Enterprise Strategy Group™
by TechTarget

RESEARCH INSIGHTS

Assessing Enterprise Browser Market Dynamics

Why Organizations Are Turning to Enterprise Browsers to More Effectively Secure Modern Work Styles

By Adam DeMattia, Senior Director, Custom Research; and Dave Gruber, Principal Analyst
Enterprise Strategy Group

December 2023

This Enterprise Strategy Group Research Insights Paper was commissioned by Google and is distributed under license from TechTarget, Inc.

Contents

Executive Summary

In recent years, the habits of knowledge workers have undergone a profound transformation, with a seismic shift toward distributed workforces, hybrid work patterns, and the widespread use of personal devices for work. At the same time, cloud-based applications and services continue to factor more and more prominently in the day-to-day tasks of knowledge workers, and organizations frequently enable direct internet access to these cloud services to optimize performance, latency, and user experience.

This evolution creates challenges to traditional perimeter-focused security approaches. The boundaries of the traditional office have dissolved, as knowledge workers now access sensitive data and collaborate from various locations, often utilizing unmanaged personal devices and networks. This increased mobility and flexibility, while fostering productivity and innovation, has simultaneously expanded the attack surface, created gaps in security control coverage, and increased the risk of successful and disruptive breaches.

Traditional security measures, which are primarily designed to secure the corporate network perimeter, struggle to adapt to this dispersed and dynamic environment. As a result, many organizations would be well served by reevaluating their security strategies to include enterprise browser technologies, which prioritize security, manageability, and the protection of sensitive data users need to access to do their jobs. However, the enterprise browser market is relatively nascent, so customer understanding is dynamic and fluid.

Google engaged TechTarget's Enterprise Strategy Group to execute a study to better understand the current state of market dynamics, including customer perceptions, user behaviors and experiences, and security outcomes. This report discusses these findings.

Survey Background

Enterprise Strategy Group (ESG) surveyed IT and security leaders knowledgeable about their organizations' tools, policies, and procedures for securing knowledge workers (52%), as well as knowledge workers themselves who spend the majority of their productive time on a laptop or desktop computer (48%).

Key questions included:

- How do knowledge workers accomplish their tasks today, and how will that shift over time?
- What are their preferences related to browser-based work experiences?
- How widespread are behaviors that increase enterprise risk?
- How often are knowledge workers successfully targeted by web-based attacks?
- What are IT and security teams doing to secure end users?
- What challenges do they face in their efforts?
- Where do enterprise browsers fit in their approaches moving forward?

ESG fielded the survey in August 2023, with 628 qualified respondents completing the survey. Respondents represented organizations in the U.S. (33%), Canada (10%), the U.K. (21%), Germany (20%), and France (16%). Additional demographic and firmographic details are presented in the *Research Methodology and Respondent Demographics and Firmographics* section of this report.

Key Findings

1. Macro-shifts in knowledge worker behavior will persist

- Looking ahead 12 months, 64% of respondents anticipate their organization will allow knowledge workers to determine their own remote work schedules, and just 12% say their organization will require knowledge workers to spend most or all of their time in an office location.
- Less than one-third of organizations (29%) prohibit knowledge workers from using personal devices for work, and when they do, only 30% of knowledge workers fully adhere to this policy.
- On average, ~63% of knowledge workers' productive time is spent working in the browser, with 48% of business-critical applications accessed through a browser.

2. Knowledge worker habits create risk

- Half of respondents admit to having circumvented security controls because they felt that their user experience was hampered or that getting a task completed was a higher priority than addressing a potential risk.
- The majority of respondents also admit their password hygiene is questionable.
- More than half of knowledge workers (54%) report browsing the web for non-work activities throughout the workday.
- Preventing successful phishing attacks continues to be the top end-user security concern.

3. Knowledge worker habits also show a clear preference for unified experiences across work and personal browsing

- 66% of knowledge workers say they are more productive using the same browser for work as they do in their personal browsing, and 61% say having a unified experience is their personal preference.
- 81% of respondents say enhancing knowledge workers' digital work experience is a top-three technology priority for the next year.

4. While organizations' efforts to secure knowledge workers are significant, security outcomes must improve

- Many organizations report significant or moderate net-new investments have been made in the past 24 months in areas such as data security and privacy (90% of organizations), cloud security (90% of organizations), endpoint security (89% of organizations), identity and access management (87% of organizations), and more.
- Despite this, 51% of knowledge workers report they have been victims of a successful web-based attack in the past year.
- Organizations are leaning into Zero Trust initiatives to help: 81% of respondents say Zero Trust initiatives are one of their top-three cybersecurity priorities, and 89% think enterprise browser technology is important to supporting their Zero Trust initiatives.

5. Enterprise browser technology is seen as a potential viable solution to protect end users from web-based threats

- While almost half (48%) say they are very familiar with enterprise browser technology, 81% say it is likely their organization will consider or make new investments in enterprise browser technologies over the next 12 months. 28% have already deployed enterprise browser solutions to date.
- Data loss prevention (DLP) is a top-tier use case for those considering enterprise browser solutions.
- Half (50%) say they would prefer to source their enterprise browser technology from a technology vendor whose browser technology is already in use by many employees and organizations. Chrome has the most mindshare as an enterprise browser (78%).

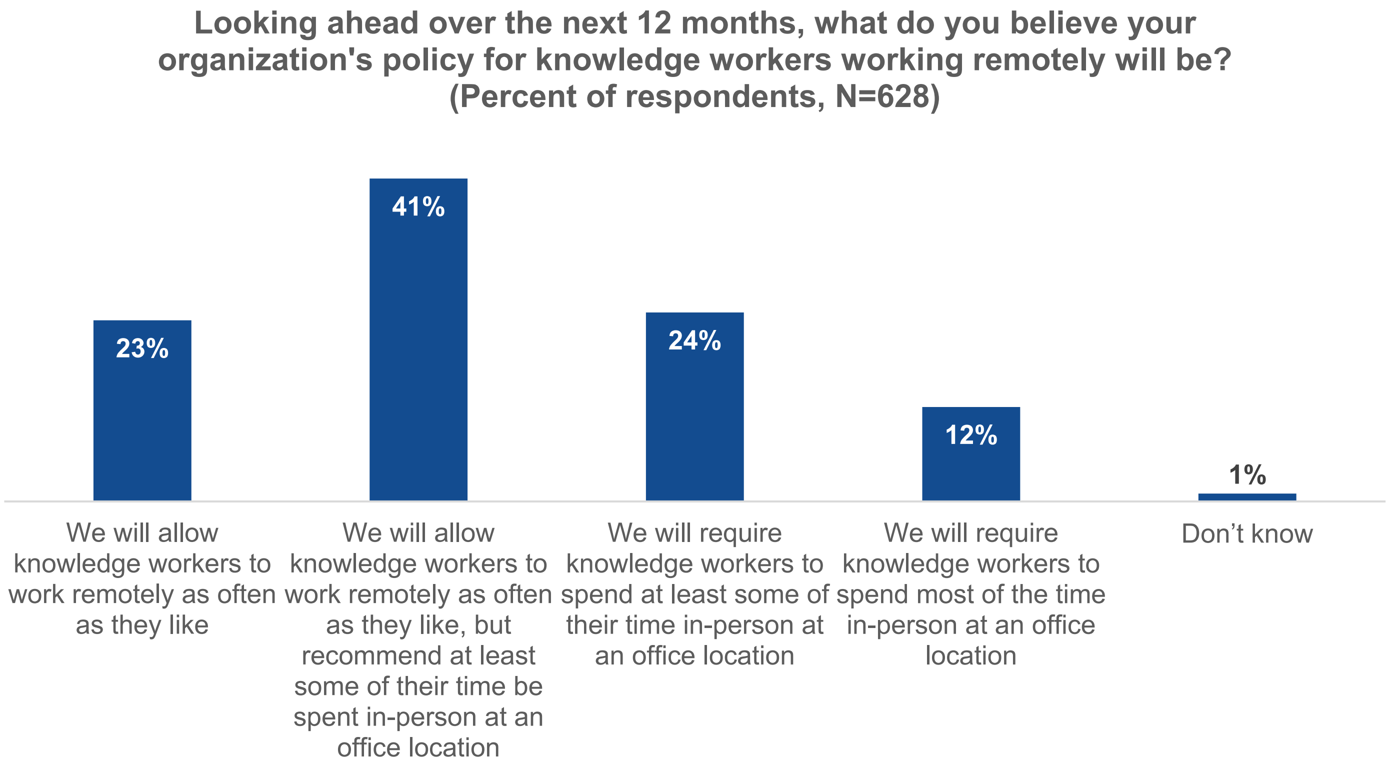
Trends in Knowledge Worker Behaviors

A key contextual aspect of this research is understanding how knowledge workers behave today. Three key trends are discussed: remote work patterns, the use of personal devices for work, and the business-criticality of browser-based activities.

While remote work does not necessarily make enterprise network security controls obsolete, it does challenge their effectiveness and necessitates a shift in the security approach. Traditional enterprise network security controls are designed with the assumption that employees are connected to a controlled corporate network, which no longer holds true in a remote work or hybrid work setting. As a result, monitoring and responding to incidents on dispersed endpoints and networks becomes more complex. Additionally, employees are frequently using home networks, public Wi-Fi, or mobile networks, each with varying levels of security. Traditional network controls cannot ensure a consistent security posture across these diverse environments.

