Arlington Research

RESEARCH REPORT

Accessing the Future:
The Need for Unified Access Management

Commissioned on behalf of OneLogin

Digital transformation is happening all around us and indeed has been for some time. No industry is immune as businesses rush to keep pace with consumer demands by expanding their IT infrastructures to allow them to innovate with technology.

The last 12 months alone has seen enterprise 'digitisation' accelerate significantly, so much so that the topic now dominates the vast majority of boardroom agendas. And there will be no slowing down in 2018 and beyond, with IDC predicting that global spending on digital transformation will hit the $1.7 trillion mark by the end of 2019, a 42% increase from 2017.

However, while this tech revolution is offering businesses a seemingly infinite number of possibilities, it is also presenting some considerable challenges.

Factors such as increasing security risks, the continued proliferation of Software-as-a-Service (SaaS) applications, the intricacies involved in running hybrid infrastructures and stricter industry regulations have all combined to drastically increase the complexity of enterprise IT.

As such, it has never been more important to get the right technology, to the right people, at the right time, but the parameters are continuing to expand with increasing frequency. They now include both personal and corporate devices, on-premises and cloud applications, and a wide range of users such as full-time employees, contractors and partners, and customers.

These challenges have helped to foster the growth of Identity and Access Management (IAM) solutions in recent years. The industry has come a long way from the days when a handful of remote employees needed access to a select few applications, which is why this flourishing market is set to be worth nearly $15 billion by 2021.

But, as IT infrastructures have become harder than ever for IT teams to manage and the access issue has become more pronounced, enterprises are realising that their current IAM solutions are simply not fit for purpose.

Methodology

OneLogin commissioned research that questioned those involved in the IT decision-making process within UK and US enterprises, to find out about their organisations' approach to Identity and Access Management and the current pain points they are experiencing. 500 online interviews – split equally between the UK and the US – were conducted among non-managers and above, who work in their company's IT department and have a responsibility for technology services and IT security. All respondents were aged 18 and over and quotas were applied to gender, the age of respondents and the region in which they reside, to ensure a nationally representative sample. The findings are outlined in this report.

Key findings

- 93% of enterprises in the UK and the US currently have a digital transformation strategy in place.
- As part of their digital transformation strategy, over half of enterprises (53%) deployed more than 50 new on-premises applications in the past year, and the same percentage deployed more than 50 new SaaS applications in the past year.

- 91% see IAM as being either 'critical' or 'important' to their business's digital transformation strategy, while just 7% say it is a low priority.

- Nearly half (48%) identified security risk (credential compromise, lack of two-factor authentication etc.) as a primary driver behind the use of an IAM solution.

- Enterprises are frustrated with their current IAM solutions. Issues around maintenance (49%), cost (48%) and complexity (46%) were identified as the biggest pain points.

- Nearly all respondents (98%) are interested in a solution offering IAM functionality such as centralised directory, automated provisioning, one SSO portal for access to all apps etc. for both on-premise and SaaS apps.

- Advanced security controls (68%) and access controls for both devices (57%) and appliances (54%) would strengthen interest in IAM functionality for both on-premise and cloud environments.

- 'Significantly reduced operational complexity' (41%) and 'unified management' (37%) are two key drivers in an organisation's decision to upgrade or replace its IAM solution.

Accelerating towards the cloud

Digital transformation has been an industry buzzword for some time, but progress has accelerated dramatically in the last couple of years. Businesses of all sizes now simply can't afford to stand still. If they do, they will quickly be overtaken by pioneering start-ups or fast-moving competitors.

This focus on innovation is illustrated by the fact that 93% of respondents to our survey now have a digital transformation strategy in place, with information technology (94%) and financial services (96%) organisations showing a particular desire to adapt.

Central to this overarching trend has been the move to cloud-based platforms and services. Some of the world's biggest companies have been born in the cloud – the likes of Uber, Netflix and Airbnb are rightly held up as shining examples of the power of cloud technology – enabling them to scale at speed and completely disrupt traditional business models.

