IBM Security

Privileged Account Management

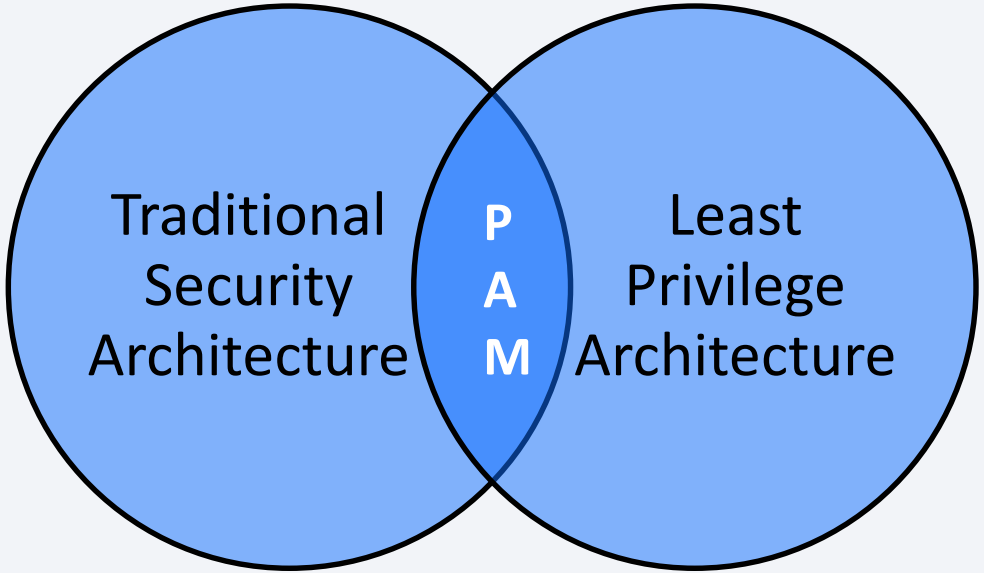
Why Least Privilege Should be The Focal Point for Your IAM Today

PATHMAKER GROUP

IBM

What is Least Privilege?

Least Privilege leans to “never trust, always verify, enforce least privilege” approach to privileged access, from inside or outside the network.



Why the Least Privilege Model?

The future of your organization's cybersecurity should be built around Privileged Access Management

Traditional network security architecture breaks different networks (or pieces of a single network) into zones, contained by one or more firewalls.

In each zone, users are granted some level of privilege, which determines the networks resources the user is permitted to reach.

The level of privilege is typically over done.

The model lends itself to vulnerabilities.

The network is always assumed to be hostile.

External and internal threats exist on the network at all times.

Network locality is not sufficient for deciding least privilege in the network.

Every device, user and network flow is authenticated and authorized.

Policies must be dynamic and calculated from as many sources of data as possible.

Least Privilege in IBM Secret Server and Privilege Manager

The principle of least privilege promotes minimal user privileges based on the user's job necessities and privilege escalation through applications not people.

HUMAN

Commonly manifest itself as policies like "only engineers are allowed access to the source code"

APPLICATION

Usually means running it under a service account, in a container or a jail, etc.

Human users should spend most of their time executing actions using nonprivileged user accounts. When elevated privileges are needed, the user needs to execute those actions under a separate account with higher privileges.

Enforce least privilege through policies for application control. Layered policies create the parameters that dictate precisely how privileges are accessed across your network. They define what actions certain people can run, and where the actions can execute.

PAM Solution in a Least Privilege Model Must Include

Trust

Attributes should be used to build trust and determine a riskiness factor around activity

