EMA™
IT & DATA MANAGEMENT RESEARCH,
INDUSTRY ANALYSIS & CONSULTING

Sponsored by:
yubico

The Rise of Low-Friction Access

Emerging Requirements and Solutions for Boosting Workforce Productivity and Security Assurance

November 2022 EMA Research Report

By Steve Brasen, Research Director

Table of Contents

Executive Summary

Driven by accelerating IT security threats, increased requirements to support remote workforces, the introduction of zero trust initiatives, and evolving user expectations on technology performance, organizations are broadly introducing new requirements for identity security. To provide businesses with actionable guidance on identifying the optimal path to streamlining authentication processes, Enterprise Management Associates (EMA) conducted primary research with the goal of identifying current requirements, challenges, and adopted solutions in relation to mitigating access friction. For the research, two independent surveys were conducted: the first eliciting responses from business workers who utilize computing technologies to perform more than 50% of their job tasks, and the second querying information from business IT managers to identify organizational requirements.

Key findings from EMA's end-user survey include:

- With pandemic restrictions mostly removed, only 9% of professionals perform all business tasks physically in the office
- 47% of all business tasks are performed outside of the physical office
- 11% of respondents stated that they would actively seek employment elsewhere if required to perform high-friction authentication
- 53% of respondents indicated that the availability of passwordless authentication technologies is a significant consideration when evaluating a new employment opportunity
- On average, business users authenticate eight times each day and must reset passwords ten times each month
- 73% of surveyed business professionals report that authentication impacts their work satisfaction and performance
- On average, business users lose or forget a credential seven times each month; however, incidents of lost or forgotten credentials only averaged three times per month among adopters of security keys
- The recovery of lost or forgotten credentials was noted to be the most frustrating identity security process by 82% of respondents
- Individuals who are required to change passwords at least once per month were ten times more likely to forget passwords than those required to reset passwords less frequently
- Business workers employing security keys have the highest satisfaction rates with their organization's authenticators, according to 91% of surveyed adopters

Key findings from EMA's business survey include:

- Improving employee experience was most frequently indicated to be a priority for adopting enterprise identity security solutions
- 87% of surveyed businesses indicated that their organization experienced an identity-related security breach in the preceding 12 months
- Security breaches were 22% more frequent among organizations with workforces that perform more than 50% of tasks outside of the office
- Security breaches were 11% more frequent among organizations using in-house-developed identity security solutions
- 93% of organizations experiencing a security breach reported severe consequences as a result, including IT service failures, employee impacts, and diminished business performance

- Employees from organizations using passwords submit an average of 95 identity-related support requests each year, while those using fully passwordless authenticators only submit 17 support requests annually
- The introduction of adaptive authentication technologies reduces the annual number of identity-related support requests by 39%
- Organizations using adaptive authentication solutions achieve the highest satisfaction rates with their adopted solutions
- Hardware tokens were noted to significantly reduce challenges related to "enabling access from non-business-owned devices"
- 83% of survey respondents have adopted FIDO standards, and the most frequently reported motivation for adoption is to "improve security effectiveness"
- 71% of adopters of FIDO standards were confident their solution will prevent "nearly all" security breaches, while only 29% of non-FIDO adopters had the same level of confidence
- The adoption of FIDO standards was noted by businesses to significantly improve end-user experiences and administrator productivity
- Adopters of passwordless authentication solutions were significantly more likely to report that their adopted identity management environment has resulted in quantifiable IT operational cost savings than those reliant on password-based authenticators

The New Paradigm in Identity Security

The key to establishing effective enterprise IT security is to positively identify end users and enforce business policies without diminishing end-user experiences. To managers of traditional IT security systems, this may sound like an impossible contradiction in IT service delivery, but it is, in fact, quite attainable. The commonly held belief is that security and user experiences are diametrically opposed forces. In other words, as you increase one, you decrease the other. However, this is typically not the case. Simply put, when users are presented with IT services that are easily accessible, they are far less likely to bypass established security controls. Additionally, most of the more modern and easier-to-use authentication methods are more challenging to defeat. As a result, organizations that focus on improving user access experiences typically achieve significant improvements to security effectiveness.

Simply put, when users are presented with IT services that are easily accessible, they are far less likely to bypass established security controls.

The term "friction" is most frequently used to indicate the number and complexity of tasks a user must perform to access business IT services. High-friction access approaches not only diminish security, but also substantially impact user productivity. Business employees in particular should not have to "jump through hoops" in order to access the IT resources they require to perform job tasks. In fact, any time a worker is distracted by engaging in a complex authentication process, it can take as much as 20 minutes for them to refocus their attention back on the tasks they need to complete.

Unfortunately, much of the business acceptance of high-friction access processes derives from legacy security practices. Since the early days of computing, system engineers have recognized the need to differentiate users by establishing individual accounts and the primary method of authentication was a shared secret, such as password. Prior to the introduction of distributed computing and the internet, the use of passwords was a reasonable approach. After all, users typically only needed to memorize a single, easy to remember set of characters. Today, however, individuals maintain hundreds of personal and professional accounts across devices, business servers, and clouds. It is simply impossible for modern users to memorize complex and unique password strings for each of these services, let alone regularly change all passwords to meet security requirements.

Faced with high-friction and impossible password security demands, most individuals will place themselves and the business at risk by violating policies and employing weak practices. For instance, nearly all users employ the same password for multiple accounts. This is particularly dangerous because when one of those accounts is compromised, the attacker can use those credentials to access any of the other accounts set with the same password. Even worse, compromised passwords are often posted on the dark web, making them accessible to the entire community of malicious actors. Other poor password hygiene practices commonly used include writing down passwords, using weak password strings, and sharing passwords with others.

The broad reliance on antiquated password security processes continues to be the weakest link in modern security management. Faced with the severe repercussions of breach events, it is common among business security professionals to blame the users for not following established policies. However, it is not the general employees' primary job to meet security protocols. Their focus is and should be on meeting their assigned tasks to drive business profitability and success. If high-friction access processes are inhibiting workers from completing their business tasks, then the processes need to change. It should not be incumbent on the users to adapt to the requirements of IT systems. Rather, IT systems should adapt to the requirements of the users.

Recognizing that traditional password-centric authentication processes are no longer effective at preventing security breaches and are the chief contributor to diminishing user productivity and experiences, a fundamental shift in identity and access management (IAM) best practices has emerged over the past few years that broadly embraces low-friction authentication solutions. Key voices establishing IT best practices, such as the National Institute for Standards in Technology (NIST), have challenged traditional authentication approaches by recommending lower-friction alternatives. For instance, the 2017 NIST Special Publication on Digital Identity Guidelines states that passwords and other credentials should never be changed unless they have been determined to have been compromised, significantly reducing the burden on the end users. The document also promotes the use of passwordless technologies as part of a multi-factor authentication (MFA) strategy.

Recent zero trust initiatives issued by the U.S. federal government have reinforced and expanded the new NIST identity security requirements. Released in January 2022, an official memo issued by the Executive Office of the President outline a set of directives to be implemented in all federal institutions by the conclusion of 2024. These included the adoption of strong phishing-resistant MFA that incorporates at least one device-level signal alongside identity information. Additionally, the memo notes that "agencies are encouraged to pursue greater use of passwordless MFA (FIDO-based or smart card) as they modernize their authentication systems."

While enhanced security is a powerful driver of low-friction authentication adoption, other motivators are also emerging that are accelerating interest in adopting more user-friendly access technologies. For example, many organizations are introducing low-friction access solutions to boost workforce productivity to help achieve performance goals, improve business agility, and attain a competitive advantage in dynamic marketplaces. This is particularly of interest as organizations have shifted to supporting knowledgeable employees who predominantly operate out of home offices. It is also increasingly becoming clear that enabling positive user experiences with the use of technology is essential for attracting and retaining talented workers.

While enhanced security is a powerful driver of low-friction authentication adoption, other motivators are also emerging that are accelerating interest in adopting more user-friendly access technologies.

Clearly, we are currently experiencing a paradigm shift in how users view and implement identity security. Adoption trends and user preferences all point to a greater acceptance and favorability toward passwordless and other low-friction access technologies. However, emerging concerns are also prevalent as businesses struggle to determine which IAM approaches will best meet their unique organizational requirements.

Research and Methodology

To quantify the value of low-friction access solutions and provide guidance on which types of solutions to adopt, EMA has conducted primary research into the evolving requirements, challenges, and outcomes resulting from utilizing modern identity security technologies. For the research, EMA conducted two independent surveys targeting technology-focused end users and business IT managers of identity services. Each survey netted at least 100 respondents distributed across a variety of industry verticals and horizontals, and all were carefully vetted to ensure they were qualified to answer the respective questions. Nearly all respondents were indicated to physically reside within North America. Survey results were tabulated to ensure statistical relevancy within a 5% margin of error. Full demographic details of survey respondents can be found in the Appendix of this report.

End-User Survey

Target respondents for the first survey were full-time business workers who use a computer to perform greater than 50% of their job tasks. No limitations were made on the respondent's department or role; however, the majority were indicated to have a vocation in IT development, management, or administration. Respondents were vetted to ensure they understand the basics of identity security (such as recognizing different types of authenticators) so they could effectively answer questions about their access experiences.

Business IT Survey

Survey respondents were identified as responsible for and knowledgeable about their organization's identity and access management (IAM) solutions. Roughly 68% of respondents held a senior position as either a manager or director of IT operations, while 84% of total respondents were part of information technology or information security departments. Eighty percent of respondents described themselves as very familiar or experts on identity and access management practices and solutions.

Emerging Business Priorities

Enterprise Identity Security Priorities

It should come as no surprise that recent years have seen a fundamental shift in how people interact with technology. This has been particularly visible in workplace utilizations of devices, applications, and other IT services, and management requirements and styles are being forced to adapt to the new paradigm. Traditional IT management approaches business technology utilization with a heavy hand by requiring workers to use the resources the business provides, in the way the business expects them to be used. Whereas, modern solutions must be flexible and incorporate user experiences. Nowhere is this more applicable than with the implementation of identity security.

In total, 71% of surveyed businesses reported that improving employee experiences or increasing workforce productivity is currently a top priority for their IAM. These requirements were more frequently identified than other identity security needs, including meeting zero trust initiatives, achieving regulatory compliance, and reducing IT management efforts and costs (Figure 1). This indicates a significant change in business priorities from previous years. EMA research conducted in 2020[1] indicated that workforce experiences and productivity were only a priority for 63% of organizations, and a similar survey in 2019[2] only indicated these to be a priority for 31% of organizations.

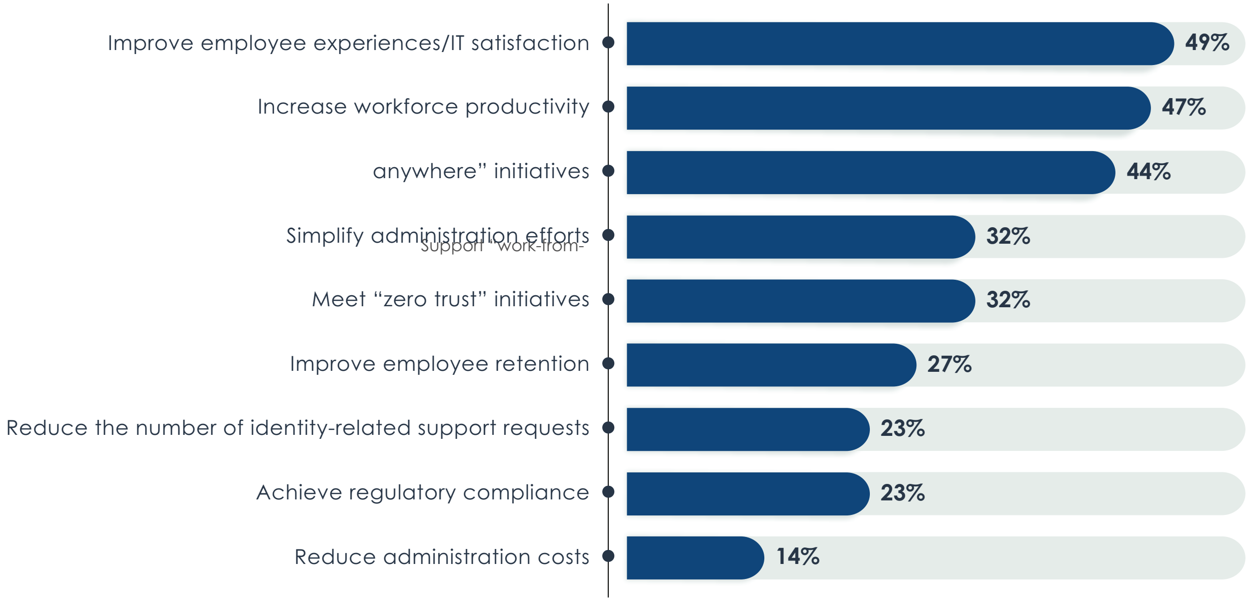


Figure 1: Percentage of surveyed businesses indicating top IAM priorities for their organization

[1] "Contextual Awareness: Advancing Identity and Access Management to the Next Level of Security Effectiveness," March 2020
[2] "Passwordless Authentication: Bridging the Gap Between High-Security and Low-Friction Identity Management," July 2019

Supporting Remote Workforces

It is not a coincidence that the prioritization of end-user work experiences broadly accelerated during the first two years of the COVID-19 pandemic. When most workers were suddenly forced to operate out of home offices, businesses scrambled to enable remote access capabilities, many of which resulted in diminished user performance. Among business survey respondents, 44% noted that supporting “work-from-anywhere” initiatives is now a priority for their organization, indicating a significant interest in resolving remote access friction challenges.

Challenges related to empowering remote workers with secure access to business IT resources have not subsided with the elimination of pandemic restrictions. Only 9% of surveyed users that use a computer to perform more than half of their job tasks reported that they had returned full time to the office. Another 9% indicated they now operate full time outside of the physical office. The remaining 82% of workers function part time in the office and part time out of the office. According to business survey respondents, roughly 48% of all business tasks are performed externally from physical offices (Figure 2).

Larger organizations (with more than 5,000 employees) reported more than half (53%) of business activities are being performed remotely from the business. The same demographic was the most likely to indicate that supporting “work-from-anywhere” initiatives is a priority for their IAM solutions, according to 63% of related organizations, as opposed to only 37% of smaller-sized businesses. This is likely due to sheer numbers—more employees means more opportunities for out of office activities. However, it does showcase that larger businesses are somewhat more apt to adopt identity solutions designed to support remote workforces. Among industry verticals, telecommunication, finance, and government institutions indicated that the highest frequency of tasks is being performed from home offices. Conversely, education and healthcare organizations were most likely to have tasks performed within the business facility.

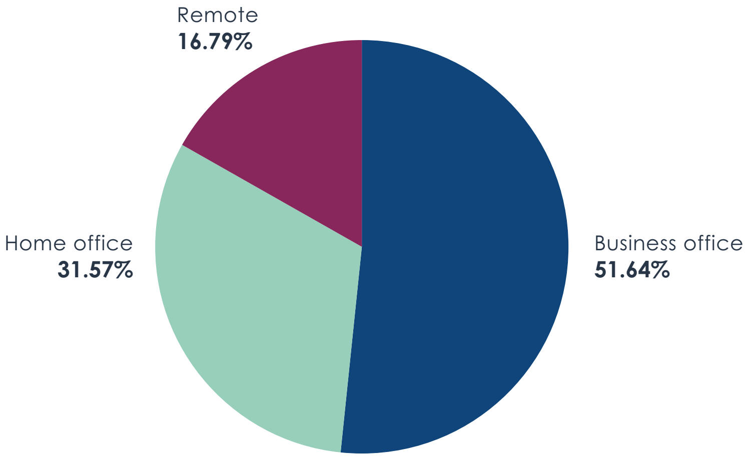


Figure 2: Average percentage of time workers perform tasks at each location, according to surveyed businesses

Attracting and Retaining Talent

Today's business employees recognize technology performance and ease of use as key components of their job performance and satisfaction. In fact, many view them as forms of compensation on par with other employment benefits. EMA research identified the performance of authentication tasks as the greatest inhibitor to workforce productivity.[3] Cumulative incidents of access friction are the cause of significant work stress, and modern workers have low tolerances for what they perceive to be performing unnecessary actions to access job-required IT services. In fact, 73% of surveyed business employees reported that authentication impacts their work satisfaction and performance.

