Identity Management (IdM) Challenges of the Hybrid Enterprise

Enterprises have a major challenge - to create a secure and response identity system in an hybrid architecture. The hybrid architecture defines an enterprise that is both enterprise-based and has components hosted in the cloud. The modern hybrid environment has usually not been dictated by a centralized decision or thought-out policy, but instead usually the result of a set of individual decisions to take advantage of particular off-premise resources.

On top of these ad hoc "cloud migration projects, enterprises are challenged by the "new user" conundrum. Most entities held by enterprises are NOT classic employees - instead they are a myriad of partner, associate, contractors and other non-employees whose identities are needed for the smooth operation of the enterprise.

The challenge is to create a workable, comprehensive security framework that handles these current identity topographies and demands.

The IdM (Identity Management) problems remain the same: create users, authorize access, attest/log the permission and usage. The "job" has just got harder with the new requirements of geography, users, devices and cloud based resources.

Risk of a Poorly Managed Hybrid Enterprise

When educated IT people think of enterprise identity theft - most think of a poorly protected identity stores, Active Directory (AD) or others. From these exposed datastores, the ID/Password file is stolen and hackers now "own" the identity.

These attacks certainly exist and their are many documented instances of these files being posted to the "dark web" and sold via various mechanisms. But it's important to note - that this is just part of the IdM risk.

Attackers are often looking for the "gift that keeps on giving": PII (Personal Identification Information). PII is the information used to identify and create a NEW account. Hackers misuse PII to create NEW identities to impersonate the original user. This is very common in the B2C world in the world of finance and credit cards.

But the threat is also relevant to B2B and B2E IdM scenarios. These enterprises have to also insure that PII and authorization information is not falling in the wrong hands. If identity information, which is handled by key enterprise control mechanisms such as Privileged Access

Management (PAM) tools, Provisioning and Identity Syncing tools and mobile management tools fall in the wrong hands - the security equation of the enterprise tips in the favor of the attackers.

Lastly for hybrid environments, enterprises need to be cognitive of the problem of “fragmented” identities. Where key parts of user information is (unnecessarily) duplicated across datastore and cloud services. This information can be stolen by attackers for both the identity credential and PII information.

This paper will discuss how these risk can be addressed, with modern identity tools.

The IdM Cloud Security Market

There is no shortage of tools that market provides to handle the cloud/enterprise IdM conundrum.

Recent industry research shows that the global cloud IdM market was valued at close to USD 1.05 billion. The study revealed the global cloud security market is expected to grow at a CAGR of over 20% until 2019. IdM solutions led cloud segment for security purchases.

The adoption of cloud IAM solutions is growing among large enterprises and SMBs with increasing amounts of critical and confidential data being transferred. These solutions provide enterprises with greater control over access to applications and sensitive information from remote locations. High professional and personal use of mobile devices is also driving the demand for cloud IdM, as these are highly susceptible to attacks.

Let’s break down IdM to its functionality to better understand what the requirements are. In it’s core, the function of these solutions is to provide:

- Account Creation/Approval
- Account Syncing
- Account Access
    - Web, Device, Mobile and Cloud
- Account Attestation
- Application/Resource Allocation

But what are the issues for these for each of the activities and the tools that attempt to solve, especially in the hybrid (cloud/enterprise) environment? And what are the issue and overlaps of the products.

In essence, how do we obtain the value for these products that they were designed to bring.

The Essential Security IdM Products in Hybrid/Cloud Environment

As discussed, the essential duties of IdM have not changed: create accounts, manager users and allocate resources. It's just the scope of the efforts is much greater. Thus the proliferation of products/services that must portend to work with both enterprise and cloud executed services.

We will break down the products and services in the (3) main categories of deployment:

- Enterprise
- IAAS (Infrastructure as a Service)
    - AWS, Google GCE, Microsoft Azure, Private Clouds
- SaaS (Software as a Service)

As stated the offering must meet all environments, but what is offered, how they function and what components they have at each domain - will differ.

- Enterprise
    - Directories
    - IdM/Provisioning Systems
    - SSO/Federation
    - 2-Factor
    - RADIUS/NAC Systems
    - CASBs (Cloud Access Services Brokers)
    - PAM (Privileged Access Management) Systems
    - Mobile Management
    - Identity Attestation Systems

- IAAS DataCenters (Infrastructure as a Service)
    - AWS, Google, Azure, Private Clouds
    - Contain virtually anything housed at the enterprise
    - For security reasons, primarily host:
        - Additional Directories
        - IdM Tools
        - Logs/SIEMS

- SaaS Services (Software as a Service)
    - Traditionally:
        - Messaging, CRM, HR, Expenses
    - Now many IdM Services
        - IdM as a Service
        - 2-Factor as a Service

The focus here is how to correctly utilize the modern IdM products and services - for your enterprise. A sample of the architecture can be seen in image #1.

