cpl.thalesgroup.com

#AMI2020

THALES

Executive Summary
2020 Thales Access Management Index
Europe and Middle East Edition

Contents

Introduction

The modern world requires stronger IT security and data protection than ever before. High profile breaches are becoming more common and cyber-attacks are the norm. There is a huge public pressure to be protecting data for customers and of course there is massive implications within any organisation who is breached.

It's clear that there is cause for concern. Not only is there an increase in threats, there's also an increase in vulnerable technologies being used. Rightly or wrongly, some of the most widely used modern technologies have a stigma attached that they are vulnerable. This is where modern technology needs modern security and authentication methods to deliver a Zero Trust approach when it comes to data security. It's far too frequently that we see vulnerable technologies and poor access management solutions, which is an unforgivable mistake.

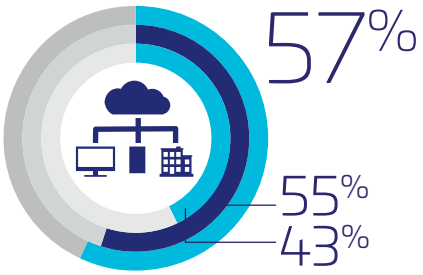
This research explores access management practices within businesses and the use and importance of two-factor authentication, smart single sign on and cloud access management tools. We aim for this to be informative and educational, while inspiring best practice.

he 2020 Access Management Index – Europe and Middle East Edition, is a survey of 400 executives in 7 countries in Europe and the Middle East with responsibility for, or influence over, IT and data security. The survey, reporting and analysis was conducted by Vanson Bourne, commissioned by Thales.

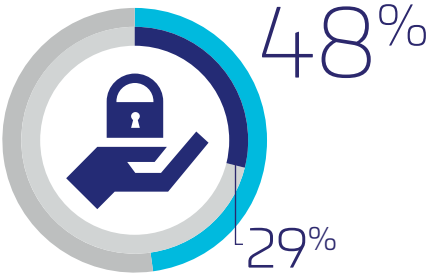
Key Findings

Give Passwords a Pass

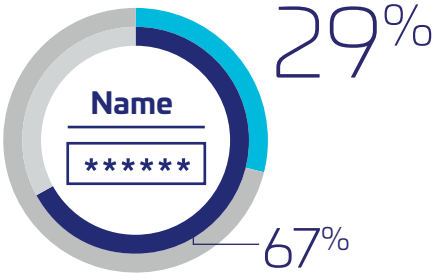
as Concerns about Cyber-attackers Targeting Unprotected Infrastructure and Cloud Apps Rise



believe unprotected infrastructure (e.g. new IoT devices) present the biggest targets for cyber-attacks, ahead of cloud apps (**55%**) and web portals (**43%**)



of IT leaders find it easier to sell the need for security to their boards compared to last year (**29%**)



rate username and password as an effective means of protecting their IT infrastructure, with **67%** planning to expand their use of it in the future

Zero Trust – Balancing Security and Convenience

67%

say their security teams feel under pressure to provide convenient access to users, but still maintain security

Access Management is Essential for Cloud Transformation

96%

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

76%

revealed employee authentication needs to be able to support secure access to a broad range of services including virtual private networks and cloud applications.

Two Steps Forward, One Step Back

75%

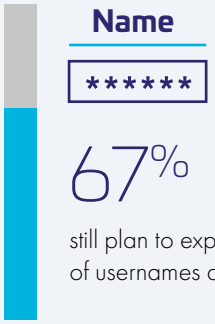
are expanding their use of biometric authentication

81%

are expanding Smart SSO in the next year.

