CORE

IDENTITY AND ACCESS MANAGEMENT

The critical component of any cloud strategy

FOREWORD

Identity Management has been an integral part of all enterprise environments for a number of years, but it's criticality in the walled garden of an on-premise infrastructure is negligible.

As a result, managing identity is commonly overlooked by customers starting their journey into the brave new world of cloud; at least that is, until the organisation adopts more than one cloud service or platform. Identity and Access Management is the gateway to securing cloud access and services; getting it right can be challenging, getting it wrong can be disastrous.

If there is one certainty for every organisation, it's that existing people will leave and new people will join on a regular basis. Making sure you have a mechanism to manage this efficiently and effectively is a critical business requirement.

It is possible to introduce an Identity and Access Management solution at any point during your organisation's cloud journey, but it is far better to build it in as an integral part of the strategy for cloud adoption and get it done early.

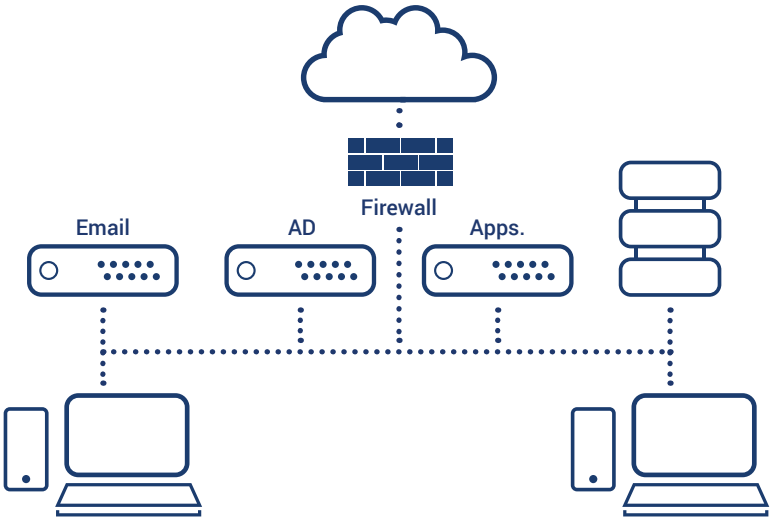
The following paper explains why identity is often overlooked by organisations and why managing identity in the cloud is critical for both security and user experience.

THE DAWN OF IDENTITY

Since the first days of computer networks, identity has been part of the IT landscape.

In the early networking days (around the time of Mainframes and Token Ring networks) each terminal needed an address so that the right packets of data could be sent to it. But systems quickly required users' credentials as a secondary form of identity to ensure access was provided to authorised users. This model continued through the rise of the PC and migration into the Client/Server topology that we use extensively today, taking identity into its "teenage" years.

This basic requirement barely changed until around 10 years ago. Identity remained a way of identifying users and providing security and control over access to organisational resources.



Most of the time, major resources sat within a walled garden of a private datacentre, behind the organisation's firewalls and physical security.

It was easy to provision and de-provision users in the walled garden. The advent of Active Directory and other similar identity services made it easier to provision and de-provision services automatically.

The onsite System Administrators owned the network and could immediately react to any unsanctioned access to resources because they could view and control the traffic. Then, the 1990s brought email, and remote users came to the fore; field-based or senior employees who travelled often and needed remote access to company resources to be optimally productive.

As a result, organisations invested in Remote Access servers and security solutions to protect their resources from the potential threats of external access.

The safety net, though, was that these resources were still fully under the control of the System Admins. The moment they saw any suspicious activity, such as a sudden uptick in network traffic, or unexpected activity on servers and storage platforms, they could essentially pull the plug and sever whatever connection they didn't like until they determined if it was valid.

As we progressed into the new millennium, the number of remote users and the devices used grew, but the principles remained constant; secure the devices and access credentials (the key for the big iron gate into the walled garden). If an unauthorised user still managed to sneak in, their activity would be spotted and terminated quickly. Risk mostly managed, threat mostly neutralised.

By this stage, identity management played a larger role in helping to reduce the physical administration of onboarding and offboarding users. Role Based Access Control came to the fore and allowed the issuing of user credentials and the appropriate licences based on the job requirements. 'Road Warriors' get the right licences and hardware for remote access, office staff don't.

Email, applications, storage are all operated on-premises, still within the walled garden. One set of credentials provided as much security as was required, because the IT Operations Centre was monitoring the key metrics in real time and could still have easy access to the kill switch if anything went wrong.

Barring some additional fortification of these security measures - mostly to counter the rise of the internet and the additional potential for malware to be introduced to devices - there wasn't any need for a paradigm shift because the basic principles of infrastructure and access hadn't changed all that much.

Then Came Cloud

By the latter stages of the 2000s, the Internet had become a common tool for the business workplace and cloud computing arrived. Suddenly, individuals were using a whole range of services that could be accessed anywhere and everywhere.

The ability to access services whenever and wherever you were, as long as you had a data connection, was a revolution of sorts.

The rise of cloud technologies brought about a paradigm shift for IT, changing users' experiences and expectations of the always-on, anywhere access model whilst also providing businesses with a surprise option for their IT infrastructure: rent instead of buy capacity.

Early adopters saw an immediate reduction in costs, lower electricity bills, lower carbon taxation, plus some improvement in performance and accessibility in many cases, and the race to adopt cloud computing started.

