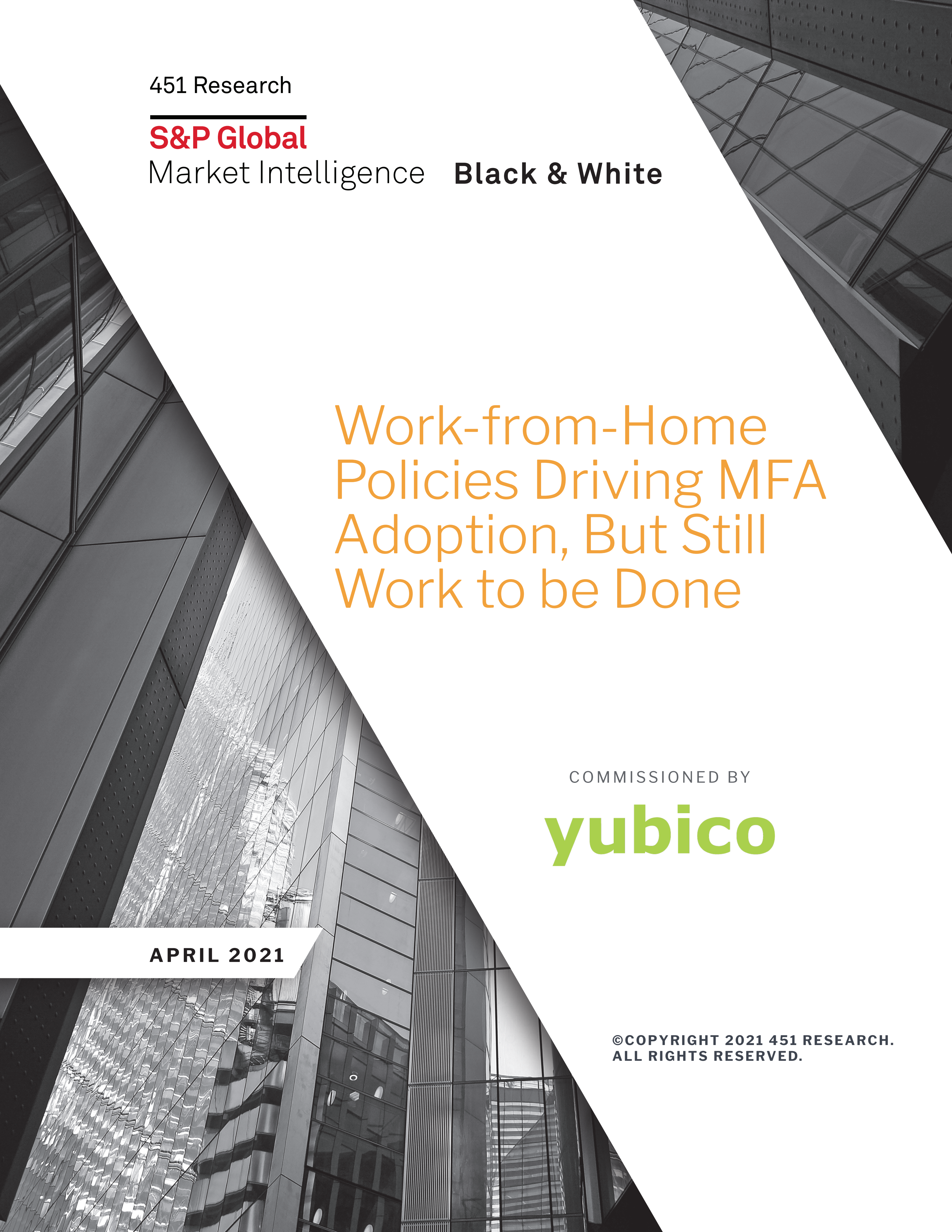


451 Research

S&P Global
Market Intelligence

Black & White

Work-from-Home Policies Driving MFA Adoption, But Still Work to be Done

COMMISSIONED BY

yubico

APRIL 2021

About this paper

A Black & White paper is a study based on primary research survey data that assesses the market dynamics of a key enterprise technology segment through the lens of the “on the ground” experience and opinions of real practitioners — what they are doing, and why they are doing it.

ABOUT THE AUTHOR

GARRETT BEKKER

SENIOR RESEARCH ANALYST, SECURITY

Garrett Bekker is a Senior Research Analyst in the Information Security Channel at 451 Research, a part of S&P Global Market Intelligence. He has viewed enterprise security from a variety of perspectives over the past 20 years.

MATTHEW UTTER

SENIOR RESEARCH ASSOCIATE

Matthew Utter is a Senior Research Associate at 451 Research, a part of S&P Global Market Intelligence. As a Research Associate, Matthew has written on topics covering Information Security; Data, AI & Analytics; and Workforce Productivity & Collaboration. He also shares an interest in cloud native and quantum technologies.

Introduction

When it comes to authentication, IT has historically relied heavily on 'shared secrets.' Although no technology is perfect, practices such as usernames and passwords, which are ubiquitous within the enterprise, have well-known and well-documented flaws. For starters, passwords are usually saved in a centralized repository, which can be a prime target for attackers. In addition, passwords typically are hard to remember, a nuisance to type on a mobile device and easily defeated by determined attackers.