70%

plan to further utilise passwordless authentication methods



67%

still plan to expand their use of usernames and passwords

Access Management Trends

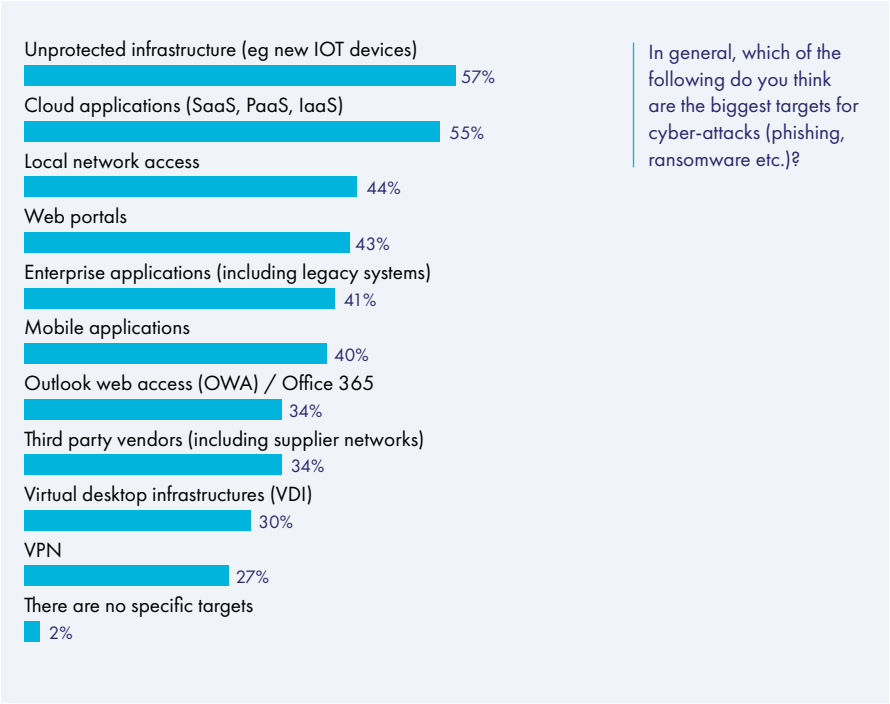
Over half of respondents identify unprotected infrastructure (57%) or cloud applications (55%) as one of the biggest targets for cyber-attacks. Intriguingly, those from larger organisations with more than 5,000 employees were more likely (64% vs. 51% of those from organisations with 250-499 employees) to identify unprotected infrastructure as a potential target. Larger organisations appear to be struggling to ensure that their entire infrastructure is protected.

Among those who feel that cloud applications are a top target for a cyber-attack, the most likely (56%) cause is the increasing volume of cloud apps in use. Organisations are in a race against themselves to protect their cloud applications as quickly as they are deploying them. But there are some other reasons why cloud applications may be targeted, including inconsistent security protection (55%), a lack of in-house skills (44%) and/or poor visibility over their cloud applications (43%).

For most (94%) organisations, their security policies around access management have been influenced by recent breaches of consumer services. Yet despite this, many (51%) would still allow employees to log on to company resources using personal, social media credentials. Regardless of a respondent's position on this, one thing is clear; almost all (98%) agree that in order to comply with regulations, tighter controls over data access are needed.

Most respondents have, or imminently plan to implement, some form of access management capability. Be that an on-premises IAM solution (61% have, 18% plan to within the next year), IDaaS (53%, 21%), Cloud SSO (51%, 18%), or smart SSO (48%, 24%) . In terms of what is motivating organisations to implement access management solutions such as these, it is more of a response to security concerns rather than for ease of use benefits. For instance, the threat of large-scale breaches (21%) or security concerns (19%) are both far more likely to be the main driver for implementing an access management solution than simplifying cloud access for end users (8%) or enabling new ways of doing business (8%).

Regardless of why an organisation is implementing such a solution, it is likely that there are plenty of voices in the decision-making process. While the CIO/head of IT is most likely (37%) to be the final decision maker, the vast majority indicate that people such as the cloud security team (85%), cloud migration team (82%), chief cloud strategy officer (80%), or digital transformation team (79%) are involved to some extent.



Also key to achieving regulatory compliance – a single, clear audit trail

99%

See it as important that their organisation has the ability to produce a single audit trail of access events taking place throughout different resources used by their organisation

