Whitepaper

Mastering Identity and Access Management

Author: Richard Diver | Cloud Security Architect – Insight Security Team

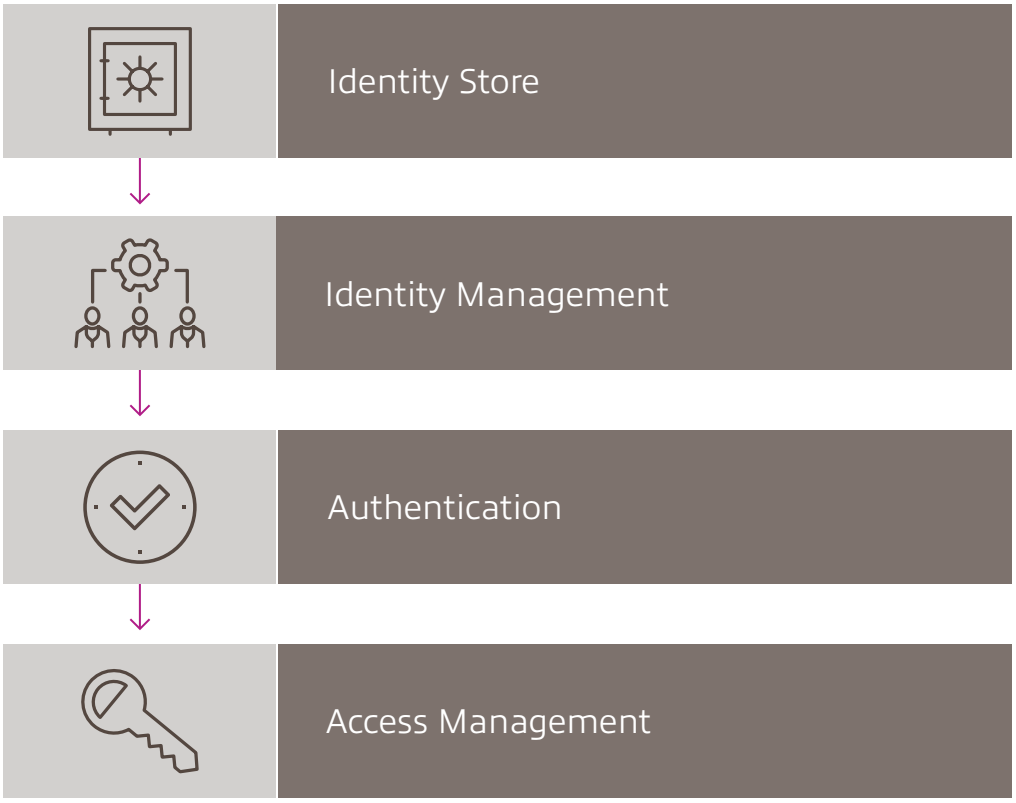
Contents

Introduction

Identity and Access Management (IAM) is a fundamental requirement of any IT system and becomes one of the most important security components for securing cloud-based services.

Depending on the size of an organization, the creation and ongoing management of identities can become very dynamic in nature and complex to manage using manual efforts.

Developing a mature IAM service requires the implementation of several components, which will likely involve the integration of solutions from multiple providers. In this whitepaper, we define and explore the following critical components:



In order to understand the complexities of the service and set a baseline reference, we first need to define the **types of users** and the **types of identities** that will be created and managed using the IAM service.

Click on the boxes above to navigate to each section.

Types of users

Across any organization there will be a variety of business roles that have different demands from the IT service due to the way they interact with different systems, handle data, travel, and use their identity to authorize transactions on behalf of the business, partners, and their customers.

The following list can be used as a starting point for mapping out your own user types and business roles:

Internal

Highly trusted people with delegated access

- Executives, managers, and knowledge workers that rely on IT systems for the majority of their work
- IT systems administrators, security, and compliance personnel implementing and maintaining the IT systems
- Frontline workforce interacting with technology as part of their work; may not have dedicated devices

External

Trusted business partners and guest user access

- Consultants, contractors, 3rd party business services adding value to the company but are not employees
- Temporary and guest user access to company IT systems during visits such as meetings
- Likely to use their own equipment and identities

Customer

Customers that require access to your services

- Consumers of systems and information published externally
- May be provided at no cost or paying a subscription for premium services

Types of identities

The following list provides a high-level separation of identities to enable simple reference. Within each of these identity types there are further sub-type identities that will be defined later in the whitepaper.

Local identities:

These accounts are specific to the individual systems, such as Windows®, Mac®, and Linux® operating systems; any device that comes with a default set of credentials, as well as any applications that are not integrated with network or cloud identity services.

These are the hardest to manage and typically at high risk of compromise due to default configurations, lack of centralized management, and weak encryption methods. They are also harder for users to interact with as they need to remember multiple credentials to sign in to each system individually.

Network identities:

The most prevalent solution for network identities is Microsoft® Active Directory® (AD). Many network systems can utilize this service to register their services and trust identities that are represented.

This service is now 20 years old and has reached a level of maturity that is demanded by the largest and most complex IT systems running on private networks. Extension service can be added to allow for federation with external/cloud services; however, there is little extra functionality being added to improve this service other than stability and security.