Passwords were initially intended for use within small, internal networks in governments and universities, where all members of the network were known, so there was an inherent level of trust within the network. However, passwords began to be used in areas outside of their original intention, exposing users and enterprises to a variety of attacks. As a result, enterprises have begun to realize – albeit slowly – that shared secrets are the root of many current security problems and are starting to supplement or replace passwords with stronger two-factor (2FA) or multi-factor authentication (MFA) methods. *(Note: although 2FA and MFA are technically different, the difference is subtle – 'two factors and only two factors' (2FA) vs. 'two or more factors' (MFA), so for brevity, we used the acronym MFA throughout the remainder of this report.)*

Multi-factor authentication can take many forms, from one-time password (OTP) tokens or authenticators that work on a user's mobile device to biometrics that leverage physical characteristics such as fingerprints, voiceprints and facial features. Additional MFA form factors include mobile push-based MFA, SMS-based authentication, hardware-based OTP, and modern hardware-based USB security keys. All of these technologies aim to boost the security of more traditional forms of authentication, particularly passwords, and some also promise ease-of-use benefits, but all MFA form factors are not created equal.

While some (mainly larger) organizations have begun to adopt stronger methods of authentication, MFA overall has lower enterprise adoption levels than firewalls, endpoint security and other common security tools. Nevertheless, enterprise usage of MFA is gaining momentum due to a confluence of several factors: the growing recognition that stolen credentials are at the root of most security breaches; the rise of work-from-home policies due to the COVID-19 pandemic; and the adoption of new authentication standards such as Fast Identity Online (FIDO) U2F, FIDO2 and WebAuthn that underpin new advances in second-factor and passwordless authentication.

This report presents key findings and takeaways from a survey conducted by Yubico in conjunction with 451 Research (part of S&P Global Market Intelligence) to understand preferences and adoption trends with respect to multi-factor authentication in the enterprise. The study examines the benefits and drawbacks of authentication technologies, spending patterns, use cases, and sentiment toward authentications standards and adoption during the coronavirus pandemic. The analysis also attempts to capture differences among diverse user personas, industry verticals and firm sizes where possible. Methodology is included at the end of the report.

Executive Findings

- Multi-factor authentication spending trends are encouraging.
    - Nearly three out of four of respondents (74%) plan to increase spending on MFA.
    - Half of respondents (50%) are increasing spending on MFA by more than 10%.
- COVID-19 and work-from-home (WFH) policies are helping to accelerate the move away from passwords toward MFA.
    - MFA was the top security technology to be adopted due to COVID-19 and the subsequent migration to WFH (49%).
    - Half of firms (50%) have restricted the use of usernames and passwords or have adopted MFA as a direct reaction to COVID-19.
- Security breaches are rampant, and MFA is a top way to protect against them.
    - Over half (53%) of all respondents have experienced a security incident or breach in the past year.
    - MFA was among the top three security technologies adopted as a response to a security breach, along with network security and cloud security.
    - The top two reasons organizations adopted MFA are for increased security (57%) and for securing sensitive data (41%).
- User experience (43%), complexity (41%) and cost (36%) are still the main obstacles to MFA adoption. They have long been common complaints about MFA, even though modern authentication technologies such as biometrics and security keys can provide a better user experience than legacy MFA technologies.
- Privileged users and third parties (contractors, consultants, partners) are the most likely to use MFA, while end customers are the least likely.
- Other than passwords, mobile OTP authenticators (58% of respondents), biometrics (54%), mobile push-based MFA (48%), SMS-based MFA (41%), and hardware-based USB security keys (40%) are among the most popular MFA form factors.
- Many organizations still rely heavily on SMS-based authentication, but only 22% perceive security as an issue – despite growing evidence of breaches and attacks exploiting mobile or SMS-based authentication methods.
- FIDO2 and passwordless authentication are gaining momentum as ways to address traditional MFA pain points.
    - Over one-third of respondents (34%) have already deployed a form of passwordless technology.
    - Nearly two-thirds (61%) described themselves as ‘very familiar’ with the new FIDO authentication standards.

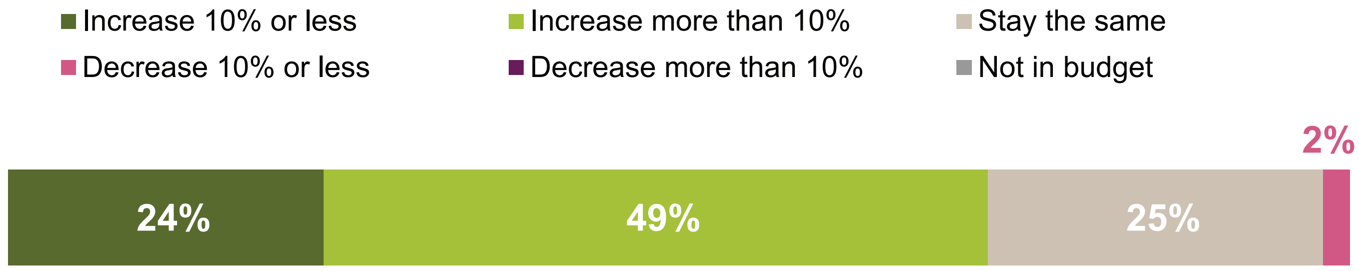
Budgets for MFA Are Expanding

Although most IT budgets decreased in 2020, cybersecurity remains a safe harbor; the highest percentage of respondents said they are planning to increase cybersecurity spending in 2021, according to 451 Research's Voice of the Enterprise (VotE): Digital Pulse, Budgets & Outlook 2021 report. MFA, in particular, is a bright spot, with nearly three-fourths of respondents (74%) planning to increase spending on MFA in 2021, and exactly half of these organizations are planning to increase spending on authentication technologies by more than 10%.