Many are now attempting to follow in the footsteps of these market-leaders. Over a third (36%) of enterprises are now deploying between 100-500 Software-as-a-Service (SaaS) apps within their organisations every year and 32% estimate that they deployed between 100-500 new commercial SaaS apps last year alone.

CHOICE	%
0	0.60% 3
1–10	11.00% 55
11–25	13.60% 68
26–50	12.40% 62
51–75	12.40% 62
76–100	9.60% 48
101–150	8.00% 40
151–200	7.40% 37
201–500	12.00% 60
501+	8.60% 43
Don't Know	4.40% 22

Table 1: Approximately how many SaaS apps are deployed within your organisation every year?

This app-driven economy is accelerating due to a range of factors. For example, businesses are constantly looking for ways to improve the productivity of their employees and regularly roll out new services to meet the ever-changing demands of consumers.

Running in tandem has been the growth of the Internet of Things (IoT), which has resulted in a well-documented boom of connected devices entering the workplace that all need to be managed and maintained. IoT growth has

already been exponential and, with 20.4 billion IoT devices set to be deployed by 2020, its steep upward trajectory is set to continue.

Keeping up with this demand can be hard work, so adopting a cloud-based approach speeds up development cycles and greatly increases business efficiency, which is especially true for large organisations that are traditionally slow-moving and dependent on lengthy development processes.

The growing number of apps means IAM currently has a key role to play in ensuring that the right people are accessing the right applications and that the data contained within them is being protected. According to Gartner, a typical small enterprise's IAM program will span one million people, ten million things and billions of relationships by 2020, with this massive scale and complexity potentially having a significant impact on business operations and security.

Indeed, security risk was identified by nearly half (48%) of respondents as the primary driver behind their organisation's use of an IAM solution, as features such as two-factor authentication (2FA) and Single Sign-On (SSO) can significantly improve a business's security posture. Other key drivers behind IAM usage include boosting process inefficiencies when it comes to provisioning, deprovisioning or rolling out new apps (28%), compliance /auditing purposes (12%) and improving the SSO user experience (11%).

These are all benefits that many enterprises have recognised. IAM solutions are primarily being used to manage application user provisioning for both on-premise and cloud apps in multiple solutions (58%), although some businesses are using such tools exclusively for either on-premise (17%) or cloud (16%) apps.

Looking towards the future, IAM is also widely being seen as central to upcoming digital transformation projects – 47% say it is 'important' and 44% say it is 'critical' – highlighting the need to get an effective solution in place ahead of time.

The problem is that, despite the many benefits IAM offers, there are some pain points that enterprises are coming up against as they accelerate towards cloud-based ways of working.

Bumps in the road

Despite the progress that is being made, enterprises in virtually all industries are still facing barriers in their digital transformations.

Respondents to our survey highlighted spiralling costs (41%), increasing project complexity (41%) and a lack of executive buy-in (31%) as three of the biggest obstacles getting in the way of digitisation, while 27% have simply found themselves too stressed to take on extra IT projects.

Enterprises are also realising that their current IAM solutions are not fit for purpose, with some similar pain points around maintenance (49%), cost (48%) and complexity (46%) rearing their ugly heads.

The key issue is that the complexities created through the growing impact of cloud and IoT, combined with the increasing number of apps being deployed, are holding businesses back from true transformation. For example, applications can now live basically anywhere, meaning corporate and customer data is crossing an ever-growing number of digital boundaries. Employees are also accessing more apps, from more devices and from multiple locations, as businesses adopt mobile ways of working.

What's more, one of the biggest complexity challenges that enterprises are coming up against – and will continue to come up against in the future – is how to efficiently manage a hybrid infrastructure. This issue was clearly identified by the respondents to our survey. Nearly half (48%) of respondents highlighted existing legacy IT systems as a barrier to digital transformation and 29% of enterprises are frustrated with their current IAM solution's fragmented access control for multiple environments, such as on-premise and cloud.

