cpl. thalesgroup.com #AMI2020

THALES

The Challenges of Trusted Access in a Cloud-First World

Zero Trust: Balancing Security & Access

2020 Thales Access Management Index Europe and Middle East Edition

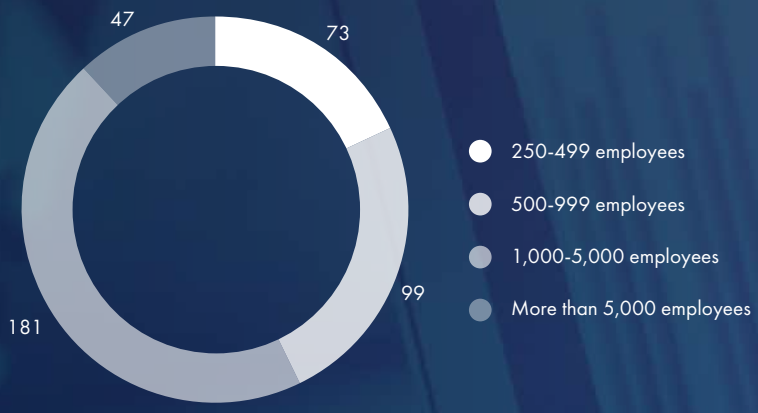
About this study

The 2020 Access Management Index – Europe and Middle East Edition, is a survey of 400 executives in 7 countries in Europe and the Middle East with responsibility for, or influence over, IT and data security. The survey, reporting and analysis was conducted by Vanson Bourne, commissioned by Thales.

Respondent country: UK: 100, France: 100, Germany: 100, Belgium and Netherlands: 50, Saudi Arabia and UAE: 50

VansonBourne

Organisation size



Organisation sector

Contents

Introduction

The modern world requires stronger IT security and data protection than ever before. High profile breaches are becoming more common and cyber-attacks are the norm. There is a huge public pressure to be protecting data for customers and of course there is massive implications within any organisation who is breached.

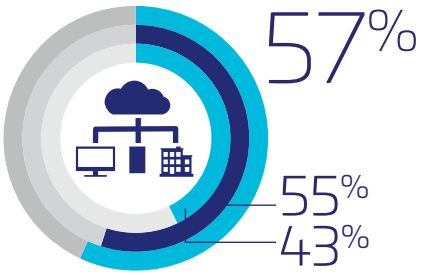
It's clear that there is cause for concern. Not only is there an increase in threats, there's also an increase in vulnerable technologies being used. Rightly or wrongly, some of the most widely used modern technologies have a stigma attached that they are vulnerable. This is where modern technology needs modern security and authentication methods to deliver a Zero Trust approach when it comes to data security. It's far too frequently that we see vulnerable technologies and poor access management solutions, which is an unforgivable mistake.

This research explores access management practices within businesses and the use and importance of two-factor authentication, smart single sign on and cloud access management tools. We aim for this to be informative and educational, while inspiring best practice.

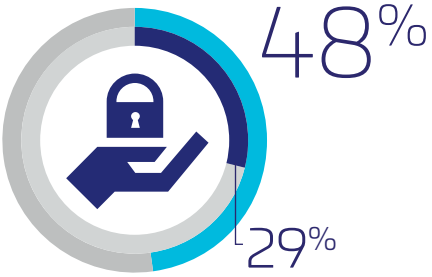
Key Findings

Give Passwords a Pass

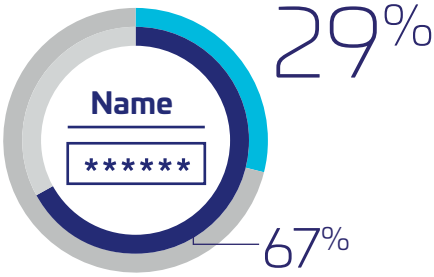
as Concerns about Cyber-attackers Targeting Unprotected Infrastructure and Cloud Apps Rise



believe unprotected infrastructure (e.g. new IoT devices) present the biggest targets for cyber-attacks, ahead of cloud apps (**55%**) and web portals (**43%**)



of IT leaders find it easier to sell the need for security to their boards compared to last year (**29%**)



rate username and password as an effective means of protecting their IT infrastructure, with **67%** planning to expand their use of it in the future

Zero Trust – Balancing Security and Convenience

67%

say their security teams feel under pressure to provide convenient access to users, but still maintain security

Access Management is Essential for Cloud Transformation

96%

believe strong authentication and access management solutions can facilitate secure cloud adoption.

76%

revealed employee authentication needs to be able to support secure access to a broad range of services including virtual private networks and cloud applications.

Two Steps Forward, One Step Back

75%

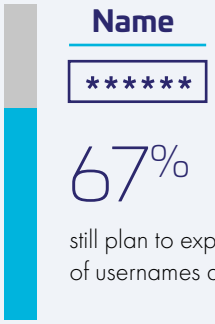
are expanding their use of biometric authentication

81%

are expanding Smart SSO in the next year.

70%

plan to further utilise passwordless authentication methods



67%

still plan to expand their use of usernames and passwords

01 Access Management Trends

Over half of respondents identify unprotected infrastructure (57%) or cloud applications (55%) as one of the biggest targets for cyber-attacks. Intriguingly, those from larger organisations with more than 5,000 employees were more likely (64% vs. 51% of those from organisations with 250-499 employees) to identify unprotected infrastructure as a potential target. Larger organisations appear to be struggling to ensure that their entire infrastructure is protected.

Among those who feel that cloud applications are a top target for a cyber-attack, the most likely (56%) cause is the increasing volume of cloud apps in use. Organisations are in a race against themselves to protect their cloud applications as quickly as they are deploying them. But there are some other reasons why cloud applications may be targeted, including inconsistent security protection (55%), a lack of in-house skills (44%) and/or poor visibility over their cloud applications (43%).

For most (94%) organisations, their security policies around access management have been influenced by recent breaches of consumer services. Yet despite this, many (51%) would still allow employees to log on to company resources using personal, social media credentials. Regardless of a respondent's position on this, one thing is clear; almost all (98%) agree that in order to comply with regulations, tighter controls over data access are needed.

Most respondents have, or imminently plan to implement, some form of access management capability. Be that an on-premises IAM solution (61% have, 18% plan to within the next year), IDaaS (53%, 21%), Cloud SSO (51%, 18%), or smart SSO (48%, 24%) . In terms of what is motivating organisations to implement access management solutions such as these, it is more of a response to security concerns rather than for ease of use benefits. For instance, the threat of large-scale breaches (21%) or security concerns (19%) are both far more likely to be the main driver for implementing an access management solution than simplifying cloud access for end users (8%) or enabling new ways of doing business (8%).