While the shift to remote and hybrid work over the past few years has been significant, the future of hybrid work styles is less clear. Enterprise Strategy Group's research shows hybrid work is expected to be a resilient trend. When asked about their organization's policy for knowledge workers' remote and hybrid schedules for the next 12 months, 64% of respondents anticipate their organization will allow knowledge workers to determine their own remote work schedules (see Figure 1). While organizations will exert pressure for material in-office time, with 77% of respondents reporting that their organizations will encourage or require in-office time, respondents anticipate significant remote work leeway. In another finding, 70% of knowledge workers surveyed anticipate working remotely multiple days per week over the next year.

Figure 1. Expectations Related to Organizations' Remote/hybrid Work Policies



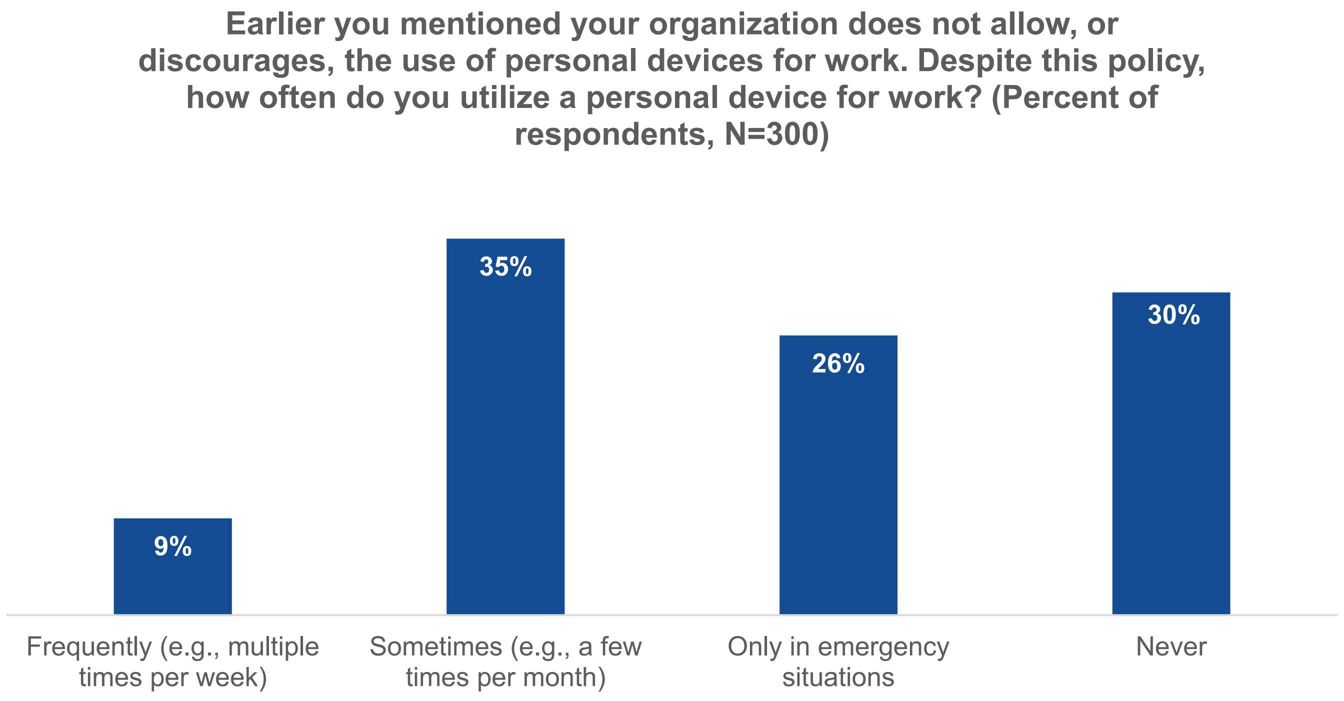
Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Another knowledge worker behavior that can have a material impact on organizational risk is the use of personal devices for work. The acceptance of personal device usage, also referred to as bring-your-own-device (BYOD) policies, increases device diversity. As workers use their personal computers, smartphones, and tablets to access corporate applications and data, the tendency is for these devices not to have the same level of security controls and agents deployed as company-managed devices. The resulting complexity, gaps in security coverage, and gaps in visibility all combine to make securing workers harder.

The data shows BYOD is a material trend. When asked about their organization's BYOD policies, just 29% of respondents said their organization prohibits employees' use of personal devices. Interestingly, this flexibility also extends to third parties like vendors, contractors, and others who need access to corporate resources: Just 32% say BYOD is prohibited for this type of user.

And standing in users' way is not an effective preventative strategy. We asked knowledge workers at organizations that prohibit personal device usage how often they violate those policies. In total, 70% acknowledged violating them (see Figure 2).

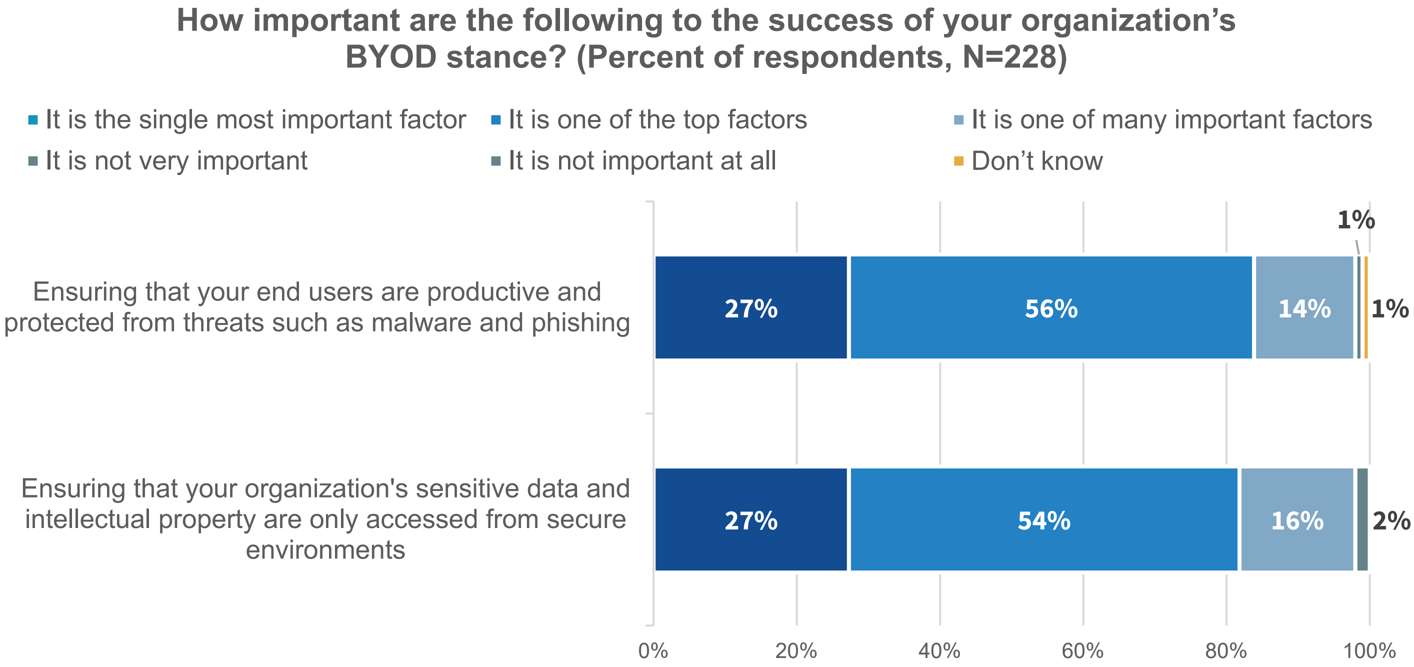
Figure 2. Knowledge Workers' Propensity to Violate Policies That Prohibit the Use of Personal Devices for Work



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

The data also shows that organizations recognize the importance of security to BYOD success. For example, 81% of respondents say the ability to ensure that sensitive data and IP are only accessed from secure environments is a top determining factor of the success (or failure) of their organization's BYOD stance (see Figure 3).

Figure 3. Security's Importance to BYOD Success



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Finally, while the pivot to SaaS-based applications and the overall importance of internet access to knowledge worker productivity is well understood, much of this market data is from the IT perspective. This data frequently lacks context that only end users can provide. This research shows that, on average, knowledge workers estimate spending about 63% of their productive time working in a browser. Moreover, 69% of respondents classify these browser-based activities as predominantly business-critical to the organization.

Taken together, the significant and persistent trend toward hybrid work, the proliferation of unmanaged personal devices accessing corporate data and assets, and the critical role browser-based work plays in end-user productivity all underscore why integrating more security capabilities within users' browsers may be a logical step for organizations to take.

