EMA
IT & DATA MANAGEMENT RESEARCH,
INDUSTRY ANALYSIS & CONSULTING

Prepared for:

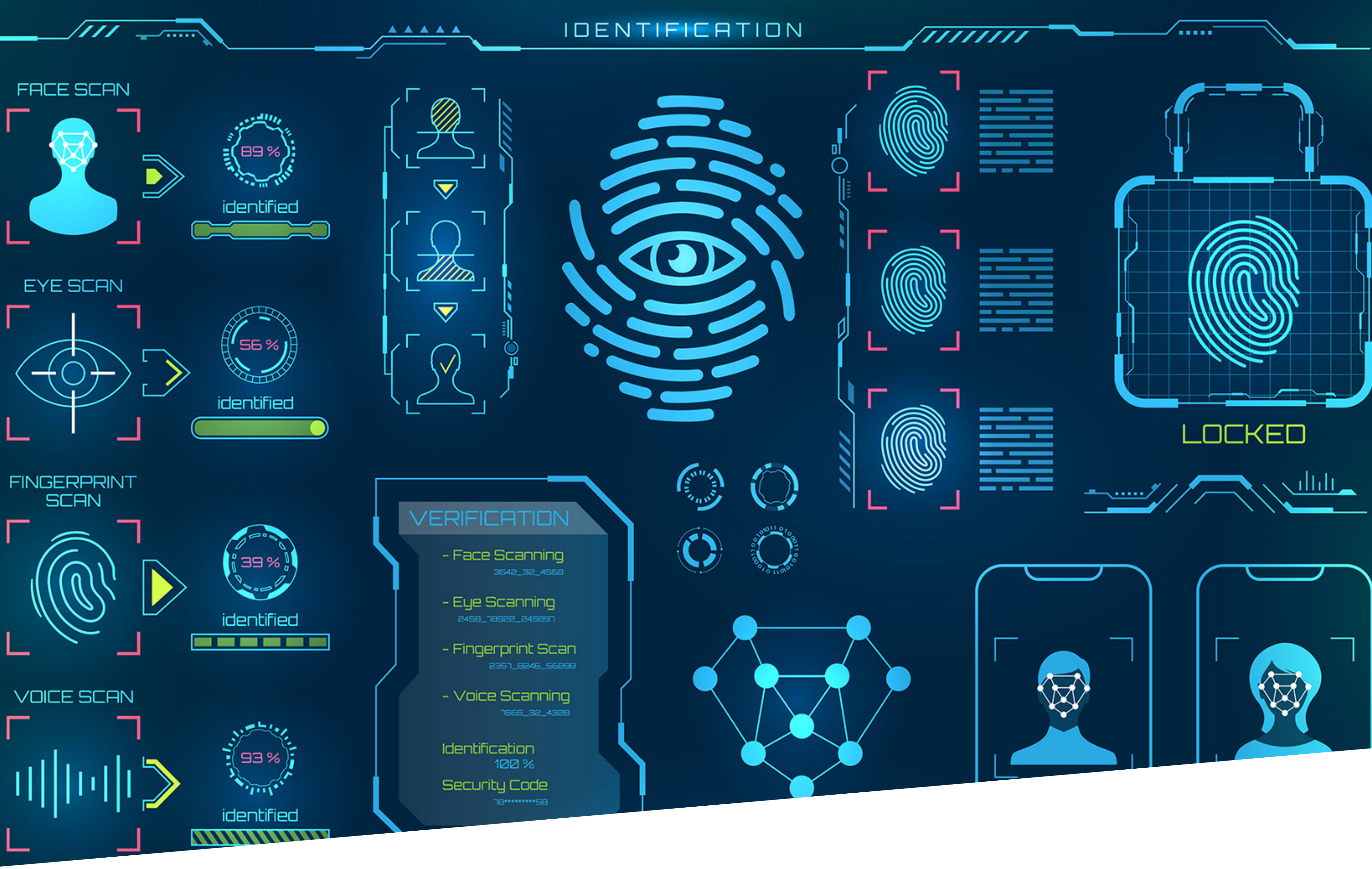
HYPR | yubico

Transcending Passwords:

The Next Generation of Authentication

November 2023 EMA Research Report
By Steve Brasen, Research Director
Endpoint and Identity Management

Table of Contents



Executive Summary

Emerging requirements for achieving security assurance in the face of accelerating threats, enhancing workforce productivity, and improving user satisfaction with IT services are driving businesses to advance access policies beyond relying on traditional passwords as the principal form of authentication. To help organizations make informed decisions on the types of authenticators to adopt, EMA conducted primary research involving surveys of end users and business IT professionals to gauge the effectiveness of adopted solutions. Key findings from the research results include:

- On average, business users authenticate ten times each day and use three different types of authenticators to access the business applications, data, and IT services they require to perform job tasks.
- 91% of businesses workers continue to rely on passwords as a primary form of authentication.
- On average, business workers lose or forget a password 1.6 times each week, and they are forced to reset a password 1.44 times each month.
- 68% of business workers admitted to violating their business' password policies, such as by using the same password for multiple business accounts, physically writing down a password, and resetting a password to one that they'd previously used.
- 82% of surveyed businesses reported IT security breaches occurred in their organizations in the last year, including virus infections, compromised credentials, and successful phishing attacks.
- On average, business users authenticating with a traditional password and an email-delivered one-time password (OTP) verifier spend 33 seconds completing the login process. This equates to 22 hours of work time spent on authentication per user each year.
- 19% of workers were reported to have been targets of phishing attack attempts in the last year, and 6% of workers were reported to be victims of successful phishing attacks during that time.
- Support for passwords is the most time-consuming access management process and, on average, administrators spend four hours per week managing employee access, including supporting account registrations, credential resets, and usability problems.
- 65% of business workers indicated they would be motivated to change employers if presented with high-friction authentication processes.
- 78% of business workers indicated they would be attracted to a new employer that offers easy-to-use authentication processes.
- 69% of business workers use some type of passwordless authentication to perform job tasks.
- The majority of surveyed IT managers recognize that the adoption of passwordless authentication will prevent most or all security breaches, particularly keystroke logging, virus attacks, ransomware, MFA/push bombing, and man-in-the-middle attacks.
- 81% of surveyed IT managers perceive passwordless authentication technologies as more secure than traditional passwords.
- 97% of organizations that have adopted passwordless authentication reported achieving quantifiable business improvements, most notably for increasing security effectiveness and employee satisfaction.
- Users employing FIDO-base authenticators (mobile device-based or security key) authenticate in only 8 seconds, or roughly 25% of the time it takes to authenticate with a traditional password/OTP combination.
- Organizations frequently using FIDO-based mobile authenticators or security keys as a primary authenticator were least likely to have been victims of a phishing attack.
- All surveyed businesses that have adopted FIDO standards reported significant quantifiable improvements, most frequently noting increased security effectiveness, reduced help desk tickets, decreased password reset frequencies, and improved user experiences.
- 56% of surveyed businesses that have introduced FIDO standards reported they were very satisfied with their adopted authentication processes compared to only 23% of non-FIDO adopters.

Moving Beyond Passwords

Passwords are inherently self-defeating. Any password simple enough for you to remember is easy for anyone else to figure out. This conundrum lies at the heart of many nefarious actors' attack strategy. Nonetheless, the majority of businesses continue to rely on passwords as the primary form of authentication. Legacy practices are hard to supplant, and when it comes to security, many IT managers have been reluctant to accept changing realities. After all, passwords have represented the foundation of security since the early days of computing, so there is a persistent misconception that any security approach must involve a memorized string of characters. However, as identity-targeted attacks continue to intensify in their frequency and sophistication, the irrational retention of passwords as an assumed standard is increasingly being recognized as unsustainable.

The first major cracks in the password-reliance wall emerged in 2017 with the release of the National Institute of Standards and Technology (NIST) Special Publication 800-63B, which advocated fundamental changes for the management of shared security, such as the elimination of forced password resets, the monitoring of compromised passwords posted on the dark web, and the use of a second authentication factor for verification. These proposed standardized practices were reinforced with the broad acceptance of "zero trust" security models that proposed that all access processes must be verified with two-factor authentication (something you know, have, or are) and policy-based management. More specifically, access processes must incorporate any two of the following three types of authenticators: something known (i.e., a password), something you have (such as a security key or mobile device), or something you are (a biometric, such as a fingerprint or face scan). The latter two options expanded the awareness of businesses of the opportunities of adopting passwordless solutions, even if only to supplement the traditional use of passwords. More recently, in 2022, an executive White House memo directed all U.S. federal agencies to adopt zero trust cybersecurity principles, noting "Agencies are encouraged to pursue greater use of passwordless multifactor authentication as they modernize their authentication systems."

The movement toward adopting passwordless authentication options is driven primarily by motivations for enhancing security in order to eliminate common password vulnerabilities while introducing authenticators that are significantly more challenging to defeat. However, the introduction of high security authenticators must not be implemented at the cost of user productivity. The number of steps it takes for a user to gain access to IT services is referred to as the level of "friction" imposed. High-friction authentications not only take longer for individuals to complete, they also result in dissatisfied and frustrated users. Unfortunately, while zero trust initiatives have pushed for more secure access processes, they also substantially increase friction on the end users. In particular, this is due to requirements for a second factor of authentication, most commonly involving one-time passwords or push notifications that require additional user tasks. Ironically, previous EMA research[1] empirically concluded that as access friction increases, security effectiveness is reduced because users find ways to bypass enterprise security controls in order to complete their tasks more rapidly. For instance, they may share credentials with colleagues or use unsecure public services, such as by distributing company data via Gmail or DropBox.

The business impact of employing high-friction authentication varies depending on the types of supported users. In support of employees, the level of access friction has bearing on the proficiency of workers in complete essential job functions, the agility of the organization to respond to customer and business requirements, and the ability of the company to attract and retain talent. However, even greater business impacts are seen in consumer identity and access management (CIAM) implementations. Online customers faced with high-friction access processes will simply leave and never come back, directly resulting in lost revenue.

With the persistent challenges high-friction authentication imposes, it is clear that we have reached an inflection point in access management. The continued use of passwords can no longer be accepted as the purveyor of security controls and the importance of creating positive user experiences must be recognized. This raises the obvious question—if not passwords, then what should people use for authentication? Numerous authentication options are readily available for adoption, and detailed analyses of the leading approaches are explored in this paper.

[1] The Rise of Low-Friction Access: Emerging Requirements and Solutions for Boosting Workforce Productivity and Security Assurance, 2022

Research and Methodology

In order to provide organizations with guidance on the types of authentication solutions that will improve security effectiveness while simultaneously minimizing access friction on the users, EMA conducted primary research into the requirements, usages, and outcomes of enterprise authentication solutions that businesses today actively employ. For the research, EMA performed two independent surveys—one collecting information on the experiences of end users and the other targeting knowledgeable IT managers responsible for access management in their organizations.

The end-user survey yielded 203 respondents from a broad range of industry verticals, but with a disproportionate number (44%) coming from high technology and financial institutions. Respondents were all determined to be full-time employees that utilize computers (PCs or mobile devices) to perform at least 40% of their job tasks. The respondents' ages ranged from 18 to 75, with an average reported age of 40.

The business survey netted 109 respondents, also from a broad range of industries, but with more substantial (68%) representation from high technology and financial institutions. Only IT professionals that were determined to be knowledgeable about their organization's adopted identity and access management solutions were included in the evaluation. Sixty-seven percent of respondents held senior-level positions within their company's technology division including IT managers, IT directors, CIOs, and CTOs.

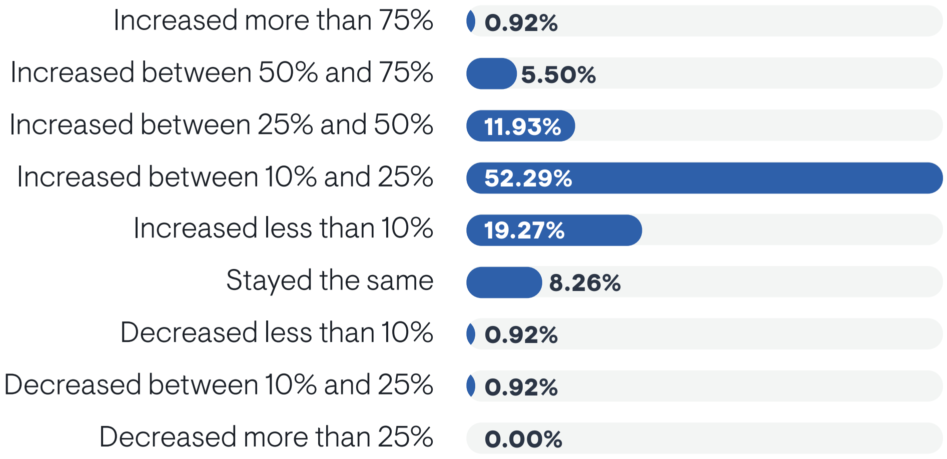
Nearly all respondents to both surveys were from North America and Europe. Only respondents from organizations supporting 100 employees or more were surveyed, and quotas were set to ensure representation across small, medium, and large business sizes. All respondents were carefully vetted to ensure their qualifications to respond to each survey and responses were tabulated to accommodate a 5% margin of error. Full survey demographics can be found in the appendices of this report.

The Current State of Authentication

Identity and Access Management Investments

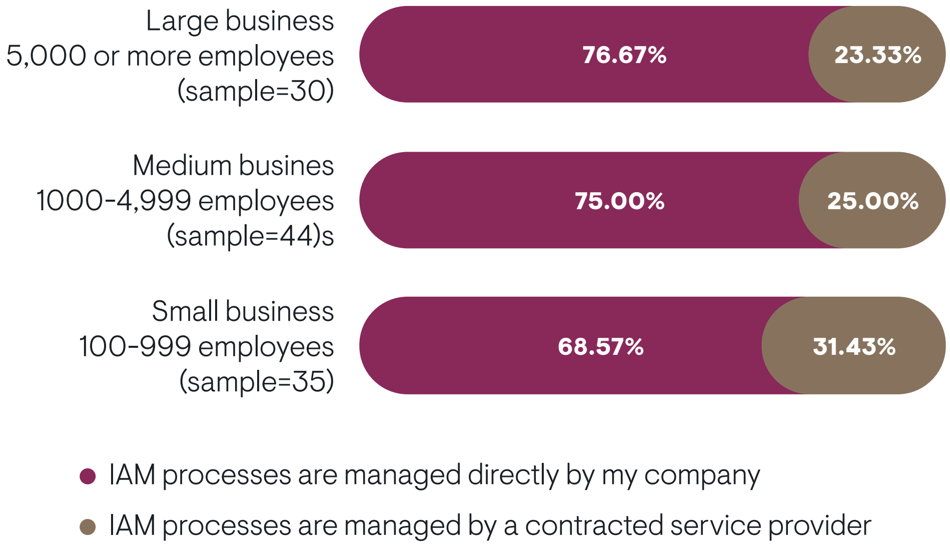
Over the past few years, processes and solutions supporting identity and access management (IAM) have systematically risen to become the primary focus of enterprise security management. Zero trust initiatives, which initially were developed to enhance network security, were recognized to be more effectively relegated to managing user access rather than just defining network microsegmentation. IAM is the doorway through which access to all business IT resources is controlled, and is thus the first line of defense against malicious attacks. Recognizing this importance and the significant vulnerabilities of traditional password-based authentication, businesses have invested heavily into adopting more effective IAM technologies. In fact, average budgets for IAM solutions increased more than 15% in 2023 compared to 2022 (Figure 1). Larger businesses (with more than 5,000 employees) have invested somewhat more in IAM solutions, averaging a 16% budget increase compared to small businesses (with fewer than 1,000 employees), which collectively saw a 14% budget increase. When purchasing enterprise IAM solutions, the primary decision-makers on which products and practices to adopt were most frequently identified as IT executives, including IT directors, IT managers, and CIOs/CTOs, according to 93% of survey respondents.

Figure 1: Percentage of businesses indicating budget increase or decrease for identity and access management solutions and services in 2023 compared to 2022



On average, one-quarter of surveyed businesses relied on contracted managed service providers (MSPs) to administer IAM processes. Small businesses were more likely to employ MSPs for this function according to almost one-third of respondents in that demographic (Figure 2). This aligns with the reality that smaller organizations often lack the internal administration resources and expertise to adequately support security and compliance requirements, particularly in support of access controls. IT budgets supporting IAM services for businesses relying on MSPs were noted to have increased by 16% over the past year, surpassing the overall average and indicating a significant increase in related service charges over that period.

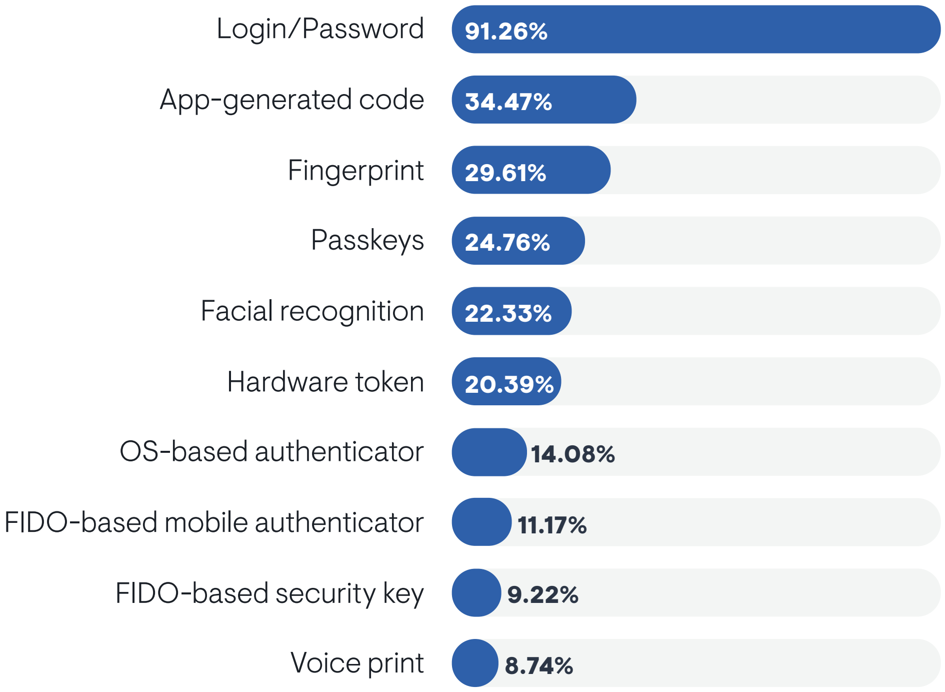
Figure 2: Percentage of businesses indicating how IAM processes are managed in their environment, segmented by organization size



Authenticator Adoption

On average, business users employ three different types of authenticators to access business applications, data, and IT services. Traditional passwords continue to be the dominant form of authentication employed in business environments, with 91% of surveyed business users noting they are needed to perform job tasks (Figure 3). Among these users, 49% utilize a password manager that records encrypted credentials so that login name and password information can be autofilled at time of authentication. While password managers reduce the friction on end users by eliminating the need to recall passwords, they are also inherently insecure because anyone accessing the user's device gains unfettered access to any accounts for which passwords are stored.