Regardless of why an organisation is implementing such a solution, it is likely that there are plenty of voices in the decision-making process. While the CIO/head of IT is most likely (37%) to be the final decision maker, the vast majority indicate that people such as the cloud security team (85%), cloud migration team (82%), chief cloud strategy officer (80%), or digital transformation team (79%) are involved to some extent.

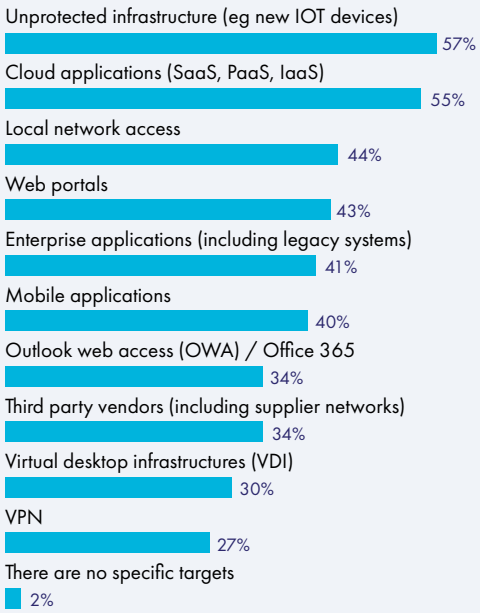
Unprotected Infrastructure and Cloud Applications are both Rapidly Expanding within Many Companies

Digital Transformation Introduces New Security Concerns

Opinion among respondents is unequivocal – nearly all believe that cyber-attackers are specifically targeting areas of their business for cyber-attack.

Foremost among these targets are unprotected infrastructure and cloud applications. These two areas have something in common – they are both rapidly expanding within many organisations.

As organisations expand their infrastructure, or deploy more cloud applications, it is crucial that they are immediately protected from cyber-attack.



In general, which of the following do you think are the biggest targets for cyber-attacks (phishing, ransomware etc.)?

The bigger the organisation, the more likely it is that respondents worry about unprotected infrastructure

While around half of respondents from organisations with 250-999 employees feel that unprotected infrastructure is one of the biggest targets for cyber-attack, this rises to almost two thirds from organisations with more than 5,000 employees.

Larger organisations naturally have larger infrastructures, making employees at these organisations more likely to be worried about this potential threat. But the message is clear, no matter how large your organisation's infrastructure is, if you leave any part of it unprotected then it may become a target for attack.

> "No matter how large your organisation, if you leave any part of it unprotected it may become a target for attack"

Showing the percentage of respondents who think that unprotected infrastructure is one of the biggest targets for cyber-attack – split by organisation size

Why are cloud applications being targeted?

According to respondents this is because the volume of cloud applications is increasing and they are protected by inconsistent security. In addition, organisations lack the skills required in-house to secure infrastructure and they lack visibility over cloud applications

In all, a 'perfect storm' of scenarios are combining to make it hard for organisations to sufficiently secure their cloud applications, a problem set to rise as cloud adoption expands.

55%

Of all surveyed respondents [400 respondents] think that cloud applications are among the biggest targets for cyber-attacks

56%

Of those [218 respondents] point to the increasing volume of cloud apps in use as the cause

55%

Feel that inconsistent security protection across cloud is the cause [218 respondents]

44%

Identify a lack of in-house skills to secure cloud applications [218 respondents]

43%

Feel that organisations having poor visibility over their applications is leading to their cloud applications being targeted [218 respondents]

Most organisations' security policies around access management have been influenced by recent breaches of consumer services

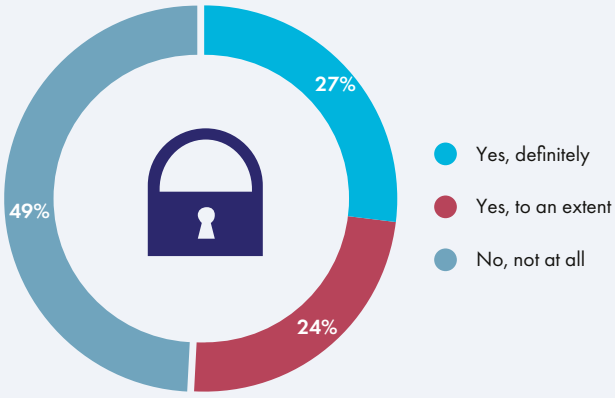
For instance, almost half of respondents tell us that staff are now trained on security and access management as a result of these high-profile breaches.

For some organisations, spending on access management has increased, or they now have a dedicated CISO.

Organisations are waking up to the threat posed by weak or ineffective access management procedures, although it is taking the misfortune of another organisation to prompt this change in approach.

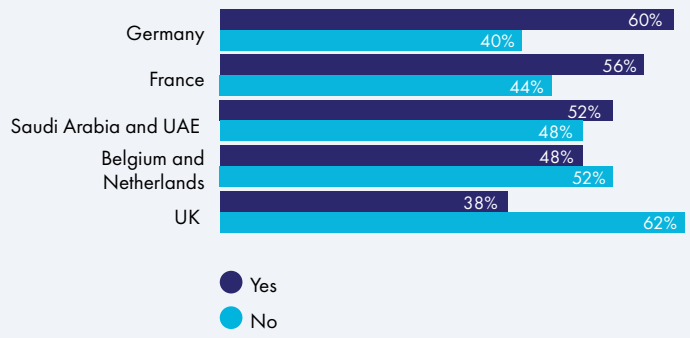
How have your organisation's security policies around access management been influenced by breaches of consumer services in the last 12 months?

Yet, many organisations still allow employees to log on to company resources using personal, social media credentials



In light of recent security breaches, would you allow employees in your organisation to log on to corporate resources using their social media credentials?

In particular, those in Germany are most likely to be more relaxed in this regard, with their counterparts in the UK being the least likely to allow this.

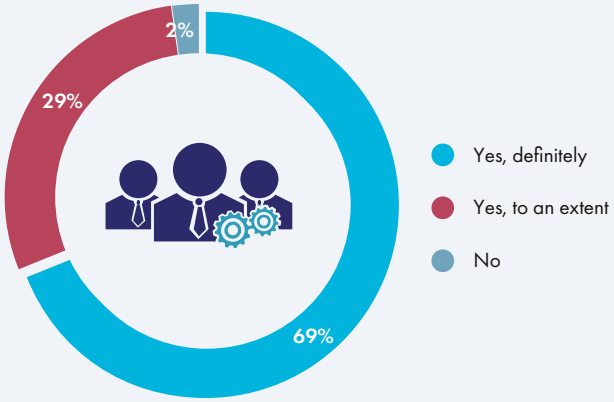


Showing respondents who would allow employees in their organisation to log on to corporate resources using their social media credentials vs. those who would not – split by respondent country

In order to comply with regulations, nearly all respondents agree that tighter controls over data access are needed

Among the respondents, it is those in Germany who are most likely to definitely think that this is true.