Why is IDAM a Critical Requirement for Cloud Strategy?

Cloud is still a relatively new concept for enterprise, with many customers operating in a hybrid model, with a very small selection of cloud services.

If your enterprise is only consuming cloud services from a single provider, such as Microsoft Office 365, the administrative burden of managing identity isn't significantly more than operating an on-premises infrastructure, and the security implications aren't extensive; at least at first glance.

It is becoming clear, though, that customers who are adopting the cloud aren't settling on a single platform. Many vendors are offering cloud-based subscription versions of their software as an alternative to on-premises licensing, with a cost advantage to reflect the economies of scale and lower risk profile; (if you don't pay for your licence, they can control your access to the service).

The proliferation of devices also means that the routes available to access services are greater than ever. This opens up more attack vectors for the modern cybercriminal.

With more cloud services being consumed across multiple devices, conditional access policies and robust password management is essential. Failure to implement these policies can seriously compromise network security. As an example, a professional services company identified by Microsoft's Detection and Response Team (DART) was affected by an advanced persistent threat (APT) that gained access to privileged organisation credentials. Using weak and commonly used passwords as part of a password spray attack, attackers gained access to Office 365 administrative credentials and a number of user accounts within the organisation.

Having engaged the DART team, the company learned that they needed to deploy controls to safeguard the cloud services they used including multifactor authentication and conditional access policies for certain cloud apps.

Identity and Access Management comes to the fore as a first line of defence against all the issues outlined above.

Cloud Identity versus Legacy

The evolution of identity has caused some additional challenges for modern organisations on a number of fronts:

Identity Composition

In the on-premises world, organisations were free to construct their identity however they saw fit. This would either be based on the IT department's preferred structure, a recommendation of general industry best practice, or to support a particular line of business legacy application. For single organisations with a simple directory structure, this doesn't present a massive challenge when migrating to the cloud. It gets challenging when previously disparate organisations merge and there is inconsistency in identity attributes.

Mergers and Acquisition

When two disparate organisations merge, the big financial impetus for this activity is a rationalisation of people and services. From an IT standpoint, this can be challenging if the disparate organisations have significantly different identity structures. This was an issue in legacy applications just as it is now an issue in cloud. Previously, organisations would have to look at significant identity re-working as part of the merger process, which is time consuming, costly and contains some risk to the organisation and the users' ability to access services. The same issue exists for cloud, except with the added factor that identity is the only security factor you can apply.

Lifecycle Management

Managing the identity lifecycle is time-consuming and a major cost for IT teams. In the on-premises days, IT teams would create an identity for new users, assign appropriate licences for joiners, change permissions and licences for people moving roles and de-provision services for leavers. Even for a single identity, this is labour intensive and time consuming. In the cloud world, users need an identity for every platform that needs managing with appropriate subscriptions for each of the platforms that you operate on, multiplying the workload and drain on IT resources.

Consumption of Multiple Platforms

From a business-continuity perspective, it makes perfect sense for any enterprise to spread its consumption of cloud services across multiple platforms.

Solution providers may only offer a cloud-based service via their cloud, where they can control access, ensure that all licence subscriptions are up-to-date and easily manage out the potential for unofficial versions of their software being used. At the very least, their cloud option is likely to be the most cost-effective solution.

The pricing model has already shifted, with all on-premises versions of software increasing in price at a higher rate than their cloud subscription-based offering. Remaining with an on-premises version, while buying, powering, cooling and supporting physical servers is a much more expensive option. Putting that on-premises licence into a virtual machine in Azure is also likely to be more expensive than their native cloud service and will require more management by the organisation. So, all roads lead back to the consumption of multiple cloud platforms.

This is where the security risk starts to develop.

The Password Dilemma

Each one of these cloud platforms is its own walled garden requiring its own security protocols to gain access. In an ideal world, each one of these should have its own user credentials. The most commonly used username credential is an email address with a complex password.

Human beings are not typically good at creating and managing complex passwords. Left to human nature, in most cases one of the following three scenarios will occur.

Scenario 1 – The Golden Password

Faced with the prospect of using a range of cloud-based services, or any multiple of services where passwords are required, the first model of behaviour is to create one complex master password that will then be used on each service simultaneously.

