Authentication&Identity
MANAGEMENT INDEX

The convergence of personal and workplace identities

October 2016

gemalto
security to be free

Convergence of personal and workplace identities are causing security challenges for businesses

Gemalto's third annual Authentication and Identity Management Index revealed that 90% of enterprise IT professionals are concerned that employee reuse of personal credentials for work purposes could compromise security.

However, with two thirds (68%) of the 1150 IT professionals surveyed globally, saying they would be comfortable allowing employees to use their social media credentials on company resources, Gemalto's research suggests that personal applications (such as email) are the biggest worry to organisations.

Convergence of Personal and Workplace Identities

The enterprise and consumer worlds are merging closer together, with enterprise security teams under increasing pressure to implement the same type of authentication methods typically seen in consumer services, such as fingerprint scanning and iris recognition. Six in ten (62%) believed this was the case, with a similar amount (63%) revealing they feel security methods designed for consumers provide sufficient protection for enterprises. In fact, over half of respondents (52%) believe it will be just three years before these methods merge completely.

> For IT leaders, it's important that they keep pushing for security to be a priority at the board level, and ensure that it's front of mind for everyone in an organisation.

Consumer breaches impacting enterprise security

Identity theft accounts for 64% of all data breaches across the globe , and consumer service breaches continue to rise, resulting in almost nine in 10 (89%) enterprises addressing their access management security policies. Half of enterprises have implemented extra training (49%) to allay their security concerns, 47% increased security spend, and 44% allocated further resources.

As well as looking to the consumer world for effective authentication methods, an increasing amount of enterprises are using two factor authentication for better access security. Four in 10 (40%) revealed two-factor authentication is the security method of choice, an increase of 2% on last year. Deployment rates are also increasing: 62% expect to implement strong authentication in two years' time – up from 51% of respondents who said the same thing last year, and nearly 40% responded they will implement Cloud SSO or IDaaS solutions within the next two years.

Enterprises are clearly seeing the benefits, with over nine in ten (94%) using two-factor authentication to protect at least one application and nearly all respondents (96%) expecting to use it at some point in the future.

Mobility security still a challenge

As more enterprises become mobile, the challenges in protecting resources while increasing flexibility for employees working on the move increases. Despite an increasing amount of businesses enabling mobile working, a third (35%) completely restricted employees from accessing company resources via mobile devices and nine in 10 (91%) are at least part-restricting access to resources. This is backed up as half of businesses (50%) admit security is their biggest concern to increasing user mobility.

In order to protect themselves against threats from increased mobility, enterprises are choosing usernames and passwords (68%) as their authentication method, with just 37% using two-factor authentication. However, like the rise for access while in the office, over half of respondents (56%) expect their company to use two-factor authentication in two years' time.

Key areas of interest

Key findings

90%

The majority (90%) of respondents have concerns about employees in their organisation reusing personal credentials for work purposes...

- ...despite this, more than two thirds (68%) are comfortable allowing employees to log on to corporate resources using their social media credentials
- A third (33%) allow employees to use their own personal accounts when logging on for work purposes

89%

High profile breaches to consumer services is influencing the access management security policies of 89% of respondents' organisations

- Despite these high profile breaches to consumer services, more than half (58%) say that employee and consumer authentication are becoming very similar

60%

Although most (60%) respondents' organisations' customers have provided mostly positive feedback on their organisation's authentication policies, 12% have experienced mostly negative feedback

- Additionally, 42% believe that their organisation's customers are completely confident in their authentication policies

94%

Nearly all (94%) protect at least one application with two-factor authentication...

- ...and the majority are using it to protect web portals (82%), VPN (81%), cloud apps (81%), and local network access (81%)

96%

A high majority (96%) of respondents expect their organisation to expand their use of two-factor authentication in the future

- 55% expect this expansion within the next year

94%

94% of respondents'' organisations either do, or want to manage two-factor authentication centrally...

- ...with 96% seeing this as conducive to reducing shadow IT in their organisation

39%

Nearly four in ten (39%) respondents' organisations have implemented SSO in their organisation...

- ...and a further 49% planning to do this in the future
- Respondents' organisations are most likely (53%) to be using a password vault to manage access and security for cloud apps

59%

Cloud-based deployment of cloud SSO is preferred by nearly six in ten (59%), with less than a quarter (23%) preferring an on-premises server

- Nearly half (47%) feel under pressure to enable SSO in their organisation
- The vast majority (95%) of respondents see SSO for cloud apps as conducive to mobility and productivity

22%

More than a fifth (22%) do not secure external users' access to online corporate resources with two-factor authentication...

- ...but most (81%) of respondents whose organisation are not using two-factor to secure external access, plan to in the future

50%

Username and password is the most widely used authentication method by users for mobility in respondents' organisations...

- ...this is likely why, given the known vulnerability of static passwords, security concerns (50%) is the most likely obstacle to increased user mobility in respondents' organisations

40%

Currently, 40% of users in respondents' organisations use two-factor authentication, on average...

- ...and this is expected to rise to 62% in the next two years, on average

97%

The CIO and CSO are most likely to be involved when selecting a two-factor authentication solution (97% and 93% respectively)

- The ability to protect as many enterprise and cloud apps as possible is a significant consideration for
  a third (33%) of these CIOs and CSOs when sourcing a two-factor authentication solution
- The most likely consideration to be most significant when selecting a solution is the total cost of ownership

External influences on authentication practices

The influence of breaches

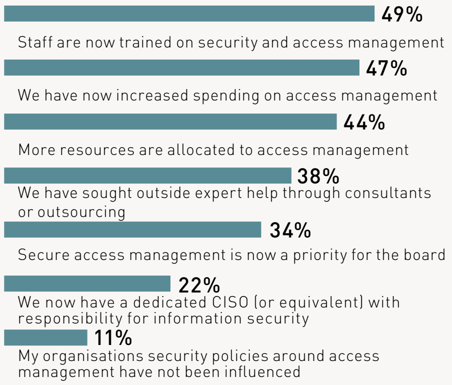
> Around nine in ten (89%) respondents admit that their organisation's access management security policies have been influenced by breaches of consumer services

Almost half (49%) of respondents say that staff in their organisation are now trained on security and access management because of public breaches

A similar proportion (47%) say that their organisation has increased spending on access management as a result The vast majority of organisations are taking notice of breaches experienced by consumer services and acting upon them. Those that are not doing this could be putting themselves at risk

Can consumer services also be an influence on authentication practices?

Figure 1.
How has your organisation's security policies around access management been influenced by breaches of consumer services?



Asked to all 1,150 respondents

The consumer influence and external pressures

> Over six in ten (63%) respondents believe that authentication methods used in the consumer world can be applied to ensure secure access to enterprise resources

A similar proportion (62%) think that their organisation's security team is feeling the pressure to use the same type of authentication for employees as consumer services, with almost six in ten (58%) claiming that this is already becoming very similar

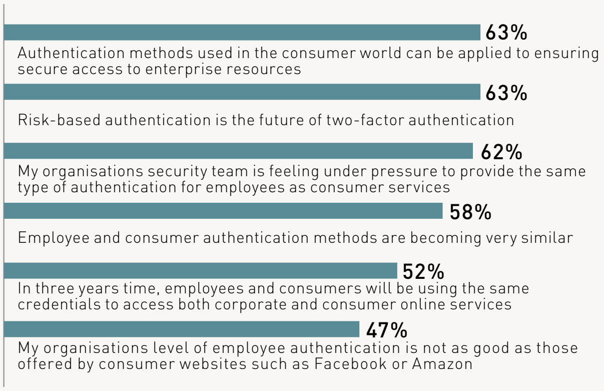
With nearly half (47%) feeling their organisations authentication is not as good as that provided by consumer services such as Amazon and Facebook, respondents are casting envious glances at these services

Perhaps the days of business leading the way in this area are over?