This is despite their more relaxed approach to allowing employees to log on to corporate resources using social media credentials.



Do you think controlling who has access to specific types of data can contribute toward your organisation's ability to comply with data protection regulations and pass security audits (e.g. GDPR)?

Showing respondents who think that controlling who has access to specific types of data can definitely contribute toward their organisation's ability to comply with data protection and pass security audits – split by respondent country

Also key to achieving regulatory compliance – a single, clear audit trail

99%

See it as important that their organisation has the ability to produce a single audit trail of access events taking place throughout different resources used by their organisation

36%

See it as **extremely** important

66%

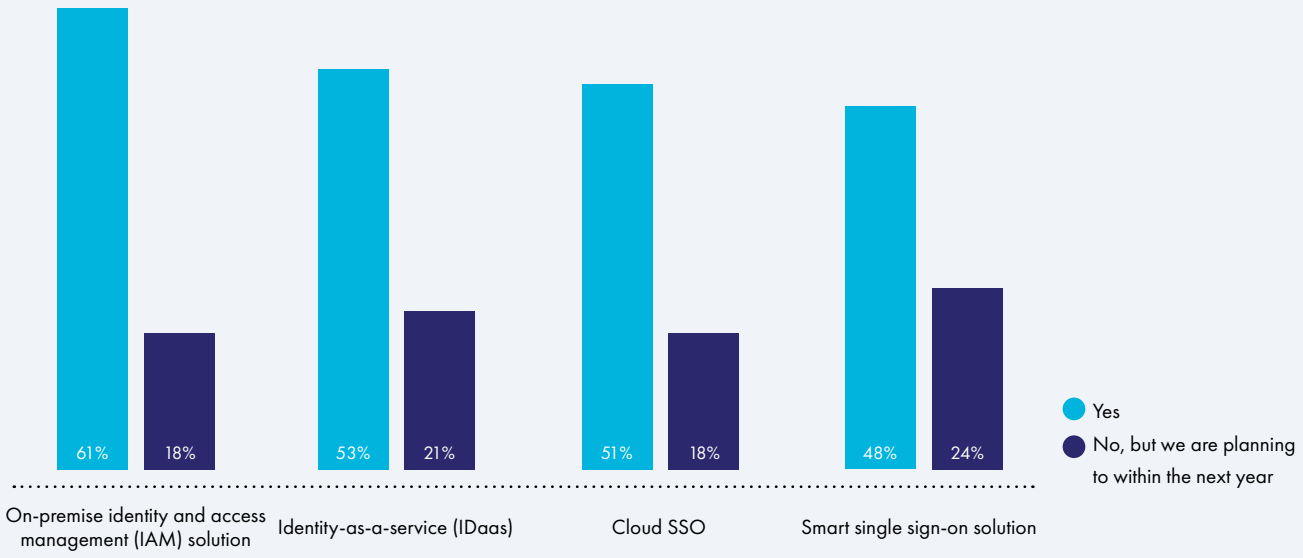
In **Saudi Arabia** and the **UAE**, two thirds see this as **extremely important**

Most have, or plan to, implement access management capabilities

On-premises identity and access management (IAM) is the most widely implemented, while IDaaS and cloud SSO are both already implemented by a slight majority.

And while smart SSO is the least likely to have already been implemented, almost a quarter plan to implement it within the next year, indicating its position as an emerging, growing solution.

Has your organisation implemented any of the following access management capabilities?

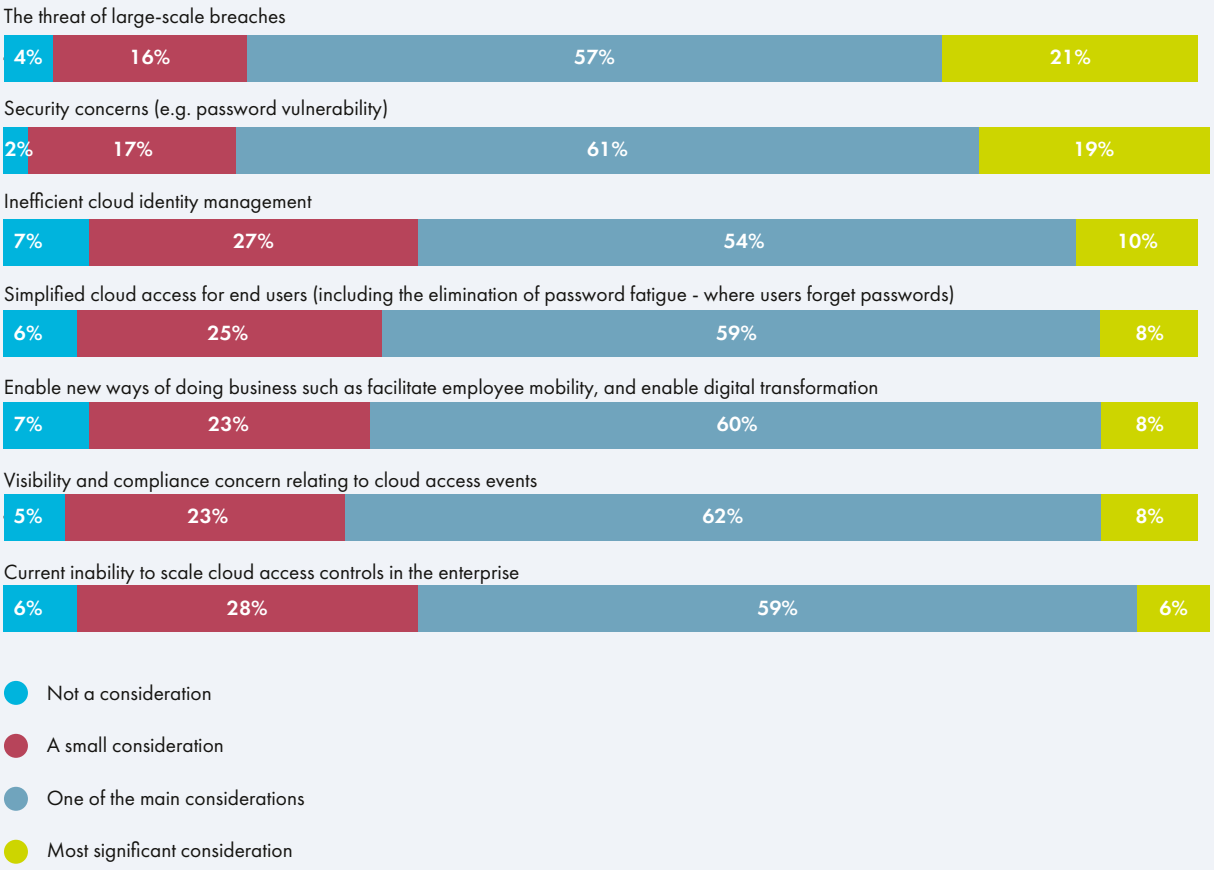


The dangers of large-scale breaches and security concerns are clear to many – and they are the primary drivers for implementing an access management solution

It seems that for many, access management is more of a reactive measure, something that they have implemented as a means to protecting themselves from cyber-attack and all of the risks that come with them.

