A Zero Trust Strategy Starts with Strong Authentication – of Both Users and Devices

Pathfinder

November 2021

Commissioned by

BEYOND IDENTITY

451 Research

S&P Global
Market Intelligence

About this paper

A Pathfinder paper navigates decision-makers through the issues surrounding a specific technology or business case, explores the business value of adoption, and recommends the range of considerations and concrete next steps in the decision-making process.

About the Author

Garrett Bekker

Principal Research Analyst, Security

Garrett Bekker is a Principal 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. Garrett started his career in security as an equity research analyst at several investment banking firms, most recently Merrill Lynch, where he covered information security, infrastructure software and networking companies. Garrett has also worked with early stage enterprise security vendors in sales and marketing role, including Bat Blue (acquired by OPAQ Networks). Prior to joining 451 Research, he also worked at a boutique investment bank focused on M&A and fundraising for small-to-midsized technology companies.

Garrett has focused on a wide variety of subsectors within enterprise security during his career, and is now focusing primarily on identity and access management (IAM), cloud security and data security. Garrett is also a member of 451 Research's Center of Excellence for Quantum Technologies.

Garrett holds a BA in international studies (with honors) from the University at Buffalo, where he was a member of the varsity ice hockey team and learned how to drive a Zamboni. He also completed all coursework for a PhD in economics from the New School University and has completed undergraduate and graduate studies at McGill University and Cambridge University (Queens' College).

Executive Summary

Zero trust has received considerable attention in recent years, and for good reason; the old perimeter-based security model, where anyone (or thing, system, etc.) on the inside of the network is trusted and anyone outside untrusted, is becoming increasingly less relevant. Why? It is partly due to the continued advance of cloud computing and mobility – and more recently the influence of the COVID-19 pandemic and work-from-home (WFH) strategies. But it's also because the things we want to protect – including apps (SaaS, cloud-native and 'lifted and shifted' traditional apps), users, IT infrastructure and devices – are scattered all over the place and no longer under IT control. Simply put, our vital resources have left the building and might not ever be coming back.

In this new world, organizations need to move toward an architecture where trust is not implicit, and access to specific resources such as servers, applications and devices – not just networks or network segments – is primarily granted using the principle of least privilege. In other words, access to resources is more about 'who' you are rather than 'where' you are. A strong zero trust strategy, therefore, eliminates implicit trust; it verifies the user's identity and checks the security of the transaction right before it occurs.

It follows, then, that the ability to verify the identity of the user (or machine, application, etc.) is a central, critical component of any zero trust strategy. Ideally, this would call for a form of strong authentication, since the security limitations of traditional static passwords are well known – they're hard to remember and easy to guess, and they lie at the root of many recent security breaches. However, based on the rate of enterprise adoption, a stronger form of authentication, specifically multi-factor authentication (MFA), is in the middle of the pack of security technologies such as firewalls, endpoint security and SIEM tools for several reasons: cost, complexity and, mainly, a poor user experience.