? Do IT decision makers have concerns about employees reusing personal credentials for work?

Figure 2.

Analysis of respondents who agree with the below statements



Asked to all 1,150 respondents

Using personal credentials

Nine in ten (90%) respondents have concerns about employees in their organisation reusing personal credentials for work purposes. Over two in ten (22%) are extremely concerned about this (figure 3)
Yet almost seven in ten (68%) would feel comfortable allowing employees in their organisation to log on to corporate resources using their social media credentials (figure 4)

This disconnect suggests that credentials used for other personal applications (such as personal email) is what would worry organisations

Figure 3

Are you concerned about employees at your organisation reusing personal credentials for work purposes?

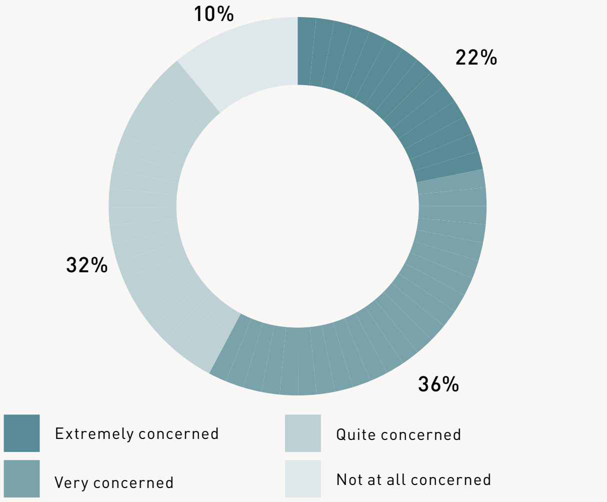
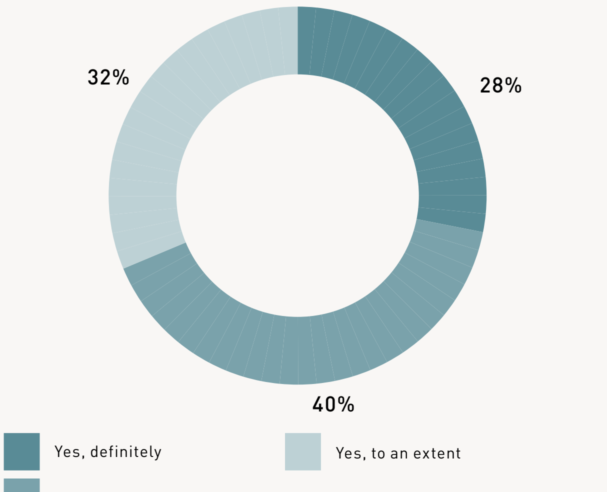


Figure 4

Would you feel comfortable allowing employees in your organisation to log on to corporate resources using their social media credentials?"



Asked to all 1,150 respondents

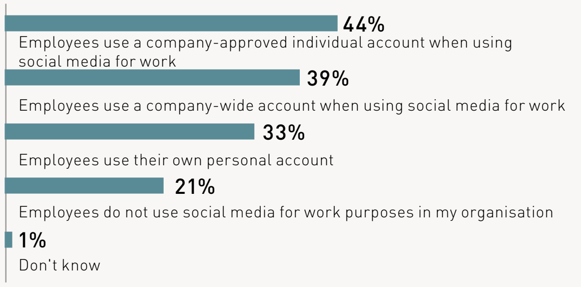
Social media use and content

The most likely (44%) approach that respondents' organisations take toward social media usage for work is for employees to use a company-approved individual account

However, almost four in ten (39%) provide their employees with access to a company-wide account and a third (33%) allow them to use their own personal account (figure 5)

Figure 5

What is your organisation's approach toward social media usage?



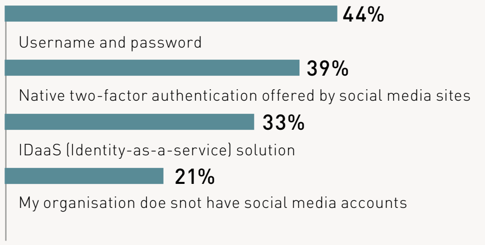
Asked to all 1,150 respondents

Over three in five (65%) respondents' organisations secure access to its social media accounts with a username and password. Only just over two in five (42%) use two-factor authentication for this (figure 6)

Organisations who are only using a username and password for their social media accounts are putting themselves at risk from having their accounts hacked. Especially for those who give their employees access to these accounts

Figure 6

How does your organisation secure access to its social media accounts?



Asked to all 1,150 respondents

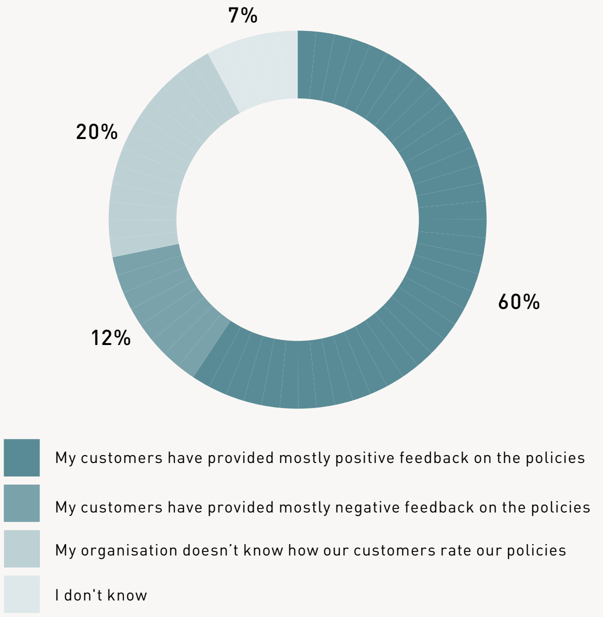
Customer feedback on authentication policies

Six in ten (60%) respondents say that their organisation's customers have provided mostly positive feedback on their authentication policies. However, over one in ten (12%) admit to this mostly being negative feedback, suggesting that these organisations need to look at improving authentication policies for their customers

Two in ten (20%) admit that their organisation does not even know how their customers rate their authentication policies, if they were to find out, they may too receive negative feedback (figure 7)

Figure 7

Has your organisation received customer feedback regarding your company's authentication policies?



