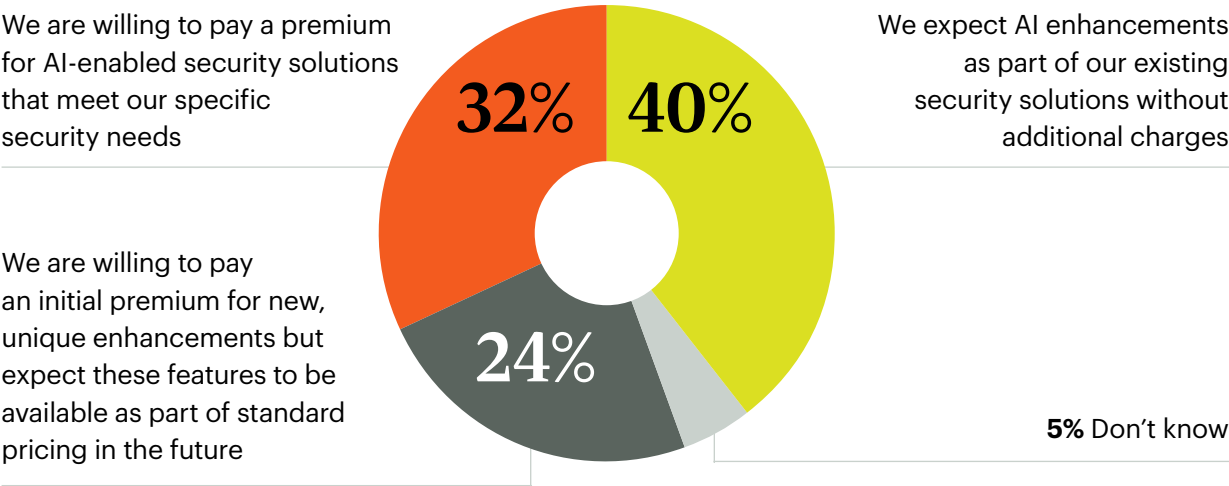
a number of cybersecurity activities. Developing cybersecurity strategy and policies will be a major focus over the next calendar year, cited by 43% of respondents, followed by risk management (39%) and security architecture and technology updates (37%). The broader remit also extends across global regions: Sixty-seven percent of this year's respondents confirmed their responsibilities include addressing security issues outside of their country or region, higher among those in EMEA (75%).

AI-related issues will consume a good part of the cybersecurity agenda over the next 12 months. Thirty-seven percent said they will spend more time managing the risks of AI-enabled technologies, higher among technology organizations (44%) and those in the EMEA region (40%). Ensuring the security of in-house and third-party AI applications will be a focal point, called out by 29% of respondents.

Security budgets hold their ground

While everything in the security world moves at a rapid clip, security budgets are holding steady, in line with prior year spending. Nevertheless, companies are not blindly bankrolling security technology investments without robust evaluations and guidance from pilot project learnings. Most companies (68%)

What is your organization’s stance on investing in AI-enabled security solutions?



were actively seeking ways to enhance the value of their security technology spend, if not to trim back in certain areas.

Of the total number of respondents, 43% were planning for an increase in their overall security budgets while 55% expect spending to remain the same. Companies in the financial services sector were more apt to expect increases (62%) while only 21% of those in health care were preparing for a spending boost.

Over the next 12 months, security budgets will be directed to AI-enabled security technology (58%), application development security (45%), and cloud data protection (44%). Technology and financial services respondents were inclined to ramp up spending on security

technologies across the board compared to other industry sectors. While there wasn't much interest in reducing investments, those categories most likely to see cuts were application development security, DevSecOps adoption, incident response, Secure Access Service Edge (SASE), and Extended Detection and Response (XDR). Deception technology (11%), DevSecOps adoption (10%), and zero trust technologies (10%) were considered new categories of spending for many of the responding organizations.

State of security technologies deployment

Given the wide swath of security technologies available, companies are in very different stages of deployment

and evaluation depending on their level of maturity and current state of need.