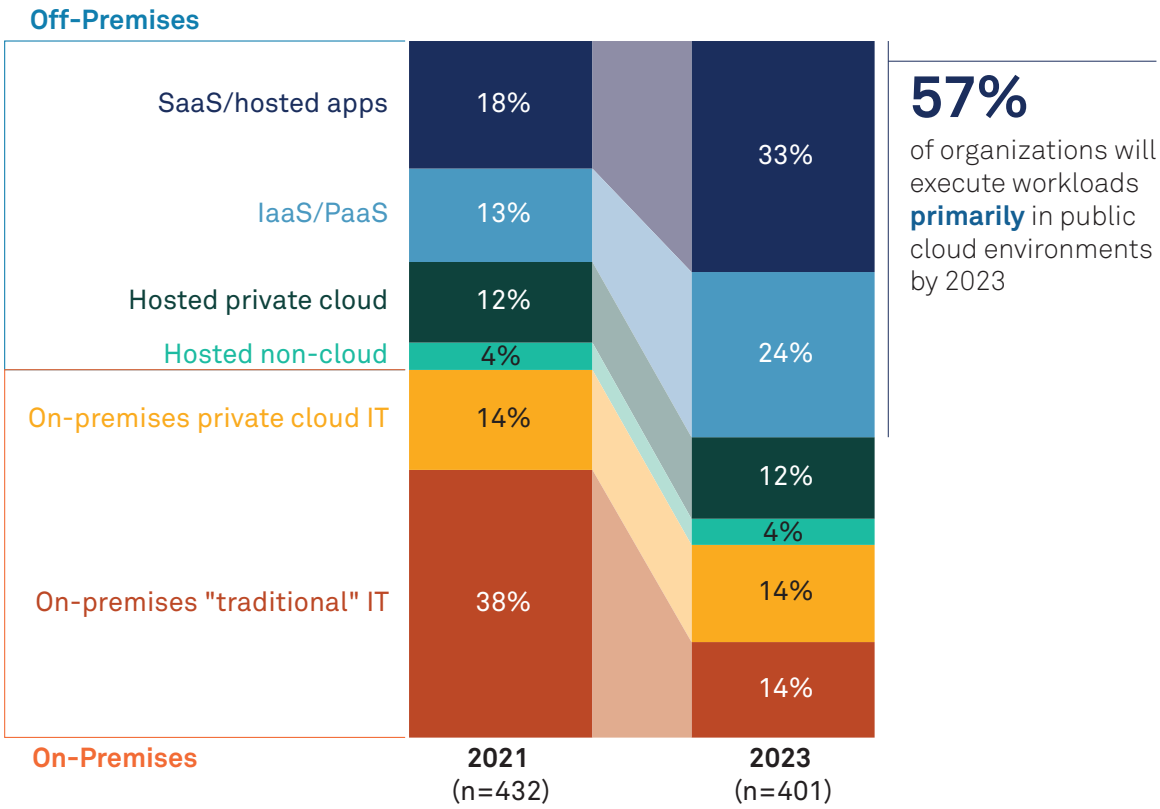
Another limitation of traditional MFA products is that while they may offer some additional protection beyond static passwords – depending on the form factor used – they provide little help in determining the security status of devices. Is this device managed or unmanaged? Is the device up to date with security batches and the latest browser? Is it running risky mobile apps? Has it been jailbroken or rooted? This paper explains how an approach based on device trust can go beyond MFA to provide a more comprehensive, granular and contextual method of accessing applications and resources. Throughout this paper, we cite data from 451 Research's Voice of the Enterprise service, which combines industry-leading analysis with insights from an extensive community of IT and line-of-business professionals, drawing on surveys of IT decision-makers with specific knowledge of their organization's security strategies.

Key Findings

- Applications are no longer confined to the corporate locations; they can be run anywhere – in the public cloud, as SaaS apps, in private clouds (both hosted and non-hosted) and in traditional datacenters, which suggests that security policies and enforcement points must be everywhere, too.
- At the same time, workers are everywhere. Most firms have some form of WFH policy in place, many of them permanent. Further, nearly 70% of organizations believe that the vast majority of their employees can work effectively while remote.
- Now that our apps, data, infrastructure and users can be basically anywhere, the older perimeter-based security model is certainly becoming less relevant. 451 Research survey data shows that zero trust is one of the top three security technologies being implemented due to increased WFH requirements.
- Although COVID-19 and WFH strategies have boosted corporate use of MFA, it remains middle of the pack amid other security technologies based on adoption rates. However, a comprehensive zero trust strategy should be built upon a foundation of strong identity as a necessary and obvious starting point, with MFA playing a key role.

- Passwordless authentication is promising but still only solves part of the problem; it ignores the role of device trust in a true zero trust framework.
- The only way to achieve zero trust is to accurately verify the identity of both users and their devices.