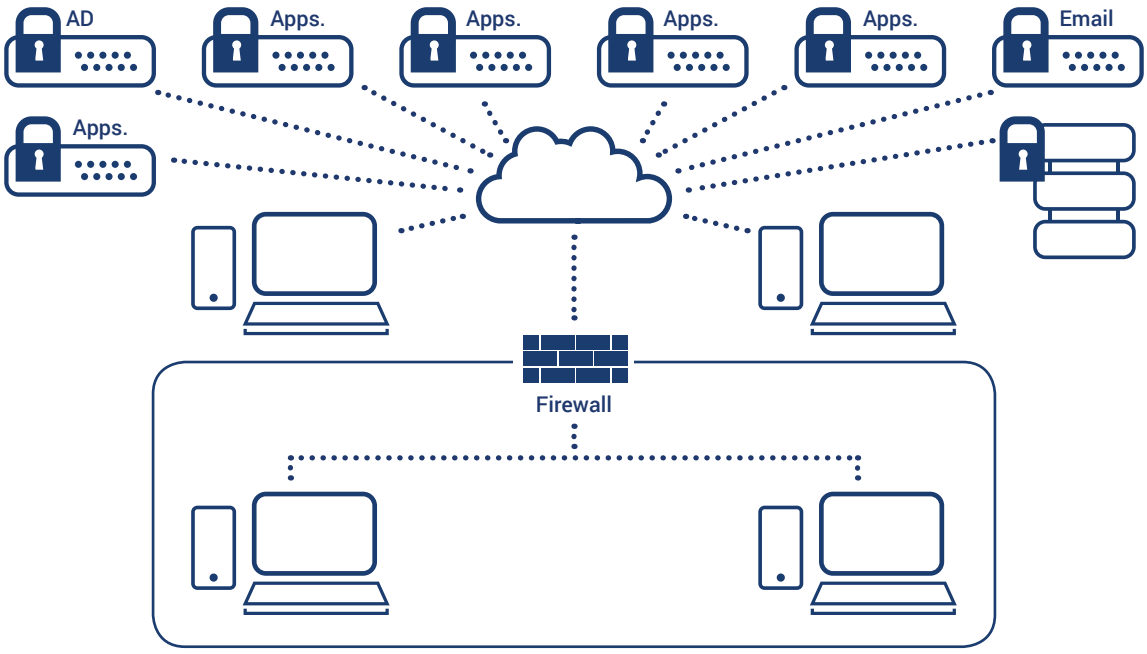


Figure 2 – Representation of all cloud platforms protected by the same "golden password"

The problem with this model is that if the password is somehow compromised through an attack, or just one of the cloud services in use is compromised, a potential threat actor suddenly has access to every resource the user has access to. In an enterprise environment, it is likely that the user's identifier is their corporate email address, so it would be relatively straightforward for someone to access the other cloud repositories.

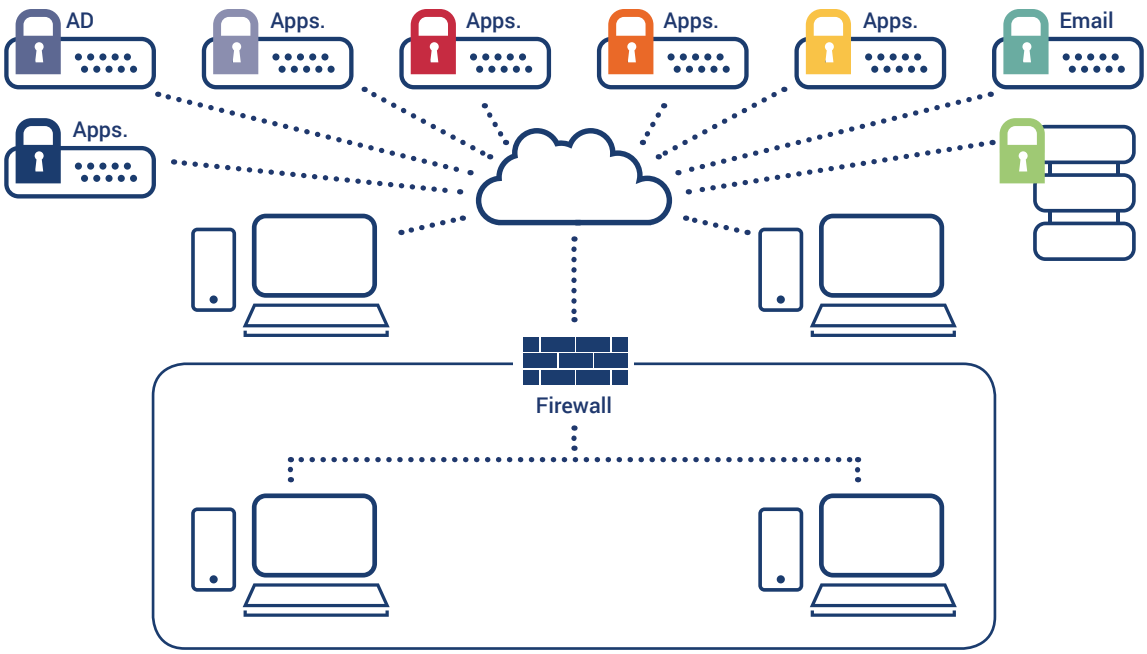
The potential for a breach of passwords extends beyond enterprise computing into consumer computing. Someone gaining a password from a phishing attack or some other platform-level breach would have a reasonable probability of success breaching a licences system with a password stolen from a consumer platform such as social media, online shopping or media streaming service.

Phishing continues to be a preferred attack method and will remain so for the foreseeable future. In 2018, Microsoft threat analysts found that phishing rates are still on the rise. Between January and December 2018, the share of inbound emails that were phishing messages increased by 250%. In November 2018, they accounted for 0.55% of inbound emails.

Going back to the first section of this paper, it is much harder to monitor the walled garden of a cloud-based service because by its virtual nature, it is used by a large and disparate community of users. It is therefore more difficult to identify unusual behaviour and take action, although many cloud platforms do have some additional security features that can help restrict unauthorised access even with valid credentials if they have been configured correctly.

A user and their employer could be blissfully unaware that a malicious user has access to their data for an extended time, which can lead to a range of reputational and financial, or legal, penalties.

From a security standpoint, it is best practice to hold a separate password for each cloud service.



The most secure option is for each cloud service to have its own dedicated password, not shared with any other cloud platform, so if it is breached the damage is limited to that single platform.