There are several reasons for this. Firstly, there are management complications. When cloud applications first began to gain traction in the workplace, IT teams were tasked with managing access to two application portfolios rather than one: a legacy on-premise environment and a collection of cloud-based apps.

IT teams now have hundreds, if not thousands of services, applications and devices to manage, sitting across a combination of on-premise, public cloud and private cloud environments. And, each environment often has separate IAM systems which are operated independently from one another.

This leads on to the issue of the costs associated with process inefficiencies. The costs incurred from running a dual approach to access management are more than most businesses think. For example, nearly a quarter (24%) of businesses estimate that 51-75% of their IT spend is currently being spent on maintaining existing on-premise applications, which is an exceedingly large proportion when we consider the growing focus on cloud-based apps.

Tasks such as provisioning access to new users, deprovisioning access for former employees, rolling out new applications, ensuring access security and enabling Multi-Factor Authentication (MFA) all combine to create a substantial workload for administrative staff.

Failing to properly manage this workload in an increasingly complex environment – as well as making the task of complying with regulations such as GDPR (General Data Protection Regulations) that much harder - also has potentially serious security implications. For example, a recent OneLogin study found that over half (58%) of people still have access to their ex-employer's corporate applications, meaning businesses are clearly failing to adequately protect themselves from the possible threat posed by former employees.

The same study also found that 92% of UK-based IT decision-makers spend up to an hour on manually deprovisioning former employees from every corporate application, with this burden going some way to explaining why over a quarter (28%) of ex-employee's corporate accounts remain active for a month or more.

Then there are external threats to consider. Cyber security is arguably the biggest threat to any business and a disjointed approach to IAM can leave security holes that hackers and criminal organisations will be only too willing to exploit.

Finally, the burden on IT departments can also be felt by current employees, as fragmented administration can quickly lead to issues when staff attempt to gain access to various applications from a range of locations and devices.

So, with enterprises struggling to manage a hybrid environment as security breaches continue to dominate headlines, what's the answer?

A Unified Future

The challenge businesses will face in the future is that the on-premise/cloud split isn't going to disappear any time soon. In fact, most businesses are settling on a hybrid approach, enabling them to manage certain legacy systems locally – perhaps for security or compliance reasons – and use cloud platforms for more innovative projects or services.

The same is true for application development, with enterprises expecting to deploy a mixture of commercial SaaS and on-premise apps over the next 12 months. That way, apps that hold private customer information, for example, can be kept on-premise to satisfy security and regulatory requirements, while less-sensitive systems receive the speed and flexibility benefits of the cloud.

CHOICE	%
0	1.40% 7
1–10	14.60% 73
11–25	12.00% 60
26–50	12.80% 64
51–75	10.20% 51
76–100	12.60% 63
101–150	8.40% 42
151–200	10.00% 50
201–500	8.20% 41
501+	4.00% 20
Don't Know	5.80% 29

Table 2: How many new commercial SaaS apps do you anticipate your organisation deploying in the next 12 months?

This approach effectively provides the best of both worlds, enabling businesses to pick whatever mix of cloud and on-premise best suits their specific needs.

What's clear is that as businesses continue their journeys towards the cloud, the complexity and security issues associated with these hybrid infrastructures are only going to increase. That's why nearly all respondents (98%) said they would be interested in a solution offering unified IAM functionality such as a centralised directory, automated provisioning and one SSO portal for access to all apps, for both on-premise and SaaS apps.

CHOICE	%
0	1.60% 8
1–10	15.40% 77
11–25	16.00% 80
26–50	11.00% 55
51–75	7.60% 38
76–100	11.80% 59
101–150	9.40% 47
151–200	7.80% 39
201–500	9.80% 49
501+	4.60% 23
Don't Know	5.00% 25

Table 3: How many new on-premise apps do you anticipate your organisation deploying in the next 12 months?