Asked to all 1,150 respondents

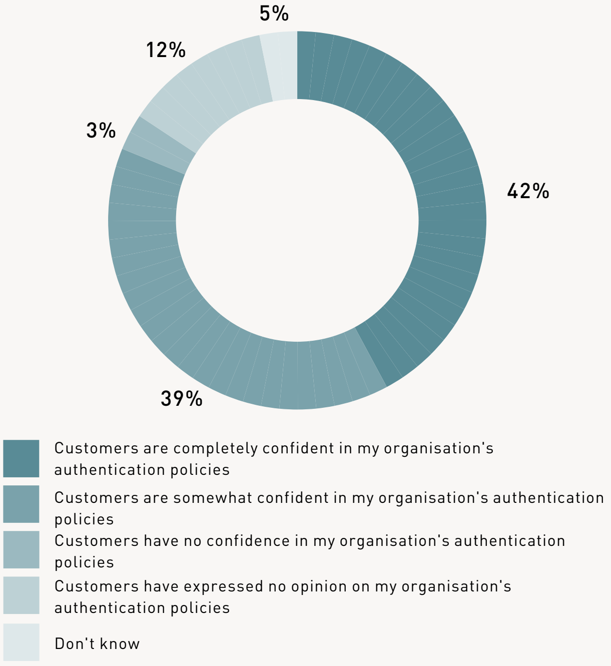
Customer feedback on authentication policies

Six in ten (60%) respondents say that their organisation's customers have provided mostly positive feedback on their authentication policies. However, over one in ten (12%) admit to this mostly being negative feedback, suggesting that these organisations need to look at improving authentication policies for their customers

Two in ten (20%) admit that their organisation does not even know how their customers rate their authentication policies, if they were to find out, they may too receive negative feedback (figure 7)

Figure 8

Would you say that your customers are confident in your organisation's authentication policies?



Asked to all 1,150 respondents

Authentication for employees and customers

The majority (58%) of IT decision makers think that the authentication methods are becoming similar (figure 2)

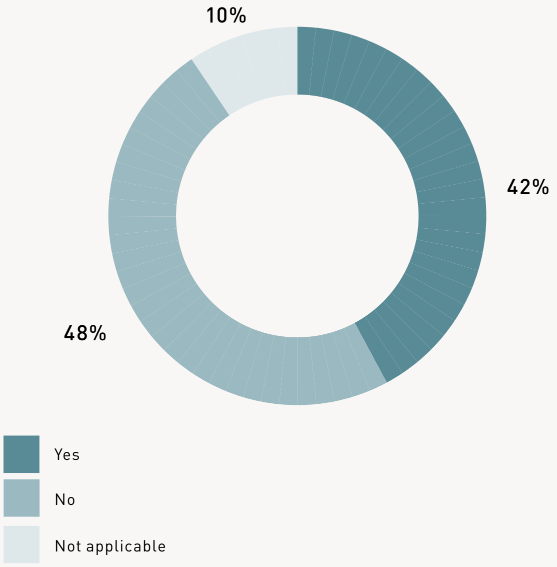
Just under half (48%) of respondents' organisations who offer online consumer services use a different authentication method for employees and consumers

The majority (62%) also think that their organisation's security team is feeling the pressure to use the same type of authentication for both parties (figure 2), which suggests that more organisations will be doing this in the near future

> While only the minority (42%) of all respondents' organisations are using the same authentication method for employees and consumers

Figure 9

Does your organisation use the same online authentication method for employees and consumers/customers?



Asked to all 1,150 respondents

Two-factor authentication

Two-factor authentication use

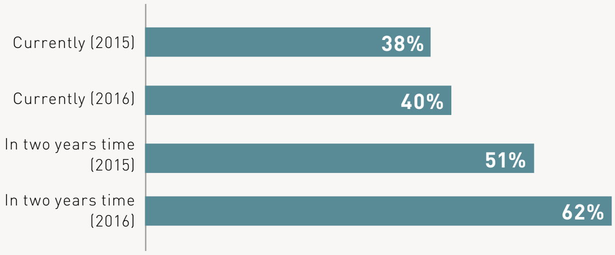
This has increased slightly, compared to 38% of users in 2015. The real difference in data between 2015 responses and 2016 comes when respondents were asked whether they were going to be using two-factor authentication in two years time, jumping from 51% in 2015 to 62% in 2016.

This indicates that perhaps respondents have switched on to the benefits of two-factor authentication in the past 12 months and the drive to implement it is gaining momentum. However the job is not complete judging by the difference in current use and the anticipates use in two years' time

? With two-factor authentication use expecting to rise, does this mean better protection for enterprise applications?

Figure 9

Does your organisation use the same online authentication method for employees and consumers/customers?



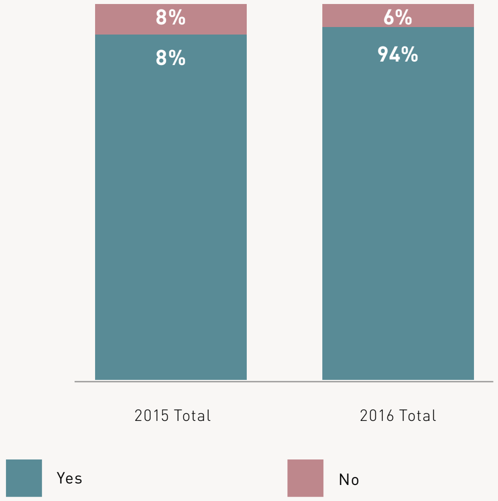
Asked to all respondents (900 in 2015, 1,150 in 2016)

Protecting applications with two-factor authentication

This has increased slightly, compared to 38% of users in 2015. The real difference in data between 2015 responses and 2016 comes when respondents were asked whether they were going to be using two-factor authentication in two years time, jumping from 51% in 2015 to 62% in 2016 This indicates that perhaps respondents have switched on to the benefits of two-factor authentication in the past 12 months and the drive to implement it is gaining momentum. However the job is not complete judging by the difference in current use and the anticipates use in two years' time

Figure 11

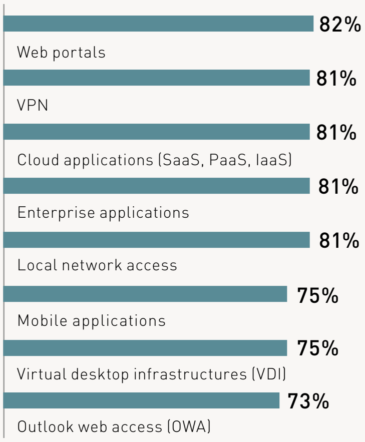
Analysis of respondents' organisations who have at least one of the listed applications in figure 10 protected by two-factor authentication. Showing results from 2015 and 2016.



Asked to all respondents (900 in 2015, 1,150 in 2016)

Figure 12.

Analysis of respondents' organisations with at least one of each application currently protected by two-factor authentication. Showing the average number of applications per type.



Asked to all 1,150 respondents

Expanding two-factor authentication use

> The vast majority (96%) of respondents expect that their organisation will expand the use of two-factor authentication to protect applications in the future

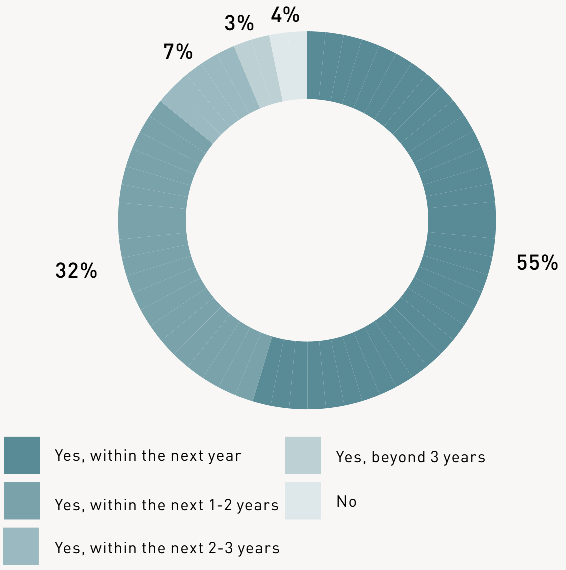
Furthermore, more than half (55%) of respondents see this expansion happening within the next year, and only 3% say this expansion will take more than three years to happen

This could be expanding into new applications that the organisations do not yet have in place, or it could be adding the functionality to existing applications where they do not yet have two-factor authentication set up

? The number of applications using two-factor authentication is set to rise, would organisations like to be able to manage this centrally?