On the radar screen or actively researching

By far, AI-enabled security technologies have commanded the most interest, with almost half of respondents (47%) exploring the potential of this emerging toolset. Most companies (73%) are more likely to consider a security solution if it employs some form of AI, even more so at large companies (78%). For the most part, companies are expecting their security vendor partners to pony up AI enhancements as part of existing security solutions without charging additional fees. Nearly a third (32%) are willing to pay a premium for AI capabilities that meet specific security needs, but another quarter (24%) say they expect those unique features to eventually be folded into the standard pricing mix as things evolve.

Identity threat detection and response (ITDR) is also high on the list of security technologies companies are evaluating (37%) followed up by deception technology (33%) and zero trust technologies (32%).

Piloting

More established technologies like application development security (24%), incident response (22%), cloud posture management tools (19%), and Security Incident and Event Management (SIEM), also at 19%, have graduated to the pilot stage. Companies in the EMEA region were

more actively involved with pilots in these categories as were larger companies.

Production

A good number of security technologies have matured enough to advance to the production phase. More than a third of companies have rolled out enterprise-scale authentication capabilities (36%) and even more so in the manufacturing space, at 46%. Security education and awareness training (35%) is spreading across the enterprise given the impact it can have on increasing cyber safeguards. Data loss prevention (DLP), at 33%, endpoint detection and response (EDR), at 32%, and managed security service providers (32%) are other technologies that are becoming staples of the enterprise cybersecurity landscape.

Outsourcing

Outsourcing security functions to a provider or other third-party is an increasingly appealing option for companies who might not have the requisite in-house skills and talent or for those who don't want to invest—and manage—a full portfolio of cybersecurity tools. Nearly all companies (89%) said they had some level of interest in enlisting a managed security service provider (MSSP) to facilitate monitoring or response to security threats. While 28% were only at the research stage, 32% were actively in production with MSSPs for a variety of their cybersecurity needs.



89%

of companies express some level of interest in enlisting a managed security services provider to facilitate monitoring or response to security threats.

Up from 79% last year.

Over the next 12 months, enterprises are mostly likely to turn to an MSSP for cloud security management (33%), threat detection and response (26%), infrastructure protection (26%), and threat intelligence (26%). Identity and access management, including capabilities involving customers, are least likely to be viewed as candidates for an MSSP solution.

In conclusion

Even as companies take aggressive action to prioritize cybersecurity strategies, the velocity and variability of attacks, coupled with the complex tool landscape, is amplifying, not reducing risk. AI has huge potential to simplify cybersecurity protections through automation and the ability to analyze massive data sets. At the same time, it can be a springboard for new, more nefarious attacks.

The bottom line is security leaders still have their work cut out for them. But with cybersecurity now squarely in the sights of the C-suite and board-level executives, security leaders are well positioned to drive effective strategies that not only protect the enterprise, but also help drive lasting business growth.

About the survey

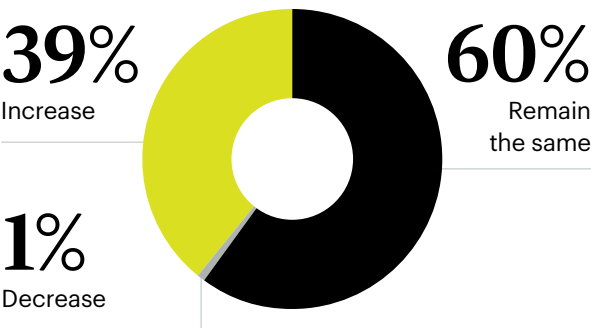
The 2025 Security Priorities survey analyzed data from a CSO online questionnaire given to 641 security professionals. All respondents are involved in IT and/or corporate IT and physical security decision-making, with 78% having an executive, IT or security title. Respondents represent companies primarily in North America (46%), with some in the Asia-Pacific region (36%) and in Europe (18%). These companies come from a variety of industries, including technology, manufacturing, financial services, healthcare, education, retail, telecommunications, and marketing. The average company has 14,494 employees.