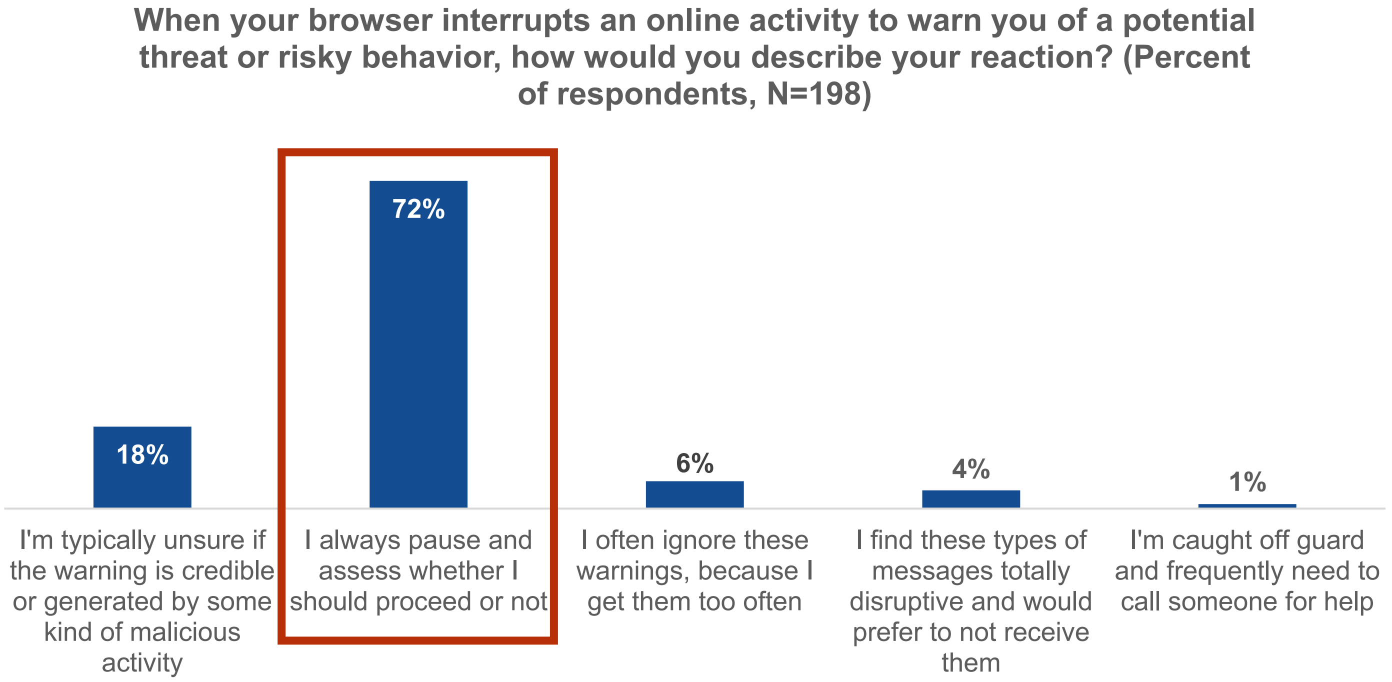
Risky Habits Reported by Knowledge Workers

The data also shows that many workers acknowledge doing things that explicitly create enterprise risk. Despite the fact that 82% of respondents said they are personally invested in protecting their company's data, 50% reported having recently circumvented a security control installed on their device (e.g., a VPN, antimalware protections, etc.) because it was impeding their work. This shows that, while users care about security, there are limits, and once security controls start to create friction in the user experience, many will look for ways around them. Organizations must strike a balance between security and user experience.

What is even more concerning is that the most senior respondents in the survey—those in the C-level—were the most likely to report *frequently* working around security controls (50% versus just 13% of middle managers and individual contributors). This means those individuals with the most access to sensitive data are also the individuals most likely to put that data at risk.

One approach organizations can take to effectively infuse user experiences with security is to leverage browser technologies that detect risky behavior, as most users heed browser-based security alerts. When asked how users respond to warnings from their browser of a potential threat or risky behavior, 72% say they always pause and assess whether they should proceed or not (see Figure 4). Browser-based security has the potential to help many users stop falling victim to web-based attacks.

Figure 4. The Effectiveness of Browser-based Alerts to Correct User Behavior

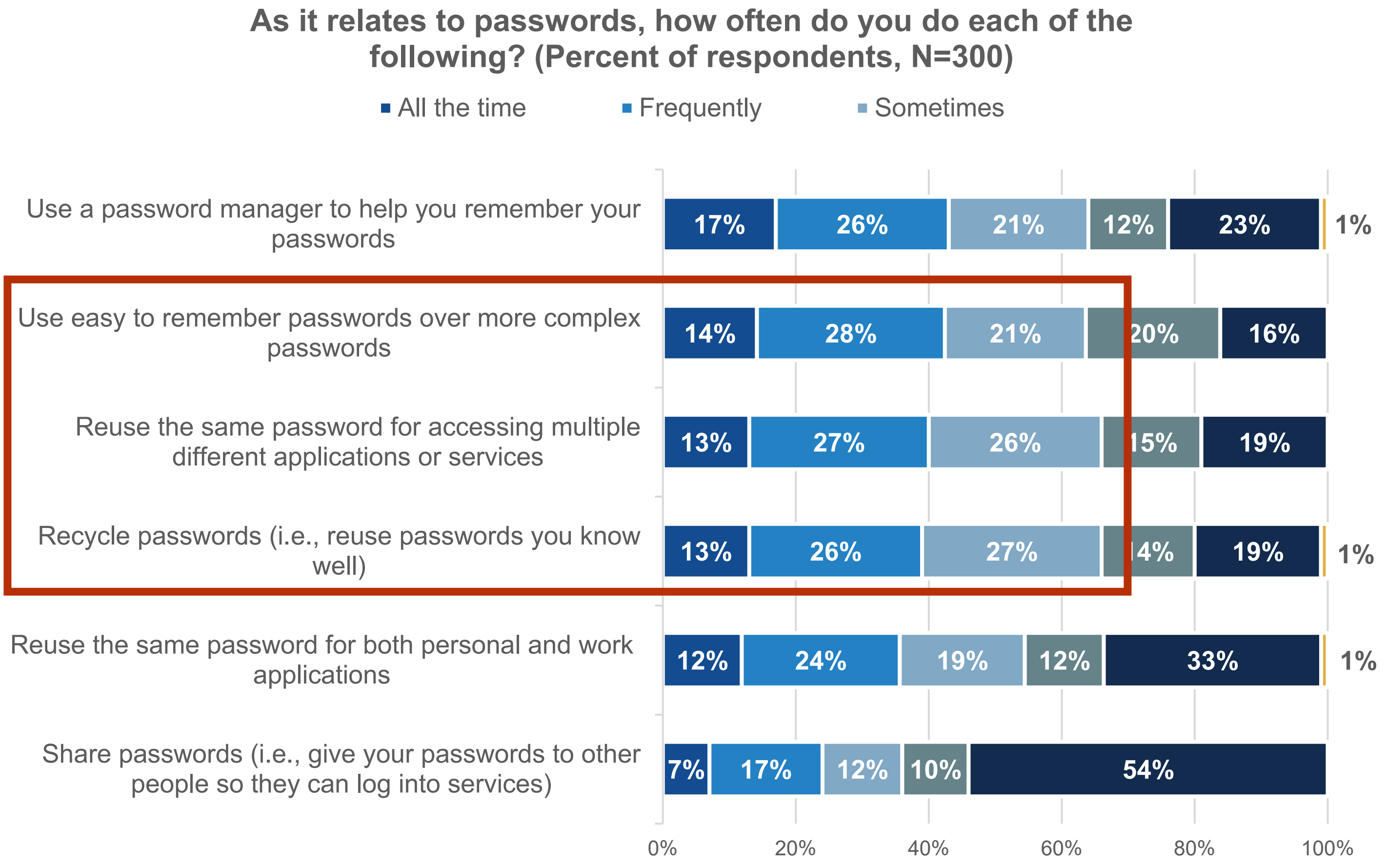


Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Beyond actively undermining security controls, many users report questionable password hygiene. This creates significant risk for companies. When employees use weak, easily guessable passwords or reuse the same password across multiple accounts, they open the door to a range of security threats. These bad habits make it relatively simple for cybercriminals to infiltrate corporate systems. Once inside, attackers can steal, manipulate, or encrypt corporate data assets, potentially leading to access issues, financial losses, and damage to a company's reputation. Beyond cybercriminals, internal risks arise when employees or former employees misuse their knowledge of poorly protected passwords.

The data shows that greater than a three-fifths majority of respondents report they at least sometimes rely on weak passwords (63%), recycle passwords (66%), and use the same passwords for multiple applications (66%), which creates the risk of a bad actor successfully moving laterally through the environment if the password is compromised (see Figure 5).