Cloud identities:

With the popular adoption of cloud-based productivity services, most organizations now maintain one or more solutions that utilize cloud identities. For organizations using Microsoft Office 365®, their cloud identities are in Azure® Active Directory (Azure AD), a natural extension of AD.

For organizations using Google G Suite, their identities are based on Google Cloud Identity service. Cloud identities can be used on their own, or they can be synchronized with the AD credentials to provide Single Sign-On (SSO) capabilities, which is easier for the user than having to remember multiple identities and security codes.

IAM concepts

There are several concepts that come up in every IAM design, each with their own approach and merit. As you review your own IAM requirements, and define your future architecture, consider how each of these approaches may be implemented to provide a layered approach to securing your organization's most sensitive information and system access:

Least privilege	This guidance ensures individuals only have the level of access they require to carry out the specific duties needed; permissions should be reviewed regularly.
Role-based access control	If you can define "roles," you can assign controls and permissions to your identities based on those roles instead of each one having individual policies and other settings.
Just-in-time provisioning	Building upon the previous items above, when a role is assigned the rights to privileged access, this access is granted on demand and revoked automatically instead of being available at all times.
Defense in depth	An approach that is not only geared toward identity, but to securing your IT assets. This should include people, process, and every layer of the technology stack.
Zero trust	The ultimate approach to security is to verify access requests at every stage of the journey, increasing the controls based on the user behavior and sensitivity of the system/data being accessed.
Passwordless authentication	This is the removal of passwords from the authentication service. Due to the inherent vulnerabilities of passwords, and the cost to manage them, invest in alternatives such as certificates and biometrics.

IAM system overview

With an overview of the components involved and the approaches we can take, let's now look at putting all this together to start mapping out the systems required to create a strong IAM solution.

The following diagram starts mapping how someone can gain access to an IT system; this basic flow can be developed into a more comprehensive mapping of all user types, identities, authentications, and authorization mechanisms.

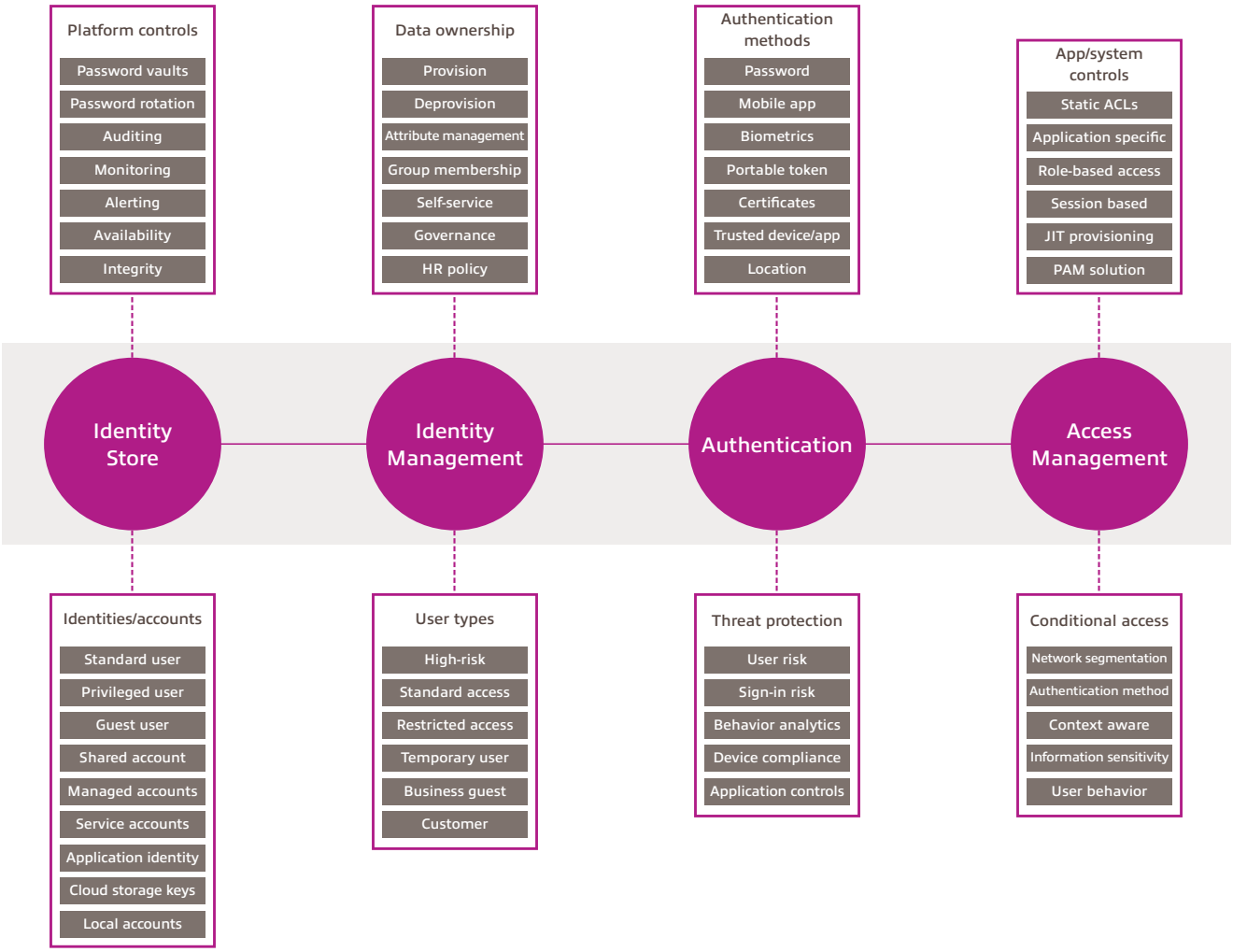
User type	What is the level of trust and the intent of this person? Where are they, and what device type are they using?
Identity type	What type of identity is being used to gain authorized access to the system, and who controls it?
Methods of authentication	What have they presented to ensure legitimate access – must include more than a user ID and password.
Authorization	Based on the information provided, and the sensitivity of the information, does the user have authorization to proceed?
System access granted	Conditional access is granted. Continue to monitor user behavior for suspicious activity.

