computing research

RESEARCH PAPER

Identity-first: How strong authentication can bolster organisations' ransomware defences

October 2021

Sponsored by

okta

CONTENTS

Introduction

In the past few years incidents of ransomware have skyrocketed and ensuring that they are protected against this type of attack is imperative for business across all industries.

While small and medium enterprises may have once considered themselves too small to be the target of ransomware attacks, a growing number of organisations are learning the hard way that this is no longer the case.

Traditional perimeter-based IT security is no longer enough. Identity first security, where security is based around confirming the identity of users rather than relying on usernames or passwords that can fall into the hands of adversaries, should therefore be a central part of organisations' security strategy.

Encompassing elements such as multi-factor authentication, single sign-on and zero-trust policy, establishing secure controls around identity is key to enabling strong authentication.

The following white paper, supported by bespoke research, will delve into how organisations can establish authentication strategies that will protect them against future threats, reduce attack surface and avoid security issues that stem from poor access control management. It will explore the tools and strategies that security practitioners can deploy to protect their organisation from ransomware and other cyber threats, and the importance of trust – or more accurately a lack of it.

Key Findings:

- 77 per cent of survey participants believe the volume of cyber security incidents have increased in the last 18 months.
- 67 per cent believe that ransomware attacks are becoming either somewhat or greatly more sophisticated.
- Only 13 per cent strongly agreed that their organisation's current ransomware defences are adequately protecting it from threats.
- The top three most widely reported security challenges from the last 18 months all relate to remote working.
- 53 per cent of those participating in our research claimed to have an Identity First security strategy.
- Only 8 per cent of participants had fully implemented a Zero Trust security architecture and 22 per cent were in the middle of doing so. A further 15 per cent were trialling and 26 planning.

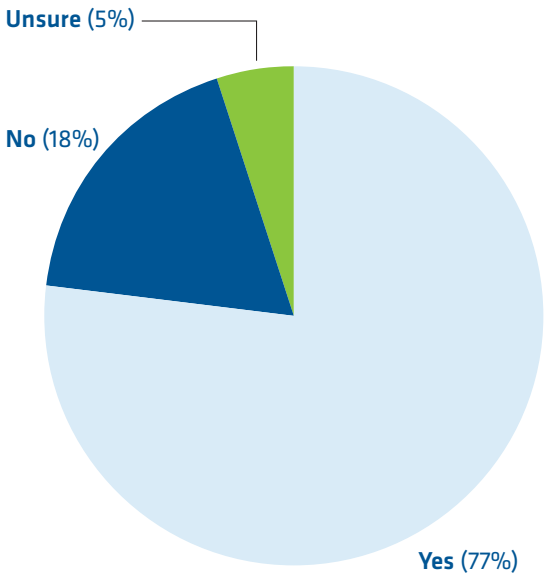
- 85 per cent agree to some or a great extent that passwords alone are no longer an adequate authentication method...
- ...However, the IAM solutions necessary for Identity First and Zero Trust such as Adaptive MFA are only being used by a small minority of participants. 15 per cent use Adaptive MFA.
- Only 25 per cent reviewed access rights at monthly or more frequent intervals. 26 per cent did so annually or even less. This sits at odds with the claim by more than half of participants that they are "Identity First."
- Seamless user experience is the most important factor when choosing an IAM solution.

Ransomware Epidemic

Ransomware trends in 2021 have followed a similar pattern to that of the COVID-19 pandemic insofar as you hear a lot less about it than you used to, and you'd be forgiven for thinking that that it was all over. However, just as with Covid, ransomware hasn't gone anywhere. Infections are increasing, and the threat of new variants is always lurking.

As the diagram below illustrates, participants in our research are feeling bombarded by cyber security incidents, and other data suggests that they are correct that attack volumes have increased significantly. Multiple security vendors have reported significant increases in attack volume, with some claiming that they have identified more attacks in 2021 than they did throughout the whole of 2020.