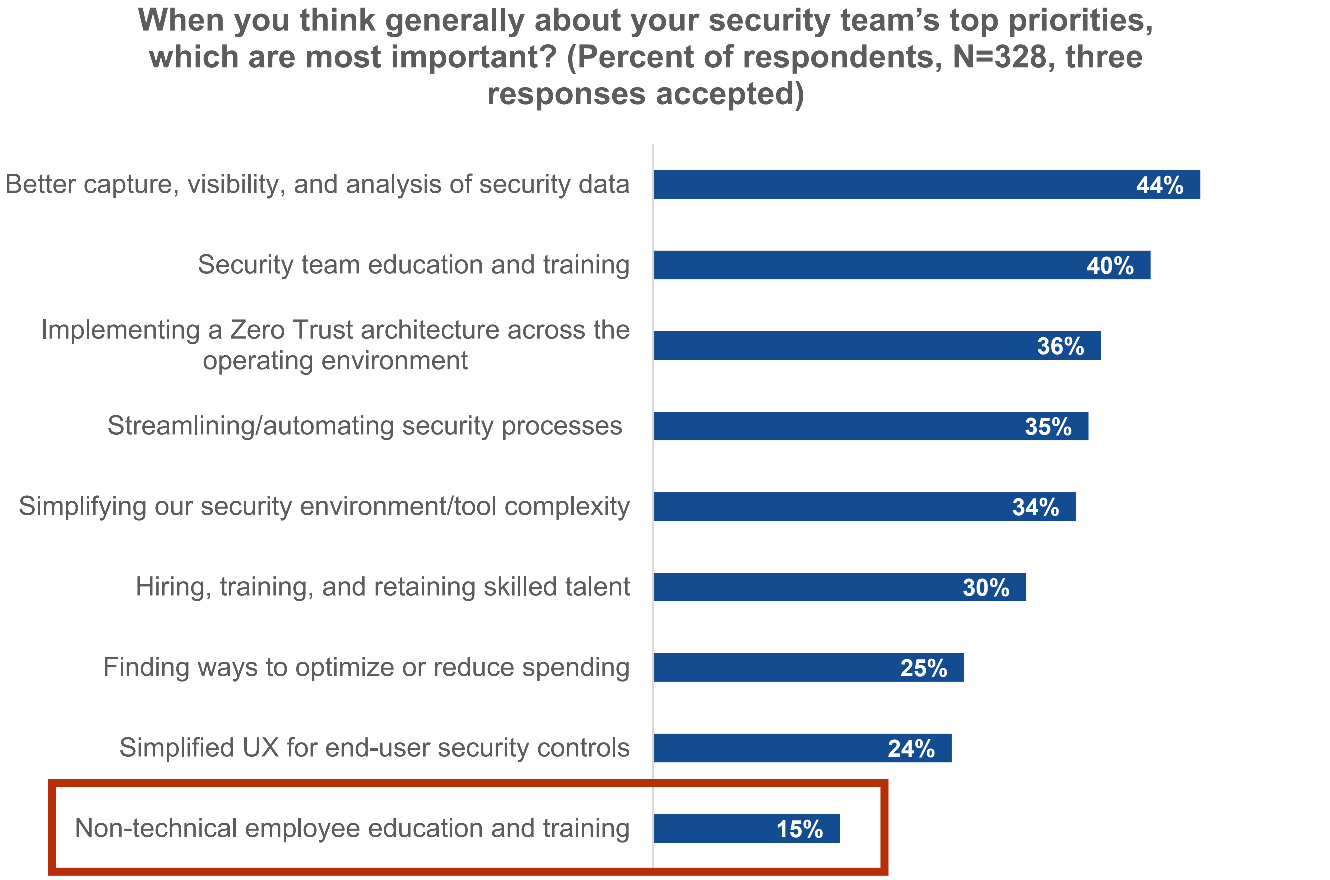
Figure 5. End Users' Practices Related to Password Hygiene



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

It is interesting to note the dichotomy between users' supposed belief they should be stewards for their company's data and their actions, which frequently put this data at risk. The data implies one explanation is a lack of user training and enablement. When IT and security decision-makers surveyed were asked about their teams' top priorities, just 15% reported end-user training was among their top three (see Figure 6). In fact, this area was least often reported as a top priority. With this lack of focus on end-user education, it is understandable how many end users are engaging in the risky behaviors discussed.

Figure 6. The Cybersecurity Team's Priority List



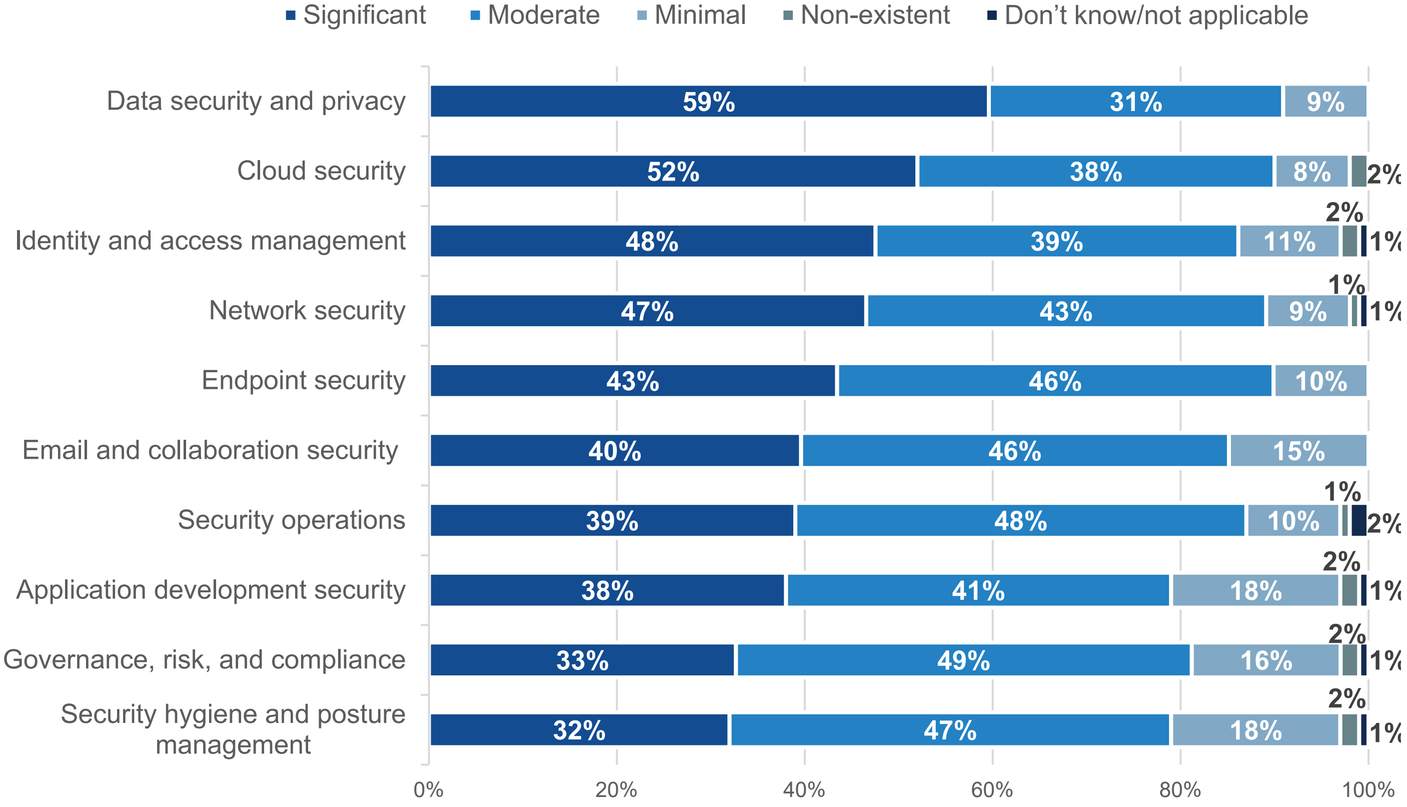
Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Current Security Controls, While Robust, Are Not Delivering

This research spanned not only user behavior but also sought to understand how organizations are working to secure users, keep them productive, and protect the organization's sensitive data assets. In short, the funding of security controls does not seem to be problematic. When asked to characterize their organization's net-new security control investments over the past 24 months, the vast majority said the investments were either moderate or significant across each type of control listed, including data security and privacy (90%), cloud security (90%), endpoint security (89%), and more (see Figure 7). This is an encouraging finding. It shows that risks are well understood and that organizations are allocating resources to enable the mitigation of those risks to levels that are acceptable.