Scenario 2 – The Password List

The second option is to follow best practice and use a separate complex password for each cloud environment. This is complicated even with two environments; upwards of that the only way of managing this system is to store passwords on a list.

It should be noted that not all lists are an immediate security threat. For instance, iOS utilises a system where passwords can be stored in a secure, encrypted enclave on the device, and then used to gain access to the service following user authentication on the device. This works well until the device is lost, stolen or damaged. The information can be recovered, but there will inevitably be an element of lost productivity from user downtime. Not every user's main business device will be an iPhone or iPad, so the rationale is that the password list will end up being written and stored somewhere that is accessible to the user, but also potentially accessible to others.

The majority of users will write a list of usernames and passwords down on a piece of paper, or in a book, which they will either leave on a desk or carry around with them, so that they have it when they need it.

Once again, the security of the complex password comes under threat. If this list is copied or lost, the entire security of the password and the environment(s) it protects is compromised.

Scenario 3 - The Password Manager

The enlightened will recognise that "one password to rule them all" is not a safe security practice, and a list of passwords physically or digitally is risky unless it is heavily encrypted. These savvy users are the main candidates for our final option – The Password Manager.

A good quality Password Manager is absolutely essential for anyone to use in their personal digital life so that they are able to maintain a suitably secure, air-gapped password fleet that will protect the user against the vast majority of breaches and cyber-attacks.

The characteristics to look for in a good quality Password Manager should be as follows:

- The Password Manager should be able to generate unique passwords on demand for each user environment
- The Password Manager should have an easy function to replace and update passwords on each platform
- The Password Manager should be available on all platforms used by the user
- The Password Manager should integrate with those platforms and enable integration either into the device web browser or into the end platforms themselves
- The Password Manager should be from a reputable company and should NOT be free
- The Password Manager should enable MFA for access on any unknown devices as a minimum

There are a few items to consider with the use of a standalone Password Manager.

Provisioning and De-provisioning Users

Another challenge is administering access to these various cloud services.

In the BC on-premises world, provisioning a user often required the set-up of a single account and a single set of user credentials, or Active Directory can be used to provide some automated provisioning.

In the cloud world, this process needs to be repeated for each environment that the user will access, and again when the user is de-provisioned. In the most part this is a manual process, which introduces elements of resource use and risk.

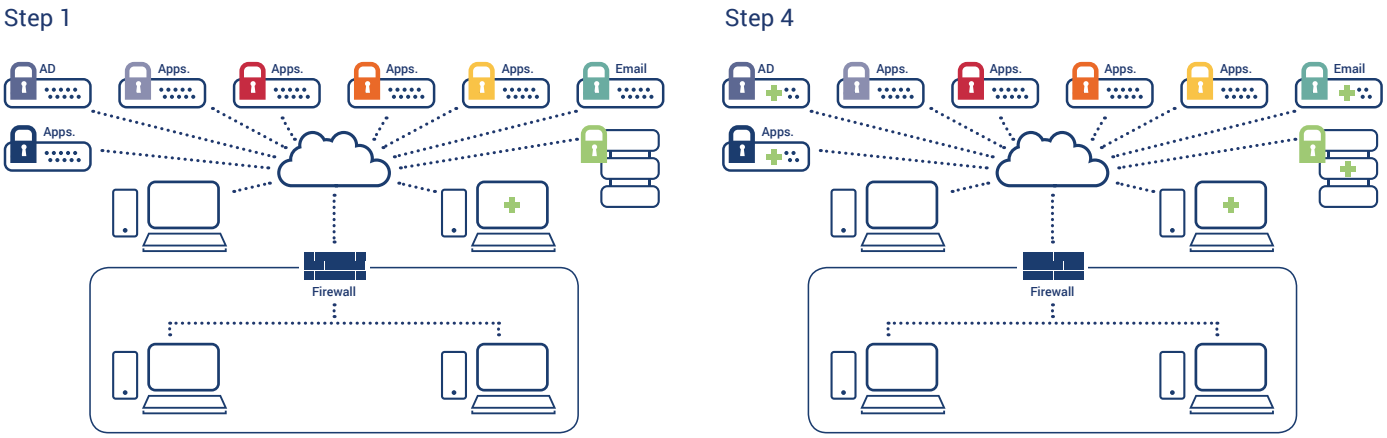
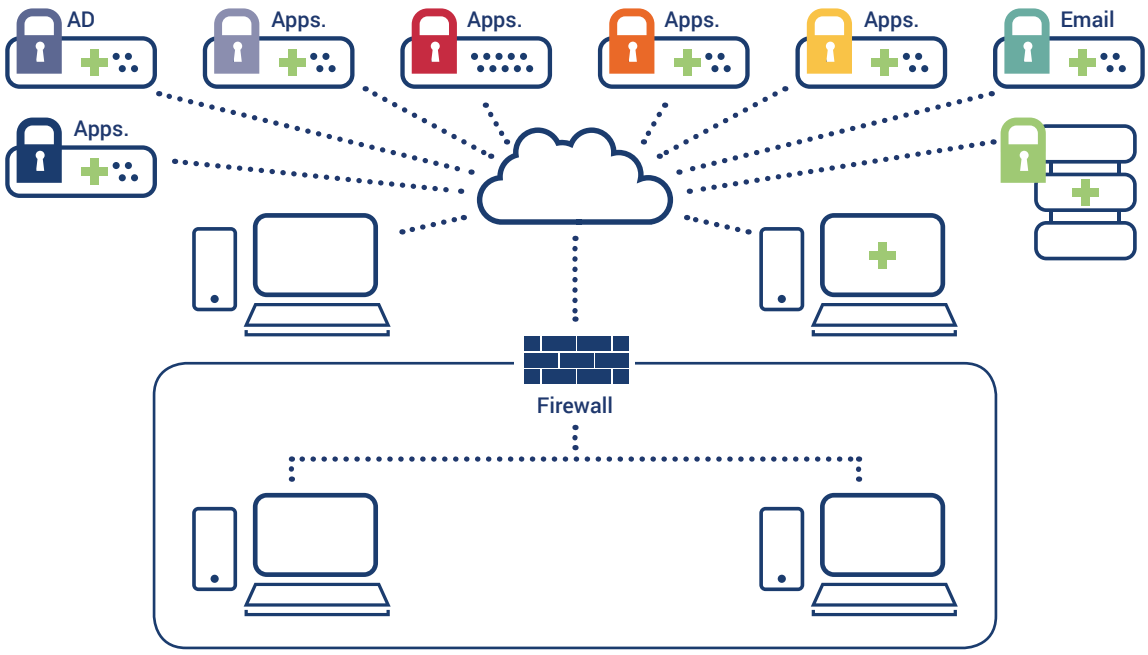
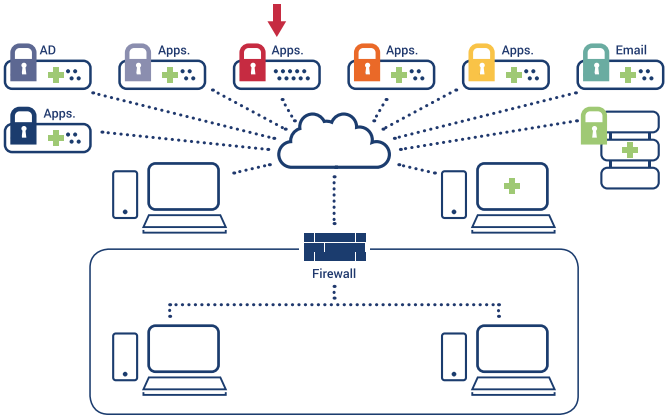