While implementing an access management solution can be a means to simplify cloud access and enable new ways of doing business, it appears that these are both merely added bonuses once security has been taken care of.

Showing respondents who think that controlling who has access to specific types of data can definitely contribute toward their organisation's ability to comply with data protection and pass security audits – split by respondent country

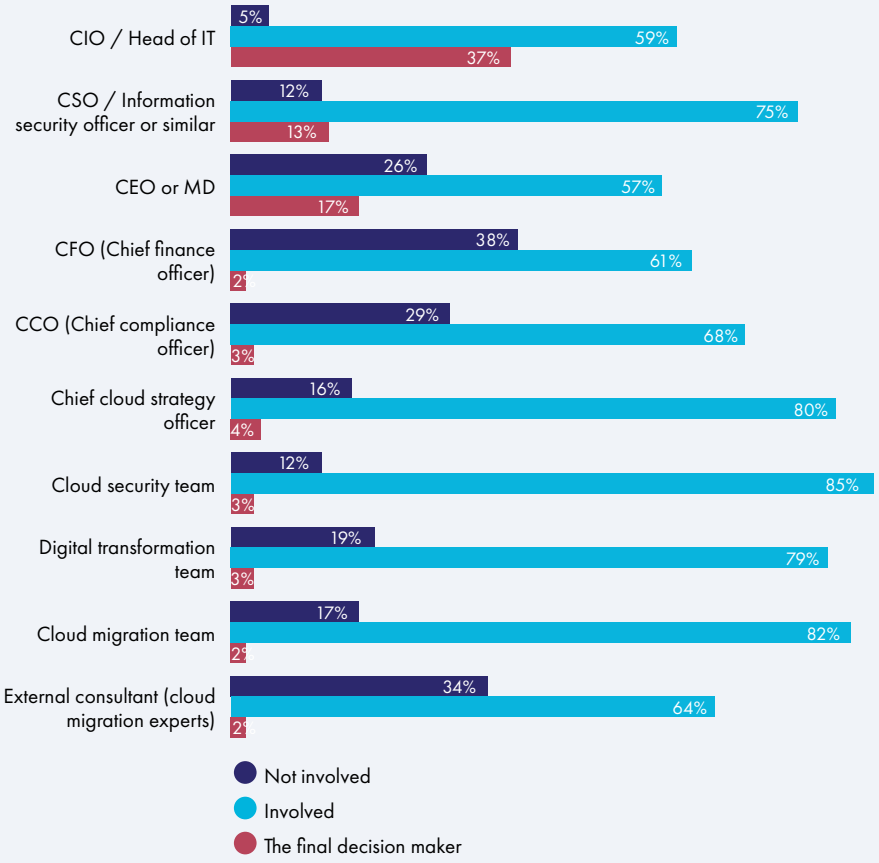


There are many voices in the decision-making process when selecting an access management solution

While the CIO is most likely to be the final decision maker when selecting an access management solutions, it is also likely that there will be a large number of other stakeholders also involved in the process.

That means that for a solution to be chosen, it needs to satisfy security, finance, compliance, and potentially cloud teams.

Who is involved, and to what extent, in the decision-making process when selecting an access management solution for your organisation?

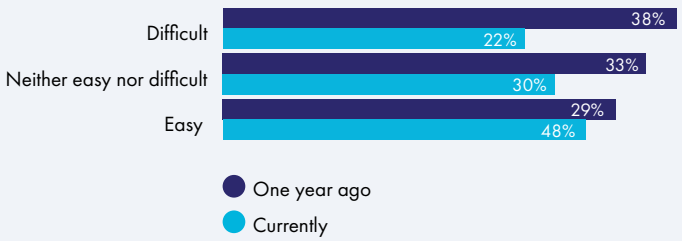


Selling the need for IT security to the board is easier now than it was 12 months ago

Despite people like the CEO, CISO, and CFO all likely involved in the decision making process when choosing an access management solution, at least they are more switched on to the need for security.

And given that security, or more specifically the threat of a large-scale breach is a key driver for implementing an access management solution, then there shouldn't be too many objections when deciding to implement a solution.

One downside however, is that while the board are all likely in agreement that they need a solution, choosing which one may be trickier!.



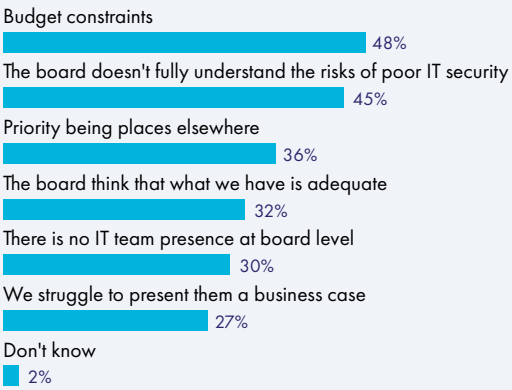
How easy or difficult do your organisation's IT leaders find it to sell the need for IT security to the board?

That's not to say that boards are going to allocate unlimited funds to an access management solution

Concerns around budget, and a general lack of understanding on the topic, are likely to make some boards reluctant to spend on IT security.

It is the job of a board to question why money is being spent on one thing or another, but with some having their priorities elsewhere perhaps the decision should be sitting with a more qualified team.

Especially as three in ten report that there is no IT presence at board level.



Why do/did your organisation's IT leaders find it difficult to sell the need for IT security to the board? [172] – respondents who are finding it difficult to sell the need for IT security to the board

02

Cloud Access Management is a priority

When it comes to protecting their organisation's cloud and web-based applications, respondents are more likely (53%) to find that two-factor authentication is best, compared to smart SSO (43%), biometrics (39%), or SSO (35%). However, it is a concern that almost three in ten (29%) still perceive username and password as best, despite its proven limitations.

Where respondents do agree is in the importance of cloud access management, with the vast majority (96%) seeing cloud access management for cloud and web applications as being conducive to facilitating cloud adoption. Just as telling is the 96% who report that there is/would be a negative impact on their organisation from ineffective cloud access management. Not only could cloud become a security issue (46%), but over a third report that IT staff's time would be used less efficiently (38%), increased operational overheads and IT costs (36%), and/or shadow IT taking place (34%). It is clear that cloud access management is an area where organisations have to be successful.