Figure 3: Percentage of end users indicating the types of authenticators they use to access business applications, data, and IT services



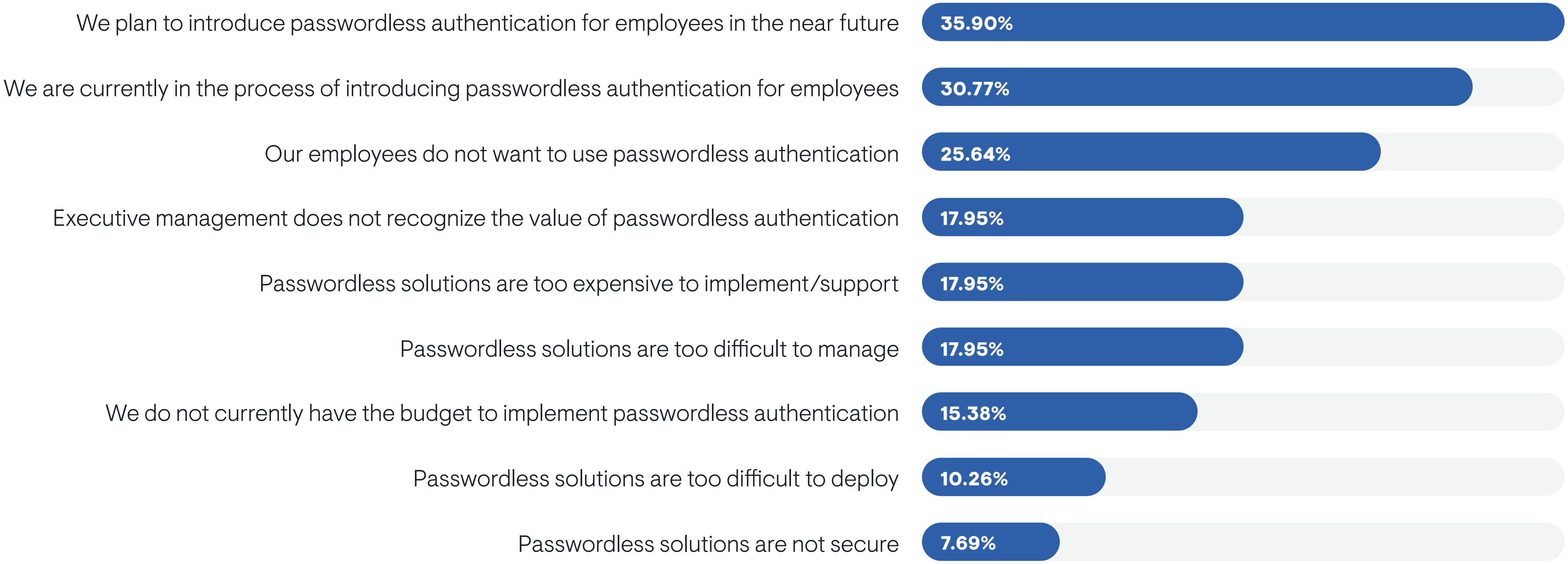
Much more encouraging is the indication that 69% of business workers now regularly use some type of passwordless authentication as part of their job routine, and 80% of businesses support at least one type of passwordless authenticator. Among organizations that support passwordless authentication, the technology is employed for 98% of access events. Biometrics—including fingerprint scans, facial recognition, voice print verification, and behavioral analysis—were most frequently noted to be in use by 61% of businesses and 39% of total businesses users. Fingerprint scans were the most frequently identified biometric in use, undoubtedly due to their common availability and employment with mobile devices.

Also noted as achieving significant adoption were passkeys, which are a fairly recent digital credential technology based on FIDO standards. Utilizing both public and private cryptographic keys, passkeys are much more secure than traditional passwords and allow users to authenticate without having to memorize password strings. The fact that passkeys have been publicly available for little more than one year and yet are indicated to be in use by one-quarter of business workers is a testament to the technology's meteoric rise and popularity. In fact, it is easy to predict that passkey adoption will continue to grow and is the most likely contender to unseat traditional passwords as the dominant authenticator.

More secure FIDO-based authenticators, including mobile authenticators and security keys, were collectively noted as being in use by 18% of users and supported by 17% of businesses. FIDO-based mobile authenticators (e.g., HYPR) enable authentication to IT services, including desktops and online apps, using biometrics built into iOS and Android devices. This fundamentally differs from app-generated codes (e.g., Authy, Google Authenticator, etc.) in that the users initiate the mobile authentication, rather than the applications they are accessing, making FIDO-based mobile authenticators much more phishing-resistant. Additionally, app-generated codes are a higher-friction solution, requiring users to manually copy characters from the mobile app to the login prompt, and are principally used as verifiers in multifactor authentication rather than as a primary authenticator that eliminates the need for passwords. Security keys (e.g., Yubico YubiKey) are physical devices, sometimes called "dongles" or "key fobs," that enable access when they are connected or in proximity to the device used for accessing IT services. Both FIDO-based mobile authenticators and security keys were twice as likely to be utilized by large businesses than small businesses and were more popularly adopted by highly-regulated industries, such as financial institutions.

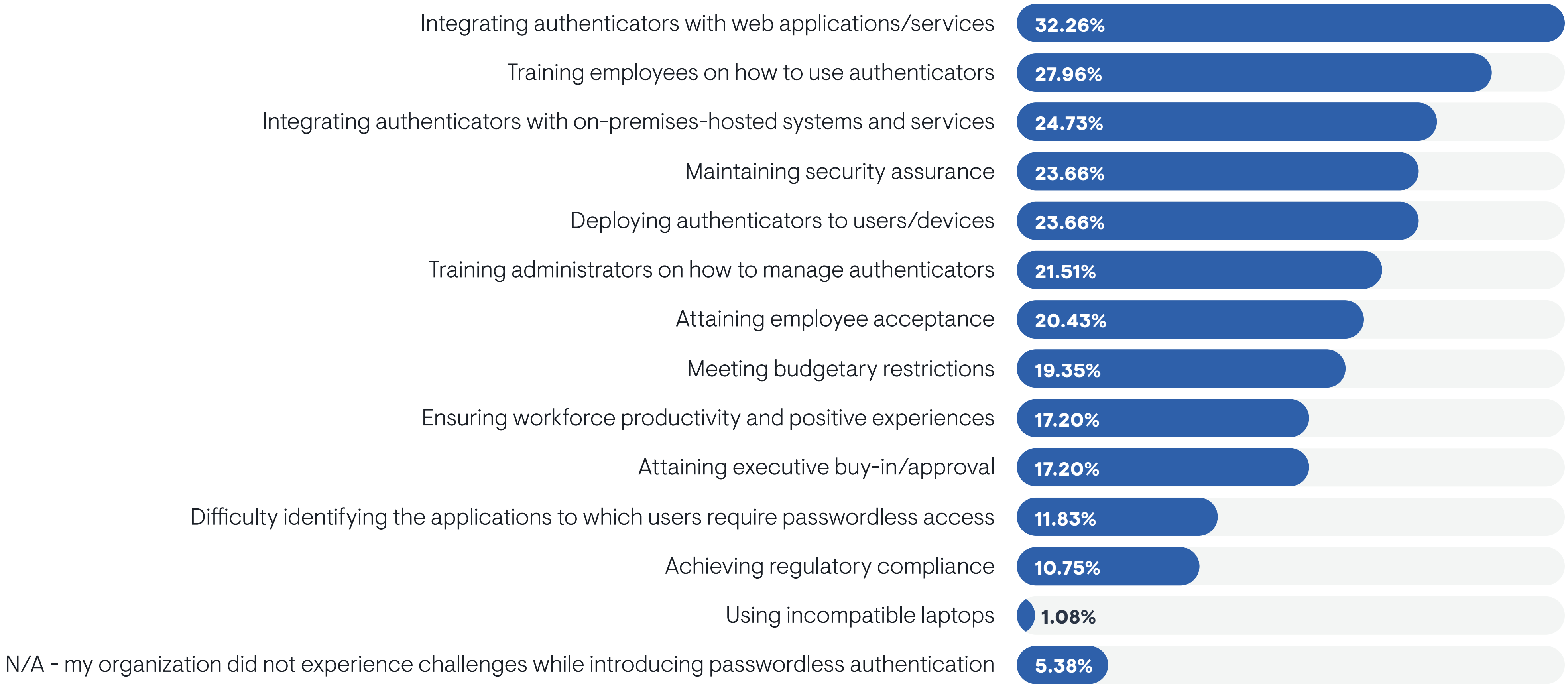
Among surveyed businesses that are not yet supporting passwordless authentication, 67% indicated they either plan to introduce related solutions or are actively in the process of doing so (Figure 4). In total, this indicates 90% of all businesses are embracing passwordless authentication as part of their security portfolios. Among organizations that do not employ or have no plans to employ passwordless authentication, the most frequently noted reason for not adopting is that the value of the solutions is not recognized by either employees or executive management. This rationale is typically associated with a fear of change, particularly in regard to IT. Users simply do not want to make the effort to learn how to use a new technology, and executives are reluctant to take a chance on disrupting business operations. However, it is very notable that these more general detractors far outweigh more specific concerns about security, costs, ease of use, and manageability.

Figure 4: Percentage of surveyed organizations that do not currently support passwordless authentication indicating the status or business reasons



Organizations that have successfully adopted passwordless authentication technologies broadly indicated the implementation processes was not effortless. In fact, 95% of survey respondents reported at least some challenges with the passwordless technology rollout (Figure 5). Most notably, 39% of adopters reported integration issues, with the majority of these respondents indicating difficulty integrating with both web applications and on-premises IT resources. Organizations using hardware tokens and non-FIDO-based push notifications were most likely to indicate that they experienced integration challenges. Points of integration are often developed using industry standards, platform APIs, and custom coding, which can be time-consuming and costly. However, 71% of the organizations indicating they had no trouble integrating passwordless authentication solutions with web applications and services had also adopted FIDO standards, strongly suggesting these will significantly simplify implementation processes.

Figure 5: Percentage of surveyed businesses that have adopted passwordless authentication processes indicating the most significant challenges to implementing the solutions



Multifactor Authentications

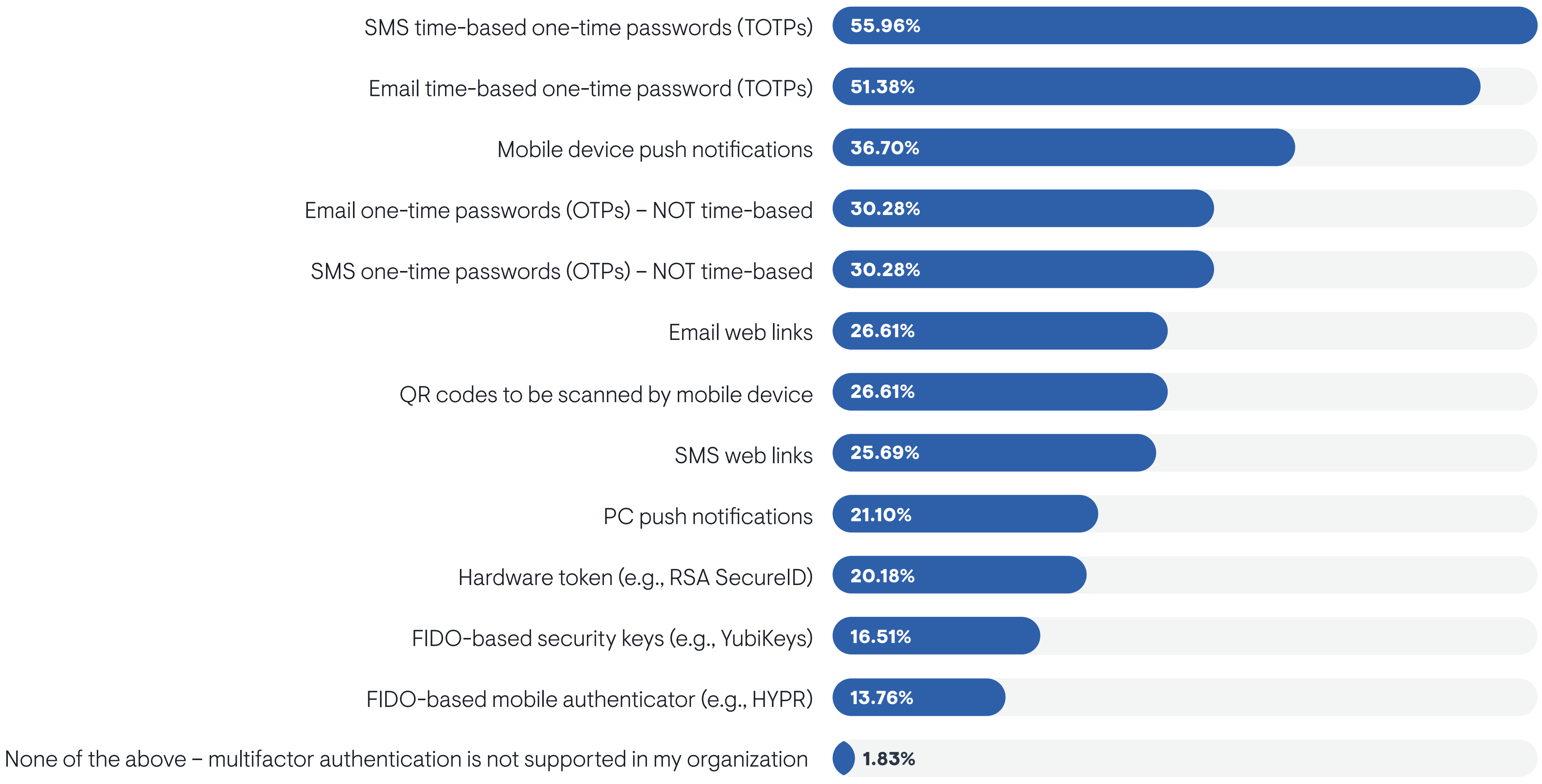
Zero trust security architectures were first defined in 2009 as a networking model that eliminates vulnerabilities inherent with perimeter-based security implementations. By around 2017, however, security experts broadly recognized that enhanced identity management practices should more appropriately be adopted as the primary mechanism for achieving a zero trust model. Early definitions of zero trust identity management proclaimed that primary authenticators, such as a password, should be supplemented with an independent secondary verifier. To meet this requirement without incurring excessive costs or deployment efforts, most organizations deployed verifiers that could be easily layered on top of existing password-based login processes. These two-factor authentication (2FA) technologies included one-time passwords (OTPs) delivered via email or text messages to mobile devices, push notifications, and hardware tokens. However, these approaches substantially increased friction on the end users because they required authentication steps that supplemented rather than replaced already time-consuming login tasks. As other verification technologies were introduced or became more viable—particularly passwordless authenticators—the term multifactor authentication (MFA) rose in prominence to refer the broader range of available verification solutions in addition to legacy 2FA approaches. Today, MFA solutions may act as a verifier to a primary authenticator or may incorporate two or more factors of authentication into a single access technology to minimize end-user friction.

Among surveyed organizations, 98% indicated they employ some types of MFA to enable employees to access business IT resources (Figure 6). Since the majority of businesses have already invested in the technology, OTPs continue to dominate as the most common identity verifier, with 85% of surveyed businesses reporting them to be in use. Time-based OTPs, which offer greater security by automatically expiring temporary passcodes after a predetermined period, were more frequently reported to be in use, as noted by 71% of organizations versus only 42% utilizing OTPs that are not time-based (including 28% that employed both types). Among businesses supporting OTP verifiers, 21% deliver the passcode via email, 22% deliver it via SMS text message, and 57% support both options. However, end users reported they were 12% more likely to employ an OTP delivered via SMS than email, indicating this to be the somewhat more preferred choice when given the option.

Push notifications also continue to be popularly in use, according to 50% of surveyed businesses. Related solutions send an alert (often a popup message) to an application on the user's endpoint device requesting the user to authorize the access. Among organizations that support push notification verifiers, 57% send the notification to mobile devices, 26% send the notification to desktop PCs, and 17% support both. Similar solutions, in use by less than one-quarter of businesses, send web links via an SMS message or require a mobile device to scan a QR code in order for users to confirm they are the ones requesting access. Another legacy 2FA technology still in use by 27% of organizations are hardware tokens, which are physical devices that display a code that must be manually entered to gain access to sensitive IT resources.

More secure and easier to use FIDO-based solutions, including mobile device authenticators and security keys, were collectively supported as verifiers by 24% of surveyed businesses and more commonly among those from highly-regulated sectors, including finance and government institutions. Among adopters, 58% use them to verify a different primary authenticator, while 42% employ them as self-contained MFA solutions.

Figure 6: Percentage of surveyed businesses indicating the types of supported multifactor authenticators



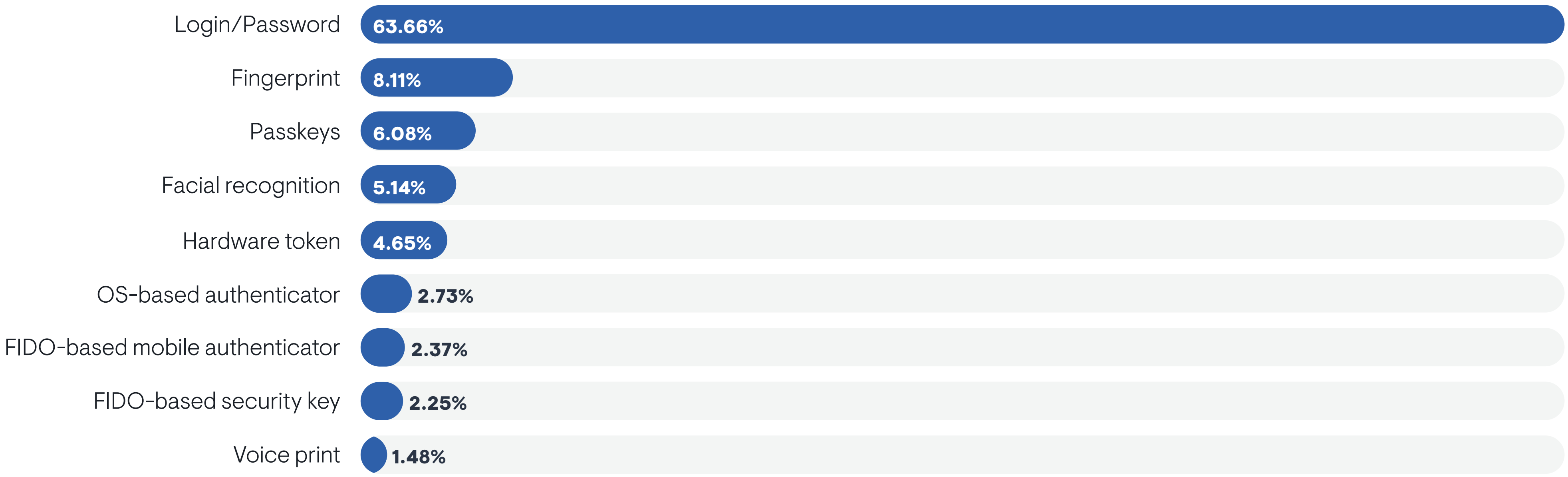
Authentication Experiences

Frequency of Authentications

User experiences with access processes have direct impacts on their productivity, job performance, and overall satisfaction with IT services. Any friction associated with authentication processes is compounded by the frequency of times a user must perform authentication tasks. On average, surveyed business users reported authenticating ten times each day to access the business applications, data, and IT services they require to perform job tasks. Even with the broad availability of single sign-on (SSO) and adaptive access technologies, the diverse range of devices, SaaS apps, web apps, servers, and networks accessed by the average business user makes it extremely challenging to further unify access processes with current IAM implementations. The frequency of authentication aligns with business user roles and the types of related tasks they must perform. According to averaged survey results, the most frequent authentications are performed by users in communications (20 times/day), sales (12 times/day), and IT administration (10 times/day) roles.

Not surprisingly, the majority of reported authentications involved entering a password, constituting 64% of total authentication tasks (Figure 7) reported by surveyed business users. Among password authentications, 29% were autofilled using a password manager, trading off security assurance in order to eliminate the need to recall complex password strings. Biometrics accounted for 15% of authentications, with fingerprint scans the most frequently employed form. These results make it clear that adoption rates of passwordless authenticators far exceed their frequency of usage and that traditional password-based authentications must be performed much more frequently than alternative authentication approaches. Likely, this is due to the fact that passwords continue to be utilized as the primary authenticators in the majority of access processes and that authentication reduction technologies, such as SSO and adaptive access, are more frequently employed in conjunction with passwordless authentication solutions.

