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
United States & Brazil Edition

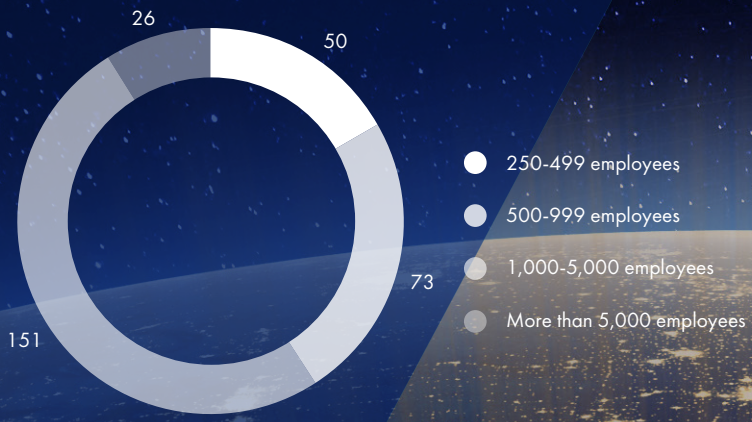
About this study

The 2020 Access Management Index - United States / Brazil Edition, is a survey of **300 IT professions across the U.S. and Brazil** with responsibility for, or influence over, IT and data security.

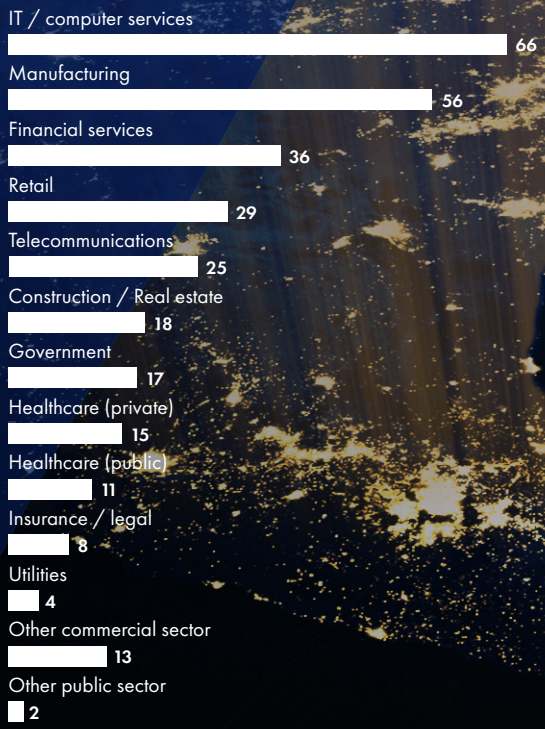
The survey, reporting and analysis was conducted by Vanson Bourne, commissioned by Thales.

VansonBourne

Organization size



Organization sector



Contents

Sponsored by

KEYFACTOR
SECURE EVERY DIGITAL IDENTITY

SENETAS

FIRST TECH

TI Safe

f5

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 organization 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 match. 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 SSO and cloud access management tools. We aim for this to be informative and educational, while inspiring best practice.

Key Findings

Weakest Link Still Prevails

41%

of respondents believe usernames and passwords are one of most effective access management tools despite known weaknesses

65%

believe that unprotected infrastructure present the biggest targets for cyber-attacks

94%

reveal that data breaches in the last 12 months have influenced their organization's security and access management policies

Balancing Security and Convenience

58%
allow employees to log on to corporate resources using social media credentials

28%
view social media credentials as one of the best tools for protecting cloud and web-based authentication

88%
cite security concerns and/or the threat of a large-scale breach (**84%**) as factors most likely to drive companies to have implemented, or plan to implement, an access management solution

Access Management is Essential for Cloud Transformation

98%

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

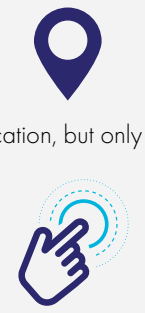
97%

anticipate problems for their organization if every cloud application in use is not secured properly

Strong Awareness for Better Access Control

95%
report they have implemented multi-factor authentication, but only

15%
say they use a dedicated multi-factor solution



59%
have adopted Smart Single Sign-on technology, with

85%
are using it or planning to further expand use of this technology in the next year

01 General access management

Almost two thirds (65%) of respondents in the Americas identify unprotected infrastructure/devices as a top target for cyber attackers. Over half think that cloud applications (54%), and/or web portals (54%) are top targets. This proliferation of targets may be why most (65%) respondents find it easy to sell the need for IT security to the board, an increase from 44% who were finding it easy 12 months ago.

According to those respondents who think that cloud applications are a top target for cyber-attackers, the most likely cause for this is the increasing volume of applications in use (59%). As organizations move more and more processes to cloud, and more cloud applications are adopted, it is essential that each application is properly secured.

For almost all (99%) respondents in the Americas controlling who has access to specific types of data is important in contributing toward their company's ability to comply with data protection regulations. However, over half (58%) of respondents would still allow employees of their organization to log on to corporate resources using social media credentials. It may be that allowing employees to do this, they may be undermining their ability to control that access to corporate resources.

The world of access management is ever changing – the vast majority (94%) of respondents in the Americas report that their organization's security policies around access management have been influenced by breaches of consumer services in the last 12 months. For half (50%) secure access management is now a priority for the board, meaning that for some their board only became alive to the dangers of poor access management after seeing other businesses fall foul of it.

That said, a majority of respondents' organization have implemented various access management solutions such as on-premises IAM (68%), cloud SSO (62%), IDaaS (60%), and/or smart SSO (59%). While a smart SSO appears to be the least widely implemented, over a quarter (26%) plan to implement one within the next year.

