Time to re-engineer Identity and Access Management

AN OVERVIEW OF THE CURRENT IDENTITY AND ACCESS MANAGEMENT LANDSCAPE

With the growing number of business applications and services moving to the cloud and the increase of mobile working, controlling and securing the access to data and applications is becoming more and more challenging. As a result, identity and access management (IAM) is evolving and has become a vital capability for any business. It is now more about ensuring a mature and high level of governance is in place when it comes to controlling and protecting business applications and systems, whilst also playing a huge part in business enablement and flexibility.

IAM was historically driven by compliance and user provisioning. It had a very limited scope of coverage in terms of applications, a low return on investment and provided very restricted controls and views of access. This has evolved to become far more driven by risk and user entitlement. Application coverage has also increased greatly and the visibility is far superior today than it ever has been. IAM is changing and moving towards a capability and business enablement driven requirement, with further progression of application and technology support.

CHALLENGES FACED BY ORGANISATIONS IMPLEMENTING IAM TODAY

Whilst the benefits of introducing an IAM solution can be vast, many organisations are unable to comprehend some of the major challenges facing them when looking to implement IAM. These challenges can cause issues when attempting to obtain senior management buy in.

Some of the most common issues faced when looking to implement an IAM project are as follows:

- **Orphaned or system accounts**
  Many organisations have system or user accounts provisioned but do not have any controls identifying who is responsible or owns these accounts. This causes issues when migrating and provisioning accounts within an IAM platform

- **Control over privileged combination access**
  Many employees will have multiple permissions at various levels across an organisation. This can cause issues as it can provide a way for a user to gain access to a system even though they do not specifically have permissions assigned to them

- **Incorrect permissions**
  Many organisations find that employees may have been provisioned with higher privileges than necessary, simply due to having a similar job title as another employee

- **IAM platform maintenance**
  Once the solution is deployed, identifying and governing the maintenance and on-going review is key for an IAM solution to be effective

TAKING A NEW APPROACH TO IAM

With the changing technology landscape, it's important to focus on what the organisation wants to achieve. Whether this is enabling a mobile workforce or migrating to cloud services, it's not a case of adapting what currently exists but rather understanding what the key requirements are in order to make the transformation within an organisation.

MOBILE SECURITY

Securing users devices is increasingly important with the growing number of employees based in remote locations, along with the rise in the number of mobile devices available to users for business purposes. Traditionally, organisations have tried to secure mobile devices with a specific MDM solution which results in additional platforms to maintain and govern, training requirements for staff and potentially costly support contracts. To simplify this requirement, choosing an IAM solution which allows the incorporation and control of mobile devices is an effective way of reducing both CapEx and OpEx, along with providing effective governance and control over data and system access. A solution, such as Ilex International's Mobility Center, provides a host of security protection methods for mobile devices including:

- Multiple authentication schemes with one or more factors (NFC/Password, Client Certificate, Out-of-band Mail/SMS, QR Code), that can be integrated with each other
- Access control and single authentication (Single Sign-On) on mobile Web applications or iOS/Android native applications
- Complete protection of corporate data on the mobile device (integrated secure web browser, secure data container per user, document read-only mode, anti-spy screen filter, etc.)
- Native application available in Apple Store and Google Play Store
- Simple integration of the API into your corporate mobile applications
- Fully secured application. No local configuration is required – self-destruction of secured containers in the event of a mobile jailbreak, all data is cleared and deleted upon user disconnection, inactivity time-out or violent shock

CLOUD SECURITY

With more and more organisations moving applications and services to the cloud, maintaining security whilst ensuring the user experience is positive is increasingly complex. One of the biggest challenges today is provisioning and de-provisioning users in a timely manner, ensuring the correct governance is in place and having clear processes and procedures. The other challenge when securing access to the cloud, is when multiple applications or platforms require access. This creates a problem for users that are required to log on multiple times with a combination of credentials and leads to poor passwords. Deploying a single sign-on capability is one of the simplest, scalable and most effective ways to ensure the user experience is positive but that access to cloud services is also secured. Ilex International's access management can overcome these issues and provide business productivity and enablement through a positive user experience, as well as the security required to protect these systems. Some of the key features are detailed below:

■   Unification of strong authentication, Web Access Management, Mobile Access Management, Identity Federation and enterprise SSO

■   Unique coverage of Identity Federation standards: SAML2, Open ID, OAuth2, WS-Federation

■   Flexible, modular and robust solution

■   Adaptability to new professional practices: Roaming, Fast User Switching (FUS), terminals, new devices, Cloud