Among surveyed end users, 26% reported they would decrease the amount of time spent accessing business IT services if faced with high-friction authentication processes, decreasing their effectiveness at meeting business requirements. Another 11% of (roughly one in ten) surveyed users indicated they would actively seek employment elsewhere if faced with access processes that were difficult and time-consuming. This loss of knowledgeable workers can be significantly detrimental to the ability of the organization to meet performance goals and profitability because they take valuable experiences and knowledge of business processes with them.

While high-friction access is a strong detractor for business workers, low-friction solutions can be a substantial incentive. When asked to rate how much of a priority the availability of passwordless authentication technologies would be to their job selection decision if they were seeking a new employer, 53% identified it as a significant consideration (Figure 3). Attracting knowledgeable and talented workers is a significant challenge in today's dynamic job markets, and many businesses are challenged to compete with salary incentives alone. Presenting the business as a modern, tech-savvy workplace with low-friction access technologies can be a powerful incentive for employment.

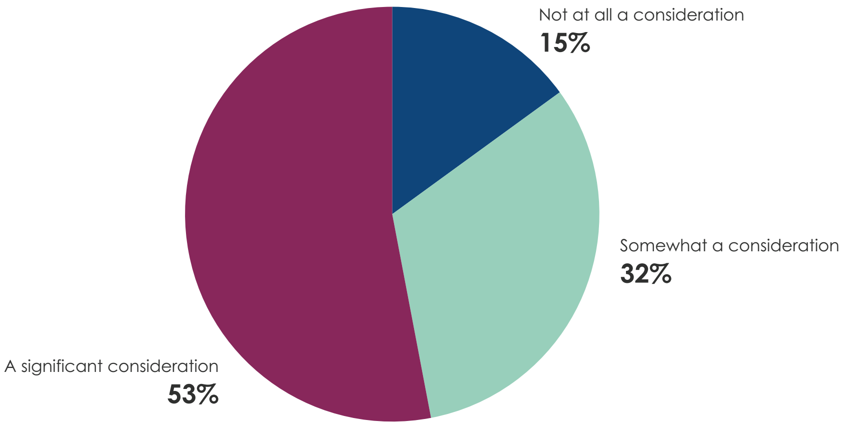


Figure 3: Percentage of survey respondents indicating how much of a consideration the availability of passwordless authentication technologies would be in selecting a new employer

[3] "Identifying Effective Digital Employee Experience (DEX) Management Solutions: A Quantitative Analysis," October 2021

Modern Employee IT Experiences

Frequency of Authentications

The number of times employees must perform authentication tasks each day is a clear indicator of the impact identity security has on their productivity. On average, surveyed business users reported they need to authenticate roughly eight times each day in order to access business IT services. Each authentication task constitutes a distraction from performing business tasks, particularly if they involve high-friction processes. Collectively, the average frequency of authentications likely results in a loss of one to two hours of productivity per worker per day.

Among business employee roles, individuals from sales departments noted the highest frequency of authentications with about 12 per day, while engineers and customer service representatives reported the lowest frequencies at only five per day. Authentication frequencies were higher among individuals who regularly log in to open screen locks on their personal PC or mobile devices, and somewhat lower among responders reliant on public web-based applications. Undoubtedly, this is due to the prevalence of single-sign on and extended login timeouts common to web applications. While average authentication frequencies were noted to be roughly identical among Windows, macOS, iOS, and Android device users, respondents utilizing Chromebooks reported significantly higher occurrence rates (10 times per day).

The location at which employees access business IT services also appears to impact authentication frequencies. Among survey respondents who perform the majority of their business tasks inside the office, authentication frequencies were noted to be significantly higher (Figure 4). While at first glance this may seem counterintuitive, it is a reflection of the relationship between identity requirements and job roles. Workers who are required to be physically in the office are more likely to be highly regulated and access more sensitive business applications and data. Home workers are more likely to rely on web apps and may even disable screen locks, reducing authentication requirements.

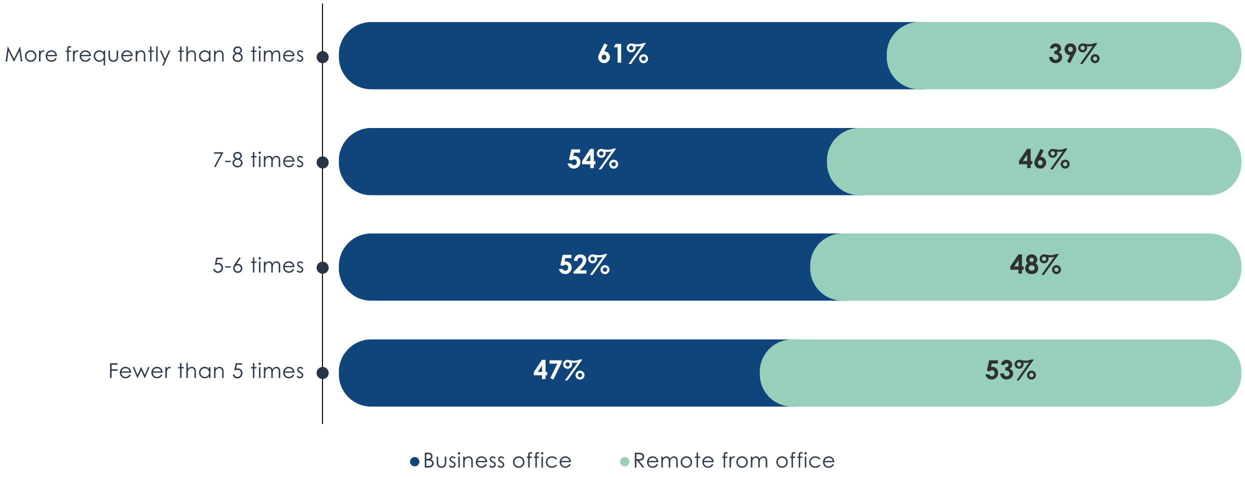


Figure 4: Percentage of time surveyed business users perform job tasks in and out of the physical office segmented by the average number of times they authenticate each day

Frequency of Forced Credential Resets

The 2017 Special Publication on Digital Identity Guidelines published by the National Institute of Standards and Technology (NIST) states that "Verifiers SHOULD NOT require memorized secrets to be changed arbitrarily (e.g., periodically)" unless there is evidence they have been compromised. Nonetheless, the majority of businesses continue to require periodic password resets on devices, applications, and IT services. On average, surveyed workers reported they had to change passwords ten times per month across the various resources they use to perform job tasks. Password resets can be extremely time-consuming and disruptive to employee productivity. Three-quarters (75%) of surveyed business workers identified "resetting passwords" as a "frustrating" task. An equal number of respondents recognized "creating new and unique passwords" as frustrating.

Password change requirements were more frequent among larger organizations (with greater than 5,000 employees), averaging 13 times per month. This is likely due to an increase in the number of supported applications and IT services among larger businesses. Additionally, credential reset frequencies were noted to be higher among organizations than their own business applications, either on-premises or in the cloud, as opposed to those using public SaaS and web applications (Figure 5).

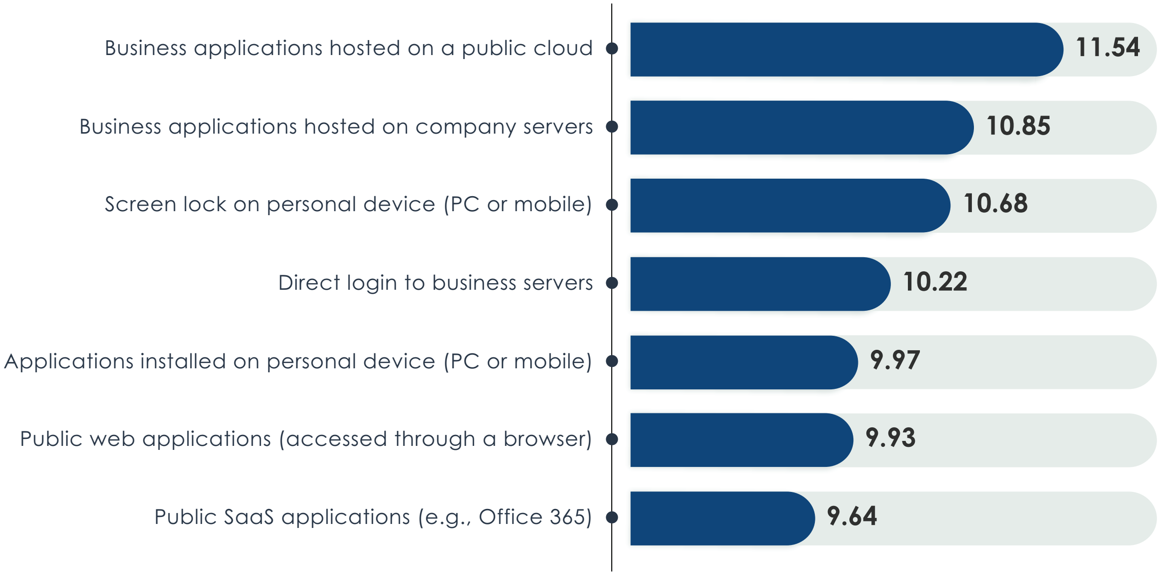


Figure 5: Average number of times per month surveyed business users reported they are required to reset passwords segmented by types of IT resources they access

Frequency of Forgotten Credentials

Tasks involved with the recovery of lost or forgotten credentials were identified by 82% of surveyed business employees as “frustrating,” indicating it to be the most impactful identity security process on workforce IT satisfaction. Given the dozens or hundreds of passwords individuals are required to set in order to access both personal and business accounts, it is not surprising that complex password strings are often forgotten. On average, surveyed business employees reported having to recover or reset a lost or forgotten credential seven times each month across the various business-related accounts they use.

Survey respondents who utilize security keys were noted to lose passwords least frequently (only about five times per month, on average). It is notable that the majority of related respondents utilize security keys as a second factor of authentication in addition to a traditional login and password. In these cases, passwords need to be recalled very infrequently on accounts supported by the security keys.

Survey results indicate a direct relationship between the frequency of forced password resets and incidents of forgotten credentials (Figure 6). Respondents noting that their organization requires them to reset a password at least once per month were roughly eight times more likely to lose or forget a credential in that timeframe. This correlation clearly exemplifies the value of NIST’s recommendations. Forcing users to frequently change passwords means they are required to memorize a greater number of character strings, substantially increasing the chances one will be forgotten. The eradication of forced password resets, therefore, has a double benefit to improving user experiences—eliminating frustrating reset processes while reducing incidents of recovery.

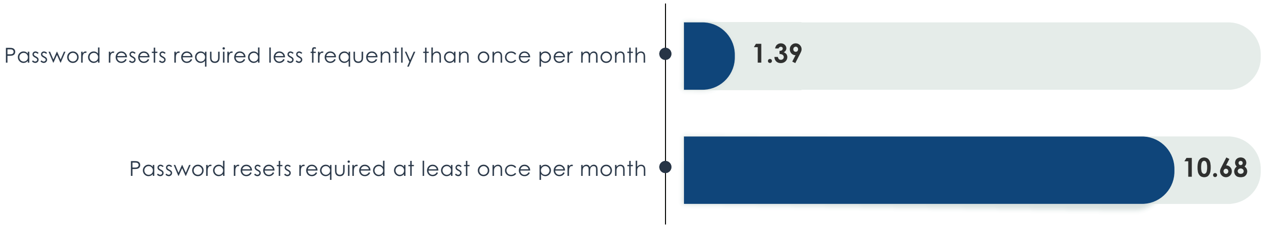


Figure 6: Comparing the average number of times credentials are lost or forgotten between those forced to reset passwords less and more frequently than once per month

Business Authenticators

Authenticator Adoption

The types of hardware or software resources used to identify an individual before authorizing access broadly determine security effectiveness and user experiences. Not surprisingly, passwords continue to be the primary form of authentication employed in business settings (Figure 7). Only 16% of respondents indicated they use entirely passwordless methods for accessing business IT resources. Among passwordless approaches, fingerprint biometrics, security keys, and hardware tokens, app-generated codes (such as Authy and Google Authenticator) were noted to be most frequently in use. Fingerprint readers are included with most mobile devices and some PC form factors, accounting for their popular use among almost half of survey respondents. Adopters of app-generated code authenticators were indicated to be 32% more likely to perform the majority of business tasks remotely from the physical office than those operating on-premises. This suggests related solutions were adopted to support "work-from-anywhere" initiatives.

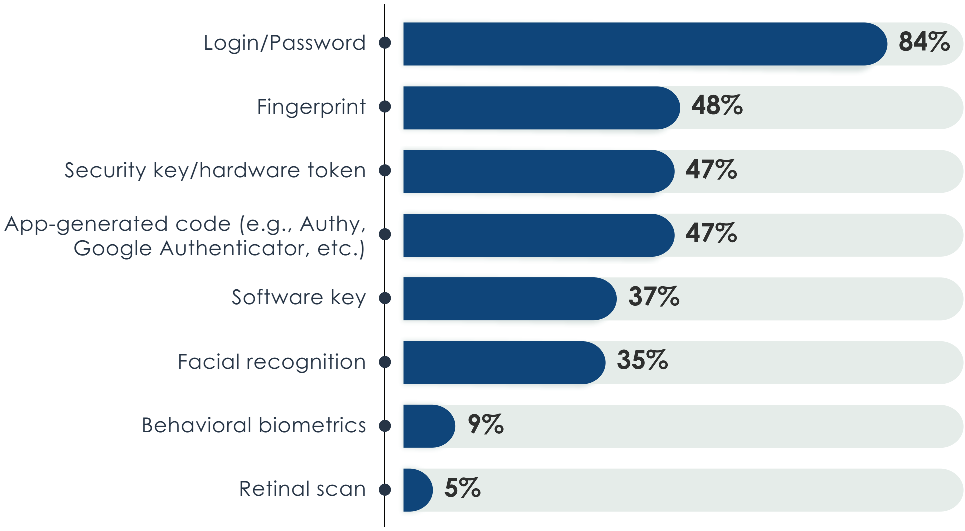


Figure 7: Percentage of surveyed business workers indicating the types of authenticators they use to access business IT resources

Despite the fact that security keys need to be purchased independently of endpoint devices, they are popularly adopted in many business scenarios. One-third of surveyed organizations indicated they support security keys today, which were particularly noted to be popular among responders from financial, healthcare, and manufacturing institutions. Security keys are physical hardware devices and are considered low-friction approaches to authentication because they enable access based on their proximity or connection to endpoint devices. By contrast, legacy hardware tokens/key fobs (also employed by about one-third of surveyed businesses) are considered higher friction because they require the user to manually copy a code from the token/key fob to the access interface. Almost half of surveyed business employees reported they regularly use either a security key or hardware token.

Interestingly, facial recognition software, which is now fairly common on mobile devices, was noted to be employed by only about one-third of survey respondents. This indicates less-favorable opinions on facial recognition likely due to the unreliability of some of the available solutions, such as challenges with centering a face in the camera or achieving a positive recognition with facial changes (e.g., makeup, hair style changes, etc.). While some facial recognition solutions are much better than others at positively identifying users, any bad past experiences will likely inhibit their broader adoption and use.