Figure 7: Average percentage of total authentications performed by each authenticator type as reported by surveyed business users

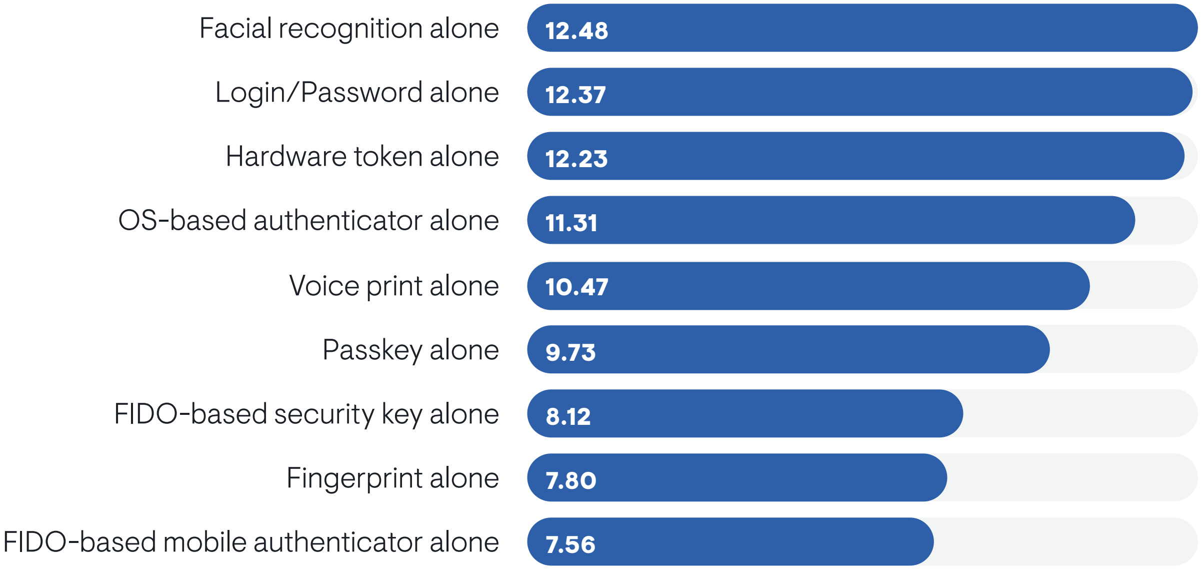


Time Spent Authenticating

The more time and effort required for a user to access business IT resources, the more distracted they will be from performing critical tasks and the longer it will take for them to refocus back to completing their intended action once access is granted. On average, across all authentication approaches, it takes 20 seconds for a user to complete the steps necessary to access a single application or IT service, including navigating login screens, entering passwords, performing biometric scans, and/or accessing a mobile device or email to perform the verification task. While at first glance this time may appear brief, human perceptions can make it seem a veritable eternity when in a rush to complete an urgent task. One need only stare at a clock for 20 seconds to get a feel for the level of disruption that can be imposed on a user's productivity.

The amount of time it takes to complete authentication tasks is directly related to the level of imposed access friction. Among single-factor authentications (i.e., authenticators used without a verifier), FIDO-based mobile authenticators were determined to provide the most rapid user access (Figure 8). These approaches allow users to simply approve access to associated IT services in a single step on their smartphone without having to initiate the access on their desktop or browser. FIDO-based security keys were also indicated to enable rapid authentication, especially for users that keep the key connected to or in proximity with their device. Among biometric authenticators, fingerprint scans were indicated to have been performed the most rapidly. Interestingly, facial recognition scans did not fare as well, landing somewhat on par with the time it takes to log in using a password. Facial recognition is inhibited by the need to center the user's face on the scanner, and a poorly posed or blurry image sometimes results in the need for the user to repeat the scan.

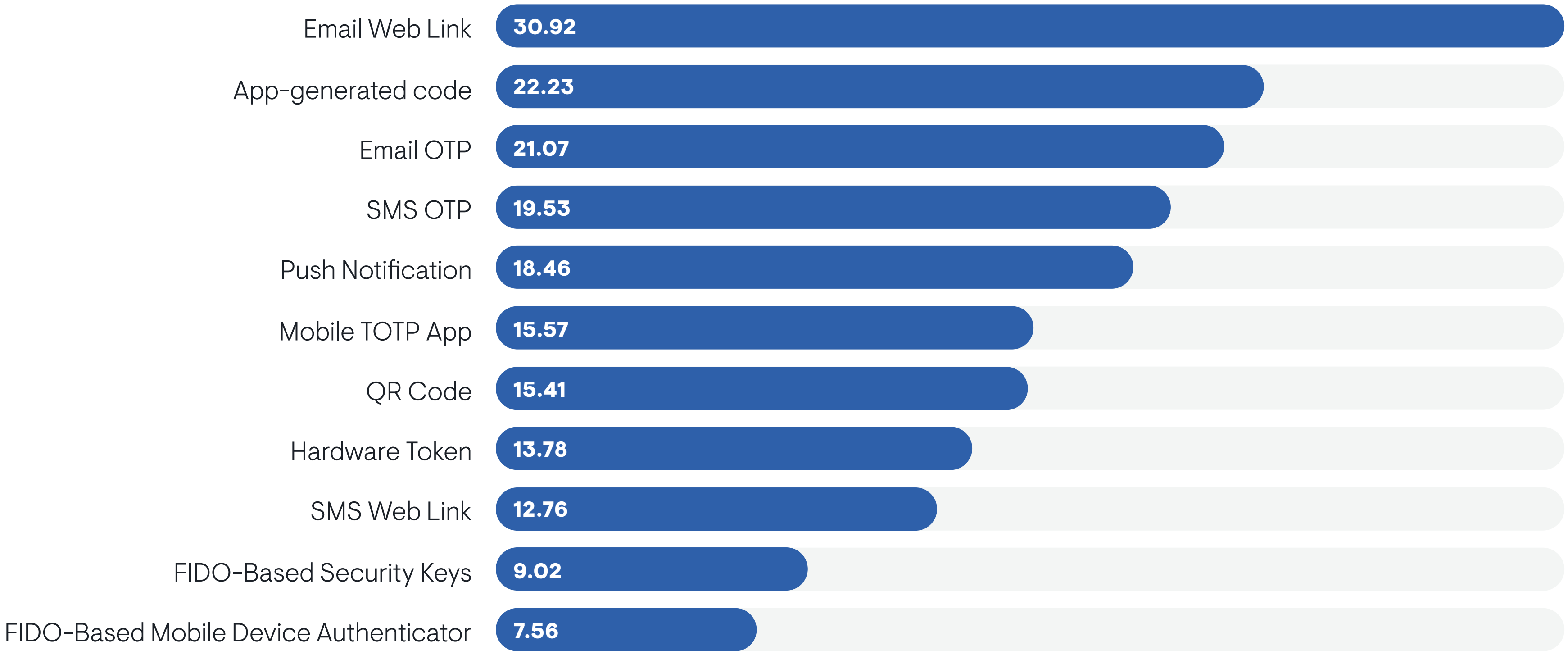
Figure 8: Average number of seconds it takes for a user to log in using each type of primary authenticator



The use of MFA substantially increases authentication times because many verifiers take substantially longer to complete (Figure 9). FIDO-based mobile authenticators and security keys again stand out as taking the briefest time to complete. Solutions requiring the delivery of a verifier component (i.e., a web link or OTP) via email were indicated to incur the most egregious times because they must incorporate the time it takes to deliver the email. Access times involving the use of app-generated codes were also noted to be excessive, likely due to the time it takes to access the application and copy over the passcode.

By adding averaged times for employing primary authenticators and verifiers (Figures 8 and 9, respectively), time estimates for different combinations of MFA authenticators can be calculated. For instance, the use of a traditional password with an OTP verifier can be expected to take roughly 32 seconds to complete, which is significantly higher than the overall average of 20 seconds. These total authentication times can rapidly add up. Assuming the average frequency of 10 authentications per day and 250 workdays in a year, a 32-second authentication time translates into 22 hours of work time spent on logins per user per year. Multiply that by the number of workers in an organization and it is clear that significant business resources are being spent on high-friction authentication processes. By comparison, users employing FIDO-based mobile or security key authenticators with built-in two-factor authentication are able to access IT resources in only about eight seconds, which equates to roughly 5.5 hours of time each year and a 75% reduction in efforts over traditional password/OTP combinations.

Figure 9: Average number of seconds it takes users to complete verification tasks in multifactor authentication implementations



Password Resets

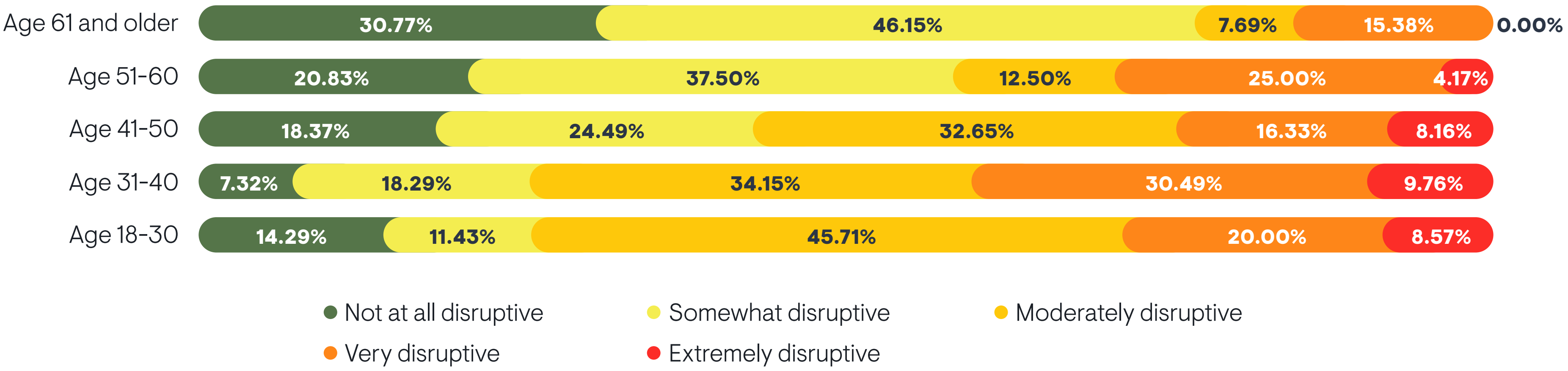
With extremely high authentication frequencies and completion times, traditional passwords can easily be identified as the authenticator most impactful to end-user productivity. However, password friction is further intensified because of the need to perform periodic password resets. It is an unfortunate fact that the typical human brain is simply not equipped to recall complex and constantly changing character sequences that are unique for each of the hundreds of accounts regularly accessed in our daily lives. As a result, according to surveyed users, a password is forgotten an average of 1.6 times by each user each week, forcing them to initiate very time-consuming and often complex password recovery processes.

In addition, many businesses and application providers continue to force periodic password resets. New best practices outlined in the NIST Special Publication 800-63B recommend never forcing a user to change a password unless the credential is known to have been compromised. The enforcement of password change policies actually decreases security effectiveness because they increase the likelihood that a user will violate password policies, such as by writing down passwords or using the same password for multiple accounts.

Nonetheless, 94% of business users indicated their organization periodically forces a password change. On average, a password reset was noted to be required every 1.4 times each month for each business employee.

Password reset processes significantly extend login times and mentally distract workers from accomplishing job tasks. Most often, the most challenging part of the process is coming up with new passwords that are unique, difficult to guess, and at the same time memorable. Employee energy spent on these tasks is better spent focusing on accomplishing business-related tasks. Among surveyed business users, 86% find it disruptive to their work productivity to perform a password reset. Interestingly, survey results indicate a correlation between the level of perceived disruption and the user's age, with younger survey responders generally less likely to be tolerant of password reset tasks (Figure 14). Older users have been using passwords for decades and are more likely to accept the need for periodic resets as status quo. By contrast, younger employees (particularly Millennials under the age of 40) are more acclimated to alternative authenticators, like biometrics, and more frequently recognize password resets as a significant nuisance.

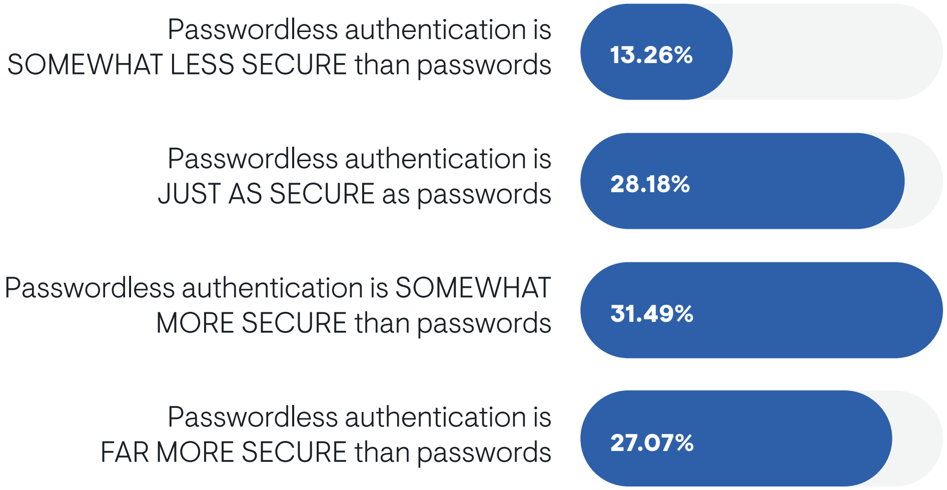
Figure 10: Percentage of surveyed business users who indicated the level of disruption caused by a password reset, segmented by responder's age



Sentiment Toward Passwordless Authentication

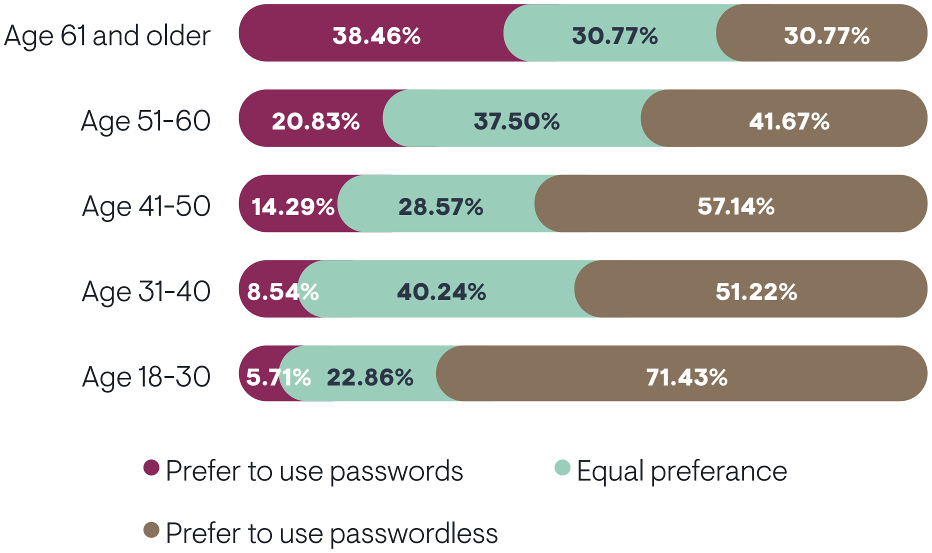
Advances in technology. coupled with revelations about the security inadequacies of traditional password approaches. have redefined many users' relationships with passwordless authentication solutions. While perceptions that passwords were central to personal IT security were prevalent only a few years ago, general recognition of passwordless security effectiveness has far eclipsed legacy thinking. Today, according to survey results, 59% of users recognize passwordless authentication as more secure. with only 13% still considering passwords to provide better protection (Figure 11). Sentiments toward passwordless authentication security effectiveness were also noted to correlate to a responder's age, with survey responders under the age of 50 twice as likely to indicate their preference of passwordless authenticators as a more secure access solution.

Figure 11: Percentage of surveyed users indicating their perception of the security effectiveness of passwordless authentication compared to traditional passwords



Of course, security is not the only consideration when it comes to user preferences in the types of authenticators they wish to regularly employ. Ease of use and the speed at which access will be granted also play a critical role. All these elements considered, 54% of survey respondents reported they prefer to use passwordless authentication over traditional passwords. Only 13% stated that they prefer traditional passwords, with the remainder indicating no preference. Again, a clear correlation can be made between the responder's sentiment and their age, with younger users more apt to prefer passwordless technologies and older users more reluctant to give up familiar password-based processes (Figure 12). Overall, 74% of responders stated they prefer employing biometric authenticators, suggesting related technologies to be the current favorite among general users.

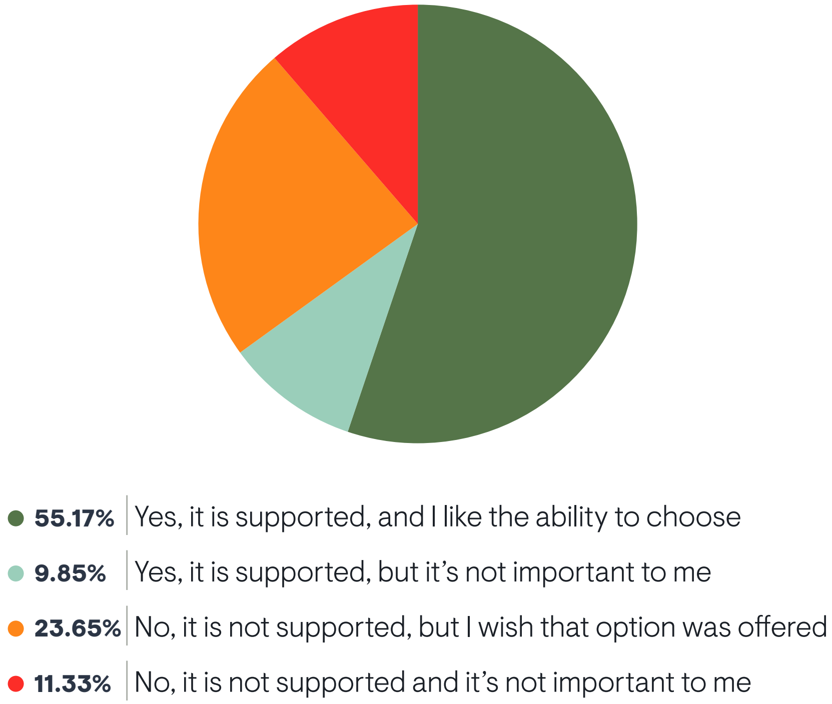
Figure 12: Percentage of survey respondents indicating their preference of using passwordless authentication compared to traditional passwords, segmented by responder's age



Authenticator Selection

Access preferences particularly come into play with login solutions that allow users to select from a list of authenticators. Among survey respondents, 75% indicated their employers offer the option to select the type of authenticator they will use during each login session. On average, users are presented with between three and four authentication options. Among respondents from organizations that do not offer authentication choices, 67% stated that they would like that option to be offered. In total, 79% of survey respondents indicated they like having or would like to have the ability to select authenticators during login processes.