Fig 3. System by system provisioning via Human Resources on HelpDesk



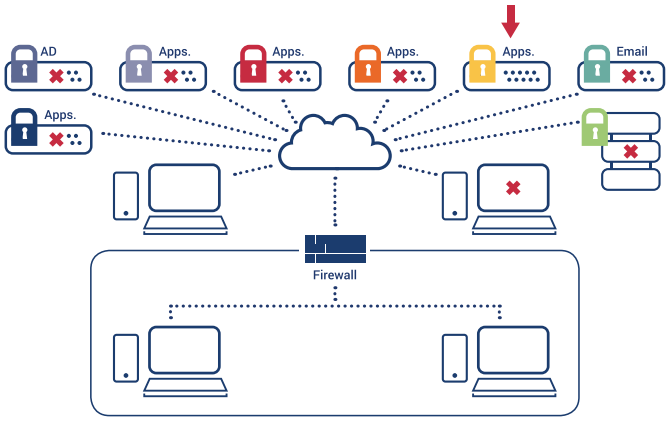
Manual provisioning can lead to human error and cause some systems that are appropriate for the user's role to not be provisioned first time.

The risk element creeps in with human error. If the provisioning process is mostly manual and time consuming, the potential for distraction during the process is high and can lead to steps being missed or completed incorrectly. This type of error can lead to the services not being provisioned properly for the user.



While by no means an irreparable error, additional productivity time is lost because the user cannot access the resources, and the administrator must revisit the provisioning for that service and recomplete it.

The same steps exist with de-provisioning users but with a further additional complication; services in the cloud that have not been correctly de-provisioned become a security threat. What if the service is for a leaver who is joining a competitor and continues to have access to your valuable data? What if the services are being withdrawn or amended because of a password breach
and one is missed?



From a reputational and business-risk standpoint the stakes are high, but there is also data protection legislation to take into consideration. Any data that exists is still the responsibility of the organisation who provisioned the service. If the data is lost or stolen, there are fierce repercussions under GDPR legislation.

If the data languishes there but reaches a point where the organisation no longer has reason to store the information, that too is a breach of GDPR.

In the protected walled garden of your on-premises infrastructure, with the servers and storage sat within your datacentre, it's very easy to audit and remediate these problems. It's not impossible in the cloud, but it is much more challenging.

Password Entry in Public

There is another emerging threat attached to anyone entering a password in public, regardless of how they created it or stored it.

Smartphones are fitted with high-quality cameras and able to record video at 4k resolution and in slow motion. This opens the potential for a "physical attack" through people videoing keypresses entered on a device when logging into a password-protected service. The attacker could also establish whether any licences were in place on the platform.

'Public' can also mean a lot of environments. The obvious locations are on a train or in a coffee shop, but public could also mean retail premises, shared office space, or any office space that contains visitors, contractors, temporary or other employees.

GDPR and the Cloud

Most cloud-based applications will hold personal data within their own walled garden. Therefore, organisations need to make sure they control access to this data rigorously. Having open access to a cloud service for an unauthorised person, even if they don't use it, is likely to be a breach in the eyes of GDPR.