36%

See it as **extremely** important

66%

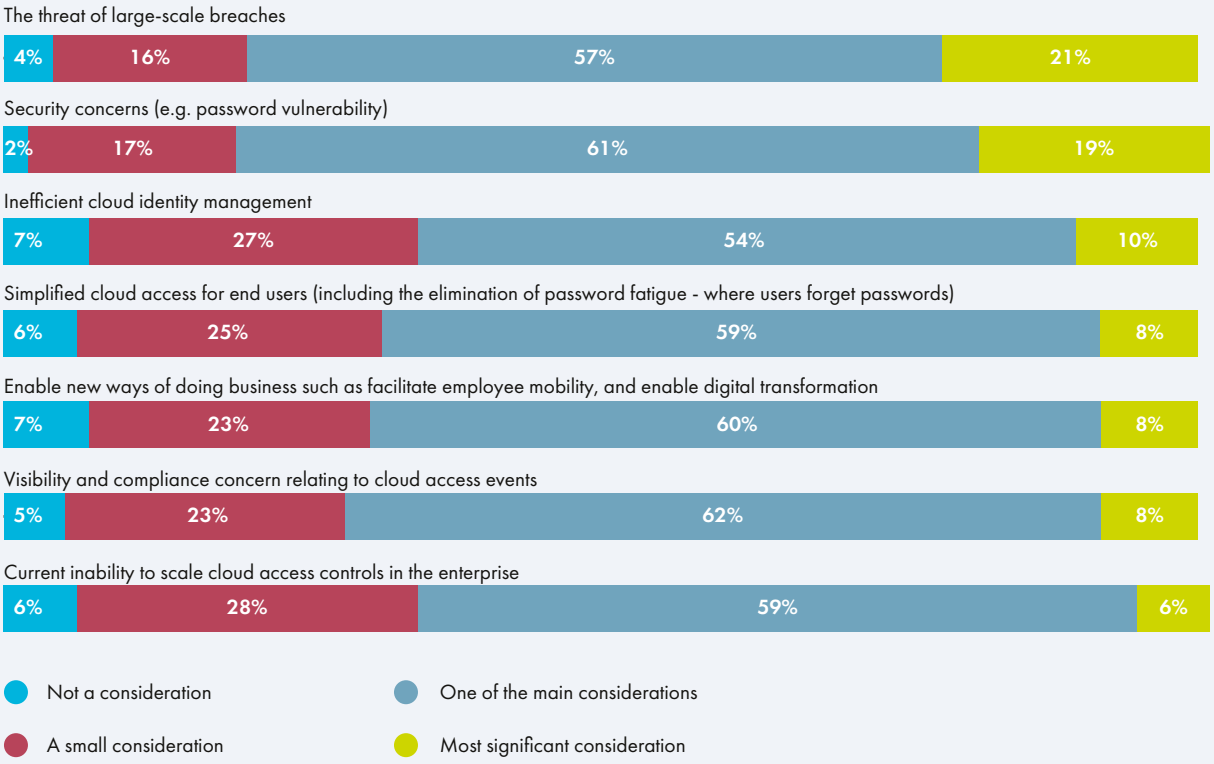
In **Saudi Arabia** and the **UAE**, two thirds see this as **extremely important**

The dangers of large-scale breaches and security concerns are clear to many – and they are the primary drivers for implementing an access management solution

It seems that for many, access management is more of a reactive measure, something that they have implemented as a means to protecting themselves from cyber-attack and all of the risks that come with them.

While implementing an access management solution can be a means to simplify cloud access and enable new ways of doing business, it appears that these are both merely added bonuses once security has been taken care of.

Showing respondents who think that controlling who has access to specific types of data can definitely contribute toward their organisation's ability to comply with data protection and pass security audits – split by respondent country



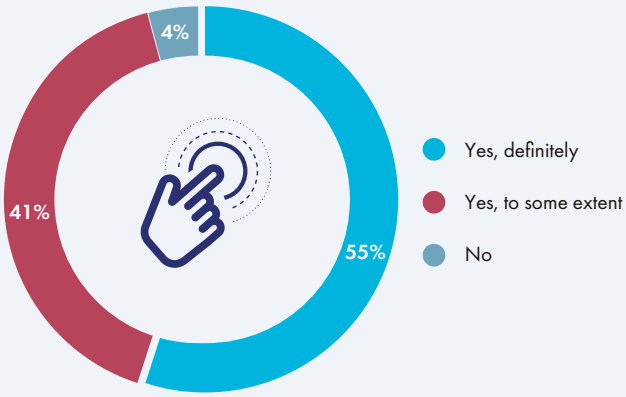
Cloud Access Management Is a Priority

When it comes to protecting their organisation's cloud and web-based applications, respondents are more likely (53%) to find that two-factor authentication is best, compared to smart SSO (43%), biometrics (39%), or SSO (35%). However, it is a concern that almost three in ten (29%) still perceive username and password as best, despite its proven limitations.

