## Contents

<table>
<thead>
<tr>
<th>Page</th>
<th>Section</th>
</tr>
</thead>
<tbody>
<tr>
<td>03</td>
<td>About the 2019 Thales Access Management Index</td>
</tr>
<tr>
<td>04</td>
<td>Executive Summary</td>
</tr>
<tr>
<td></td>
<td>04 Concerns over cloud services as source of cyberattacks</td>
</tr>
<tr>
<td></td>
<td>04 Data breaches driving security budget increases</td>
</tr>
<tr>
<td></td>
<td>04 Obstacles to effective cloud access management</td>
</tr>
<tr>
<td>05</td>
<td>Key Findings</td>
</tr>
<tr>
<td></td>
<td>05 Cloud services are targets for cyber attacks</td>
</tr>
<tr>
<td></td>
<td>05 Top access management technologies</td>
</tr>
<tr>
<td></td>
<td>06 Data Breaches driving access management adoption</td>
</tr>
<tr>
<td></td>
<td>06 Access management is essential for cloud transformation</td>
</tr>
<tr>
<td>07</td>
<td>Access management background</td>
</tr>
<tr>
<td></td>
<td>09 Major targets for cyber-attacks</td>
</tr>
<tr>
<td></td>
<td>10 Cloud applications are a target</td>
</tr>
<tr>
<td></td>
<td>11 Using social media credentials</td>
</tr>
<tr>
<td></td>
<td>12 Changes to security policies</td>
</tr>
<tr>
<td></td>
<td>13 Access management use on the rise</td>
</tr>
<tr>
<td></td>
<td>14 Drivers for access management solutions</td>
</tr>
<tr>
<td></td>
<td>15 Controlling access to comply with data protection regulations</td>
</tr>
<tr>
<td></td>
<td>16 Access management decision makers</td>
</tr>
<tr>
<td></td>
<td>17 Difficulty selling the need for IT security to the board</td>
</tr>
<tr>
<td>18</td>
<td>Cloud access management trends</td>
</tr>
<tr>
<td></td>
<td>19 Cloud Access Management Trends</td>
</tr>
<tr>
<td></td>
<td>20 Best access management tools to protect cloud &amp; web-based apps</td>
</tr>
<tr>
<td></td>
<td>21 Cloud access management being conducive to cloud adoption</td>
</tr>
<tr>
<td></td>
<td>22 Managing cloud access management</td>
</tr>
<tr>
<td></td>
<td>23 Securing external users’ access</td>
</tr>
<tr>
<td></td>
<td>24 Challenges to cloud-based security</td>
</tr>
<tr>
<td></td>
<td>25 Impact of ineffective cloud access management</td>
</tr>
<tr>
<td></td>
<td>26 Authentication policies</td>
</tr>
<tr>
<td>27</td>
<td>Smart Single Sign On</td>
</tr>
<tr>
<td></td>
<td>28 Smart Single Sign On</td>
</tr>
<tr>
<td></td>
<td>29 Factors Driving Smart Single Sign On (SSO) Policies</td>
</tr>
<tr>
<td></td>
<td>30 Benefits of smart SSO</td>
</tr>
<tr>
<td>31</td>
<td>Two-factor authentication trends</td>
</tr>
<tr>
<td></td>
<td>32 Two-Factor Authentication Trends</td>
</tr>
<tr>
<td></td>
<td>33 Current use of two-factor authentication</td>
</tr>
<tr>
<td></td>
<td>34 Growth of two-factor authentication</td>
</tr>
<tr>
<td></td>
<td>35 Authentication methods within organizations</td>
</tr>
<tr>
<td></td>
<td>36 Authentication methods used in two years</td>
</tr>
<tr>
<td></td>
<td>37 Two-factor authentication facilitating cloud adoption</td>
</tr>
<tr>
<td>38</td>
<td>Key takeaways</td>
</tr>
<tr>
<td>38</td>
<td>About Thales Cloud Protection &amp; Licensing</td>
</tr>
</tbody>
</table>
About the 2019 Thales Access Management Index

The 2019 Access Management Index is a survey of 1,050 executives in 11 countries with responsibility for, or influence over, IT and data security.