On the next page, we will expand this out to show the four key pillars of an IAM solution, and how each one has multiple components that need to be considered when implementing new IAM systems.

IAM system options

This diagram starts the exploration of options required to fully implement an IAM system; each area will be explored in more detail throughout this document. The complete solution is likely to be made up of multiple services integrated to create the end-to-end system.

You can use this as a map to understand which product you are using to manage each area, where there may be gaps, and where there is overlap in solution capabilities.



The rest of this document should be read in sequential order; however, you can jump to the chapter that most interests you. The following sections are aligned to the previous diagram:

Identity Store | Identity Management | Authentication | Access Management

Section 1: Identity Store

The Identity Store covers the ability to create and manage identities of any type, to be used in any application, in any location. As you read this section, consider how many different "stores" you have in your environment, and how well secured, integrated, and manageable they are.

Definition and discovery

The identity store is a service that enables the organization to create unique identities in order to provide authentication and authorization services. It should be integrated with other solutions, using industry standard protocols such as LDAP, SAML, WS-Fed, OAuth, and OpenID Connect.

Ideally, all identities should be maintained in a single repository to ensure each person only needs to maintain one user ID and use that to gain access to all resources; this is known as Single Sign-On (SSO). However, many organizations have more than one identity store, due to multiple reasons:

- One for internal accounts that all employees use, another for external accounts such as partners, and another for customer-facing websites and mobile applications
- One for Windows-based devices (AD), one for Unix-based devices (LDAP), perhaps another for industrial control systems or building controls (e.g., security badge entry doors)
- Each new system may also provide its own identity store. This is common for larger platforms such as ERP, SAP, AWS, Google, Salesforce, and many more.

The first step in discovery is to list all locations and which users have identities in these stores. Then look at how many could be consolidated to utilize a single identity store.

Core capabilities

Successful authentication and authorization are critical to operations of any IT solution; therefore, every component of the IAM solution is critical to the success of your business. The following list should be reviewed for each of the identity stores and taken into consideration when investing in new solutions that will add to or replace these components:

Availability: The solution needs to be available to the user at all times, from all locations. In the modern world of hypermobility, your users will need to authenticate 24/7, globally. Look for any single points of failure and mitigate for potential failure. Any solution that needs to run on a server, on your local network, has the potential to cause a serious outage.

Resiliency: The identity system needs to remain online under any circumstance. It may come under attack and will need to be able to identify requests from valid users trying to authenticate, from malicious attempts that can cause a denial of service. Modern solutions have these protections built in and will only block access to malicious attempts.

Integrity: Every modification to the identity store must be well governed, tracked, and reversible if necessary. Modifications can enable an attacker to gain unauthorized access to resources.

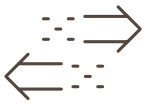
Automation: The identity store needs to enable automated synchronization between other IAM solutions, as well as self-service capabilities to allow business users to interact and update the system, within certain boundaries. *(For more information, see Section 2: Identity Lifecycle Management.)*

Integration and automation

One key aspect of managing an IAM solution is to understand where the authoritative source of information is generated from and how changes to the information are governed to prevent accidental or malicious modification.

If you have multiple identity stores across your systems, you will need a way of integrating them to enable a user to move from one system to another, without having to enter a different user ID. This is usually achieved by one of the following methods, using standard protocols for interoperability:

Replication:
A copy of the source information is used to create or update records in the secondary systems.



Federation:
Usually implemented for external solutions, federation allows one system to talk to another system and confirm that the source authority can authenticate and authorize access.

With these solutions in place, we also want to ensure automation is enabled between the systems to prevent the need for manual creation and updates of the identities. For example, if the HR database contains the authoritative source of information for all employees in the company, this data should be automatically populated in the identity store for the creation of new accounts.

Any updates made within the HR database should flow to the identity store to ensure consistency of information. These changes may have an impact on the authentication and authorization mechanisms, especially if the employee changes their role within the company, or they leave the company and need to be denied access to the systems immediately. If these processes are maintained manually, there is potential risk of mistakes and a time lag between notification of change and implementation in the system.