Figure 13

Do you expect your organisation will expand the use of two-factor authentication to protect applications in the future?



Asked to all 1,150 respondents

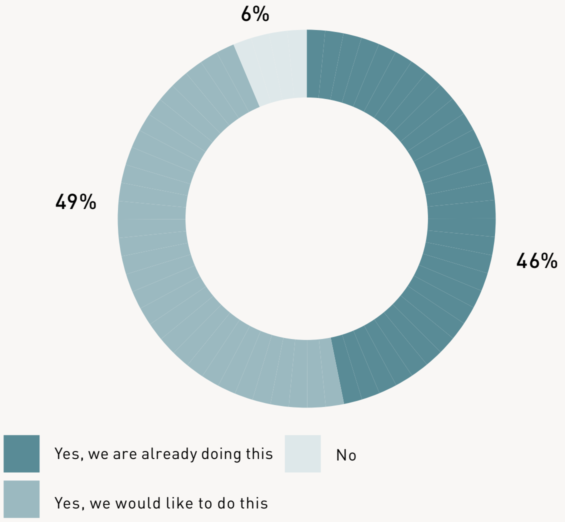
Managing two-factor authentication centrally

Over nine in ten (94%) respondents say that they would like to be able to manage two-factor authentication centrally for all applications in their organisation. However, less than half (46%) say that their organisation is already able to do this (figure 14)

Organisations who are not yet able to do this should investigate solutions that would allow them to do so, as they are likely to experience benefits from it.

Figure 14

Would you like to be able to manage two-factor authentication centrally for all applications in your organisation (cloud apps, on premises apps, VDI, enterprise apps, etc.)?



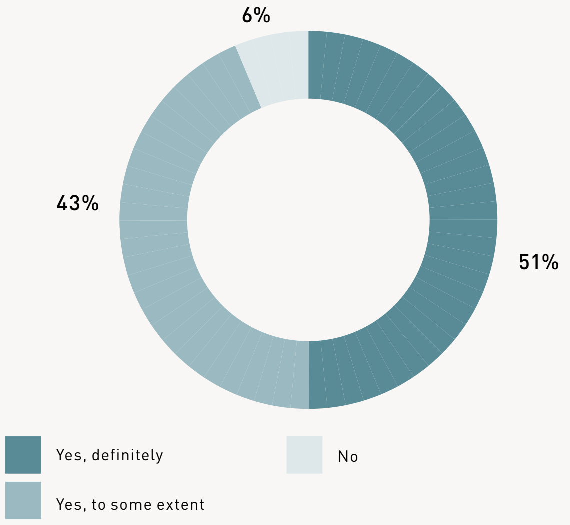
Asked to all 1,150 respondents

One of the benefits of central authentication management, according to the vast majority (96%) of respondents, is that would be conducive to reducing shadow IT within their organisation (figure 15)

As only the minority of organisations already use a central approach, the majority of organisations may be expose to the risks of shadow IT

Figure 15

Do you see central authentication management of two-factor authentication for cloud applications as being conducive to reducing shadow IT in your organisation?



Asked to the 1,077 respondents whose organisation uses cloud apps

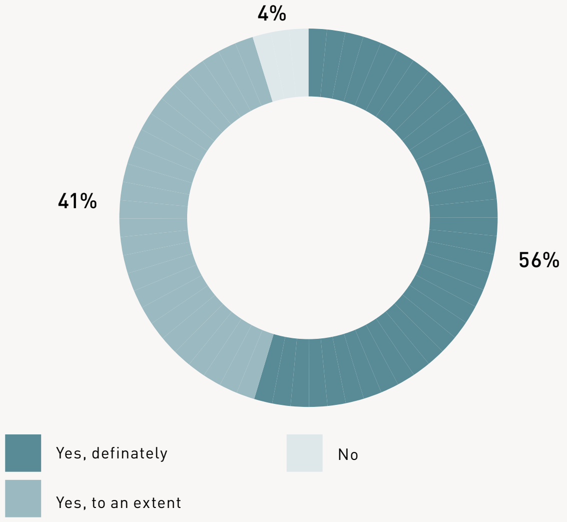
Compliance and auditing

Almost all (96%) respondents think that two-factor authentication can contribute towards their organisation's ability to comply with data protection regulations and pass security audits (figure 16)

This could be a reason why almost all respondents see the use of two-factor authentication increasing in their organisation in the future (figure 11)

Figure 16

Do you think two-factor authentication can contribute toward your organisation's ability to comply with data protection regulations and pass security audits?



Asked to all 1,150 respondents

The vast majority (96%) of respondents think that it is important that their organisation has the ability to produce a single audit trail of access events taking place throughout different resources used in the organisation (figure 17)

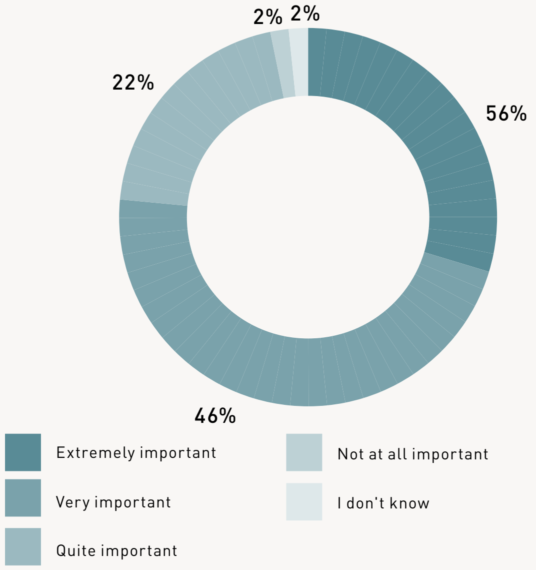
Many respondents recognise the importance of a clear audit trail and two-factor is seen as something that can help this (figure 16)

The vast majority (96%) of respondents think that it is important that their organisation has the ability to produce a single audit trail of access events taking place throughout different resources used in the organisation (figure 17)

Many respondents recognise the importance of a clear audit trail and two-factor is seen as something that can help this (figure 16)

Figure 17

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



Asked to all 1,150 respondents

Cloud access management (including SSO)

Access management capabilities

Currently, just under two in five (39%) respondents' organisations have already implemented SSO

This is similar for on-premises identity and access management (IAM) solutions and Identity-as-a-Service (IDaaS), where 38% and 36% respectively have already implemented this, and a further 47% and 45% respectively plan to.

> Almost half (49%) of respondents' organisations are planning to implement SSO in the future

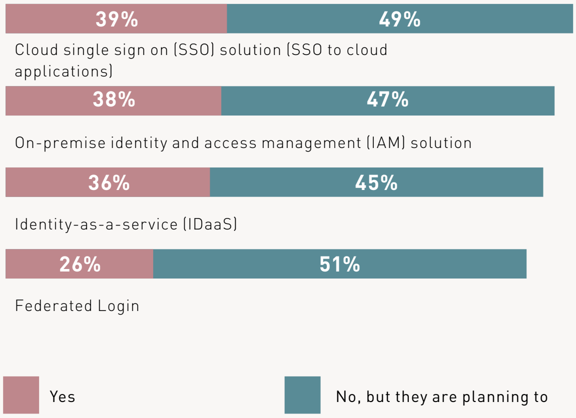
Federated Login is the access management capability that is least likely (26%) to already be implemented in respondents' organisations, however just over half (51%) say that their organisation is planning on doing this

Many IT decision makers are seeing the potential benefits of a federated login solution but are yet to take action

? How are organisations managing access to cloud apps?