Any personal data stores that are provisioned by the organisation, or any 3rd party applications that a user could access from their organisational IT, need to be managed. The organisation needs to ensure that they are removing access when appropriate and cleansing or deleting data when they no longer have any reasonable cause to hold it.

It's very difficult to audit and manage data, or access to data, that you don't know you have. Reporting breaches on cloud services that you aren't monitoring (because you believe they have been de-provisioned, or perhaps didn't even know they existed) is almost an impossible task.

Regulators now have authority to issue penalties equal to the greater of €10 million or 2% of the entity's global gross revenue for violations of record-keeping, security, breach notification and privacy impact assessment obligations.

However, violations of obligations related to legal justification for processing, (including consent), data subject rights, and cross-border data transfers may result in penalties of the greater of €20 million or 4% of the entity's global gross revenues.

For many organisations, reputational risk is worse than the potential fine. A number of well-known businesses have been irreparably damaged over the last 5 years because of public data breaches that have caused consumers to lose trust in the brand and take their business elsewhere.

In the public sector space, this type of issue generally leads to a complete senior management change within the organisation and in some cases, significant change to the structure and identity of the organisation to help distance themselves from the confidence issues caused by the breach. This is a very expensive process in itself, but also has a knock-on effect on the mission and deliverables of the organisation for a long period of time. In these austere times, this is a significant strain on the public finances and will have a profound operational impact for years following the event.

Challenges with Outsourcing

Another common challenge that is often overlooked when customers want to implement a new Identity and Access Management solution, is who should manage it.

Identity is a constant factor in all IT solutions and has been a requirement since the early days of computing. It's likely to be a constant factor in your IT strategy for the next 10-15 years or beyond.

As a result, organisations must consider this long-term requirement when deciding how to tackle identity management moving forward.

It is extremely common for organisations that outsource IT to place Identity and Access Management in the hands of their incumbent IT provider. There is nothing especially wrong with that, as long as the identity management is taking place in your infrastructure.

All too often, global system integrators will provide the infrastructure for their Identity and Access Management solution in their hosted environment; which is fine until you want to change providers. The organisation then faces a painful cost and risk of change factor, facing a migration of the entire solution to a new provider as part of the changeover.

All outsourced services carry some risk of change. Migrating hosted infrastructure and hosted desktops is a challenge, but Identity and Access Management is the most critical service - without it, no one has access to any services. The major outsource providers are fully aware of this and, unless challenged, will often propose to host this service knowing the complexities of migration will either support renewal of their contracts or enable them to add an extended offboarding period if they are exiting the organisation. This is due to the critical nature of the service and the need to migrate the services in a careful and controlled manner.

AURORA – IDENTITY AND ACCESS MANAGEMENT

Thankfully, there is a solution to all these challenges; a robust cloud Identity and Access Management solution which resolves the issues outlined above.

Aurora, from Core, provides a policy-based administration solution that meets the needs of modern enterprises. This solution is used to securely manage the user logon and authentication process for a variety of cloud-based services.

Aurora leverages Role Based Access Control (RBAC) protocols to allow our customers to automatically enable the right services for joiners and movers, as well as disabling all services for leavers, reducing your IT staff's involvement in completing operational tasks and freeing them up for higher value activities.

Aurora provides the ability to incorporate two-factor authentication (2FA) for added security where required. We can also enable users to access their services through any internet-connected device through a secure web-based solution.

The Aurora platform is accessible from any PC, laptop, tablet or smartphone, regardless of OS or vendor. It can also be branded in the organisation's livery and customised to your organisational requirements.

For management and administration, Aurora has over 50 enterprise-level audit reports enabled as standard, allowing administrators to immediately get visibility on policies, users and access. All user and group changes are audited with 'before and after' values so there is a trail of change information to monitor activity on an administrative level.

For public sector users, the platform has been certified to Official – Sensitive level.

Aurora is designed to operate as the single authority on identity and authentication for cloud and on-premises solutions - the primary identity vault. This can have an added benefit in environments where users have multiple aliases, or where HR systems must operate in a specific model with attributes that may change independently from what would normally be the key identity attributes in an Active Directory model.

Identity Lifecycle Management

The key benefit of Aurora is its ability to provide significant management and automation of the identity lifecycle. Its powerful automation capabilities let IT teams reduce the physical resource workload in creating, changing and closing user accounts. Users can have accounts created with the right permissions and licences on the correct platforms for their role through one creation activity. Aurora can also be integrated with the HR system to fully automate this process when new HR records are created, changed or a user is exiting the business. For organisations with 10,000+ employees, the service will often cost less than the resources required to provide this service manually, with the added benefits of consistency that are listed below.

One-touch Provisioning and de-provisioning

Administrators can create, change or close user accounts and access across multiple platforms from one console, with the workflow process managing the various cloud platforms and legacy applications. This drastically reduces resource time that the organisation must use to set up, change or close down users. With full HR system integration, this can be reduced to Zero Touch.

Role-based Provisioning and Access Control

Policies set within Aurora automatically provision the correct services and licences for users based on their role type. This ensures that joiners or movers are consistently provided with the access they need to complete their role in a productive manner and ensures consistency of identity structure by removing the human element. This reduces the danger of users being provisioned for services that are not appropriate for their role, and users not being able to access services that are role-specific because a person has made a mistake.

Licence Allocation

Aurora can provision licences for users appropriate to their role type and platform access requirements as part of its automated process. This ensures that users can access the services they need, but also ensures that your organisation is protected from licence compliancy issues for users that are not licensed correctly, which can also mean being over-licensed, due to human error.