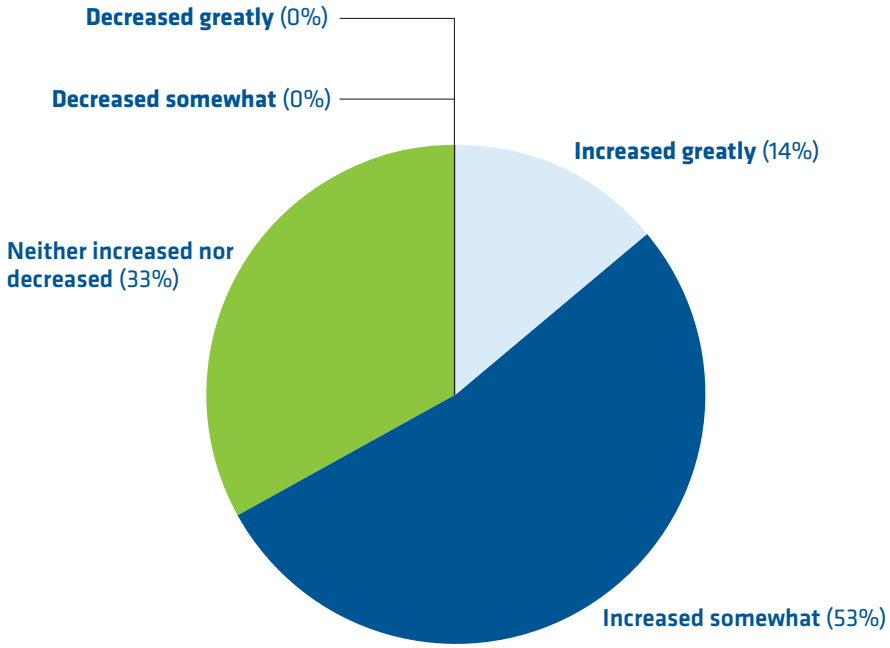
Fig. 1 : "In your opinion, has the volume of cybersecurity incidents increased in the past 18 months?"



What's fuelling this onslaught of attacks? There is no one cause, but it seems that cyber criminals are exploiting the fact that many employees are still working at least partly from home, although more challenging for cyber security professionals is the fact that those employees aren't staying at home anymore. They're working from coffee shops, enterprising pubs and restaurants and pop-up office spaces. They're meeting colleagues informally rather than in offices. All of these scenarios are problematic for cyber security solutions designed for the pre-pandemic, predominantly office-based era.

The increase is also being caused by criminals exploiting the very current global supply chain issues. Supply chains aren't really chains at all – they're eco-systems. If one part of that system is compromised it opens door to the rest of the system, and this is exactly what is happening. In addition to the first victim having data encrypted or stolen, attackers often threaten to release it publicly and customers, supplier and partners of compromised businesses are also being targeted. The 67 per cent of those surveyed who think attacks are becoming either somewhat or greatly more sophisticated really aren't imagining it.

Fig. 2 : "How has the sophistication of ransomware attacks changed at your organisation in the last 18 months?"



27 per cent of the organisations that took part in our research admitted to having been compromised within the last 18 months. This is a lower proportion that has been reported in other surveys[1] but may reflect the fact that those taking part in our research may have more sophisticated cyber security measures in place than the average organisations. It may also reflect a more general unwillingness to admit to attacks for fear of being targeted again or of other reputational repercussions.

Gaps in Defences

Interestingly, when asked the extent to which they agreed with the statement, **"my organisation's current ransomware defences are adequately protecting it from threats,"** only 13 per cent agreed strongly. 54 per cent agreed somewhat, with the remainder either neutral or in disagreement. This suggest that in a majority of cases, our respondents know that the there are gaps in their organisation's defences against ransomware.

