Businesses under pressure
Employees want same simple access to cloud applications as consumers

The proliferation of cloud applications and use of a disparate range of devices within businesses has led to nearly two-thirds of IT decision makers admitting that their security teams are considering implementing consumer-grade access to cloud services for employees. Surveying more than 1,000 IT decision makers globally, Gemalto’s 2018 Identity and Access Management Index reveals that the majority believe that the authentication methods they implement in their businesses are not as good compared to those found on popular sites including Amazon and Facebook.

The key findings of this report clearly show that IT decision makers are struggling to balance the need for a simple and easy login experience with security. While there is a need to make things easier for employees, there is a fine line to be walked. IT and business line managers would do best to figure out the risks and sensitivities associated with the various applications used in their organizations and then use access management policies to manage risk and apply the appropriate authentication method. In this way, they can ensure a convenient login experience for their users, while still maintaining access security.
SECTION 1

External influences on access management practices
External influences on access management practices

Nine in ten IT decision maker respondents state that their organization’s security policies around access management have been influenced by breaches of consumer services, which shows how powerful these breaches can be. Concerns over breaches has resulted in increased spending on access management (forty five percent), staff being trained on security and access management (forty four percent), and more resources being allocated to access management (forty two percent). In addition, around two in five say that secure access management is now a priority for the board (thirty eight percent), rising slightly from thirty four percent in 2016 [Fig 1]. It is evident from the changes made as a result of consumer service breaches that businesses take these very seriously. While they may not have been directly impacted, the ripple effect is clear.

We have increased spending on access management 45%
Staff are now trained on security and access management 44%
More resources are allocated to access management 42%
Secure access management is now a priority for the board 38%
We have sought outside expert help through consultants or outsourcing 33%
We now have a dedicated CISO (or equivalent) with responsibility for information security 28%
Policies have less focus on the uptake of cloud 9%
My organization’s security policies around access management have not been influenced 10%

Fig 1
How has your organization’s security policies around access management been influenced by breaches of consumer services?

Ninety percent of respondents admit that their organization’s security policies around access management have been influenced by breaches of consumer services.
Influence of consumer authentication solutions

Seven in ten respondents agree that authentication methods used in the consumer world can be applied to ensuring secure access to enterprise resources. So it’s perhaps unsurprising to hear that around two in three believe that their organization’s security team is feeling under pressure to provide the same type of authentication for employees as consumer services. Surprisingly, over half of respondents indicate that their organization’s level of employee authentication is not as good as those offered by consumer websites, such as Facebook or Amazon (Fig 2).

On the other hand, the vast majority of respondents are concerned about employees at their organization reusing personal credentials for work purposes. While it may be difficult to align these findings they indicate that there is a clear desire on the part of IT professionals to meet user expectations about convenience, keep up with consumer trends and maintain security.

Over half say that their employee authentication is not as good as those offered by consumer websites such as Facebook or Amazon.

![Image: Analysis of respondents who agree with the above statements]
Use of personal credentials at work

The survey also highlights the extent to which social media platforms play a role in marketing. Interestingly, despite social platforms having been used in the past as an attack route for malicious actors to breach organizations, it seems IT departments fall short in being able to apply cohesive access security for social platforms. For example, over two fifths indicate that employees use a company-approved individual account when using social media for work.

Around four in ten say that employees use a company-wide account when using social media for work, and three in ten report that employees use their own personal accounts, which suggests that there is no one method that is leading the way when it comes to social media accounts and policies [Fig 5].

Ninety two percent are concerned about employees at their organization reusing personal credentials for work purposes.
Social media security

Over half of respondents report that their organization secures access to its social media accounts via a relatively simplistic method of username and password, a slight drop from the sixty five percent who reported doing so in 2016.

Meanwhile, around two in five say that their organization uses native two-factor authentication provided by social media sites, but this also drops from forty two percent in 2016 (Fig 6).

Approaches towards social media vary, with the majority having a preferred approach and security method.
SECTION 2
Two-factor authentication
Two-factor authentication use in organizations

On average, respondents indicate that around two fifths of users in their organization use two-factor authentication currently, and that they expect this to rise quite significantly to sixty percent in two years’ time [Fig 7].

Fig 7
Analysis of the average percentages of users in respondents’ organizations who use two-factor authentication currently, and who are expected to use two-factor authentication in two years’ time, showing historical data.