Retail and financial services stand out as the two sectors most likely to increase spending on MFA (81% and 80%, respectively). Conversely, just 2% of organizations are planning to reduce spending on MFA technologies in the coming year. Extended WFH strategies and the continued shift toward cloud-based computing models will likely remain drivers of spending on MFA technologies for the foreseeable future.

Figure 1: MFA spending trends for 2021

Source: 451 Research and Yubico custom enterprise security landscape study
Q: Has/will your organization's 2021 budget for MFA change(d)?
Base: All respondents (n=200)



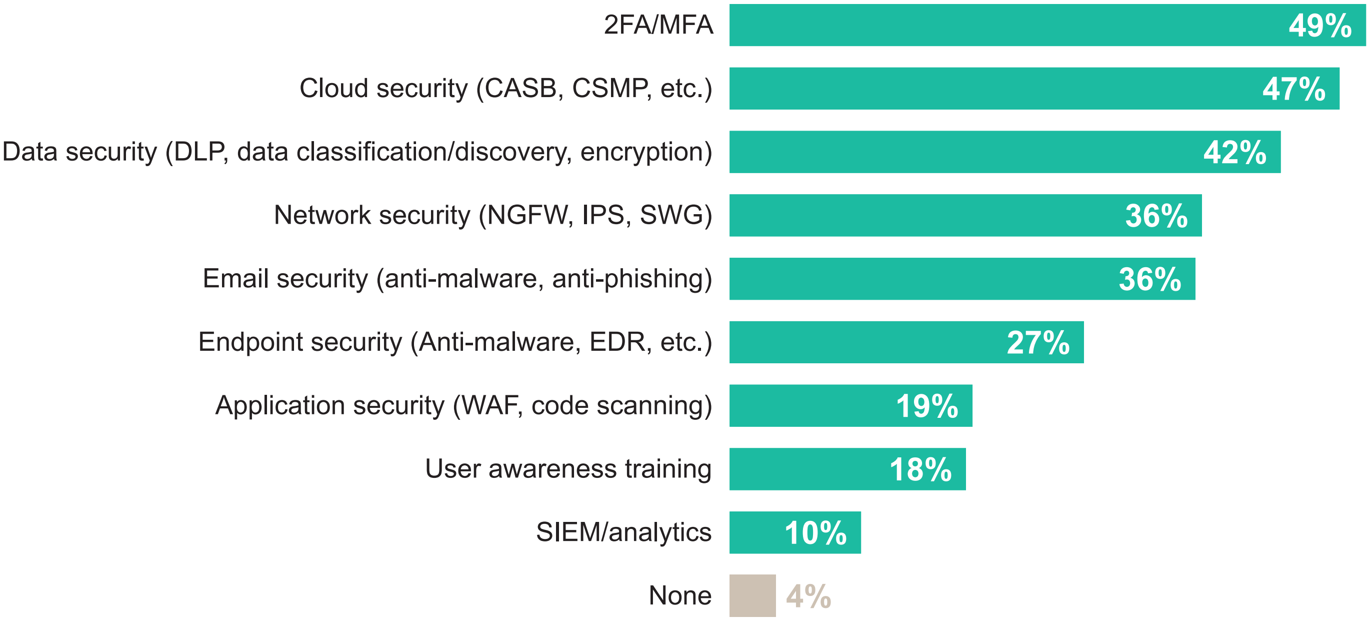
COVID-19 a Key Driver of MFA Adoption

As organizations continue their adjustments to COVID-19, the shift away from passwords toward MFA has accelerated – 50% of firms have restricted the use of usernames and passwords and adopted MFA more broadly as a direct response to the outbreak and shifts in corporate strategies. This is particularly true for the media sector, where 72% of companies have shifted from passwords toward MFA. Overall, MFA was the top security technology chosen due to COVID-19 and WFH policies (49%), followed by cloud security (47%) and data security (42%).

Figure 2: The effects of COVID-19 on MFA adoption

Source: 451 Research and Yubico custom enterprise security landscape study

Q: Which of the following security technologies will you be more likely to increase usage of due to COVID-19 and increased number of employees working from home?