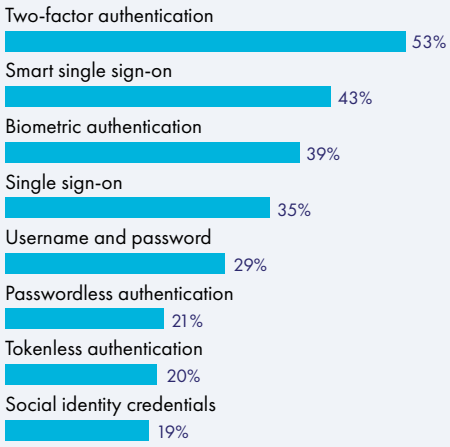
Yet, there are many challenges when addressing cloud-based security, that could potentially undermine the efforts of an organisation to sure up cloud access management. In fact, over nine in ten (94%) tell us that there are challenges. The most widely felt (35%) is the cost of a secure solution, but difficulty keeping up with new technology (31%), trouble integrating with other systems (30%), and/or a lack of clarity on the ownership of responsibility for cloud-based security (28%) are all challenges making their presence felt for around three in ten.

When it comes to protecting cloud and web-based apps, two-factor authentication is seen as best

Although over a third of respondents see the merit of smart SSO, biometrics, or SSO.

Slightly worrying is that almost three in ten think the best way to protect cloud and web-based applications is through username and password – an approach with known vulnerabilities.

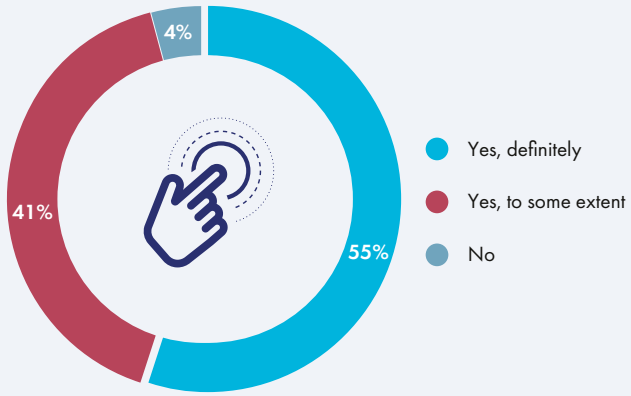
Interestingly, fewer than a fifth of respondents think that social identity credentials is best – almost half allow this type of authentication for company resources.



In your opinion, which of the following access management tools are the best at protecting cloud and web-based applications?

Want to adopt more cloud services? Then sorting out your cloud access management strategy is key

Nearly all respondents see cloud access management for cloud and web applications as being conducive to facilitating cloud adoption.



Do you see cloud access management for cloud and web applications as being conducive to facilitating cloud adoption?

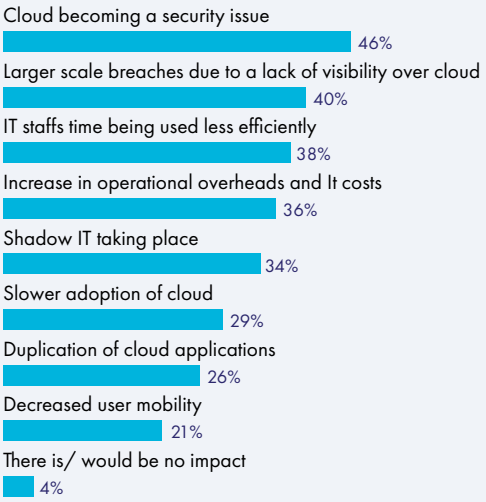
This view is particularly widely held in Saudi Arabia and the UAE, and far less so in the UK.

Showing respondents who think that cloud access management for cloud and web applications is definitely conducive to facilitating cloud adoption – split by respondent country

Ineffective cloud access management could ultimately lead to cloud becoming a security issue

But that's not all, as for some, it could also lead to IT staff's time being used less efficiently, or even shadow IT taking place. By failing to correctly manage cloud access management some organisations are unable to get the most out of its cloud and web resources.

And these negative impacts, such as an increase in operational overheads and IT costs may grow into a more significant challenge when trying to improve cloud access management.



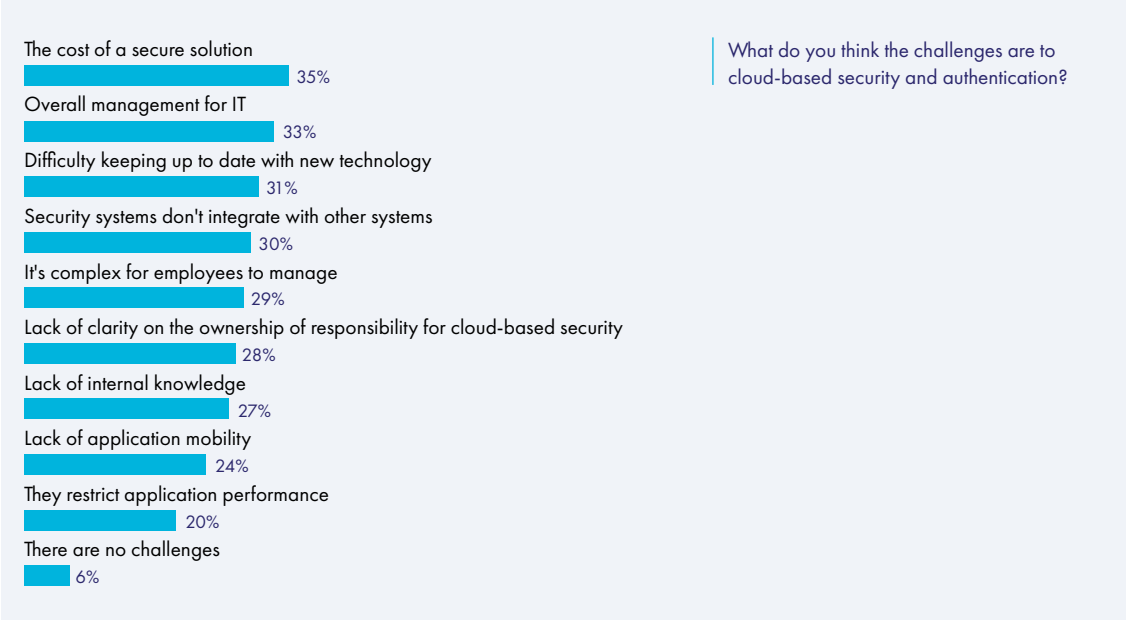
What impacts does/ could your organisation see to its cloud and web resources as a result of ineffective cloud access management?

There are many challenges when addressing cloud-based security

The cost of a secure cloud-based security and authentication solution is a challenge for over a third of respondents.