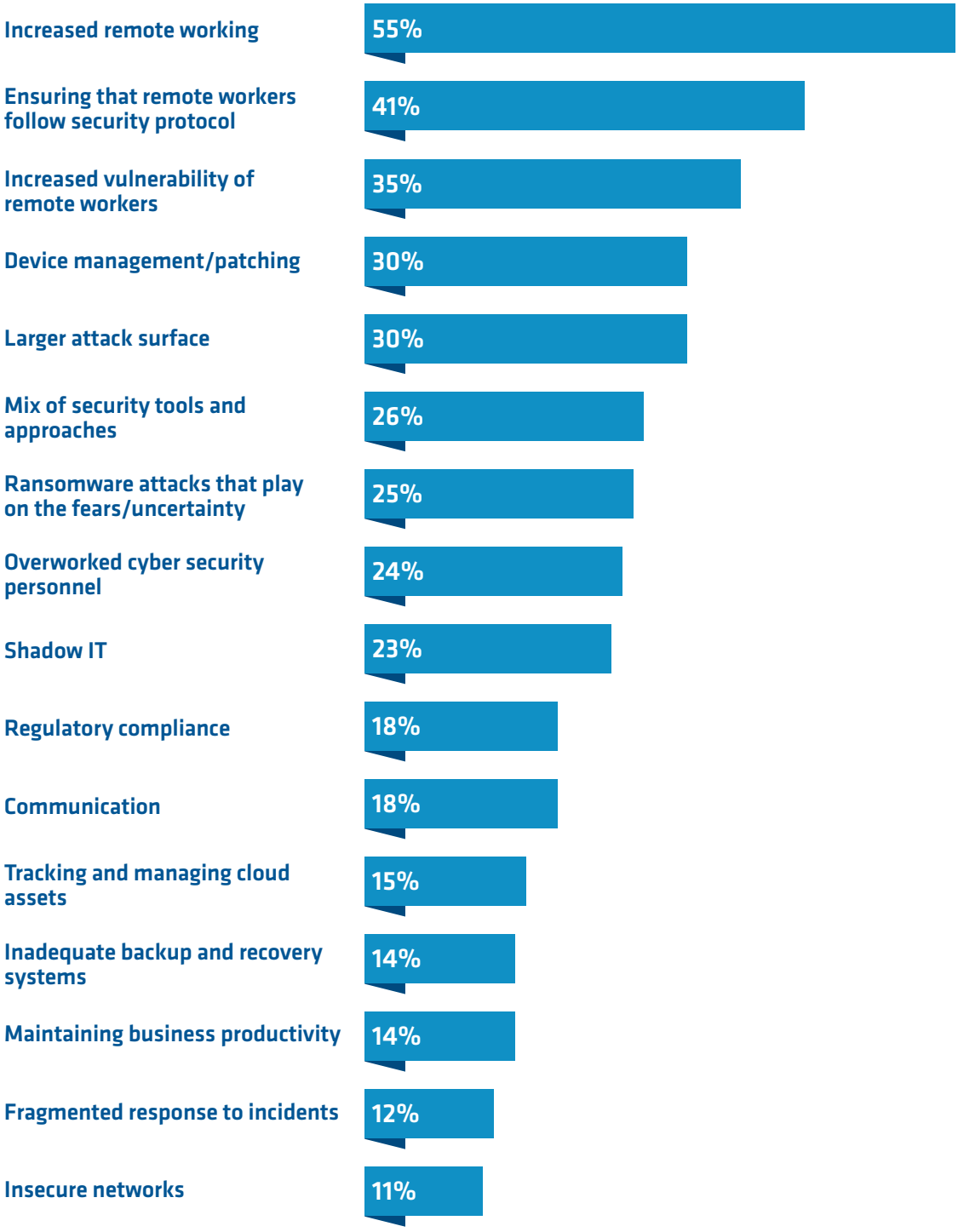
Our researchers asked participants what they considered the main weaknesses that can lead to ransomware attacks. Top of the rankings at 60 per cent was a lack of employee training. This is undoubtedly a tough nut to crack. Most would agree that employees have a responsibility to safeguard both their employers' data, their own personal data and data belonging to any third parties. However, although the risk of malevolent insiders and disgruntled soon-to-be ex-employees should never be minimised, the vast majority of employees are not wilfully negligent. They're busy, keen to be as productive as possible and in many cases, eager to meet up in person as much as they can if they aren't back in offices full time. The problem is that this situation means that employees are targetable via social engineering which was the third highest scoring weakness (50 per cent) via mediums such as email (second highest at 54 per cent.)

