thalescpl.com

THALES

The Challenges of Trusted Access in a Cloud-First World

2019 Thales Access Management Index

Executive Summary

#AMI2019

Contents

Introduction

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

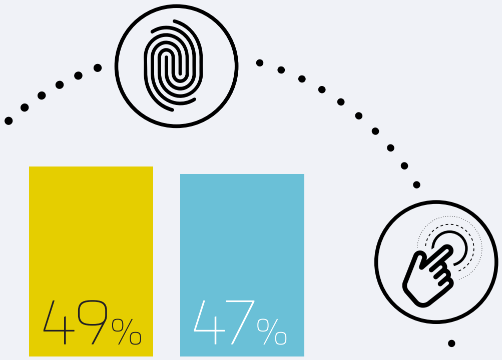
49%

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

Top access management technologies

58%

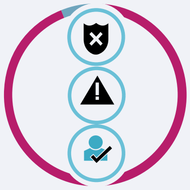
believe two-factor authentication is the best access management tool to protect cloud and web-based apps



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

Key Findings

Data breaches driving access management adoption



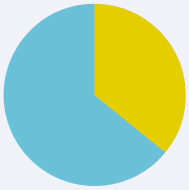
94%

of organizations' security policies have been influenced by consumer breaches in the last 12 months

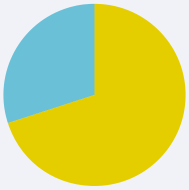
62%

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

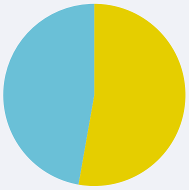
Access management is essential for cloud transformation



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

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 polices, access management practices are evolving to bridge the nexus of cloud, mobile and social.

Over half (54%) of interviewed ITDMs report that 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.

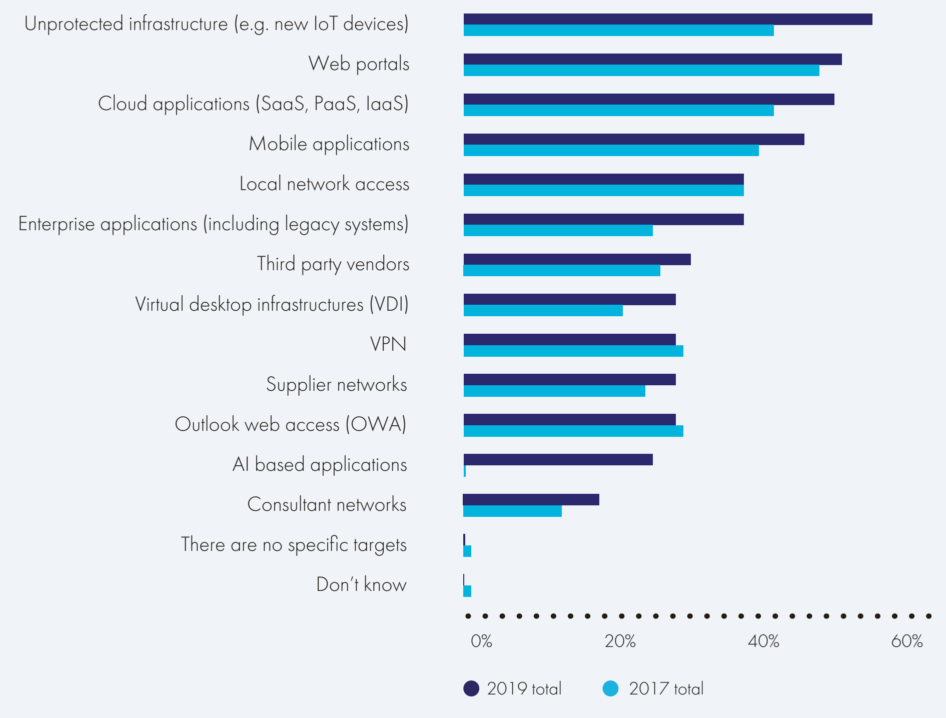


Figure 1
"In general, which of the following do you think are the biggest targets for cyber-attacks?", split by historic data, asked to all respondents (1,050 respondents)

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.