■   Portability of SSO on tablets and Smartphones (iOS/Android) thanks to the Ilex's Mobility Center module
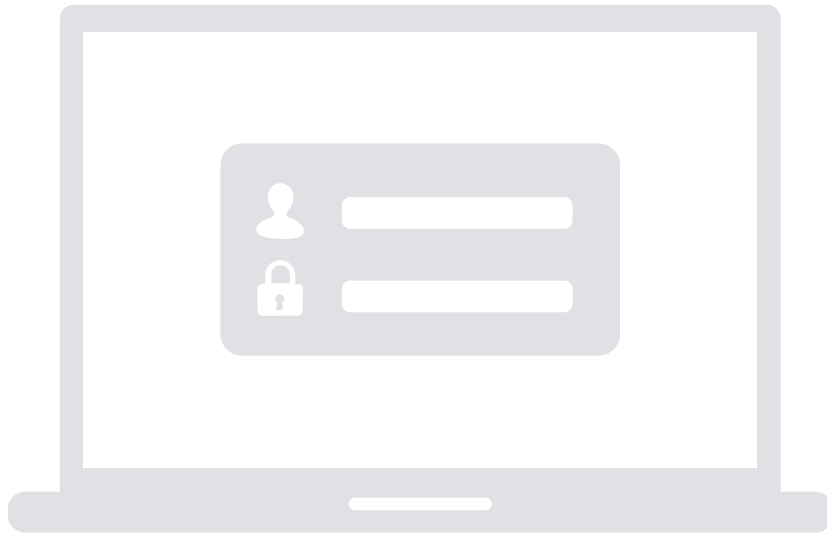
UNIVERSAL ACCESS MANAGEMENT

One of the challenges with IAM is the lack of capabilities provided by any one vendor or solution thus creating a requirement to integrate multiple platforms or solutions. This creates additional overheads, poor user experiences and the inability to correlate events, reports and alerts. However, this can be overcome by adopting a single solution that provides all the access control required on one platform or at the very least, from one vendor which enables total integration.

Ilex International's access management products provide exactly this, multiple access controls and capabilities which can be deployed and scaled in a modular fashion. This ensures a single source of information as well as full integration, resulting in reduced overheads and a positive user experience. It also allows organisations to roadmap capability and rollout to minimise disruption, and spread the commercial impact.

By enabling users to carry out self-help services, such as password resets and account unlocks, it reduces the load on the help desk and employee down time, again resulting in a cost saving for the business.

STANDARDISED IDENTITY MANAGEMENT FOR GROWING BUSINESSES

Most IAM solutions are not suitable or don't cater for smaller growing organisations, with many not being able to justify the necessary spend to embark upon an IAM journey. This is changing with vendors such as Ilex International providing a very effective and powerful out of the box IAM solution for smaller organisations. It can be delivered in a packaged approach, in a short timeframe, whilst also providing enterprise level features which have historically only been available to larger deployments. Ilex International also offers a more bespoke solution which offers a full enterprise identity solution. Both options fully integrate with Ilex's access management products. Combined, this provides organisations of all sizes with an end to end IAM solution which is simple, scalable and secure.

CONCLUSION

Taking the first steps with IAM can seem daunting but providing a clear understanding of the business requirements and the desired outcome has been captured, it no longer needs to be a painful and technically complex project. Once these are understood, a clear strategy and roadmap should be produced to ensure all business requirements and other elements are considered and incorporated. The deployment should be risk based and delivered in phases - the all at once approach simply does not work in today's landscape. Ensuring the correct governance and processes are in place is also vital for an IAM solution to be effective, deliver value and enable the business.

With more regulations being enforced, such as the GDPR which carries substantial fines should a business be found in breach, ensuring data and systems are protected and having visibility into the network and user activity is becoming even more important. Couple this with the fact perimeter devices are no longer an effective means of protecting and governing access, organisations need to change their strategy. It's time to embrace IAM and view it as a business enabler, not just 'another security tool'.

ABOUT THE AUTHOR

Gabriel Wilson provides Identity and Access Management consultancy to Ilex International. He has over 10 years' IT experience and specialises in technical information security. He leads Rivington Information Security's Managed Service practice (Ilex International's implementation partner) and as a Managing Consultant has worked with many high-profile clients across a multiple of industries, most notably Oil & Gas, Finance and Retail, both within the UK and Internationally. His broad range of experience includes managing complex teams and solutions, the design and operation of Security Operation Centres determining the most appropriate security technologies to support the business aims. He is further experienced in Identity Management, Threat Prevention, Vulnerability and Incident Management, Malware analysis and Intrusion detection. His projects range from multimillion pound international deployments to smaller-scale compliance audits and assessments.

ABOUT ILEX INTERNATIONAL

Ilex International is a European Identity & Access Management (I&AM) software vendor. Founded in 1989 Ilex offers a comprehensive solution including identity management (identity, rights and role management) and access management (authentication, access control, SSO, identity federation and card management). The organisation invests heavily in R&D, providing state of the art technology and services to a large international customer base across finance, defence, healthcare, government and retail sectors.