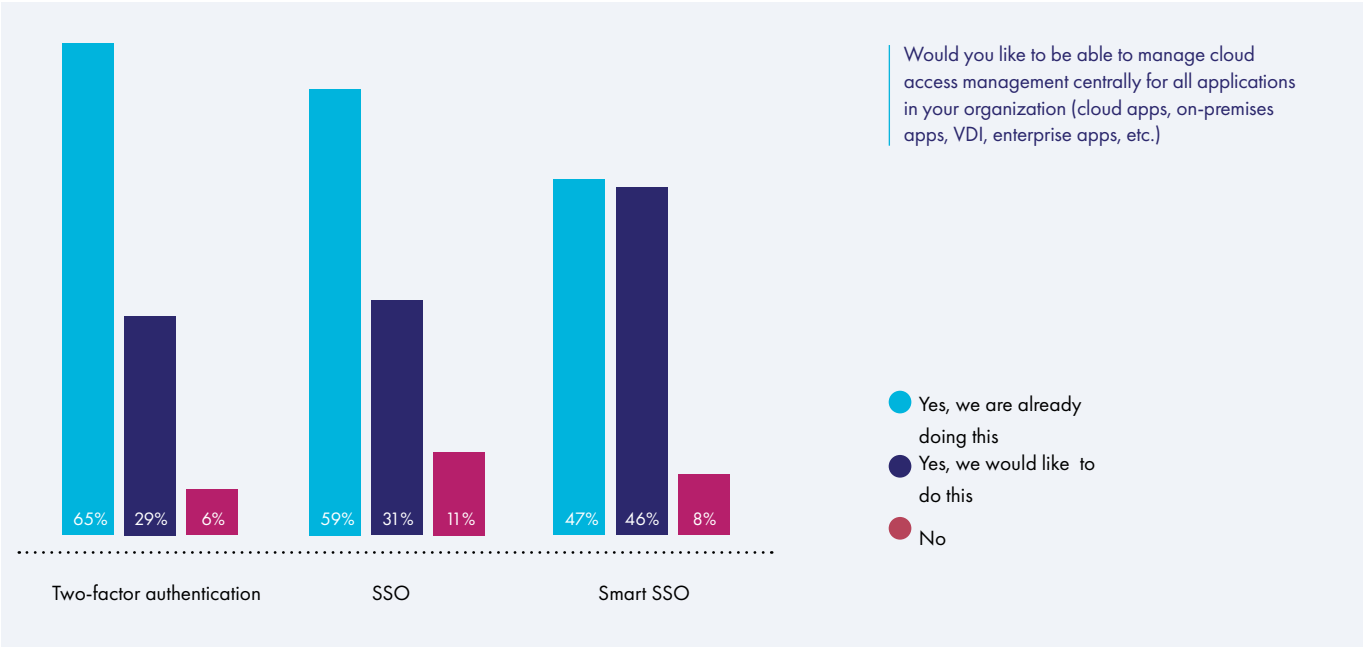
However, given the impacts of ineffective cloud assessment management, perhaps this is an outlay that organisations will find will earn itself back in savings.

But some of the other widespread challenges will need addressing, in particular integrating security solutions, complexity to manage, lack of clarity regarding ownership, and a lack of internal knowledge.



There is also a desire among respondents to manage cloud access management centrally

The majority of respondents are already managing their two-factor authentication and SSO centrally. While fewer are already doing this for smart SSO, approaching half report that they would like to, indicating the future trajectory of the management of this authentication method.



03 Multi-Factor Authentication Trends

The majority of respondents' organisations plan to expand their use of various types of two-factor authentication, including but not limited to smart SSO (81%), biometrics (75%), software tokens (73%), passwordless authentication (70%), and/or hardware tokens (68%).

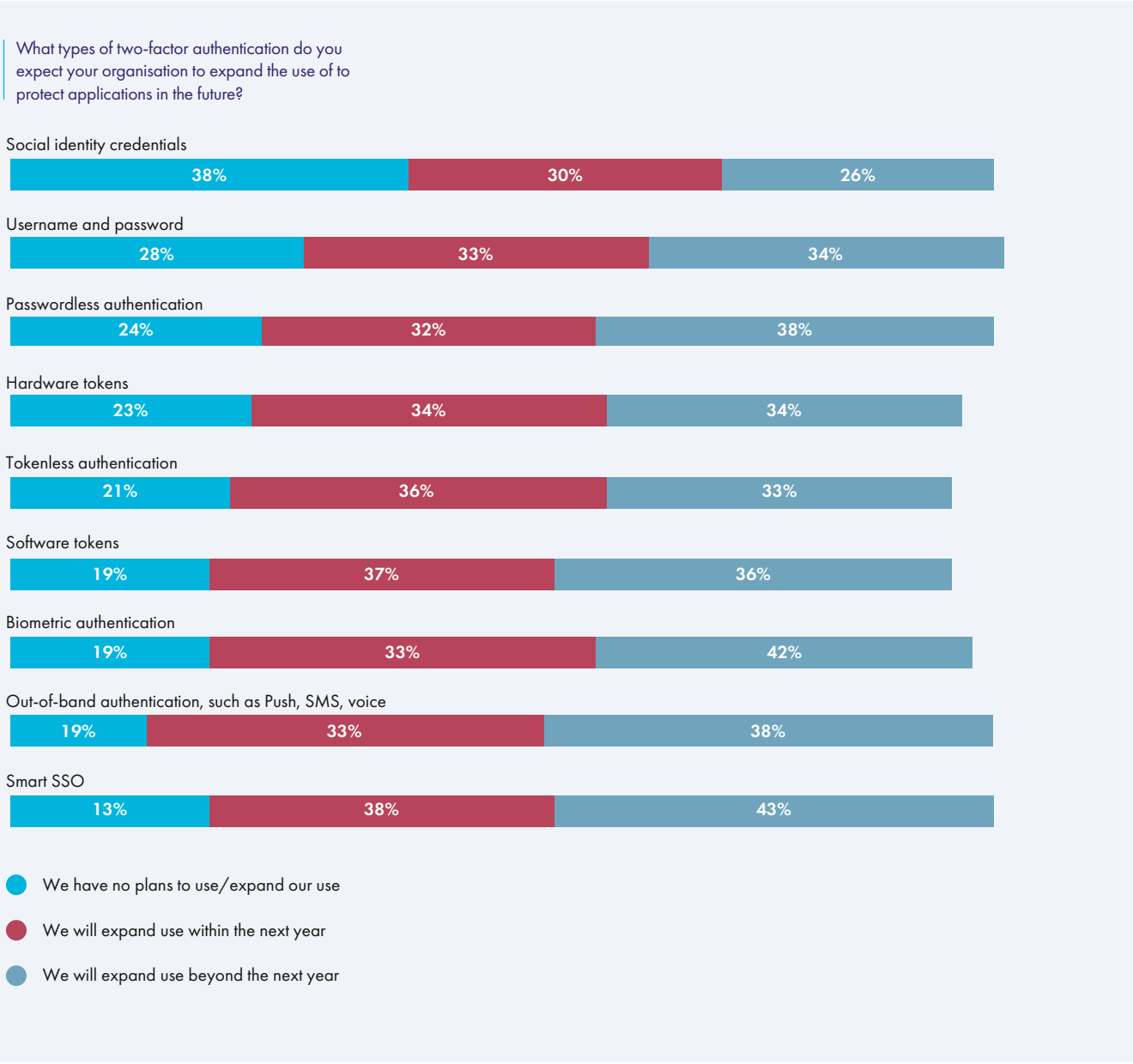
Among those whose organisation is planning such an expansion in at least one form of two-factor authentication, respondents are pretty split as to how they will achieve this expansion. Just over half (52%) will use a dedicated multi-factor authentication solution, while four in ten (40%) will use an IDaaS/access management solution.