Figure 7. The Level of Organizational Investment in Security Controls

Compared to 24 months ago, how would you characterize your organization's net-new investments in each of the following types of cybersecurity controls and technologies? (Percent of respondents, N=328)



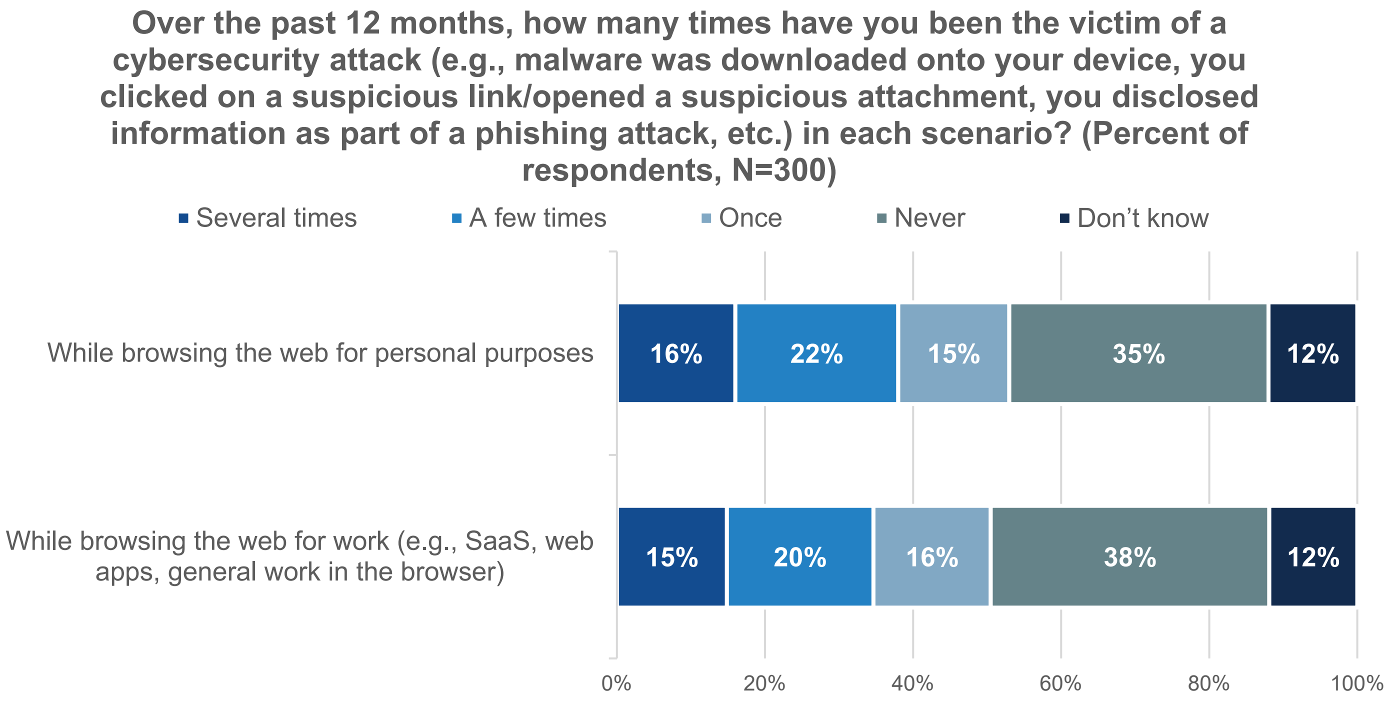
Source: Enterprise Strategy Group, a division of TechTarget, Inc.

However, while investments are significant, successful attacks are still occurring at an elevated level. When IT and security practitioners were asked approximately what percentage of knowledge workers at their organization they would estimate have fallen victim to any web-based threat/attack in the last 12 months, the average response was ~13%.

If accurate, the idea that more than 1 in 10 workers are being compromised on an annual basis is certainly concerning, but data directly from end users is even more troubling. The survey asked end users how many times in the past 12 months they had been the victim of a security attack while browsing the web for work. More than half (51%) reported they had been successfully attacked once, a few times, or several times (see Figure 8). And the fact that the problem is just as rampant when users are browsing in their personal lives is also problematic, as we will see many users browse the internet for work and personal reasons concurrently.

This end-user-reported data implies that the scope of successful attacks happening at organizations is likely much broader than most IT and security teams realize, and it also shows that organizations likely have a lot of work to do to accomplish their top security priority of gaining better capture and visibility into their environments.

Figure 8. The Frequency With Which End Users Report They Have Been Successfully Attacked



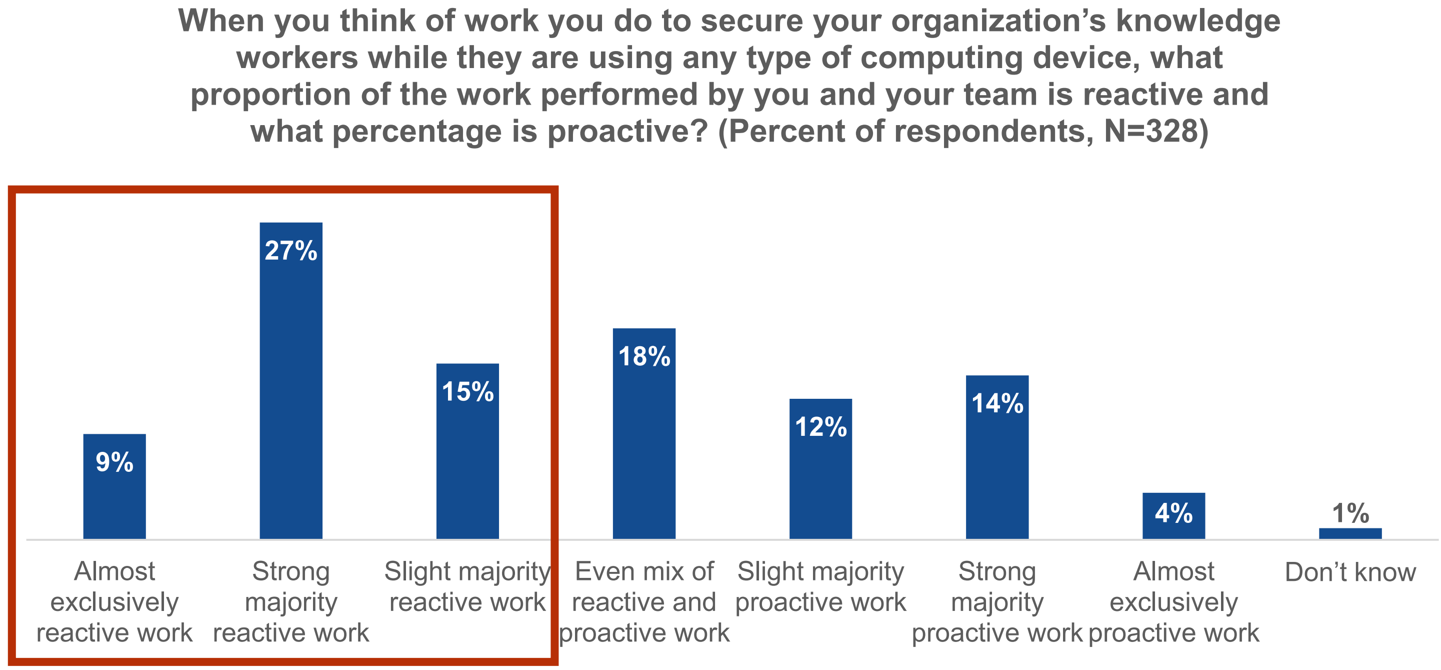
Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Factors That Make Effectively Securing Users So Challenging

Of course, protecting distributed workers who are using unsecured devices and have risky habits is a challenge, and we've already seen all of these dynamics at play within organizations. However, there are additional headwinds uncovered in the research.

First, most organizations are stuck in a mostly reactive mode when it comes to securing knowledge workers: 51% say the majority of tasks can be classified as "reactive," like responding to issues and remediating infections (see Figure 9). Just 30% say the majority of their tasks can be classified as "proactive," like enforcing best practices and educating users. Reactive approaches, in which organizations tend to respond to incidents as they occur, leave them vulnerable to both known and emerging threats. A proactive approach is essential to stay ahead of cybercriminals and to protect an organization's digital assets and reputation. It is worth noting that, regardless of their current mix of tasks today, a three-fifths majority (61%) of respondents do report that a shift to a more proactive approach to securing knowledge workers is desired.