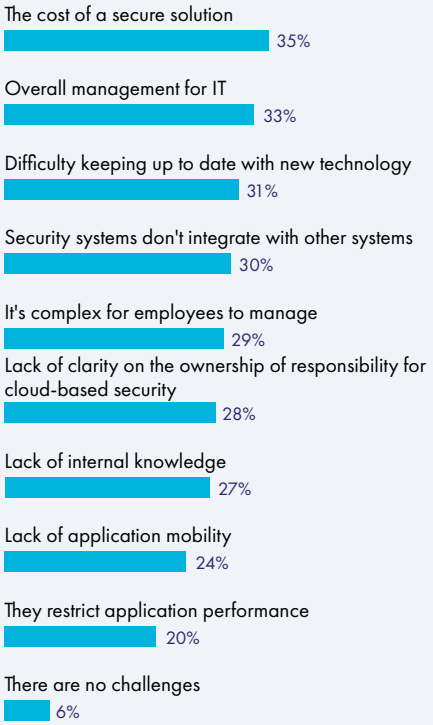
Where respondents do agree is in the importance of cloud access management, with the vast majority (96%) seeing cloud access management for cloud and web applications as being conducive to facilitating cloud adoption. Just as telling is the 96% who report that there is/would be a negative impact on their organisation from ineffective cloud access management. Not only could cloud become a security issue (46%), but over a third report that IT staff's time would be used less efficiently (38%), increased operational overheads and IT costs (36%), and/or shadow IT taking place (34%). It is clear that cloud access management is an area where organisations have to be successful.

Yet, there are many challenges when addressing cloud-based security, that could potentially undermine the efforts of an organisation to sure up cloud access management. In fact, over nine in ten (94%) tell us that there are challenges. The most widely felt (35%) is the cost of a secure solution, but difficulty keeping up with new technology (31%), trouble integrating with other systems (30%), and/or a lack of clarity on the ownership of responsibility for cloud-based security (28%) are all challenges making their presence felt for around three in ten.

Do you see cloud access management for cloud and web applications as being conducive to facilitating cloud adoption?