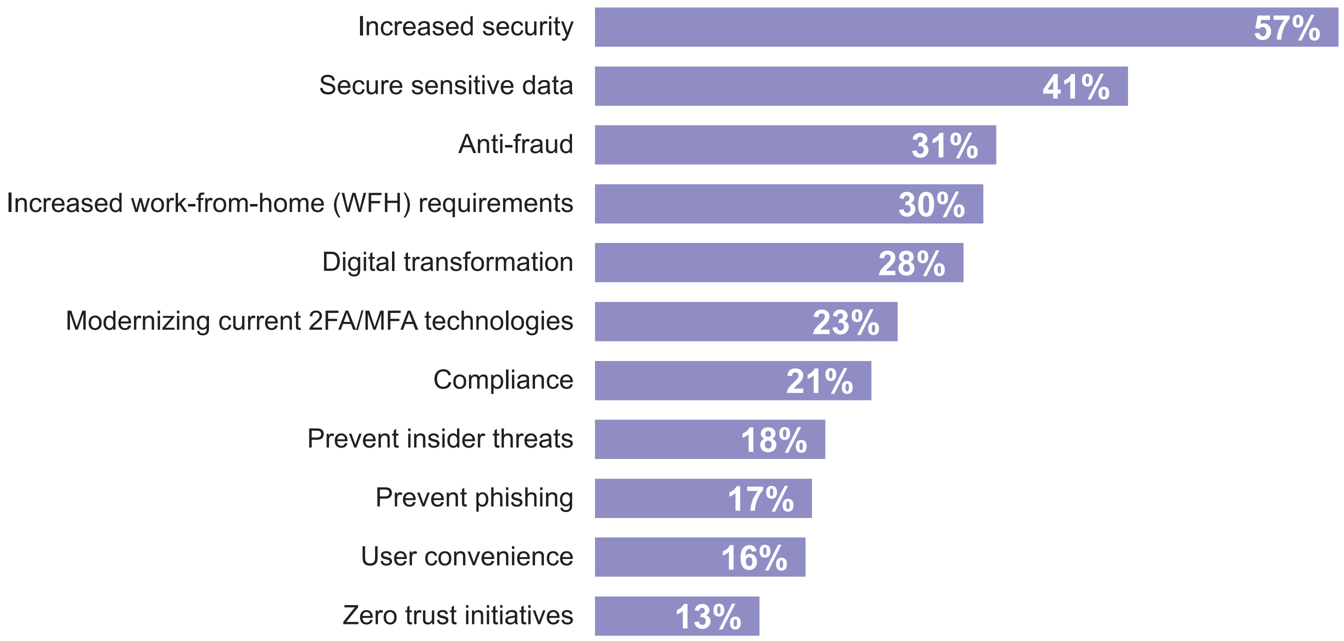
Furthermore, a high percentage of the workforce continues to work from home, and more organizations – such as Dropbox, Facebook, Square, Shopify and Twitter – are adopting extended or permanent WFH policies. Indeed, survey data from 451 Research's Voice of the Enterprise service shows that nearly two-thirds of firms have more than 40% of their employees currently working from home. Additionally, fully two-thirds (66%) see working from home as a long-term or permanent situation. Simply put, COVID-19 is directly impacting the rate of adoption for many security technologies, none more so than MFA.

Reasons for Adoption, Benefits and Pain Points of MFA

Over the last few years, security breaches have grabbed major headlines. Unfortunately, companies, governments and academic institutions still struggle to prevent common security challenges such as ransomware and phishing attacks, despite all of the money they are spending on cybersecurity tools and defenses. In just the past year, over half of respondents experienced a security incident or breach, with 21% occurring within the past six months alone. It is not surprising, then, that increased security is the number one reason for deploying MFA (57%) – by a wide margin – followed by securing sensitive data (41%) and anti-fraud (31%). It's worth noting that user convenience was not a substantial driver of MFA adoption and is near the bottom of the list at just 16%. Similarly, phishing was not a large player in MFA adoption, chosen by only 17% of respondents. This result is a bit surprising, since modern forms of FIDO-based MFA have been shown to be highly effective at preventing phishing attacks, which have increased dramatically since the COVID-19 breakout. Google, for example, claims that it has essentially eliminated phishing attacks by requiring all users accessing Google resources to use hardware-based MFA in the form of USB security keys.

Figure 3: Reasons organizations adopt MFA

Source: 451 Research and Yubico custom enterprise security landscape study
Q: In your experience, what are the main reasons for adopting MFA?



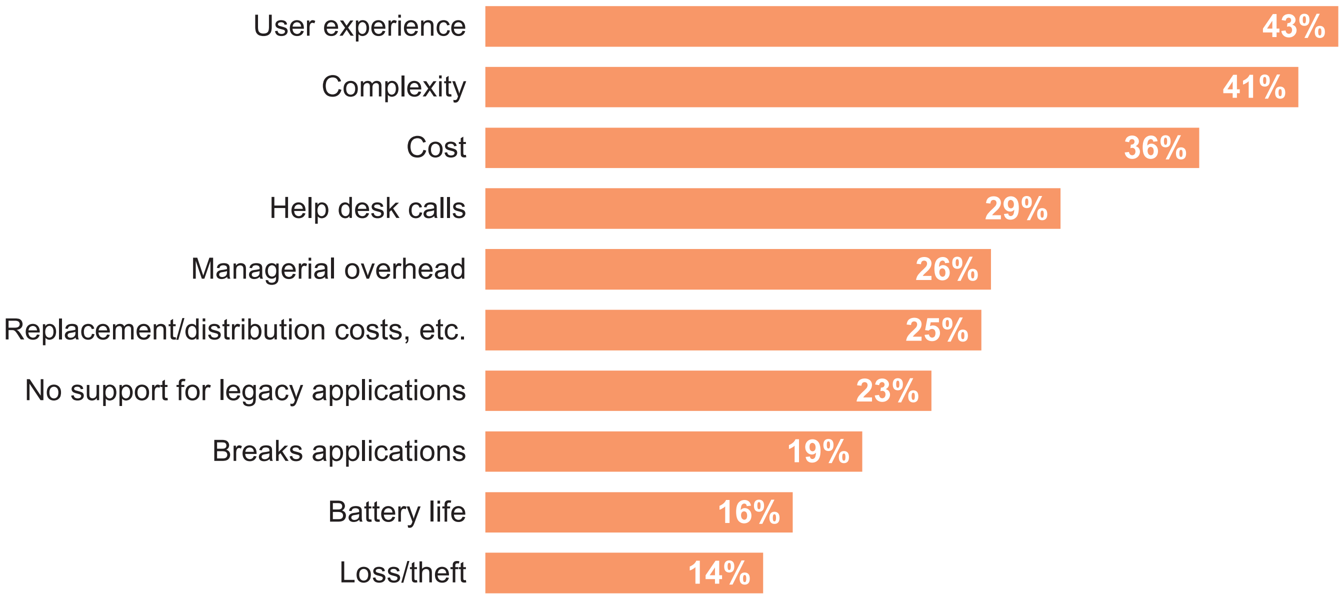
It's also worth pointing out that MFA was among the top three choices in terms of the specific technologies adopted following a security incident (chosen by 42% of respondents), closely following network security (44%) and cloud security (43%).