Consistency of Identity

Aurora will provision identities in a consistent manner, based on the policies set at its creation. This again removes the human error element where Administrators may have different ways of setting up user attributes. More importantly, it ensures that any identity pre-requisites for specific applications or cloud platforms are fully met, ensuring the security and access capability of the user.

Seamless Co-existence in Legacy and Cloud

One of the major challenges currently facing larger enterprises is managing the transition from legacy on-premises applications to cloud-based services. Typically, these organisations will have a range of existing legacy services that are business-critical but may depend on the identity structure being a certain way to enable it to function.

In many cases, that structure may not fit with the identity structure needed for consuming cloud services, where some modern standards have been applied.

Managing this co-existence is a significant challenge for a lot of organisations due to the technical complexities and the need to ensure that the user experience is not degraded during the period of dual running - which can last for years in many cases.

This is an area where Aurora is significantly ahead of many of the market-leading solutions available today.

Identity Transformation

Aurora is configured to take the existing identity structure and reorganise it into a suitable format to access cloud services. This may be a simple re-positioning of attributes from an existing Active Directory, but more often than not it will also require accessing attributes from other areas and creating attributes that may be required, such as an immutable ID.

Cloud Identity Vault

Aurora will build the cloud identity in a cloud identity vault, which can either exist in the Aurora platform or another suitable platform such as Azure Active Directory. The composition and location of the vault will ultimately depend on the services currently consumed by the organisation and their overall strategy.

Synchronisation

In order to function, the cloud identity vault will need to stay in sync with the legacy directory services in order to update user attributes such as password changes. Aurora's powerful workflow engines ensure that changes made in one platform are updated in all other relevant platforms, so the user identity is always up-to-date and fully functional.

Single Sign-On / Seamless Sign-On

Aurora is designed to support all modern authentication protocols, enabling the user experience to be streamlined through the use of Single Sign-On or Seamless Sign-On capabilities. This has numerous security benefits and enhances productivity for the user. Aurora has the capability to deliver an SSO-like experience for users on platforms that do not natively support SSO, which can help to improve user productivity and security on older platforms.

Independence from Traditional Outsourced Services

Core is a leading independent provider of Identity and Access Management solutions. We regularly work with customers who have identity challenges that are beyond the capability of a normal system integrator to manage.

Our recommended model is to keep the Identity and Access Management solution ringfenced from other outsourced providers. We can host the identity vault solution in a dedicated Azure tenancy which we host on behalf of the customer, in their own environment or in Azure Active Directory. This means when the organisation wants to change IT outsourced services, Identity and Access Management remains constant, which considerably de-risks a lot of service provider changes.

FEATURES AND BENEFITS

To provide some greater detail on the main elements of the Aurora solution, the following section provides a more detailed explanation of the key features and benefits.

Administrative Policy Enforcement

The administrative policy enforcement featured by Aurora considerably reduces administrative workload, improves network security and ensures consistency across the entire enterprise. Automating administrative workflow significantly reduces the amount of time to complete tasks and can eliminate certain tasks altogether. It also minimises errors, reduces the need for rework and combines related actions into a single batch.

Aurora IDM provides the facility to specify how, when and what must change whenever directory objects are created, modified or deleted. Furthermore, it is possible for Aurora IDM to only accept data changes that conform to certain formatting requirements. This helps maintain control of the data stored in the directory and how it looks in other systems, like email.

With the ability to enforce administrative policies and automate administrative workflow, Aurora IDM saves time and keeps network objects in a consistent state in relation to each defined policy. This addresses important security, usability and integrity issues that are central to the management of network object data.

Policy Objects

In Aurora IDM, administrative policies are defined by using Policy Objects—collections of policies. Policy Objects define the behaviour of the system when directory objects are created, modified or deleted.

There is the ability to create a Policy Object that includes any number of different policies, such as format validation, generation rules for the values of object attributes, scripts that supplement administrative operations, automatic creation of user mailboxes on prescribed Exchange servers, automatic creation of user home folders and home shares, and relocation of an object to a specified container when it meets certain criteria, such as changing department.

Aurora IDM provides extensive capabilities for automating administrative processes. Policy Objects can run customisable scripts before or after the execution of any specific task, and multiple tasks can be combined into one operation. This functionality significantly reduces the amount of time to complete administrative tasks and minimises errors.

Workflow

Aurora IDM also provides a rich workflow system for directory data management automation and integration. Based on Microsoft's Windows Workflow Foundation technology, this system lets IT define, automate and enforce management rules quickly and easily. Workflows extend Aurora IDM's capabilities by combining versatile management rules, like provisioning and de-provisioning of identity information in the directory, enforcement of policy rules on identity data changes, routing data changes for approval, and email notifications of events and conditions. It can also implement custom actions using script technologies such as Microsoft Windows PowerShell.

Workflows may also include approval rules that require certain changes to be authorised by designated approvers. The administrator designing the approval workflow specifies which operations cause the workflow to start and adds approval rules. These determine who's authorised to approve the operation, the required sequence, and who needs to be notified of tasks or decisions. The workflow can trigger automatic escalation if an approval sits waiting. Designated secondary approvers can be automatically emailed to approve changes so requests don't stagnate.