Most employees are aware of the more obvious cyber security risks, but the working conditions that the pandemic has created, even as they evolve into hybrid working, have the potential to create greater risks, as devices and passwords are shared between household members, and corporate resources are accessed from networks and devices that employers have minimal control over.

Indeed, the three most widely reported security challenges were all related to remote working, the increased vulnerability of remote workers and the difficulties inherent in getting them to follow best security practice.

[1] https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2021/cyber-security-breaches-survey-2021

Fig. 3 : Which of the following challenges have you experienced over the past 18 months? Please select all that apply



Identity First

Identity and Access Management (IAM) tools are crucial in the fight against ransomware because they prove that people trying to gain access to corporate resources are who they say they are.

A majority of our research participants (63 per cent) use IAM to protect against both unauthorised internal access and external threats. This is wise. Although access enables from inside enterprises are most likely to be the result of a mistake rather than a malicious act, access gained externally is almost certain to be malicious – although both of these have the potential to be extremely damaging.

The risk of ransomware finding internal as well as external vectors has led more and more organisations to consider the design of their security architecture and whether that architecture is fit for the hybrid working era. "Identity First" is simply the more concise iteration of the "any user, any device, any place," cyber security model that has been slowly taking shape since network perimeters initially became increasingly elastic, but then corroded and broke down altogether with Covid considerably hastening the final stages of the process.

Identity First puts identity at the centre of security architecture – and everything else builds from there. More than half,53 per cent to be exact, of those participating in our research claimed to have an Identity First security model. 25 per cent said that they have not adopted this approach, and the remainder were unsure – an unusually high proportion given the technical roles held by those taking part on our research. The prevalence of this level of uncertainty suggests that many organisations are struggling to bring their cyber security defences in line with the threats that they face.

The use of IAM among those we surveyed was almost universal. In fact, two thirds of those responding used more than one IAM solution. Whether this situation has come about by accident or design is a moot point. Most enterprises would choose to streamline their cyber security solutions as much as possible, but the security stack is large and unwieldy in many enterprises, and IAM is a part of that stack. Some solutions traditionally do MFA or PAM very well, but some are more focused on areas such as API access management or hybrid gateway. Also, some organisations choose multiple solutions because of fears of the consequences of becoming tied to one vendor – both commercially and technically.