Main Obstacles to the Adoption of MFA

Despite their many shortcomings – and the frequent predictions of their pending obsolescence – passwords have proven to be surprisingly resilient. A big reason passwords continue to linger has as much to do with the alternatives to passwords than it does with passwords themselves. Simply put, replacing passwords with MFA has in many ways meant exchanging one set of headaches for another, and it appears that the overall perception of MFA hasn't changed much over the years: user experience (43%), complexity (41%) and cost (36%) all remain top barriers to MFA adoption – more so for larger enterprises – even though modern authentication technologies, such as biometrics and security keys, arguably provide a much better user experience than legacy MFA technologies. Respondents are less concerned, however, with loss and theft (14%), battery life (16%) and breaking applications (19%), which are often cited as reasons for rejecting MFA.

Figure 4: Barriers to MFA adoption

Source: 451 Research and Yubico custom enterprise security landscape study
Q: In your experience, what are some of the main concerns or drawbacks for deploying MFA?



Form Factors and User Groups

As mentioned above, WFH strategies are causing firms to move away from passwords, and most organizations view MFA as the main response to increased WFH. Furthermore, 451 Research VotE data shows that MFA adoption continues to edge higher. That said, our survey data also shows that overall, passwords are still the most used authentication method and are nearly ubiquitous within the enterprise: 100% of respondents indicated passwords are in use.

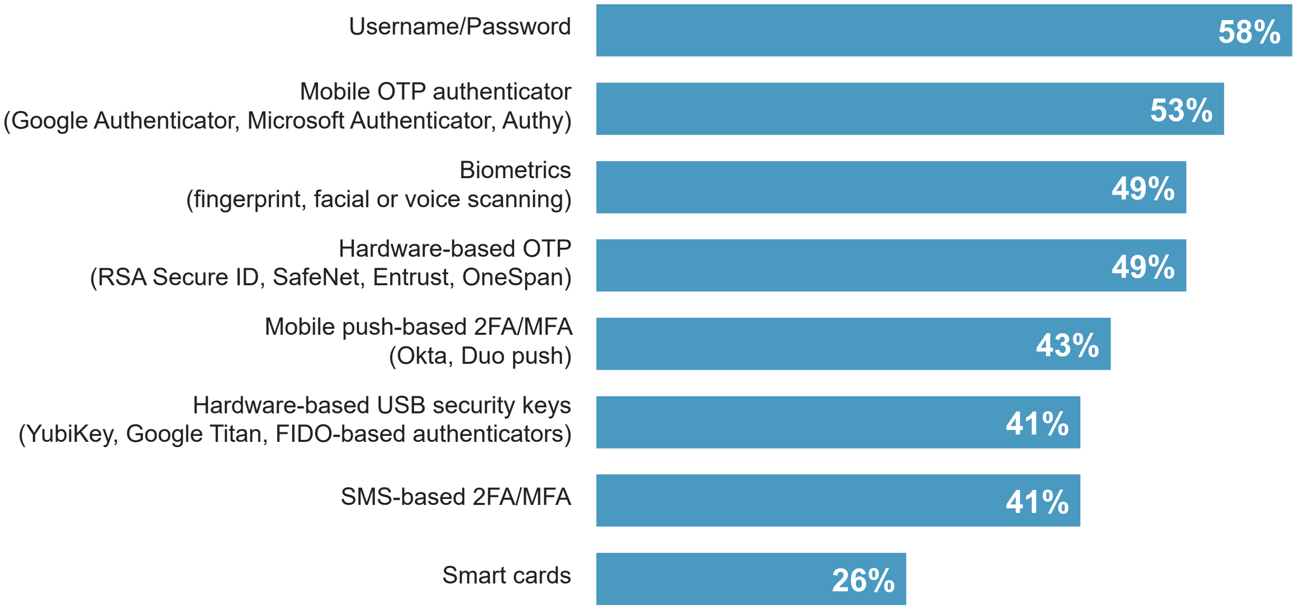
Beyond passwords, organizations face a wide array of choices in terms of MFA form factors, most of which have their own strengths and weaknesses in terms of overall security and usability. In terms of adoption, passwords are followed by mobile one-time password authenticators such as Google Authenticator and Windows Authenticator (58% of respondents), biometrics such as TouchID and Windows Hello! (54%) and mobile push-based MFA (48%). Mobile OTP is just another form of a password that needs to be typed in, while over time, users of push-based MFA can be conditioned to indiscriminately click 'yes' every time an authentication request comes their way. At the other extreme, the least deployed overall are smart cards (24%). SMS-based MFA and hardware-based USB security keys are in the middle, cited by 41% and 40% of respondents, respectively.

Adoption of MFA is fairly similar across user personas and company sizes, although some subtle differences emerged from the survey data. For example, smaller organizations with under 2,000 full-time employees are less likely to adopt certain types of MFA technologies, especially smart cards, biometrics and hardware-based USB security keys. Additionally, passwords are essentially ubiquitous among non-IT internal staff, and organizations are less likely to implement MFA within this group compared to privileged admins and IT staff and third parties. That said, 64% of organizations employ MFA technologies for their non-IT internal staff. The top choices of technologies deployed within this group include mobile OTP authenticators (49%), biometrics (47%) and hardware-based USB security keys (40%).