Figure 13: Percentage of survey respondents indicating whether they have the ability to choose an authenticator when logging in to business IT services and if they like that functionality



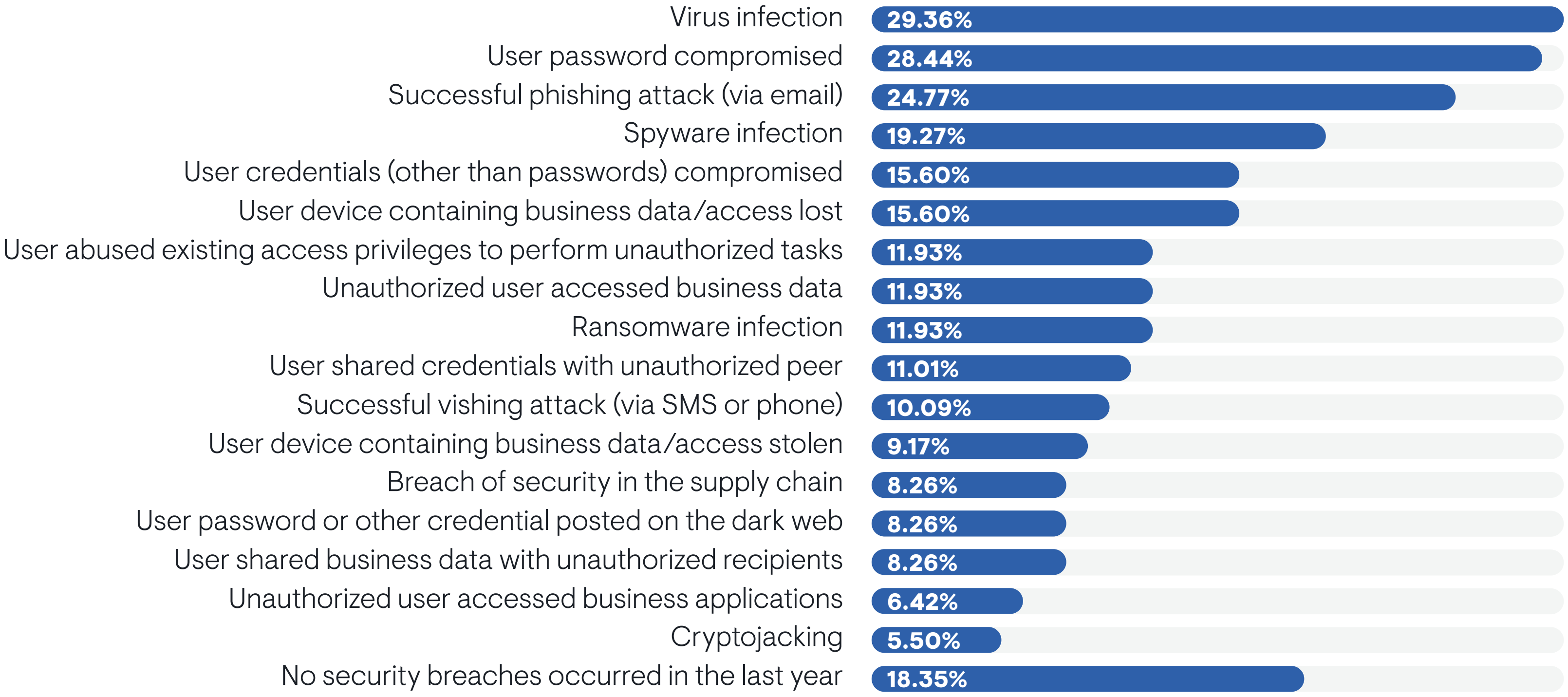
Security Effectiveness

Breach Events

Despite broad adoption of zero trust recommendations calling for two-factor authentication with policy-based control, security breaches continue to increase. Malicious actors have adapted to changing security landscapes by introducing new and revised attack strategies. In total, 82% of surveyed businesses reported that IT security breaches occurred in their organizations in the last year, most frequently noting incidents of virus infections, compromised passwords, and successful phishing attacks (Figure 14).

Software-based attacks, including viruses and spyware, are most frequently not related to identity management because they occur when users open compromised emails or run infected software. However, they can also occur when hackers breach identity security and intentionally deploy the software on a user's device. Interestingly, businesses supporting user access with a mobile device push notification were most frequently noted as having contracted a virus, spyware infection, and ransomware. Users who regularly respond to push notifications may reflexively respond to fake popups that deploy malware. Similar "push bombing" attacks have also become prevalent, which involve multiple login attempts against a company's SSO portal, triggering push notification verifiers to a large number of employees in the expectation that at least one will reflexively authorize the access.

Figure 14: Which of the following security breaches occurred in your organization in the last year?

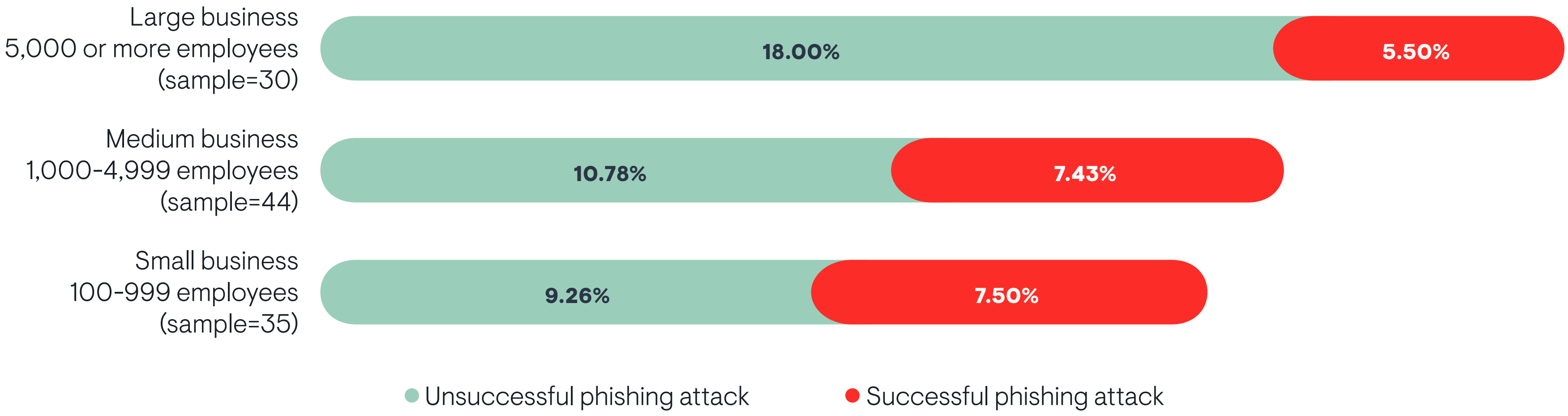


Phishing Attacks

In the last year, 19% of all business workers were noted to be the target of phishing attacks, of which 6% were successful. Phishing attacks involve emails delivered as part of a scheme to trick users into providing login credentials and other sensitive information, and techniques evolved significantly in recent years to include sophisticated social engineering to increase the chances of successfully deceiving business users. While the majority of phishing attacks continue to broadcast to a wide and random number of people, more advanced "spear phishing" attacks that target specific individuals are also on the rise. In total, one-quarter of surveyed businesses reported that at least one of their employees experienced a successful phishing attack.

Larger businesses were more frequently reported as being the target of a phishing attack; however, small businesses more frequently reported phishing attacks that were successful (Figure 15). Similarly, highly regulated industries, such as finance and government, were less likely to have contended with a successful phishing attack. The implication is that large businesses are more frequently employing phishing-resistant security technologies. In particular, research results clearly indicate that organizations adopting FIDO-based mobile device authenticators or security keys were least likely to experience a successful phishing attack, with only 2% of solution adopters reporting a related breach.

Figure 15: Percentage of surveyed businesses indicating successful and unsuccessful phishing attack attempts, segmented by organization size

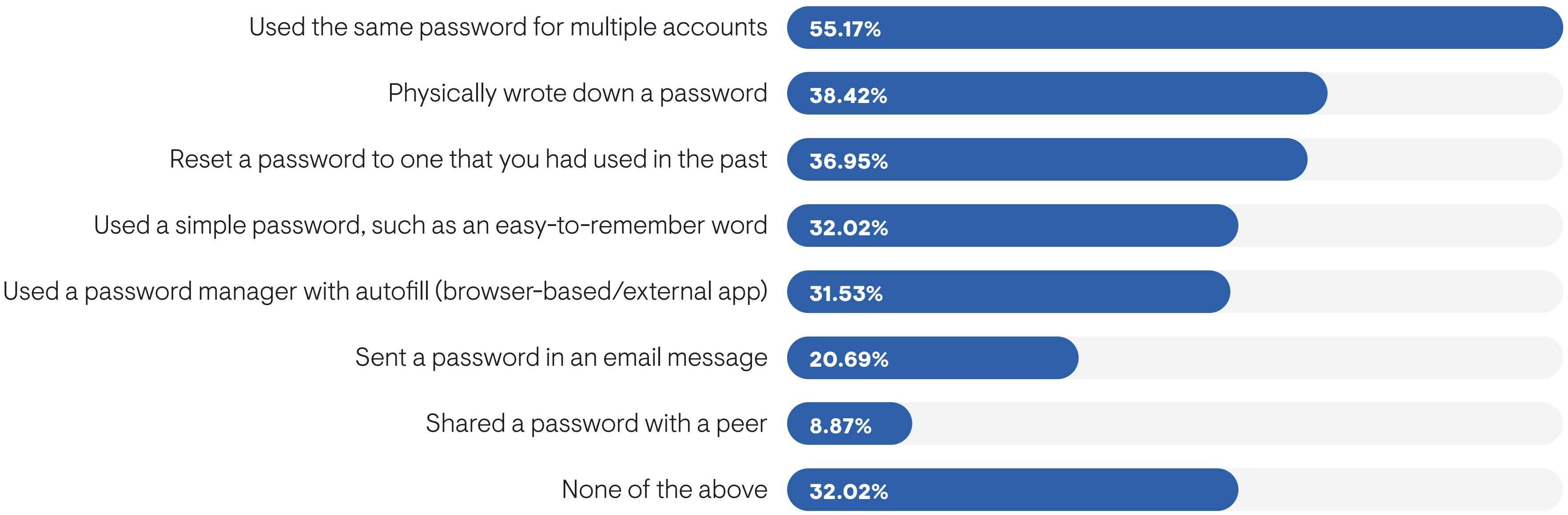


Password Policy Violations

Malicious actors employ a wide range of techniques for acquiring user account passwords, including brute force, keylogging, man-in-the-middle, rainbow table, mask, and good old-fashioned dictionary attacks. Unfortunately, the effectiveness of all these methods is greatly increased by poor password policy control. Despite the fact that businesses have broadly cracked down on policy enforcement within their organizations, end users persist in circumventing these policies in order to simplify authentication processes. In total, 68% of surveyed users admitted intentionally and knowingly violating their business' password policies (Figure 16) and 93% of surveyed businesses reported at least one incident of a password policy violation. The most frequently noted violation was the use of the same password for multiple accounts, as noted by more than half of respondents. Among this group, 47% admitted they employ the same password for both business and non-business accounts, which is particularly egregious since any breaches on services such as public email and social media websites will also compromise any business systems to which that user has access. Once passwords have been stolen from public services, they are posted on the dark web and used to seed guessing tables when attacking business networks.

The reason users use passwords for multiple accounts as well as violate other password policies—such as physically writing down passwords, reusing past passwords during a reset, and employing easy-to-guess passwords—is to reduce or eliminate the chance that they will forget the password and have to go through the pain of resetting it. Similarly, users who employ a password manager that saves passwords and then autofills them during authentication requests are also placing the business at risk. Any malicious actor who gains access to a user's application or browser-based password manager, such as by breaking the master password, will have access to any business services for which passwords have been stored.

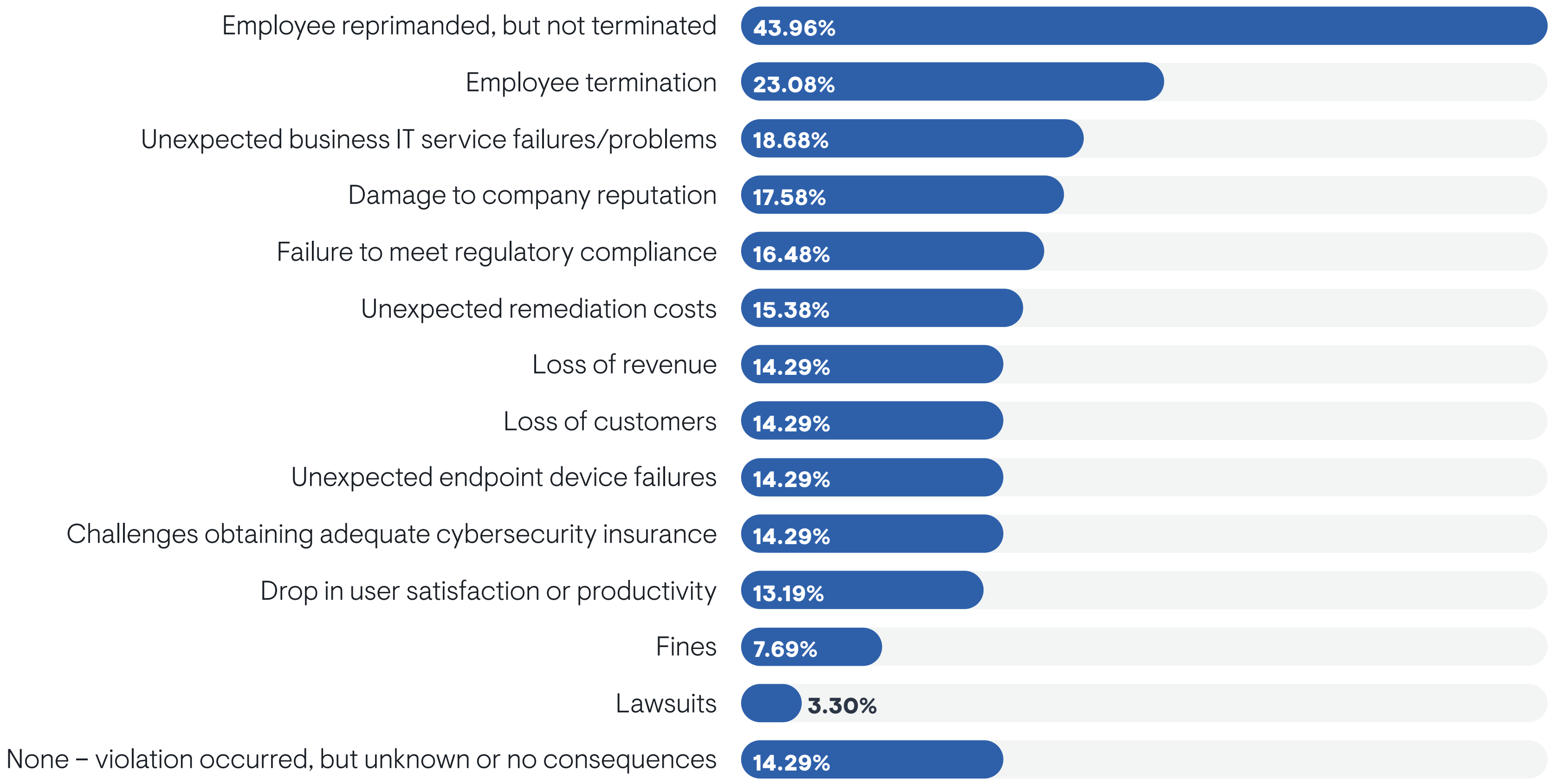
Figure 16: Percentage of surveyed end users indicating password policy breaches they committed when using business IT systems



Security Breach Consequences

Identity security breaches frequently result in significant and long-lasting ramifications to the business. In fact, among surveyed organizations that experienced a security breach in the last year, 72% reported business-impacting consequences as a result (Figure 17). Most frequently noted were penalties imposed on employees who violated security policies. More than half of all surveyed businesses that were breached indicated employees were reprimanded and/or terminated as a result. More serious direct business consequences—including business service interruptions, damage to company reputation, failure to meet regulatory compliance, loss of revenue, loss of customers, fines, and lawsuits, were collectively reported by 54% of qualified respondents. One out of every seven breached businesses additionally reported difficulty obtaining cybersecurity insurance following breach incidents.

Figure 17: Which of the following occurred due to a violation of your organization's access policies?

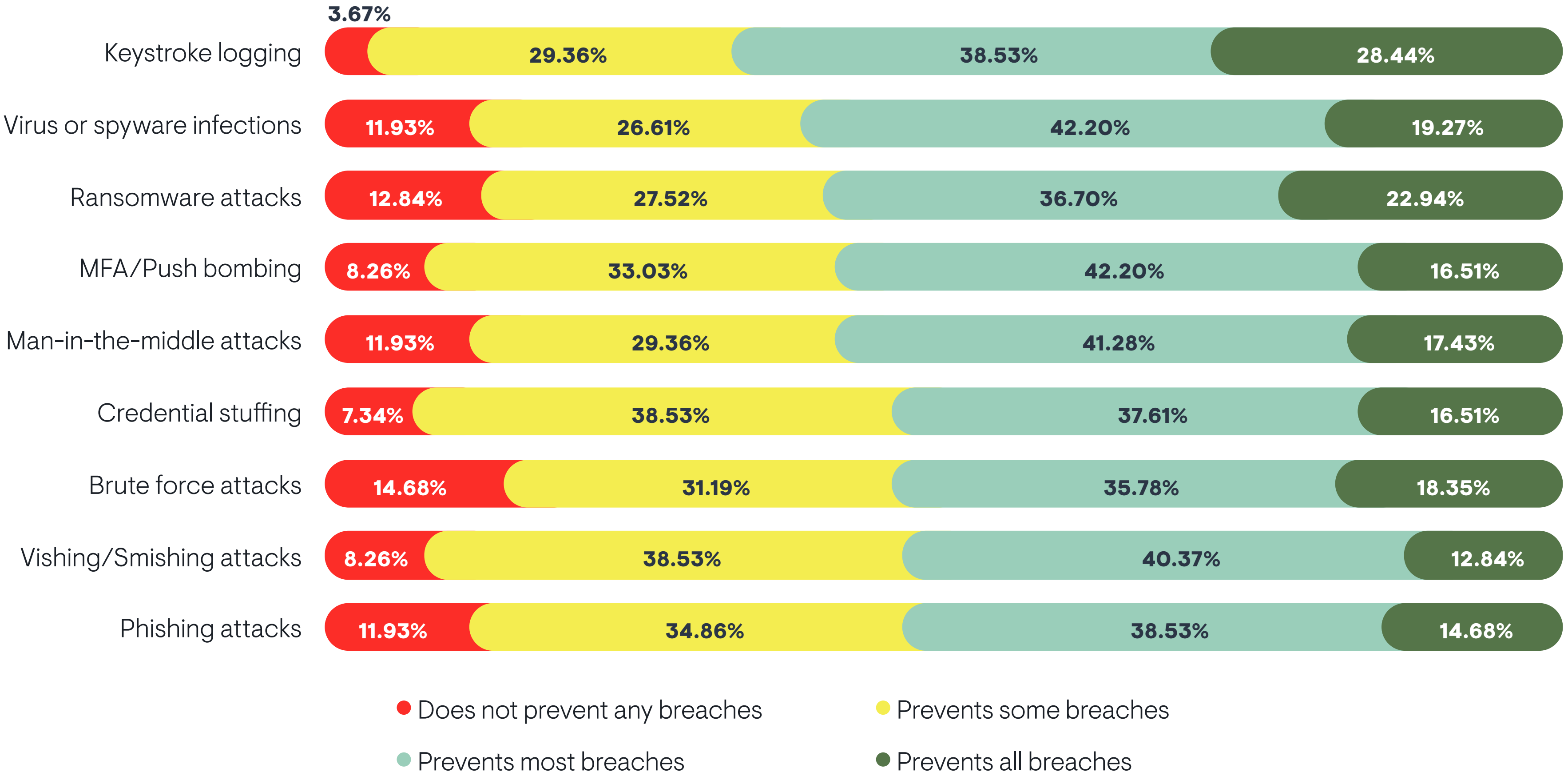


Passwordless Security Perceptions

Faced with escalating attacks and significant consequences to breach events, many organizations are looking to adopt passwordless authentication technologies as security enhancements. Overall, 81% of surveyed IT managers reported that they perceive passwordless technologies as more secure than traditional passwords, with 13% believing they provide the same level of security.

Furthermore, more than half of respondents stated they believe passwordless authentication solutions will prevent all or nearly all of the most challenging cybersecurity threats, including keystroke logging, virus attacks, ransomware, MFA/push bombing, and man-in-the-middle attacks (Figure 18).