Behavioral biometrics offer another low-friction alternative to traditional passwords by identifying users based on their unique interactions with technology. For instance, related solutions may identify users by the amount of pressure they apply to mobile device screens, typing speed, mouse movements, and gait detection. More advanced approaches will collect multiple physical and cognitive identifiers and employ intelligence technologies (such as machine learning) to determine the probability that users are who they claim to be. While the technology is promising, only 21% of surveyed businesses reported they support related solutions, and only 5% of surveyed workers reported actually using them. According to business responders, the primary reasons they are not more broadly adopted are because they are considered too expensive and difficult to implement.

Authenticator Preferences

The level of friction imposed by an authentication process directly impacts its favorability by its users. According to surveyed workers, security keys and hardware tokens achieved the highest approval ratings, with 91% stating they were satisfied with the authentication solution (Figure 8). This favorability can be attributed to a reduction in the frequency and complexity of authentication steps. On average, adopters of security keys and hardware tokens noted 10% fewer authentications per month than those employing other technologies.

Software keys and behavioral biometrics also achieved high favorability ratings. Both offer solutions that principally operate autonomously—authenticating users without requiring them to perform actions. Software keys are encrypted strings stored on endpoints that authorize actions performed on the device to automatically access business IT services. This is the principal method employed with device authentication solutions that presume the identification of an endpoint device is sufficient to identify the user to which that device is associated. Passkeys, a new term for passwordless WebAuthn/FIDO2 credentials, are now popularly being discussed as replacements for traditional passwords. Passkeys are presented in two forms, as hardware bound, non-copyable credentials on security keys, or cloud-based, multi-device copyable credentials, which can be considered examples of software keys.

It is notable that fingerprint readers have a favorability rating on par with traditional passwords, and facial recognition solutions have a significantly lower satisfaction rate. The indication is that both approaches to passwordless authentication are not sufficiently considered low-friction because they still require the users to perform periodic actions.

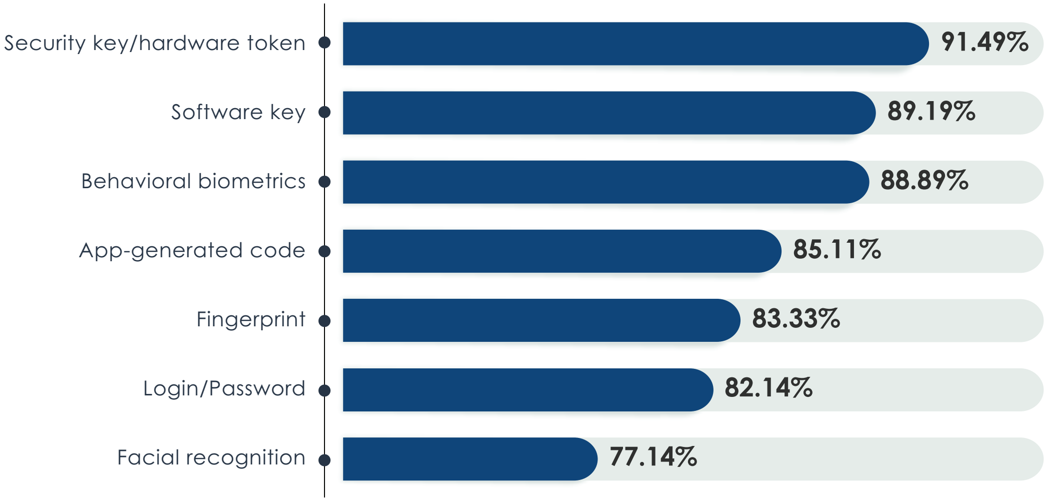


Figure 8: Percentages of business employees indicating they are "satisfied" with the authenticators they actively use

79%
64%
MATCHING
MATCHED
ID 96421654174
Hashcode RTY4 1DSE BTW4 ZWQ1
##READING
/:FSGKLJJ33 13244%#S 1315FHRS A3124#31D14412D
/:31245FFR44 %#3110 0134
/:AW3232FGG8##3214 FGTG;J1134
/:32132144HSD %%PKKKJ 13444881 ZAZ3
/:JSFE1134 841%S11 #32144
/:JUDJ434% GLK##::AA7 S4777431145 8SFR 1
/:OO1001 ASW475#7414 SSFE% FGJJJ1154 314845
/:SDW31115 1AS5WD11 S2QQQ11 S2213%A #ZS411
ACCESS GRANTED
PROCESSING.....
PROGRAM RUNNING..

Security Achievement

Breach Events

Among surveyed businesses, 87% indicated they had experienced a security breach over the preceding year (Figure 9). Most frequently noted were incidents of devices providing access to or containing business data that was lost or stolen. Increased support for remote workforces has accelerated opportunities for portable devices (such as laptops and mobile devices) to be forgotten or placed in locations where they may be pilfered by thieves. This is a particular problem for device authentication solutions reliant on software keys and for autofill passwords common to most vaulting solutions. Once a malicious actor has direct access to a device, they have access to all the personal and business resources to which that device has been granted access. This reality typifies the importance of introducing additional factors of authentication that operate independently of device authentication technologies. Incidents of lost devices were noted to be significantly higher among larger organizations. This is easily attributed to the larger number of employees—the more workers there are, the greater the likelihood one will lose a device.

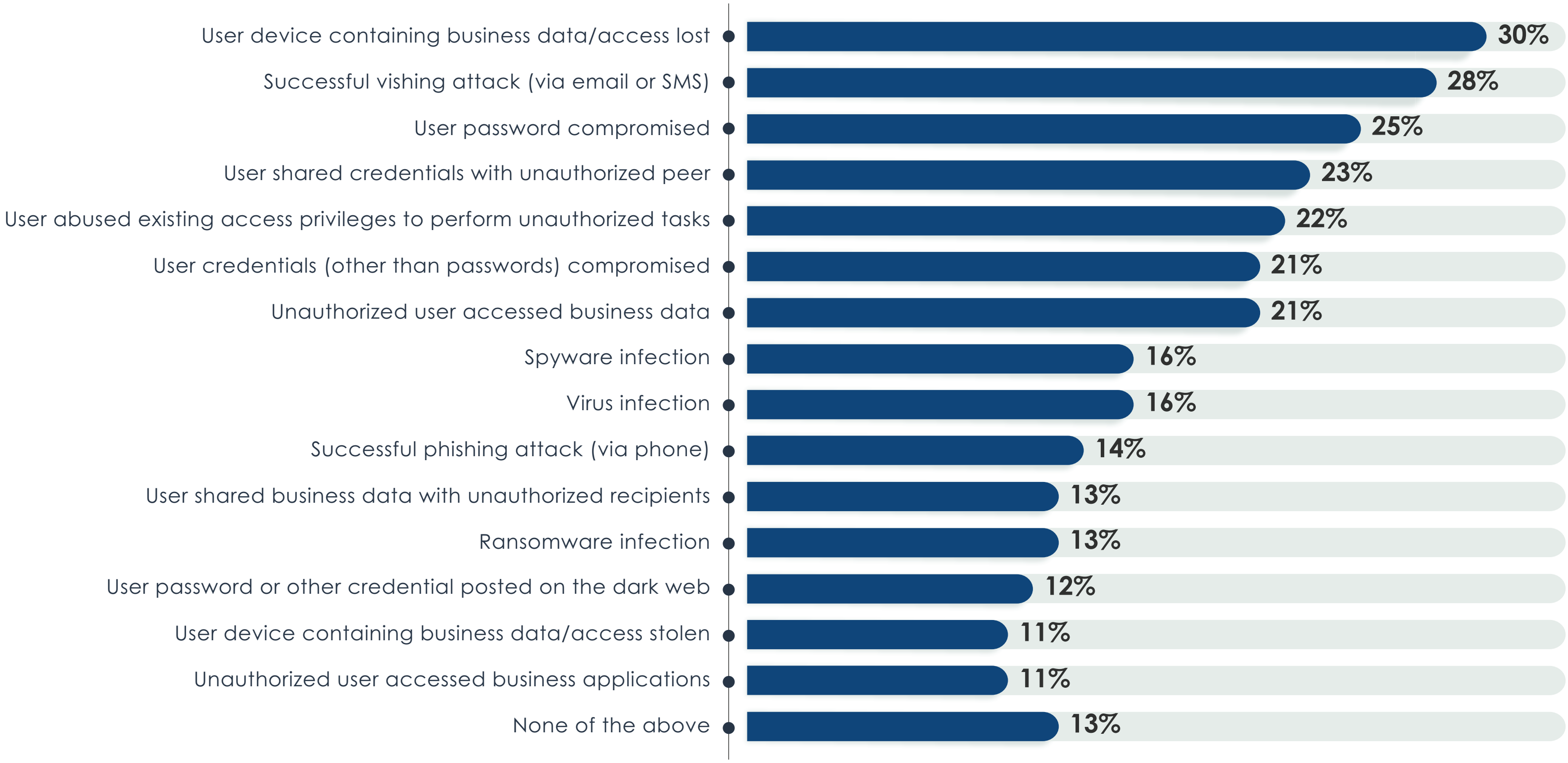


Figure 9: Percentage of surveyed businesses indicating security breach events that occurred in their organization over the preceding 12 months

Passwords continue to offer the least effective form of authentication. Organizations that rely on passwords were indicated to have a 34% greater chance of experiencing a compromised credential. Additionally, incidents of an unauthorized user accessing business applications was noted to be three times higher among organizations employing passwords than those using passwordless approaches. Among surveyed business employees, 34% stated that they "would find creative ways to bypass business security" if forced to use high-friction authentication options, such as frequent password authentications. Also, 37% of workers reported that they regularly write down passwords on a physical piece of paper or online document, greatly increasing the chances they will be compromised.

Overall, security breaches were reported to be 22% more frequent among organizations with workforces that perform more than half of their job tasks outside of the office. In particular, incidents of user credentials being compromised and successful phishing attacks were noted to be significantly more common among remote workers than office-bound workers. The less structured environments of home offices provide malicious actors with broader opportunities to deceive users into unwittingly providing them with access to protected services. However, incidents of ransomware and virus infections were more common among businesses with principally in-office employees. When workers operate off a common network, the odds of contracting and sharing malware substantially increases.

Security breaches were also indicated to be 11% more frequent among organizations using in-house-developed identity security solutions as opposed to those who purchase or subscribe to a service from a vendor. Some businesses choose to architect their own platform in order to meet unique business requirements, provide capabilities they perceive are not available elsewhere, or simply minimize costs. However, homegrown solutions are not regularly updated to address new and emerging threats, and environment changes (such as patches, updates, and new software installations) can alter the effectiveness of custom-built security solutions. Supportability is particularly a challenge when the individuals who wrote the custom code or scripts leave the company's employ, since others may not have the expertise to maintain the software or remediate problems. All of this makes custom-built identity security solutions less effective than platforms designed, maintained, and actively supported by a reliable solution provider.

Breach Consequences

Among organizations that experienced a security breach in the preceding year, 93% reported that significant consequences occurred as a result (Figure 10). More than one-third noted an impact to the performance of their production environments, while 42% indicated that an employee had been reprimanded or terminated following the incident. Direct business impacts—including damages to company reputations, loss of customers, loss of revenue, and a failure to meet regulatory compliance—were collectively experienced by 45% of surveyed businesses. Additionally, 35% reported direct financial consequences to the breach event, including remediation costs, fines, and lawsuits. It is also notable that 22% of breached businesses would subsequently have difficulty obtaining cybersecurity insurance.

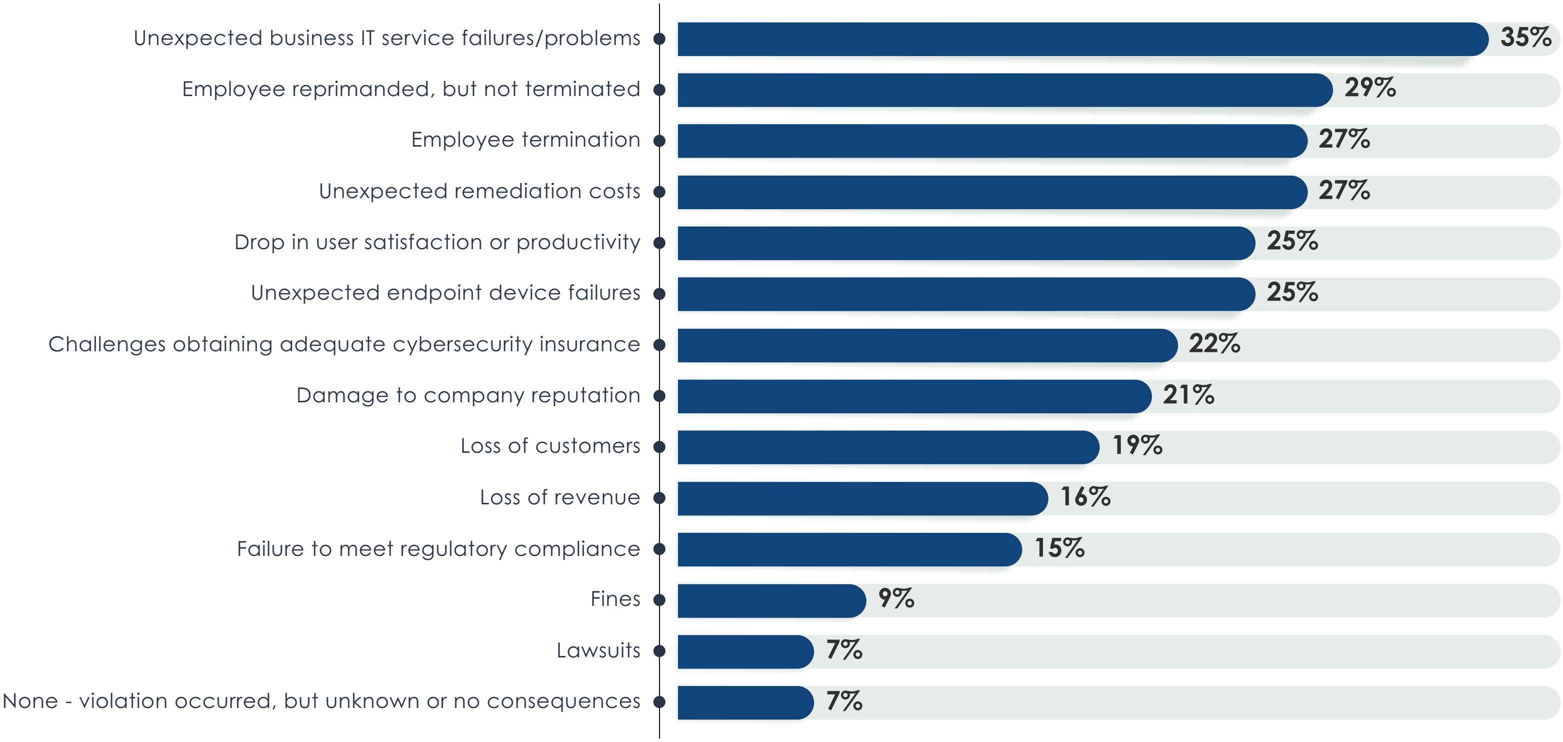


Figure 10: Percentage of surveyed businesses indicating consequences that occurred following a security breach or violation

Identity Security Confidence

While the majority of surveyed businesses maintain a high level of confidence in the security effectiveness of their adopted identity security solutions, 38% stated that they did not believe their IAM capabilities would prevent all or nearly all security breaches (Figure 11). The highest confidence assessments were achieved among organizations that support software keys, behavioral biometrics, and security keys, while the lowest were among businesses principally relying on passwords and app-generated codes. Higher confidence ratings were also achieved across organizations supporting adaptive authentication solutions as opposed to those using traditional high-friction two-factor authentication (2FA) (e.g., mobile device-based one-time passwords and push notifications). In both scenarios, security confidence is significantly higher with solutions enabling low-friction access.