Two-factor authentication usage is expected to increase, but there could be barriers.
Applications protected by two-factor authentication

The vast majority of respondents’ organizations are using two-factor authentication for at least one application. Specifically, just under eight in ten respondents report their organization has at least one application that is currently protected by two-factor authentication for cloud applications (SaaS, PaaS, IaaS), seventy eight percent for local network access and web portals, with seventy seven percent for VPN and enterprise applications 77% [Fig 8].

On average organizations are protecting three cloud applications using two-factor authentication, while according to a recent Ponemon Study, they use an average twenty seven cloud applications that they could be securing.
Biggest targets for cyber-attacks

Data shows that there is a correlation between the use of two-factor authentication and the perceived sensitivity of an application, as these same applications are amongst those that respondents consider most likely to be targeted for cyber-attacks. Around half highlight web portals as one of the biggest targets, around two in five say the same for cloud applications (SaaS, PaaS, IaaS), thirty nine percent mobile applications, thirty seven percent local network access and just under three in ten say so for VPN.

In addition, two fifths of respondents consider unprotected infrastructure (e.g. new IoT devices) to be a big target for cyber-attacks [Fig 9]. Given that each application represents an attack route for potential cyber-attacks, organizations are facing a rising challenge in securing access and achieving a cohesive access strategy across the board with this large number of targets.

Web portals and unprotected infrastructure are the biggest targets for cyber-attacks.

**Fig 9**
In general, which of the following do you think are the biggest targets for cyber-attacks?
Expanding use of two-factor authentication

Almost all respondents expect their organization to expand the use of two-factor authentication to protect applications in the future, with nearly half expecting this to happen within the next year, suggesting that mainstream adoption is only around the corner. On average, respondents expect it to take 15 months for their organization to expand the use of two-factor authentication to protect applications [Fig 10], although with the right support, this could be sooner.

96% expect that their organization will expand their use of two-factor authentication to protect all applications in the future.

Fig 10
Do you expect your organization will expand the use of two-factor authentication to protect applications in the future?
Managing two-factor authentication centrally

Over half of respondents report that their organization is already managing two-factor authentication centrally for all applications, and over a third say that their organization is not but would like to be. Thinking about the previous year’s research, the fifty eight percent of those who are already doing this has grown considerably from the forty six percent reported in 2016 (Fig 11) and this only seems set to increase.

---

58% are already managing two-factor authentication centrally for all applications (an increase on previous years).
Dealing with compliance and auditing

Nearly all respondents think that two-factor authentication will be able to contribute towards their organization’s ability to comply with data protection regulations and pass security audits, with over half believing that this is definitely the case [Fig 12]. Similarly, the majority of respondents believe that it is important that their organization is able to produce a single audit trail of access events taking place throughout different resources used by the organization, with nearly three in ten viewing this as extremely important [Fig 13]. The ability to encourage better compliance and easier auditing may not often be the primary reason to implement two-factor authentication, but is certainly an added bonus.

**Fig 12**
Do you think access management (including two-factor authentication) can contribute towards your organization’s ability to comply with data protection regulations and pass security audits [e.g. General Data Protection Regulation - GDPR]?  

- Yes, definitely: 54%  
- Yes, to an extent: 42%  
- No, not at all: 4%  

**Fig 13**
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?  

- Extremely important: 29%  
- Very important: 46%  
- Quite important: 21%  
- Not at all important: 2%  
- I don’t know: 2%

Almost all say that access management can contribute towards their organization’s ability to comply with data protection regulations and pass security audits [e.g. GDPR].
SECTION 3

Cloud access management (including SSO)
Targeting cloud applications for cyber-attack

Over four in ten respondents see cloud applications as one of the biggest targets for cyber-attacks [Fig 15]. Of these respondents, seventy one percent indicate the reason behind this may be the increasing volume of cloud applications in use, and fifty five percent, the lack of strong cyber security solutions to implement appropriate solutions. Over two fifths also indicate cloud applications may be targeted for cyber attacks because access management solutions are currently in place for the cloud are poor, which is something that organizations could improve [Fig 14].

Cloud applications could be a target for cyber-attacks, largely due to the increasing volume and lack of strong security.

Fig 14
Why do you feel that cloud applications are a target for cyber-attacks?”, asked to respondents who think that cloud applications [SaaS, PaaS, IaaS] are a target for cyber-attacks (426)

![Graph showing reasons for cloud applications being a target for cyber-attacks]

- The increasing volume of cloud applications in use: 71%
- Lack of strong cyber security solutions to implement appropriate solutions: 55%
- Lack of in-house skills to secure cloud applications: 51%
- Poor access management solutions in place for the cloud: 42%
- Organizations have poor visibility over their applications in the cloud: 35%

Fig 15
Analysis of those who think cloud applications are one of the biggest targets for cyber-attacks.
Implementation of access management capabilities

More than four in ten respondents report that their organization has already implemented cloud single sign on (SSO) solutions as an access management capability, an increase on the thirty nine percent who had done so in 2016 – a small but positive step forward. A further forty seven percent report that their organization is planning to implement cloud SSO, with almost a quarter planning to do so within the next year (Fig 16).