When it comes to deciding which type of two-factor authentication to deploy, perhaps it is a good idea to look at who in particular will be the primary user, as respondents tell us that different types of two-factor authentication suit different employees. For instance, when it comes to employees outside of IT respondents are most likely (38%) to think that username and password fits best, while hardware (48%) or software (48%) tokens best suits IT staff. And as for the c-suite, biometrics is the form of two-factor authentication that best suits (30%) these busy employees.

For most, use of various types of two-factor authentication is set to increase in the future

Approaches such as hardware or software tokens, biometrics, and smart SSO are all set for increase, but so is the seemingly out of date username and password approach.

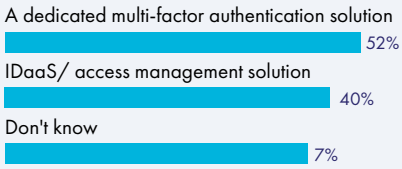
Least likely to see an increase is the use of social identity credentials, underlining the polarising nature of this approach that means that half allow it and half do not.



Respondents are split on how best to expand their two-factor authentication

While over half plan to use a dedicated multi-factor authentication solution, a significant minority plan to use IDaaS/access management solution.

But whatever the approach, the solution must be adaptable to organisations' needs, given that there is expected growth in a number of different types of two-factor authentication.

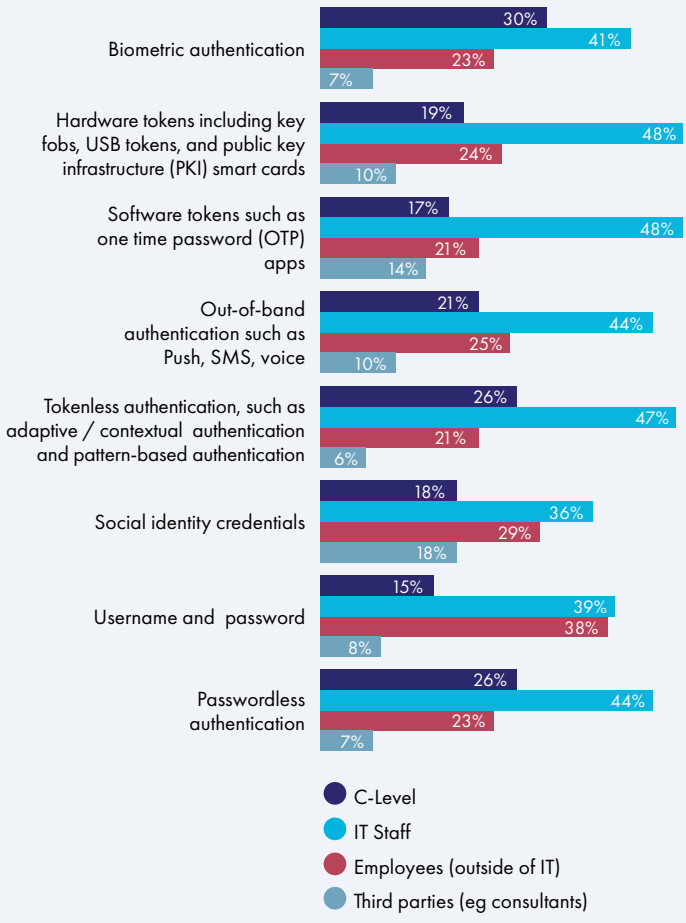


How does your organisation plan to expand its use of two-factor authentication? – respondents whose organisation is planning to expand the use of at least one type of two-factor authentication

Different types of two-factor authentication suits different employees

While username and password authentication is among the least appropriate for IT staff, according to respondents, it is at the same time considered the most appropriate for non-IT employees.

Respondents are more likely to consider hardware and software tokens as more appropriate for IT staff, while biometrics is seen as best for members of the c-suite. But can an organisation implement and manage all of these different types of solution?



Which type of authentication methods best suits which stakeholders for your organisation?

04

Smart Single Sign-On (SSO) on the Rise

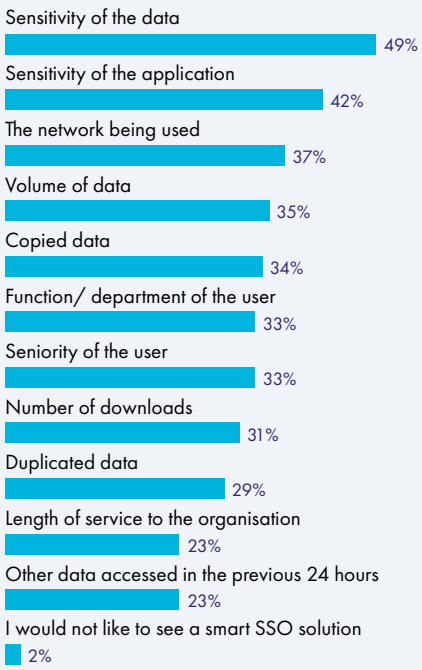
Nearly all (98%) respondents would like to see a smart SSO solution in use in their organisation. And this trend continues with another overwhelming proportion (99%) who report that there are/would be benefits to their organisation implementing smart SSO.

In order to achieve a more secure smart SSO, over a quarter (28%) of respondents would allow their organisation to collect and hold any of their personal data, while 43% would allow much more data to be used, but nothing sensitive. Only a minority (14%) would be against their organisation holding any more data about them, indicating that the prevailing view is that a secure smart SSO is worth providing more personal data for.

Nearly all respondents would like to see a smart SSO

On average they want to see four different types of data and information associated with the parameters of smart single sign on. At the forefront is the data itself, with respondents more likely to want to see things such as the sensitivity of the data, sensitivity of the application, volume of the data, and copied data taken into account than certain information about the user.

In fact, the function/department of the user, the seniority or the user, and the length of service to the organisation are all less likely to be desired in a smart SSO by respondents.