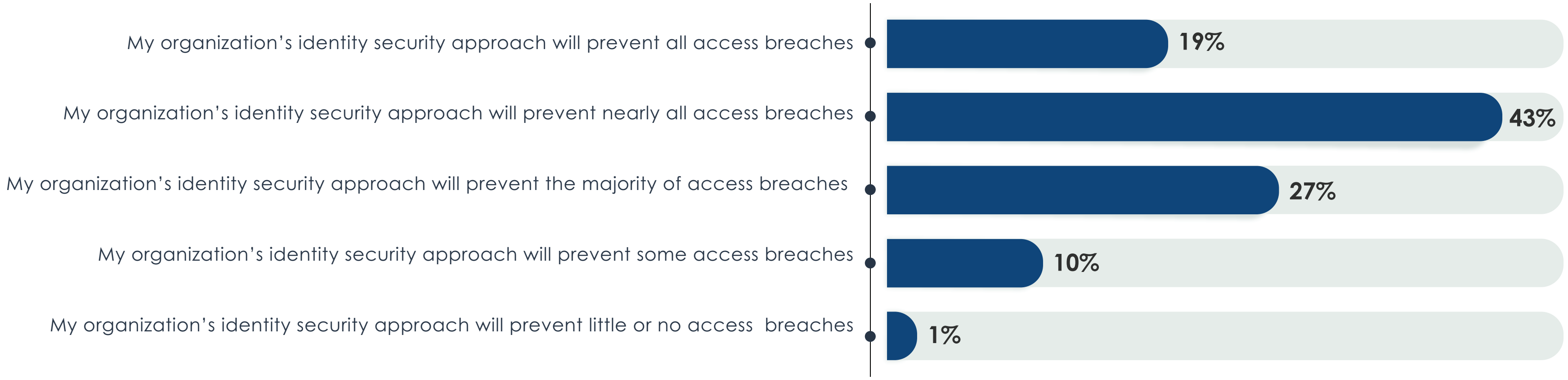


Figure 11: Percentage of surveyed businesses indicating their level of confidence in the security their adopted identity management solution offers

Authenticator Usage

MFA versus 2FA

Early implementations of zero trust initiatives called for adding a second factor of authentication in addition to a password, accompanied by policy-based controls to reduce identity breach risks. The majority of organizations addressed these new requirements by introducing what at the time were considered the easiest and least expensive solutions to implement. Commonly adopted were one-time passwords and push notifications distributed via email or SMS calls (a.k.a., text messaging) to smartphones. Unfortunately, these approaches proved to do little to curb security threats, as evidenced by the fact that nearly all businesses have adopted them, yet breach events continue to rise. Additionally, these processes have served to increase friction on the end users by adding additional steps they must perform to gain access.

Recognizing the deficiencies of legacy zero trust approaches, many businesses are adopting modern MFA technologies as a replacement for traditional and basic 2FA. The chief difference between the two is that MFA incorporates multiple passwordless and low-friction authentication processes. According to research results, fewer than one-third of businesses have introduced modern MFA solutions, with the majority relying on more basic 2FA approaches (Figure 12).

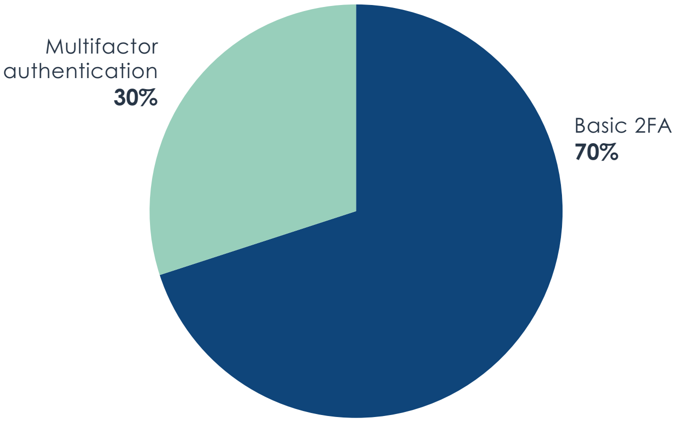


Figure 12: Percentage of surveyed businesses indicating whether they support basic 2FA or modern MFA

Second Authentication Factor Friction

Surveyed workers from organizations requiring a second factor of authentication broadly recognized emails delivering a one-time passcode (OTP) to be the most impactful to their productivity (Figure 13). Users must manually type OTPs into account verifiers to gain access, which can be very time-consuming considering users must perform this on every authentication event. Push notifications were recognized as less disruptive to employee productivity. While these approaches do not require users to type codes into verifiers, they do still require manually accessing a mobile device, email account, or web browser to independently authorize access. Security keys were identified as the second authentication factor that is least impactful to workforce productivity. Once registered, security keys require no user interactions other than to ensure the physical keys are within proximity of (via NFC) or connected to endpoint devices.

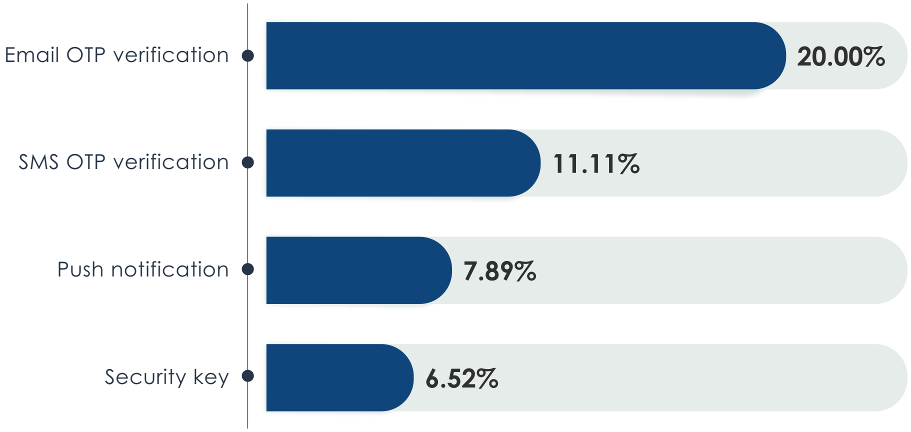


Figure 13: Percentage of surveyed business employees indicating second factors of authentication methods currently in use are "very disruptive" to their productivity

Low-Friction Access Technologies

Single Sign-On and Autofill

Roughly 70% of surveyed business employees reported that their organization utilized single sign-on (SSO) functionality, enabling them to reduce password access friction by only requiring one authentication before accessing multiple IT resources. SSO solutions can have a significant impact on reducing the frequency of password authentication. In fact, research results indicate that SSO users authenticate 20% fewer times, on average, than non-SSO users (Figure 14). It is important to recognize, however, that the value achieved from SSO adoption is directly proportional to the number of independent IT services (both cloud and business-hosted) employees regularly access. Organizations supporting a broad number of disparate IT services are more likely to have introduced SSO solutions than those who do not. It is therefore likely that organizations adopting SSO technologies have achieved much greater reduction in authentication frequencies than indicated here.

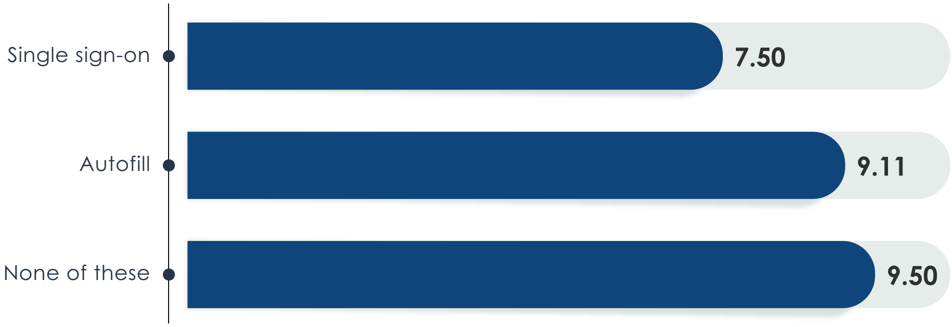


Figure 14: Average number of authentications per day by adopters of low-friction authentication technologies

Another method commonly employed to reduce access friction with passwords is to locally cache the password string on endpoint devices so they can be automatically filled in when prompted for authentication. Autofill solutions were noted to be in use by 45% of surveyed business employees for accessing company IT resources. While this solution does not on its own reduce the frequency of required authentications, it can greatly simplify password-based authentication actions.

Although SSO and autofill solutions reduce password authentication friction, they have a negative impact on preventing forgotten credentials. On average, surveyed business workers using autofill forgot passwords four times more frequently than those using SSO, who forgot passwords six times more frequently (Figure 15). In reducing the number of times a user must enter a password, these tools also reduce opportunities to refresh memories of password strings. SSO solutions time out after a predetermined period, forcing a reauthentication, and autofill solutions are only applicable to a specific device, so at some point the password will need to be recalled with both resources. Given that password resets are the most difficult and time-consuming authentication process, it can be assessed that SSO and autofill solutions provide only limited reductions in overall access friction.

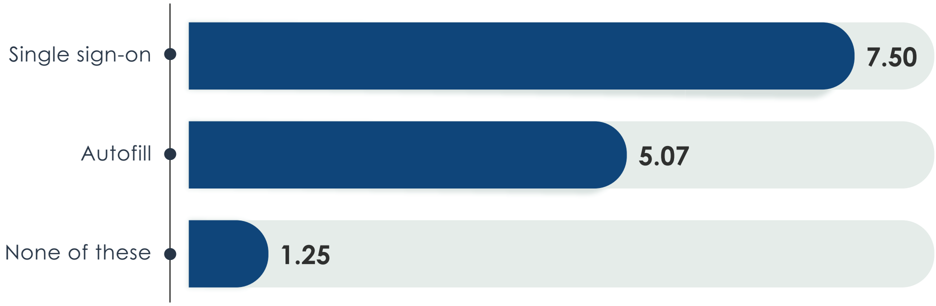


Figure 15: Average number of times surveyed business employees reported resetting a forgotten password per month by tool employed

Adaptive Authentication

The most effective approach to minimizing access friction without diminishing security effectiveness is to dynamically alter access requirements based on contextual conditions and assessed risks. Among surveyed businesses, 38% reported they support adaptive authentication technologies today. Adopters of adaptive authentication were 31% more likely to state they were "very satisfied" with their implemented access management solution than non-adopters. This indicates the highest overall satisfaction rates for access management technologies. Additionally, adopters of adaptive authentication solutions noted the highest levels of confidence in the security effectiveness of their environment, with 71% stating they believe their supported solution will prevent all or nearly all security breaches, versus only 56% of non-adopters.

Adaptive access solutions are offered with a variety of feature sets and capabilities. Common among all the related solutions is the ability to collect detailed contextual information on user, devices, networks, and other elements against which predefined access policies can be applied. For instance, a device that is connecting over an unsecured network (such as a public Wi-Fi) may be granted only limited access to IT services or may require more stringent authentication processes. Among surveyed businesses employing adaptive access, 58% noted they collected contextual information in real time (Figure 16). Access conditions are constantly changing—a device that is deemed secure one moment may be insecure the next—so it is important to detect conditions at the time of authentication. Even better, continuous detection (supported by 45% of surveyed businesses) monitors environments even after authentication so access can be denied or limited if warranted by changing conditions. Organizations supporting continuous contextual data collection for adaptive authentication were four times less likely to report user credentials had been compromised or that an unauthorized user was able to access business applications in the preceding year.

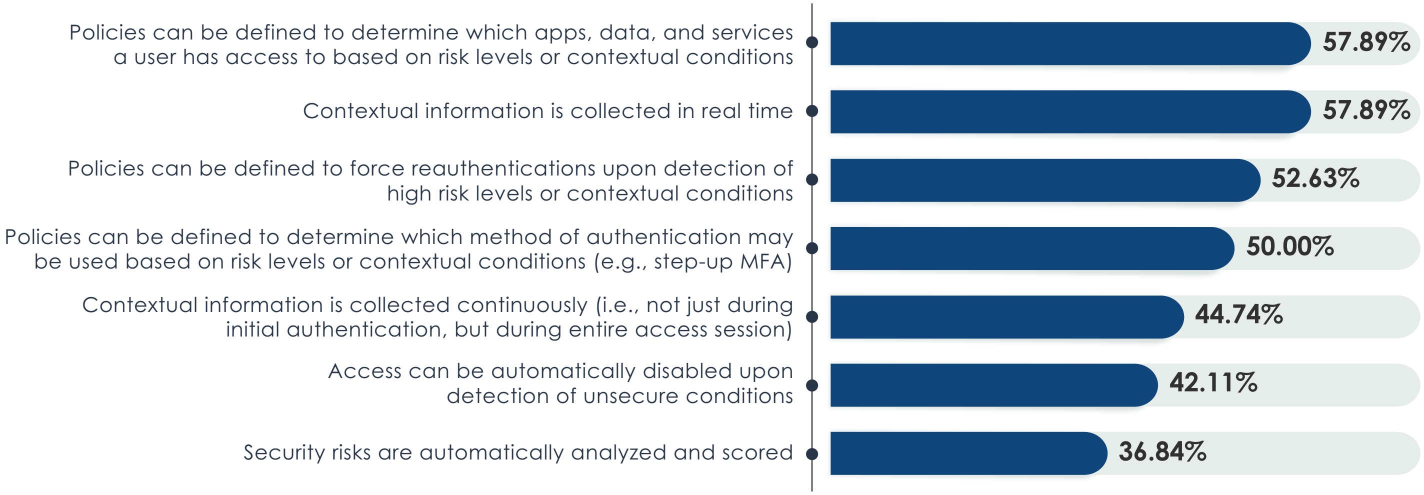
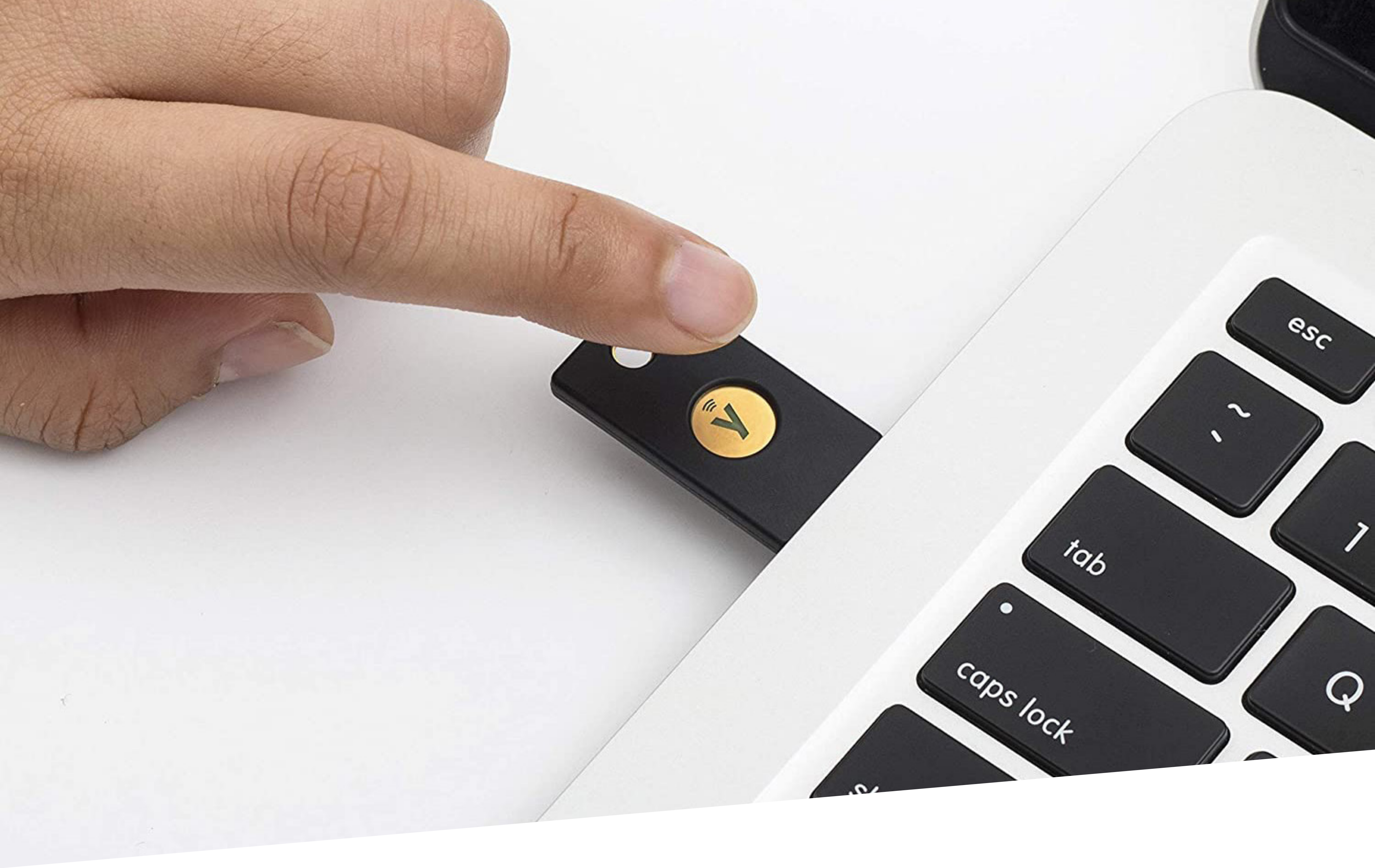