Furthermore, nearly six in ten agree that their organization is under pressure to enable SSO, an increase on the forty seven percent who reported the same in 2016 (Fig 17).

96% expect that their organization will expand their use of two-factor authentication to protect all applications in the future.
Drivers for access management/SSO implementation

Regarding their organization’s main drivers for implementing an access management or cloud single sign on solution, More than nine in ten respondents report security concerns, the threat of large scale breaches, with ninety percent reporting visibility and compliance concerns relating to cloud access events, and eighty eight percent announcing inefficient cloud identity management among their considerations. Nearly a quarter report the threat of large scale breaches is the most significant consideration for their organization, suggesting media coverage of large scale breaches is sinking in (Fig 18).

There is an array of drivers for implementing an access management or cloud single sign on solution.

Fig 18
What are the main drivers for implementing an access management or cloud single sign on solution in your organization?
Cloud SSO solutions

When it comes to choosing a SSO solution, six in ten would choose a cloud-based service as their preferred method of deployment, with less than a quarter indicating they would prefer on-premises server deployment, highlighting the prevalence of cloud in organizations (Fig 19).

Encouragingly, two fifths report their organization is already managing SSO centrally for all applications. Meanwhile, a further fifty percent report they are not currently doing this, but that they would like to be able to do so (Fig 20).

Only forty percent manage SSO centrally, but half would like to do this.
The impact of SSO on cloud adoption in general

The majority of respondents see cloud access management (such as SSO) for cloud applications as being conducive to facilitating cloud adoption, with forty eight percent believing that this is definitely the case (Fig 21).

Around nine in ten (91%) say that cloud access management for cloud applications is conducive to facilitating cloud adoption.

Furthermore, nearly all respondents believe that ineffective cloud access management can or does cause issues for their organization, with over half commonly reported being cloud becoming a security issue. Around four in ten report IT staff’s time being used less efficiently, an increase from thirty eight percent in operational overheads and IT costs, and thirty seven percent larger scale breaches due to a lack of visibility over cloud as other potential issues caused by ineffective cloud access management (Fig 22).

Impacts are likely to be seen as a result of ineffective cloud access management.

Cloud becoming a security issue: 52%
IT staff’s time being used less efficiently: 41%
Increase in operational overheads and IT costs: 38%
Larger scale breaches due to a lack of visibility over cloud: 37%
Slower adoption of cloud: 37%
Shadow IT taking place: 33%
Duplication of cloud applications: 22%
There is/would be no impact: 4%
Don’t know: 2%

Fig 22
What impacts does/could your organization see as a result of ineffective cloud access management?
External users’ access to corporate resources/applications

Currently, only forty three percent of respondents indicate their organization uses two-factor authentication to secure external users’ access to online corporate resources [Fig 23]. However, a further forty six percent plan to introduce this in future, suggesting many organizations are not finished on their two-factor authentication journey [Fig 24].

Only forty three percent of organizations secure external users’ access to online corporate resources with two-factor authentication.

![Image]

**Fig 23**
Does your organization secure external users’ (such as partners, consumers and contractors) access to online corporate resources with two-factor authentication?

| Yes | 43% |
| No, but we will within the next year | 23% |
| No, but we will within the next 1-2 years | 14% |
| No, but we will within the next 2-3 years | 5% |
| No, but we will beyond 3 years | 4% |
| My organization does not offer, or plan to offer, external users access to online corporate resources | 11% |

**Fig 24**
Analysis of the average percentage of respondents’ organizations’ users that require remote access to corporate applications.

Users in respondents’ organizations that require remote access to corporate applications, on average

43%
Policies for accessing corporate resources

The vast majority of respondents report that at least some of their organization’s users require remote access to corporate applications. On average, this is the case for forty-three percent of users. Nearly nine in ten respondents say their organization restricts users from accessing corporate resources from mobile devices on some level, however, slightly worryingly, only thirty-five percent report their organization has complete restrictions in place (Fig 25).

Currently, thirty-six percent of organization’s users are required to use two-factor authentication to access corporate resources from mobile devices, and this proportion on average is expected to rise to fifty-seven percent in two years’ time, which falls in line with the anticipated usage increase (Fig 26).