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



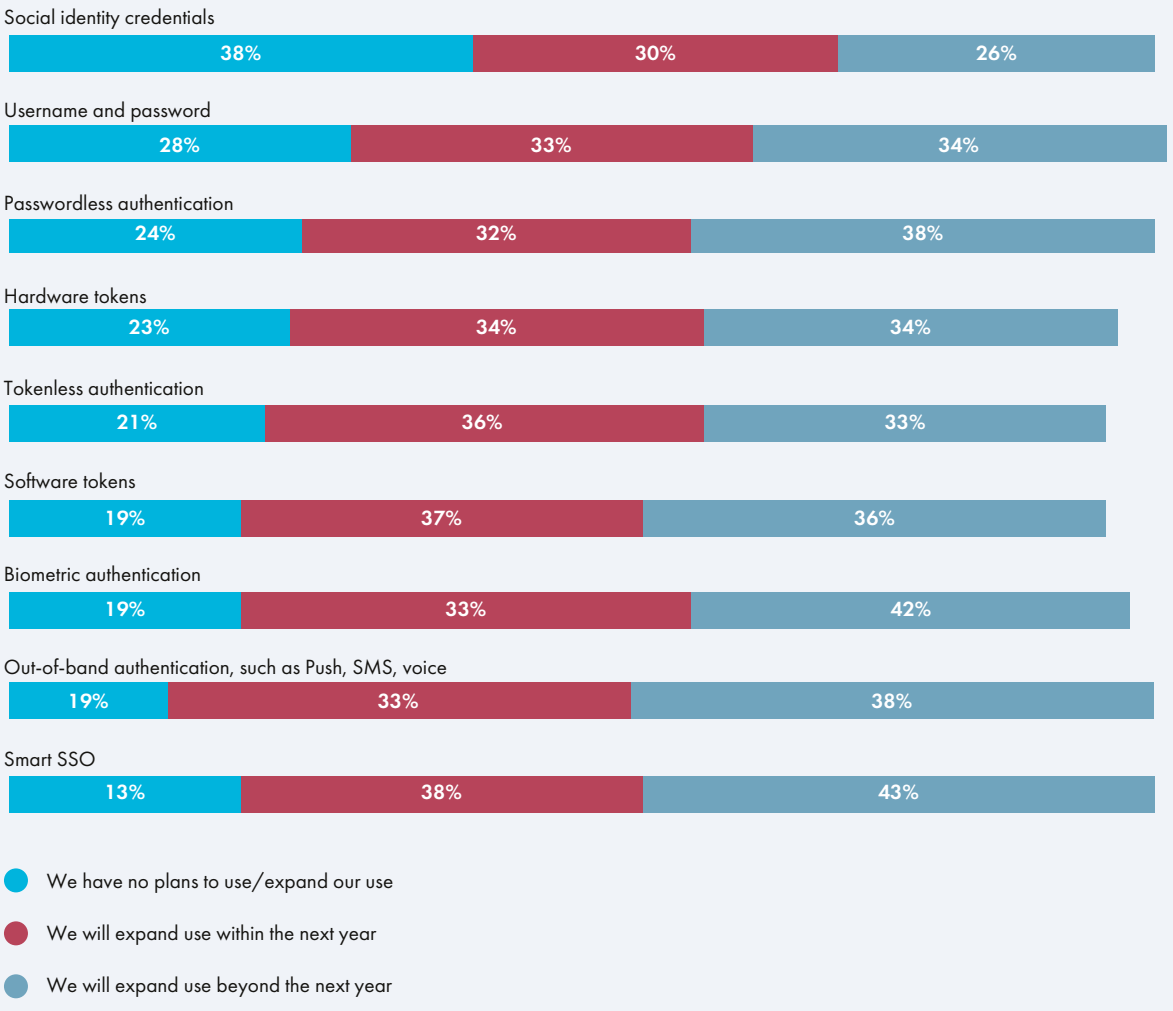
Multi-Factor Authentication Trends

The majority of respondents' organisations plan to expand their use of various types of two-factor authentication, including but not limited to smart SSO (81%), biometrics (75%), software tokens (73%), passwordless authentication (70%), and/or hardware tokens (68%).

Among those whose organisation is planning such an expansion in at least one form of two-factor authentication, respondents are pretty split as to how they will achieve this expansion. Just over half (52%) will use a dedicated multi-factor authentication solution, while four in ten (40%) will use an IDaaS/access management solution.

When it comes to deciding which type of two-factor authentication to deploy, perhaps it is a good idea to look at who in particular will be the primary user, as respondents tell us that different types of two-factor authentication suit different employees. For instance, when it comes to employees outside of IT respondents are most likely (38%) to think that username and password fits best, while hardware (48%) or software (48%) tokens best suits IT staff. And as for the c-suite, biometrics is the form of two-factor authentication that best suits (30%) these busy employees.