Privileged admins and IT staff are the most likely group to utilize MFA, with more than three-fourths of respondents reporting usage of MFA (79%) within this group, followed by third parties (70%); customers were the least likely to have MFA deployed to them (45%). The types of MFA technologies most used for privileged admins include mobile OTP authenticators (53%), hardware-based OTP (49%) and biometrics (49%). However, 58% of this group is still using passwords.

Figure 5: Multi-factor authentication for privileged admins and IT staff

Source: 451 Research and Yubico custom enterprise security landscape study
Q: Which types of authentication have you deployed for privileged admins/IT staff?



Organizations are also less likely to use passwords for remote and mobile non-IT users when compared to internal non-IT staff. Additionally, remote and mobile non-IT users are reliant on mobile-phone-based authenticators (mobile OTP, SMS-based MFA and mobile push-based MFA).

In terms of industry verticals, educational institutions are more likely to adopt an additional form of authentication for privileged admins and IT staff and third parties. For technology companies, MFA is more often used for privileged admins and IT staff and remote and mobile non-IT staff. Financial services fall under the average for certain user groups, especially remote and mobile non-IT staff and customers (both of which were at about 44% adoption) and also for privileged admins and IT staff (68%).

Hardware-Based USB Keys, SMS-Based Authentication and Passwords

When compared to SMS-based authentication, hardware-based USB security keys are used nearly equally within every user group. Media and retail companies along with larger organizations (5,000+ employees) implement SMS-based authentication more often than the other sectors and companies studied. Educational organizations have higher adoption rates of hardware-based USB security keys than other sectors, while financial services companies have the lowest (12%).

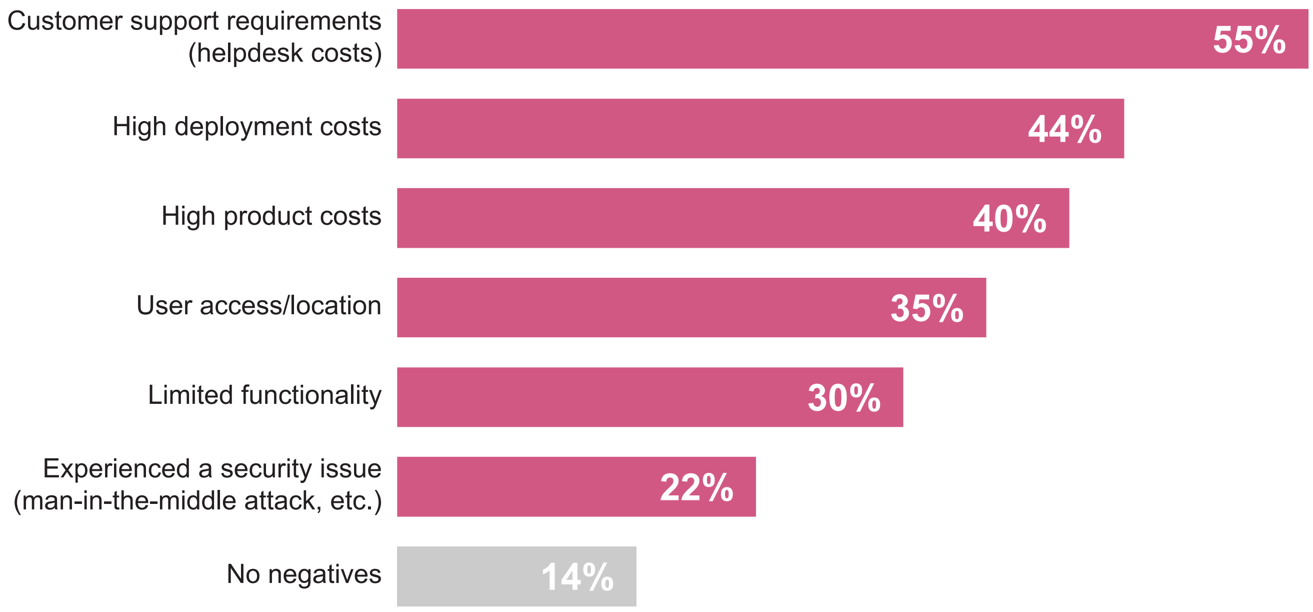
As mentioned above, some organizations rely heavily on SMS-based authentication, and we attempted to gain insight into any potential negative impacts related to the technology. The results indicate that the main drawbacks of SMS-based authentication are customer support requirements and helpdesk costs (55% of respondents), deployment costs (44%) and product costs (40%).

Interestingly, only 22% perceive security as an issue, despite growing evidence of breaches and attacks exploiting mobile or SMS-based authentication – these include phishing schemes and social engineering attacks such as SIM swaps where attackers trick phone carriers into porting a phone number to another device. Furthermore, only 28% of respondents have discouraged the use of SMS or phone-based MFA due to new WFH situations. This suggests that there is a gap in perception that needs to be addressed in order to educate and demonstrate the inherent risks of SMS-based authentication methods.

Figure 6: SMS-based authentication negative impacts

Source: 451 Research and Yubico custom enterprise security landscape study

Q: Considering your deployments for mobile or SMS-based authentications, have you experienced any of the following negative impacts?