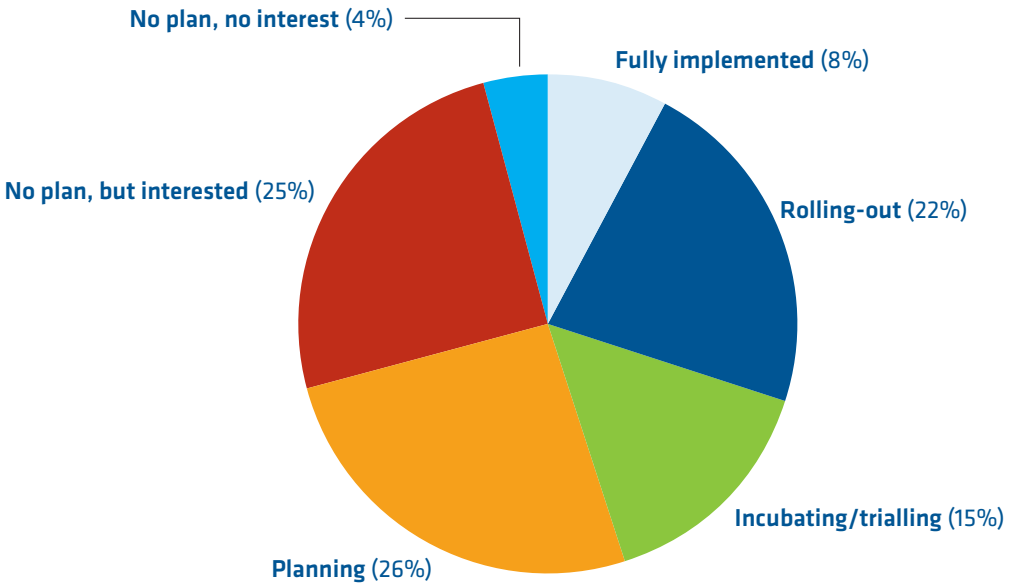
However, many enterprises have been trying to simplify, streamline and consolidate their security stacks, and many are concluding that new generation IAM solutions have the capability to span multiple areas of their infrastructure – rendering previous "best of breed" approaches less relevant. A Single Sign On powered by an MFA solution such as a fingerprint on a mobile or a "magic link" sent over email can reduce the risks posed by cyber criminals whilst also increasing the productivity of employees. The gains that hard pressed support teams can realise through simplified management is also a big incentive for streamlining IAM.

Zero Trust and Access Rights

The concepts of Identity First and Zero Trust are inextricably linked. The traditional perimeter model of security means that once a user has authenticated to gain access into the primary corporate network, they are free to move laterally through corporate data and applications. They are, by virtue of their authentication, trusted. Cyber criminals using ransomware have taken advantage of this model, using this ability to move through networks to find and either encrypt or steal data, often now disabling back-ups as well.

Zero Trust turns this approach on its head by quite literally not trusting anybody and dynamically validating users and their devices as they attempt to access data. Among our research participants, zero trust security models were not as entrenched as Identity First which is a counter intuitive finding. The fact that only 8 per cent had already fully implemented such a policy and 22 per cent were rolling it out sits slightly at odds with the 53 per cent stating that their security model was Identity First.

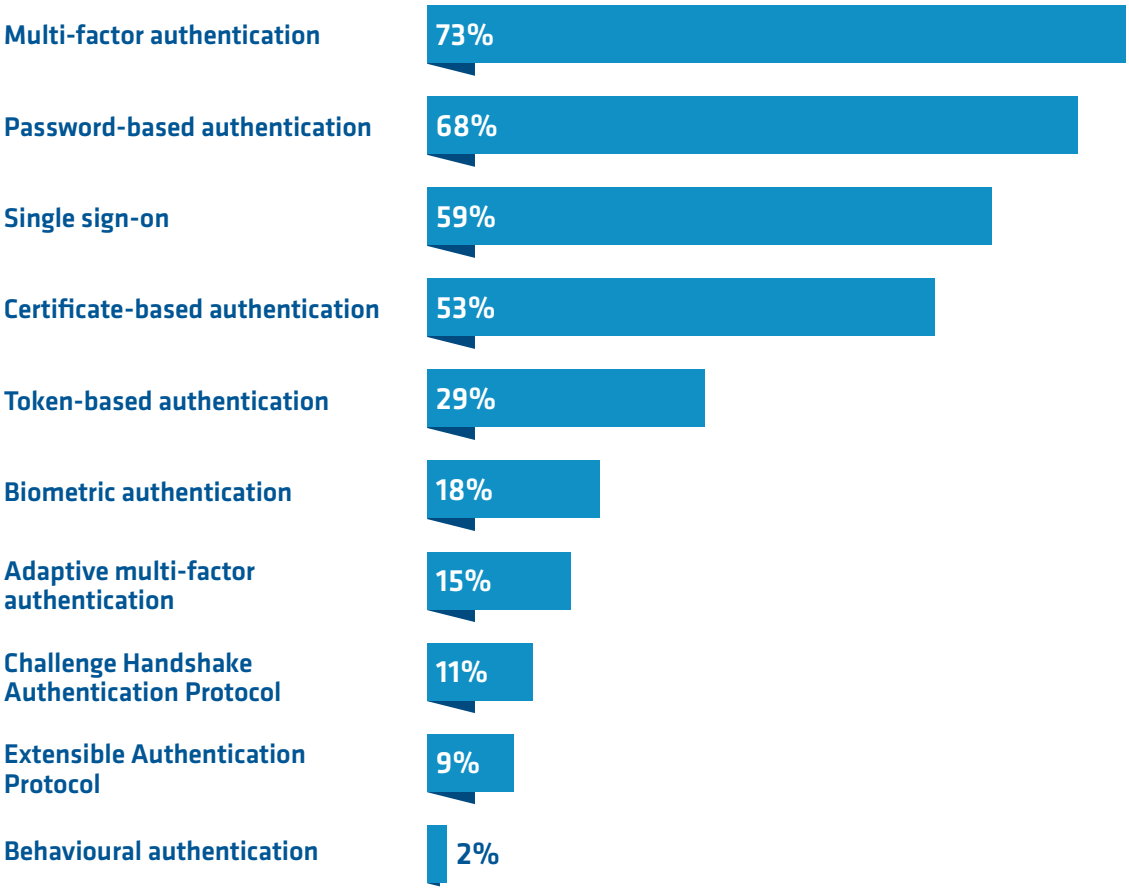
Fig. 4 : What stage is your organisation at in implementing a zero-trust strategy?