Figure 18: Percentage of surveyed IT managers indicating how effective they believe the adoption of passwordless authentication is at preventing leading security threats



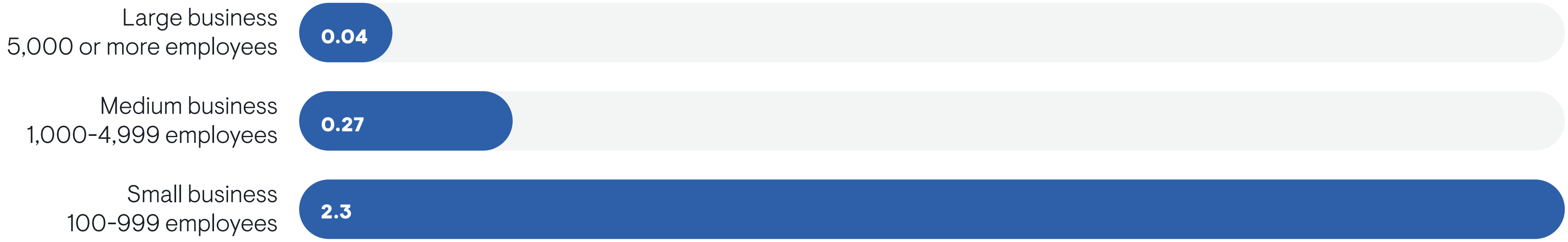
Authentication Management

Administration Time

Business costs related to authentication solutions are not limited to just end-user productivity, but also apply to the time and effort IT administrators invest in maintaining adopted solutions. According to research results, administrators across all surveyed businesses collectively spend an average of 3.56 hours per week managing user access for all employees in their organization, including supporting account registrations, credential resets, usability problems, and other access-related issues. This equates to roughly 14 minutes of administration each week for every 100 employees. However, this amount of administration time does not scale evenly across organization sizes. Smaller organizations (supporting fewer than 1,000 employees) spend more than two hours each week supporting every 100 users, while larger businesses (supporting more than 5,000 employees) spend little more than two minutes for every 100 users addressing authentication issues (Figure 19).

The discrepancy in access management administration times across organization sizes can be attributed to the complexity of adopted authentication solutions. Larger organizations are more apt to invest in more comprehensive access management solutions, including adaptive access, self-service access portals, and support for FIDO-based authenticators. By contrast, smaller businesses are more likely to rely on traditional passwords with high-friction verifiers (OTP and push notifications) that increase the likelihood of user issues.

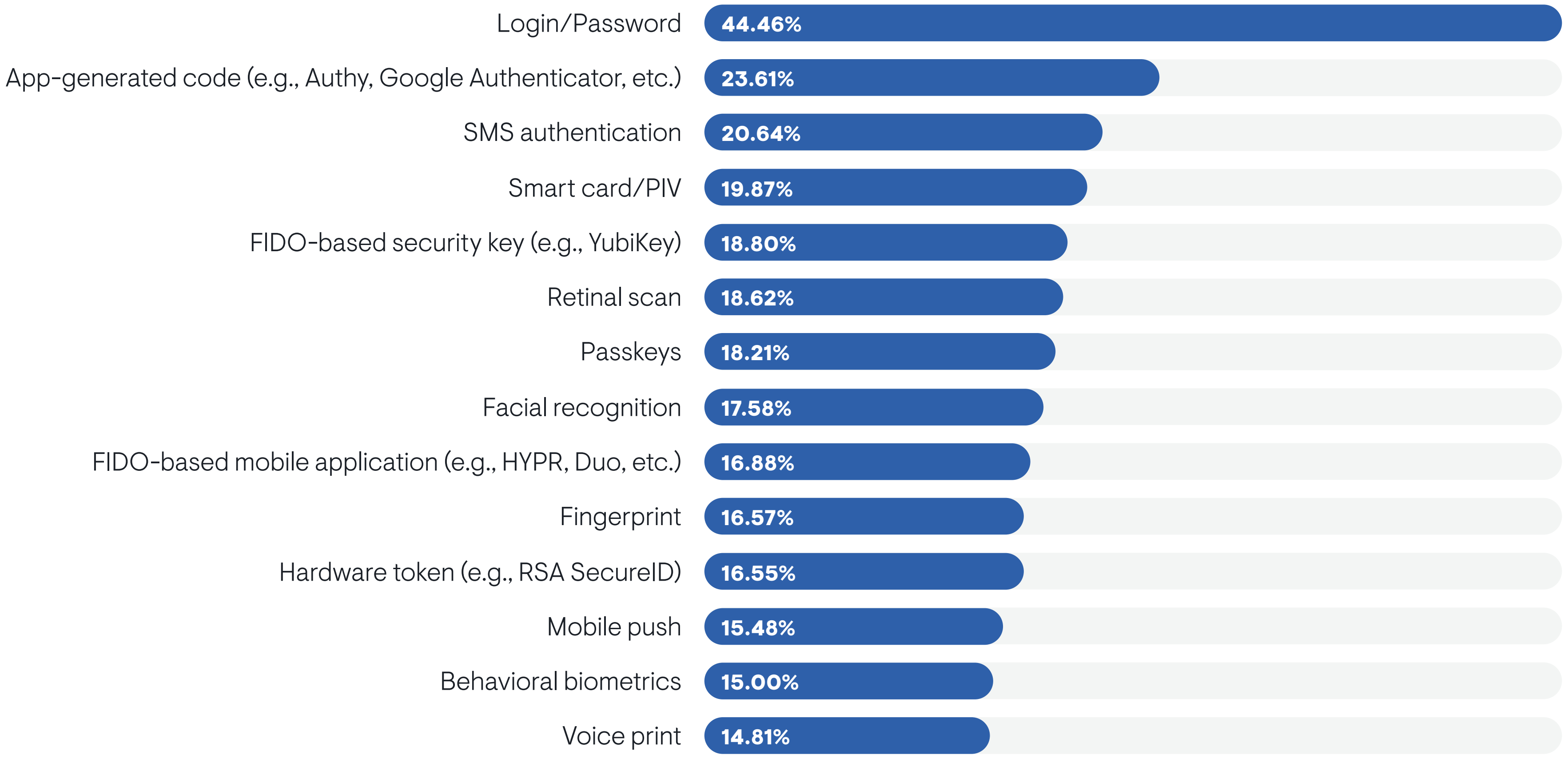
Figure 19: Average number of hours per week IT administrators spend managing access for every 100 employees, segmented by organization size



Authentication Management Efforts

Not surprisingly, the majority of administrator time spent on managing authentication is attributable to supporting passwords (Figure 20). Organizations supporting passwords spend nearly half of access management administration time supporting processes such as password resets, password policy enforcement, and investigations of password breach events. The management of app-generated codes (e.g., Authy, Google Authenticator, etc.), SMS authentication, and smart cards was also noted to be significantly time-consuming to administer, accounting for, on average, roughly one-fifth of access management administration time each, according to surveyed solution adopters.

Figure 20: Average percentage of total administrator time spent managing access, segmented by type of managed authenticators



Business Value of FIDO Standards

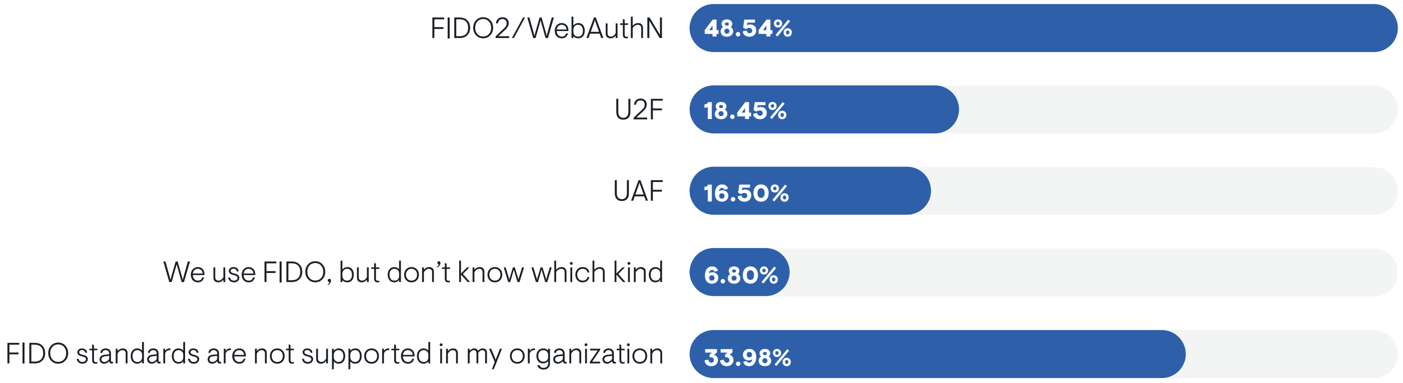
FIDO Adoption

Passwordless authentication was not a viable identity management option for broad business adoption until the release of Fast ID Online (FIDO) standards. In brief, FIDO standards provide a common language for passwordless authentication technologies to communicate with IT services. As long as both the authenticator and the services accessed conform to FIDO standards, businesses no longer need to develop costly and time-consuming points of investigation. Initial definitions released by the open industry consortium, the FIDO Alliance, focused on the enablement of passwordless technologies as a single authentication factor or MFA verifier and included the Universal Authentication Framework (UAF) and Universal 2nd Factor (U2F) standards. However, a giant leap forward was attained with the release of the FIDO2 standards, which incorporate a user-controlled cryptographic authenticator with W3C Web Authentication (WebAuthn) to enable built-in MFA without the need to rely on traditional passwords.

Among surveyed businesses, 66% support at least one type of FIDO standards (Figure 21). Legacy UAF and U2F standards were reported to collectively be in use by 29% of organizations. The adoption of FIDO2 standards, however, was indicated by nearly half of surveyed companies. FIDO2 adoption was more frequently noted by large businesses than small businesses, according to 57% and 40% of respondents in each demographic, respectively.

Thirty-seven percent of organizations that have not adopted FIDO standards reported they are currently planning or in the process of deploying FIDO solutions. Organizations with no plans to support FIDO most frequently cited concerns that adoption would be too expensive and/or difficult to implement and maintain as the primary reason. However, given that FIDO standards are designed to simplify the implementation of passwordless authentication, it can be presumed that these businesses have already invested in developing custom points of integration or are simply reluctant to support passwordless technologies.

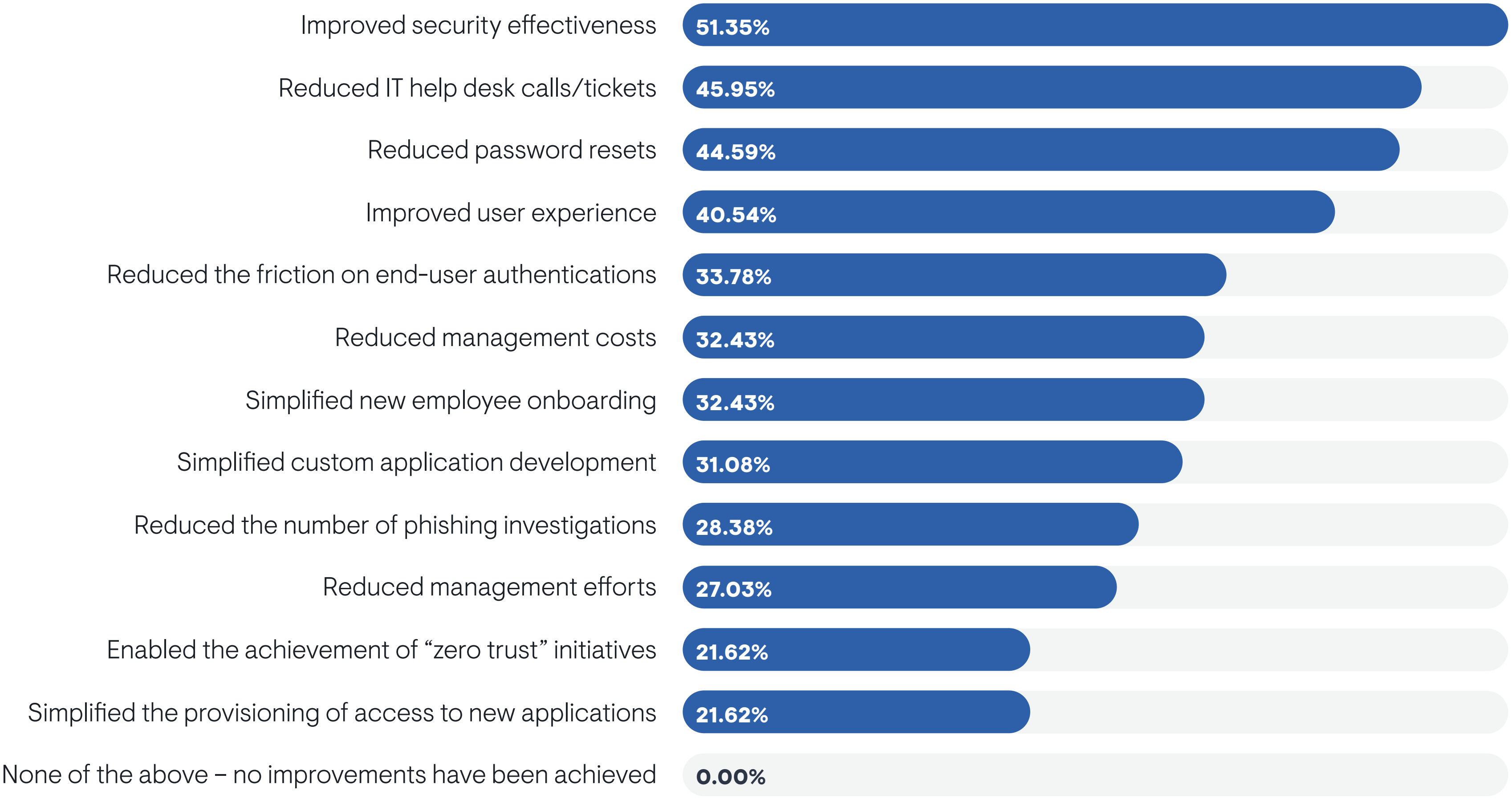
Figure 21: Percentage of surveyed businesses indicating FIDO standards that have been adopted to support workforce authentications



FIDO Benefits

All surveyed businesses that have adopted FIDO standards reported significant and quantifiable business improvements (Figure 22). Overall, the most frequently reported benefit was improvements to security effectiveness. This was particularly true for smaller organizations, according to 65% of respondents in that demographic. Large businesses most commonly cited reduced help desk tickets and password resets as FIDO adoption benefits. Eliminating the need for these mundane tasks frees up IT administrators to support more business-focused IT improvements. Improved user experiences were also reported by 41% of total respondents, recognizing the significant decreases in access friction enabled by the introduction of passwordless authentication solutions.

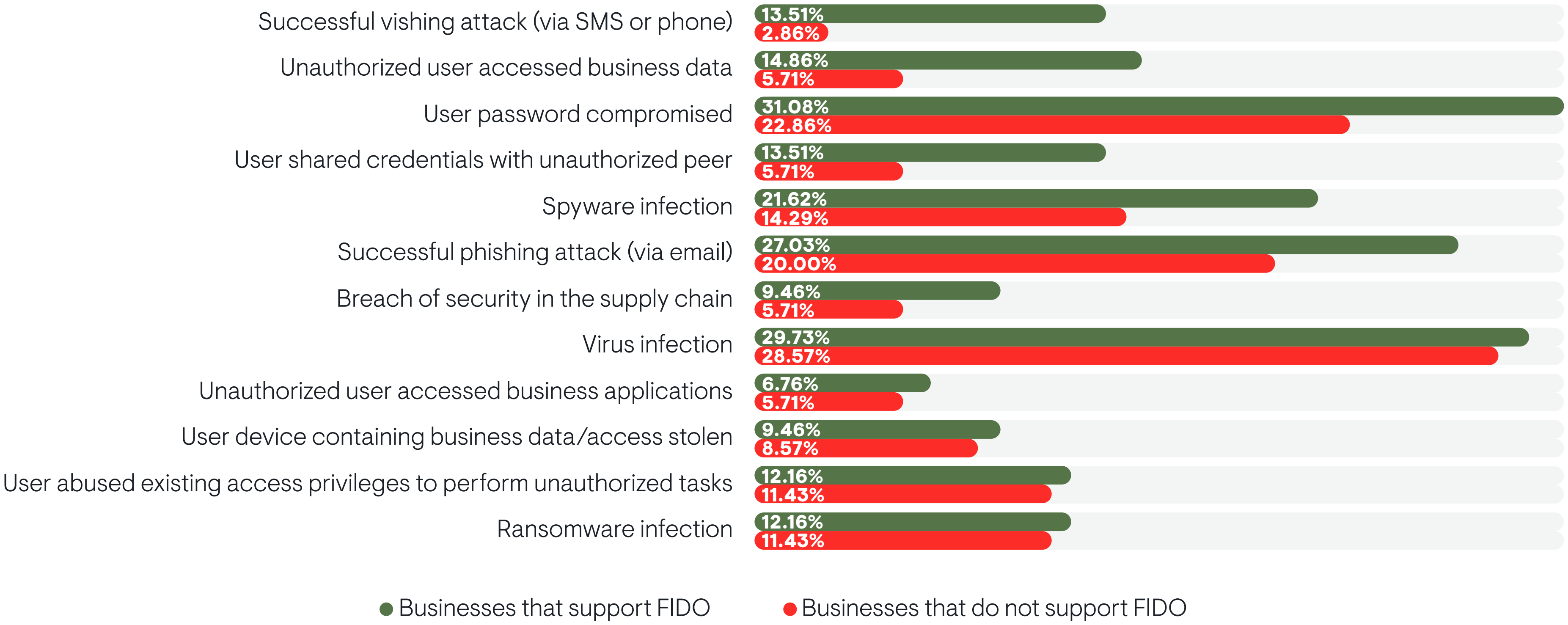
Figure 22: Percentage of surveyed businesses that support FIDO standards indicating quantifiable benefits that have been achieved since adoption



Overall, the most frequently reported benefit was improvements to security effectiveness. This was particularly true for smaller organizations, according to 65% of respondents in that demographic. This was not unexpected, since FIDO adopters were determined to be 42% less likely to have been breached in the preceding year than non-adopters and were indicated to inhibit the most significant threats (Figure 23). Most notably, FIDO adopters noted 79% fewer successful vishing and smishing attacks, which are social engineering strikes executed over phone calls or text messages. Similarly, successful phishing attacks were reduced by 26%. While malicious social engineers may easily scam users into revealing a login and password, it is much more difficult for them to convince users to directly authorize access using their passwordless credentials. "Phishing resistance" is particularly enabled when a FIDO2 authenticator encapsulates MFA and eliminates traditional passwords entirely.

Significant threat reductions were also indicated in incidents involving unauthorized access and compromised passwords, with 61% and 26% fewer successful attacks reported by FIDO adopters than non-adopters, respectively. While passwords themselves may be compromised if used as one factor in an MFA configuration, threat actors would still need to breach the FIDO-based passwordless verifier to gain access to business data. Of course, the chances of a successful breach are further reduced when traditional passwords are removed from access controls entirely. Further, the use of FIDO-based passwordless authentication makes it challenging for workers to share their credentials with peers because they would need to be physically involved during each authentication rather than just giving a coworker a password to use at his or her discretion. Incidents of credential sharing were noted to be 58% less likely among FIDO adopters.