Figure 18

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



Asked to all 1,150 respondents

Pressure to implement SSO

And only a minority (10%) strongly disagree that they are under pressure

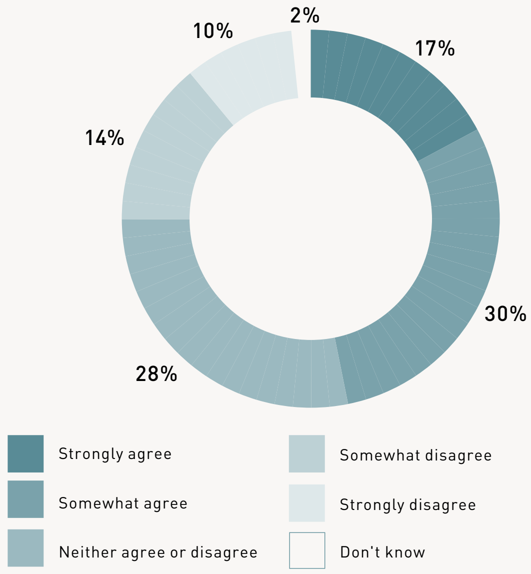
This may be why there is likely to be an increase in SSO adoption in the near future (figure 18)

An external pressure could be the high profile breaches that are already having an influence on authentication practices in respondents organisations (figure 1)

? Considering these pressures to enable SSO, is it being used to manage cloud apps in respondents organisations?

Figure 19

To what extent do you agree that your organisation is under pressure to enable SSO



Asked to all 1,150 respondents

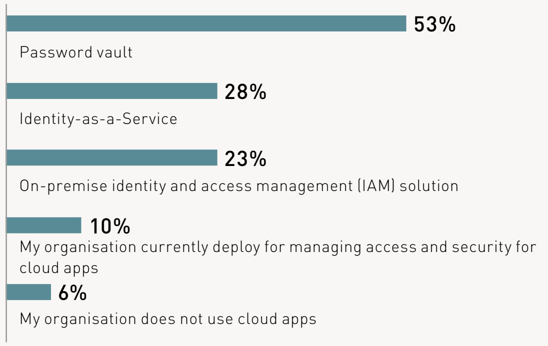
Managing access to cloud apps

One in ten (10%) respondents admit that their organisation does not currently deploy anything for managing access and security for cloud apps. These organisations are likely to be putting themselves at unnecessary risk

The most common (53%) method used for managing access and security for cloud apps among respondents' organisations is a password vault (figure 20)

Figure 20

What does your organisation currently deploy for managing access and security for cloud apps?



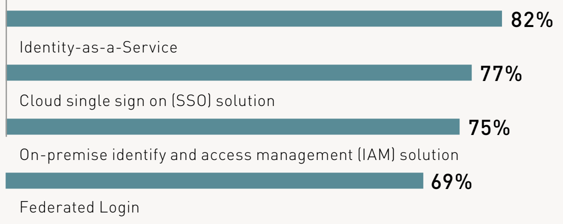
Asked to all 1,150 respondents

Where organisations have implemented an access management solution, they are likely to be using the access management offered by the service

Federated Login was the least likely method to have been implemented in respondents' organisations (figure 18), and it is the least likely to be used. However, almost seven in ten (69%) are using it where it is implemented (figure 21)

Figure 21

Does your organisation use access management offered by one of the following solutions?



Asked to all 1,150 respondents

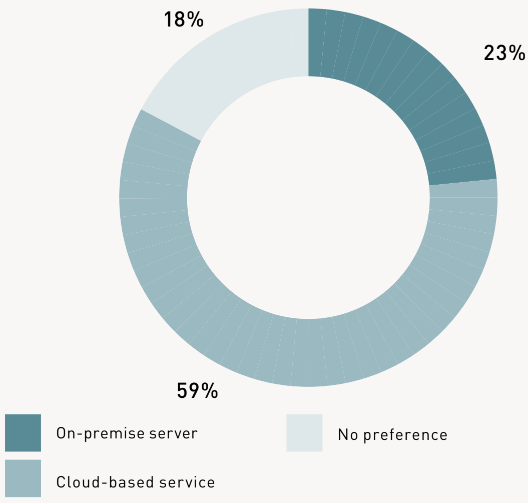
Cloud SSO solutions

Almost three in five (59%) IT decision makers surveyed would prefer to choose a cloud-based service for an SSO solution. However, there is a minority (23%) who would prefer to deploy SSO to an on-premises server (figure 22)

This preference for an on-premises or cloud based service is likely to be influenced by the infrastructure and resources of the organisation

Figure 22

As an IT professional, what method of deployment would you prefer when choosing a cloud SSO solution?

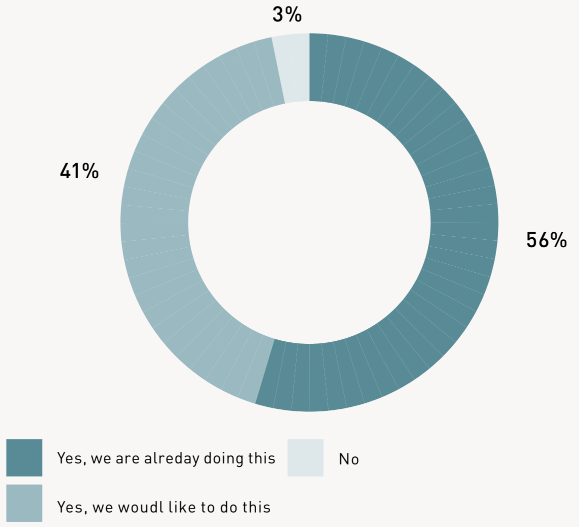


Asked to all 1,150 respondents

Where respondents' organisations have already implemented SSO, over half (56%) are already managing it centrally for all applications. A further four in ten (41%) would like to do this, but are not yet doing so (figure 23) With more than four in ten (41%) wanting to manage SSO centrally but not currently doing so, there may be barriers that are preventing more organisation doing this

Figure 23

Would you like to be able to manage SSO centrally for all applications in your organisation (cloud apps, on premises apps, VDI, enterprise apps, etc.)?



Asked to 448 the respondents whose organisation has implemented SSO

Using SSO for mobility

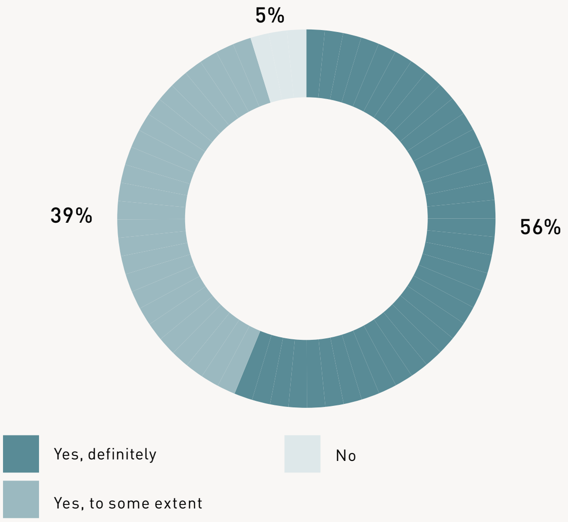
More than half (56%) definitely see this. SSO is likely to make it easier for employees to work outside the office, and also quicker to log in to cloud apps no matter their location.