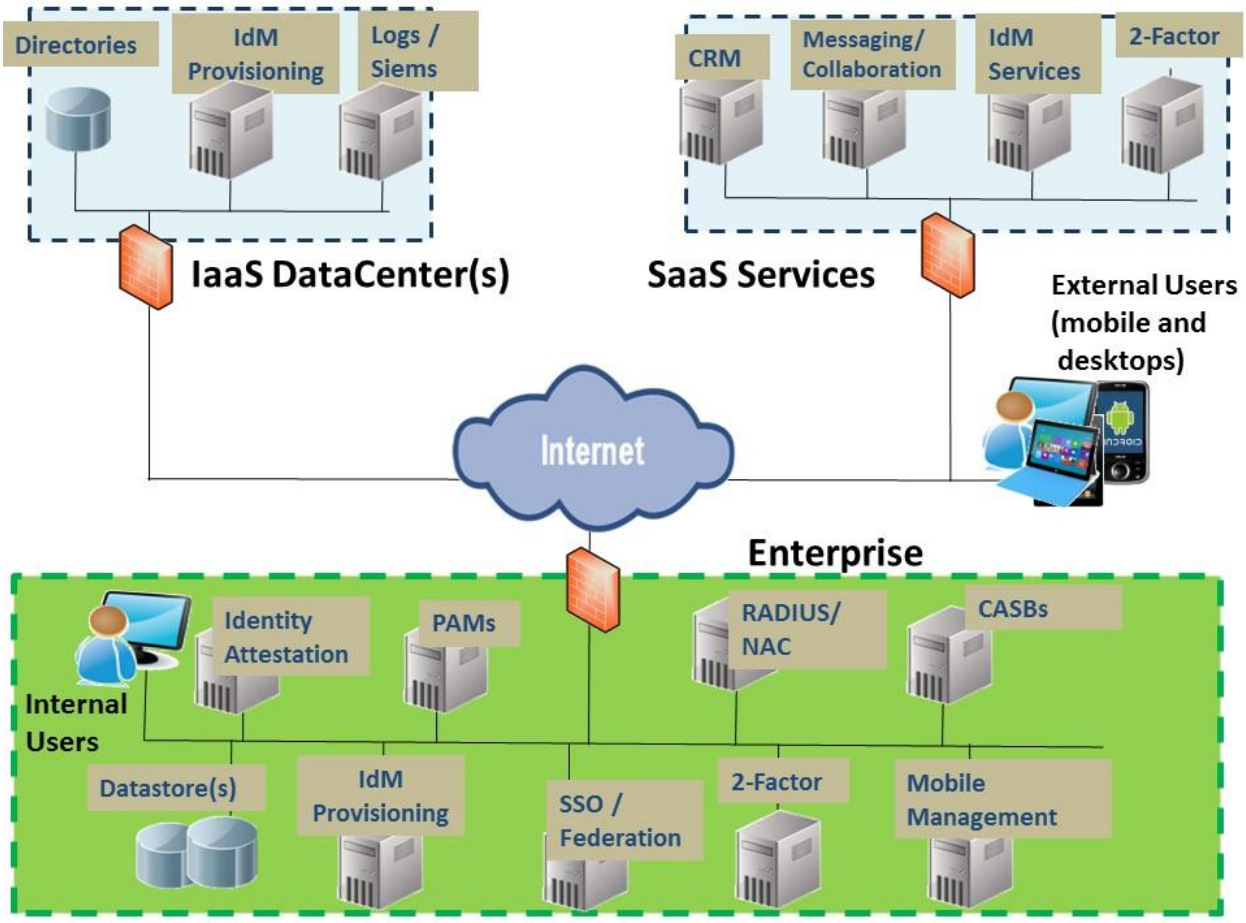

Image #1: The current IdM environment must encompass IaaS (Infrastructure as a Service), SaaS (Software as a service) and Enterprise components.

The key to these products are taking their “silo’d” abilities and insuring they are harmoniously working together to insure that privileges, access and control is managed across all resources.

Breakdown of Each IdM Component

1. Directory/Datastore

The key objective of this IdM component in the modern age is to create an "identity store of record", e.g. the primary source of the identity. This datastore can thus serve as the identity source for all the other components - be the identity sync'd, federated and/or authenticated.

Some key points to this datastore.

- Primary information stored in the datastore:
  - ID
  - First Name, Name
  - User ID
  - Employee ID
  - Associated Groups or Attributes for Groups

What's important to remember on this component is that this IS your PII, "Personal Identification Information" for your users. Thus this information falls under many regulatory compliance measures that pertain to the storage, dissemination and usage of this information. In addition, if you are doing business with foreign entities, especially Europe - you come under Safe Harbor regulations that regulate where European PII can be held and how it can be used.

