Support your remote employees with digital identity

Executive summary

Organisations have recently had to greatly expand the scale and scope of their use of digital technologies to support a transition towards new ways of working. Identity and Access Management (IAM) is key to a successful transition by reducing the cost and complexity of provisioning services simply and securely to users, wherever they are. This whitepaper considers the three main challenges faced by IT in making this transition: supporting remote employees, securing the business, and delivering more for less.

Document Date: August 2020

Author: Josh Howlett

Introduction

2020 has posed exceptional challenges for business. With organisations greatly expanding the scale and scope of their use of digital technologies in recent months, it would be fair to say that IT has been instrumental in supporting the transition to new ways of working.

The value of Identity and Access Management (IAM) in supporting these new ways of working is not always as visible to end users as the new applications they have adopted. But the rapid growth in the use of these applications, and their increasingly dispersed users, makes IAM more important than ever by reducing the cost and complexity of provisioning services simply and securely to users, wherever they are.

This whitepaper considers the key challenges faced by IT in transitioning to these new ways of working, and how organisations can use IAM to respond to these more effectively.

Supporting remote employees

Having hitherto been housed within highly managed office environments, most employees are now working from diverse locations, using multiple and often unmanaged devices, and sometimes outside core business hours. Almost overnight home working has switched from being a rarely implemented business continuity measure to business as usual.

IAM solutions that consider homeworkers as edge cases – or not at all – can lock the organisation into an office-based mode of delivery. And so, not surprisingly, many organisations are now finding gaps in their provision. Assumptions that were previously unquestioned are now turned on their head as corporate policy and practices have tried to keep pace with events.

An effective IAM solution must respond to this unconventional and unpredictable landscape. In part this is about the ability to reflect these new policies and practices within the provision of IT services, such as managing the use of multifactor authentication (MFA) across a broad portfolio; or enforcing policies based on a user's geographic location rather than their physical presence in an office.

But it is also about the delivery of the IAM solution itself. For example, an on-premise IAM solution is now a significant risk to the delivery of an organisation's cloud-based services if it is reliant on an office internet connection. The delivery of the IAM solution needs to align with the operational context of the services and users that it supports.

Securing the business

It goes without saying that access management is fundamental to information security. Historically access management has been a mix of network-level controls (such as the source IP address) and identity-orientated controls (such as the role of a user).

Industry trends, such as the adoption of public cloud, were already resulting in a gradual shift towards identity-orientated controls. With remote working, the loss of control over end users' network connectivity renders such controls ineffective and so the transition to the new ways of working will only accelerate this trend.

This does not mean that network security can be neglected or avoided, but it does require a shift in mindset from "securing the network" to "securing identity". This has a few consequences for IT provision.

First, there is an opportunity to reduce complexity from network by replacing some network-orientated controls with identity-orientated controls at the application layer. Network investment can then be focused on gains in network manageability and availability, for example, which the application layer relies upon.

Secondly, it becomes even more important that identity-related processes such as identity management, authentication, and authorisation are performed with a level of rigour consistent with the security requirements. This may require closer collaboration with other parts of the business, such as HR, to ensure that employees are onboarded and offboarded from the IAM system efficiently. An effective IAM solution will facilitate this by providing the tools and capabilities needed to manage and perform these functions reliably and efficiently, without the need to develop bespoke solutions tailored to the organisation.

Finally, it is essential that end user credentials are secure, particularly as SSO can potentially result in unauthorised access to multiple systems. This is partly a matter of user education, but also the adoption of technologies that can detect and prevent the unauthorised use of user credentials. These include capabilities such as MFA, which can prevent the misuse of credentials, and Privileged Access Management (PAM), which can put sensitive user accounts under a heightened level of scrutiny.

Delivering more for less

The financial impact of recent events has been profound for many organisations and it seems likely that these pressures will persist. Budgets are under scrutiny; while, at the same time, more – often much more – is being asked of IT.

Despite these pressures, a forward-looking business will make investments where those are really needed. The most attractive investments will be those that support the bottom line and the business' transition to new ways of working.

We touched on IAM's contribution to that transition previously. It can also help to support the bottom line by, for example:

reducing the administrative burden on IT by providing a single point of IAM configuration and control for all the organisation's services

easing the support burden on IT by making user access simpler through single sign-on (SSO) and self-service provision for operations such as password resets

increasing user productivity by ensuring that access to services is simple; and

providing offer insights into the use of subscription services and resources, so that resources can be used most effectively.

How to prepare for the 'new normal'