Figure 16: Average percentage of surveyed businesses that have adopted adaptive access solutions indicating specific features of their introduced product sets

Adaptive access policies were most frequently noted as authorizing which resources users may utilize based on contextual conditions. This feature was specifically noted to significantly reduce instances of virus and ransomware infections by limiting interactions with unsecured devices. While more than half of surveyed businesses also defined policies that force users to reauthenticate when conditions are deemed risky, only 37% use intelligence technologies to evaluate and score risk levels. Those lacking intelligent risk analysis rely on Boolean if/then logic to define responses in policies. For instance, if a device has been rooted or jailbroken, do not allow access. However, this approach requires each specific response to be defined and does not allow for non-deterministic conditions that may not indicate a risk on their own, but in conjunction with other conditions may indicate a compromised device or other threat. Survey results indicate that organizations utilizing intelligence risk scoring achieve the lowest incident rates of phishing attacks (via email or text messaging), vishing attacks (via phone), and unauthorized users accessing business data. This significant boost to security effectiveness is achieved because related solutions are able to identify and block inappropriate activities before business IT resources are compromised.

While there are strong security advantages to employing adaptive authentication, the exceptionally high satisfaction rates the technology achieves also speak to its ability to substantially reduce access friction. One popular method for doing this, supported by exactly half of surveyed adaptive access adopters, is to vary authentication methods based on the level of risk determined from the contextual conditions. Sometimes referred to as “step up MFA,” this approach allows businesses to present low-friction authentication actions under low-risk conditions and then increase (or “step up”) the complexity or number of authentication factors commensurate to the level of risk posed. In this way, users are always presented with the least-friction option while the business still maintains a maximum-security posture.



Identity Administration

Frequency of Support Requests

While IAM technologies are principally introduced to achieve security requirements and improve user experiences, related solutions can also significantly reduce management efforts and related costs. According to surveyed businesses, individual users in their organization submit, on average, 77 IAM-related support requests each year. Each support request disrupts IT administrator activities and can take hours to investigate and resolve. The highest frequency of support requests (92 support requests per year) was indicated to be for enabling access to business applications hosted on company servers or on public clouds. Android and Chromebook device users also reported an increased number of support requests, averaging 88 and 102 requests per user per year, respectively. Organizations utilizing adaptive authentication solutions reported significantly lower support request frequencies, averaging only 47 requests per user per year.

Segmenting survey responses by types of supported authenticators reveals that users principally employing password-based authentication submitted the most support requests (Figure 17). In fact, while password authentication users were noted to submit 95 help desk tickets per user annually, organizations utilizing exclusively passwordless authentication only needed to respond to fewer than 20 requests per user each year. Authenticator brands also have an impact on the reliability of adopted solutions. This is evidenced by the fact that surveyed businesses employing Yubico security keys (YubiKeys) reported they received the lowest frequency of support tickets at only about 18 per user per year, which is only one-quarter of support tickets received by other security key brands.

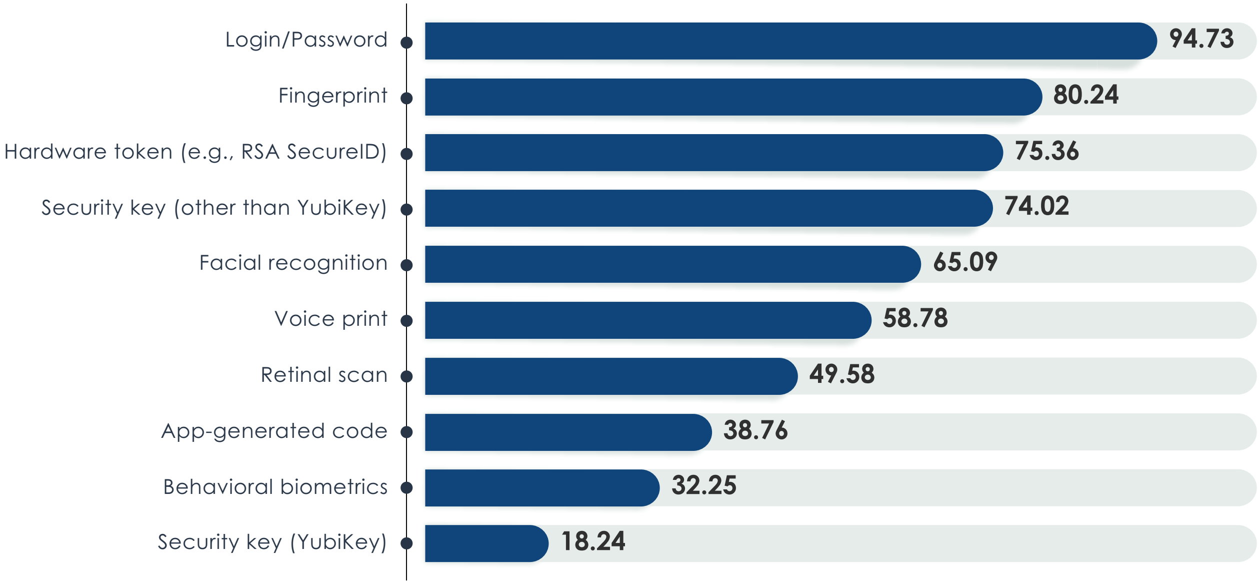


Figure 17: Average number of support requests submitted per user per year segmented by types of supported authenticators

Administration Challenges

IT administrators face a wide range of challenges for meeting business IAM goals. Among surveyed businesses, more than half (51%) reported they found adapting authentication processes to match the level of risk to be a significant challenge, identifying it as the most difficult IAM process (Figure 18). Organizations that build solutions in-house or adopt IAM platforms that support MFA but lack comprehensive risk intelligence and adaptive authentication functionalities are often forced to universally deploy the highest-friction authentication solutions in order to meet security requirements. Similarly, half of survey respondents indicated they experience significant challenges collecting contextual information on access events. A rich set of contextual data—including details on users, device states and configurations, network performance, and the sensitivity of accessed IT resources—is foundational for determining risk levels and determining access parameters.

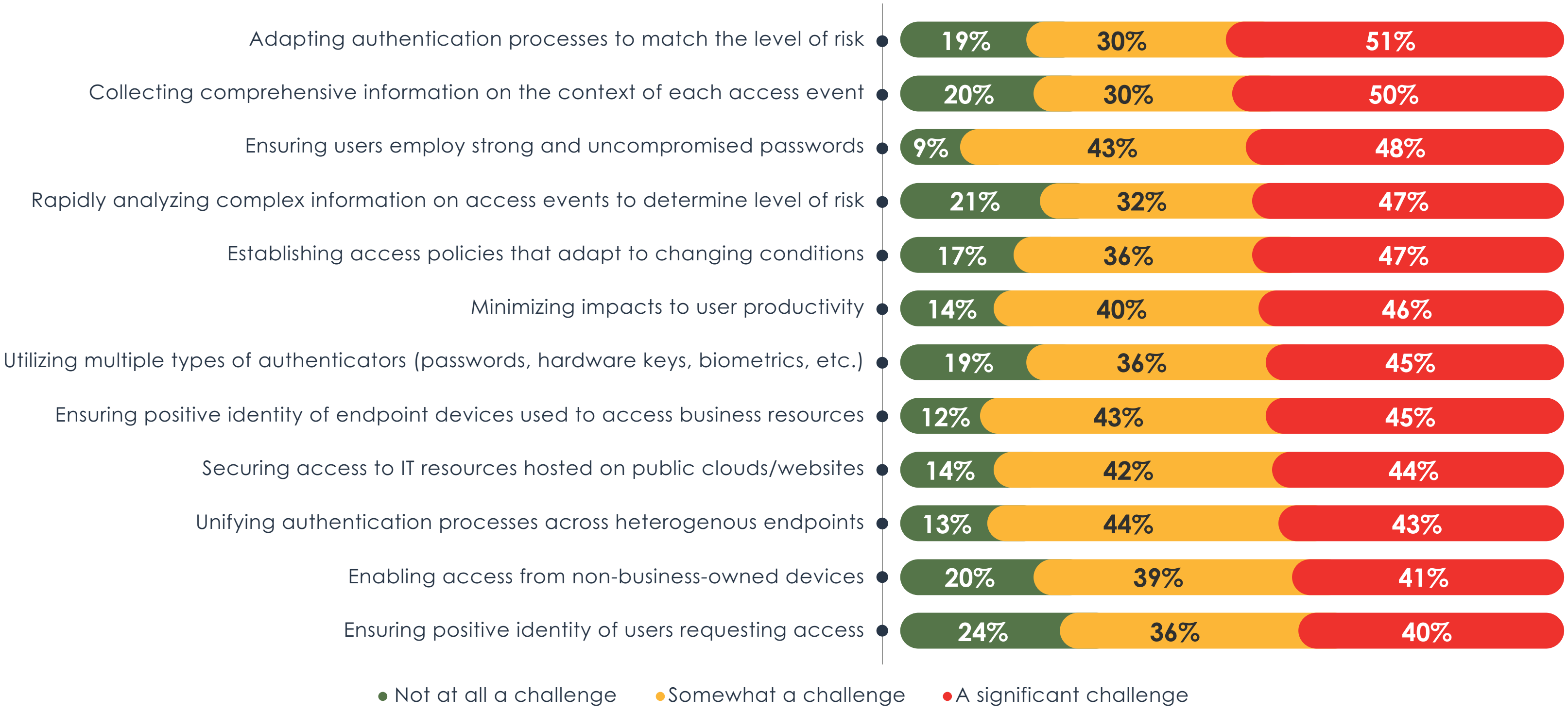


Figure 18: Percentage of surveyed businesses indicating how much of a challenge it is for IT administrators to meet IAM requirements

Across all evaluated IAM processes, challenges were indicated to be significantly higher among organizations supporting workforces that perform more than half of their job tasks physically remote from the office (Figure 19). Supporting remote workers requires monitoring a greater number of contextual details, including the security of connections over internet and public Wi-Fi networks and active processes running on remote devices. Remote workers are also more likely to employ multiple devices to perform job tasks, such as by having workstations at both work and home offices, and to more frequently utilize mobile devices. For each managed device, administrators must define access policies and support for unique authenticators in order to ensure consistent and secure user access experiences.

The adoption of low-friction access management solutions was noted to substantially reduce IAM challenges. In particular, surveyed businesses supporting passwordless authenticators were determined to be 34% more likely to report administrator productivity had "greatly improved" since their IAM solution adoption over businesses reliant on password approaches. Similarly, businesses supporting adaptive authentication were 25% more likely to see admin time and efforts greatly improved over organizations supporting other approaches.

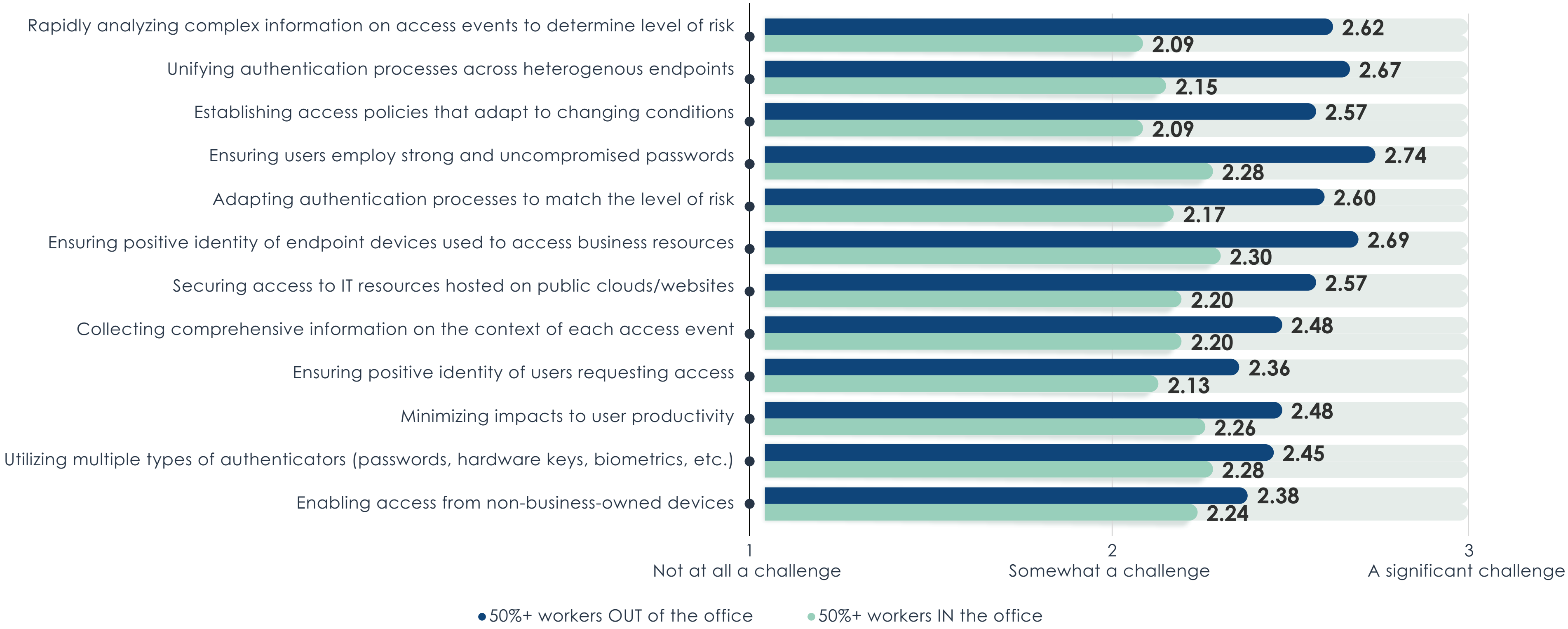


Figure 19: Comparing average responses of surveyed businesses IAM administration challenges between those supporting a majority of workers physically in the office with those supporting remote workforces

Impacts of FIDO Adoption

A core requirement for enabling MFA is the ability to centrally integrate with a variety of passwordless authenticator types and brands. Traditionally, this could only be accomplished by developing custom points of integration for each authentication resource. Among surveyed businesses, 45% reported that they continue to find it a significant challenge to enable access using multiple types of authenticators. However, that percentage has dropped significantly in recent years thanks to broad adoption of fast identity online (FIDO) standards. The FIDO Alliance is an open industry organization solely dedicated to establishing standards for the easy integration of passwordless technologies. To date, the standards body has released three principle specifications that have seen broad adoption: the universal authentication framework (UAF) specifically designed for mobile devices, the universal second factor (U2F) to provide second factor authentication to supplement passwords, and FIDO2, which integrates WebAuthn standards to enable completely passwordless 2FA.