Figure 23: Comparing the percentage of surveyed businesses that experienced a security breach in the last year between FIDO adopters and non-adopters

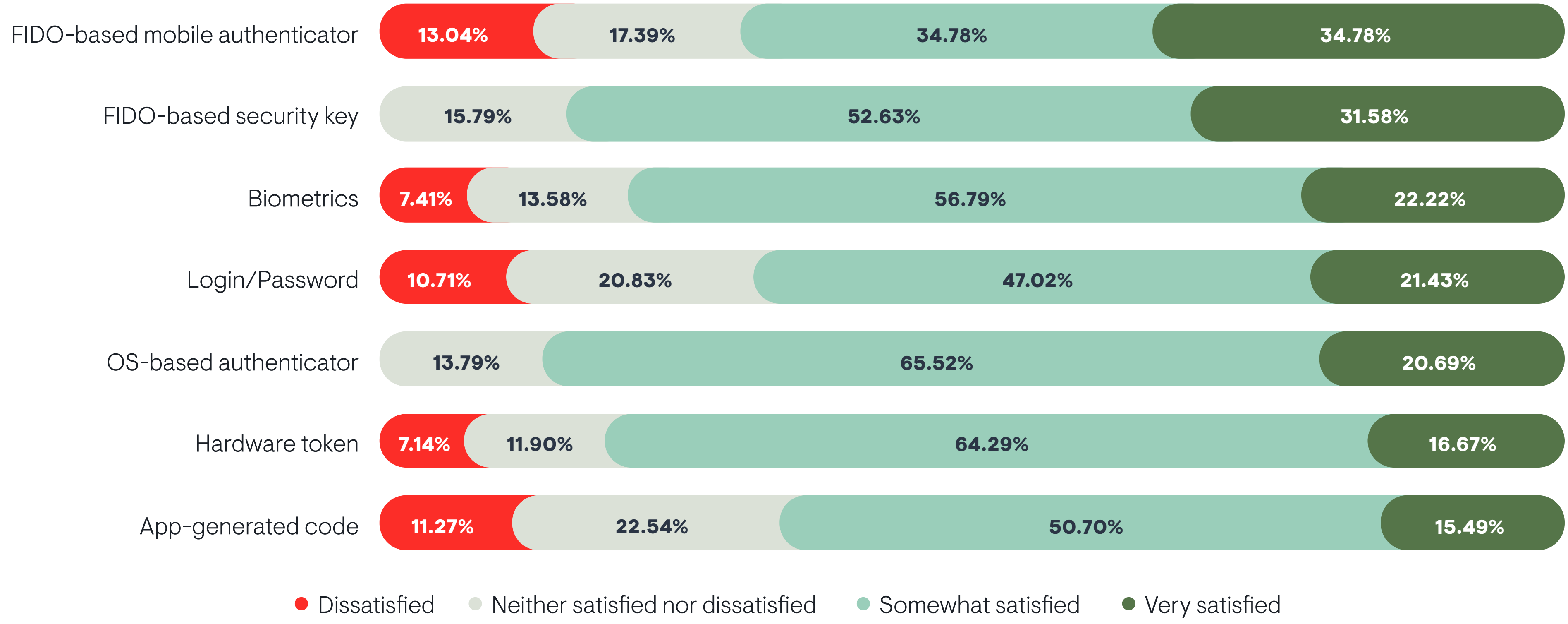


Outcomes and the Future of Authentication

Authenticator Satisfaction

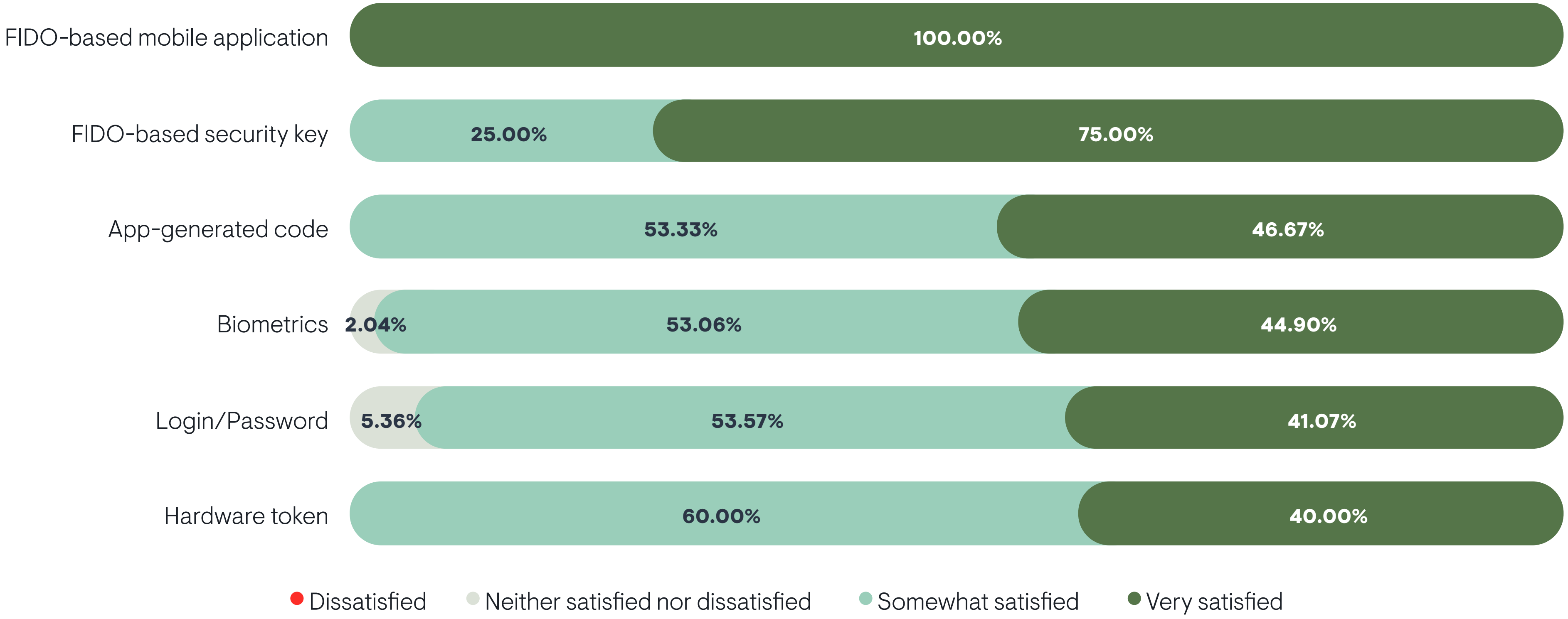
Overall, surveyed end users reported general satisfaction with the authenticators they currently use to access business IT resources, with 71% reporting they were somewhat or very satisfied. Business users employing FIDO-based mobile authenticators and security keys were most likely to indicate they were very satisfied with the solutions (Figure 24). Users of OS-based authenticators, such as Windows Hello and TouchID, were most likely to indicate they were at least "somewhat satisfied" with their adopted solution, while users of app-generated codes, such as Authy and Goole Authenticator, were least likely to indicate satisfaction.

Figure 24: Percentage of surveyed business users indicating the overall level of satisfaction they have with the authenticators they actively use to access business IT services



By comparison, surveyed business IT managers indicated much higher satisfaction rates with their adopted authenticators (Figure 25). While end users tend to focus on the usability of the authenticators they use, IT managers place higher value on the manageability and security effectiveness of adopted solutions. Overall, businesses that adopted FIDO-based mobile authenticators showed the highest satisfaction, with 100% of IT managers reporting they were very satisfied with the technology. FIDO-based security keys also garnered high satisfaction rates, according to three-quarters of survey business adopters. It is also notable that 56% of surveyed businesses that have adopted FIDO standards reported they were very satisfied with their authentication processes compared to only 23% of non-FIDO adopters.

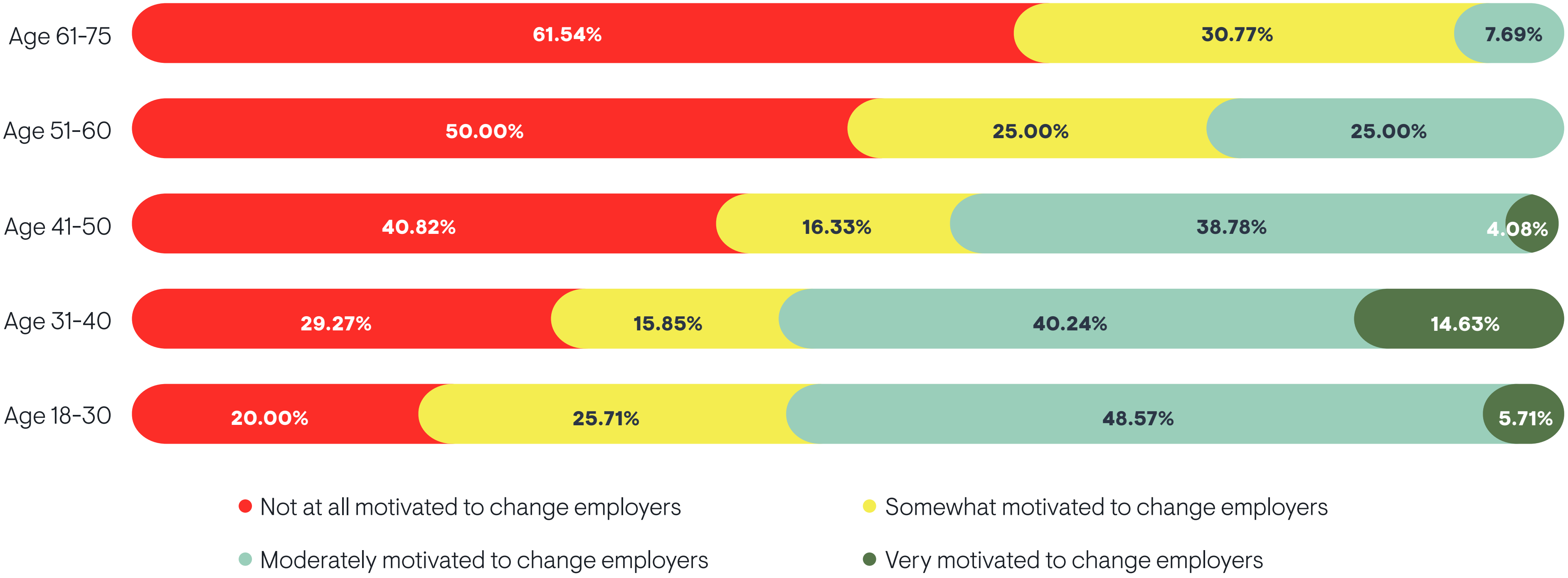
Figure 25: Percentage of surveyed businesses indicating overall satisfaction with authenticators used by more than 25% of employees in their organization



Attracting and Retaining Talent

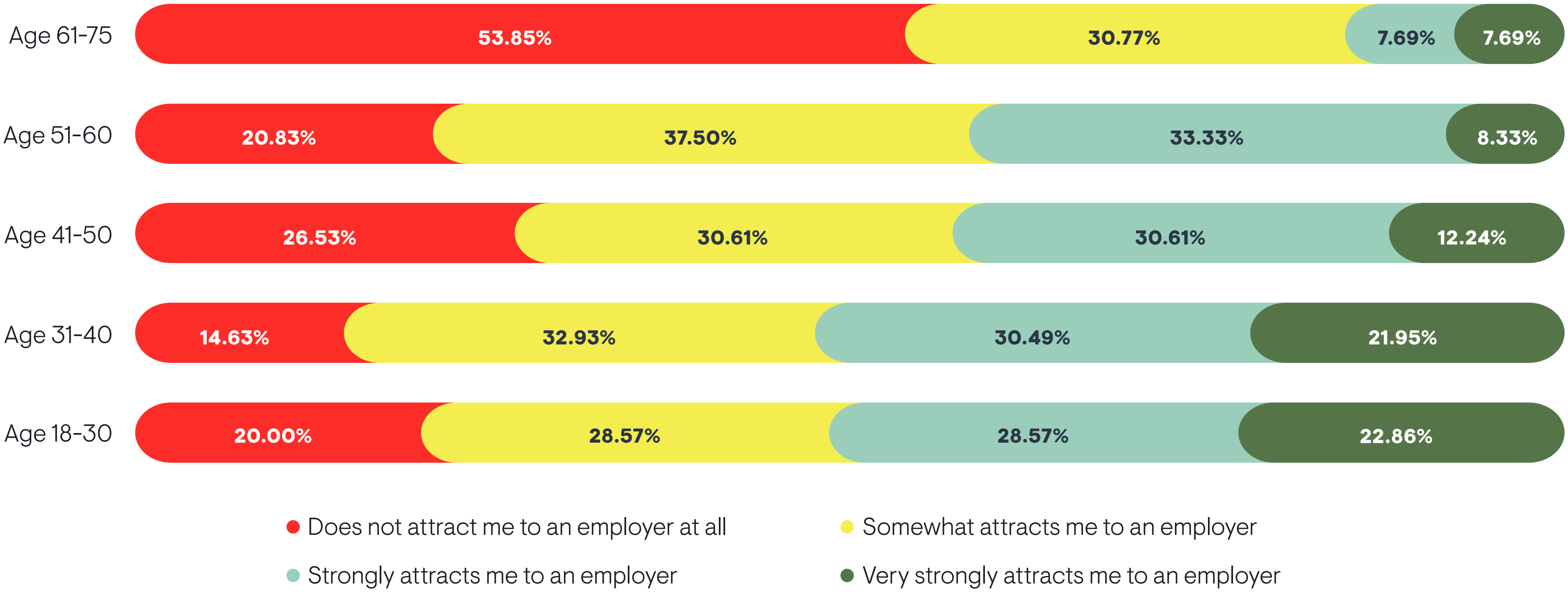
Today's workers are very sensitive to the types of technologies they use to perform job tasks. The solutions adopted for identity management provide a very visible indication of the investment employers are willing to make into keeping their workers productive and satisfied, and a majority of business professionals now make employment decisions based in part on their access experiences. Among surveyed business users, 65% indicated they would be motivated to change employers if presented with high-friction authentication processes. The level of impact authentication solutions have on employment decisions was noted to directly correlate to the responder's age (Figure 26). More than half of surveyed Millennials under the age of 40 reported they would be moderately to very motivated to seek new employment if they were frustrated with access security solutions.

Figure 26: Percentage of survey respondents indicating their level of motivation to change employers if presented with high-friction authentication, segmented by respondent age



Finding knowledgeable and experienced business professionals is challenging in today's very competitive job markets, and the types of supported technologies also play a role in attracting new talent. Potential employees want to know they would be free to focus on their job performance without being inhibited by antiquated and challenging access processes. In total, 78% of surveyed users reported they would be more attracted to a new employment opportunity if they offered easy-to-use authentication solutions. Again, age is a factor in the level of importance identity security plays in employment decisions. Millennials were significantly more likely to indicate they would be "strongly" or "very strongly" attracted to employers supporting low-friction authentication solutions (Figure 27). Of course, this is not to suggest that this will be the only consideration in their decision-making process, but it is undeniable that business internal technology solutions are now as much a part of attracting and retaining employees as salaries and benefits. Indeed, these results were predicted by Modern Management Theory, which postulates that employee retention and motivation is driven more by their job satisfaction than fiscal compensation.

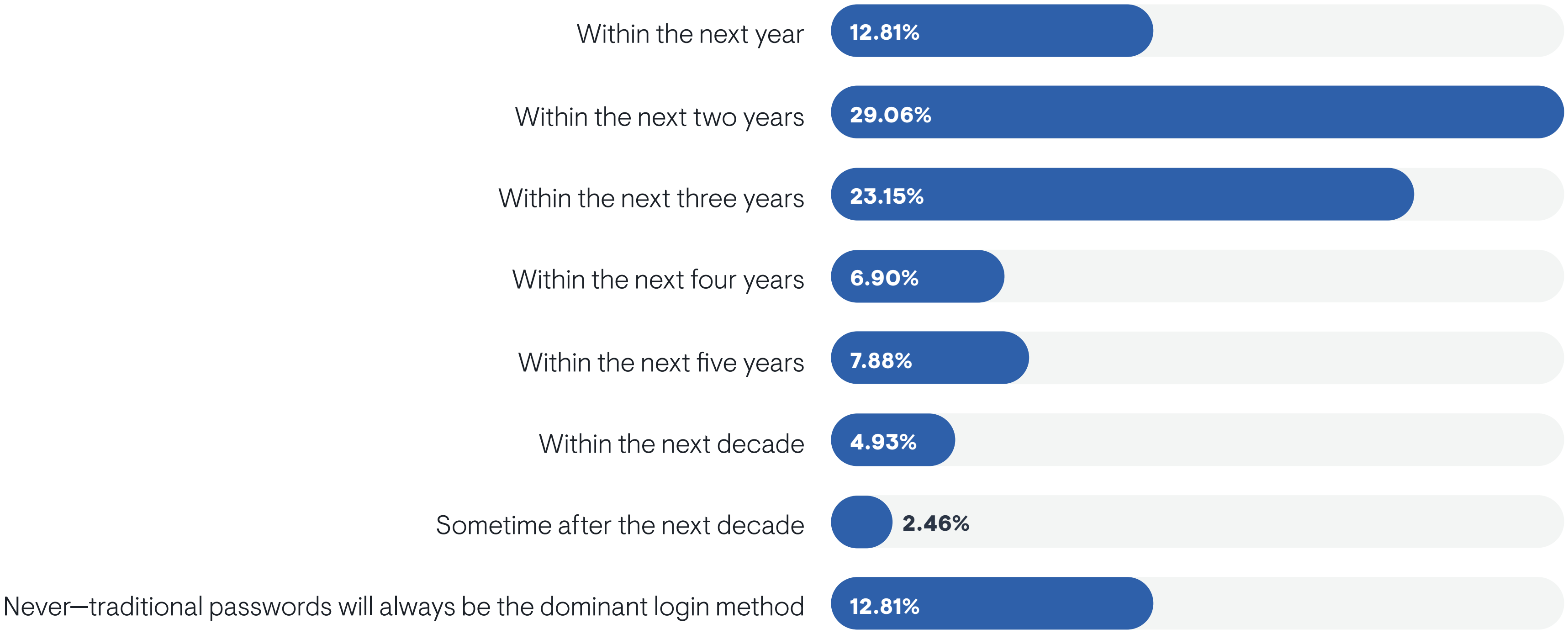
Figure 27: Percentage of surveyed business employees indicating how attractive the availability of low-friction authentication would have in selecting a future employer



Perceptions on the Future of Authentication

Less than a decade ago, the idea of completely eliminating business IT security dependencies on passwords was virtually unthinkable outside of science fiction media. Since then, however, technological advances in the development of passwordless authenticators, the ubiquitous adoption of mobile devices, and the introduction of FIDO standards have set the stage for usurping the dominance of high-friction and unsecure password-based access controls. In fact, 87% of surveyed end users indicated the replacement of passwords with passwordless authenticators is inevitable, reporting, on average, that passwords will no longer be dominant in their company within the next three years (Figure 28). Younger respondents, under the age of 30, were most optimistic, predicting passwordless solutions will replace passwords within the next 2.6 years on average. While responders over the age of 60 were slightly more skeptical, they nonetheless prophesied the fading of passwords within the next 3.6 years, on average—which is still a rather short period considering how long passwords have dominated identity security practices.

Figure 28: When do you think passwordless authentication solutions will replace the majority of traditional passwords in your organization?



Conclusions

The greatest inherent danger of relying on passwords is their dependence on fallible human memories. For decades, security managers pointed fingers at users' poor password hygiene practices as the greatest threat to enterprise security. As a result, more than half of all breach events are blamed on employees, resulting in reprimands and termination rather than directing the blame at the insecure access security practices. This mentality undermines the precept that IT should exist to serve the users, rather than the other way around. Line of business employees, after all, were hired to perform specific job functions, not prioritize the enforcement of IT security. While 68% of surveyed business users admitted to violating password policies, it should be remembered that if a worker has to bypass high-friction security in order to perform business tasks efficiently and effectively, they are actually doing what they are being paid to do. The failure in that scenario is the continued use of IT security practices that inhibit workforce productivity, not the workers themselves.