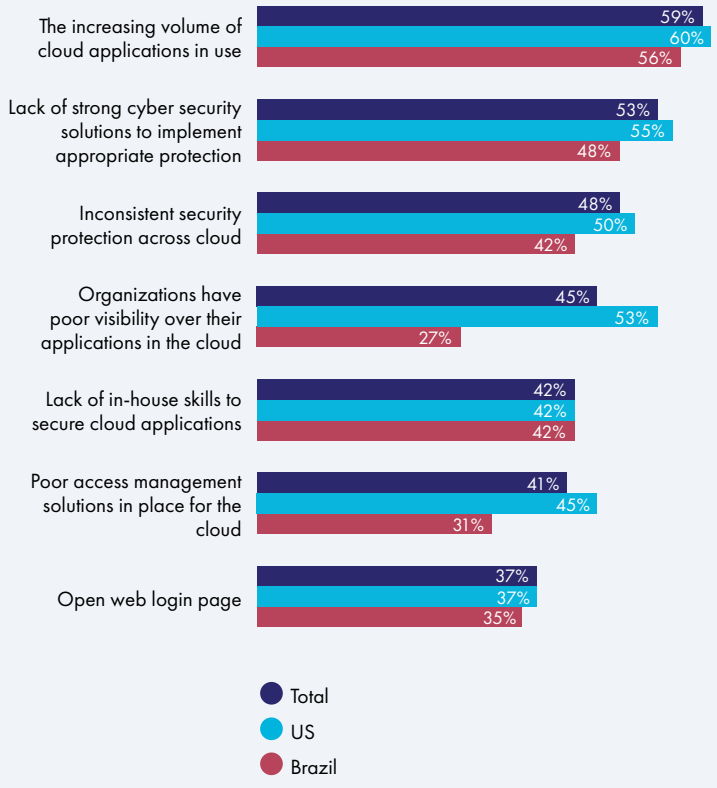
Security concerns (88%), and/or the threat of a large-scale breach (84%) are the factors most likely to be driving organizations in the Americas to have implemented, or plan to implement, an access management solution. Again, this highlights the reactive approach that many companies are taking, reacting to what is happening to other organizations, out of fear of the same happening to them.

There are many reasons why cloud applications may be the target of cyber-attackers

For a majority of respondents who feel that cloud applications are a target for cyber-attacks, it is the increasing volume of these applications in use that is placing these applications in peril, a perfect example of the tightrope that organizations have to walk as they adopt and role out new technologies.

But perhaps most interesting of all is the divergence between respondents in the US vs. those in Brazil when it comes to poor visibility and poor access management solutions – those in the US are far more likely to see these as a reason for cloud applications being targeted, perhaps indicating where respondents feel that their organization is falling short.

Why do you feel that cloud applications are a target for cyber-attacks?



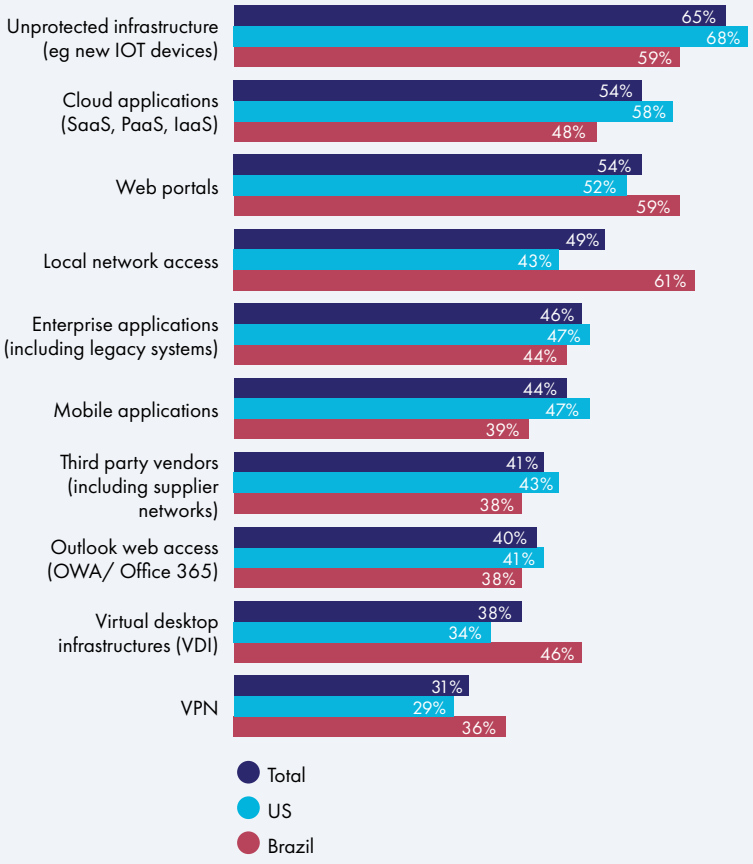
According to respondents, a number of business areas are potential targets for cyber-attacks in 2020

Nearly all respondents from the Americas fear that particular areas of their organization are prime targets for cyber-attackers.

Particular areas of concern include, but are not limited to unprotected infrastructure, cloud applications, and web portals.

Respondents in Brazil are especially concerned about local network access, while those in the US are more likely to be worrying about mobile applications, perhaps an indication as to their importance to respondents' organizations in this market.

Which of the following do you think are the biggest targets for cyber-attacks?

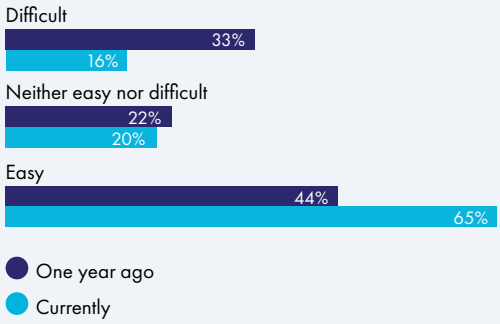


As a result, it has become easier than ever to sell the need for IT security to the board

With more and more areas of the organization at potential risk of cyber-attack, respondents are more likely to be finding the board of directors at their organization more receptive to the need for IT security now than they were one year ago.

Among those who used to find it difficult to sell IT security to the board, or who still do to this day, the primary reasons for this difficulty is priority being placed elsewhere, or budget constraints.

IT security used to be a 'nice to have' but this is no longer the case – what can be of more importance to an organization than the security of its IP and data?



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

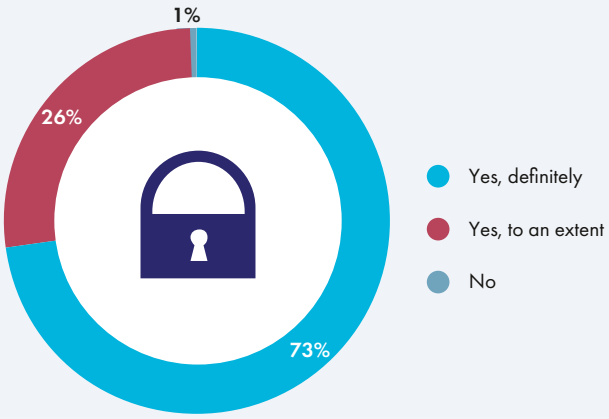
Why do/did your organization's IT leaders find it difficult to sell the need for IT security to the board? [110] – respondents who are finding it difficult to sell the need for IT security to the board

Access control is important for data protection compliance, but social media credentials are still being used to log on to corporate resources

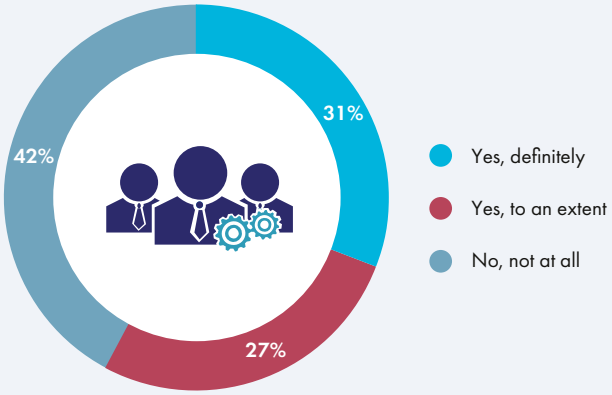
Nearly all companies feel that controlling access to specific types of data will contribute towards data protection compliance, even though almost two thirds would still allow employees to use their social media credentials to log onto corporate resources.