Other questions are raised about the true extent of Identity First security modelling by the findings illustrated below. Respondents could choose more than one answer so the proportions using password authentication alone is likely to be very small. 48 per cent of our respondents strongly agreed that "passwords alone are no longer an adequate authentication method," and a further 37 per cent somewhat agreed.

However, the fact that 68 per cent are using passwords at all gives some cause for concern. Passwords are damaging to both security and productivity. Approximately 61 per cent of security breaches are caused by stolen and hacked credentials[2]. Poor password practice among employees has led to employers mandating more complex passwords and more regular changes, but employees dislike this because they have to spend more time generating and resetting passwords before they get to the resources that they need, and are therefore more likely to try and find workarounds for security policies that hamper productivity. The only party that wins from password-based authentication is cyber criminals.

Fig. 5 : Which of the following authentication methods does your organisation currently use?



[2] https://www.verizon.com/business/resources/reports/dbir/

Multi-factor authentication and SSO were commonly used, but the low levels of token-based authentications, likely to be due to the difficulties in managing and scaling such solutions mean that much of this authentication is likely to be SMS or email security codes which do not constitute an identity first platform.

In order to ensure that employees are really who they say they are, and also to dynamically validate their access to services and data, both of which are essential components of Identity First and Zero Trust, different tools are needed such as Adaptive MFA, Challenge Handshake Authentication, Extensible Authentication Protocol and Behavioural Authentication. These are being used by only a minority of participants – a tiny minority in the case of Behavioural Authentication.

Adaptive MFA is just that. Contextual analysis is applied to access decisions so when an employee requests access to corporate resources, a decision is made on the basis of when, where and how they are trying to access those resources. Behavioural analysis is part of context. Policy rules can change alongside user behaviour. An example would be stepping up authentication requirements if an employee tries to sign in on a new device. Enterprises can set granular policies to allow, require step-up authentication, restrict scope, or deny access dependent on these factors. Authentication protocols are also key for security when using public networks.

If organisations do not have these authentication measures in place – and our research suggest most of them do not – they cannot be said to have an Identity First, or indeed a Zero Trust security model.

Access Rights and regular reviews of those rights are also part of Zero Trust. This can be a huge problem with cloud applications such as SaaS, where permissions are set at roll out and then rarely revisited. "Set and Forget" is the very antithesis of Zero Trust. 59 per cent of respondents had updated their access control management strategy in response to the increase in remote working. However, only 25 per cent reviewed access rights at monthly or more frequent intervals. 26 per cent did so annually or even less.