In total, 83% of survey respondents indicated their organization utilizes FIDO standards, with the majority (53%) noting specific use of FIDO2. Among FIDO adopters, 82% reported that the standards are very or extremely important for "improving security effectiveness" to their organization, indicating this to be the primary motivator for adoption (Figure 20). Adopters of FIDO protocols also indicated significantly higher confidence rates in the ability of their supported IAM solutions to prevent security breaches. Roughly 71% of FIDO adopters reported they believe their implementation will prevent all or nearly all security breaches. By contrast, only 29% of non-FIDO adopters achieved this same level of confidence. Higher security confidence is likely due to the fact that adopters are employing no fewer than two factors of authentication and at least one is a passwordless approach, which is considered much more secure than a basic password.

Among FIDO adopters, the standards were also indicated to reduce deployment and administration costs and efforts. Any IAM platform supporting FIDO standards can directly manage any authenticators supporting FIDO standards, eliminating time-consuming development and maintenance processes. Roughly 70% of surveyed FIDO adopters reported the standards were very or extremely important to reducing identity management costs and simplifying authenticator integration. FIDO adopters were also 27% more likely to indicate their IAM solutions had improved administrator productivity.

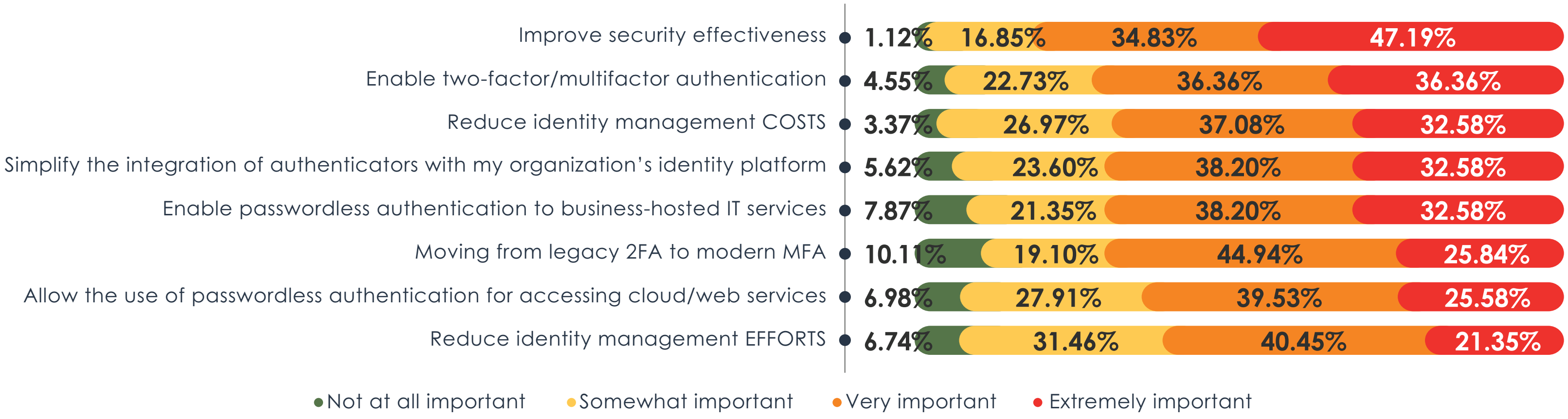


Figure 20: Percentage of surveyed businesses employing FIDO standards indicating how important it is for supporting individual IAM goals

Operational Costs of Identity Security

Expenses related to the purchase of IAM solutions and authenticators, as well as deployment and ongoing maintenance costs, continue to be significant concerns among surveyed businesses. In fact, the most frequently noted detractor to adopting passwordless authentication solutions was a belief that it would be too costly to support. Overall, surveyed businesses indicated mixed experiences with the financial impacts of IAM, with 36% reporting operational costs had decreased, 29% stating they had stayed the same, and 35% noting they had increased. Ironically, despite concerns, passwordless authentication approaches were most frequently recognized as decreasing operational costs, particularly security keys, fingerprint readers, and hardware tokens (Figure 21).

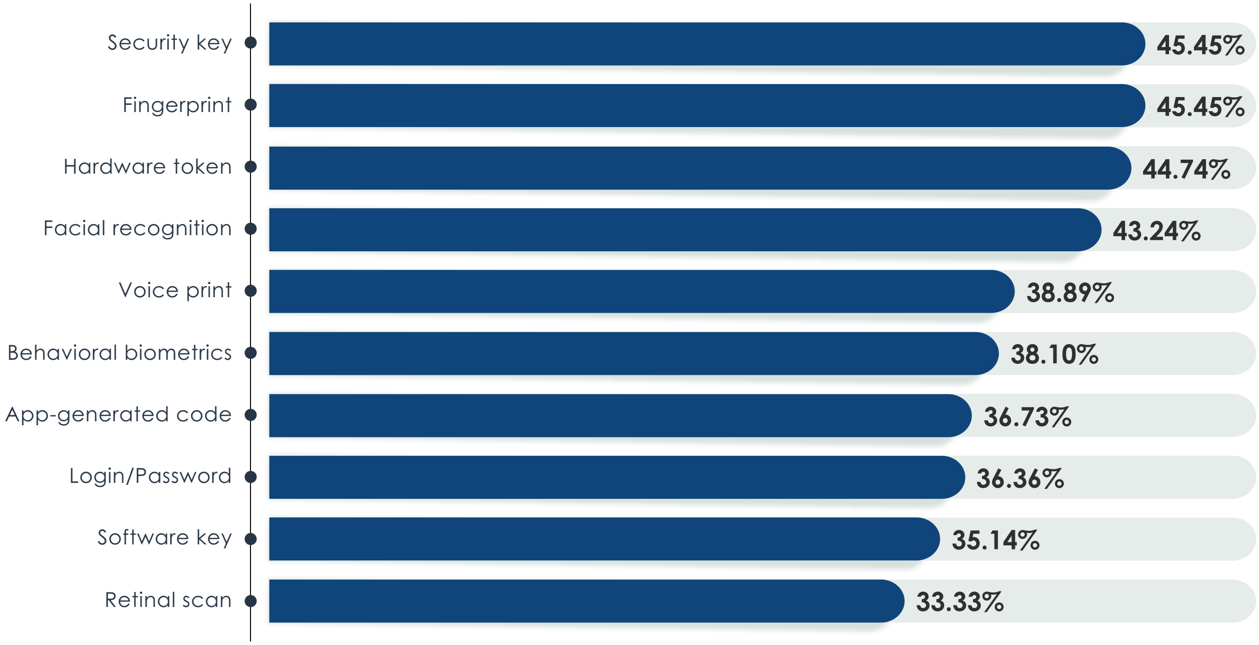


Figure 21: Percentage of surveyed businesses indicating their adopted identity management solutions resulted in decreased operational costs

EMA Perspective

Business performance in today's competitive markets is fundamentally dependent on the ability of its workforces to effectively access and use digital resources. High-friction identity and access management processes are the leading cause of worker disruption and performance degradation. In recent years, the majority of organizations have sought to address increasing security threats and zero trust initiatives by adopting what they perceived to be solutions that would be the easiest to implement. However, a continued reliance on password-based controls, along with mobile device-centric second factor authentication solutions (such as SMS or email one-time passwords and push notifications), have only served to further increase access friction, inhibiting worker productivity and reducing security effectiveness.

Results from both EMA surveys clearly conclude that low-friction authentication solutions provide significant benefits to business environments. Specific advantages were associated with passwordless technologies and adaptive authentication. Key benefits to these approaches quantified by the research include:

- **Improved employee satisfaction** – Business workers more frequently noted they were "satisfied" with passwordless approaches to authentication than traditional passwords.
- **Ability to attract and retain talented employees** – Among surveyed workers, 11% stated they would change jobs if required to perform high-friction authentication tasks. Fifty-three percent indicated that the availability of passwordless authentication is a significant enticement for prospective employers.
- **Increased security effectiveness** – Organizations supporting passwordless and adaptive authentication reported the highest confidence in their ability to secure business IT assets.
- **Simplified IT management** – Adaptive authentication reduces identity-related support requests by 39%, while passwordless solutions reduce ticket volumes by 82%.
- **Reduced operational costs** – Adopters of passwordless authentication solutions were significantly more likely to report they had achieved quantifiable cost savings since introducing their identity security solution.

The business value of low-friction access solutions is undeniable, and adoption rates of related technologies indicates the values are increasingly being recognized. With 71% of organizations citing the need to improve workforce experiences and productivity as a top business priority, even broader introduction of low-friction access solutions seems inevitable. In particular, it appears likely that business communities are finally poised to move beyond high-friction passwords with mobile device confirmations toward truly secure passwordless approaches coupled with adaptive, risk-based policy engines.

Appendix

End-User Survey Demographics

The following charts provide demographic details on the business employee respondents to EMA's survey of end-user access low-friction requirements and experiences.

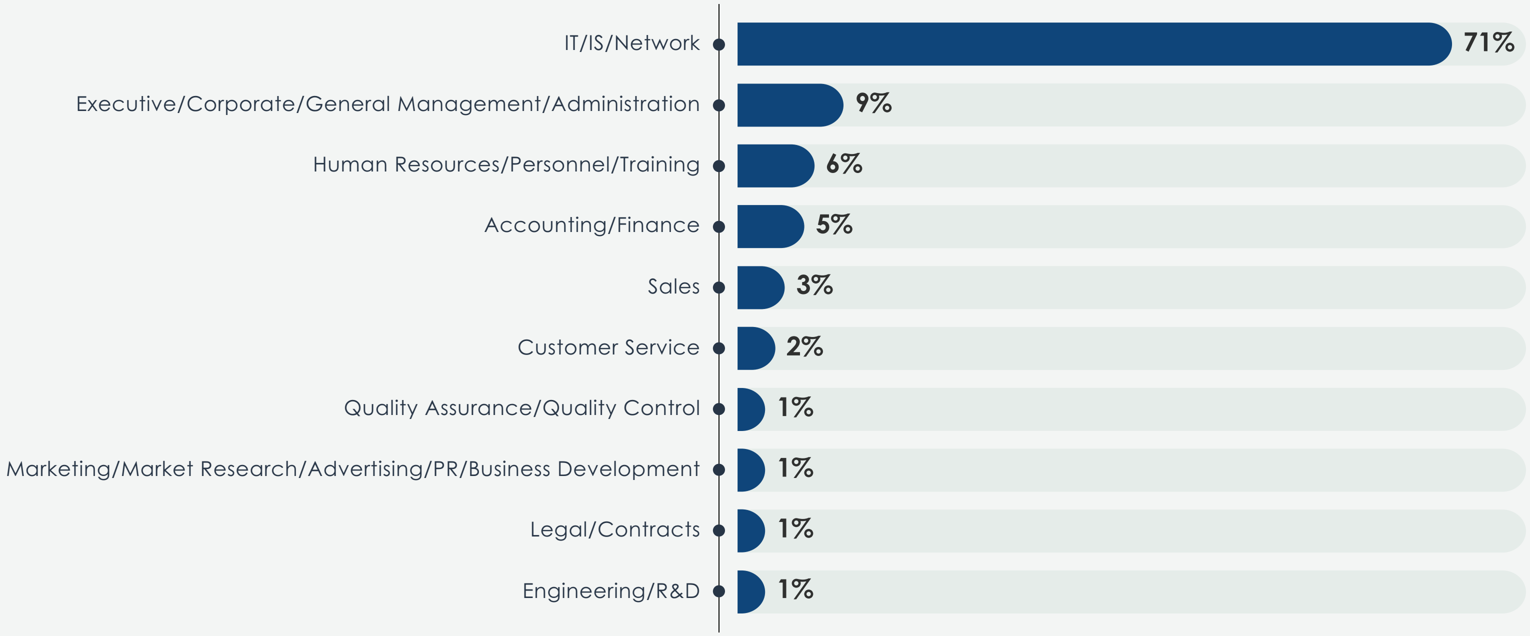


Figure 22: Which of the following best describes the department or functional area in which you work?

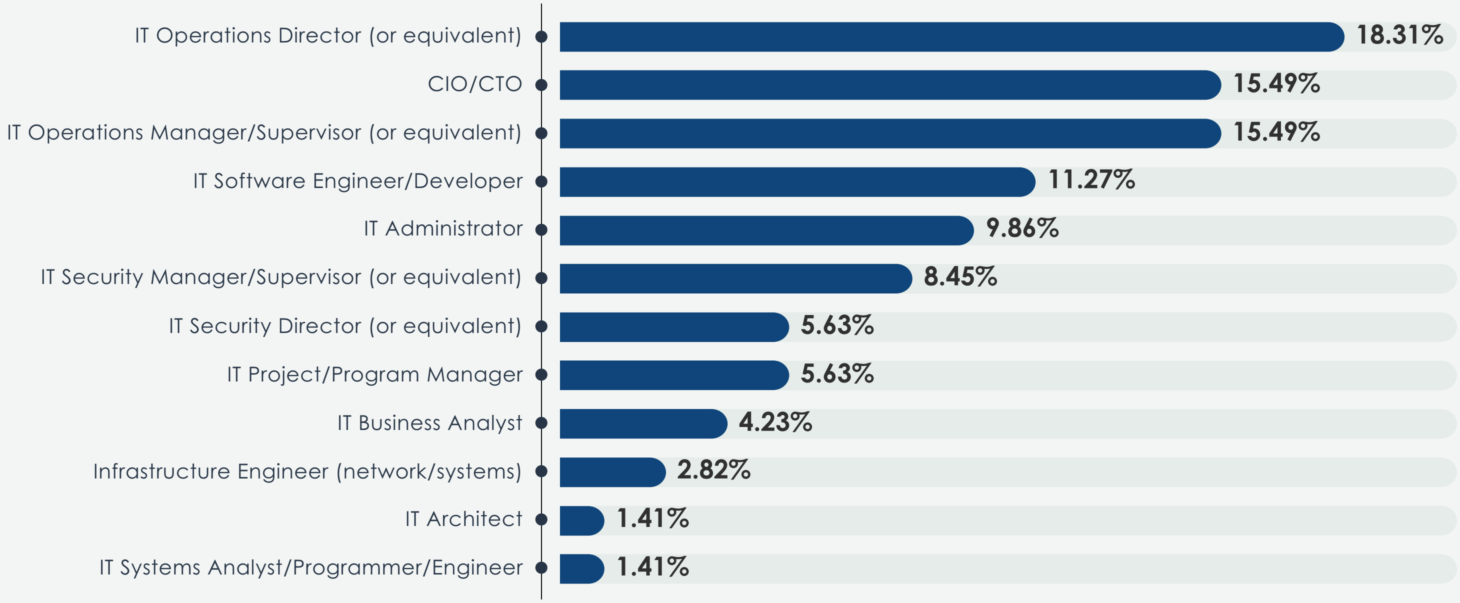


Figure 23: (Among IT respondents) You indicated that your department is IT-related. Which of the following best describes your specific role?