Regional key takeaways

Is your marketing scope region-specific? Explore the key research findings from North America, Europe, and Asia-Pacific. Contact us to dive deeper into the regional results.

North America

Security budget expectations



Security decision-makers say their role is expanding to include:

1. Cybersecurity strategy and policy development
2. Risk management
3. Security architecture and technology updates
4. Innovation and emerging technologies
5. Managing the risks of AI-enabled technology

Key priorities for the next 12 months:

- Strengthen protection of confidential and sensitive data **(46%)**
- Simplify IT infrastructure **(44%)**
- Secure cloud data and systems **(43%)**
- Improve understanding of external threats **(41%)**

Top five challenges inhibiting security goal achievement:

1. Too many competing priorities
2. Employee awareness and training issues
3. Retaining qualified security employees
4. Lack of a sufficient budget
5. Addressing the risks presented by disruptive technologies (AI, machine learning, IoT)

How engagement with the board has shifted last year v. this year:

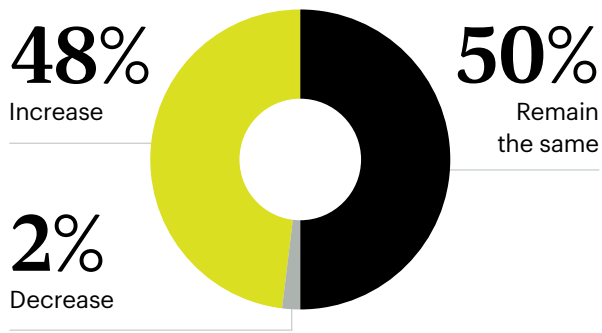
- **93%** of top IT security executives have engagement with their Board of Directors. Up from **90%** in 2024.
- **65%** say that someone on their organization's board has specific responsibilities or oversight for cybersecurity or cybersecurity management. Up from **54%** in 2024.
- **71%** agree that their engagement with the board helps improve cybersecurity initiatives. Up from **63%** in 2024.

No. 1 security solution on the radar for this year:

AI-enabled security technology **(51%)**

EMEA

Security budget expectations



Security decision-makers say their role is expanding to include:

1. Managing the risks of AI-enabled technology
2. Cybersecurity strategy and policy development
3. Risk management
4. Innovation and emerging technologies
5. Security architecture and technology updates

Key priorities for the next 12 months:

- Secure cloud data and systems **(53%)**
- Strengthen protection of confidential and sensitive data **(45%)**
- Simplify IT infrastructure **(43%)**
- Enhance security awareness through end-user training **(42%)**

Top five challenges inhibiting security goal achievement:

1. Process complexity
2. Lack of a sufficient budget
3. Addressing the risks presented by disruptive technologies AI, machine learning, IoT)
4. Lack of automation and integration
5. Employee awareness and training issues

How engagement with the board has shifted last year v. this year:

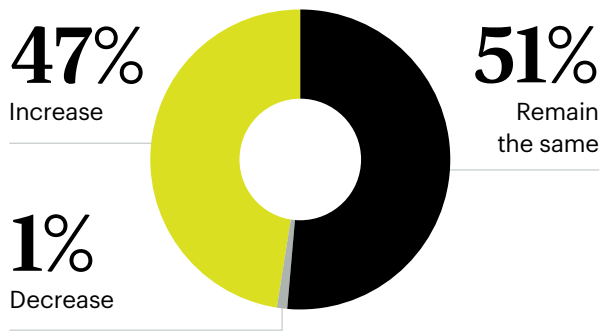
- **99%** of top IT security executives have engagement with their Board of Directors. Up from **95%** in 2024.
- **77%** say that someone on their organization's board has specific responsibilities or oversight for cybersecurity or cybersecurity management. Up from **71%** in 2024.
- **81%** agree that their engagement with the board helps improve cybersecurity initiatives. Up from **69%** in 2024.