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

Vanson Bourne is an independent specialist in market research for the technology sector. Their reputation for robust and credible research-based analysis, is founded upon rigorous research principles and our ability to seek the opinions of senior decision makers across technical and business functions, in all business sectors and all major markets. For more information, visit www.vansonbourne.com

The respondents represented the following countries, sectors and organization sizes:
Executive Summary

Concerns over cloud services as source of cyberattacks

The explosion of cloud applications and identities have set IT decision makers on a quest for reconciling the speed of cloud with the security, compliance and scalability needs of the enterprise. Surpassing the user experience offered by mainstream consumer applications, cloud access management solutions have emerged to address the multi-faceted challenges of the new identity perimeter.

Surveying more than 1,050 IT decision makers globally, the 2019 Thales Access Management Index revealed that almost half (49%) of businesses believe cloud applications make them a target for cyber-attacks. Cloud applications are listed in the top three reasons an organization might be attacked, just behind unprotected infrastructure such as IoT devices (54%) and web portals (50%).

With cloud applications now a crucial part of day-to-day business operations, the majority (97%) of IT leaders believe that cloud access management is necessary to the adoption of cloud services within their organizations. However, despite four in 10 (38%) organizations now having a CISO, just one in 10 (14%) CISOs are given the final decision on cloud access management solutions deployed within their organization. In fact, companies are more likely to put their faith in a traditional IT role, such as CIOs (48%) when dealing with this, suggesting a disconnect between the decision-making and implementation of cloud security.

The rapid increase of cloud applications and services within organizations has brought many benefits, but these findings clearly show that without the ability to properly secure cloud-based services organizations are exposing themselves to unnecessary security threats. Cloud technology has become ubiquitous enough now that securing it should be second nature to any business. However, without a dedicated CISO, organizations lack the leadership required to implement the correct security strategy or solutions to keep them secure in the cloud.

Data breaches driving security budget increases

The growing awareness of consumer data breaches has led to organizations taking action to increase investments in IT security. Almost all (94%) have changed their security policies around access management in the last 12 months. In addition, the biggest areas of change have focused around: staff training on security and access management (52%); increasing spend on access management (45%), and access management becoming a board priority (44%).

Obstacles to effective cloud access management

In spite of the updates to security policies, the majority of IT leaders (95%) believe ineffective cloud access management is still a concern for their organization. In fact, their biggest concerns are its impact on security (48%), IT staffs’ time (44%) and on operational overheads and IT costs (43%). Worse, when it comes to implementing access management solutions, they cited costs (40%), human error (39%) and difficulty integrating them (36%) as the biggest obstacles.

When it comes to cloud solutions, three-quarters (75%) of organizations already rely on access management to secure their external users’ logins to online corporate resources. In particular, two-factor authentication is the most likely (58%) tool to be seen as effective at protecting cloud and web-based apps, followed by smart single sign-on (49%) and biometric authentication (47%).
Key Findings

Cloud services are targets for cyber attacks

49% of businesses believe cloud applications are among the biggest targets for cyberattacks.

Top access management technologies

58% believe two-factor authentication is the best access management tool to protect cloud and web-based apps.

49% while 49% believe it is smart single sign-on and 47% biometric authentication...
Key Findings

Data breaches driving access management adoption

94% of organizations’ security policies have been influenced by consumer breaches in the last 12 months.

62% of companies continue to operate without a CISO despite increased cybersecurity awareness.

Access management is essential for cloud transformation

36% are using smart SSO.

70% are using two-factor authentication.

53% are using SSO.

97% say that cloud access management for cloud applications is conducive to cloud adoption.

95% believe that ineffective cloud access management can or does cause issues for their organization.

49% of businesses believe cloud applications are among the biggest targets for cyberattacks.

58% believe two-factor authentication is the best access management tool to protect cloud and web-based apps.

49%...while 49% believe it is smart single sign-on and 47% biometric authentication.

94% of organizations’ security policies have been influenced by consumer breaches in the last 12 months.

62% of companies continue to operate without a CISO despite increased cybersecurity awareness.
01 Access Management
Background
Access Management Background

Spearheaded by the reality of data breaches, as well as the adoption of cloud and social identities in the enterprise, the new IT perimeter has decision makers recalculating their IT management route. Inspired by consumer-grade convenience that meshes single sign-on with risk-based policies, access management practices are evolving to bridge the nexus of cloud, mobile and social.

Over half (54%) of interviewed ITDMs report that unprotected infrastructure is one of the biggest targets for cyber-attacks, while around half state the same regarding web portals (50%) and/or cloud applications (49%). Organizations are likely to be battling against more than one target for a cyber-attack, which makes security critical.