A Look into the Future – FIDO and Passwordless Authentication

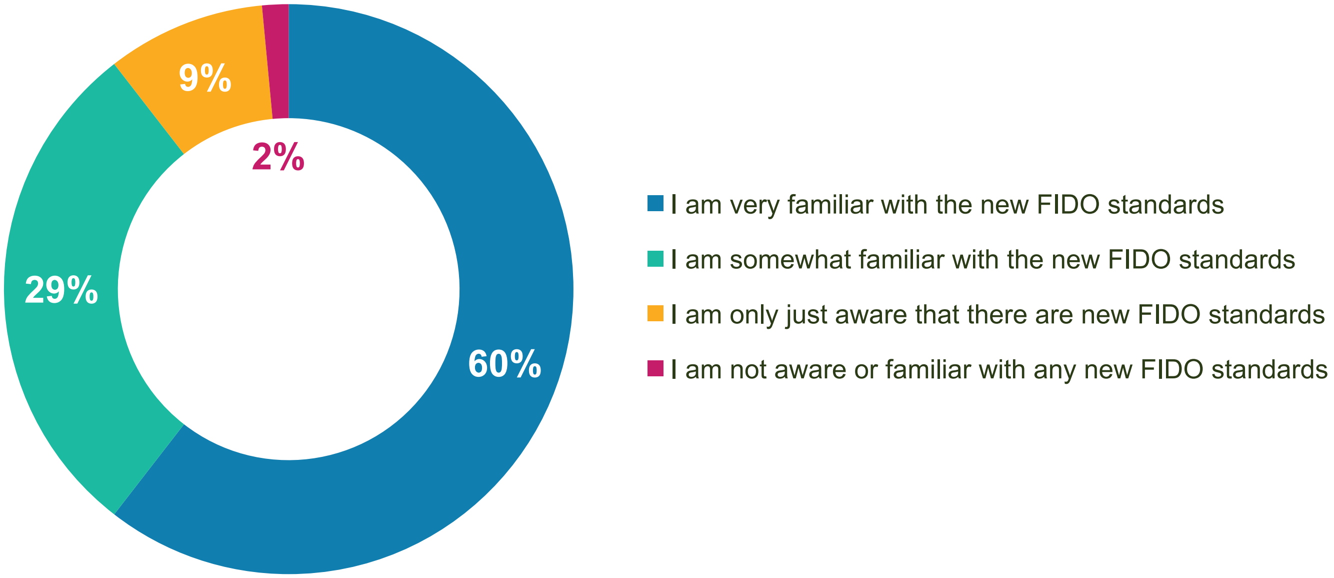
Although adoption of MFA lags behind other security technologies within the enterprise, new developments in recent years have sought to address the various friction points encountered during adoption and implementation of MFA. Like any other security technology, the user experience is paramount, and frustrated users will find other ways to get their work done if the tools they are forced to use are inconvenient. To that end, the FIDO Alliance was founded in 2012 as a consortium of companies that worked to adopt common standards and practices for online authentication. The intent was to help address the security and user experience issues with passwords by relying on public key encryption that allows users to authenticate to their local devices rather than a central repository of passwords.

Though FIDO remains at an early stage of adoption, we found it encouraging that fully 90% of respondents said they are 'very' or 'somewhat' familiar with FIDO. Like overall MFA adoption, however, FIDO adoption tends to be strongest among larger enterprises, particularly those with sizable consumer-facing businesses.

Figure 7: FIDO familiarity among organizations

Source: 451 Research and Yubico custom enterprise security landscape study

Q: Which of the following statements applies, considering the new Fast Identity Online (FIDO) authentication standards (FIDO, U2F, FIDO2, WebAuthn)?