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.

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.

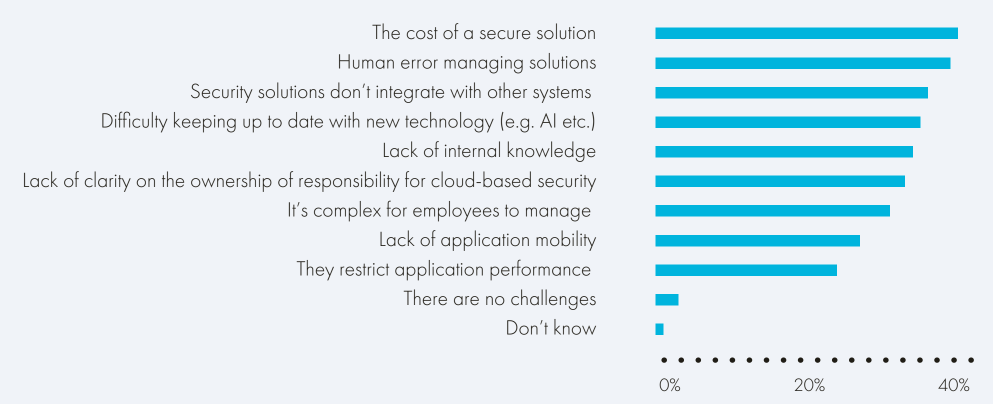


Figure 2
"What do you think the challenges are to cloud-based security and authentication?", asked to all respondents (1,050 respondents)

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%).

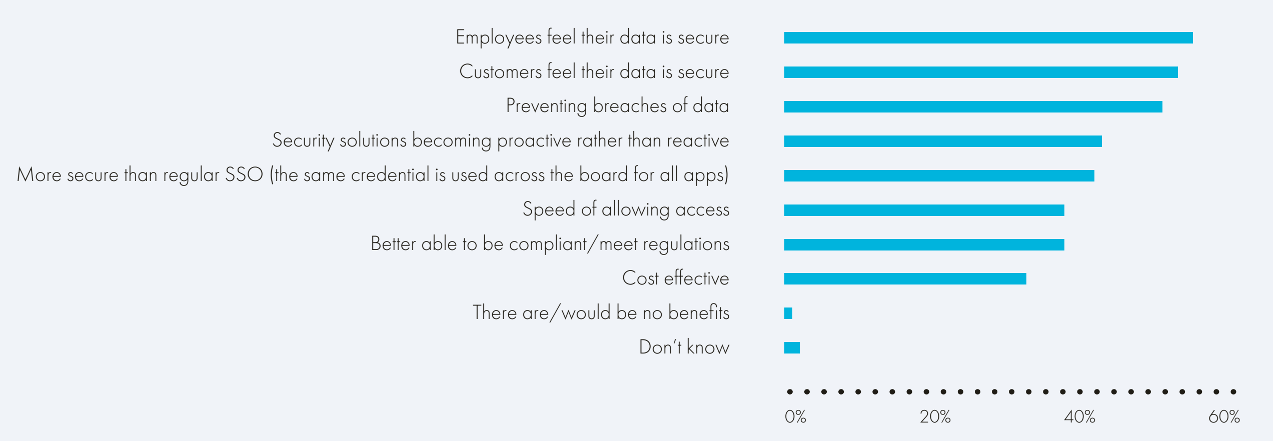


Figure 3
"What are/would be the benefits of your organization using smart SSO?", asked to all respondents (1,050 respondents)

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%).

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.