Figure 1: IaaS, PaaS, SaaS and On-Prem – Workloads Are Everywhere



Q. Which of the following best describes the current state of your organization's IT environment? Base: All respondents (n=423)

Q. How often do workloads/applications move between on-premises and off-premises deployment venues in your organization's hybrid IT environment? Base: Hybrid users (n=230)

Source: 451 Research's Voice of the Enterprise: Cloud, Hosting & Managed Services, Workloads & Key Projects 2021

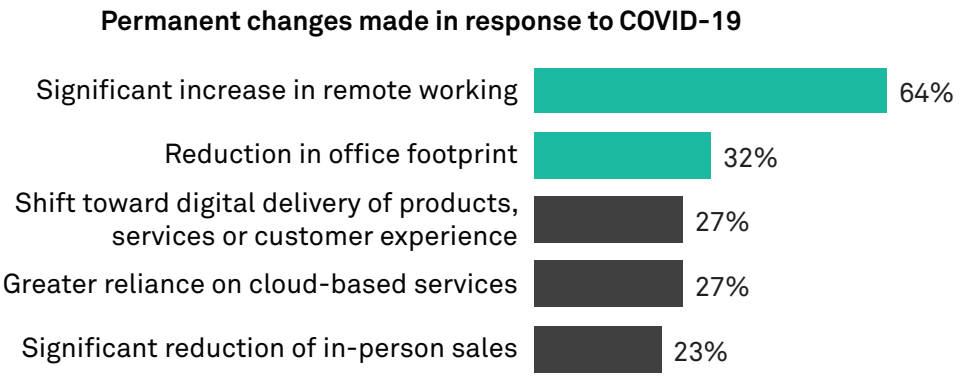
It may seem fairly obvious these days to state that cloud adoption is growing, but each year more workloads are moving to the cloud, and as they continue to migrate, security will remain a front-burner issue. In fact, according to 451 Research Voice of the Enterprise (VotE) data, more than half of all workloads will run in some form of public cloud in the next two years, while workloads that run on-premises in traditional datacenters will be cut sharply – in fact, respondents expect on-prem workloads to decline by almost two-thirds to less than 20%. The movement to the cloud itself presents security issues, in part driven by the architecture of cloud environments and the fact that the underlying infrastructure, as well as data and applications, no longer resides on-premises.

It's also important to note that the distribution of workloads remains fairly wide and spans a variety of architectures, which means it's necessary to maintain a variety of security tooling and approaches. In other words, applications are no longer confined to corporate locations; they can be run anywhere – in the public cloud, as SaaS apps, in private clouds (both hosted and non-hosted) and, yes, in traditional datacenters, which means that security policies and enforcement points must be everywhere, too.

Thanks to the Pandemic and WFH, Users Have Left the Building

At the same time, workers are everywhere. Before the COVID pandemic hit, 451 Research VotE data showed that just over a quarter of employees spent all or most of their time either working from home or from another 'non-office' fixed location (Starbucks?), and that almost two-thirds worked remotely during at least part of their week. Now, most firms have some form of WFH policies in place – many of them permanent. Further, nearly 70% of organizations believe that the vast majority of their employees can work effectively while remote.

Figure 2: Work from Anywhere Is Here to Stay



69%

of enterprises indicate at least 75% of their workforce **can work effectively remotely.**

Q. Which, if any, of the following permanent changes has your organization made due to the influence of the coronavirus (COVID-19) outbreak? Please select all that apply. (n=378)

Q. Approximately what portion of your organization's workforce is unable to work effectively remotely? (n=345) Base: All respondents