Cloud identity

Digital transformation and cloud adoption are currently the main drivers for many organizations to review and improve their IAM strategy and architecture. Organizations that have relied on AD for the last twenty years will be looking to extend this platform to the cloud, to integrate with the thousands of applications that may potentially be used by employees and other user groups.

While some IAM solutions will claim to provide "cloud identity," they just provide another identity store to manage, running on your servers or in their data centers. A true cloud identity platform should follow the Software as a Service (SaaS) cloud model:

Price per person, with ability to scale up and down

Globally distributed services for speed of access and load distribution

Cloud-scale security features, such as threat intel and protection against Distributed Denial of Service (DDos) attacks

The cloud identity platform should be the first point of contact for all user, application, and device access to your organization's data. By centralizing the authentication, you will strengthen your security posture, gain better visibility, and apply controls in a timely and consistent manner.

You should also consider the implementation of a Cloud Access Security Broker (CASB) solution to provide visibility of the cloud apps in use and enhanced controls for the identity platform, including reverse-proxy and in-session controls.

Section summary

The image below shows some of the key components of the identity store, which were discussed in this section. You can use this as a guide when gathering information about each of your identity stores. As well as understanding the types of users that are stored there, and how well the technology is meeting your current needs, consider how secure the solution is at storing and transmitting sensitive information, such as passwords and Personally Identifiable Information (PII).

Just take a look at https://haveibeenpwned.com/ for examples of data breaches where entire identity stores were compromised and leaked to the internet. If you have a weak solution in place, prioritize the security and replacement urgently.

Note: You can also register your organization's domains and your private email addresses with this service, to be notified if/when your credentials are found in a data breach. Thank you to Troy Hunt for this free service!

In the next section, we will explore the identity lifecycle management capabilities you will need to efficiently manage the complexities of onboarding, updating, and removing identities from the identity stores.

Section 2: Identity Management

The Identity Management section covers the lifecycle of the identities created in one or many identity stores. Consider how you currently manage the creation, update, and deletion of your identities, where there may be duplication, and how well you can secure the most sensitive and highly privileged identities across your organization.

Provision and deprovision

In the previous section, we covered the various identity stores that may be used across your IAM solution. In this section, we look at how accounts are created and managed within those identity stores. Managing identities can be expensive if all the work is done manually by IT administrators. Automation is the key to increasing efficiency and user satisfaction.

One of the first considerations will be the creation of new accounts:

- For internal user accounts, all creation and modification should be triggered by a change in the HR database. If the IT team is still manually creating user accounts, you may want to review your options.
- For any other user type, a self-service request process should be implemented, allowing for the automated workflow from request to authorization and on to creation.

Once the identity is active and in use, the next consideration is how to maintain the identities. This should be achieved by continuous integration with the source authority (such as the HR database), and by allowing users to update their own accounts through a self-service portal. Any manual intervention becomes prone to the risk of mistakes that may lead to unintended consequences.

Finally, we need to consider when and how identities are deactivated and eventually removed from the system. This may be due to an employee leaving the company or the end of a contract with a partner. Each scenario needs to be planned out, and ensure all access methods relying on the identity are updated to reflect this change, which may need to be done urgently.

Attribute management

Each account is comprised of several attributes that provide information to assist with the identification and authorization of the account. While each system will provide a complex range of attributes, the following high-level groupings summarizes how they are used:

Owner: These may include a user's name, job role, account type, work location, and other unique identifiers to help assess who they are and why they may need access to systems and sensitive data.

Authentication: Attributes that securely store information regarding authentication, such as passwords and biometric data, are used to ensure the authentication process provides a high degree of certainty that the login is from a genuine user, and not compromised through credential theft.

Authorization: The standard method of authorization is based on group membership, which defines the specific access granted to one or more systems, ideally developed around role-based access controls and the system of least privileged access *(group membership is covered in more detail on the next page)*.

Self-service options should be made available for many attributes, such as their authentication tokens and passwords; however, some should remain under strict control, such as the group member details used for authorized access to systems and sensitive data.

Group membership

As discussed on the previous page, group membership is one of the key methods for granting access to resources. A good group structure requires a strong naming standard to assist with the identification of the purpose and appropriate audience, and highly governed attribute management to ensure the account information accurately reflects the current state of the owner – both of these can be hard to manage without a solution that provides automation.

Group nesting is a term used when one group is added to another group. For example, you may choose to create a group called "*Department A*" to ensure all users can be assigned permissions that are appropriate for that team. Then you create another group called "*Department B*" for similar purposes. Both departments are located in the New York office so you create another group called "*Location-NYC*" which is used to grant access to resources in that office. Department A and Department B are added to Location-NYC as nested groups; now you can choose to assign permissions based on the group scope.

While this is a convenient way to manage complex relationships and minimize the number of groups a user needs to be added to (and ongoing updates), it quickly becomes unmanageable when deployed at large scale (usually anything more than a few hundred groups).

Instead, group membership should be defined by rule-based policy engines, known as **dynamic groups**. The rules are configured to look at other attributes of the user account and either add or remove the user from the group if they meet that criteria. Group nesting may still be used but is not necessary or recommended.

Privileged access management

One of the most critical aspects of identity management is the security of those identities that have high-privileged access within certain systems. These types of accounts are typically used by IT administrators and developers. However, this may also cover specific duties, such as the ability to modify financial records or authorize large financial transactions.