Enterprises want tools that provide advanced security controls (68%), access control for devices (57%) and access control for appliances (54%), but they can only be truly effective if they extend across a hybrid environment.

This is where the new era of Unified Access Management comes into play. We've discussed how the current approach to IAM is largely unstructured and disparate, leading to increased risk of data breaches, credential compromise and process inefficiencies.

Modern companies need to be able to easily deploy cloud applications on an international or even global scale, as well as provision a widespread workforce on demand while still maintaining robust security processes. But the reality for many enterprises is that most workloads remain in on-premise data centres, where access for employees is awkward and applications are saddled by legacy management tools.

The majority (72%) of companies still have a legacy web access management solution in place, burdening them with issues including the associated costs (identified by 40% of respondents), maintenance complexities (38%) and – perhaps most tellingly – a desire to move to the cloud (35%).

So, what enterprises really need to do is take a holistic approach to IAM and solve the complexity issue by having one unified platform that simplifies the management of access control across all environments – cloud, on-premise and a mixture of the two.

And this is something they are quickly starting to realise. 41% of respondents rated 'significantly reduced operational complexity' as being either an influential or extremely influential factor in their organisation's decision to upgrade or replace their IAM solution. 'Unified management' was deemed to be equally as important for over a third (37%) of respondents.

With a unified IAM platform, businesses can protect their customer and employee data from exposure and malicious misuse by linking it to all of their directories in real time, which can greatly improve organisations' security posture, while also optimising the end user and administrative experience.

Having one integrated interface, one audit trail and one support experience will speed up deployment, improve ongoing operations, and avoid the potentially costly delays that can come from having multiple systems.

Finally, with a unified tool businesses can apply innovative, cloud technologies to the entirety of their application portfolio, including SaaS and on-premises apps. For example, adaptive authentication technologies, which benchmark typical user behaviour against multiple variables to detect anomalies across the entire organisation, can now be applied in places it has not been historically possible.

The combination of these capabilities gives enterprises unparalleled visibility across their IT environment and the flexibility to be able to respond to any access and identity issues immediately, all without sacrificing usability for the rest of the workforce.

Conclusion

If there's one thing we learned in 2017, it's that no business is immune from the need to modernise and embrace technological progress. Companies of all sizes and in all industries – from retail and finance to healthcare and utilities – are being swept along by the digital transformation wave.

In conjunction with 'buzzword' innovations such as the Internet of Things (IoT) and artificial intelligence (AI), cloud computing is enabling the rapid development and deployment of apps and services that have already made entire industries obsolete.

But, as businesses continue to transform through technology over the coming months and years, they will come up against some significant challenges. The use of cloud-based applications has opened the doors to a great many opportunities, but it also introduces a huge amount of complexity.

As they continue to invest more in the cloud, many organisations are spreading themselves out across hybrid architectures. As a result, IT teams now have two disparate app environments to manage instead of one. From an IAM point of view, this effectively doubles their workloads and opens their organisations up to attacks from sophisticated

cyber criminals, as well as the risks of insider data theft and gaps in compliance.

If that wasn't enough, it also saps the productivity and efficiency of both IT staff and end users, both of which negatively impact the bottom line.

To counter these issues, businesses desperately need an IAM solution that addresses the complexities and security requirements of enterprise networks, whilst also providing visibility across the entire infrastructure.

The key for large companies – especially those with lots of legacy infrastructure – lies in finding a way to efficiently manage user access to applications both on-premise and in the cloud, without impacting the user experience.

Ultimately, they need a unified solution. One that brings together these different environments and simplifies access management to protect confidential data no matter where it resides.

Not only will Unified Access Management improve security, compliance and operational efficiency, it will also make IT teams more productive than ever and give employees the quality experience they now demand from their business apps.

There can be no doubting the fact that the future of Identity and Access Management is here, and it's well and truly Unified.