Should these social media credentials be undermined in some way, or if they are simply less secure, then organizations are opening themselves up to risk.

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



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

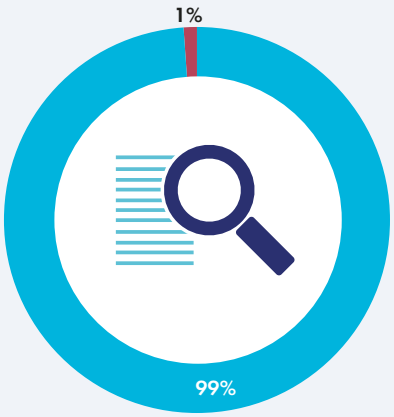


Single audit trails are important to organizations, as security policies evolve in response to recent events

Half of respondents report that secure access management is now a priority for the board in light of recent breaches of consumer services in the last 12 months, while a similar proportion are now training staff of security and access management.

As cyber security becomes more and more prominent in the minds of business leaders, so too does access management with resources being diverted toward improving it.

To what extent is it important that your organization has the ability to produce a single audit trail of access events taking place throughout different resources used by your organization?



- Important
- Not at all important

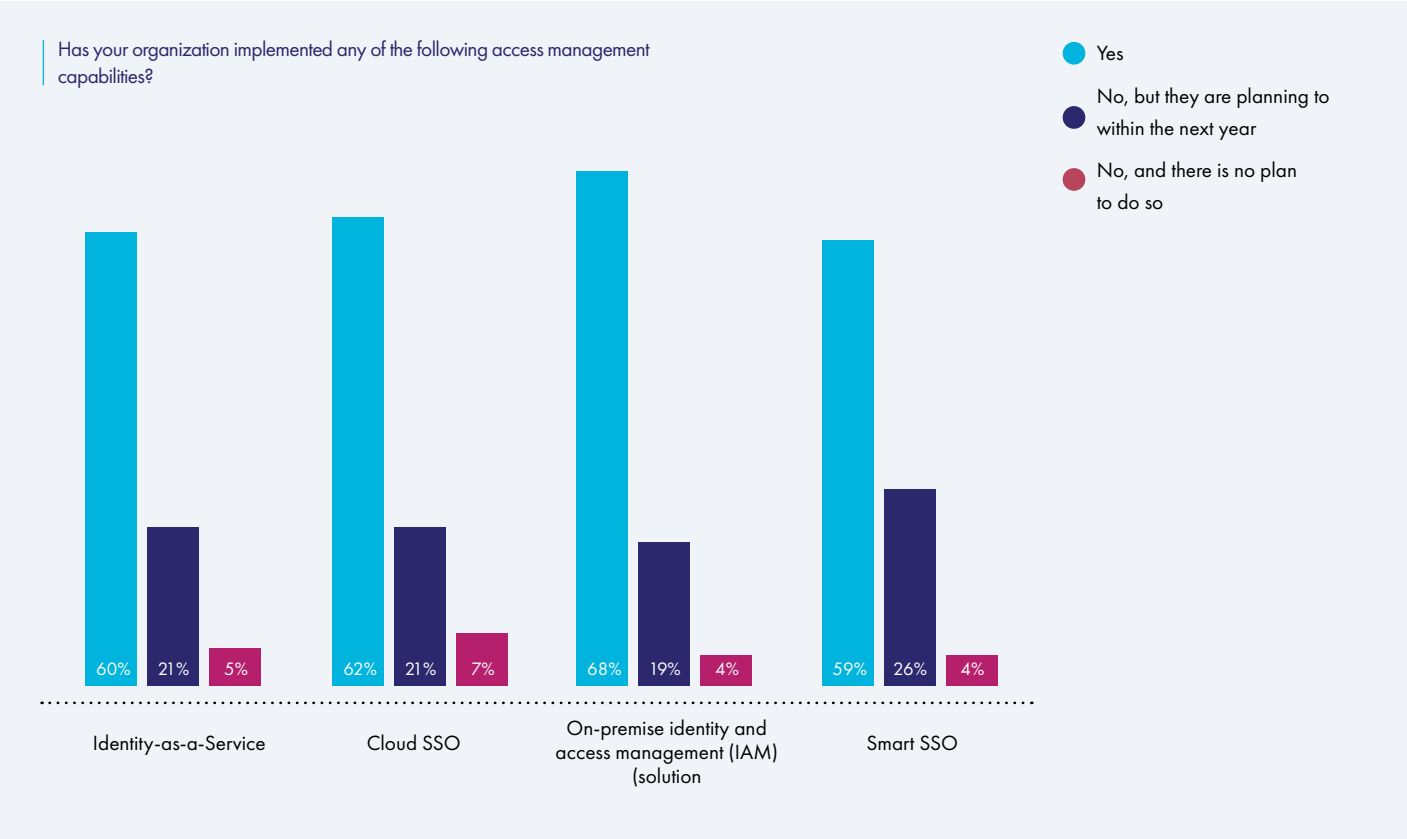
How have your organization's security policies around access management been influenced by breaches of consumer services in the last 12 months?

Companies are implementing a variety of access management capabilities

There are a variety of access management capabilities available to organizations, with an on-premise IAM solution proving to be the most popular choice currently among respondents.

However, the utilization of solutions such as smart SSO and cloud SSO are set to increase over the course of the next year.

In a world where the need for renewal and increasing complexity of passwords increases the risk of them being forgotten, solutions such as cloud SSO and smart SSO will become more vital for companies.