Nearly all (94%) respondents say that their organization’s security policies around access management have been influenced by breaches of consumer services in the last 12 months. Despite this, approaching three in five (56%) would allow their organization’s employees to log on to corporate resources using their social media credentials, even with recent security breaches in mind.

An on-premise IAM solution is the most likely (62%) form of access management being used within respondents’ organizations, although a significant proportion have adopted IDaaS (58%), Cloud SSO (54%) and/or smart single sign-on (46%). The most likely main or significant considerations for implementing access management are large scale breaches (78%) and/or security concerns (77%); this highlights security as being a main driver, despite the other benefits access management may bring.

It seems that a shift in perception around the importance of IT security is currently underway; more than a third (36%) of respondents say that it was difficult to sell the need for IT security to the board a year ago, however only 20% say that this is now the case.

“49% of those surveyed said that cloud applications are among the biggest targets for cyber attacks”
Major targets for cyber-attacks

Around half say the same when it comes to web portals (50%) and/or cloud applications (49%). This pattern largely remains the same as in 2017, although web portals was the most likely (47%) reported target at that time. As targets are still comparable, it suggests that organizations could still be getting to grips with how they can best protect the areas which are most likely to be a target.

Why are cloud applications a target for cyber-attacks?

Respondents in South Africa (68%), Australia (67%) and the UK (63%) are even more likely to state that unprotected infrastructure is a target for cyber-attacks. Respondents in India are most likely (57%) to say that mobile applications are a target for cyber-attacks.

Figure 1
“In general, which of the following do you think are the biggest targets for cyber-attacks?”, split by historic data, asked to all respondents (1,050 respondents)
Cloud applications are a target

There was a greater proportion (71%) of respondents who said that this was the case in 2017, which could suggest that the speed organizations are adopting cloud applications has plateaued or slowed slightly.

Would respondents allow their organization’s employees to log on to corporate resources using their social media credentials?

Figure 2

“Why do you feel that cloud applications are a target for cyber-attacks?”, split by historic data, asked to respondents who think that cloud applications are a target for cyber-attacks (310 respondents in 2019 and 426 respondents in 2017)

Those in Brazil are far more likely (83%) to say that the increasing volume of cloud applications makes them a target.
Using social media credentials

However, this is a positive step from the 2017 data, where 66% stated that they would allow this.

This suggests that there is a greater awareness of the vulnerability that this may cause, with more and more organizations being caught out by weaknesses in their security and authentication methods.

How have security policies been influenced by breaches of consumer services?

<table>
<thead>
<tr>
<th>Yes, definitely</th>
<th>Yes, to an extent</th>
<th>No, not at all</th>
</tr>
</thead>
<tbody>
<tr>
<td>29%</td>
<td>28%</td>
<td>44%</td>
</tr>
</tbody>
</table>

Of respondents say that they would allow employees in their organization to log on to corporate resources using their social media credentials even with recent security breaches in mind.

Respondents in India are much more likely (85%) to say that this would be allowed, with 71% even going as far as to say that they definitely would allow this. Those in the UK (29%) and South Africa (26%) are the least likely to say that this would be allowed.

**Figure 3**

“In light of recent security breaches, would you allow employees in your organization to log on to corporate resources using their social media credentials”, split by historic data, asked to all respondents (1,050 respondents)
Changes to security policies

Staff being trained on security and access management (52%), increasing spend on access management (45%) and it becoming a board priority (44%) are the most likely changes.

Secure access management being a board priority has increased from 2017 (38%) and 2016 (34%), which shows that access management is an area that is starting to gain traction with senior decision makers.

94% of those surveyed cite that their organization’s security policies around access management have been influenced by breaches of consumer services in the last 12 months – this is even higher than in 2017 (90%) and 2016 (89%)

Figure 4

*How have your organization’s security policies around access management been influenced by breaches of consumer services in the last 12 months?*, split by historic data, asked to all respondents 1,050 respondents in 2019 and 2017, and 1,150 in 2016

All (100%) respondents in the Middle East say that their organization’s security policies around access management have been influenced by breaches of consumer services in the last 12 months, with only slightly fewer (98%) in India saying that this is the case.
Access management use on the rise

Respondents’ organizations are most likely (62%) to have adopted an on-premise IAM solution, with a smaller proportion having adopted IDaaS (58%), Cloud SSO (54%) and/or smart single sign-on (46%) (fig. 5).