There are key points for the secure IdM enterprise on the datastore. These include:

- Need to insure that the servers housing the datastore are secured
- The hardware, firmware, OS and application level must be kept updated and secured
- The network access should be quantified and limited

That's just the starters, the real challenge, comes with the PII (user data) itself. Concerns include:

- Store "least amount" of data needed
  - Audit should be conducted to insure that "extra" data is NOT being stored
- Audit what personnel /services have access
  - "Least privilege" model should be maintained
- Audit what services have access to data
  - What services have access
  - What is the access?
  - Is transmission authenticated/encrypted

2. Identity Provisioning System

How/Why/When and by Who are the current identities in the system. This is what your identity provisioning system should be capable of handling and answering.

What is needed is a quantifiable and auditable system that provides trusted identities for all your roles: employees, contractors, partners, managers and customers. This systems should also have workflow which includes approval and audit processes. Especially around users with financial abilities.

Most internal fraud involves roles not being validated and checked. E.G. users with purchasing power should not also have approving authority. What system is in check to validate these roles.

The modern tools around this include not only user/role provisioning - but also include attestation. Which can run auto checks and balances on the roles and authorities on you current systems - as well as on the new users inputted to your systems.

It's important to note that the practices of good administration need to be extended to the cloud resources. The provisioning/attestation tools must be able to reach into, no only your enterprise resources but your servers in your IAAS deployments and your SaaS applications.

Solution with this level of cloud/enterprise provisioning and account attestation includ Sailpoint, Oracle, NetIQ and EmpowerID.

For thorough inspection and assurance that the SaaS services are being used correctly by users the new CASB (Cloud Access Security Brokers) are best designed for this task. These solutions utilize federation to proxy the traffic to the cloud vendors and thus can monitor traffic to the key cloud services. Leaders in this space are Netskope, CipherCloud, Elastica and Blue Coat

3. Identity Syncing System

Though this appears to be the same as the IdM provisioning system - it's not that easy. Many identity creation systems are excellent at workflow, provisioning and initial rule manager.

But they do not provide 2 or multi-way identity syncing to insure modified and deleted accounts are sync'd across systems.

The cloud systems are key in this system. Often tools via SAML-provisioning or other mechanism are allowed to create accounts. But no verification is done when account privileges are modified on the enterprise account and/or if the account is deleted on one of the other cloud based resources.

The cloud tools themselves often have their own provisioning/syncing services - and may or may not be tied to an enterprise data system.

A thorough inventory should be conducted on all cloud resources to validate that both role modifications and updates are kept in sync with enterprise resources. The key decision for the enterprise here has to be whether a full blown identity syncing tool is needed or if a set of reliable tools customized for the enterprise would make sense. Organizations with that are centered about SaaS solutions and have primary data store in Azure or Google, may be well served by a set of on-premise identity syncing services to connect these datastores.

Key products in this space include: Oracle OIM, CA Identity Minder and the libraries from ForgeRock OpenIdM and Ping Federate.

4. Federation and SSO

The key to a successful cloud/hybrid environment is a secure and scalable federation and SSO environment. If there is NO federation system - an enterprise is forced to do unnecessary provisioning and syncing of authentication credentials - which greatly increases an enterprise's exposure to hacking.

The whole point of federation is to conduct a SSO for the user - without having to copy/sync the user's authentication credentials. Many of the key cloud attacks are done for this reason - because enterprises keep credentials in weak SAAS or IAAS services and thus the attackers are able to retrieve valuable PII information from these resources. (Which then get sold on the open market and/or re-used against the relevant enterprises.)

The remedy to this situation is a cryptographically strong federation/SSO system. The federation system should always, as first attempt to do the strongest form of SSO, be it a digitally-signed SAML or some other form of crypto token, like a WS-* assertion. Posting of credentials should be the last resort - and if it is being executed it should be validated to be a tested vendor's product or from a cryptographically sound consultancy service like OSC. (OSC has 10+ patents in X.509 technology.)

Weakly encrypted credential post are easily hacked and used against the enterprise.

The SSO system should support:

- SAML 2.0 IdP and SP-initiated transactions
- WS-* if Microsoft product utilized
- OAUTH 2.0 for mobile integrations
- Desktop SSO for enterprise users
- 2-Factor
- Step-up Authentication
- Varying authorization/authentication across resources

There are exception and mature SSO/Federation system in production from Okta, Ping, Microsoft, Centrify and other. Ping and Microsoft have both on-premise (Ping Federate and ADF2, respectively) and cloud solutions (Ping One and Azure ACS). Pure play cloud vendors include Okta, Centrify and OneLogin. Oracle AM is big player in large organizations and is a leading on-premise solution for enterprises - especially when tied in with their identity management solution: OIM. ForgeRock OpenAM is a strong SSO system based on Sun's

OpenSSO product. Like Ping Federate, Forgerock OpenAM is on premise and has an extremely robust set of connectors.