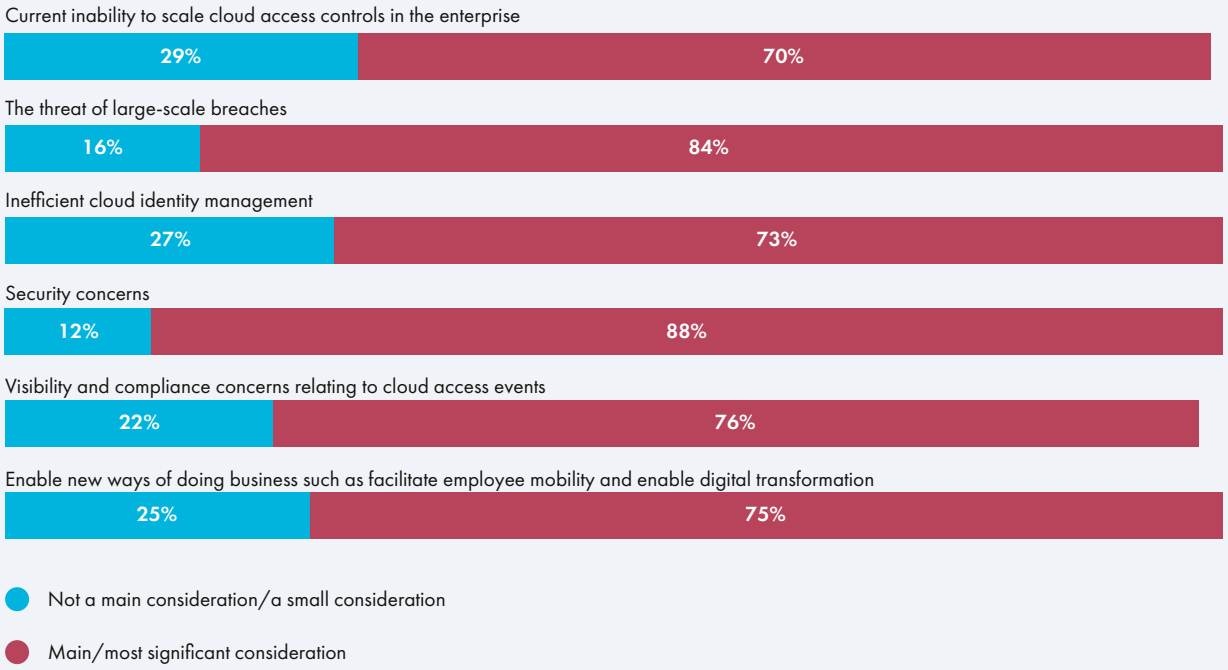
The threat of large-scale breaches and security concerns are driving organizations towards implementing an access management solution

Access management solutions are here to improve security, but they can offer much more than that – streamlining and simplifying access processes and allowing businesses to embrace new technologies such as cloud, and new ways of working, such as remote working are all within reach with the right solution.

However, when the discussions start surrounding using access management solutions, it is that security element that speaks loudest.

Vendors will perhaps encounter more success when selling these solutions if they put the security message front and center.

What are the main drivers for implementing an access management solution in your organization?



02
Cloud access management

When it comes to protecting cloud and web-based applications, respondents are most likely to feel that two-factor authentication (64%) is the best approach. However, it is worrying that over four in ten (41%) feel that username and password is one of the best tools, despite the many failings of this method of authentication.

Also, only 28% see social media credentials as one of the best tools for protecting cloud and web-based authentication, despite a far larger proportion being willing to allow employees to use social media credentials to access corporate resources.

Regardless of how they protect it, effective cloud access management is essential for organizations. If this is not done, nearly all (97%) respondents anticipate problems for their company. Chief among these is IT's staff being used less efficiently (53%), cloud becoming a security issue (47%), and an increase in operational overheads and IT costs (45%). In short, effective cloud access management makes organizations more secure for less work and money.

Yet, cloud-based security and authentication also presents challenges for the overwhelming majority (95%) of respondents' organizations. If left unabated, they may manifest into the challenges that businesses set out to avoid by investing in it. For instance the overall management by IT of cloud-based security and authentication is seen as a challenge for almost half (47%) of respondents. If unresolved, this could lead to IT's staff being used less efficiently, the most widely recognized outcome from ineffective cloud access management.

Cloud access management is simply unavoidable, almost all (98%) see it as conducive to facilitating cloud adoption. And once adopted, respondents in the Americas prefer to manage it centrally for two-factor authentication (77%), SSO (64%), and/or smart SSO (50%).

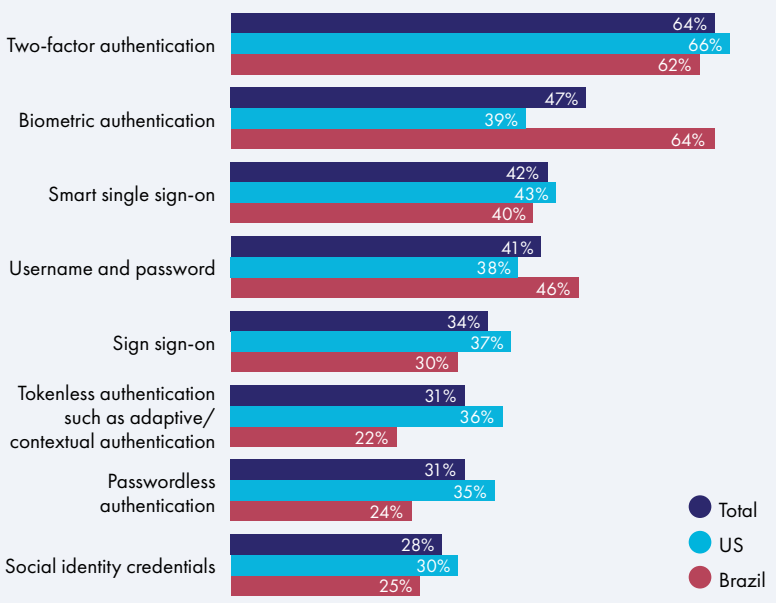
Two-factor and biometric authentication stand out as the best tools for protecting cloud and web-based applications

Respondents in Brazil are thoroughly bought into the idea of biometric authentication. On one hand, this would indicate a high level of maturity among respondents in Brazil compared to those in the US, but on the other hand respondents in Brazil are more likely to identify username and password as one of the best methods of protecting cloud and web-based applications than their US counterparts.

Intriguingly, despite most respondents willing to allow employees to log onto corporate resources using social media credentials, these are least likely to be rated as one of the best ways to protect these same resources.