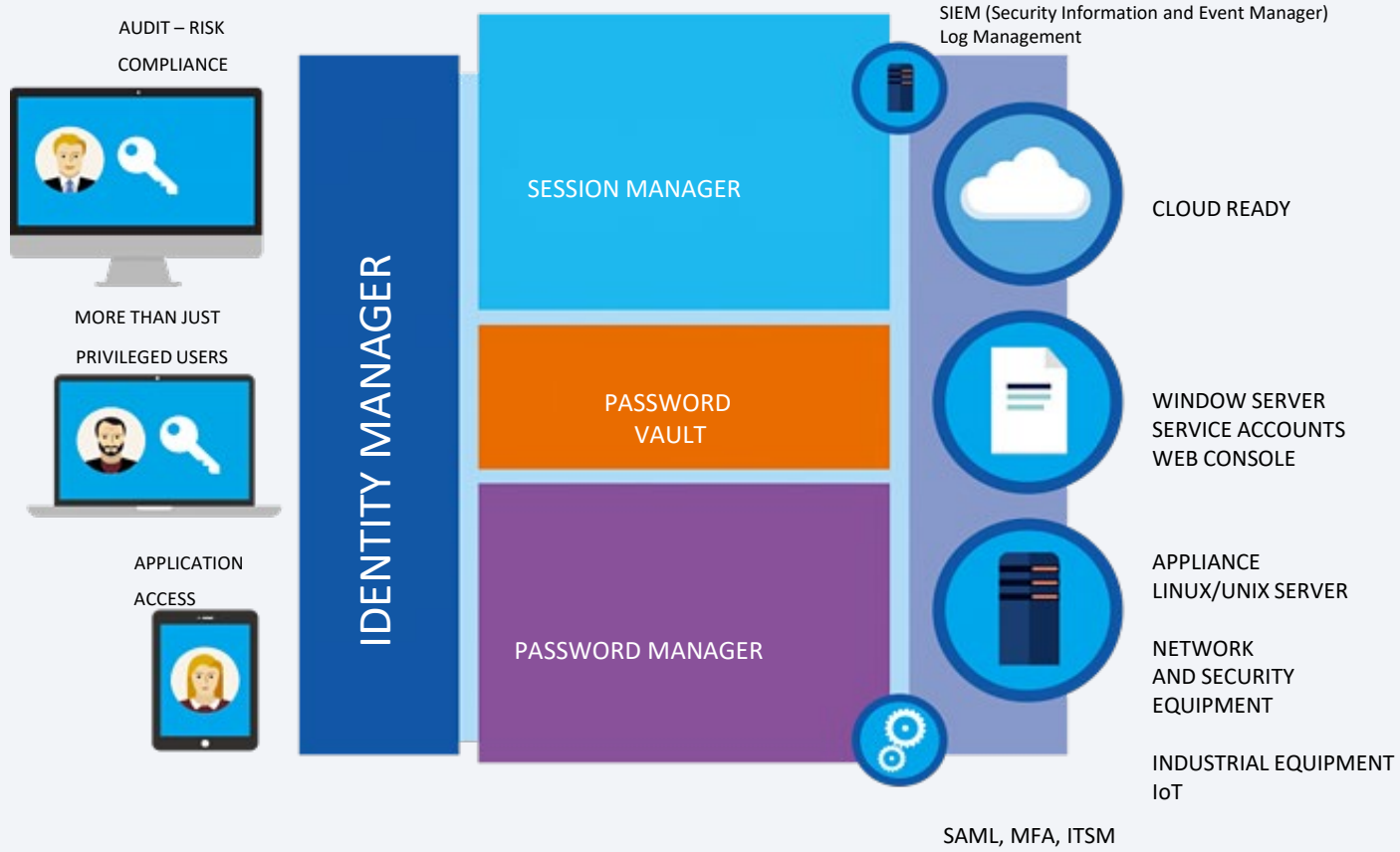
User/Application Authentication

Once authenticated, a user or application should only be granted required permissions

Device Authentication

Combing a user or application and the device being used determines the privilege level granted

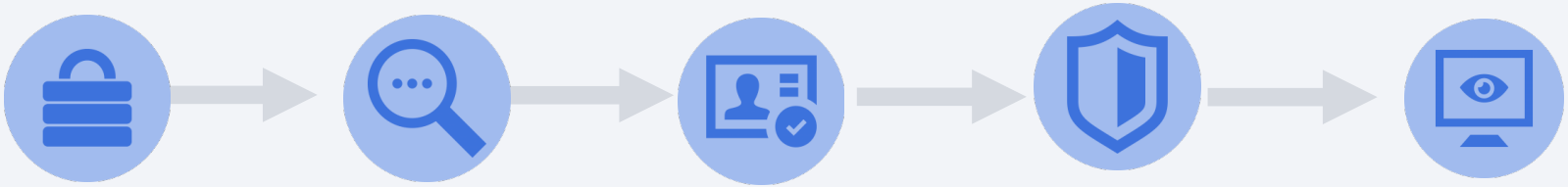
A holistic approach to Privileged Access Management



- Enforce least privileges on endpoints
- Robust integration into the security ecosystem
- Quick time-to-value through easy deployment and intuitive interface

IBM Security Secret Server

Quickly discover, control, manage, and protect privileged accounts.



ESTABLISH VAULT

Setup secure encrypted vault, permissions, users, and structure

RUN DISCOVERY

Discover all of your unknown privileged accounts

DELEGATE ACCESS

Implement RBAC, Access Requests, and other controls

PROTECT SECRETS

Store and Rotate your sensitive accounts within Secret Server

CONTROL SESSIONS

Add session launching, proxies, monitoring, and recording

IBM Security Privilege Manager

Ease the burden of implementing least privilege and managing local privileged credentials.

DEPLOY AGENT

Deploy an agent to discover users, applications & capture all processes

MANAGE ACCOUNTS

Control local credentials and permanently define privileged group membership

CREATE POLICIES

Create simple policies for whitelisting, blacklisting & greylisting

ELEVATE APPLICATIONS

Allow standard users to run apps without requiring admin credentials

REDUCE ATTACK SURFACE

Least privilege with app control keeps endpoints secure

Contact PathMaker Group for additional information on IBM Secret Server and Privileged Access Management

INFO@PATHMAKER-GROUP.COM

(817) 704-3644

PATHMAKER GROUP

WWW.PATHMAKER-GROUP.COM