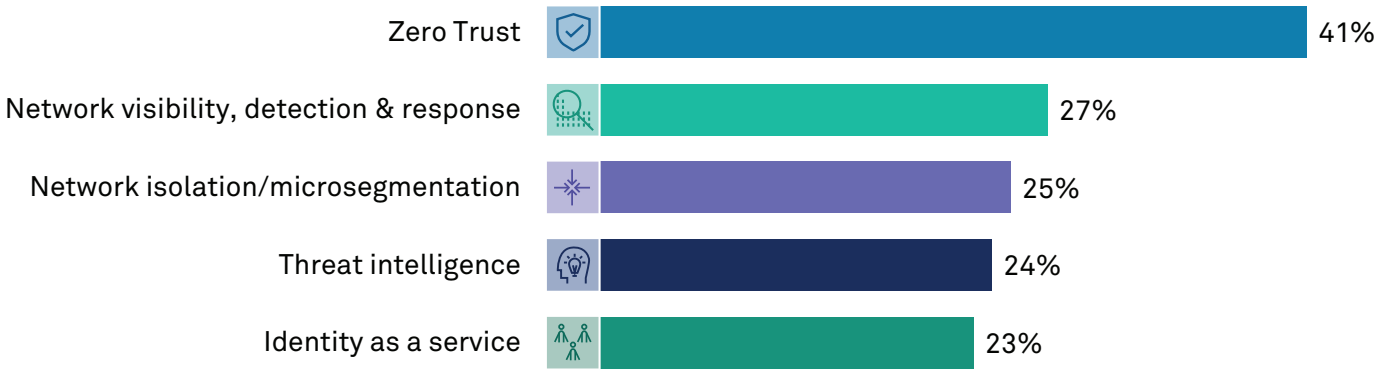
Source: 451 Research's Voice of the Enterprise: Digital Pulse, Coronavirus Flash Survey October 2020

We Need a New Approach to Security – and Zero Trust Leads the Way

Now that apps, data, infrastructure and users can be located basically anywhere, the older perimeter-based security model is certainly becoming less relevant. How do you provide security when the network isn't yours anymore (it's the public internet), the devices aren't yours (some or all may be BYOD, even if you issue corporate-owned devices), the datacenter isn't yours (it's in the cloud), the application is not yours (SaaS), and even users (contractors, outsourcers, etc.) might not be yours? A zero trust strategy can help. In this increasingly distributed world, organizations need to move toward an architecture where trust is not implicitly granted, and access to specific resources such as servers, applications and devices – not just networks or network segments – is primarily granted using the principle of least privilege.

Considering all this, it's not surprising that 451 Research survey data shows that zero trust is one of the top three security technologies being implemented due to increased work-from-home requirements, with 41% of respondents planning to deploy zero trust within the next two years.

Figure 3: Zero Trust Is a Top Planned Security Objective in Next Two Years



Q. What is your organization's status of implementation for the following information security technologies?
Base: Respondents planning to deploy in next 6-24 months (n=84-98)
Source: 451 Research's Voice of the Enterprise: Information Security, Workloads & Key Projects 2020

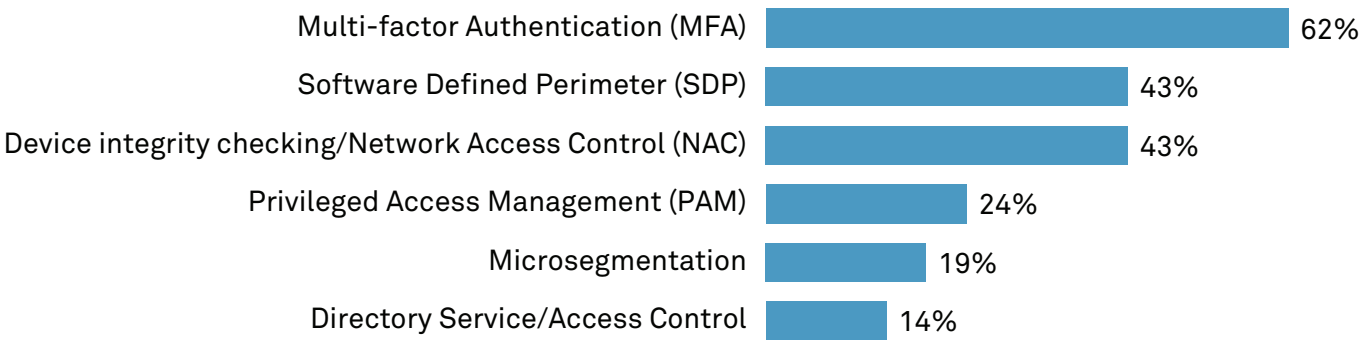
The Zero Trust Journey Starts with Strong Authentication