> "As organizations move more and more processes to cloud, and more cloud applications are adopted, it is essential that each application is properly secured"

The best access management tools for protecting cloud and web-based applications



Regardless of how you protect it, effective cloud access management is essential

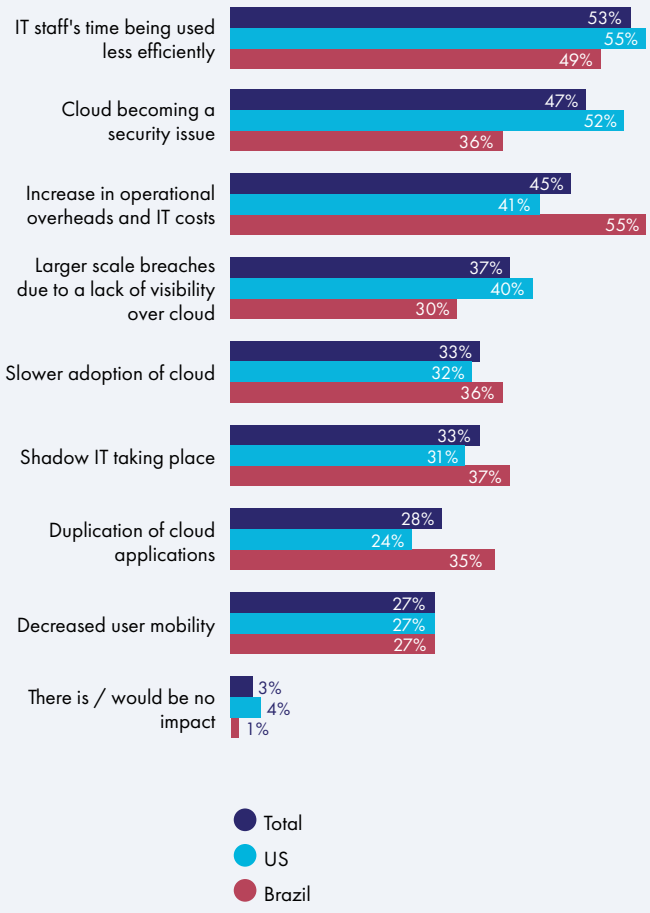
Reflecting on the growing importance of cloud to the average business, nearly all respondents foresee impacts to their organization's cloud and web resources as a result of ineffective clod access management.

Yet when defining what these impacts may be there is a difference between respondents in the US and Brazil, giving a key insight into these markets.

In the US, respondents are more likely to foresee cloud security becoming an issue as a result of ineffective cloud access management, indicating just how highly these respondents regard cloud security and its importance to their company.

Meanwhile, those in Brazil are more likely to foresee operational and IT costs increasing, shining a light on the priorities of these respondents' organizations.

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



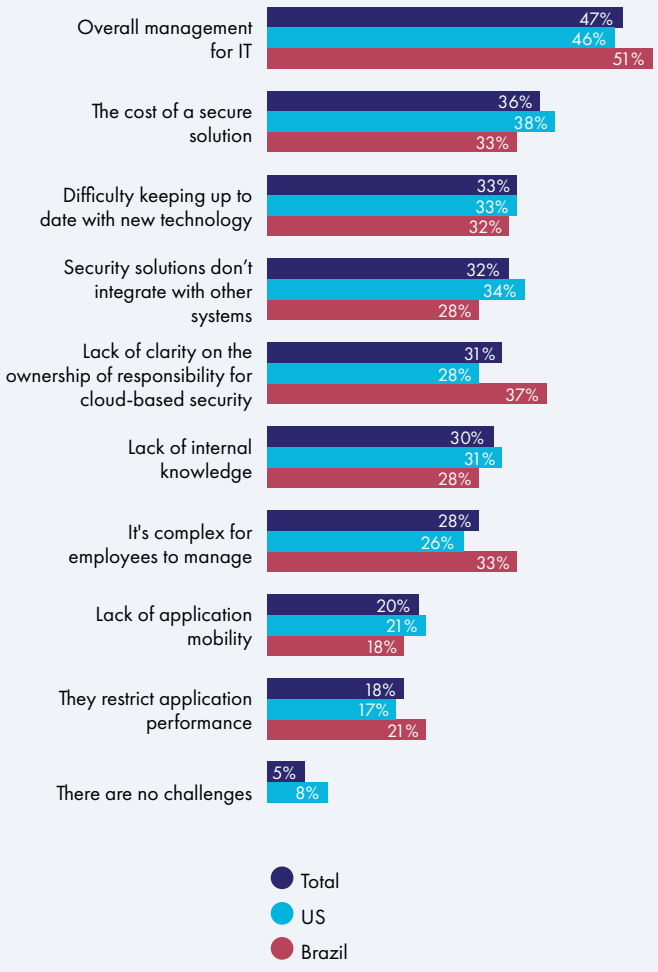
Cloud-based security and authentication also presents challenges

While these challenges pale in comparison to the impacts of simply neglecting cloud-based security and authentication, if left unabated they will only lead to potential issues becoming reality.

And the data here is intrinsically linked to the issues faced from ineffective cloud access management – for instance the overall management of cloud-based security and authentication by IT is the most widely experienced challenge, which if not corrected will lead to IT employees' time being used less efficiently, the most widely foreseen impact.

Interestingly, the security measures restricting application performance is the least widely experienced challenge, indicating that there is nothing inherently wrong with the solutions, rather how organizations are interacting and using them.

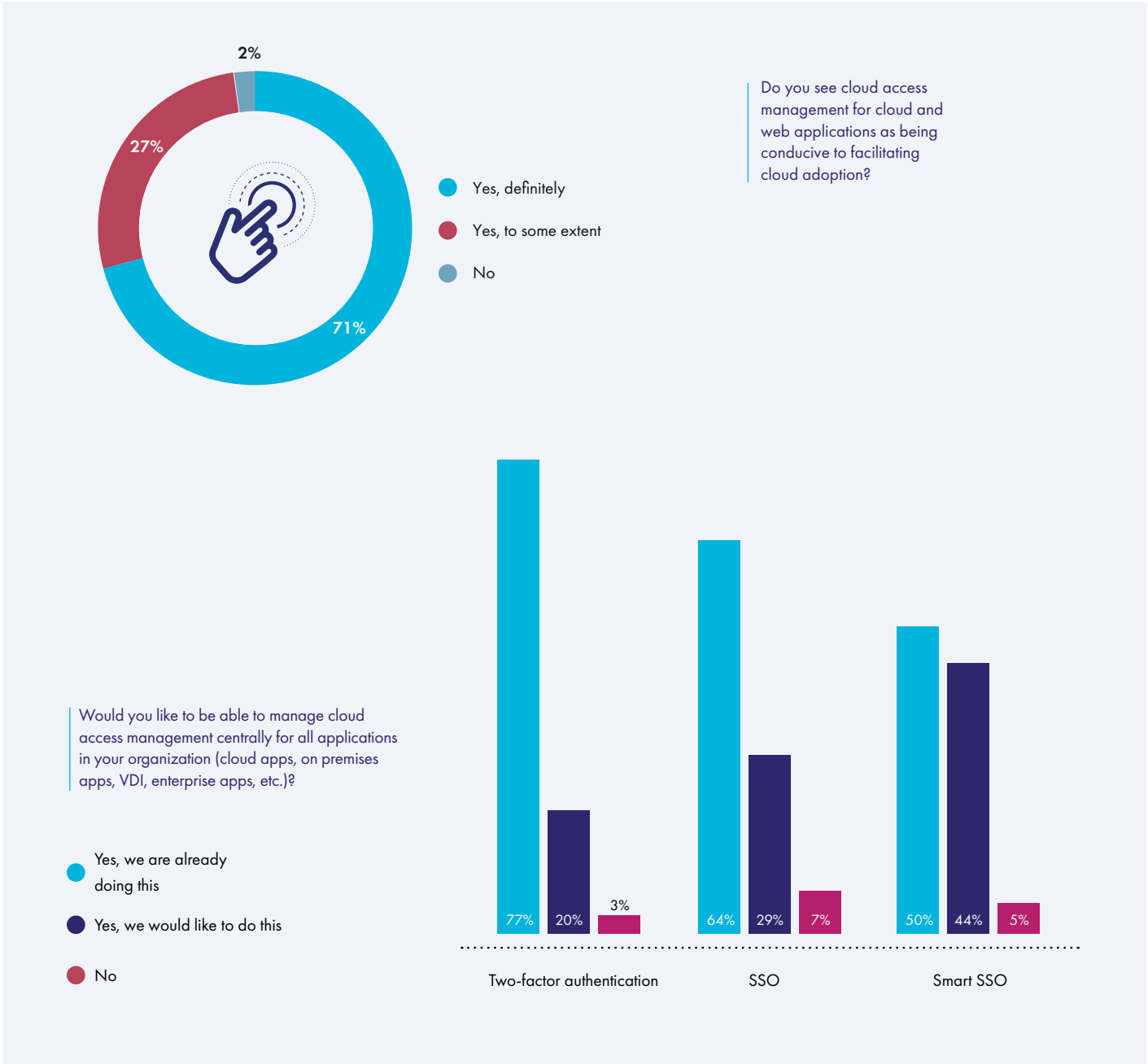
What do you think the challenges are to cloud-based security and authentication?