There are two methods to consider when implementing this approach:

1. **Use a separate account:**
   This method has been the predominant recommendation for many years and adopted by organizations due to the simplicity of separating roles/duties. Additional controls can be applied to these accounts, such as limiting the devices and locations where they can be used, as well as increasing the complexity of the password and enforcing token-based authentication (TBA) methods. The main risk with this approach is that the account usually retains the sensitive access permanently; if left unchecked it could lead to malicious usage.

2. **Just-in-time access:**
   This method is enabled by dynamically managing the permissions granted to a user account. Self-service options are available to ensure an authorized user can gain access to elevate their privileges when required, with automated deprovision mechanisms upon completion of the task or based on a time limit (hours or days).

You may choose to combine these methods to gain multiple layers of security, but do consider the additional complexities and costs of managing multiple accounts.

Section summary

The image below shows some of the key components of the identity management lifecycle considerations, as discussed in this section. You can use this as a guide when assessing your policies and procedures for managing identities across your organization.

Governing the creation and maintenance of your identities is paramount to keeping your system secure and functional. If standards are not enforced, then accounts can become compromised and used for malicious intent.

Reduce the burden and risk potential of manually managing identities; instead, go for automation, system integration, and delegation of control to enable the business to manage and maintain their own accounts, groups, and authorizations (within defined boundaries, of course).

In the next section, we will explore the authentication methods available to secure the identities, ensuring only authorized individuals can gain access to the sensitive data and privileges associated with that account.

Section 3: Authentication

Improving the strength of authentication mechanisms is one of the primary drivers for improving an identity and access management strategy, architecture, and individual solutions. As we move away from the age-old world of "passwords" as an authentication mechanism, consider how you can start to embrace a solution that is not only more secure, but also more user-friendly for the people who have to use it every day to be productive.

Authentication policies

We start this section by reviewing what types of authentication are acceptable, based on the sensitivity of the data being accessed, or the level of privileges and criticality of the system accessed.

Today, the systems at most risk are those that rely on a simple combination of a user ID and a password – no matter how complex that password is. In the next few years, we hope to see the end of passwords, at least for the majority of business users in their day-to-day activities. To achieve this goal, we need to invest in alternative, more secure and convenient authentication mechanisms, such as:

Biometrics, unique identifiers securely stored for authentication purposes

Token-based authentication, such as a code on a mobile app or USB key

Device-based authentication, such as a digital certificate or management profile

The location of the authentication request, such as an IP address or GPS coordinate

Multi-Factor Authentication (MFA) is the combination of these "claims" to ensure a high degree of certainty that the authentication request is made from a legitimate user and not from compromised credentials.

For each of these methods, there needs to be defined standards and policy governing how the user can register the authentication types, how they reset them, and what happens when they are lost, or fail to work. Contacting the help desk for support should be a last resort as it is very difficult for many organizations to confidently authenticate the request and provide the reset options without risk of compromise through social engineering or other malicious activities.

Passwords

Let's start with the most obvious method of authentication: passwords have been around for a very long time and continue to be the basis of authentication on almost every IT system today – but that is all about to change. Passwords can no longer be trusted as a reliable method of authentication and need to be reinforced by at least one other method, which is known as Multi-Factor Authentication (MFA) – *more details on the next page*.

Identity is the number one access method for malicious actors (internal or external), as long as passwords still exist; it is imperative we make more effort to secure them using newer standards for password management policies, complexity rules, and threat detection technologies.

Every local account password must be changed regularly and made unique from all other passwords. This will prevent the compromise of one device leading to the spread and compromise of multiple systems.

Modern guidance advises against forcing a user to change his/her password regularly. Instead, we need to ensure the password is complex enough to prevent easy cracking, while remaining easy enough for the user to remember. When a password is created, modern IAM systems will check against a database of other passwords that are known to be compromised and available on the dark web and prevent that password from being used *(no matter how complex it might be)*.

Alternatively, you may utilize a password manager solution to enable passwords to be set to 64 characters and extremely complex. The user is never expected to type this password into any system; instead, the password manager securely stores it and automatically enters it when prompted.

Alternative authentication methods

As discussed previously, there are several options available to replace or complement the use of a password to authenticate a valid access request. Review each of these options for suitability in your organization and consider implementing at least two of the four options as soon as possible:

1. **Biometrics:** This is one of the most successful mechanisms developed to ensure an increase in security and an improvement in user experience. Facial recognition is now available in most modern mobile devices and laptops, and fingerprint technology can be easily deployed to most devices.

2. **Compliant devices:** Another simple authentication factor is the trust of the device. When a device is enrolled in a device management solution, policies can enforce the deployment of secure configuration rules and enforce software updates to prevent compromise. An authentication request from a trusted device adds to the confidence level that it is a genuine request.

3. **MFA tokens:** When a user cannot interact with biometrics, or they are not on a compliant device, then they may choose to use a token. The simplest and widely adopted method is to install an application on their smartphone and register this specifically to their own account. If they do not have access to a smartphone, then physical tokens, such as a USB key fob, may be used instead (some combine biometrics in the key fob for advanced security options).