While zero trust can offer marked improvements to security in our modern world, it can also be a complex and time-consuming undertaking for any firm, even those with substantial financial and internal resources. Google, for example, reportedly took several years to roll out its well-known BeyondCorp zero trust model, and many firms don't have Google's internal expertise or financial wherewithal.

And while zero trust certainly has gained a lot of attention in recent years, it is still in the early stage of its evolution. The industry has yet to settle on consistent terminology and a definition of what zero trust actually means, as well as how it fits into related concepts such as zero trust network access (ZTNA) and the emerging secure access service edge (SASE) framework. There is still a considerable amount of confusion, and many organizations looking to get started on their zero trust journey simply don't know where to start.

In a zero trust world, access to resources is more about 'who' you are than 'where' you are, and whether the device being used to access resources is trustworthy. This suggests that any zero trust strategy should be built upon a foundation of strong identity and device trust as a necessary and obvious starting point. Indeed, respondents to a 451 VotE survey cited MFA as the security technology that is most important for enabling a zero trust strategy, ahead of privileged access management by more than a factor of two to one.

Figure 4: Most Important Technologies for Enabling Zero Trust



Q. What technologies are most important to enabling a zero trust network access/software-defined perimeter strategy?
Base: Respondents currently using zero trust network access/software-defined perimeter technology (n=21)
Note: Base sizes below n=50 should be interpreted anecdotally
Source: 451 Research's Voice of the Enterprise: Information Security Workloads & Key Projects 2021