This shows an increase on the adoption of 2017 (47%, 35% and 42% respectively) and 2016 (38%, 36% and 39% respectively) (fig. 6), which could be due to the increasing priority that this area is being shown by the board (fig. 4).

The use of smart SSO is going to increase in the near future (fig. 5) and these solutions will need to factor in a range of different types of data/information in order to be appealing to the mass market.

Figure 5
Analysis of respondents who say that their organization is using, or planning to use, the above access management capabilities, asked to all respondents (1,050 respondents)

Figure 6
Analysis of respondents who say that their organization is using the above access management capabilities, split by historic data, asked to all respondents (1,050 in 2019 and 2017, and 1,150 in 2016)
Drivers for access management solutions

When it comes to drivers for implementing an access management solution, respondents are most likely to say that the threat of large scale breaches (24%) or simplified cloud access for end users (18%) are the most significant considerations.

Almost eight in ten report that the threat of large scale breaches (78%) and/or security concerns (77%) are one of the main or the most significant consideration, which highlights security as being a key issue within organizations and suggests that its core functionality could be more important to organizations than its ability to support other areas of the business.

Figure 7

“What are the main drivers for implementing an access management solution in your organization?”, asked to all respondents (1,050 respondents)

The threat of large scale breaches was also the most likely (24%) most significant consideration in 2017.
Controlling access to comply with data protection regulations

Slightly more than two in three (68%) go as far as to say that this is definitely the case, which is a much bigger proportion than in previous years (54%, 56% and 48% respectively).

The increase in this level of thinking could also be a factor as to why there has been a rise in access management capabilities in use (fig. 6) – particularly with regulations becoming ever more strenuous, or new regulations being put in place altogether (such as GDPR).

99% of respondents say that controlling who has access to specific types of data can contribute toward their organization’s ability to comply with data protection regulations and pass security audits.

Respondents in India (88%), the Middle East (76%) and South Africa (74%) are the most likely to state that this is definitely the case.

---

Figure 8

“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)?”, split by historic data, asked to all respondents (1,050 respondents in 2019 and 2017, 1,150 in 2016, and 900 in 2015)
Access management decision makers

Who is involved in the decision-making process when selecting access management solutions?

The CIO/Head of IT is the most likely (48%) final decision maker in respondents’ organizations when it comes to selecting an access management solution; more than nine in ten (95%) say that they are involved to some extent (fig. 9).

This has been the case since 2015 (47%, 53% and 54% respectively), indicating that the primary decision has and will continue to sit in the IT department (fig. 10) – perhaps as these decision makers are closer to the security issues within organizations (figs. 1 and 7).

Respondents in France are almost as likely to report that the CSO (26%) is the final decision maker, as they are to say the same about the CIO/Head of IT (31%). In Japan, the CEO/MD is most likely (22%) to make the decision (CIO/Head of IT – 20%).

Figure 9

“Who is involved, and to what extent, in the decision-making process when selecting an access management solution for your organization?”, asked to all respondents (1,050 respondents)

Figure 10

Analysis of respondents who say that the above roles are the final decision maker when selecting their organization’s access management solution, split by historic data, asked to all respondents (1,050 respondents in 2019 and 2017, 1,150 in 2016, and 900 in 2015)
Difficulty selling the need for IT security to the board

However, it is only 20% who say that this is currently the case; in fact, it is over half (56%) who now say that it is easy.

This change in thinking reflects the increase in access management capabilities that are being adopted (figs. 5 and 6) and the security concerns that are driving this adoption (fig. 7). Cyber threats are likely to continue and even increase in the future, so decision makers will need to keep liaising closely with the board.

Respondents in Japan are the most likely (48%) to state that it is difficult to sell the need for IT security to the board a year ago.

Figure 11
“How easy or difficult do your organization’s IT leaders find it to sell the need for IT security to the board?”, asked to all respondents (1,050 respondents)
Cloud Access Management Trends
Cloud Access Management Trends

Organizations are seeing increased pressure to implement a cloud access management solution. The vast majority cite security concerns and the threat of large scale breaches as the primary driver for implementation. With access management, users maintain a single identity for all their resources with cloud SSO, and secure that single identity with risk-based policies and 2FA. This lets businesses lock down access to cloud-based services without sacrificing speed.