> 95% of respondents see SSO for cloud apps as conducive to mobility and productivity in their organisation

Organisations desire to experience these benefits to mobility and productivity could be one of the pressures pushing organisations to enable SSO (figure 19)

Figure 24

“Do you see SSO for cloud applications as being conducive to mobility and productivity in your organisation?



Asked to the 1,077 respondents whose organisation uses cloud apps

External users and mobility

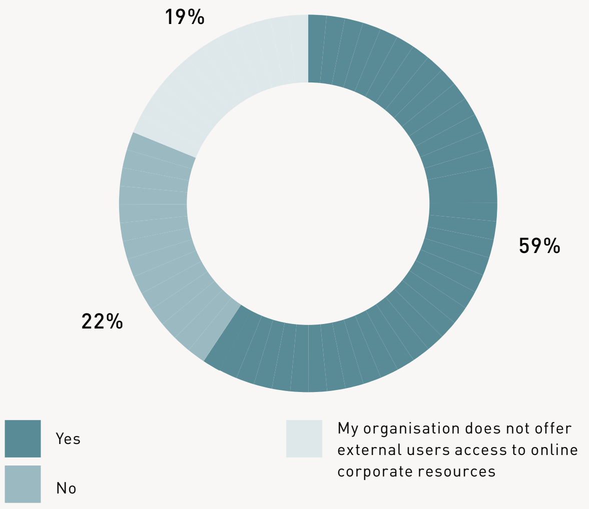
Access for external users

The majority (59%) of respondents' organisations secure external users' access to online corporate resources with two-factor authentication. However, over one in five (22%) say that they do not do this (figure 25)

Where organisations are not doing this, or do not currently offer external access, the vast majority (81%) of those surveyed say that their organisation is planning on implementing two-factor authentication in the future (figure 26). This suggests that these organisations are aware that they are putting themselves at risk, and are planning on doing something about it

Figure 25

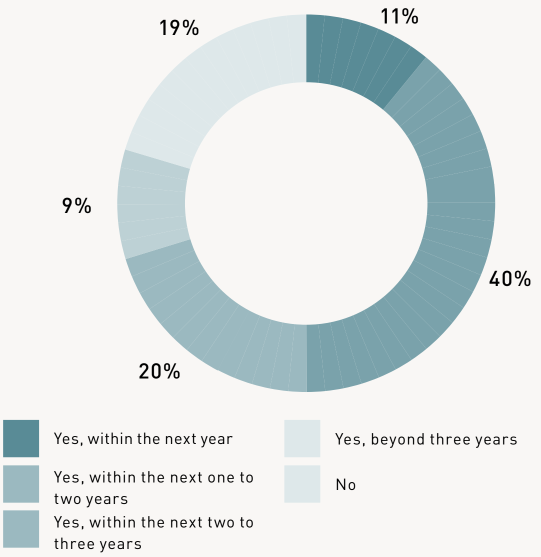
Does your organisation secure external users' (such as partners, consumers and contractors) access to online corporate resources with two-factor authentication?



Asked to all 1,150 respondents

Figure 26

Do you expect your organisation will implement two-factor authentication for external users accessing online corporate resources in the future?



Asked to the 468 respondents whose organisation does not secure external users' access to online corporate resources with two-factor authentication, or does not offer external users access at all

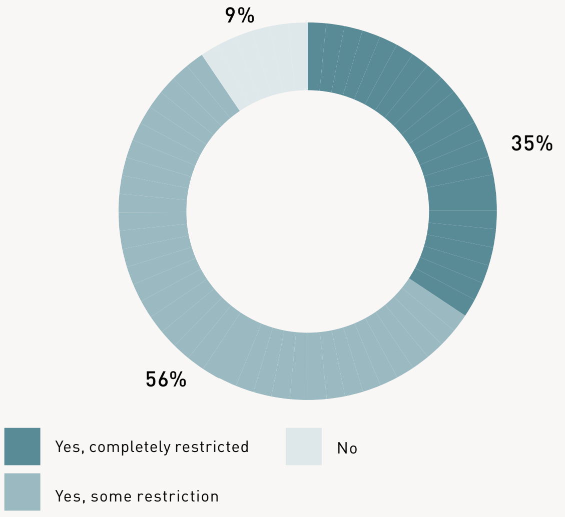
Using mobile devices to access corporate resources

Just over nine in ten (91%) respondents' organisations restrict users from accessing corporate resources from mobile devices, however only 35% say that users are completely restricted (figure 27)

Perhaps the 56% who are offering some restriction are not confident enough in their security to remove them

Figure 27

Does your organisation restrict users from accessing corporate resources from mobile devices, such as smartphones and tablets



Asked to all 1,150 respondents

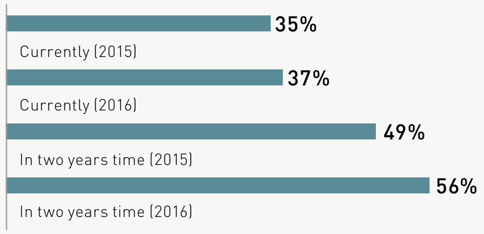
Using mobile devices to access corporate resources

Currently, 37% of users in respondents' organisations, on average, are required to use two-factor authentication to access corporate resources from mobile devices - this has slightly increased from an 35% of users in 2015, on average

The percentage of users required to do this is set to increase further, with respondents estimating 56% of users will be required to do this in two years' time, on average (figure 28)

Figure 28

Analysis of the average percentage of users in respondents' organisations who are currently required to use two-factor authentication to access corporate resources from mobile devices, and the expected percentage in two years' time. Showing results from 2015 and 2016.



Asked to all respondents (900 in 2015, 1,150 in 2016)

Users requiring remote access

This has very slightly increased since 2015, where the average was 42%

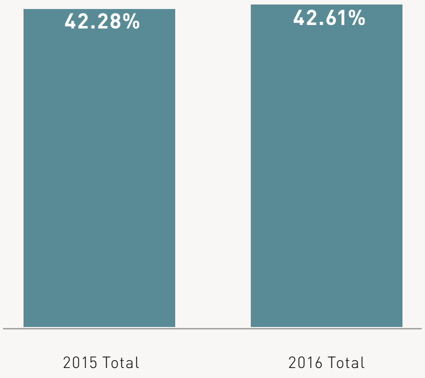
Organisations need to ensure that they are providing their users with a secure method to gain access to corporate applications remotely, as a significant number of employees need/want that access

> 43% of users in respondents' organisations require remote access to corporate applications, on average

? What authentication methods are organisations using?

Figure 29

Analysis of the average percentage of users that require remote access to corporate applications in respondents' organisations. Showing results from 2015 and 2016. .