Security threats continue to evolve and increase, and password-based security solutions are unable to keep up. Layering on 2FA solutions, such as OTPs and push notifications, has not significantly reduced the number of breach events. Malicious actors simply adapted by changing tactics, since the core of the problem—easily compromised passwords—continues to persist. The future of security casts an even bleaker picture. The advent of quantum computing will place in the hands of nation states the ability to breach any encrypted password in seconds. Additionally, the rise of generative AI will enable attackers to emulate targeted user characteristics. The foundation for addressing the challenges must be established now, and it begins with a rejection of traditional password-based authentication.

Future-proofing identity security begins with the broad adoption of FIDO standards, particularly with the native MFA features inherent in FIDO2 authenticators. EMA's research bears this out, since FIDO adopters were determined to be 42% less likely to have experienced a breach event in the last year, with significant reductions quantified across the most insidious attack vectors. What's more, FIDO protocols greatly simplify the adoption of passwordless authenticators that work with end-user practices rather than distracting away from them. FIDO-based passwordless authenticators drive improved workforce productivity and job satisfaction which, in turn, translate into greater employee retention rates.

For decades, identity management professionals have professed that the brass ring of IT security is to bridge the gap between security effectiveness and user experience. Those technologies now exist, and the shelf life of traditional passwords is coming to a close as businesses collectively embrace the next generation of authentication.

GLOBAL
174/02455
0.29
0.38
0.24
10
25
F-2
RPI
<uL><a
<sys><b
<exit> = 0xFF & (val_>>>0x00)
<sys><[illegible]rgb ['r'] = 0xFF & (to aktivirovat Central z
<gravity> $Hex2rgb = 0xFF «there is a probability
214/01
Silver
Gold
Ruby
4256.04
1552.04
3245.04
MMB5
PTC
A11
244,00
214,00
26,653
5000
10000

Appendix A: End-User Survey Demographics

Figure 29: Percentage of survey respondent indicating the department or functional area in which they work

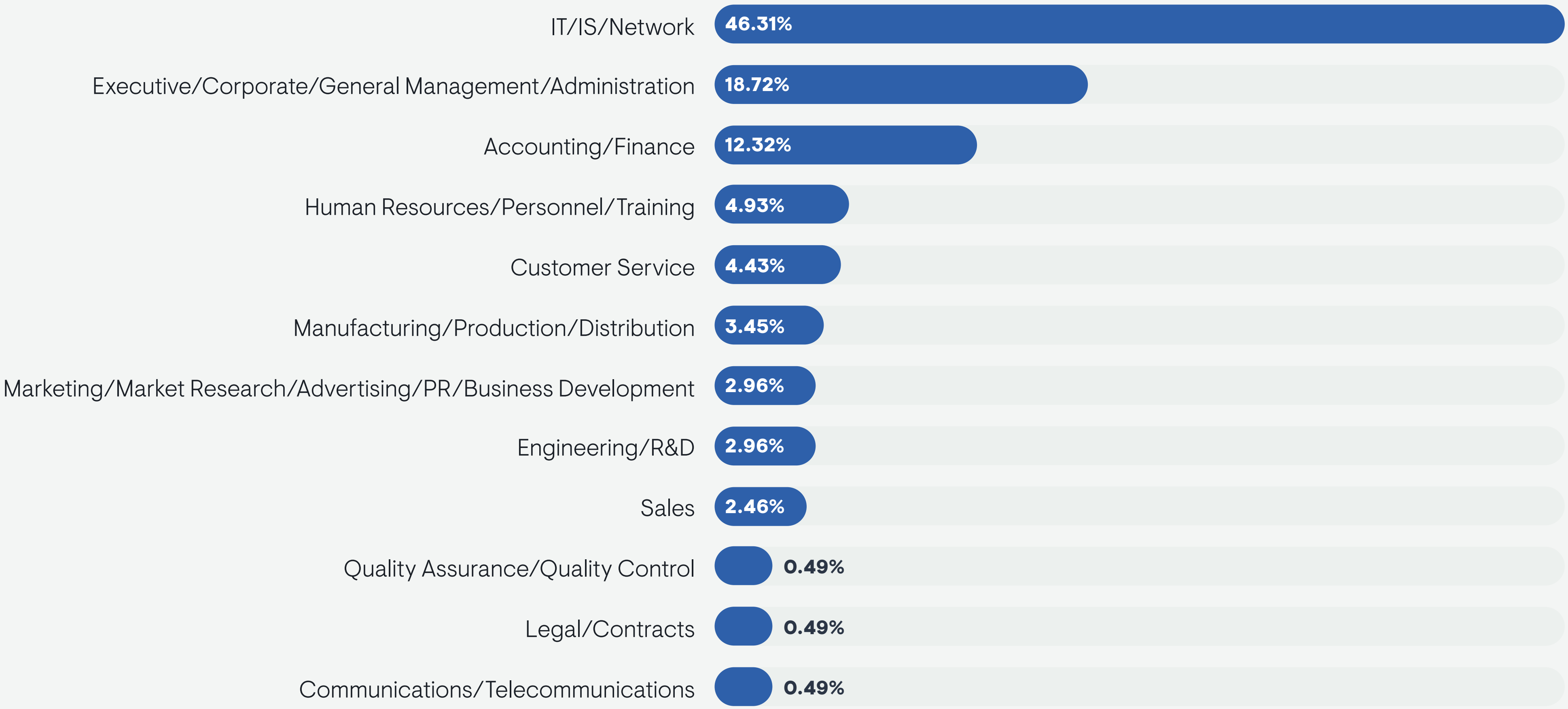


Figure 30: Percentage of survey respondents from an IT-related department indicating their specific job role

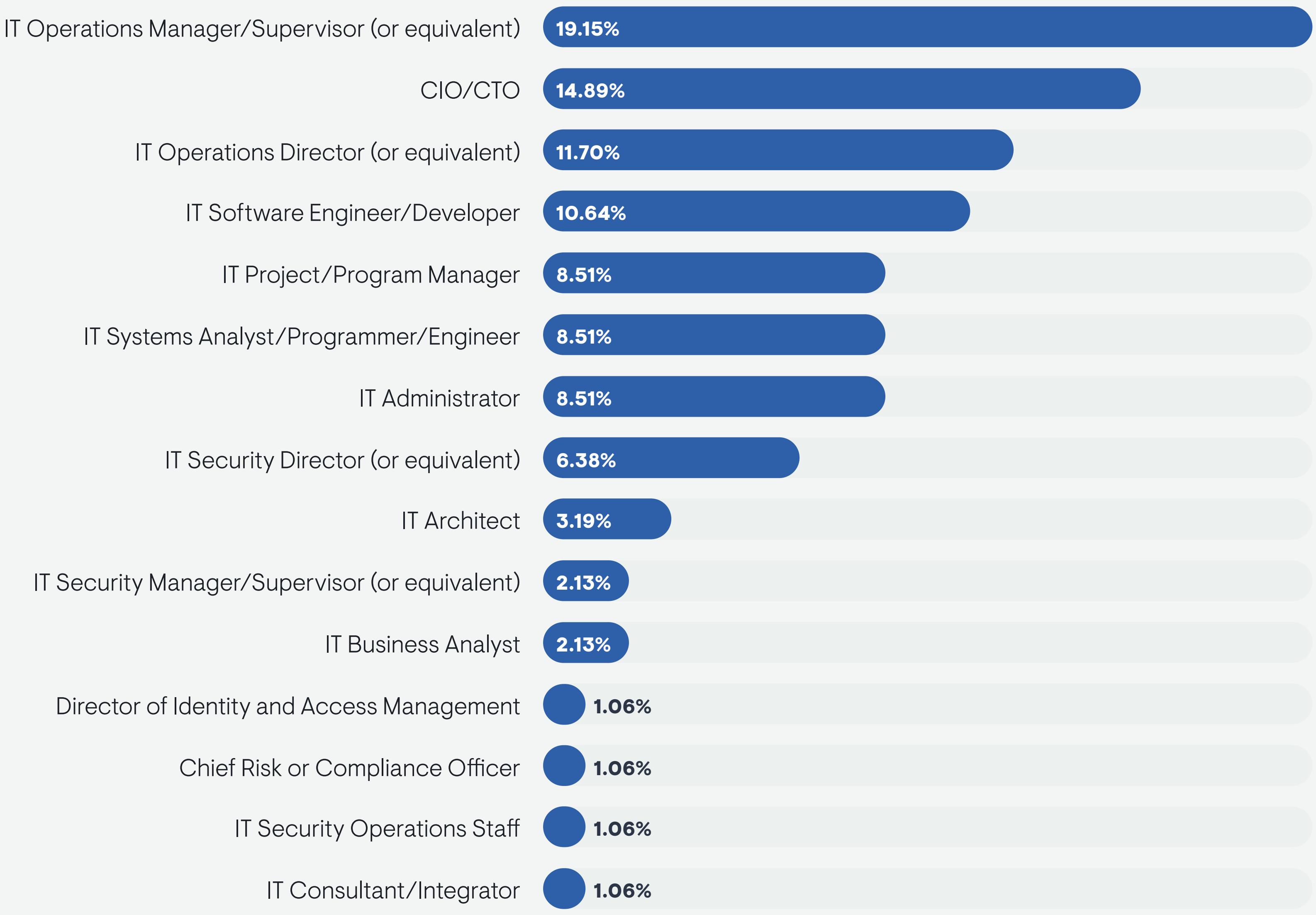


Figure 31: Percentage of survey respondents from a non-IT-related department indicating their specific job role

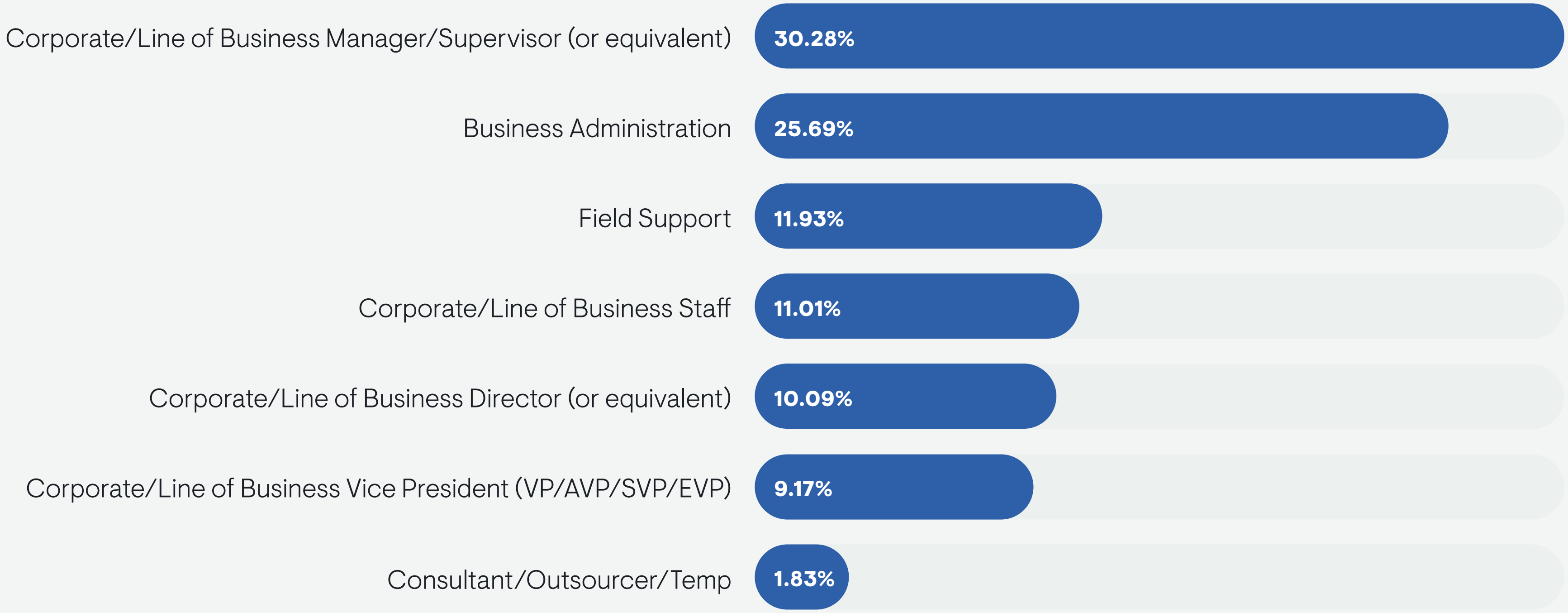


Figure 32: Percentage of survey respondents indicating the number of employees in their organization worldwide

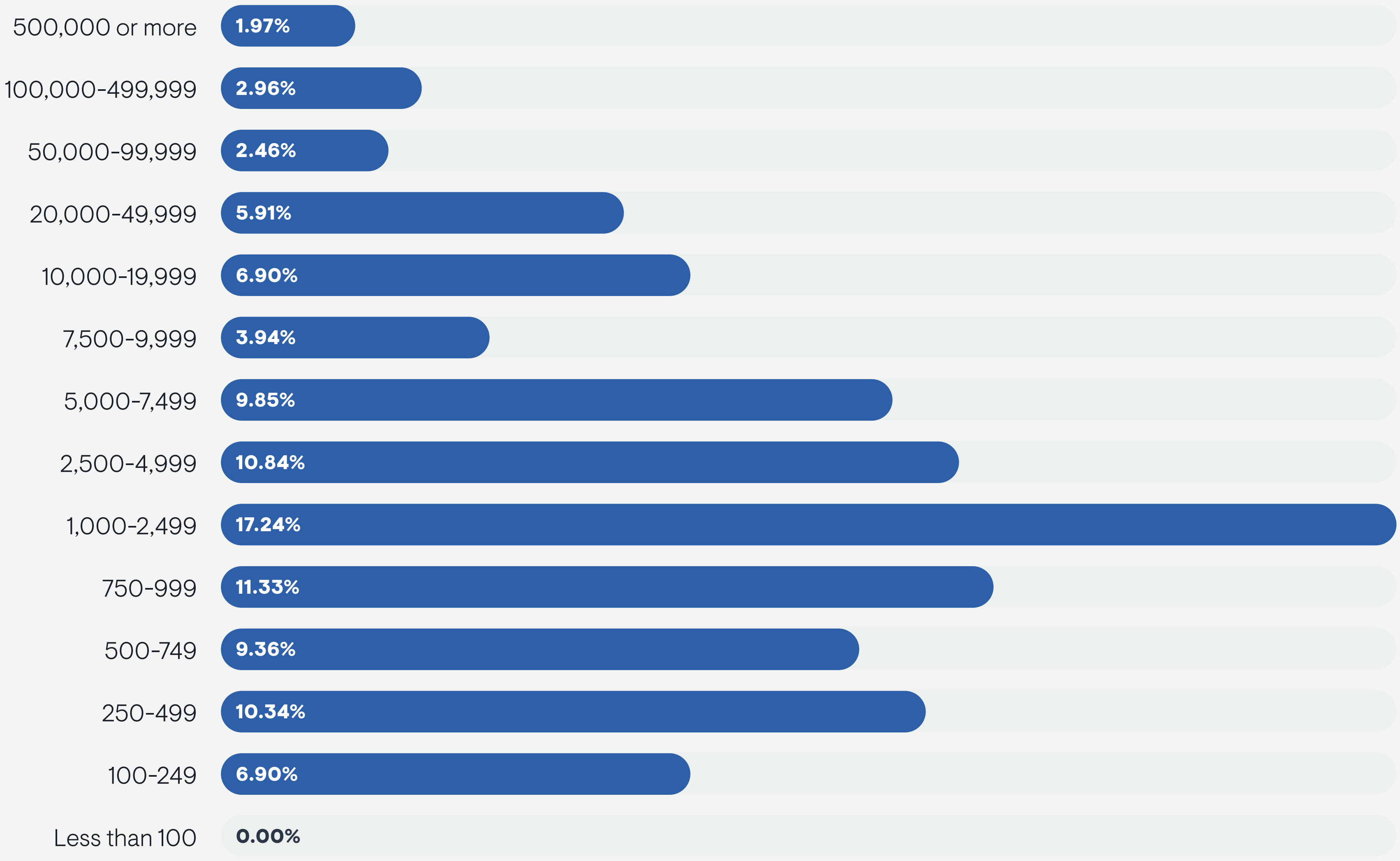


Figure 33: Percentage of survey respondents indicating their company's primary industry

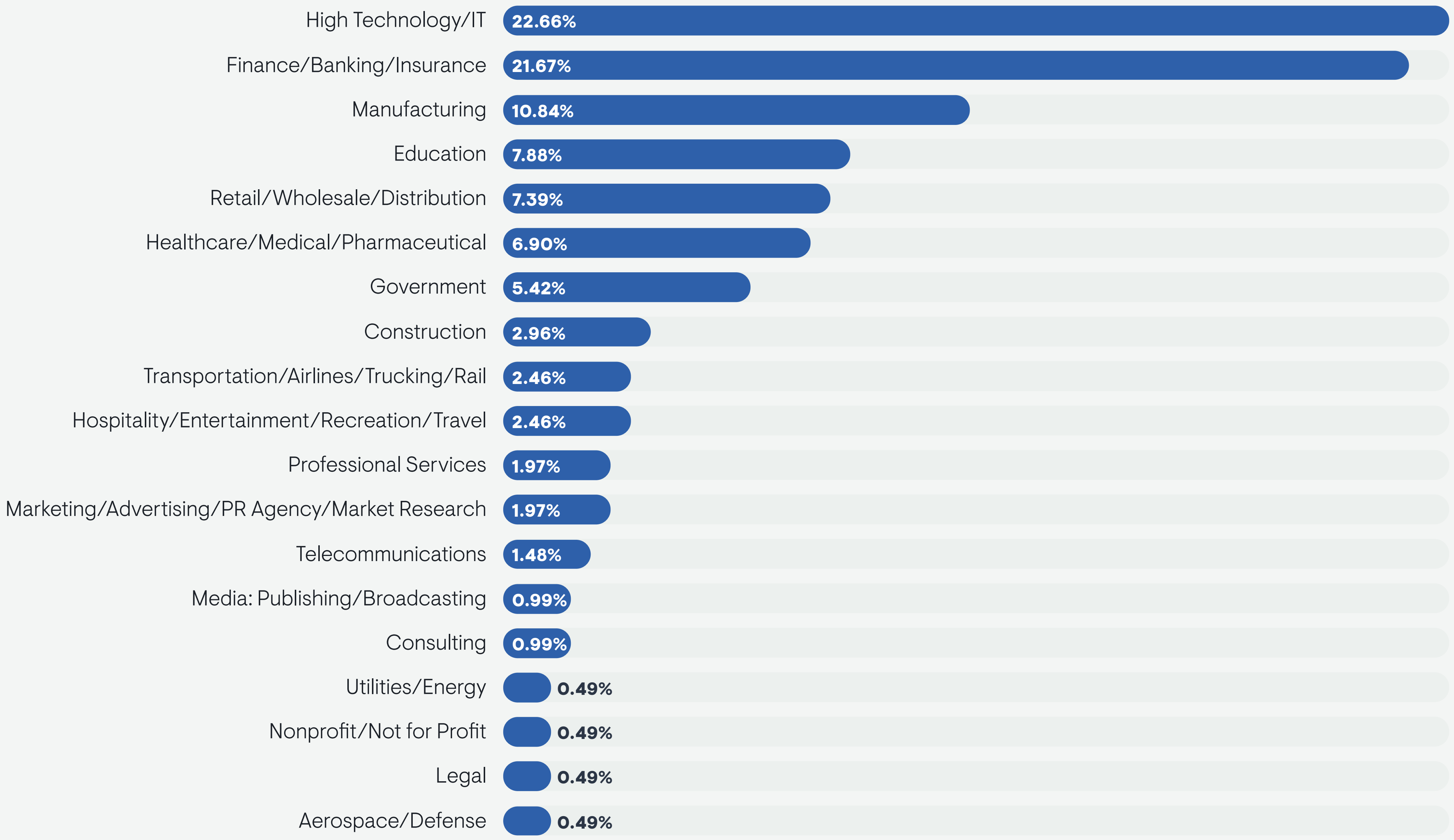


Figure 34: Percentage of survey respondents indicating the region in which they are located