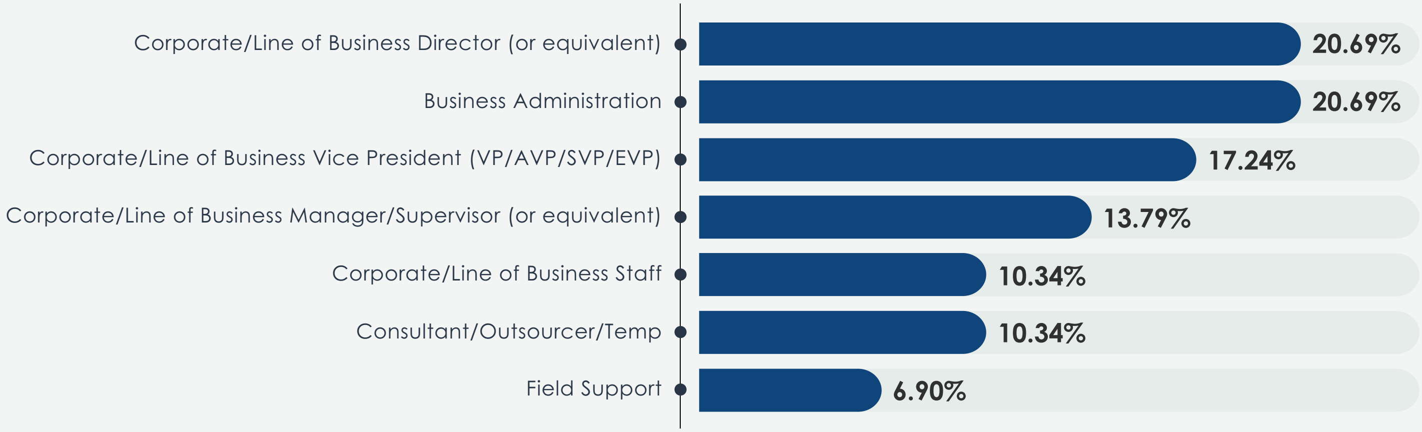


Figure 24: (Among non-IT respondents) Which of the following best describes your specific role in your organization?

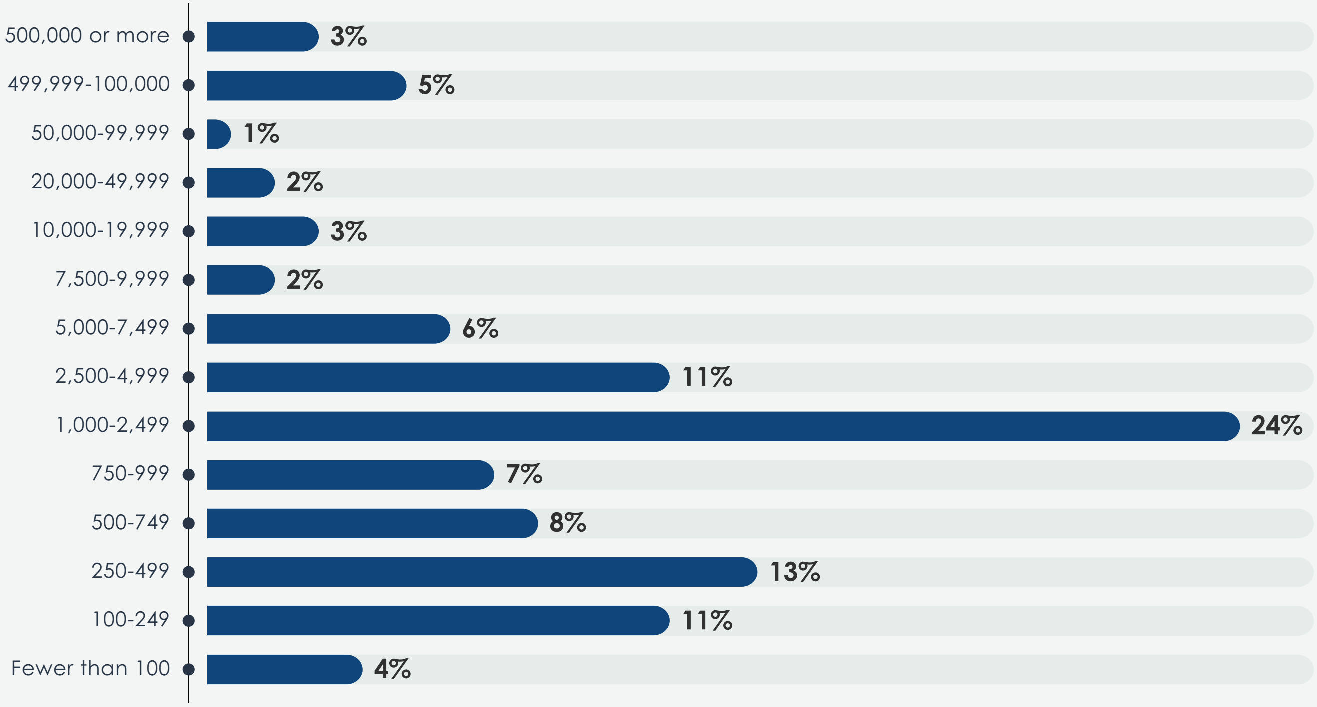


Figure 25: How many employees are in your organization worldwide?

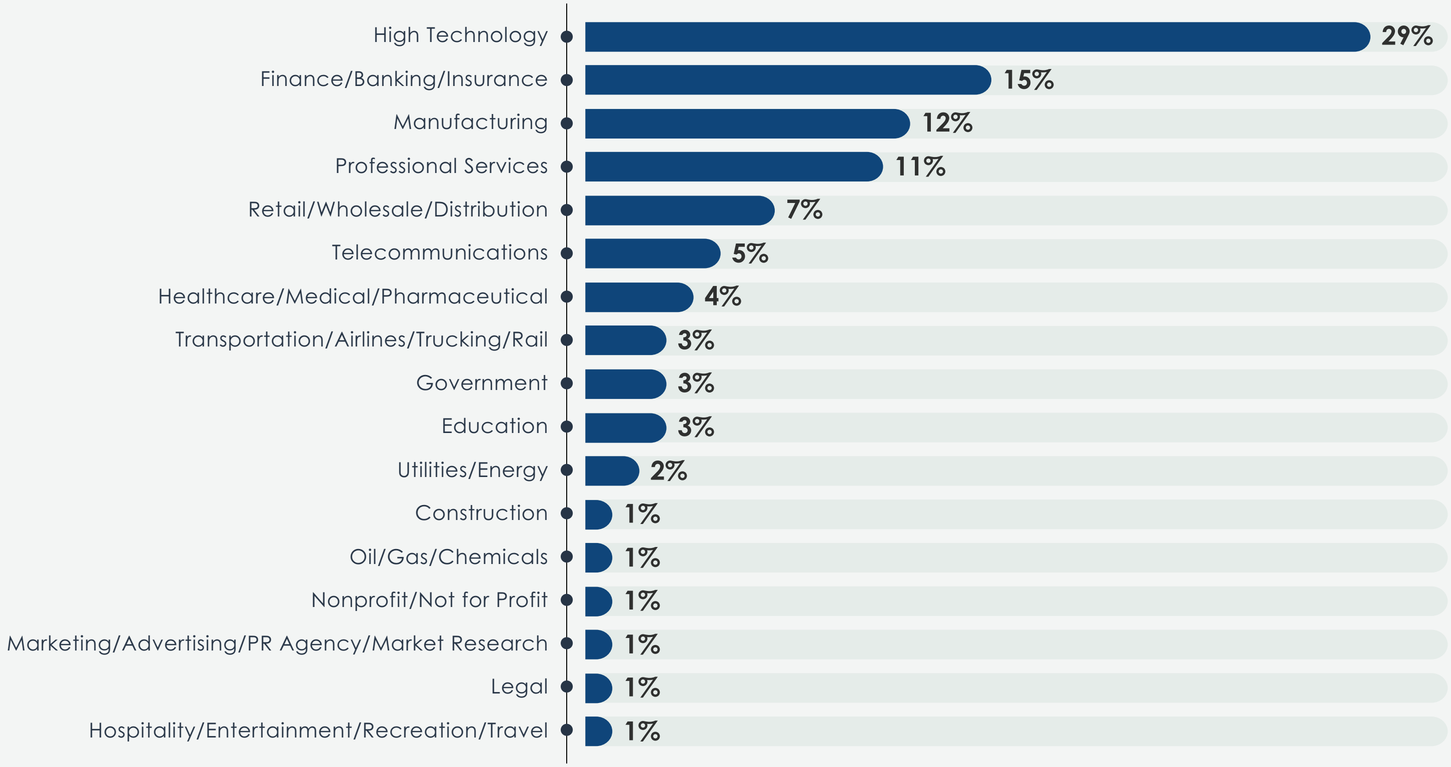


Figure 26: Which of the following best describes your company's primary industry?

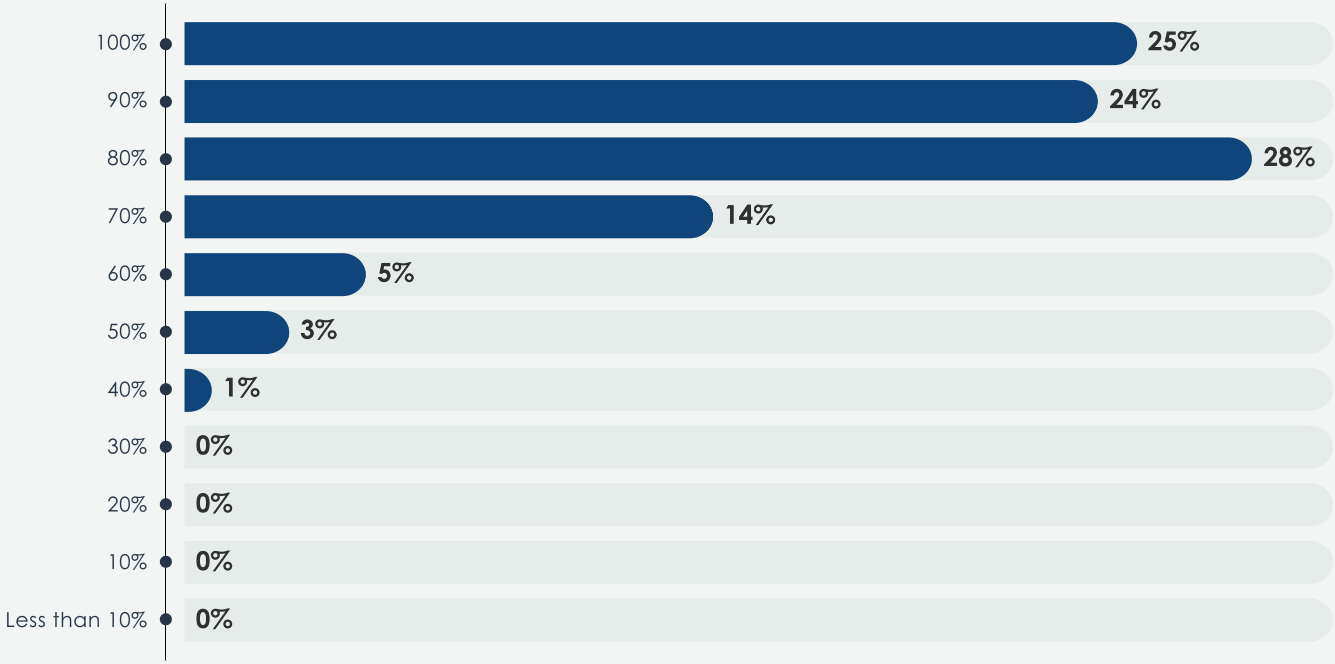


Figure 27: Approximately what percentage of your professional job tasks require the use of a computer?

Business Survey Demographics

The following charts provide demographic details on the business IT manager respondents to EMA's survey of business low-friction access requirements, solutions, challenges, and outcomes.

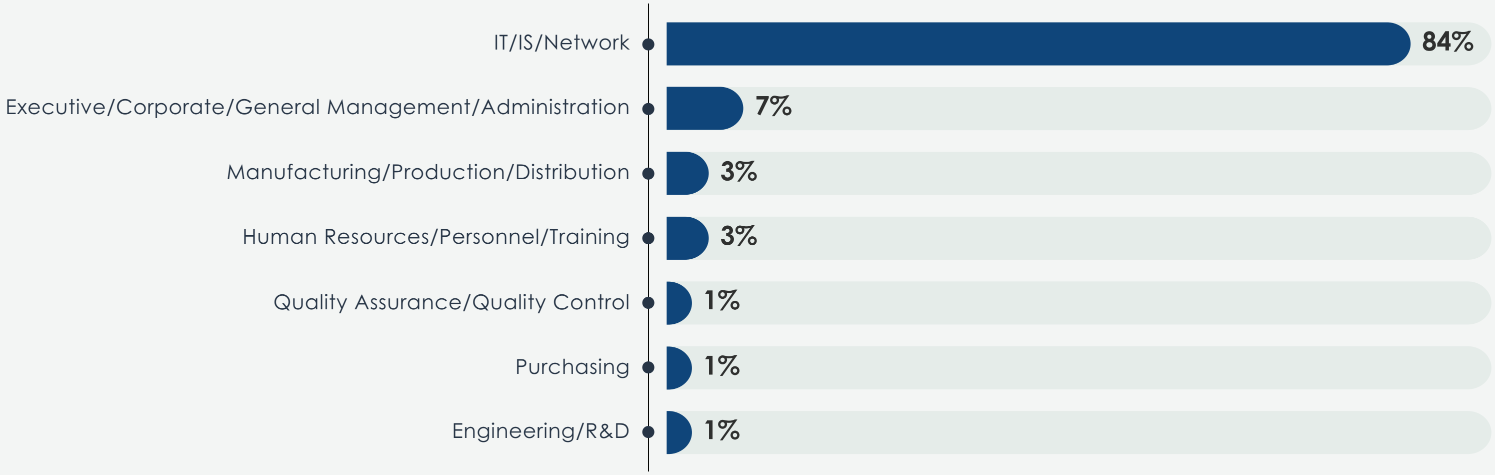


Figure 28: Which of the following best describes the department or functional area in which you work?

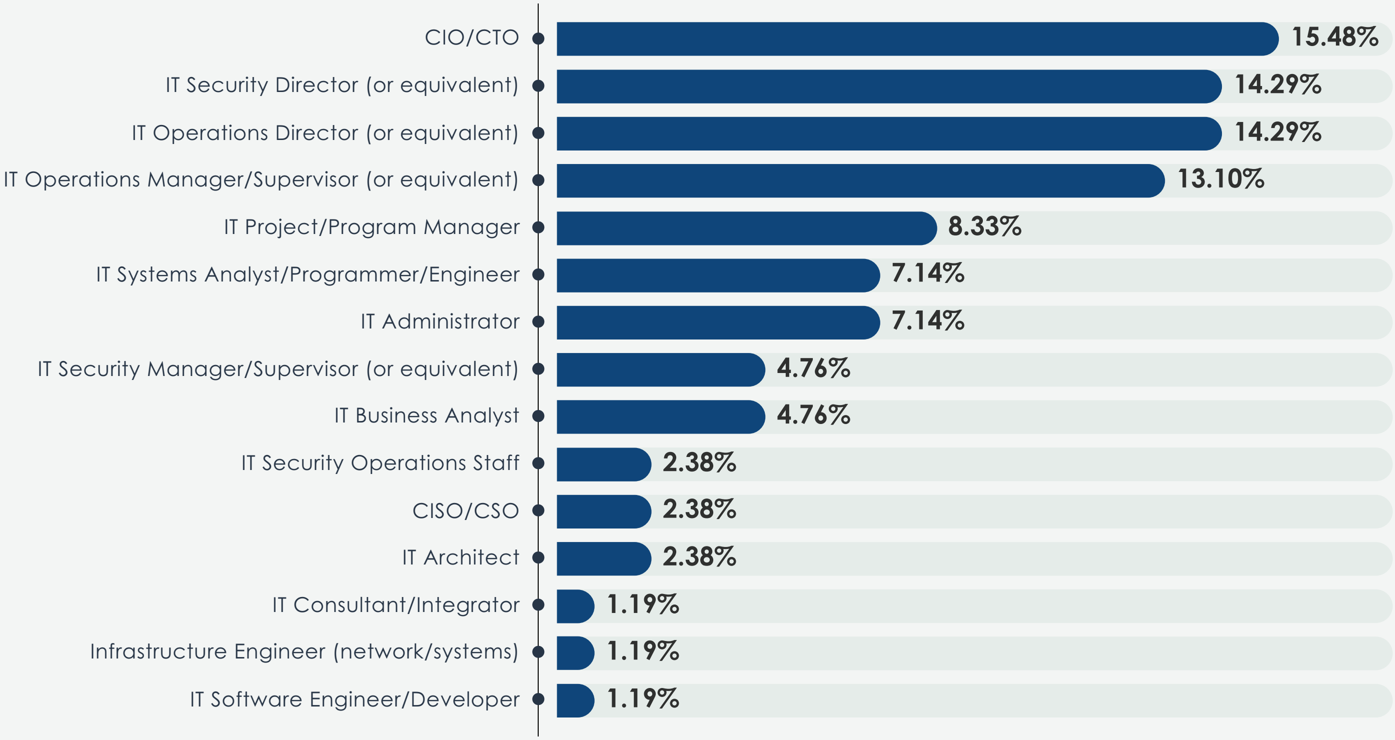


Figure 29: (Among IT respondents) You indicated that your department is IT-related. Which of the following best describes your specific role?