MFA Adoption Has Lagged Other Security Technologies

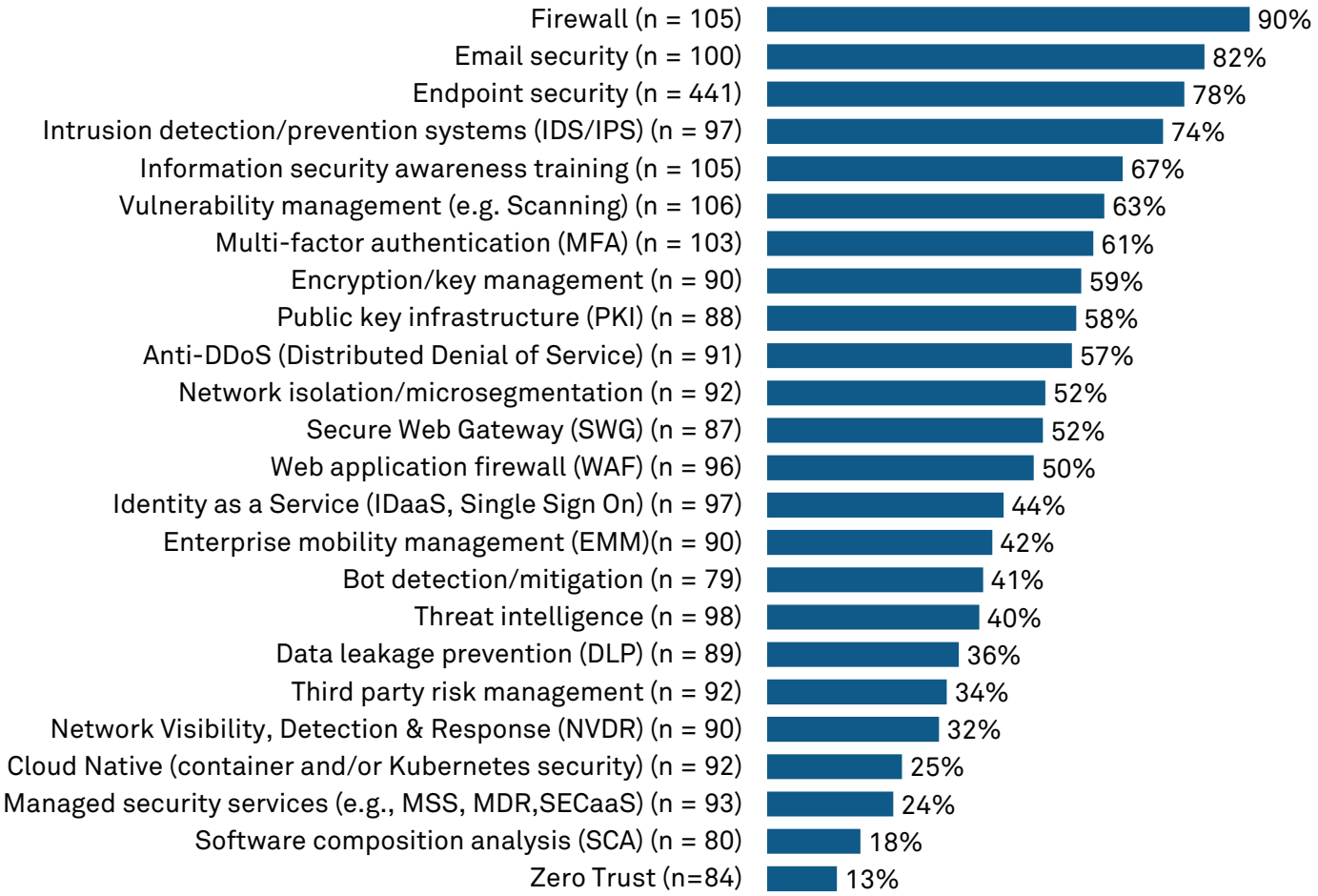
There is still room for improvement in authentication technologies. The drawbacks of passwords are well known; simply put, they can be hard to remember, easy to hack and a general nuisance for both end users and security personnel. However, passwords remain a staple of many firms' security frameworks, despite the fact that the cybersecurity industry has been calling for the death of passwords for nearly 20 years now.

Part of the reason for the ongoing resilience of passwords is that when organizations look at stronger forms of authentication, they 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. Authentication form factors include one-time password; authenticators such as Google Authenticator and Windows Authenticator; biometrics such as TouchID and Windows Hello; mobile push-based MFA, biometrics, smart cards, SMS-based MFA; and hardware-based USB security keys.

Further, many of these forms of MFA don't fully eliminate passwords since users often still need to type in a username, PIN or both, along with their MFA authenticator, which presents a security risk but also potential issues in terms of user experience and potential helpdesk costs for locked-out users. The key factors holding back broader adoption of MFA include user experience, complexity and cost, and to a lesser extent, loss and theft, battery life, and impact on application functionality. For example, admins often set session timeouts to days, weeks or months to help counterbalance a poor user experience. The upshot is that a bad user experience can also lead to bad security outcomes that violate the very essence of zero trust – never trust, always verify – in addition to being an inconvenience for users. Simply put, replacing passwords with traditional MFA has in many ways meant exchanging one set of headaches for another.

One of the biggest issues with MFA, however, is that, like other security tools, it is binary: you're either in, or you're out; there's no in-between. In a sense, MFA is like a bouncer at a night club; once past the outer security, nobody knows what you are doing on the inside; if an attacker gets hold of a compromised credential or bypasses the authentication process, that attacker can do a lot of damage before being detected.