Despite challenges, cloud access management is seen as conducive to facilitating cloud adoption, and organizations want to manage it centrally

No matter how an organization views cloud access management, or their experience of it, it is essential if an organization wants to use cloud, with the two inextricably linked – the more you use cloud, the more you have to engage with cloud access management.

In terms of how this is managed, the overwhelming desire is to do so centrally, something that respondents' organizations are having more success in achieving for two-factor than they are for SSO or smart SSO.



03
Two-factor authentication

Multi-factor authentication is widely used by organizations in the Americas, with a strong majority (95%) of respondents in the Americas reporting that they use it. However, only a minority (15%) choose to use a dedicated multi-factor authentication solution.

Approaching half use cloud SSO (47%) and/or an on prem IAM solution (46%) for multi-factor authentication, with around four in ten using IDaaS (40%) and/or smart SSO (37%).

The use of smart SSO as a part of two-factor authentication is set to rise with a majority (86%) of respondents planning to expand/adopt this in the future. However, also set to be expanded by most (77%) is the use of username and password, despite its limitations and dubious track record.

> Nearly all (99%) respondents in the Americas feel that two-factor authentication for cloud applications is conducive to facilitating cloud adoption"

When it comes to deciding on the best approach to act on that expansion of two-factor authentication, respondents in the Americas are generally split. Almost half (49%) plan to use a dedicated multi-factor authentication solution, while almost the same proportion (48%) plan to use an IDaaS/access management solution.

Two-factor and cloud applications are intrinsically linked, with nearly all (99%) respondents in the Americas feel that two-factor authentication for cloud applications is conducive to facilitating cloud adoption.

Multi-factor authentication is now the norm

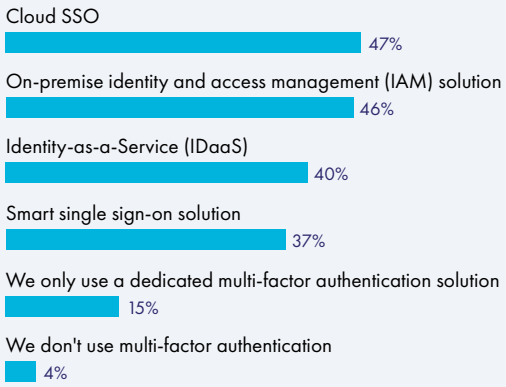
However, the use of a dedicated multi-factor authentication solution is still in the minority.

Despite on-premise IAM solutions being the most widely used, cloud SSO solutions are slightly more likely to be used for multi-factor authentication.

There is a discrepancy between the number of organizations using each access management solution and the number using these solutions for multi-factor authentication.

This perhaps indicates that username and password as a form of access management is not only prevalent, but may be widely used in multi-factor authentication.

Is your organization using any of the following for multi-factor authentication?