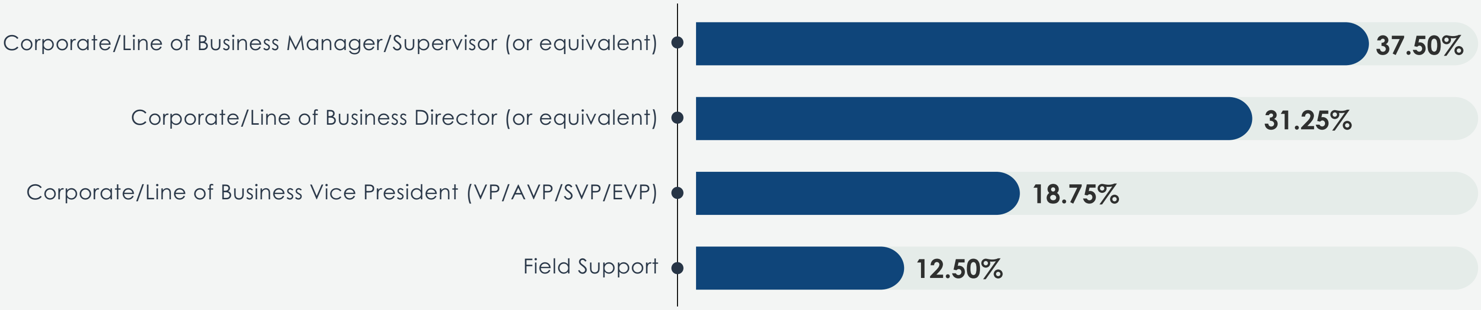


Figure 30: (Among non-IT respondents) Which of the following best describes your specific role in your organization?

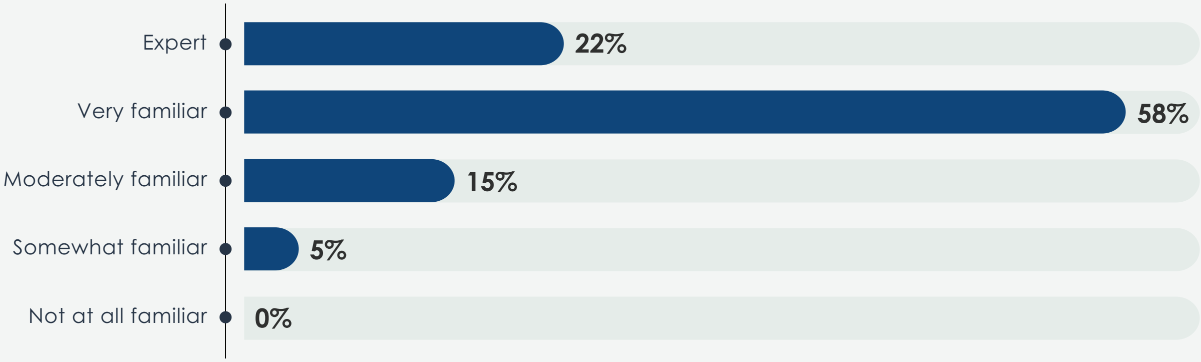


Figure 31: Which of the following best describes your familiarity with the identity and access management (IAM) practices and solutions used in your organization?

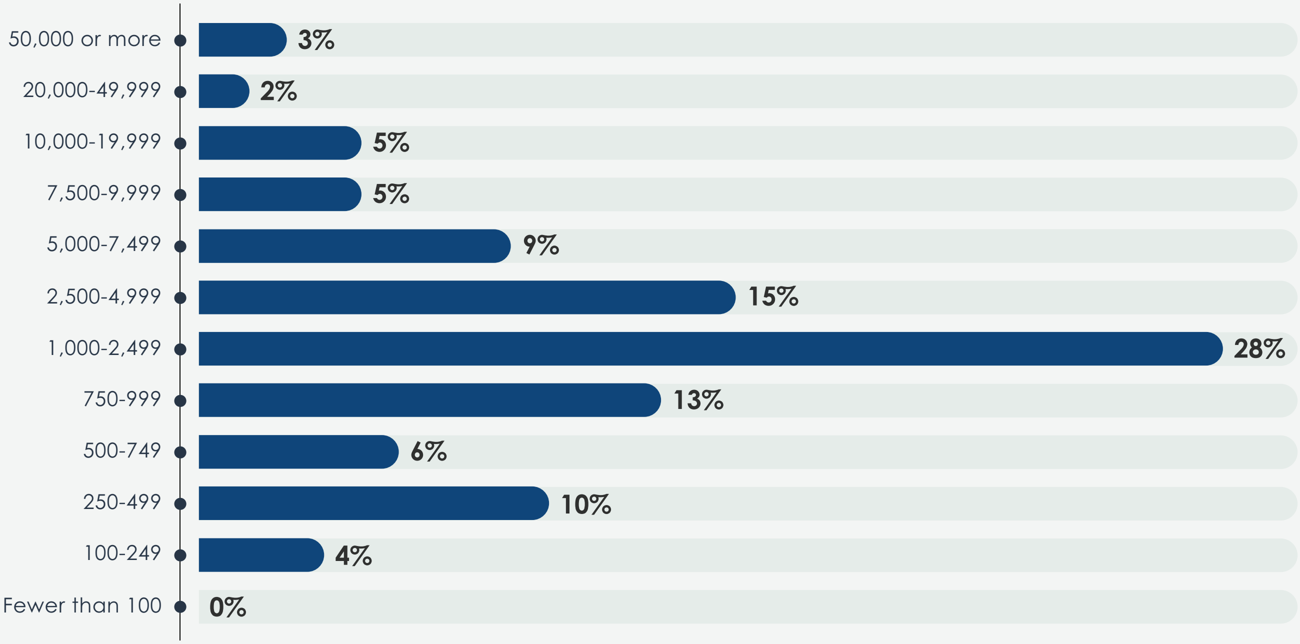


Figure 32: How many employees are in your organization worldwide?

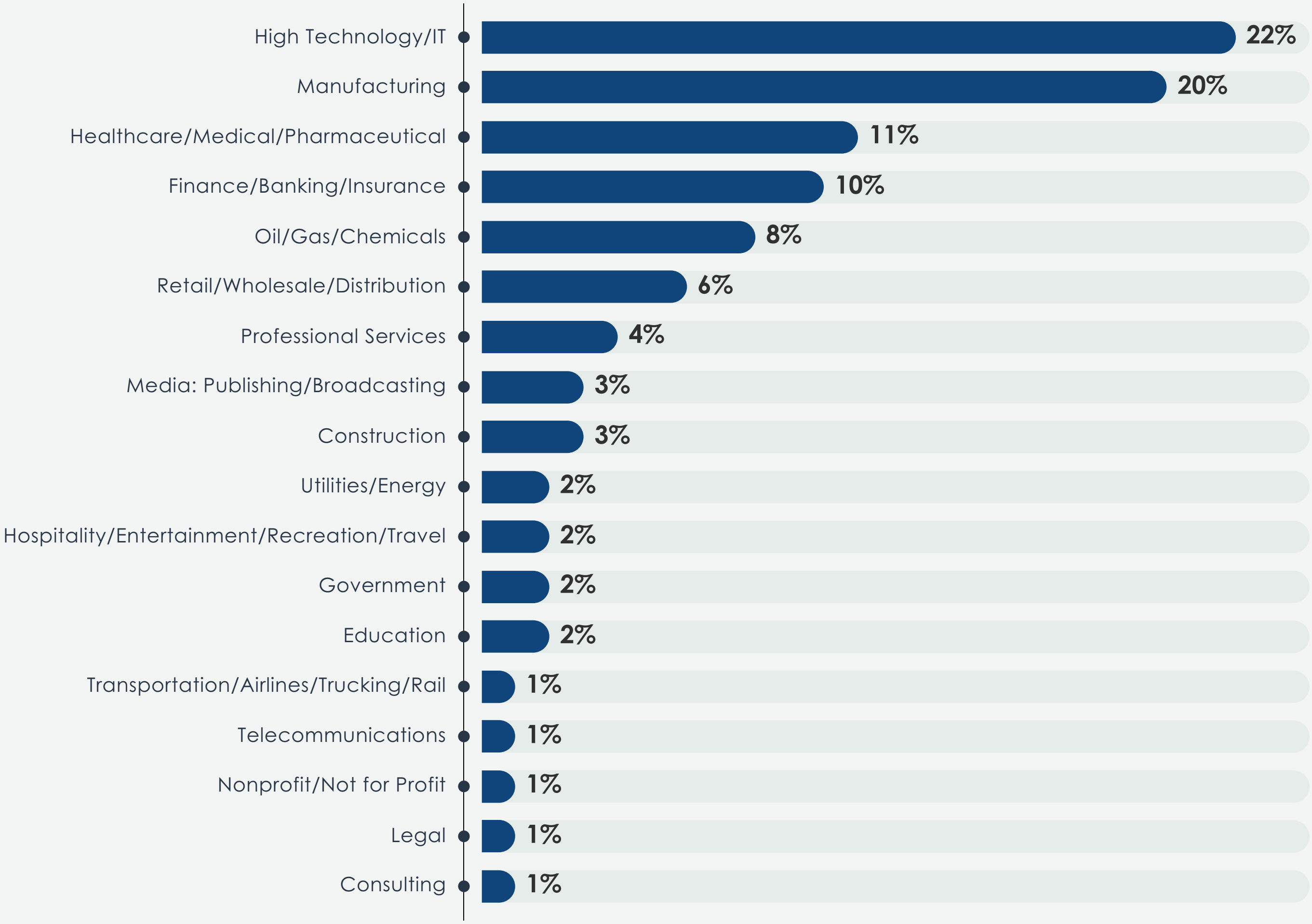


Figure 33: Which of the following best describes your company's primary industry?

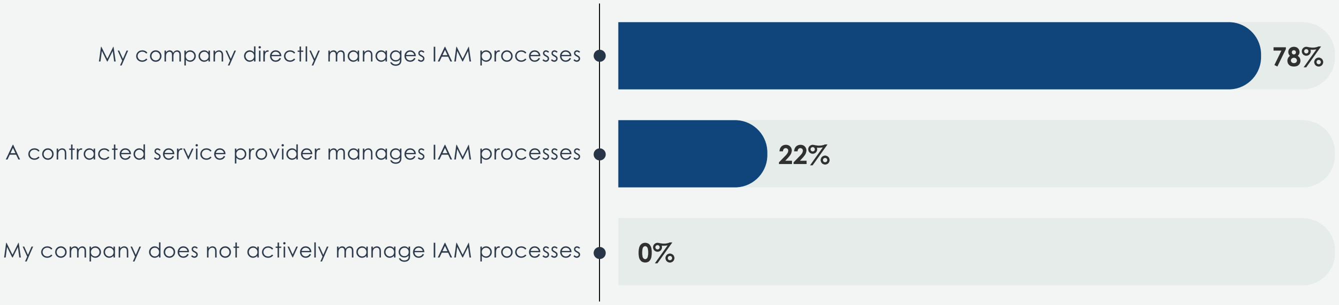


Figure 34: Which of the following best indicates your organization's current employment of identity and access management (IAM) processes?

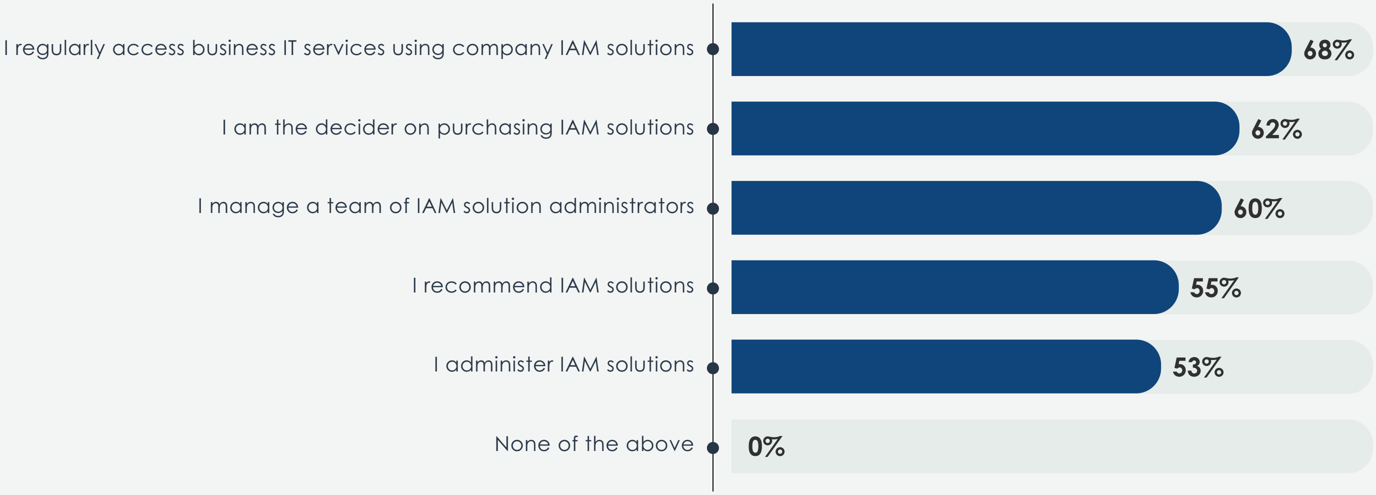


Figure 35: What is your personal role in supporting your organization's identity and access management (IAM) solutions?

0 11 0 1
1 10 1001 01010110
10
0 11 0010

About Enterprise Management Associates, Inc.

Founded in 1996, Enterprise Management Associates (EMA) is a leading industry analyst firm that provides deep insight across the full spectrum of IT and data management technologies. EMA analysts leverage a unique combination of practical experience, insight into industry best practices, and in-depth knowledge of current and planned vendor solutions to help EMA's clients achieve their goals. Learn more about EMA research, analysis, and consulting services for enterprise line of business users, IT professionals, and IT vendors at www.enterprisemanagement.com You can also follow EMA on Twitter or LinkedIn

1995 North 57th Court, Suite 120, Boulder, CO 80301 +1 303.543.9500 www.enterprisemanagement.com 4198.110822