Which of the following types of data/information would you like to see used in a smart SSO solution?

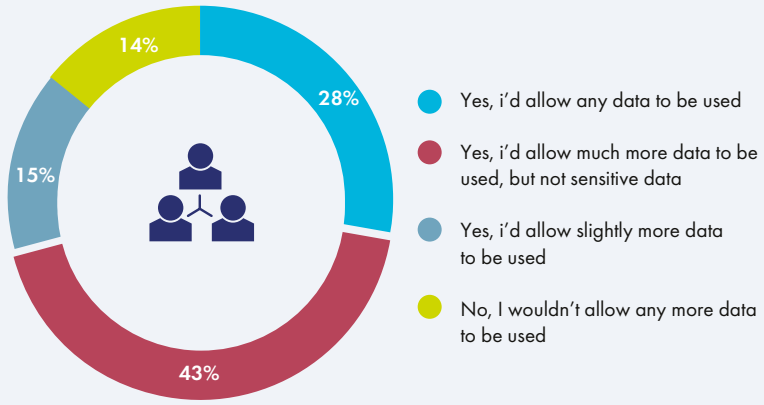
Almost all organisations see benefits from using smart single sign on

The leading benefits for smart SSO are breach prevention, ease of use for users, and more secure than traditional single sign on

What are/would be the benefits of your organisation using smart SSO?

For most, a secure, smart, SSO solution is worth providing more personal data for

However, it is only a minority who would allow any data to be used, indicating that there is some level of caution from respondents when sharing personal data, no matter what the cause.



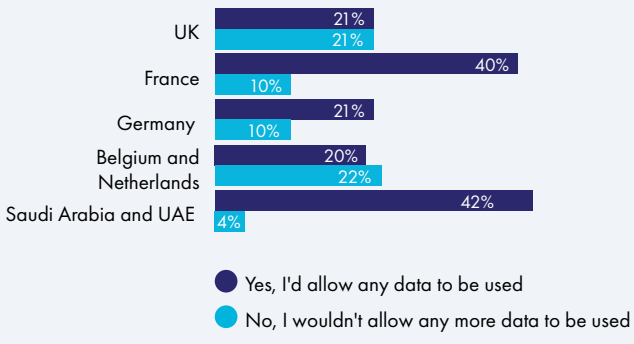
Would you be willing for your organisation to collect and hold more data about you if it resulted in a secure smart SSO solution?

When it comes to providing more data for a smart SSO, respondents in some countries are more willing than others

Respondents in France and the Middle East are far more likely to allow any data to be collected and held if it resulted in a secure smart SSO.

Those in Germany, the UK, or Belgium and the Netherlands are far less compliant, with those last three markets being far more likely to not allow any data to be used.

For many this decision is a balancing act, weighing the pros vs. the cons of allowing the collection and use of their personal data. And it's a very personal decision, depending more on the individual than the organisation that they work for.



Showing the percentage of respondents who would be happy for their organisation to collect and hold more data about them if it resulted in a secure smart SSO solution vs. those who wouldn't allow any data to be used – split by respondent country

Next Steps and Guidelines

As noted in the previous sections of this paper, the majority of respondents agree that cloud access management is conducive to facilitating cloud adoption, and most of them plan to expand the use of various types of multi-factor authentication. Nearly all (98%) respondents would like to see a smart SSO solution in use in their organization.

From a practical perspective, what should the next steps be and what considerations should IT professionals take into account when selecting an Access Management and Authentication solution? Below are a few recommendations.

1. **Efficiency and Deployment**
   A cloud-based solution will allow you to get up and running quickly without the need for heavy on premises installations. When assessing your solution, it is advisable to check how many on-premises components you will need to install, and how many servers you will need, and how the additional servers you'll need in order to maintain redundancy.

2. **Automation**
   It is recommended to subscribe to a service that offers automated token enrollment workflows and one-click token installment for end users, your organization will be able to self-enroll quickly and reduce IT burdens.

3. **Authentication and Token Flexibility**
   To support all users' needs, look for a solution that can offer a range of authentication methods that can accommodate varying needs and security levels. These include: Push OTP app (which can be installed on a mobile device or desktop); SMS or email code sent to a mobile device or email address; pattern-based authentication, or a token-less method that does not require users to install any software on an end device.

4. **Ability to Access all Apps and Cloud Services**
   Look for a solution that can secure access to apps via SAML, RADIUS and non-standards-based apps and avoid any solution that can only secure cloud and web-based apps. This way you will be able to protect all apps with a single solution and offer convenience with single-sign-on.

5. **Smart SSO for Optimal Security and Convenience**
   To offer the most frictionless experience possible without sacrificing security, organizations can leverage cloud SSO combined with contextual information and step-up authentication. This allows users to access all their cloud and web applications with a single identity, while IT only needs to enforce stronger access security in high-risk situations.

6. **Provide Flexible Policies**
   By subscribing to a cloud access management service with flexible policies, you will be able to step up authentication for untrusted networks and ease the level of authentication method required for the trusted networks and devices.

7. **Transparent Licensing Model**
   Many services have very complicated pricing models. A dedicated access management and authentication solution with a transparent pricing model which includes the features you need will allow you to easily analyze and forecast costs moving forward.

Conclusion

As more and more businesses move to adopt cloud-based services for CRM, email, employee collaboration and IT infrastructure as part of their digital transformation strategies, the struggle to extend old solutions, designed to protect internal resources, to the outside world becomes very problematic. Often, in an effort to adapt to the new working habits of users connecting from anywhere, businesses tend to revert back to old password-based logins for cloud services in despair, knowingly increasing their security exposure through credential stuffing and phishing attacks.

For a long time, the biggest battle IT leaders have faced is increasing board awareness around taking security threats seriously. Now they have that buy in, the focus should be on highlighting to the powers that be, the importance access management plays in implementing a Zero Trust security policy. With this in place, risk management professionals will be able to put in place a 'Protect Everywhere - Trust Nobody' approach as they expand in the cloud.

THALES

Americas
Arboretum Plaza II, 9442 Capital of Texas Highway North,
Suite 100, Austin, TX 78759 USA
Tel: +1 888 343 5773 or +1 512 257 3900
Fax: +1 954 888 6211 | E-mail: sales@thalesesec.com

Asia Pacific
Unit 4101-3, 41/F, Sunlight Tower, 248 Queen's Road East
Wanchai, Hong Kong | Tel: +852 2815 8633
Fax: +852 2815 8141 | E-mail: apacsales.cpl@thalesgroup.com

Europe, Middle East, Africa
350 Longwater Ave, Green Park,
Reading, Berkshire, UK RG2 6GF
Tel: +44 (0)1844 201800 | Fax: +44 (0)1844 208550
E-mail: emea.sales@thales-esecurity.com

cpl.thalesgroup.com/euro-access-management-index