4. **Location awareness:** The location of the authentication request, such as an IP address or GPS coordinate, can be used to make a policy-based decision on whether to bypass other prompts for additional mechanisms or not. Blocking users outside of a geographic location is one simple action to take but prevents user roaming. Another example is to allow fewer prompts if a user is signing in from the company-owned network; however, this is only secure if the building, and the network, have been appropriately secured from unauthorized access.

Note: It is not recommended to allow other methods, such as a telephone call or an SMS message to a cell phone. These methods can be easily exploited and so provide very little protection.

Authentication risks

While no IT system is 100% secure, implementing multi-factor authentication will improve the security posture beyond almost any other solution available. Still, it is possible to thwart even the strongest solutions if you know how to socially engineer the user to give up their sign-in credentials.

Here are a few considerations about the inherent risks to authentication mechanisms, with some ideas on how you might mitigate them:

- Legacy authentication protocols still win; using strong authentication will be bypassed if the system still allows for simple and outdated protocols. Disable all legacy authentication mechanisms and enforce modern client authentication standards across all systems.
- Visiting a spoofed website or login page may lead to a user entering the password directly into the malicious site (the most common method of business email compromise!) – SSO with MFA would prevent the need to enter passwords anywhere. You should also deploy web traffic filtering and URL scanning solutions.
- Connecting to malicious networks may allow for man-in-the-middle attacks, or credential replay. Avoid using unknown networks when away from your home or company network. VPN clients can also mitigate this risk by ensuring a secure channel through the network prior to transmitting sensitive information.
- Using unsecured devices may allow a keylogger malware to track all keystrokes, revealing critical information that is transmitted even across secured channels. Ensure access to your systems and data is granted only when using approved and compliant devices that have regular health checks and software updates.

Section summary

Authentication standards are improving all the time, yet adoption of these new technologies is usually slow. Unfortunately, many organizations only realize the value of a strong authentication system after they have felt the effects of a successful compromise and breach of their systems or sensitive data.

Change management is key to ensuring adoption of new standards; however, you may be surprised to find how easy it can be to deploy these technologies when the user experience is both easier than a password, and provides multiple options to choose from – anything has to be better than a long and complex password that is difficult to remember or type correctly when needed.

We don't have to turn off passwords tomorrow, but we do need to reduce the trust given to them, and the ease with which they are compromised and successfully used to gain access to our most critical information.

In the next section, we will explore the options for access management control, which governs exactly what a user account can do after successful authentication.

Section 4: Access Management

Access management is where we really need to focus our investments in an IAM strategy; without strong governance, controls, and the latest technological solutions, everything else in the IAM strategy will be a wasted effort. Successful attacks against an organization are mostly due to successful subversion of access management controls, through one method or another. As you read this section, consider carrying out a mapping exercise of your systems and the controls in place today, with a regular review to ensure all of them adopt the recommendations laid out below.

Conditional access

In Section 3, we looked at the various methods available to ensure we improve the strength of successful authentication, and the combination of those methods to ensure MFA to make it more difficult for a malicious actor to gain unauthorized access. In this section, we take the idea to the next level and look at how we can secure access to critical resources and sensitive information, even for legitimate users, by enforcing condition-based access rules, which forms the basis of a zero trust strategy.

Conditional access is the dynamic analysis of the authentication methods, with the risk assessment of the access request:

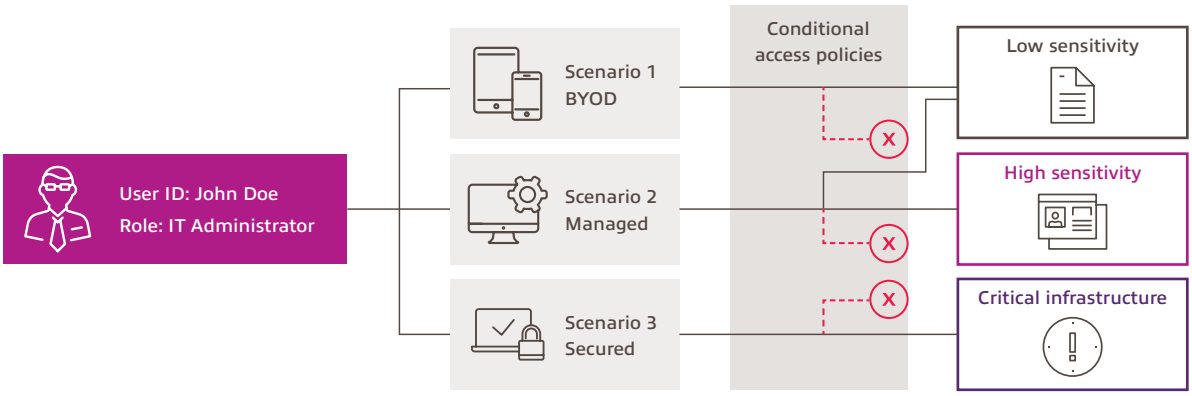
- **Device:** What is the trust level of the device being used to authenticate? Combining the compliance rules, security posture, and physical location of the device (IP/GPS-based location), we can determine if the device should be allowed to access specific types of data and other resources.
- **Application:** Approved and secured applications gain a higher level of trust than non-approved applications.
- **Data controls:** The level of sensitivity should govern where data is stored, and how it can be accessed. Preventing malicious activity on file data requires strong governance of controls, down to the object level (file-based encryption).
- **Layered controls:** Other elements of control include the ability to monitor the session activity for changes in behavior and intent, segment the network to restrict lateral movement without reauthorization, and isolate access to specific use cases.