Figure 9. Security Teams' Posture When Securing Knowledge Workers

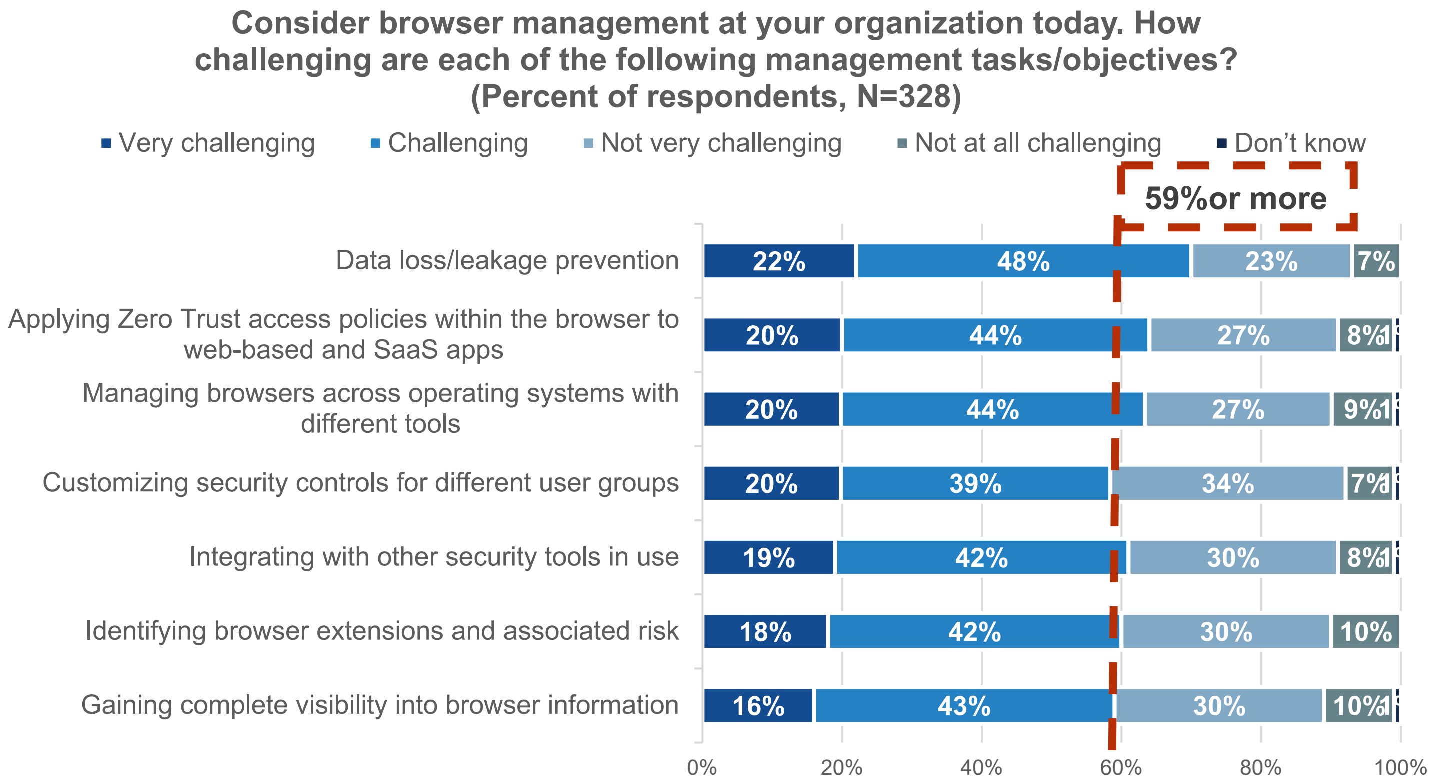


Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Next, in an interrelated finding, it is clear that organizations are grappling with the complexity of managing their browsers. When asked about the challenges associated with browser management tasks and objectives, 59% or more of IT and security respondents reported that each of them was challenging. These challenges include preventing data loss (70%), managing browsers across operating systems with different tools (64%), integrating with other security tools in use (61%), and more (see Figure 10). For many organizations, these challenges will make it difficult to achieve a more proactive approach to knowledge worker security.

Finally, the data reconfirms the adage that people are an organization's biggest vulnerability. When asked what is making it most difficult to secure users from web-based threats, the top two responses were that users are falling victim to phishing or malware (46%) and that end-user negligence is creating risk (38%). These points, taken together with the earlier finding that few organizations are prioritizing user training, make the case that IT and security teams would be well served by increasing their focus on security training for end users.

Figure 10. Challenges Associated With Browser Management



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Organizations Are Turning Their Attention Toward Enterprise Browsers

While challenges abound, organizations are not standing flat-footed in their efforts to better secure their knowledge workers. One step many organizations are beginning to consider is the adoption of an enterprise browser. Enterprise browsers are a relatively nascent security technology and the result of specifically designing a browser that prioritizes security and manageability. They typically include features like policy-based security, centralized management, and integrations with other enterprise security controls, helping to ensure a secure browsing experience for employees and protecting sensitive data.

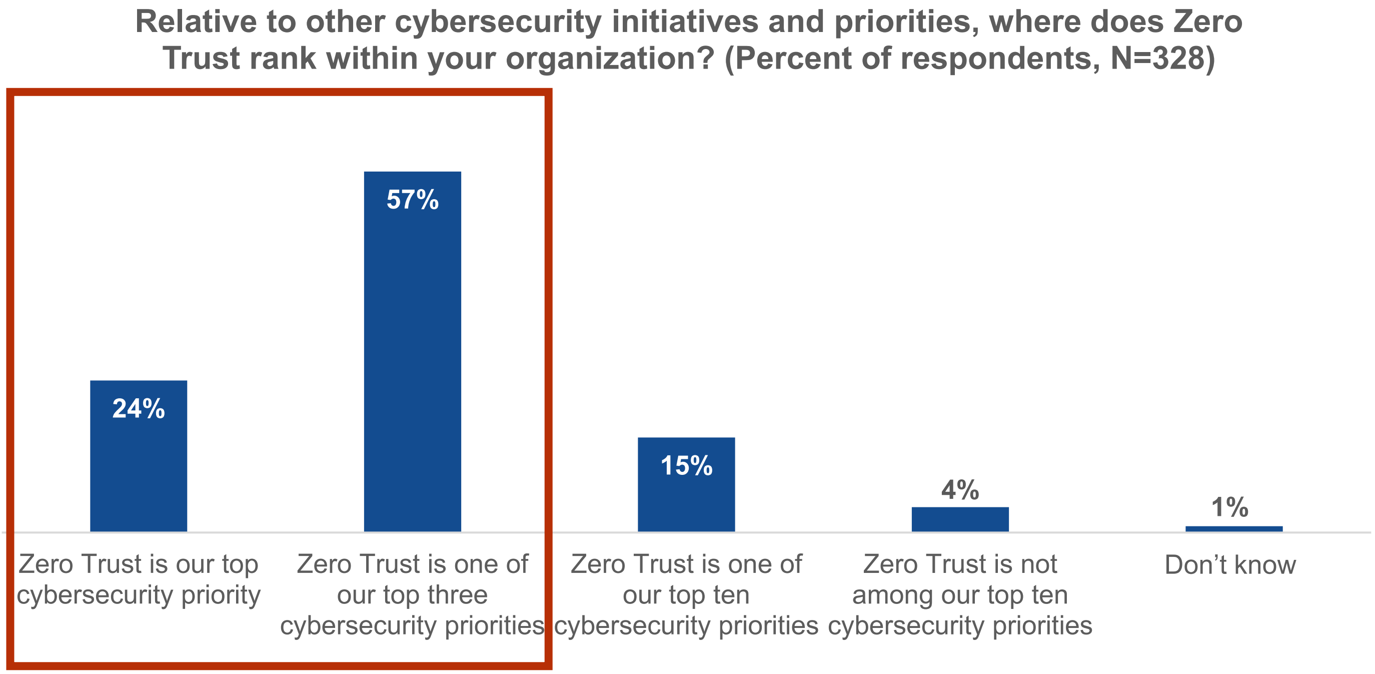
When asked, more than four out of five (81%) IT and security respondents reported their organization was very likely (38%) or likely (43%) to consider or invest in enterprise browser technologies in the next 12 months.

Organizations Are Turning Their Attention Toward Zero Trust Approaches

Another trend in cybersecurity is the adoption of Zero Trust strategies, which assume, by default, an organization's IT environment may be compromised and advocates for resource-specific (i.e., data, compute, and applications) access through a least-privilege model supported by continuous authentication, authorization, and risk evaluation for every request. The data clearly shows organizations are leaning into Zero Trust approaches to help: 81% of respondents say Zero Trust initiatives are one of their top-three cybersecurity priorities (see Figure 11).

Given that 64% of respondents say integrating Zero Trust access policies into the browser is a challenge today and that organizational focus on Zero Trust is so high, organizations should definitely prioritize enterprise browser technologies with proven integrations of Zero Trust solutions.

Figure 11. Zero Trust Takes Center Stage



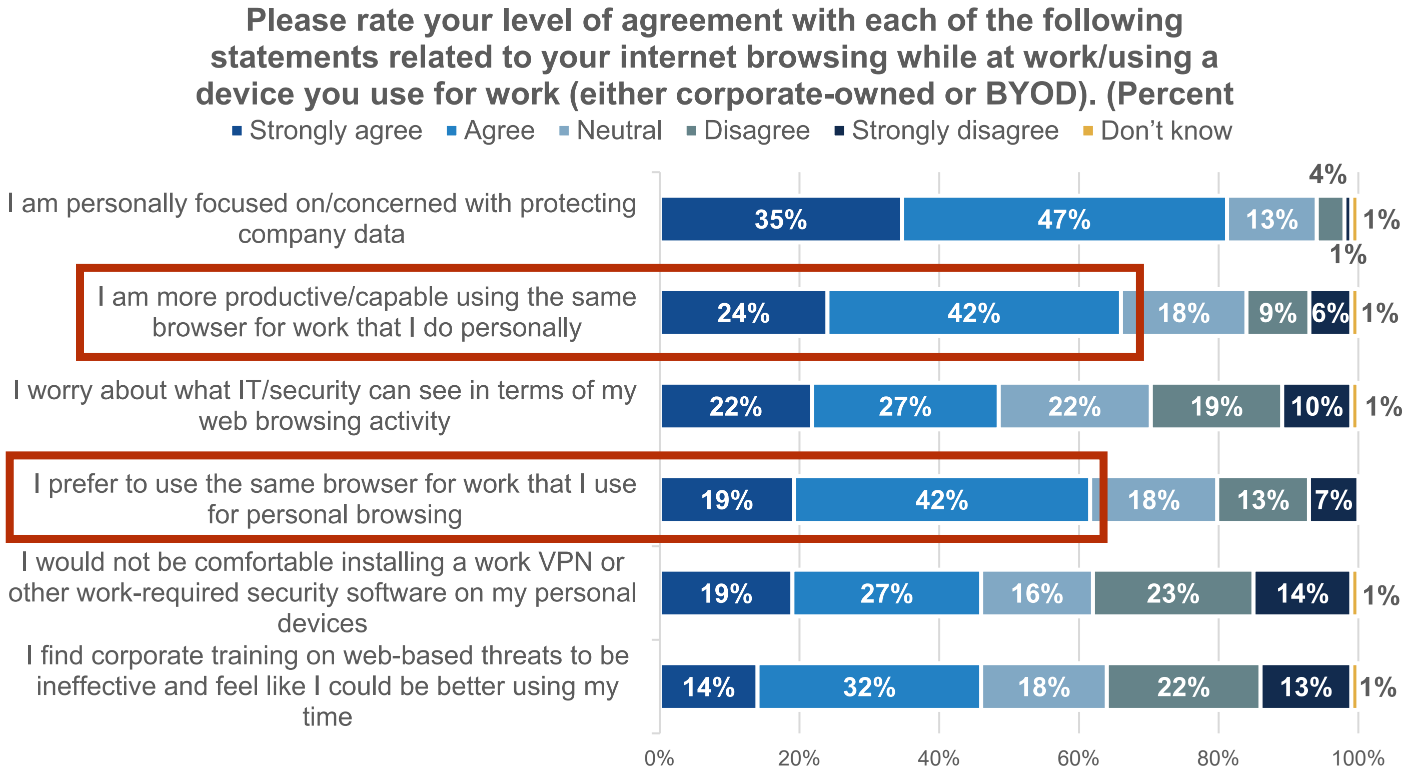
Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Data Shows Enterprise and Personal Browsing Should Be Unified