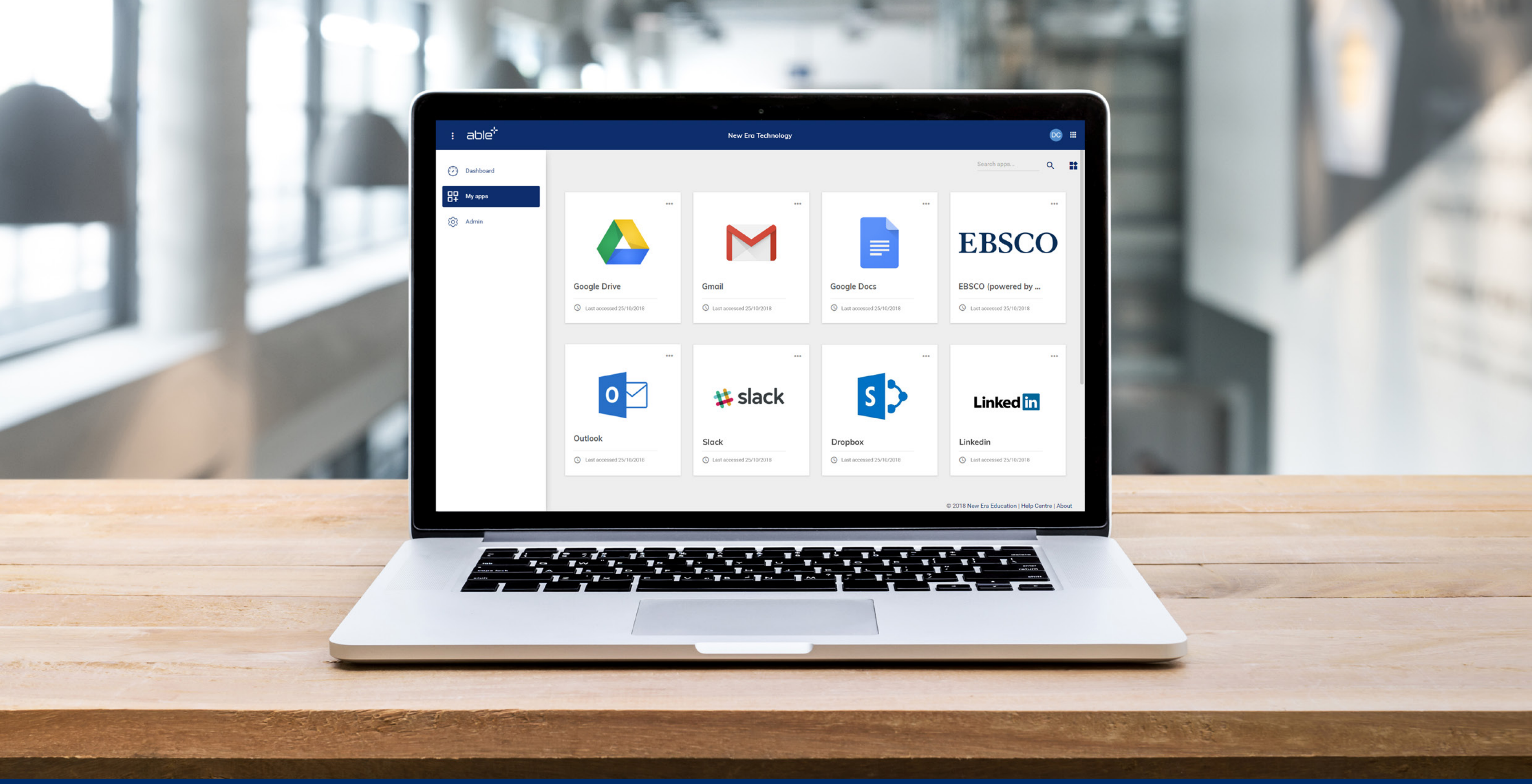
You should consider the following three key questions when reviewing your current IAM solution:

What is your organisation's strategy regarding office-based and remote working?

What are your current IAM solution's strengths and weaknesses with respect to this strategy?

How could your IAM solution be improved to meet your organisation's needs?

If you are starting to move your workforce back into offices, now is the time to reflect on the changes you need to make to ensure you are prepared for future eventualities.

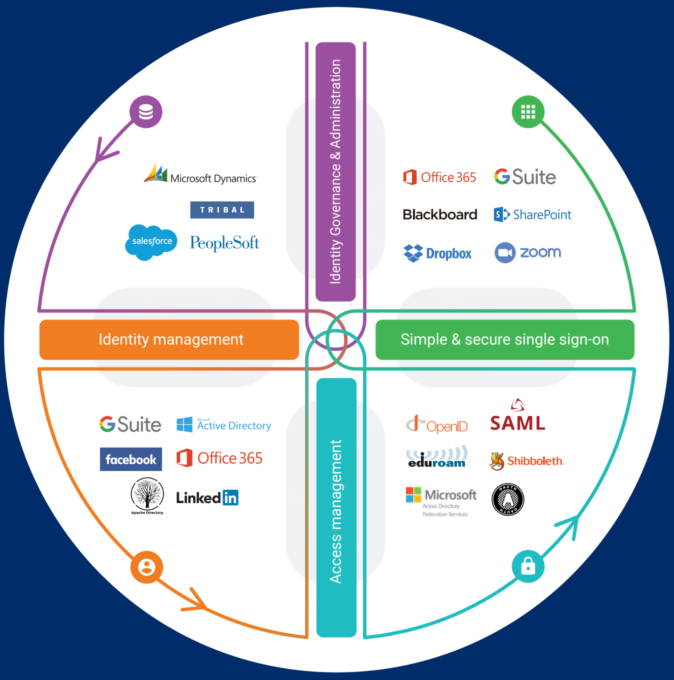


Powerful and intuitive identity and access management solution

Simplify your users' access and streamline your identity governance

Able+ is an identity & access management (IAM) solution that transforms user productivity by enabling simple and secure single sign-on access to applications and services using corporate or social identities.

It's also an identity governance & administration (IGA) solution that makes it easy to align your IAM with organisational policies and processes. The powerful workflow engine and visual workflow editor can bring together different sources of identity data to create a single source of truth and its system attestation ensures that your users' privileges will remain compliant with policy.



03334 559424

info@neweratech.co.uk • neweratech.co.uk

able+ | Powered by new era. TECHNOLOGY