When thinking about the access management tools that are best at protecting cloud and web-based apps, nearly three in five (58%) respondents cite that two-factor authentication is one of the best. Slightly fewer than half say the same when it comes to smart single sign-on (49%) and/or biometric authentication (47%).

Approaching all (97%) of those surveyed state that cloud access management for cloud and web applications is conducive to facilitating cloud adoption. In addition, 75% of respondents’ organizations are securing external users’ access to online corporate resources with access management, which shows that access management can have an impact on more than just the immediate users.

Although there are benefits to authentication, 96% of respondents admit that there are challenges to cloud-based security and authentication. The most likely of which are the cost of a secure solution (40%) and human error in managing solutions (39%). Furthermore, nearly all (95%) state that their organization does/could see impacts to its cloud/web resource as a result of ineffective cloud access management.

“Although there are benefits to authentication, 96% of respondents admit that there are challenges to cloud-based security and authentication.”
Best access management tools to protect cloud & web-based apps

Almost half of surveyed ITDMs state smart single sign-on (49%) and/or biometric authentication (47%) are some of the best tools at protecting cloud and web-based apps.

Social identity credentials is the area which is least likely (24%) to be perceived as the best, which makes it even more surprising that over half (56%) would allow employees in their organization to log on to corporate resources using their social media credentials (fig. 3).

Two-factor authentication is the tool most likely to be considered as the best across all countries (44%-72% respectively).
Cloud access management being conducive to cloud adoption

Is cloud access management for cloud and web applications conducive to facilitating cloud adoption?

Over half (56%) go as far as to say that this is definitely the case.

In 2017, slightly fewer (91%) reported that cloud access management for cloud and web applications is conducive to facilitating cloud adoption; this suggests that there is an even bigger bond forming between cloud access management and cloud adoption.

Would organizations like to be able to manage cloud access management centrally for all applications?

Those in India (84%) are the most likely to say that cloud access management for cloud and web applications is definitely conducive to facilitating cloud adoption, while those in Japan (43%) and Australia (42%) are the least likely.
Managing cloud access management

When it comes to managing cloud access management centrally for all applications, seven in ten (70%) respondents’ organizations are currently doing this for two-factor authentication, while fewer say the same regarding SSO (53%) and/or smart SSO (36%) (fig. 14).

This is an increase from 2017 where smaller proportions were doing this for two-factor authentication (58%) and/or SSO (36%) (fig. 15).

Central management seems to be the way that organizations are moving and this may further facilitate the adoption of cloud (fig. 13).

---

**Figure 14**
“Would you like to be able to manage cloud access management centrally for all applications in your organization (cloud apps, on-premises apps, VDI, enterprise apps, etc.)?”, asked to all respondents (1,050 respondents)

**Figure 15**
“Would you like to be able to manage cloud access management centrally for all applications in your organization (cloud apps, on-premises apps, VDI, enterprise apps, etc.)?”, asked to all 2017 respondents (1,050 respondents)
Securing external users’ access

Slightly more than one in ten (14%) say that their organization does not offer, or plan to offer, external users access to online.

This relatively high adoption could be due to the rise in access management capabilities which are being used in organizations generally (fig. 6) and/or the changes in security policy that are happening (fig. 4), but ultimately, the end goal should be using access management for all internal and external users.

Figure 16
“Does your organization secure external users’ (such as partners, consumers and contractors) access to online corporate resources with access management?”, asked to all respondents (1,050 respondents)

Those in India (90%) and Brazil (89%) are the most likely to say that their organization secures external users’ access to online corporate resources with access management, while those in Australia (66%) and Japan (65%) are the least likely.
Challenges to cloud-based security

What challenges are there to cloud-based security and authentication?

The cost of a secure solution (40%) and human error in managing solutions (39%) are the most likely challenges to cloud-based security.

These challenges and weaknesses could explain why cloud applications are often a target for cyber-attacks (fig. 1); if organizations want to protect themselves as best as possible then they should invest in cloud access management solutions (fig. 12).

Figure 17
“What do you think the challenges are to cloud-based security and authentication?”, asked to all respondents (1,050 respondents)

Cost is least likely (30%) to be a challenge in Belgium/Netherlands, while security solutions not integrating with other systems is the most likely (40%) challenge within BeNe.
Impact of ineffective cloud access management

What impact is ineffective cloud access management having on cloud and web resources?