Most organizations restrict users from accessing corporate resources from mobile devices, with an average of thirty-six percent of users being required to use two-factor authentication when accessing corporate resources from mobile devices.

Fig 25
Does your organization restrict users from accessing corporate resources from mobile devices, such as smartphones and tablets?

Fig 26
Analysis of the average percentage of users in respondents’ organizations who are required/expected to be required in two years’ time to use two-factor authentication when accessing corporate resources from mobile devices, showing historical data.
The majority of organizations’ respondents say there are obstacles to increasing user mobility in their organization. Half indicate that security concerns are among these, with other commonly cited obstacles being around data compliance: two fifths think restrictive mandates, thirty nine percent think a lack of centralized visibility into access events, and twenty seven percent think other data compliance issues [Fig 27].

Ninety five percent of those surveyed admit that there are obstacles to increasing user mobility in their organization.

Fig 27
What are the main obstacles to increased user mobility in your organization?
Employee vs. consumer authentication methods

Over two fifths of respondents report their organization is using the same authentication method for employees and consumers/customers, but on the flipside, the same proportion indicate their organization is using different authentication methods for these groups [Fig 28].

Organizations are not always using the same authentication method for employees as consumers/customers, which could be ineffective and inefficient.

Despite this, around two thirds of respondents agree employee and consumer authentication methods are becoming very similar, and fifty six percent agree that employees and consumers will be using the same credentials to access both corporate and consumer online services in three years’ time. So we should be anticipating the authentication methods that we use to change in the near future [Fig 29].

Fig 28
Does your organization use the same authentication method for employees and consumers/customers?

- Yes, we use the same authentication for employees and consumers/customers
- No, we use different authentication for employees and consumers/customers
- Not applicable, we do not offer consumer online services

Fig 29
Analysis of respondents who agree with the above statements.

Employee and consumer authentication methods are becoming very similar

In 3 years’ time, employees and consumers will be using the same credentials to access both corporate and consumer online services

- 45% Yes, we use the same authentication
- 45% No, we use different authentication
- 10% Not applicable

56% In 3 years’ time, employees and consumers will be using the same credentials
Authentication methods in use

Respondents report, on average, sixty nine percent of staff are still using usernames and passwords as authentication methods - more than any other authentication method. However, this is only expected to rise to seventy one percent in two years’ time.

Conversely, although respondents report only just over a quarter of their organization’s users are currently using biometric authentication, this is expected to rise to forty four percent in two years’ time, a much larger jump, suggesting that more advanced methods are on the horizon (Fig 30).

![Chart showing various authentication methods and their usage percentages.]

**Fig 30** Analysis of the average percentage of users in respondents’ organizations who use the above authentication methods currently/are expected to use them in two years’ time.
Authentication methods in use

Similarly, respondents report around a third of users in their organization use software tokens and hardware tokens currently. These methods are also expected to rise considerably over the next two years, with approaching half expected to use software tokens, and forty six percent for hardware tokens in this time frame. Likewise, increases in usage are also expected for the following authentication methods: out-of-band authentication, tokenless authentication, and social identity credentials, which are all expected to rise from just under three in ten to just under four in ten (Fig 31).

In general, a similar proportion of users report using these authentication methods now, when compared with 2016 and 2015.

---

Fig 31
Analysis of the average percentage of users in respondents’ organizations who use the above authentication methods currently, showing historical data.
Demographics

1,050 IT decision makers were interviewed in September, October and November 2017, Split by Country, Industry and employee size.
Breaches and cloud proliferation bringing a mindset shift

The rapid increase of cloud applications has brought organizations lots of benefits, but also caused a high degree of fragmentation in their ability to manage access security across numerous cloud and on-premises applications. Without effective access management in place, this is liable to lead to higher risk of breach, a lack of visibility into access events, regulatory oversite - and hamper organizations’ ability to scale in the cloud.

Recent high-profile data breaches are influencing businesses’ security policies, with nine in 10 respondents admitting making changes as a result. In fact, the role of a dedicated Chief Information Security Officer within organizations has increased by a quarter in the last year, while 58% of businesses have implemented access management solutions to account for these concerns.

Research By Vanson Bourne
Vanson Bourne is an independent specialist in market research for the technology sector. Our 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

For regional data, visit the Access Management Index website: www2.gemalto.com/authentication-identity-management-index/

Learn more about Gemalto’s SafeNet Access Management Solutions: https://safenet.gemalto.com/access-management/
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.