Asked to all respondents (900 in 2015, 1,150 in 2016)

> Username and password (68%) is the most widely used authentication method by users for mobility in respondents' organisations

Authentication methods

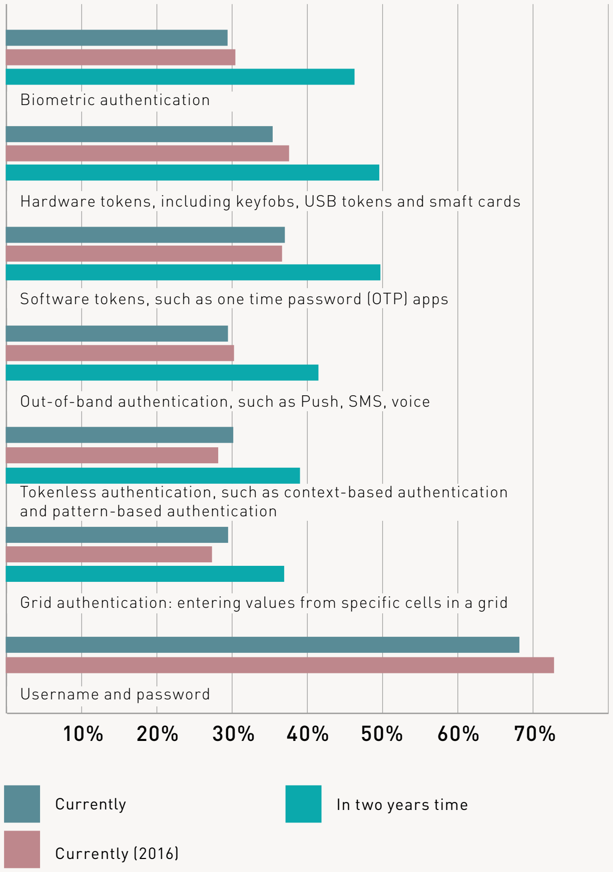
There has been a slight decline in the average percentage of users who use tokenless authentication (30% in 2015 down to 28% in 2016) and grid authentication (29% in 2015 down to 27% in 2016)

However, respondents estimate that a greater proportion of their organisation's users will be using each authentication method in two years' time. This suggests that organisations are looking to increase their mobility security using several different methods

? What events would trigger an increased stakeholder buy-in of an authentication solution?

Figure 30

Analysis of the average percentage of users that use the above authentication methods for mobility currently in respondents' organisations, and the estimated average percentage in two years' time. Showing results from 2015 and 2016.



Showing results from 2015 and 2016. Asked to all respondents (900 in 2015, 1,150 in 2016) The answer option 'Username and password' was not provided in 2015

Stakeholder buy-in of authentication solution for mobility

> Nine in ten (90%) respondents think that an event could increase stakeholder buy-in of an authentication solution that supports increased user mobility in their organisation

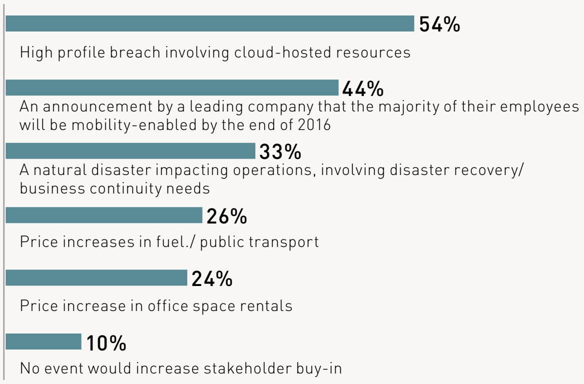
A high profile breach involving cloud-hosted resources is the most likely (54%) event to increase stakeholder buy-in in respondents' organisations.

A significant minority (44%) also think that stakeholder buy-in would increase if there was an announcement by a leading company that the majority of their employees will be mobility-enabled by the end of the year

? What is holding organisations back from investing further in mobility?

Figure 31

Which of the following events would increase stakeholder buy-in of an authentication solution that supports increased user mobility in your organisation?



Asked to all 1,150 respondents

Challenges to increasing user mobility

Security concerns are the main obstacle for half (50%) of respondents' organisations

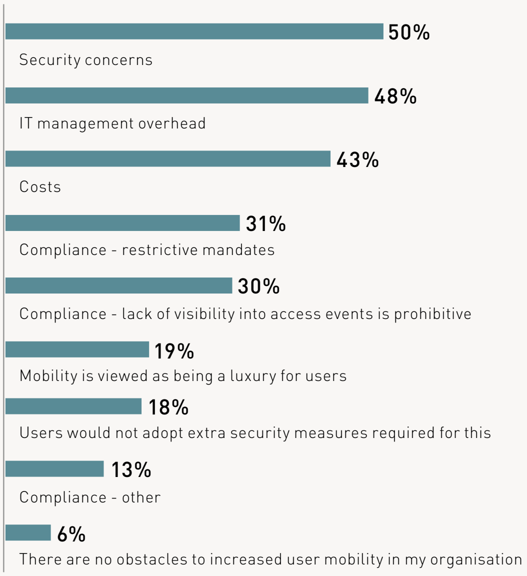
Other common obstacles include IT management overheads (48%) and costs (43%), however both of these are only seen by a minority of respondents' organisations

> The vast majority (94%) of respondents admit that there are obstacles to increased user mobility in their organisation

In fact, there is no clear majority obstacle, suggesting that different organisations are facing a variety of different obstacles when it comes to increasing user mobility.

Figure 32

What are the main obstacles to increased user mobility in your organisation?



Asked to all 1,150 respondents

Decision-making process for authentication

Decision-makers when selecting a two-factor authentication solution

Where the CIO/head of IT is not the final decision maker, they are likely (44%) to be involved in the decision, and are not involved in only 3% of organisations. The CSO is the second most likely role to have an involvement (93%) in this decision

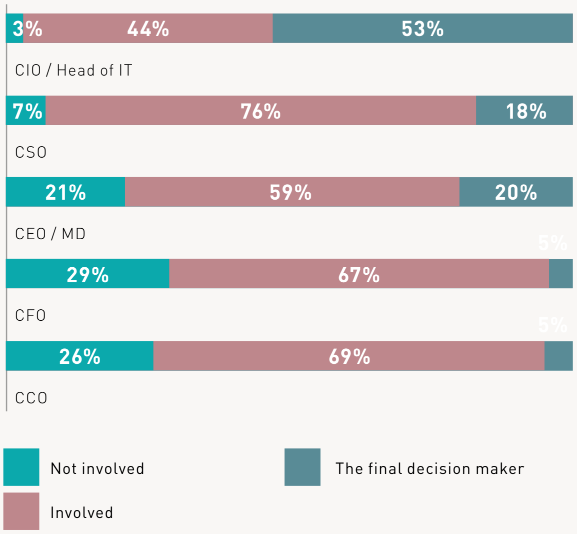
The two most likely roles to have involvement in selecting a two-factor authentication solution are both intrinsically linked to IT and IT security (CIO and CSO), compared to roles that may be occupied by individuals with less knowledge or experience in IT (CEO/MD, CFO, CCO)

> For over half (53%) of respondents' organisations the CIO/head of IT is the final decision maker when selecting the two-factor authentication solution

What considerations do decision makers make when choosing two-factor authentication?

Figure 33

Who is involved, and to what extent, in the decision-making process when selecting a two-factor authentication solution for your organisation?"



