Privileged Access Management

Privileged Access Management (PAM) is the management of accounts, passwords, keys, files and other secrets that provide any type of privileged access to a system within an organisation's infrastructure or across the cloud. Although the concept of management is straightforward, the organisational environment, business and security requirements rarely are.

How can PAM tools assist?

PAM tools assist organisations in providing secure access to critical assets and meet specific compliance requirements. PAM tools manage and monitor privileged accounts and access to systems.

However, a toolset alone will not provide a successful outcome to a PAM project. In addition to the technology toolset (as a core), for a PAM project to be successful, it is equally reliant upon people and processes. Years of poor technology practice cannot be changed overnight! There can be significant change management within an organisation when the PAM processes and solutions are deployed. PAM projects require continued stakeholder support and sponsorship to ensure a successful journey.

PAM is a program of works, not a project!

In our experience, successful PAM projects are a journey that the entire organisation must embrace. They should be seen as an ongoing program of works, rather than an initial project and tool (set and forget!). PAM will permeate an organisation, affecting a number of business units and quite often-external partners and technology vendors.

As the digital transformation initiatives change an organisation (cloud, new in-house workloads etc.), so to do the requirements for the PAM implementation.

The effectiveness of the processes as they relate to PAM should be revisited on an ongoing basis, to ensure that the overall program continues to deliver on the originally agreed outcomes for the business.

PAM Maturity Levels

When evaluating a privilege program, it can be considered against a PAM maturity scale:

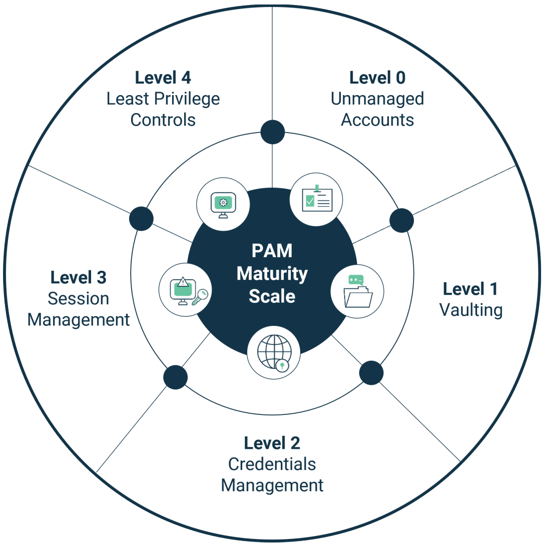
Level 0 : Unmanaged Accounts – Perhaps processes in place to store privileged account passwords within the organisation.

Level 1 : Vaulting – Replacing a Password Database such as KeePass or LastPass etc.

Level 2 : Credentials Management – Obfuscating Passwords from users and Rotating Passwords across an organisation.

Level 3 : Session Management – Provide Audit and Recording of privileged sessions for training and breach purposes.

Level 4 : Least Privilege and removal of hard coded credentials – Introduction of least privilege controls within an organisation and removing hardcoded credentials from applications and machine to machine engagements.



Identity & Access Management

Multi-factor authentication (MFA) adds a second layer of security to an identity by essentially authenticating that identity against 2 of the 3 methods:

Something you know (e.g. Password).

Something you have (e.g. Mobile device or token).

Something you are (Biometrics).

Verifying your identity using a different factor (like your phone or another device – something you have) prevents anyone but you from logging in, even if your password is compromised.

Single sign-on (SSO) integrates with MFA extremely well. Once a user is authenticated via a process of multiple authentication, a business can confidently assume the user is who they say they are and therefore can now access all of their enterprise cloud applications securely by logging into a web portal once, saving time and increasing productivity.

A Zero Trust Approach

We believe in a zero-trust approach when it comes to user authentication. This means; we verify every user every time, because we have to assume that we cannot separate the “good guys” from the “bad guys.”

Traditional approaches that focused on establishing a strong perimeter to keep the bad guys out no longer work. Resources (data, applications, infrastructure, devices) are increasingly hybrid or outside of the business perimeter entirely.

With Zero Trust, no one can be trusted until they have been verified. It is a holistic, strategic approach to security that will ensure everyone and every device granted access into a business is who and what they say they are.

The three elements to a zero-trust approach are:

1. Verifying Every User

Making sure users are who they say they are may sound easy, but when an organisation only relies on one verification method like SSO it may improve certain aspects of a security gap, but not all. SSO is best balanced with other technologies like multi-factor authentication and behavioural analytics to ensure that the user is properly verified and the interaction with their environment has a baseline. Once there is a deviation, an employee may be blocked until they are again verified.

2. Validate Every Device

Ensuring the user has a safe device within the network can get complicated, with proliferation of different operating systems, versions, corporate owned and privately owned devices. What if a user device, irrespective of what device it is, could be validated against an adaptive MFA solution? When MFA-supported passwords are combined with a level of mobile device management, the right policies are put on the device, locked in place and the context of the device (where it’s used, what browser it has, etc.) is understood, it can be considered safe. Once confirmed as a safe device an access decision can be made.

3. Limit Access

It is important to consider a least privilege stance when granting access to different user roles. The idea is to understand what is required for that user to accomplish their job tasks. One needs to ensure from day one a user is set up with the applications and accounts access needed to fulfil job roles. When a user changes roles, the access changes to fit the new job, or if they leave, those privileges are automatically revoked. It is essential that all these capabilities are integrated and work together so they can be applied in real time without adding delays.