No. 1 security solution on the radar for this year:

AI-enabled security technology **(39%)**

APAC

Security budget expectations



Security decision-makers say their role is expanding to include:

1. Cybersecurity strategy and policy development
2. Risk management
3. Security architecture and technology updates
4. Managing the risks of AI-enabled technology
5. Compliance oversight

Key priorities for the next 12 months:

- Strengthen protection of confidential and sensitive data **(53%)**
- Secure cloud data and systems **(45%)**
- Streamline compliance and privacy efforts **(40%)**
- Accelerate the use of AI to improve security effectiveness

Top five challenges inhibiting security goal achievement:

1. Addressing risks from cyber threats (inside and outside threats like ransomware, APTs, DDoS)
2. Employee awareness and training issues
3. Lack of a sufficient budget
4. Network complexity and/or lack of visibility (including multicloud)
5. Demonstrating a return on security investments (ROI)

How engagement with the board has shifted last year v. this year:

- **95%** of top IT security executives have engagement with their Board of Directors. Up from **94%** in 2024.
- **72%** say that someone on their organization's board has specific responsibilities or oversight for cybersecurity or cybersecurity management. Up from **61%** in 2024.
- **68%** agree that their engagement with the board helps improve cybersecurity initiatives. Up from **67%** in 2024.

#1 security solution on the radar for this year:

AI-enabled security technology **(46%)**

Examining the marketplace

Research is an invaluable way for marketers to better understand customers and prospects, with the goal of building quality connections. At Foundry this is one way we are focused on building bridges between tech buyers and sellers. Our first-party relationships with the most important tech buyers and influencers around the world, allows us to apply value across our customers marketing stack. Our research portfolio explores our audiences' perspectives and challenges around specific technologies—from analytics and cloud, to IoT and security—and examines the changing roles within the IT purchase process, arming tech marketers with the information they need to identify opportunities.

To see what research is available, visit foundryco.com/tools-for-marketers.

For a presentation of full results from any of these studies, contact your Foundry sales executive or go to foundryco.com/contact-us.

Buying process

Each year we take a deep dive into the enterprise IT purchase process to learn more about who is involved and who influences decision-making, what sources purchasers rely on to keep up to date with technology—and throughout the purchase process—and how they want to engage with the vendors they are working with. Visit foundryco.com/customerjourney for more information.

Buying process studies

- Customer Engagement
- Role and Influence of the Technology Decision-Maker

Technology insights

Each year we explore the technologies that are top of mind among our audiences to understand the business challenges, drivers, and adoption within the enterprise. These research studies are designed to help IT marketers understand what their customers are focused on and where the market is moving.

Role and priority studies

- CIO Tech Poll: Tech Priorities
- State of the CIO

Technology-specific studies

- AI Priorities
- Cloud Computing
- Security Priorities
- Partner Marketing

Stay in touch with us

Email: Sign up for Foundry's newsletters and receive media and marketing trends as well as our proprietary research, product and event information direct to your inbox. Go to foundryco.com/newsletter.

Social: For research, services and events announcements, visit us on [LinkedIn](#).

Find it all on foundryco.com.

About Foundry

Foundry's vision is to make the world a better place by enabling the right use of technology, because we believe that the right use of technology can be a powerful force for good.

Foundry is a trusted and dependable editorial voice, creating quality content to generate knowledge, engagement and deep relationships with our community of the most influential technology and security decision-makers. Our premium media brands, including CIO®, Computerworld®, CSO®, InfoWorld®, Macworld®, Network World®, PCWorld® and Tech Hive®, engage a quality audience of the most powerful technology buyers with essential guidance on the evolving technology landscape.

Our trusted brands inform our global data intelligence platform to identify and activate purchasing intent, powering our clients' success. Our marketing services create custom content with marketing impact across video, mobile, social and digital. We simplify complex campaigns that fulfill marketers' global ambitions seamlessly, with consistency that delivers quality results and wins awards. Additional information about Foundry is available at foundryco.com.