Asked to all 1,150 respondents

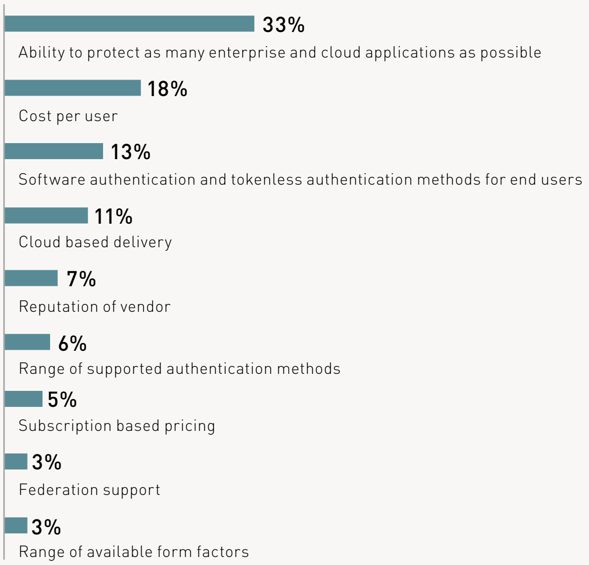
Considerations and criteria when selecting two-factor authentication

When sourcing a two-factor authentication solution a third (33%) of respondents say that the ability to protect as many enterprise and cloud applications as possible is the most significant consideration (figure 34)

This may be because organisations assume that this will allow them to manage the solutions centrally for each application, which is something the majority would like to do (figure 14)

Figure 34

Analysis of the respondents who said each factor is the most significant consideration when sourcing a two-factor authentication solution



Asked to all 1,150 respondents

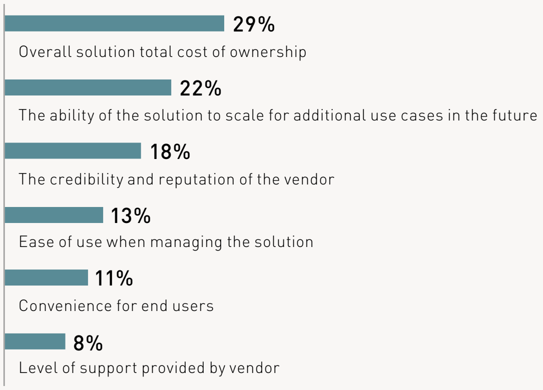
For more detailed analysis and regional data please visit: **www.gemalto.com/aim**

When sourcing a two-factor authentication solution a third (33%) of respondents say that the ability to protect as many enterprise and cloud applications as possible is the most significant consideration (figure 34)

This may be because organisations assume that this will allow them to manage the solutions centrally for each application, which is something the majority would like to do (figure 14)

Figure 35

Analysis of the respondents who said that the above factors are the most significant consideration in their organisation for selecting a two-factor authentication solution

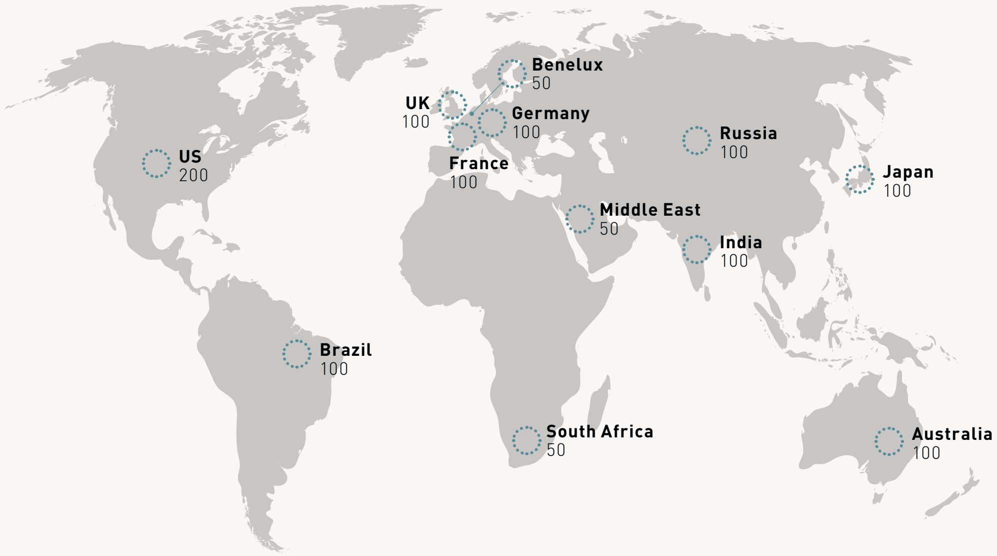


Asked to all 1,150 respondents

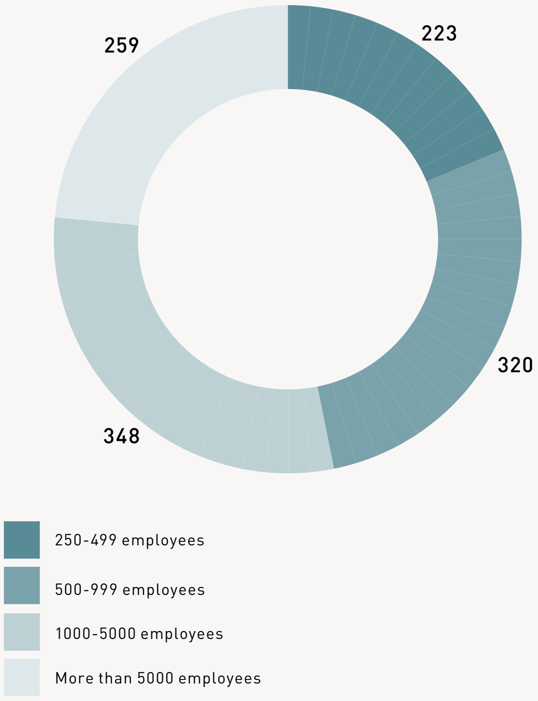
Demographics

1,150 IT decision makers were interviewed in August and September 2016, split in the following ways

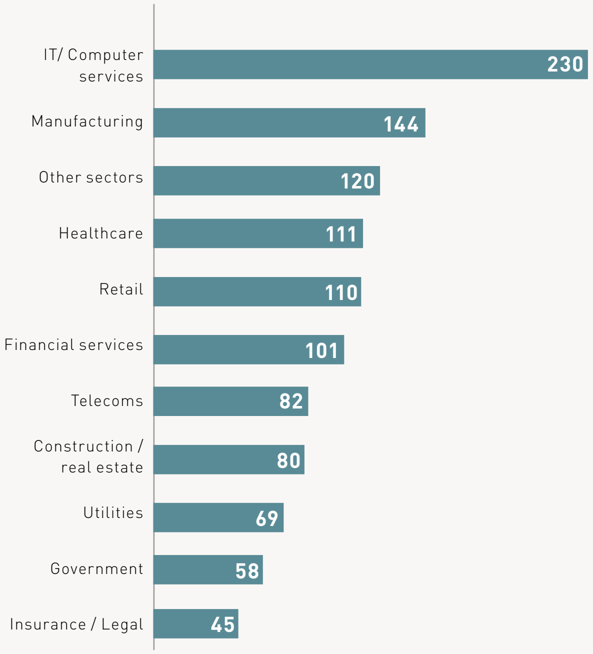
Country



Size



Sector



Gemalto offers one of the most complete portfolios of enterprise security solutions in the world, enabling its customers to enjoy industry-leading protection of digital identities, transactions, payments and data – from the edge to the core. Gemalto's portfolio of SafeNet Identity and Data Protection solutions enable enterprises across many verticals, including major financial institutions and governments, to take a data-centric approach to security by utilizing innovative encryption methods, best-in-class crypto management techniques, and strong authentication and identity management solutions to protect what matters, where it matters. Through these solutions, Gemalto helps organizations achieve compliance with stringent data privacy regulations and ensure that sensitive corporate assets, customer information, and digital transactions are safe from exposure and manipulation in order to protect customer trust in an increasingly digital world.

GEMALTO.COM/AIM

gemalto
security to be free