The way employees work, some of their questionable behaviors, and the rate of successful attacks all advocate for the deployment of enterprise browsing technology that enables organizations to implement stricter control over web access, monitor internet traffic for potential threats, and maintain a centralized policy management framework. The next question for an organization to address is how that experience should be delivered to employees. Here, the data points to unification.

First, when asked to agree or disagree with a series of statements about browsing the internet at work, we see a majority of knowledge workers (66%) reporting that they are more productive and capable when using a browser for work that they are familiar with from their personal lives. A similar majority (61%) also explicitly report they actively prefer to use the same browser for work that they use personally (see Figure 12). Additionally, it is heartening to observe that 82% of knowledge workers agree they are personally focused on protecting their company’s data. This indicates that organizations are effectively fostering a feeling that security really does require the full organization’s active participation. It is also instructive to note that many knowledge workers express a preference to maintain a level of privacy in their browsing: 49% are worried about what IT can see in terms of their browsing activity. Given that users will circumvent security when it is viewed as intrusive, browsers with the capability to allow employees to switch from personal to work profiles easily should be prioritized so that users can keep their work and personal lives separate.

Figure 12. End-user Perspectives Related to Browsing the Internet for Work



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Beyond improvements to productivity and aligning with user preference, another argument for unification is that users already intertwine their business and personal browser use. Respondents were asked how often they access non-work websites during the workday, and the majority (54%) reported this type of behavior on a daily, hourly, or continuous basis.

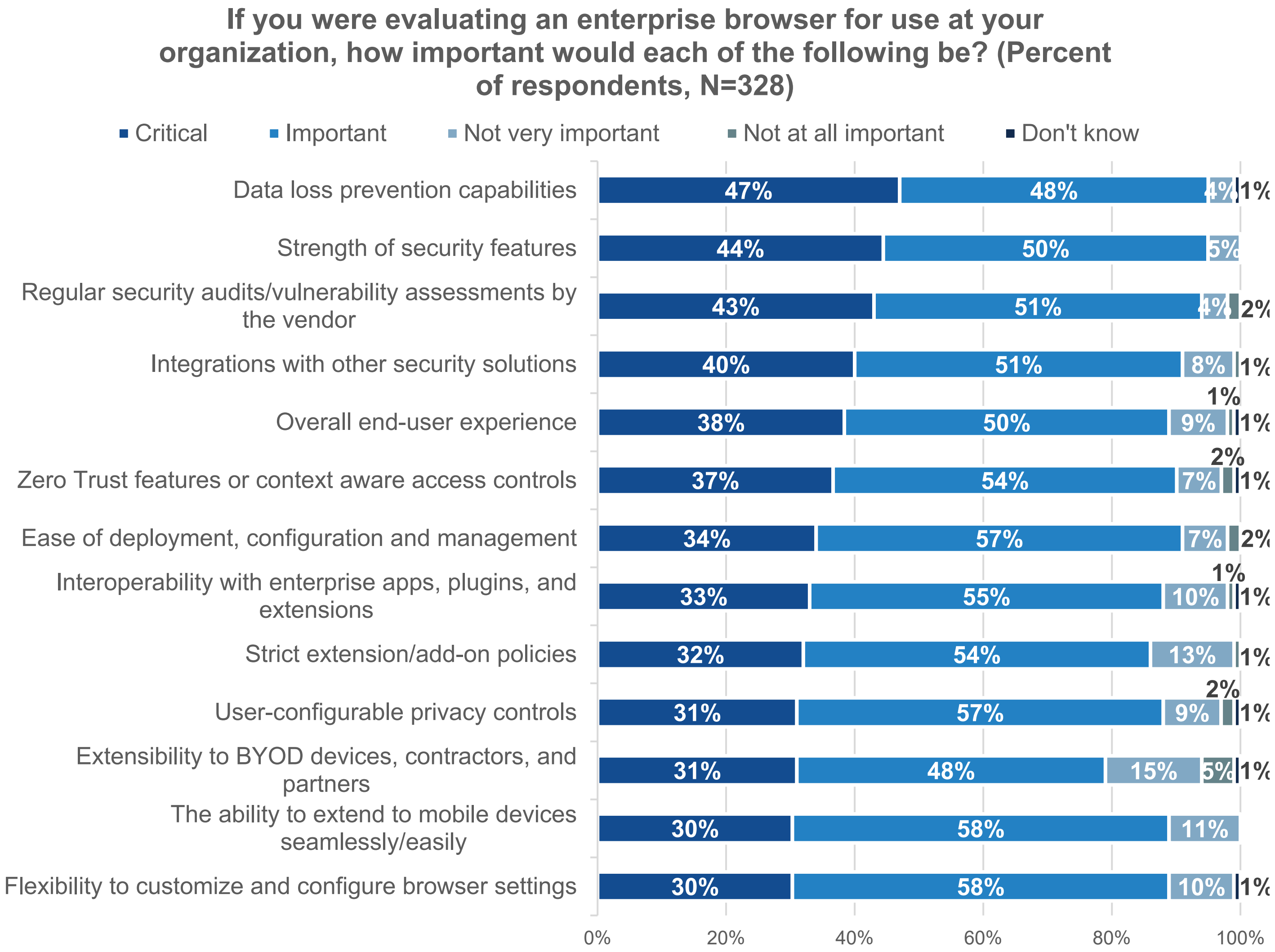
Peer-based Insights on What to Prioritize When Seeking Enterprise Browser Technologies

The data also provides insight into what IT and security decision-makers are prioritizing in terms of enterprise browser solution evaluation.

First, it appears a plurality of buyers are recognizing the merits of a unified browsing solution that can deliver work browsing in an experience that mirrors personal browsing. When asked to choose between two hypothetical sources of such a solution, the plurality (50%) reported wanting to buy from a vendor whose browser technology is already familiar to many employees, while just 36% reported a preference for sourcing this solution from a specialized provider of enterprise browser technology.

Second, in terms of what features are most important, the data shows that respondents prioritize data loss prevention capabilities (which is not surprising given the challenges associated with data loss discussed previously), results of regular security audits and vulnerability assessments provided by the vendor, strong integrations, and the end-user experience (see Figure 13). The recent advent of public generative AI tools is likely one reason why DLP capabilities are so top of mind. As more and more knowledge workers leverage these tools over time and potentially use sensitive information in their prompts, the ability to mitigate this risk will continue to be critical.

Figure 13. Importance Associated With Various Enterprise Browser Capabilities



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Finally, when asked which browsers on the market today are considered to be enterprise browsers, Google's Chrome led the way with 78% of respondents (outstripping Mozilla Firefox [51%] and Microsoft Edge [47%]).

Each of these insights can be instructive for IT and security decision-makers who want to adopt an enterprise browser but may not be sure where to start.

Conclusion

It's clear that there are several trends in how knowledge workers do their jobs that make securing an organization's data difficult. It's also clear that IT and security teams need to adapt their approaches, as the level of successful attacks targeting knowledge workers on the web is very high. Based on the data in this report, we have five recommendations for IT and security decision-makers:

1. **Enterprise browsers have merit and momentum.** If your organization has not begun evaluating solutions in this area, or if you are unaware of developments in this space, further exploration is warranted.
2. **When evaluating different browser technologies, focus on DLP.** Technology decision-makers are putting this functionality at the top of their requirements list, and with the use of browser-based generative AI solutions only poised to grow over time, the importance of controlling data leakage cannot be overstated.
3. **Integrations with Zero Trust should be prioritized.** In the course of evaluating enterprise browser technologies, special consideration should be given to their ability to integrate with Zero Trust solutions your organization is using or considering. The data shows applying Zero Trust policies to browsers has been problematic to date, and with so many organizations heading down a Zero Trust path, solving this problem should be top of mind.
4. **Renewed focus on end-user training is warranted.** While organizations are ramping up investments in security controls, the data implies end-user training is lagging in importance. While more can be done from a technology perspective to protect users from themselves, for many organizations, better user enablement is likely to improve outcomes.
5. **Digital experience is heavily influenced by the end-user browser experience.** As users depend on the browser to provide access to half of their business-critical applications, providing a unified, consistent, least-friction browser experience has a direct impact on user satisfaction. Care should be taken when considering adding security controls to the browser that may add friction or create roadblocks to accomplishing tasks.