As stated, this is a very developed field and the solutions exist for for virtually any SSO scenario - it's just a matter of quantifying the issue and having an SSO expert map a solution.

One of the changes in this area, is now the inclusion of Privileged Access Management (PAM) solutions. These solutions control access to servers in the enterprise - Linux, Windows and Network based. These are the admin accounts. The PAM solutions must be strongly integrated in the role creation solutions. Key vendors in this space include Centrify, CA Technologies, Lieberman and CyberArk.

This is also an area begging for more 2-Factor. In a study in late 2015 by ISMG, only 42% of respondents are utilizing 2-factor for these accounts. This is an area that needs to be address. Hackers with access to these accounts and servers - have access to the key data and resources of the enterprise.

5. Multi-Factor Authentication

Another mandatory of a secure cloud/hybrid IdM enterprise is a robust multi-factor system of solutions. In the modern enterprise - one form of authentication does NOT fit everyone.

Authentication should be strengthened according to the value of the asset, the vulnerability of location and the trust of the user. Of course, this means strong, at-least 2-factor authentication for all valued resources.

And… if the resources do not have an effective SSO system - across resources, you will certainly have a user revolt.

An enterprise should see SSO and 2-Factor as the flip-sides of the same coin. Users will not fight a strong authentication system if the initial multi-factor authentication leads to a full set of resources that user is authorized to utilize.

Key point to an authentication system include:

- Need to create a system of authentication that:
  - Meets Regulatory standards
    - PCI-DSS, NCUA/FFIEC, HIPAA/HITECH, CJIS
  - Meets requirements of:
    - Applications
    - Devices
    - Locality
    - Users

- ONE SIZE DOES NOT FIT ALL
  - Should have ability to adjust authentication to:
    - Value of Assets
    - Value of UserID
    - Vulnerability of Resource

The technology players in this space are assorted, with Duo and RSA having the most user-friendly and accepted technologies. Other technologies are acceptable, included the integrated 2-factor services provided by the clouds - as long as they are just a part of the authentication equation.

6. Need to Ensure Mobility Security/Usage

The above components, provisioning, syncing, attestation and cloud security are all amplified in complexity with the proliferation of mobile devices. One of the key points that an enterprise needs to first do, is a policy self-assessment.

Does the enterprise wish to have a full “ownership” model of the mobile devices - and thus absorb both the cost and the responsibility of the mobile devices. This model allows the enterprise to utilize strong yet intrusive technologies for application and user deployment. This model is supported by the traditional MDM vendors, AirWatch and MobileIron being the most robust.

This model has been replaced in all but the most restricted environments to a more open BYOD policy. In this model - the phone is owned by the user, and the user is just allowed access via corporate-approved application and services. Though traditional MDMs have made a lot of movement and have solid progress in the area - the single-sign-on vendors like Okta, Centrify and OneLogin have a strong application approach - with 2-factor upfront and integrated SSO.

The space of application SSO for mobile apps, is nascent - with technologies/methodologies in the “shake-out” phase.

For the enterprise, the decision has to be decided what comfort level they have for mobile access to data. Requiring all users to log in via a restricted VPN for access is often both financially and for usability, impractical.

Applications, that quantify data access, with strong authentication and enforced authorization are often the better solution. A discussion on what data is needed, by who and what can be left on a device needs to be determined before any solution can be decided.

Summary:

The IdM space is complex for the modern hybrid cloud/enterprise environment. The experts at OSC Technologies can lead your organization to a path of securable, scalability and deployment.

Modern identity management (IdM) is not just cloud, enterprise and mobile resources. It's also the regulations and risk involved with the identity. Enterprises in various industries come into regulations concerning how enterprises create identities, provide authorization and approve of these new accounts. These processes must be quantified for many key industries including: Health Care, Law Enforcement, Retail and Government. There are specific mandates on these enterprises that can only be met via tools and implemented procedure on identity services.

OSC Technologies is unique capable of handling these IdM challenges..

Not is the team trained on key 3rd party solutions like Oracle OAM/OIM, CA SiteMinder and others - the team has actually been involved in many of the coding of the key IdM solutions in play in the market today. The OSC team has 12 patents in SSO/IdM solutions and has innovative ideas on how to solve the challenges of enterprise who struggle with enterprise, cloud and mobile deployments.