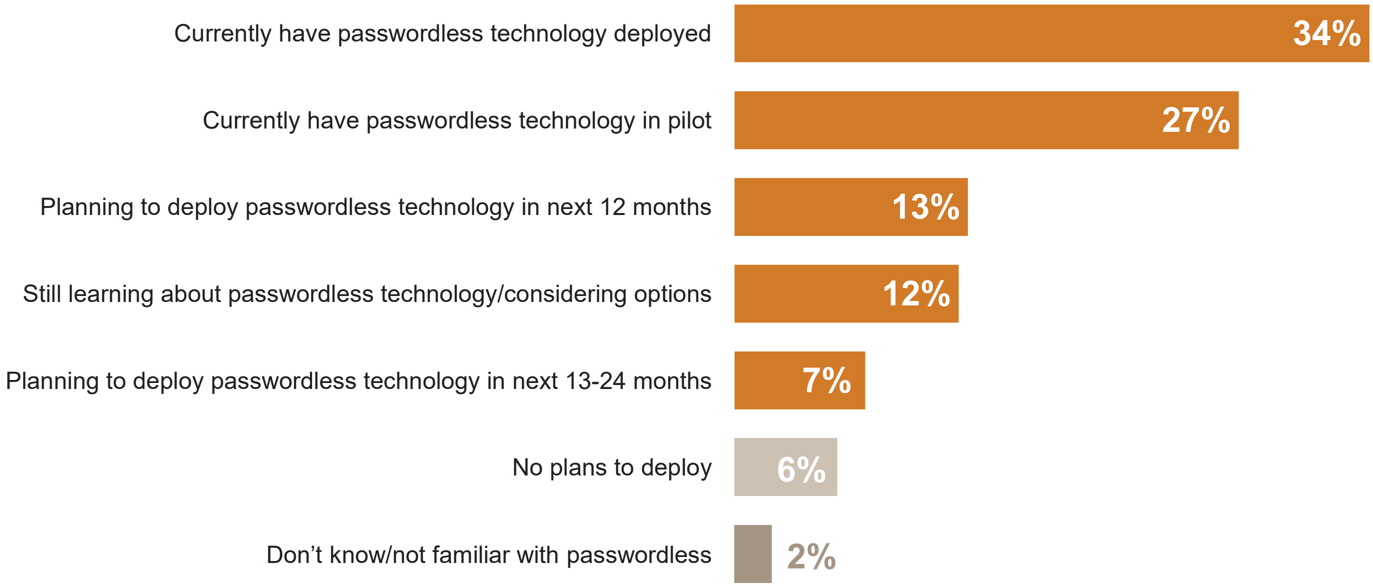


In similar spirit, users also seem to be more amenable toward the deployment of passwordless technologies. As its name implies, passwordless authentication aims to move beyond the use of passwords *when authenticating services and applications*. Passwordless authentication can take many forms, including external hardware security keys and biometrics such as fingerprint ID and voice, palm, facial and behavioral recognition, and can also leverage established methods such as public key cryptography. In general, however, it combines a streamlined user experience with a secure authentication flow that lessens – or, ideally, eliminates – the reliance on passwords.

More than half of the organizations surveyed (61%) have either deployed or have passwordless authentication in pilot (34% of respondents have already deployed passwordless technology, 27% in pilot). As with FIDO familiarity, large organizations are more likely to have already deployed passwordless technology than smaller organizations, though small companies are actually more likely to deploy passwordless technology in the next 12-24 months compared to other groups.

Figure 8: The current state of passwordless technology

Source: 451 Research and Yubico custom enterprise security landscape study
Q: Which of the following best applies to your organization with respect to passwordless technology.



Conclusion

Although MFA adoption has lagged other areas of security, ongoing migrations to the cloud, digital transformation projects and extended WFH policies have collectively helped to accelerate spending on and adoption of MFA. As noted earlier, three out of four respondents now plan to increase spending on MFA within the next year, and half of those are planning to increase spending by greater than 10%. It should be noted that all MFA is not created equal; organizations should invest time to make sure they are choosing the right method for their security profile. COVID-19 has also accelerated the move away from passwords, with 49% of organizations claiming to have adopted MFA directly due to the pandemic, and 50% restricting the use of usernames and passwords in favor of more secure authentication technologies.

Although the initial response to the pandemic was largely tactical, many of the strategic decisions and spending plans will likely have long-term consequences as WFH policies become a permanent part of the landscape for many firms and workers. Survey data from 451 Research's VotE service has shown that two-thirds (66%) of organizations plan to make WFH policies long-term or permanent, and the list of companies announcing permanent work-from-home policies for at least a portion of their workforce has grown steadily (Dropbox, Facebook, Shopify, Square, Twitter, etc.).

That said, not all news is favorable for those hoping MFA usage will become more widespread. Will passwords ever go completely away? Probably not any time soon, in large part because long-standing MFA pain points such as inconvenience, complexity and cost are still notable obstacles to MFA adoption, particularly for larger organizations. There are also opportunities to make gains on the security side of the ledger. For example, many users remain largely unaware of the security defects found within SMS-based authentication that can provide an opportunity for attackers to exploit both network security flaws and social-engineering-based attacks.

As such, new initiatives around passwordless authentication hold great promise to guard against fraud, protect employees while working from home and to reach overall digital transformation milestones by enabling both more secure access to resources and a better overall user experience. It is encouraging that over one-third of respondents currently have some form of passwordless technology deployed, while two-thirds describe themselves as 'very familiar' with the new FIDO standards.

Methodology

In November 2020, 451 Research conducted an online survey of organizations that have implemented two-factor or multi-factor authentication across North America. The objective of the survey was to understand perceptions and adoption of these types of authentication overall and to gain a deeper view of how those perceptions and adoption change among the various user groups, industries and company sizes. The survey targeted 200 executive management, senior IT management, mid-level management, senior security and risk staff, and senior risk staff in verticals such as technology, financial services, education, professional services, retail and the government sector. In addition, the survey captured data from respondents representing companies with 1-10,000+ full-time employees.

451 Research

S&P Global
Market Intelligence

About 451 Research

451 Research is a leading information technology research and advisory company focusing on technology innovation and market disruption. More than 100 analysts and consultants provide essential insight to more than 1,000 client organizations globally through a combination of syndicated research and data, advisory and go-to-market services, and live events. Founded in 2000, 451 Research is a part of S&P Global Market Intelligence.

The information contained herein has been obtained from sources believed to be reliable. 451 Research and S&P Global Market Intelligence disclaim all warranties as to the accuracy, completeness or adequacy of such information. Although 451 Research may discuss legal issues related to the information technology business, 451 Research does not provide legal advice or services and their research should not be construed or used as such.

The content of this artifact is for educational purposes only. S&P Global Market Intelligence does not endorse any companies, technologies, products, services, or solutions. S&P Global Market Intelligence shall have no liability for errors, omissions or inadequacies in the information contained herein or for interpretations thereof. The reader assumes sole re-sponsibility for the selection of these materials to achieve its intended results. The opinions expressed herein are subject to change without notice.

NEW YORK
55 Water Street
New York, NY 10041
+1 212 505 3030

SAN FRANCISCO
One California Street, 31st Floor
San Francisco, CA 94111
+1 212 505 3030

LONDON
20 Canada Square
Canary Wharf
London E14 5LH, UK
+44 (0) 203 929 5700

BOSTON
75-101 Federal Street
Boston, MA 02110
+1 617 598 7200