The most likely impacts are cloud becoming a security issue (48%), IT staff’s time being used less efficiently (44%) and an increase in operational overheads and IT costs (43%).

Interestingly, 28% say that it could result in a slower adoption of cloud; while cloud access management can be conducive to cloud adoption (fig. 13), there is also a danger that it can harm adoption if the solutions being used are not effective.

In 2017, a smaller proportion of respondents stated that it could result in IT staff’s time being used less efficiently (39%) and an increase in operational overheads and IT costs (38%).
Authentication policies

What else do we know about authentication methods?

A similar proportion (78%) agree that policy-based access management is the future of access security.

Just under three quarters agree that access management and identity governance administration is more effective when separated (73%) and/or that authentication methods used in the consumer world can be applied to enterprise resources (72%).

While organizations may not feel comfortable allowing employees to use social media credentials (fig. 3), it seems that in the long run there could be a big crossover between consumer and enterprise authentication.

**Figure 19**
Analysis of respondents who agree with the above statements, asked to all respondents (1,050 respondents)
04 Smart Single Sign On
Smart Single Sign On

Smart Single Sign-On lets users log in to all their cloud applications with a single identity, eliminating password fatigue, frustration, password resets and downtime while ensuring that access remains secure at all times. By applying SSO intelligently, based on previous authentications in the same SSO session and the specific contextual policy relevant for each access attempt, users may authenticate just once in order to access all their cloud applications, or provide additional authentication, when needed.

On average, it is 23% of employees in respondents’ organizations who use smart SSO, however, this could rise to 46% in two years; smart SSO isn’t commonplace in organizations yet, but it seems that there is a desire for it to be. Additionally, 96% of respondents say that they would like to see a smart SSO solution being used. This drive for adoption is justified when considering that almost all (97%) respondents feel that there are/would be benefits of their organization using smart SSO. The most likely benefits are employees (54%) and/or customers (52%) feeling that their data is secure, and/or preventing data breaches (50%).

“Additionally, 96% of respondents say that they would like to see a smart SSO solution being used.”
Factors Driving Smart Single Sign On (SSO) Policies

The most likely desired types of data/information being used in a smart SSO are the sensitivity of the data (65%), the sensitivity of the application (57%) and the function/department of the user (44%).

Figure 20
“Which of the following types of data/information would you like to see used in a smart SSO solution?”, asked to all respondents (1,050 respondents)

96% of respondents say that they would like to see a smart SSO solution being used.

Over half of respondents in Brazil (55%) and the UK (55%) would like the network being used to be considered in a smart SSO solution.
Benefits of smart SSO

What are the benefits of using smart SSO?

More than half say that employees (54%) and/or customers (52%) feeling that their data is secure is a benefit, while 50% report the same when it comes to preventing data breaches.

Organizations seem keen to give the perception that the data they hold is secure, but in reality, data will be held securely and be more convenient to access through a smart SSO solution.

97% of respondents state that there are/would be benefits of their organization using smart SSO.

Half (50%) of respondents in South Africa state that being cost effective is a benefit of smart SSO.
03 Two-Factor Authentication Trends
Two-Factor Authentication Trends

Two-factor authentication is an integral part of access management. It serves as the first line of defence against data breaches and it is expected to rise in organization-wide deployment over the next two years. The majority of IT leaders already manage 2FA centrally for all their enterprise applications, be they cloud, VPNs, VDI, web portals or mobile applications.

Around eight in ten (81%) respondents report that their organization uses two-factor authentication to protect mobile applications, while a similar proportion do so for enterprise applications (81%) and/or cloud applications (85%). This usage looks likely to increase; 96% expect that their organization’s use of two-factor authentication will expand in the future. And, this could happen fairly soon, just over three in five (61%) say that this will happen within the next year.

Positively for organizations, more than nine in ten (94%) respondents see two-factor authentication for cloud applications as being conducive to facilitating cloud adoption. Not only will two-factor authentication increase security levels, it can also help pave the way for cloud adoption.

“...96% expect that their organization’s use of two-factor authentication will expand in the future.”
Current use of two-factor authentication

Currently, the vast majority (87-94% respectively) of those surveyed say that their organization uses two-factor authentication to protect the below applications.

Mobile applications (31%) and enterprise applications (30%) are the areas where four or more of these applications are most likely to be protected by two-factor authentication.