Figure 5: Implementation of Security Technologies



Q. What is your organization's status of implementation for the following information security technologies?
Source: 451 Research's Voice of the Enterprise: Information Security, Workloads & Key Projects 2020

COVID-19 and WFH Have Boosted MFA Adoption

The COVID-19 pandemic and WFH trends appear to have accelerated the adoption of MFA; 61% of enterprises have deployed MFA, according to 451 Research survey data. This is up from just over 50% in recent surveys, but it's still well below other security staples such as firewalls (90%) and endpoint security (78%). Further, it's likely that within the 61% of firms that do use MFA, deployments are not enterprise-wide but reserved for just a subset of the total user population and are used mainly for specific use cases, like remote access VPNs.

Passwordless Is a Step in the Right Direction

Passwordless authentication aims to improve adoption of authentication by making stronger forms of authentication more seamless. It would allow for a more positive user experience by completely eliminating passwords or other 'shared secrets' – knowledge factors such as mother's maiden name or city you grew up in. Recent initiatives toward 'passwordless' authentication have gained a lot of attention in the past year or so, in part thanks to momentum of the Fast Identity Online (FIDO) Alliance and the ratification of new passwordless authentication standards such as FIDO2 and WebAuthN.

However, passwordless authentication presents its own challenges. Passwordless technologies that rely on the FIDO protocols can require changes to browsers, applications and devices in order to support public key cryptography. Passwordless can also require an up-front commitment of time and resources, although that commitment should pay off in the long run. However, the goal is to deliver an access control system that takes into account the identities of users and their devices, user behavior, the security posture of the devices, and the risk of the applications and resources that are being accessed, and to prevent common attacks such as credential stuffing/reuse and password-replay attacks. Therefore, we view passwordless authentication as just the first step on the journey toward the 'holy grail' of continuous, risk-based authentication.

Device Trust Is a Fundamental Building Block

Broader adoption of MFA is a good first step, but perhaps the largest drawback of MFA – passwordless or not – is that it only solves part of the problem. Authenticating the user is a great first step, but the device also needs to be secure – is it one that you have seen before? Has the device been rooted or jailbroken, are patches up to date, does it have malware on it? In addition, is there a way to separate personal from company data? And Is company data encrypted?

Those questions are all important, and MFA alone can't answer them. To illustrate, a fully authenticated user can attempt to log into a critical application such as Salesforce from an infected PC in the library or a café, even with an MFA challenge. MFA has no concept of device trust but needs to do more. Is the device known? Which user does it belong to? Is it secure enough? And in order to implement a true zero trust framework, firms need to be able to trust all of the devices accessing their resources, including both managed devices and unmanaged BYOD devices used by employees, external contractors, suppliers, partners and customers.

This transaction-oriented approach is a completely new way of looking at access management; at every transaction, how do you know it's a live human on the other end, and is that user who you think it is? Is the device secure? The impact of each transaction is weighed and mitigated against the risk dimensions associated with it, based on all the available context.

Conclusions

Although MFA adoption has lagged other areas of security in the past, ongoing migrations to the cloud, digital transformation projects and extended WFH policies have collectively helped to accelerate spending on and adoption of MFA. Long-standing MFA pain points such as inconvenience, complexity and cost are still notable obstacles to MFA adoption, particularly for larger organizations. 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 more secure access to resources, as well as a better overall user experience.

Zero trust is never going to be achievable until we're able to accurately verify the identity of both users and their devices. A strong zero trust strategy, therefore, eliminates implicit trust, verifying a user's identity, and checking the security of each transaction right before it occurs.

CONTACTS

The Americas
+1 877 863 1306
market.intelligence@spglobal.com

Europe, Middle East & Africa
+44 20 7176 1234
market.intelligence@spglobal.com

Asia-Pacific
+852 2533 3565
market.intelligence@spglobal.com

www.spglobal.com/marketintelligence