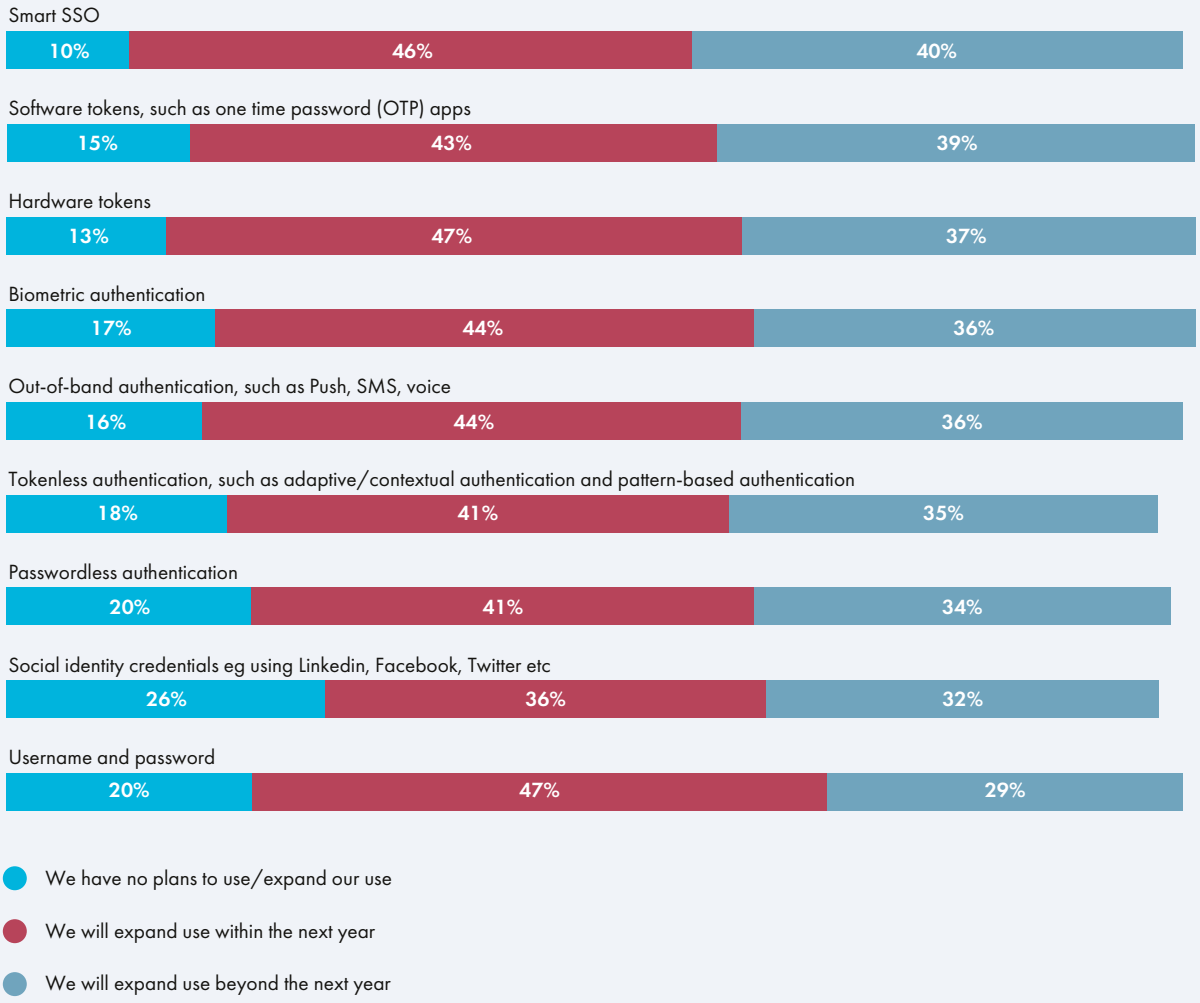


Use of emerging authentication methods such as smart SSO, tokenless, and biometrics is set to jump, but username and password isn't going to vanish in the near future

If anyone thought that the days of using a username and password to access critical corporate resources were in the past, then they are in for a rude awakening, as most respondents indicate that their company plans to expand their use of this system in the future.

However, it is encouraging that this number is not as high as the number planning to expand their use of smart SSO or biometrics for instance.

What types of two-factor authentication do you expect your organization to expand the use of to protect applications in the future?



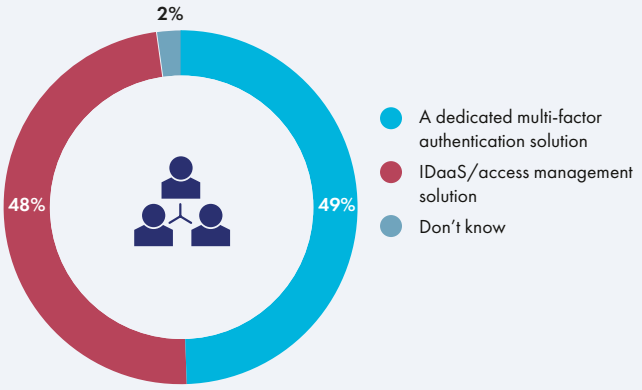
Respondents are split on the best way to act on these plans to expand two-factor authentication

About half plan to use a dedicated multi-factor authentication when expanding their organization's use of two-factor authentication, while a similar proportion plan to utilize an IDaaS/access management solution.

Given how, when it comes to cloud-based authentication at least, the management of any authentication solution is the most widely experienced challenge, perhaps a dedicated multi-factor authentication solution would be better suited?

Regardless of how they get there, each company must chose the approach that best suits them, and minimizes the challenges involved.

How does your organization plan to expand its use of two-factor authentication?

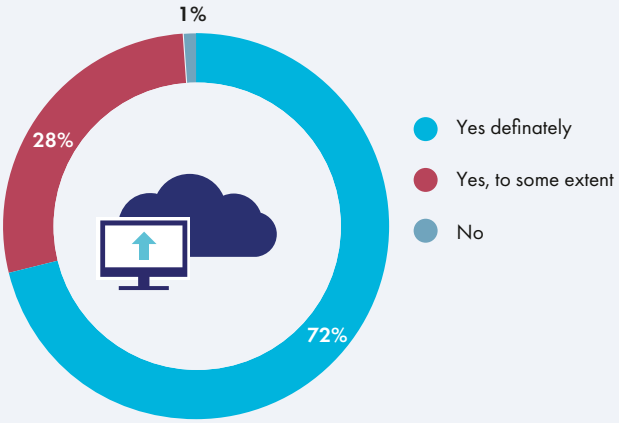


Nearly all organizations think that two-factor authentication is conducive to facilitating cloud adoption to some extent, but there are still doubts

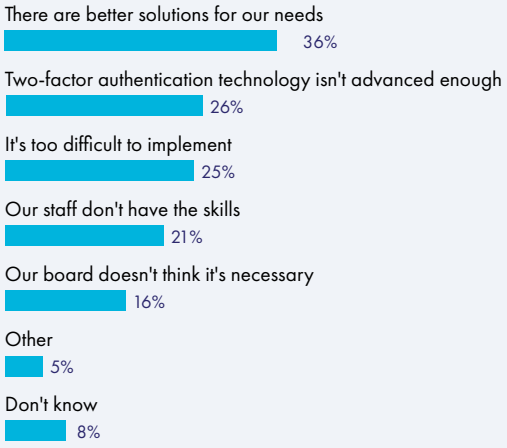
With most planning to expand their use of two-factor authentication, a key driver may be their belief that it is conducive to facilitating cloud adoption, as a way of keeping their cloud applications safe.

But some respondents cast doubt over just how conducive it is, with some expressing concern over the suitability of two-factor authentication, it's level of advancement, and difficulty to implement.

Do you see two-factor authentication for cloud applications as being conducive to facilitating cloud adoption?



Why don't you think that two-factor authentication for cloud applications will be conducive to cloud adoption? [85] respondents who don't think two-factor authentication will definitely be conducive to facilitating cloud adoption



04
Smart SSO

When it comes to protecting cloud and web-based applications, respondents are most likely to feel that two-factor authentication (64%) is the best approach. However, it is worrying that over four in ten (41%) feel that username and password is one of the best tools, despite the many failings of this method of authentication.