Two-factor authentication is widely used and becoming a more mature method of authentication, however it is still surprising that not all respondents have adopted it wherever possible.

![Bar chart showing the percentage of respondents who use two-factor authentication across different applications.](chart.png)

**Figure 22**

“How many of the above applications in your organization are currently protected by two-factor authentication?”, asked to all respondents (1,050 respondents).

Generally, two-factor authentication is more widely used now than it was in 2017 (83-92% respectively).
Growth of two-factor authentication

Around six in ten (61%) think that this will happen within the next year – this is the biggest proportion over the last three years (47%, 55% and 48% respectively).

This ongoing feeling that two-factor authentication use will increase shows that it could be a long road to reach the end of the journey and that organizations will have to keep increasing and improving their use of two-factor authentication.

Respondents in India (84%) and the Middle East (78%) are the most likely to report that their organization will increase its use of two-factor authentication to protect applications in the next year.
Authentication methods within organizations

What proportion of users are using authentication methods?

On average, just under two thirds (64%) of respondents’ organizations’ employees use a username and password as an authentication method, although this has dropped slightly compared to the last two years (69% and 68% respectively).

But, all other authentication methods are being used more in 2019 (31%-39% respectively) than they were in 2017 (27%-35% respectively).

This shows a movement away from more traditional and risky authentication methods, to more advanced and secure methods; organizations should aim to keep this trend going over the next few years, or they could find themselves susceptible to cyber risks.

![Figure 24](image)

*Figure 24*

Analysis of the average percentage of users in respondents’ organizations who use the above authentication methods, split by historic data, asked to all respondents (1,050 respondents in 2019 and 2017, 1,150 in 2016, and 900 in 2015).
Authentication methods used in two years

A similar proportion will be using software tokens (49%), hardware tokens (47%) and/or smart SSO (46%).

This shows that these authentication methods are likely to see a big rise in usage over the next two years and should reduce the risk of organizations being subject to a successful cyber-attack.
Two-factor authentication facilitating cloud adoption

Over nine in ten (94%) respondents see two-factor authentication for cloud applications as being conducive to facilitating cloud adoption (fig. 26).

Of the few who do not feel that this is the case, around three in ten say that it is because it’s too difficult to implement (31%) and/or two-factor authentication technology isn’t advanced enough (29%) (fig. 27).

Cloud adoption could increase rapidly with cloud access management (fig. 13) and two-factor authentication paving the way; in particular, the use of two-factor authentication is set to increase (fig. 23) and this may be the push that organizations need to delve deeper in cloud.
Key takeaways

While organizations are getting to grips with access management solutions, IT and business decision makers must ensure they understand the risks to their cloud solutions in order to implement the relevant ones. These solutions must be perimeter-free, compatible with a zero-trust model and flexible and adaptive in order to make the most of the latest technologies such as smart single sign on. Without effective access management tools in place organizations face a higher risk of breaches, a lack of visibility and incur extra costs from poorly optimized cloud. Key takeaways from this year’s report include:

• Almost three in five (56%) of those surveyed say that they would allow employees in their organization to log on to corporate resources using their social media credentials.

• 94% IT professionals say their organizations’ security policies around access management having been influenced by breaches of consumer services in the last 12 months.

• IAM solutions (62%), IDaaS (58%), cloud SSO (54%) and/or smart SSO (46%) have all been adopted by a significant proportion of respondents’ organizations. Only 20% of IT professionals state that it is difficult to sell the need for IT security to the board currently.

• Nearly half (49%) of IT professionals cite smart single sign-on is the best access management tool for protecting cloud and web-based applications and services.

• In two years nearly half of organizations’ users will use smart SSO.

About Thales Cloud Protection & Licensing

Today’s enterprises depend on the cloud, data and software in order to make decisive decisions. That’s why the most respected brands and largest organizations in the world rely on Thales to help them protect and secure access to their most sensitive information and software wherever it is created, shared or stored – from the cloud and data centers to devices and across networks. Our solutions enable organizations to move to the cloud securely, achieve compliance with confidence, and create more value from their software in devices and services used by millions of consumers every day.
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: asia.sales@thales-esecurity.com

Europe, Middle East, Africa
Meadow View House, Long Crendon,
Aylesbury, Buckinghamshire HP18 9EQ
Tel: +44 (0)1844 201800 | Fax: +44 (0)1844 208550
E-mail: emea.sales@thales-esecurity.com

> thalescpl.com <