Access reviews can be time consuming if conducted manually but can be automated to remove this issue. IAM solutions should have pre-built adaptors to be easily integrated with access review tools. Automated access reviews are crucial for an Identity First approach to security and, by extension. Zero Trust architecture.

Conclusions– Identity is the Foundation of Zero Trust

Although the majority of organisations taking part in this research agreed that their organisations current ransomware defences were adequately protecting them, that agreement was fairly soft. Only 13 per cent agreed strongly with that sentiment which indicates gaps in our collective defences against ransomware.

The new hybrid working environment has created extra challenges for cyber security professionals, with corporate resources being accessed from a far greater variety of devices and from wireless networks that enterprises have no control over. The most widely reported security challenges were all related to remote working, and the difficulties of ensuring employees followed best security practice.

The majority of organisations represented were using multiple IAM solutions, probably because resources are all over the place – in multiple clouds and on-premise. As infrastructures have become more complex so has security. Not only can cyber security teams benefit from streamlining IAM solutions and moving to a SSO type solution, so can employees as they are freed for having to continually reauthenticate to access different resources.

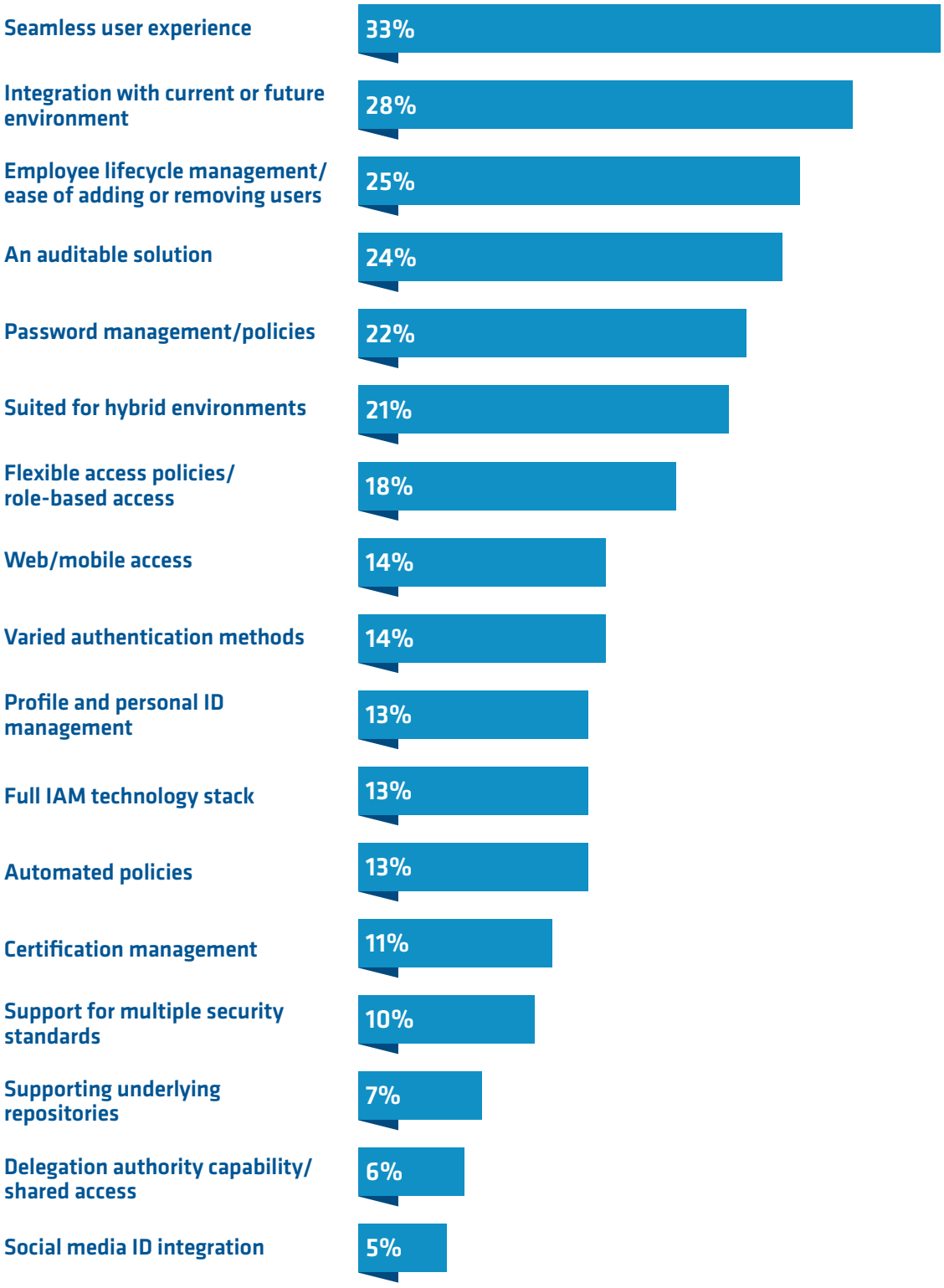
More than half – 53 per cent – of represented organisations claimed to have an Identity First approach to cyber security. Identity First simply puts identity front and centre of security architecture as opposed to the legacy perimeter model which built a wall around resources – a wall which to all intents and purposes might as well not exist. Why bother to scale corporate firewalls when you can target a privileged user who might well be working from an insecure device or network?