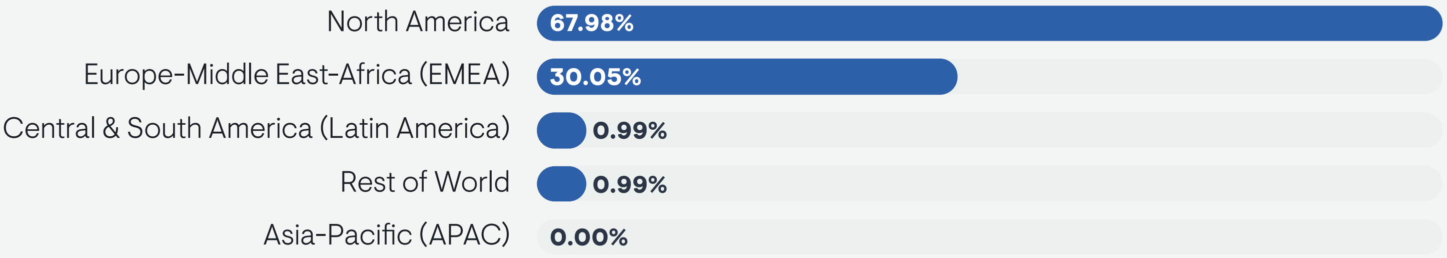
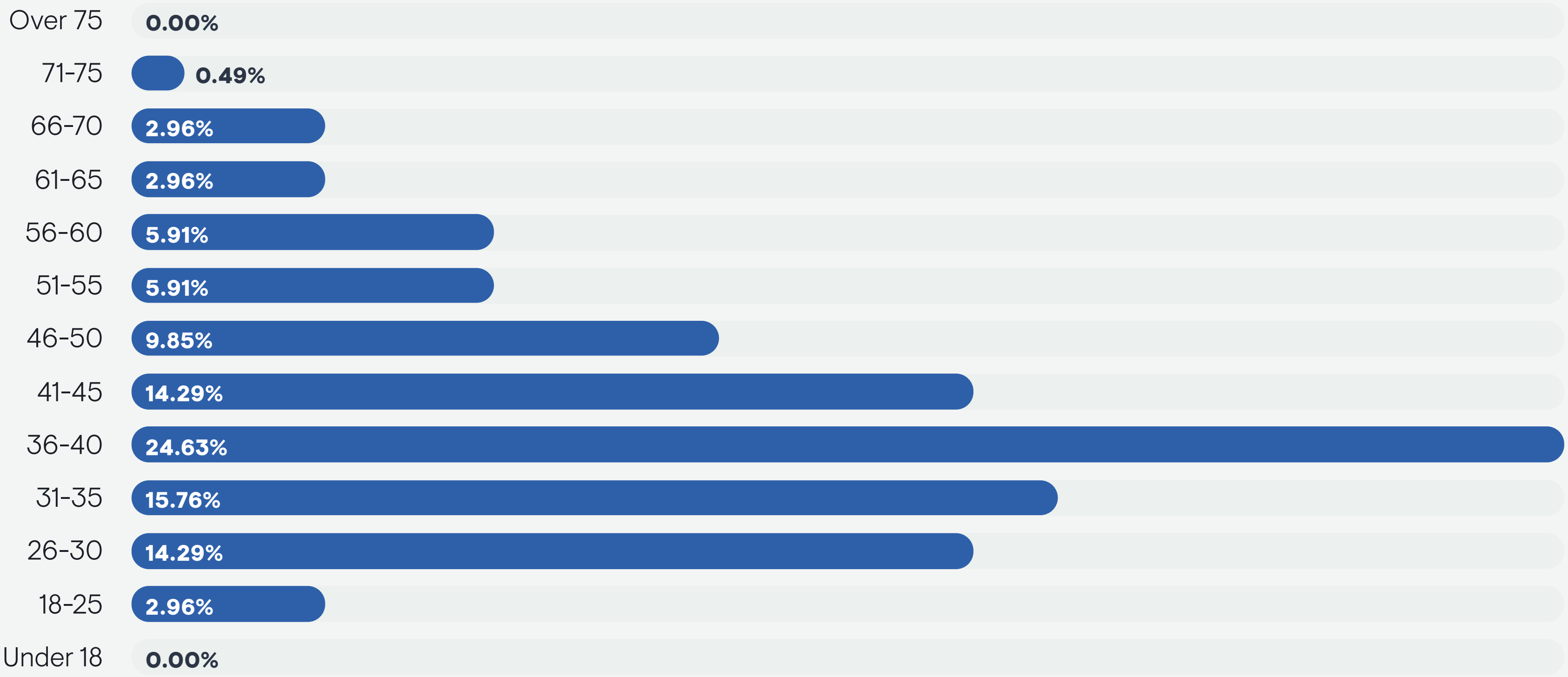


Figure 35: Percentage of survey respondents indicating their current age



Appendix B: Business Survey Demographics

Figure 36: Percentage of survey respondent indicating their specific role in IT management

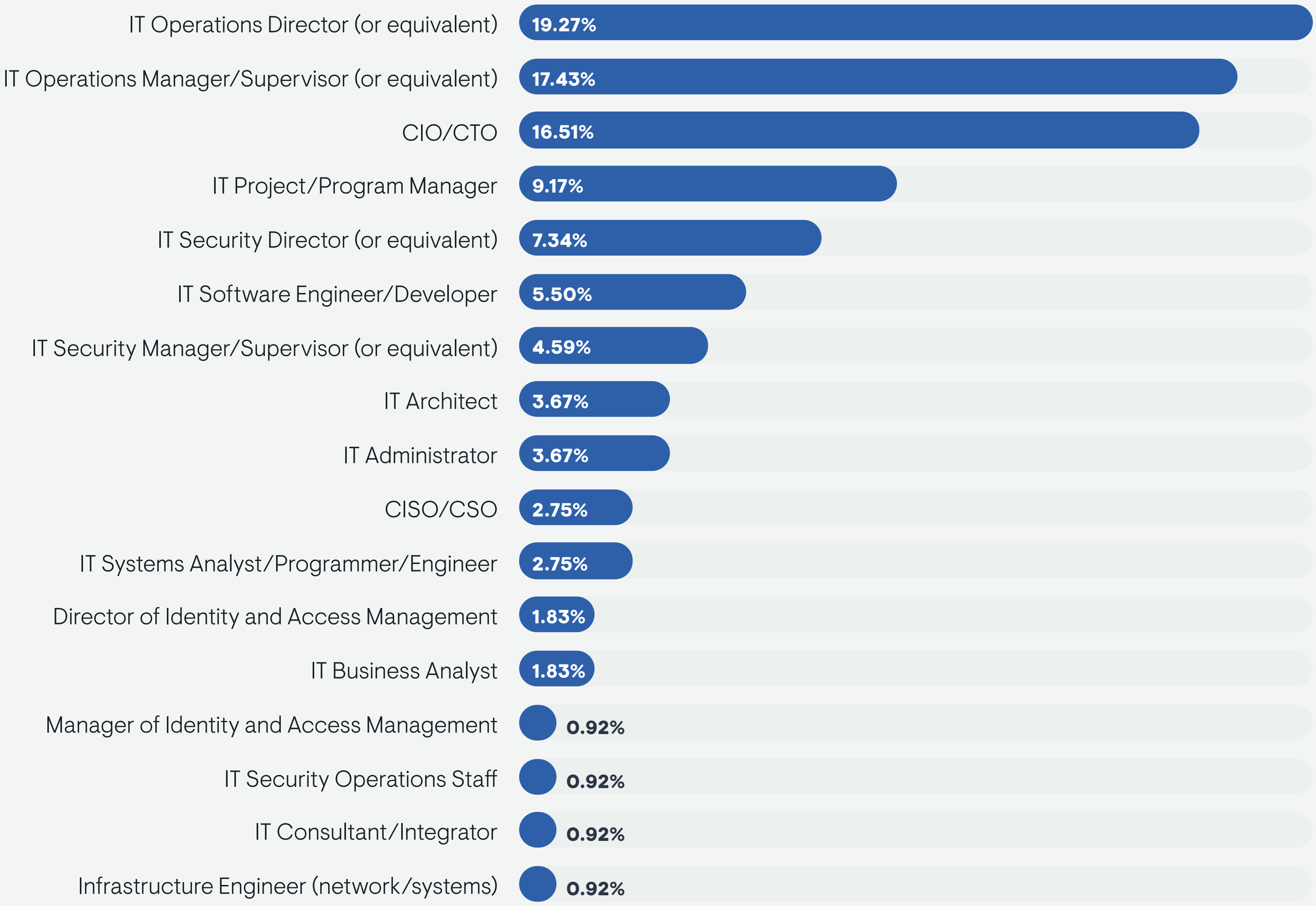


Figure 37: Percentage of survey respondents indicating the number of employees in their organization worldwide

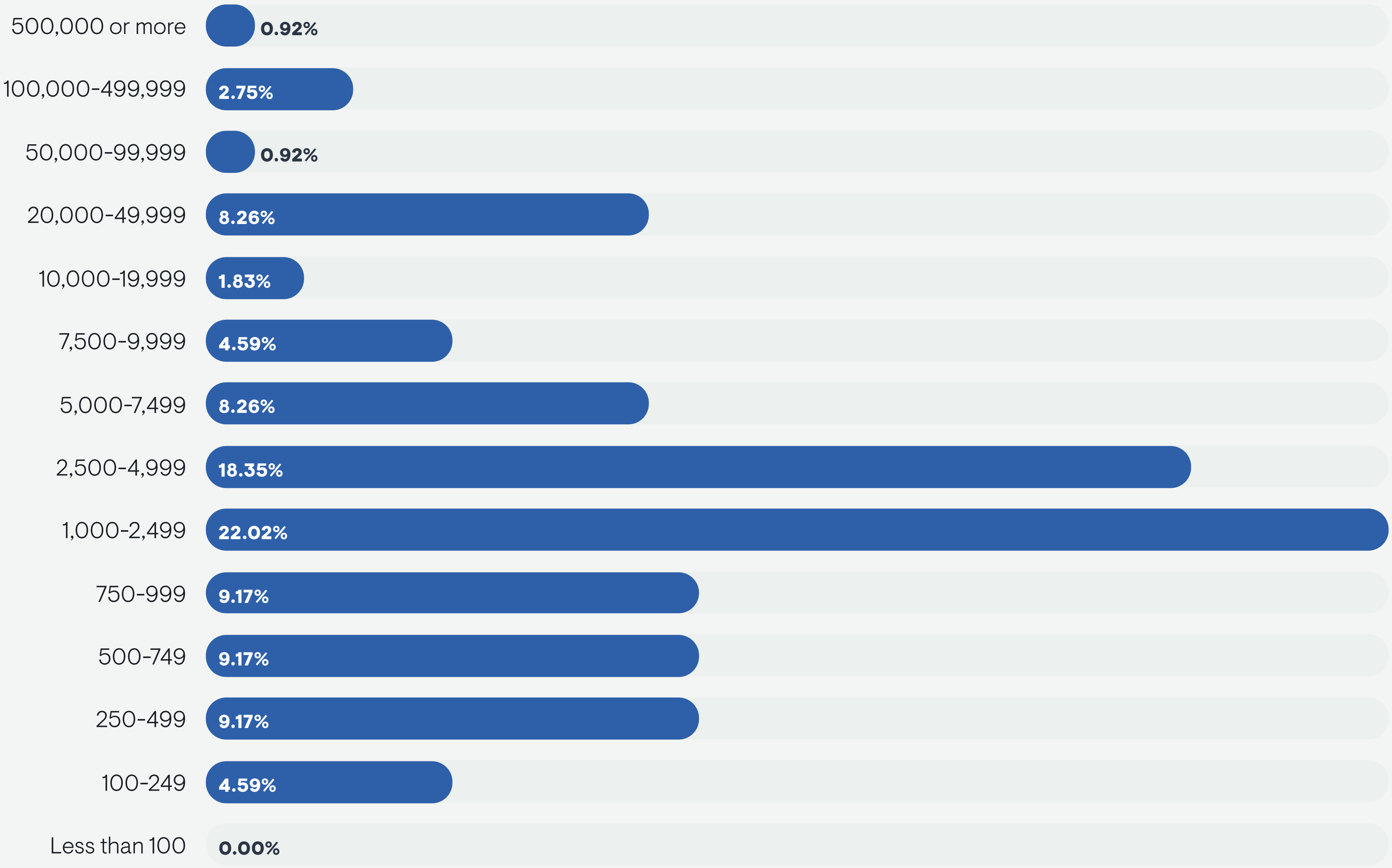


Figure 38: Percentage of survey respondents indicating their company's primary industry

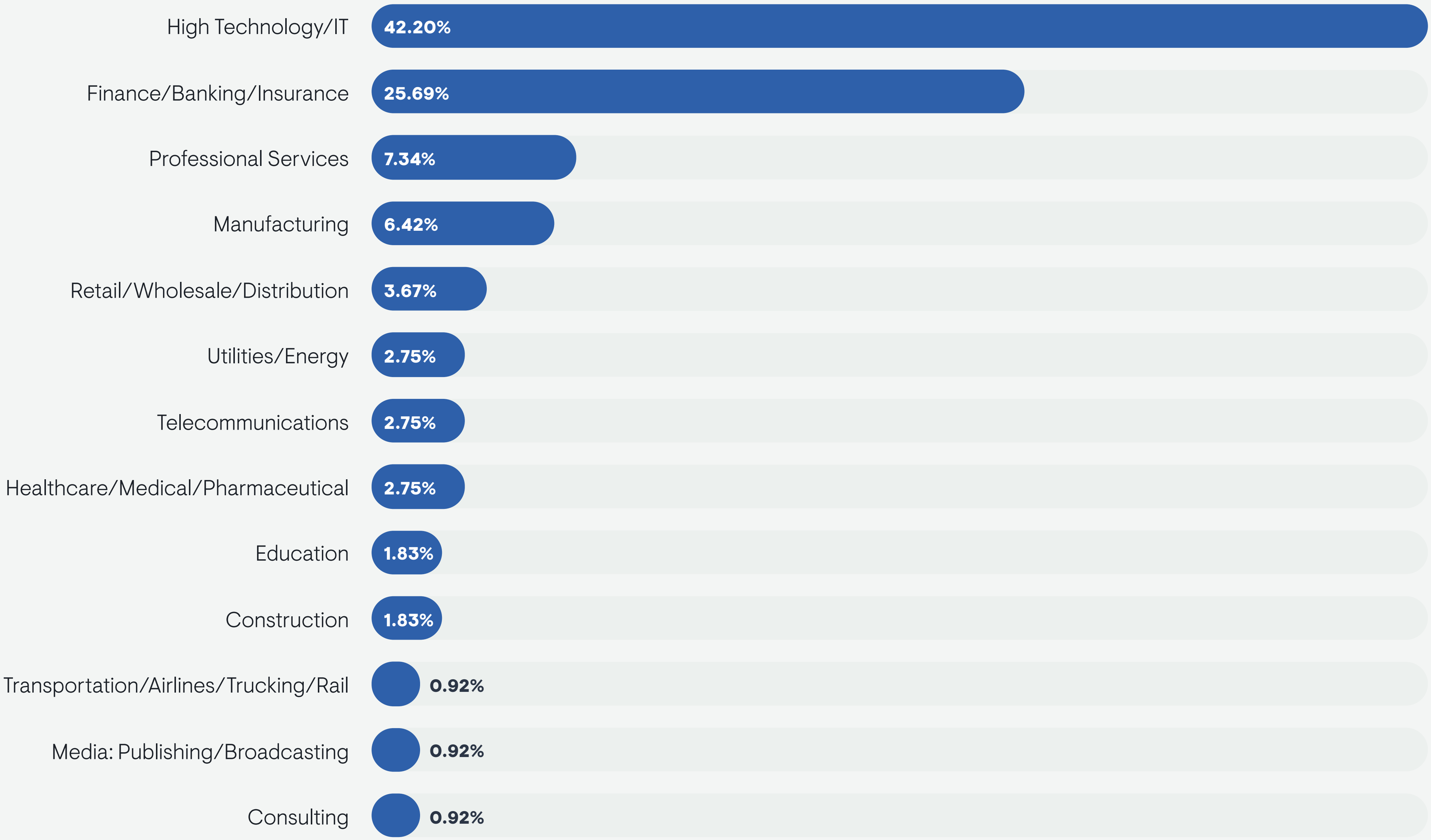
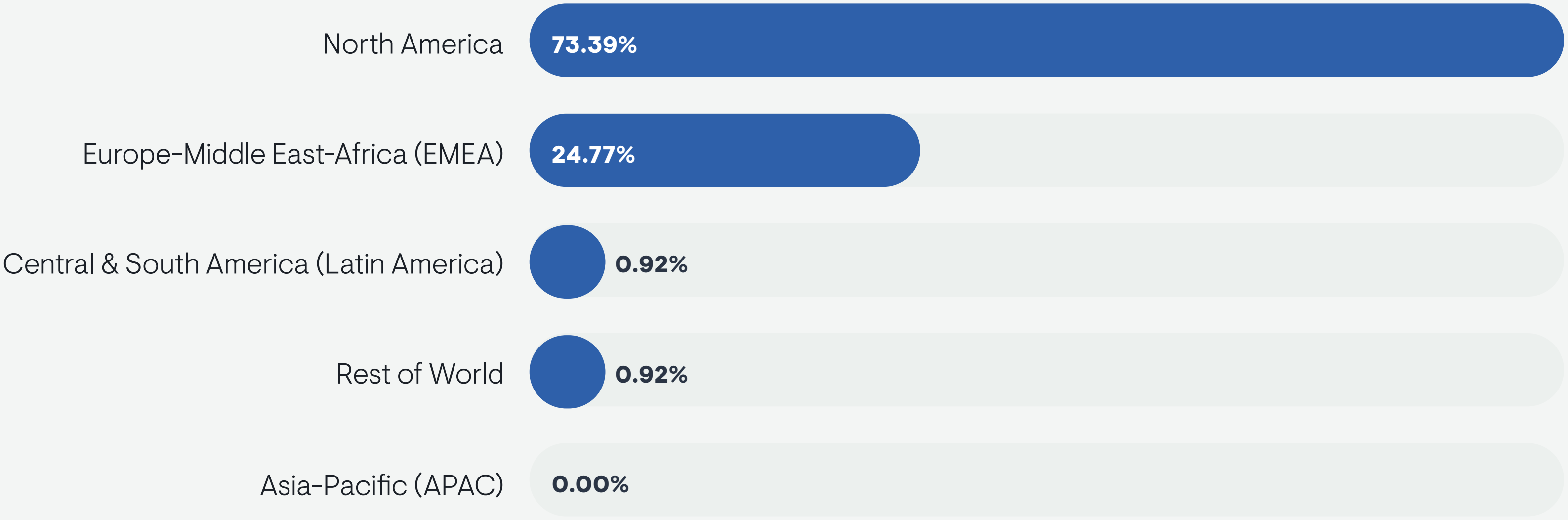


Figure 39: Percentage of survey respondents indicating the region in which they are located



About Enterprise Management Associates, Inc.

Founded in 1996, Enterprise Management Associates (EMA) is a leading IT analyst research firm that specializes in going "beyond the surface" to provide deep insight across the full spectrum of IT 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 its clients achieve their goals. Learn more about EMA research, analysis, and consulting services at **www.enterprisemanagement.com** or follow EMA on **X** or **LinkedIn**.

2770 Arapahoe Road, Ste 132 - 544, Lafayette, CO 80026 +1 303.543.9500 www.enterprisemanagement.com 4359.111423