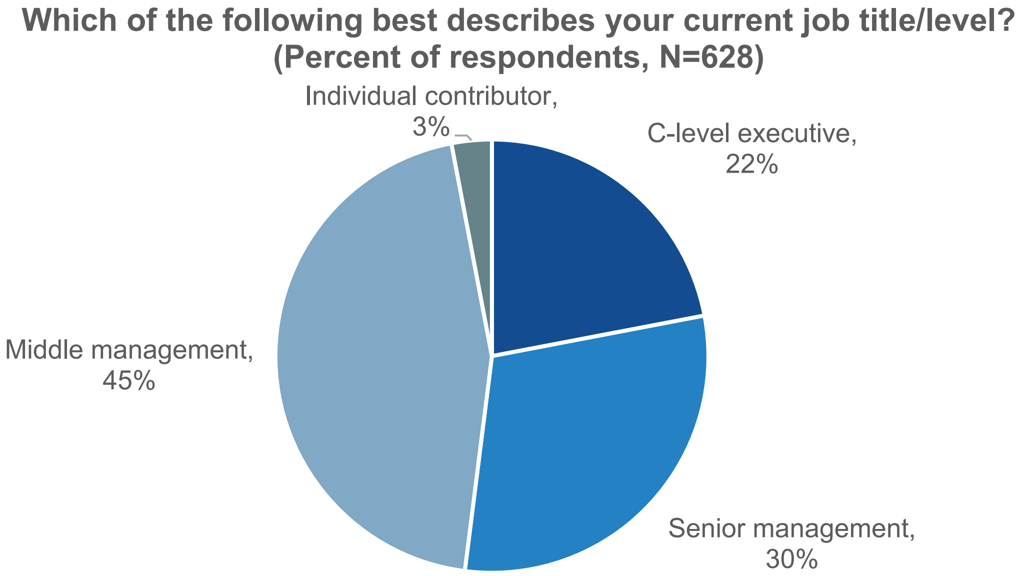
Research Methodology and Respondent Demographics and Firmographics

This report is based on a comprehensive survey of IT and cybersecurity decision-makers knowledgeable about their organizations' tools, policies, and procedures for securing knowledge workers, as well as knowledge workers themselves who spend the majority of their productive time on a laptop or desktop computer. Respondents represented organizations in the U.S. (33%), Canada (10%), the U.K. (21%), Germany (20%), and France (16%). Organizations represented spanned enterprises (i.e., organizations with 1,000+ employees, 75%) and midmarket entities (i.e., organizations with 100-999 employees, 25%).The survey was fielded between August 15 and August 29, 2023. All respondents were provided an incentive to complete the survey.

After applying screening criteria and data quality control best practices, a final sample of 628 respondents completed the survey. Figure 14 through Figure 16 detail the demographics and firmographics of the respondent base.

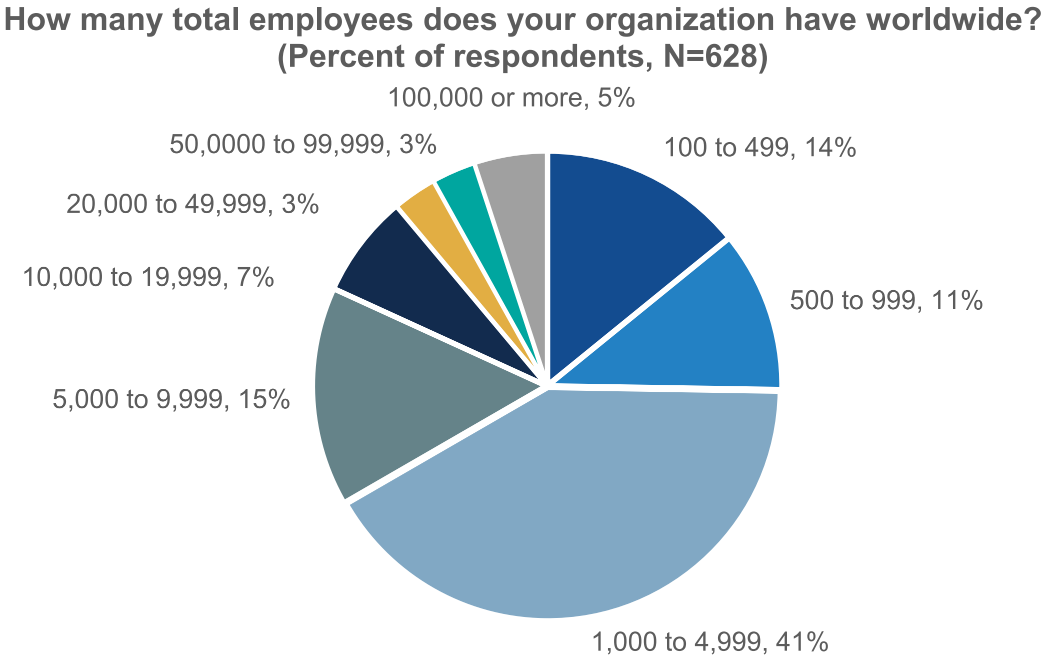
Note: The margin of error of a sample of N=628 is + or – 4 percentage points. Totals in figures and tables throughout this report may not add up to 100% due to rounding.

Figure 14. Respondents, by Seniority



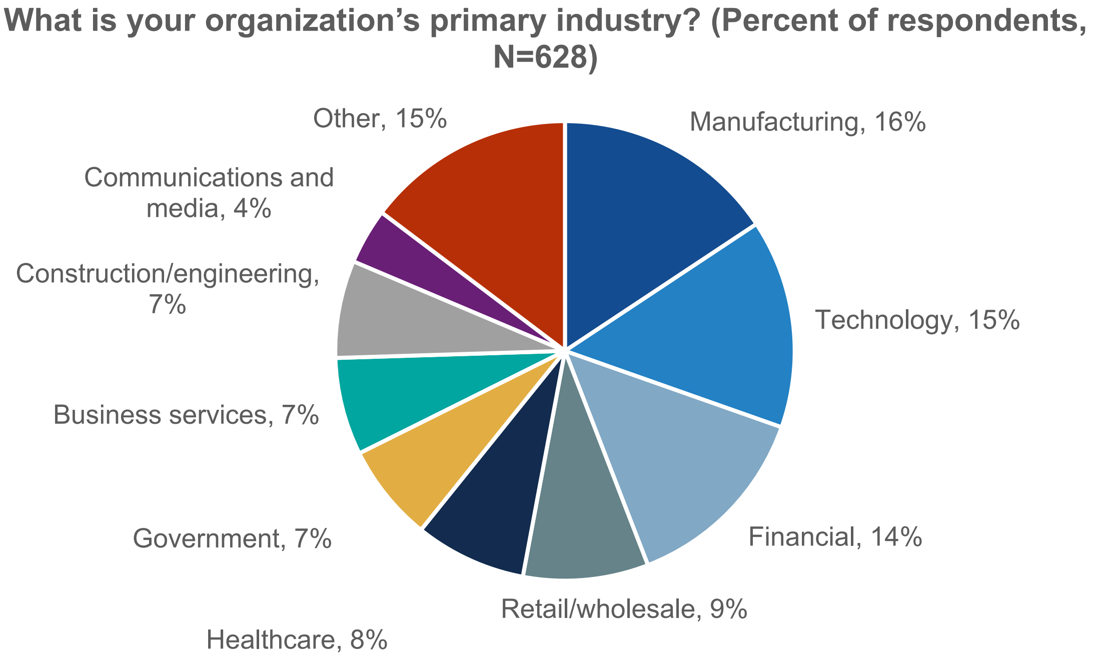
Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Figure 15. Respondents, by Company Size



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Figure 16. Respondents, by Industry



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Information contained in this publication has been obtained by sources TechTarget considers to be reliable but is not warranted by TechTarget. This publication may contain opinions of TechTarget, which are subject to change. This publication may include forecasts, projections, and other predictive statements that represent TechTarget's assumptions and expectations in light of currently available information. These forecasts are based on industry trends and involve variables and uncertainties. Consequently, TechTarget makes no warranty as to the accuracy of specific forecasts, projections or predictive statements contained herein.

About Enterprise Strategy Group
TechTarget's Enterprise Strategy Group provides focused and actionable market intelligence, demand-side research, analyst advisory services, GTM strategy guidance, solution validations, and custom content supporting enterprise technology buying and selling.

✉ contact@esg-global.com
🖥 www.esg-global.com