We will look at each of these in more detail. First, let's review what access management is, and how conditional access policies can strengthen the IAM infrastructure by ensuring continual enforcement through re-evaluation.

Authorization

Access management can be defined as the governance of authorized access to restricted resources and sensitive information. While authentication controls ensure the legitimacy of the identity requesting access, authorization models define what that identity can access and any restrictions placed upon the interaction, such as enforcing read-only mode, or preventing copying and sharing of sensitive information.

The following diagrams provide a high-level overview of a basic access management policy that may be enforced to reduce the risks associated with allowing access based only on the identity of the user or by restricting actions based on the device trust level.



- The user is authorized to access all of these resources, if successful authentication is achieved.
- If using a Bring Your Own Device (BYOD), the user can gain access to basic information, but may be restricted from downloading content.
- When the user signs in to their corporate managed computer, they can now access all resources, except for administration of critical infrastructure.
- In order to gain access to critical systems, the user must log in via a highly Secured Access Workstation (SAW), which is blocked from all other activities to prevent compromise through malware.

Operating system and device controls

If we only allow access to trusted devices, the real first line of defense is to prevent unauthorized access to the device. There are multiple security controls that can be enforced on devices to ensure strong authentication:

Encryption for local storage: By encrypting the local storage on the device, we are preventing someone from hacking into the data by directly accessing the hardware components. This protection can be extended to removable storage when content is copied locally to a USB drive, etc.

Operating system login: All operating systems provide a local account for gaining access to the system; this password must be secured and unique across devices. If this credential is stolen, it can be re-used to gain unauthorized access to the device to install unwanted software and make configuration changes. The preference should be to use network or cloud accounts, instead of ensuring a user does not have local administrative rights to the device. For example:

- Local accounts on Windows® operating systems can be managed by the Local Admin Password Solution (LAPS).
- Network accounts can be added by joining the computer to an AD domain.
- Cloud accounts are now the preferred method; these can be used directly when the device is joined to Azure AD.

Configuration hardening: There are some well-known tactics for securing a range of different devices and operating systems. To ensure your devices are trusted, follow this guidance and deploy using a cloud-based device management solution to ensure all policy changes are implemented instantly, regardless of where the device is located (AD Group Policy Object (GPO) only works when the device is connected to the local network).

Refer to the CIS Benchmark resources for detailed recommendations: https://www.cisecurity.org/benchmark

Application authentication

Once the device has been accessed, the next layer of control for access management is based on the application that is used to gain access to the data. This guidance also applies for devices that are not managed by the organization, such as a BYOD model where the user provides their own devices to gain access to systems.

Applications can be divided into several categories to assist with applying a level of trust and control:

Command Line Interface (CLI), such as PowerShell®: These applications are usually restricted to use by IT administrators and developers; if they are discovered in use by general information workers, this may show signs of compromise through malware and other malicious code.

Web browser: There are many options available on almost every device. Ensure controls are in place to assess the security and control the session when applications are accessed via a web browser.

Enterprise applications: This software is managed by a formal IT organization that can ensure it meets the required standards for security and privacy. All enterprise applications should be secured using the SSO identity.

Personal applications: Used for non-business purposes, such applications may have no authentication or be used to access social media accounts. Implement restrictions to block sensitive data from being shared and stored with these applications.

Enterprise, mobile, and web application authentication should utilize the latest security standards for encrypting the session end to end (such as HTTPS) and utilize managed cloud identities. Any application that stores the credential locally, or on the backend server, is at risk of compromising those accounts. Also consider investing in a Web Application Firewall (WAF) to provide layer 7 protections against threats that are not visible to network- and host-based firewalls.

Identity-based data access

One way to secure data is to store it in a repository and control access based on individual identities or group membership. Controls usually state if the account is authorized for read-only access or edit capabilities, and if they can upload or download content to the repository. Example repositories include file shares and network storage, remote File Transfer Protocol (FTP) sites, collaboration platforms such as SharePoint®, and other cloud storage solutions that allow synchronization and replication at scale. There are inherent risks with this approach that are frequently exploited:

- If repository-based permissions are manually managed, they become stale and complex to manage. It is easy for misconfiguration, allowing for sharing with the wrong people.
- Visibility is usually limited; therefore, content may be added to a repository that is not appropriate for sharing with the audience that has access.
- Crypto malware (such as the Locky virus) is extremely effective as it only requires the user account permissions to make modifications to the content, which can impact every file and folder for which the individual has edit rights.
- If content is successfully removed from the secured repositories, it has no protection and can easily be shared via other platforms and email, without restriction.

A more secure method of storing and sharing content is to implement digital rights management, which will encrypt the content and confirm authentication and authorization on every attempt to every individual document. When authorization is revoked, the impact is immediate, regardless of where the document is stored and what type of application or device is used to gain access to it. This is also known as object-level security.