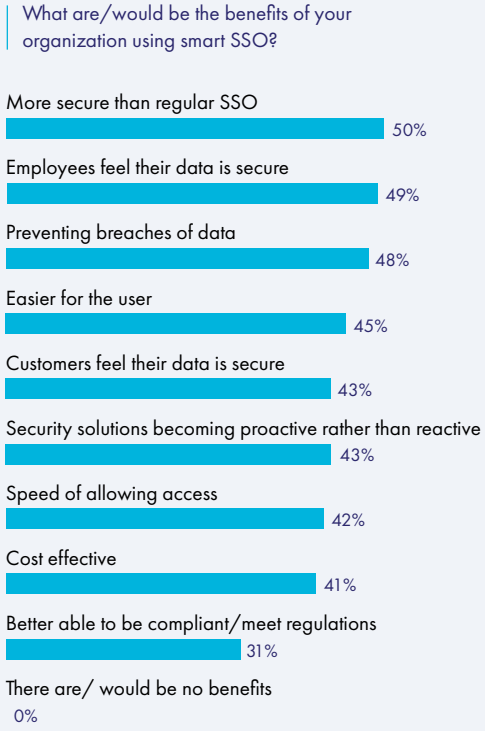
Also, only 28% see social media credentials as one of the best tools for protecting cloud and web-based authentication, despite a far larger proportion being willing to allow employees to use social media credentials to access corporate resources.

Regardless of how they protect it, effective cloud access management is essential for organizations. If this is not done, nearly all (97%) respondents anticipate problems for their company. Chief among these is IT's staff being used less efficiently (53%), cloud becoming a security issue (47%), and an increase in operational overheads and IT costs (45%). In short, effective cloud access management makes organizations more secure for less work and money.

Smart SSO comes with multiple benefits

Respondents in the Americas see smart SSO as secure, cost effective, and fast, three essential ingredients in any solution for a modern business.

Furthermore, approaching half see smart SSO as easier for the user, again highlighting how a truly effective authentication management solution brings performance benefits along with the security.



Yet, cloud-based security and authentication also presents challenges for the overwhelming majority (95%) of respondents' organizations. If left unabated, they may manifest into the challenges that organizations set out to avoid by investing in it. For instance the overall management by IT of cloud-based security and authentication is seen as a challenge for almost half (47%) of respondents. If unresolved, this could lead to IT's staff being used less efficiently, the most widely recognized outcome from ineffective cloud access management.

Cloud access management is simply unavoidable, almost all (98%) see it as conducive to facilitating cloud adoption. And once adopted, respondents in the Americas prefer to manage it centrally for two-factor authentication (77%), SSO (64%), and/or smart SSO (50%).

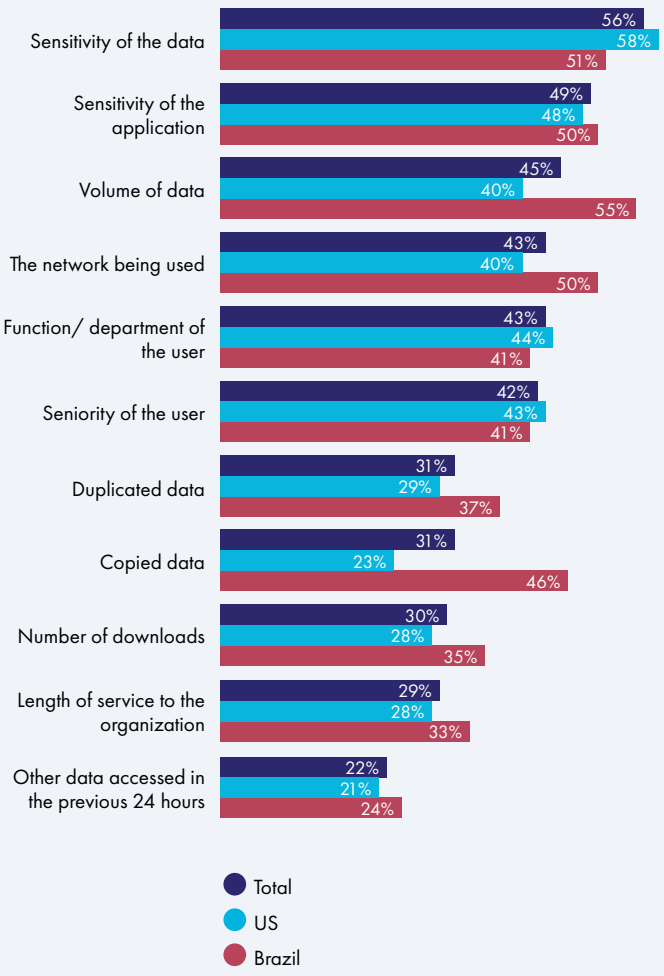
Organizations want to see a variety of information in a smart SSO solution

Respondents are alive to the potential of smart SSO as a means to protect their company, with over four in ten rating them among the best at protecting their organization's cloud and web resources, and over a quarter planning to implement this technology within the next year.

In terms of the information that respondents want to see used in a smart SSO, factors such surrounding the data itself (the sensitivity of it and the volume) are more likely to be desired than information about the user (function/department, seniority).

Respondents in the US and Brazil are mostly on the same page in terms of what they'd like to see used in a smart SSO solution, although those in Brazil are a bit more likely to want to see factors like the volume of data, the network being used, and whether the data has been copied or not.

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

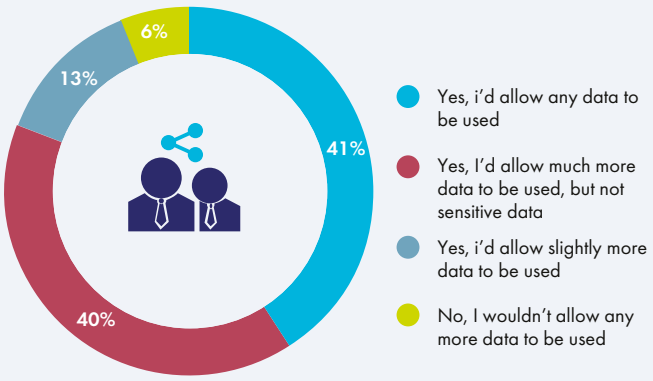


In exchange for a secure smart SSO, employees are more willing for their data to be collected and held

Four in ten respondents are willing to provide any data to their organization if it results in a secure smart SSO, but there are an equal number who would be less inclined to share sensitive data.

A small minority of respondents wouldn't be willing to share any more data, showing that there is still some level of cautiousness when thinking about sharing personal data, regardless of this resulting in a secure smart SSO.

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



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 selfenroll 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

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 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.

Innovation in access security allows us to overcome the reliance on passwords, which are proven to be insufficient in protecting data. Organizations that utilize cloud-based access and passwordless authentication to scale secure cloud adoption will be able to meet the increased need for improved security, especially at a time when access control is critical for today's remote workforce. The elimination of username and passwords as sole method of authentication and broader use of smart single sign on will result in a greater level of security and convenience as more and more applications are delivered from outside the security perimeter.

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/us-access-management-index