This why enterprises are turning to Zero Trust systems which, instead of trusting users once they have authenticated, takes a lack of trust as a default and dynamically assess each request for access. Just because an employee has accessed one application, it does not mean that they can automatically access another. Zero Trust is still in its early days in many businesses – only 8 per cent of organisations represented had fully implemented it and 22 per cent were in the midst of doing so.

Part of the reason for the slow adoption of Zero Trust is that many organisations are stuck with a security stack designed in the perimeter era. Password authentication belongs to this era. 85 per cent of our participants agreed that passwords alone are no longer an adequate authentication method.

A true Zero Trust architecture has to have identity at its heart, and at present, very few of the organisations represented here are using the kind of adaptive MFA consisting of contextual and behavioural analysis necessary for Identity First. The best Adaptive MFA solutions aggregate data across their own customer bases to detect suspect IP addresses to help prevent credential-based attacks.

Fig. 6 : "Which of the following factors are most important when choosing an IAM solution?"



Adaptive MFA, combined with passwordless SSO, removes the other big obstacle to Zero Trust which is employees, who tend not to like being treated as a liability or having their productivity limited by having to continually re-authenticate or work from specific devices in specific locations. In fact, as we can see in Figure 6, a seamless user experience was the most important factor to organisations choosing IAM solutions.

Organisations also need to review access rights more frequently. The longer the gaps between reviews, the larger the holes in your cyber defences. IAM solutions should integrate into automated access review tools to ensure that legacy "ghost" accounts are not allowed to linger and create vectors for cyber-attacks.

Neither hybrid working nor ransomware – or indeed other risks to cyber security – are going anywhere. Enterprises are under pressure to make hybrid work without compromising either security or employee satisfaction and productivity. By putting identity at the heart of a Zero-Trust security architecture, and using IAM solutions which provide Adaptive MFA, SSO and powerful integrations, enterprises can both secure their access and simplify it for employees and support teams alike.

About the sponsor, Okta

Okta is the leading independent identity provider. The Okta Identity Cloud enables organizations to securely connect the right people to the right technologies at the right time. With more than 6,500 pre-built integrations to applications and infrastructure providers, Okta provides simple and secure access to people and organizations everywhere, giving them the confidence to reach their full potential. More than 9,400 organizations, including JetBlue, Nordstrom, Siemens, Slack, T-Mobile, Takeda, Teach for America, and Twilio, trust Okta to help protect the identities of their workforces and customers.

For more information:

Visit: www.okta.com/uk