Layered security

Following the guidance of defense in depth, consider every step in the authentication and authorization process to identify where assumptions are made that access is secure. Like the weakest link in the chain, if you put all your effort into securing just a few layers, you may miss the gap that allows for failure, leading to a compromise.

The following list supplements the other layers of access management already covered:

Network segmentation: This is a critical strategy to ensure isolation between various infrastructure components, ensuring a breach in one segment does not allow for direct breach of another. Start by ensuring only specialized administrative workstations are allowed access to critical infrastructure and cloud services.

Virtual desktop infrastructure (VDI): If you need to keep your data in a contained environment, implement a VDI solution to ensure data remains within the network boundaries defined. With only the screen, keyboard, and mouse to interact with, data extraction and malicious activities are severely hampered.

Behavior analytics: By watching the activities of an identity across networks, devices, applications, and cloud platforms, it is possible to detect malicious intent and unwanted behaviors. These capabilities are built into multiple security products, such as an Endpoint Detection and Response (EDR) solution or a CASB, and may also be available as part of the Security Information and Event Management (SIEM) solution that most Security Operation Centers (SOC) have already deployed. Expand these detections to also enable automated response and remediation actions, ensuring threats are mitigated at wire speed, and not reliant on human response times alone.

All of this leads to the approach of "Conditional Access" – if the authentication request meets the defined requirements, then authorization is approved not only on the user credentials provided, but also based on the context of where the user is located, what device and application they are using, and what data or systems to which they intend to gain access. This is more advanced and secure than standard MFA approaches, which mainly aim to improve the password security layer only.

Section summary

Access management is the pinnacle of security; however, it is only made possible by strengthening the other three pillars of the IAM solution:

- Identity stores: The solution needs to minimize the number of identity stores used to manage accounts and credentials.
- Identity management: Lifecycle policies ensure attribute and group membership rules are enforced consistently and timely.
- Authentication: Multiple methods of authentication assist in proving the validity of the access attempts and allow for additional methods to be used in case one is compromised.

As you review your options to secure sensitive data and critical systems, ensure you are taking a layered approach and have the visibility to identify changes in configuration and behaviors, as well as the ability to immediately respond when threats are detected.

A strong option is to take a zero trust approach: ensure all authentication attempts are challenged and re-challenged frequently, without causing a major impact to user productivity, and all authorizations are frequently renewed and updated based on changes in activity and threat levels.

Summary

Identity breaches continue to be the number one threat to all organizations because they lead to unauthorized access that is hard to detect: if the attacker can log in as a legitimate user, they have the same level of access and can quickly escalate their malicious activities.

The following recommendations are a good starting point when reviewing your current Identity and Access Management (IAM) architecture and taking steps to secure your sensitive data and critical systems:

- When possible, **maintain all identities in a single repository** to ensure each user only needs to maintain one user ID to gain access to all resources.
- **Integrate and automate multiple identity stores** to minimize potential risk of mistakes from manual entry and data updates.
- **The cloud identity platform should be the first point of contact** for all user, application, and device access to your organization's data.
- **Consider implementing a Cloud Access Security Broker (CASB) solution** to provide visibility of the cloud apps in use and enhanced controls for the identity platform.
- Identity maintenance should be achieved utilizing **automation, system integration, and delegation of control.**
- Group membership should be defined by **rule-based policy engines** (dynamic groups).
- Ensure the security of high-privileged access accounts **via separate accounts or just-in-time access.**
- **Eliminate the use of passwords** or reinforce security strength with Multi-Factor Authentication (MFA).
- **Implement a zero trust strategy** to secure access to critical resources and sensitive information by enforcing condition-based access rules.
- **Implement digital rights management** to securely store and share content.
- **Implement a layered security approach** and ensure visibility to identify changes in configuration and behaviors, as well as the ability to immediately respond when threats are detected.

Getting help and more information

Insight Cloud + Data Center Transformation (CDCT) helps clients modernize their security programs spanning cloud (multi, hybrid, private), as well as on-premises and edge environments. From risk assessment and strategy, all the way to execution, we are a trusted partner that can help you enhance data and network security and defend against digital threats. Our Managed Network and Security Services deliver day-to-day and proactive support for your technology environment as it evolves and transforms.

To learn more about how to leverage your Identity and Access Management (IAM) architecture to protect your data and systems, contact us at: insightCDCT.com/About/Contact-Us.

You can also explore the following resources on security and identity management in the cloud:

- Video: *Identity management in the cloud with Senior Cloud Security Architect Richard Diver*
- Whitepaper: "Mastering Email Security"
- Whitepaper: "Migrate to the Cloud Securely: 10 Key Factors"

Follow us online to stay up to date and receive the latest news in data center technologies and practices:

Meaningful solutions driving business outcomes

We help our clients modernize and secure critical platforms to transform IT. We believe data is a key driver, hybrid models are accelerators, and secure networks are well integrated. Our end-to-end services empower companies to effectively leverage technology solutions to overcome challenges, support growth and innovation, reduce risk, and transform the business.

Learn more at:
insightCDCT.com | insight.com

Insight | Cloud + Data Center Transformation