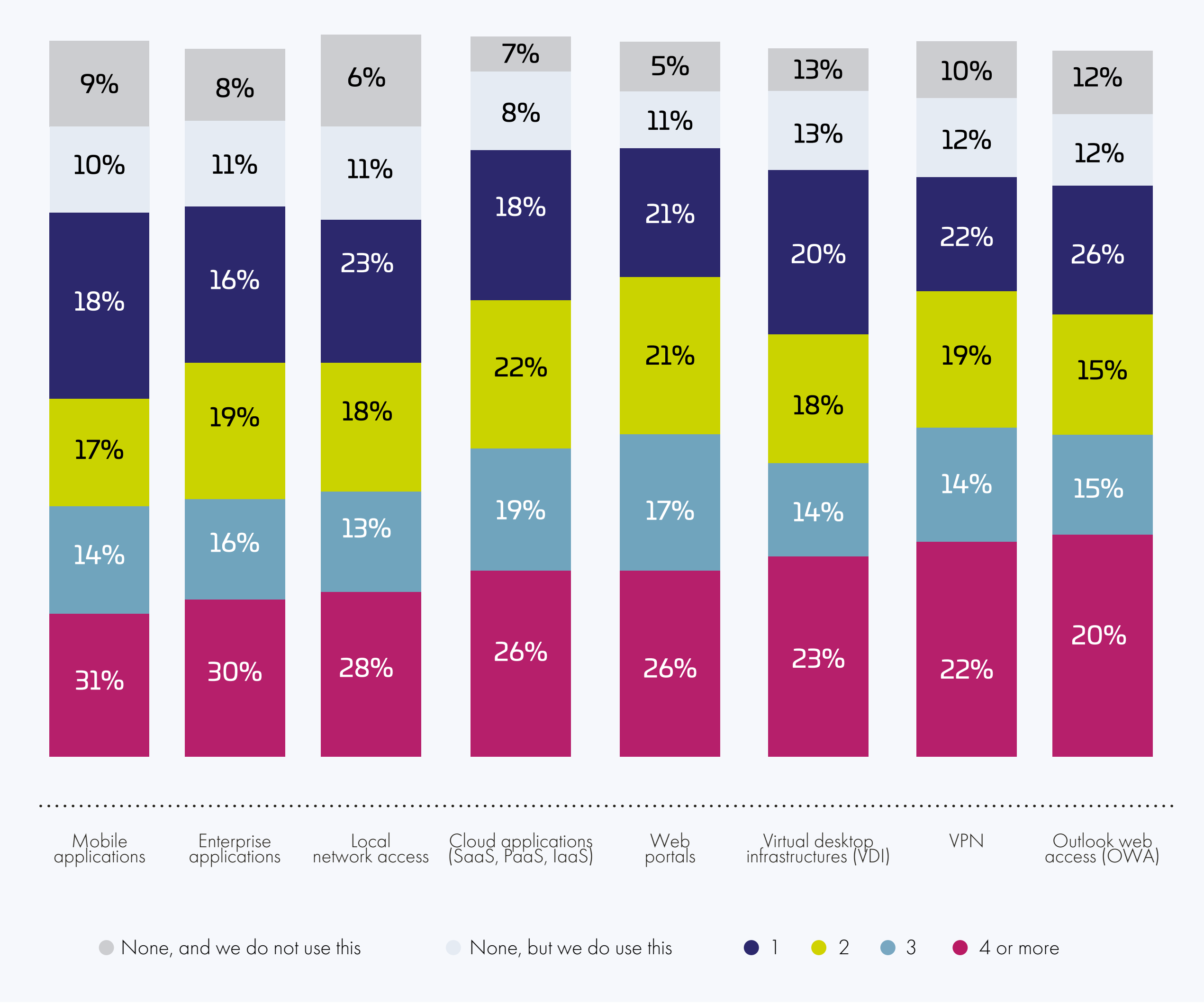


Figure 4
"How many of the above applications in your organization are currently protected by two-factor authentication?", asked to all respondents (1,050 respondents)

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.

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

The people you rely on to protect your privacy rely on Thales to protect their data. When it comes to data security, organizations are faced with an increasing number of decisive moments. Whether the moment is building an encryption strategy, moving to the cloud, or meeting compliance mandates, you can rely on Thales to secure your digital transformation.

Decisive technology for decisive moments

THALES

Americas
2860 Junction Avenue, San Jose, CA 95134 USA
Tel: +1 888 744 4976 or +1 954 888 6200
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 <

© Thales - JulY 2019 • DBv3