By delivering email notifications, workflows extend the reach of management process automation throughout the enterprise. Notifications email people about events, conditions or tasks awaiting attention. For example, approval rules can notify of change requests. Separate notifications can inform about directory data changes. Notification messages include supporting information and hyperlinks which let recipients take action using a standard Web browser or accept or reject the change via email.

Single Sign-On

One great way of tackling the password list issue and improving user experience is to provide a simple, secure Single Sign-On (SSO) facility for all approved cloud services.

The Aurora platform integrates with (but does not include by default) Windows Azure Active Directory Premium, which offers SSO to these cloud-based services, plus around 2,500 other cloud applications.

The Aurora platform also includes a fully-managed and supported Windows Active Directory Federation Services server infrastructure, where customised authentication connections can occur to support custom applications that might exist within the environment or in the cloud, but which may not have been written to the correct standard for WAAD Premium to provide the SSO. The ADFS farm also provides an enhanced SSO experience for on-premises users of Office 365 services (this requires a two-way trust from the identity vault to the users local AD).

Each service needs to be on-boarded to the Aurora platform, but once this is complete users have a full Single Sign-On experience to all approved cloud applications, without having to enter the application's specific user credentials and password. Onward authentication from Aurora to the connected service will be managed through a suitable protocol, (i.e., SAML), based on compatibility with the connected service and the security requirement of the customer.

A secondary benefit of the improved user experience is that users are less likely to use non-approved cloud services (such as the consumer version of DropBox) to their cloud portfolio when they can easily access an approved service (such as OneDrive for Business), with a single click.

This can be a powerful way of tackling the current rise in "shadow IT" that is causing concern for many CIOs.

Security

Security of cloud services, and the platform that manages their provisioning, de-provisioning and administration is critical to ensure the health of the organisation.

Aurora has been designed with the following arrangements for security, availability and continuity.

Azure datacentres and connectivity

The Aurora authentication service is hosted on Microsoft's Azure Infrastructure as a Service platform, with physical datacentres located in Ireland and Amsterdam. It makes use of the "Virtual Machine" and "Networking" services of the platform:

- ISO/IEC 27001:2005
- SSAE 16/ISAE 3402 (Service Organization Control [SOC] 1, SOC 2, SOC 3)
- FISMA
- PCI data security standard

Aurora has been fully penetration-tested and is approved to Government Official-Sensitive level.

All administration is carried out with separate, user-identifiable accounts to ensure clarity of auditing, and access is provided using "Least Privilege" principles.

From a user perspective, another key benefit is that users will not hold the specific credentials to access their cloud services outside of Aurora.

ORGANISATIONAL ADMINISTRATION

Aurora enables administrators to provision and de-provision users with ease.

User Self-Service

Users are able to self-serve a number of common administrative tasks, such as password resets.

Platform Resilience

Aurora is designed to be highly resilient and provide maximum uptime for users.

Aurora achieves an SLA of 99.95% availability, with co-located arrays delivering a geographically dispersed service to counter any local power or connectivity issues. All user data is replicated to the power of six, allowing us to deliver a Return to Operations time of zero minutes in the event of any issues at the storage layer.

Managed Service

Core provides Aurora as a full managed service offering, with access to our Managed Service Centre for support, either during office hours, or 24x7x365 as required.

Key Benefits

- One username and one password for your users to remember
- Empower user self-service and flexible working locations with access from any device or browser
- Put the organisation back in charge of group membership
- Reduce administrative mistakes/workload with automated workflows
- Reduce administrative mistakes with locked value drop-down lists
- Workflows can automate typical manual changes during the provisioning/de-provisioning cycles
- All user and group changes are audited with before/after values
- Automated user synchronisation from multiple source systems
- De-couple identity from your other outsourced IT services to simplify and de-risk any changes in your supplier landscape.
- Core is always at hand with 24x7 multi-lingual support

ABOUT CORE

Core is a managed services technology company for people and businesses who want control of their IT and to drive their business forward using it. As a trusted Microsoft Gold Partner, Core offers innovative technical solutions tailored to individual business objectives, and specialises in implementing the latest systems, both on-premises and in the cloud. At Core, our focus and priority is putting our customers in control of business transformation through implementation of the right systems and Core team members, to drive businesses forward and make IT work for the users at the heart of that business.

We do this through our four Core Values:

- **Customers:** We put our customers first, taking responsibility for our actions
- **One Core:** We recruit, develop and retain the best talent in a supportive environment
- **Responsiveness:** We're flexible, approachable and responsive to our customers' needs
- **Expertise:** We act professionally to our customers, peers, partners and constantly strive to achieve excellence

We are proud of our rich history of technical achievements, since our inception in 1990. Core's main focus industries include Government & Local Authority; Legal & Professional Services; Financial & Insurance; Retail and Membership organisations. Core is proud of the work they do in the Not for Profit sector. Core has an impressive track record, dating back to 2001 when we implemented the UK's first Microsoft SharePoint system. Since then, Core has been involved in some of the largest such projects Microsoft has seen. Most notably across our specialist sectors, Core works with The Law Society; TotalJobs; The National Autistic Society; The Royal College of Ophthalmologists; East Midlands Ambulance Service NHS Trust and Wolverhampton Council.

If you would like further information on what Aurora can do for your organisation, please contact Core on **0207 626 0516**, or email **hello@core.co.uk**, or contact your Account Manager.

Core
Frazer House,
32-38 Leman Street
London E1 8EW

Company No. 02502866