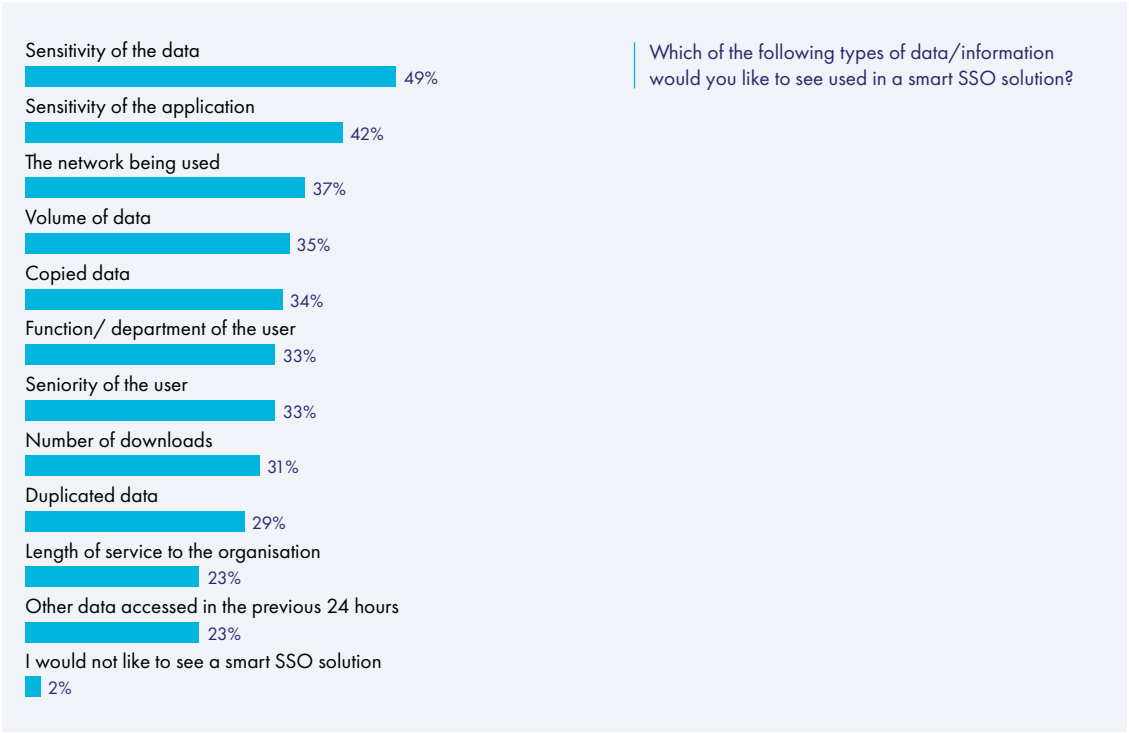
What types of two-factor authentication do you expect your organisation to expand the use of to protect applications in the future?

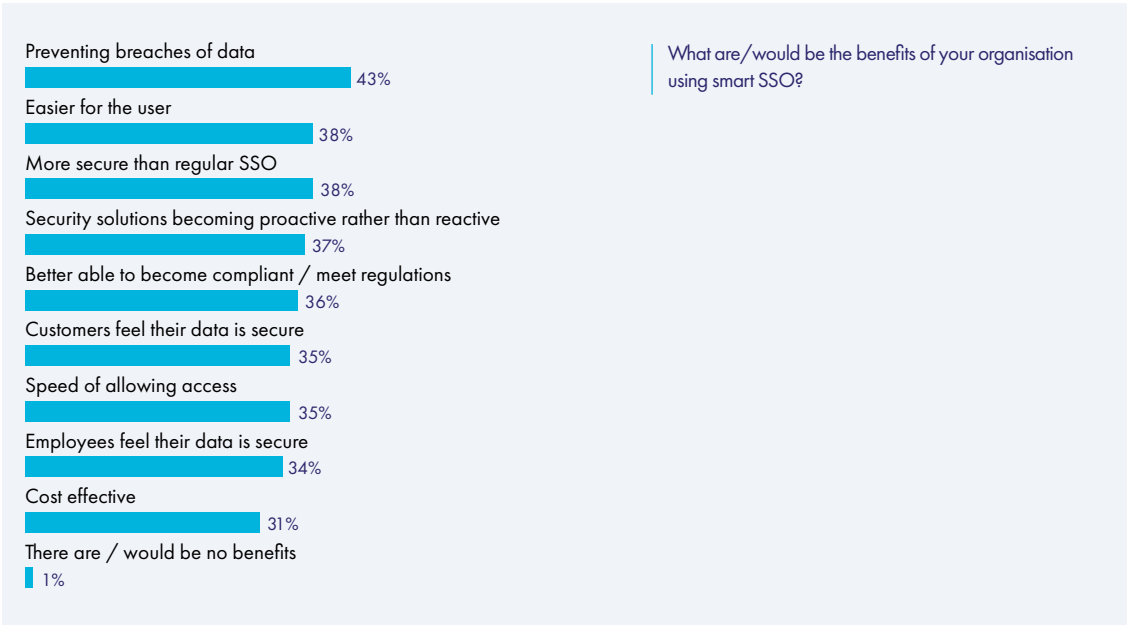


Smart Single Sign-On (SSO) on the Rise

Nearly all (98%) respondents would like to see a smart SSO solution in use in their organisation. And this trend continues with another overwhelming proportion (99%) who report that there are/would be benefits to their organisation implementing smart SSO.

In order to achieve a more secure smart SSO, over a quarter (28%) of respondents would allow their organisation to collect and hold any of their personal data, while 43% would allow much more data to be used, but nothing sensitive. Only a minority (14%) would be against their organisation holding any more data about them, indicating that the prevailing view is that a secure smart SSO is worth providing more personal data for.





Next Steps and Guidelines

As noted in the previous sections of this paper, the majority of respondents agree that cloud access management is conducive to facilitating cloud adoption, and most of them plan to expand the use of various types of multi-factor authentication. Nearly all (98%) respondents would like to see a smart SSO solution in use in their organization.

From a practical perspective, what should the next steps be and what considerations should IT professionals take into account when selecting an Access Management and Authentication solution? Below are a few recommendations.

1. **Efficiency and Deployment**
   A cloud-based solution will allow you to get up and running quickly without the need for heavy on premises installations. When assessing your solution, it is advisable to check how many on-premises components you will need to install, and how many servers you will need, and how the additional servers you'll need in order to maintain redundancy.

2. **Automation**
   It is recommended to subscribe to a service that offers automated token enrollment workflows and one-click token installment for end users, your organization will be able to self-enroll quickly and reduce IT burdens.

3. **Authentication and Token Flexibility**
   To support all users' needs, look for a solution that can offer a range of authentication methods that can accommodate varying needs and security levels. These include: Push OTP app (which can be installed on a mobile device or desktop); SMS or email code sent to a mobile device or email address; pattern-based authentication, or a token-less method that does not require users to install any software on an end device.

4. **Ability to Access all Apps and Cloud Services**
   Look for a solution that can secure access to apps via SAML, RADIUS and non-standards-based apps and avoid any solution that can only secure cloud and web-based apps. This way you will be able to protect all apps with a single solution and offer convenience with single-sign-on.

5. **Smart SSO for Optimal Security and Convenience**
   To offer the most frictionless experience possible without sacrificing security, organizations can leverage cloud SSO combined with contextual information and step-up authentication. This allows users to access all their cloud and web applications with a single identity, while IT only needs to enforce stronger access security in high-risk situations.

6. **Provide Flexible Policies**
   By subscribing to a cloud access management service with flexible policies, you will be able to step up authentication for untrusted networks and ease the level of authentication method required for the trusted networks and devices.

7. **Transparent Licensing Model**
   Many services have very complicated pricing models. A dedicated access management and authentication solution with a transparent pricing model which includes the features you need will allow you to easily analyze and forecast costs moving forward.

Conclusion

As more and more businesses move to adopt cloud-based services for CRM, email, employee collaboration and IT infrastructure as part of their digital transformation strategies, the struggle to extend old solutions, designed to protect internal resources, to the outside world becomes very problematic. Often, in an effort to adapt to the new working habits of users connecting from anywhere, businesses tend to revert back to old password-based logins for cloud services in despair, knowingly increasing their security exposure through credential stuffing and phishing attacks.

For a long time, the biggest battle IT leaders have faced is increasing board awareness around taking security threats seriously. Now they have that buy in, the focus should be on highlighting to the powers that be, the importance access management plays in implementing a Zero Trust security policy. With this in place, risk management professionals will be able to put in place a 'Protect Everywhere - Trust Nobody' approach as they expand in the cloud.

THALES

Americas
Arboretum Plaza II, 9442 Capital of Texas Highway North,
Suite 100, Austin, TX 78759 USA
Tel: +1 888 343 5773 or +1 512 257 3900
Fax: +1 954 888 6211 | E-mail: sales@thalesesec.com

Asia Pacific
Unit 4101-3, 41/F, Sunlight Tower, 248 Queen's Road East
Wanchai, Hong Kong | Tel: +852 2815 8633
Fax: +852 2815 8141 | E-mail: apacsales.cpl@thalesgroup.com

Europe, Middle East, Africa
350 Longwater Ave, Green Park,
Reading, Berkshire, UK RG2 6GF
Tel: +44 (0)1844 201800 | Fax: +44 (0)1844 208550
E-mail: emea.sales@thales-esecurity.com

cpl.thalesgroup.com/euro-access-management-index