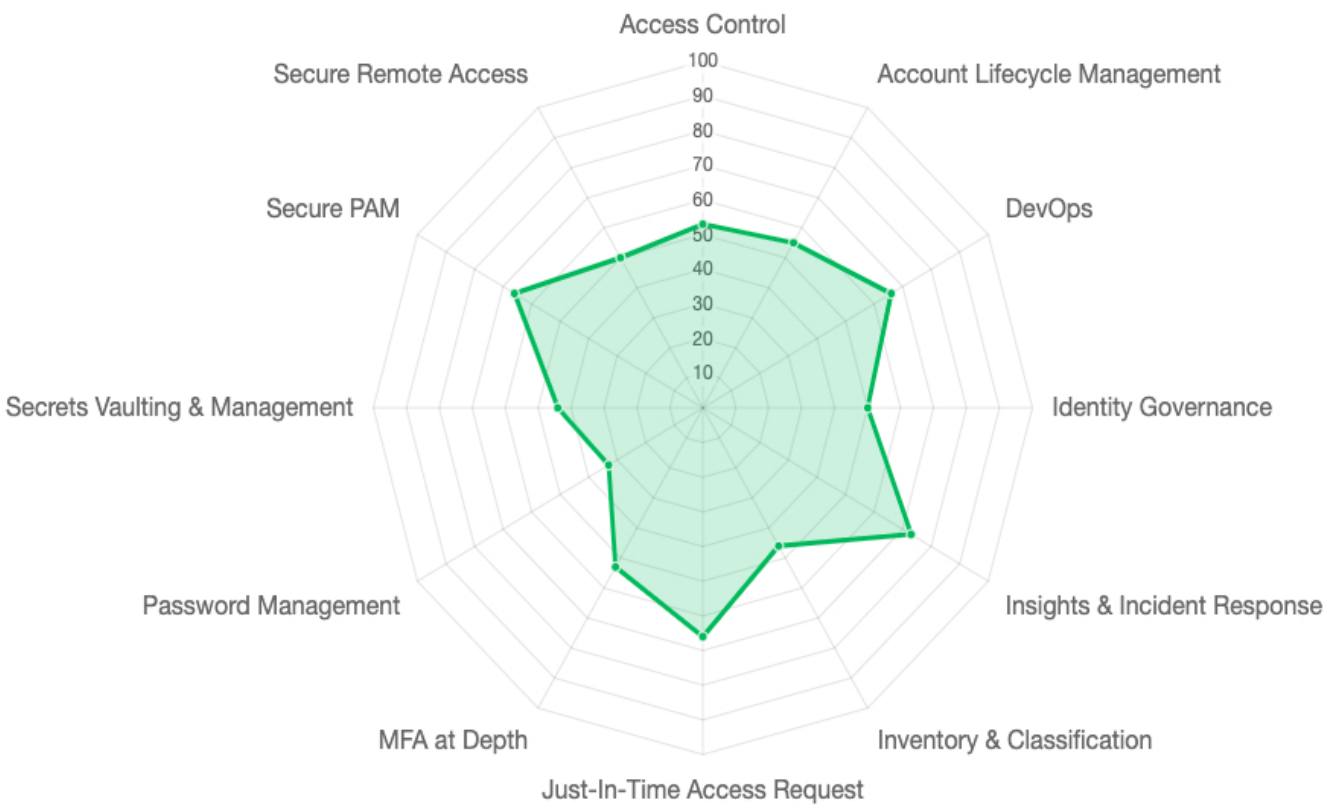
Results of Your PAM Maturity Self-Assessment

Congratulations on completing the self-assessment of your PAM maturity!
The chart below demonstrates your current level of PAM maturity for 12 categories.

Assessment Testers

Date of assessment: 03/29/2024

Category Assessment



Percent your security activities address each category of PAM
Access Control: 53%
Account Lifecycle Management: 55%
DevOps: 66%
Identity Governance: 50%
Insights & Incident Response: 73%
Inventory & Classification: 46%
Just-In-Time Access Request: 66%
MFA at Depth: 53%
Password Management: 33%
Secrets Vaulting & Management: 44%
Secure PAM: 66%
Secure Remote Access: 50%

Maturity Dimensions, Categories, and Security Objective Alignment

Each category relates to one of three dimensions of PAM maturity

- **Governance, Risk, and Compliance:** Visibility and management of privileged accounts throughout their lifecycle.
- **Privilege Administration:** Credential management and authorization controls.
- **Identity and Access Management:** Authentication for identity assurance.

You can improve your PAM maturity in each dimension and category by continuing to address the associated security objectives.

Accelerating Your Maturity Path

DIMENSION OF PAM MATURITY	CATEGORY	SECURITY OBJECTIVE
Governance, Risk, and Compliance	Account lifecycle management	Vault and manage the lifecycle of services/applications from provisioning to deprovisioning to rationalize the number of accounts and reduce the attack surface.
		Enable automatic rotation of discovered service/application account passwords. Password complexity rules can be configured. Frequent rotation and password complexity contribute to password entropy and reducing the window of opportunity for password cracking.
		Automate the credential management for service/application accounts and their dependencies. Ensure that when rotating a service/application account password, you don't break any other service dependent on the same account.
	Insights and incident response	Integrate the vault with a SIEM tool such as Splunk Cloud or Azure Sentinel for vault activity monitoring and alerting.
		For routine administrative activity, don't use shared (anonymous) accounts. Admins use their individual account for all access, ensuring that logged events tie back to a unique user. This streamlines incident response and audit activities.
		Record remote sessions initiated from the vault. Sessions can be replayed and meta data searched (e.g., typed commands) to facilitate incident investigations and audits.
		Enforce session, file, and process auditing for detailed event intel at the host operating system level. Integrate with solutions such as Splunk Cloud to forward events to a centralized SIEM.
		Leverage audit data, machine learning, behavioral analytics, and automation to detect, track, and alert on anomalous activities.
	Inventory and classification	Import Excel, or automatically discover and classify AD and Azure AD accounts and groups, local Windows and Linux privileged accounts, and local *NIX SSH Keys and vault them to ensure you have centralized management and control over their use.
		Continuous discovery to detect creation of new privileged accounts whether sanctioned, shadow IT, or by an adversary.
		Discover and classify privileged admin groups, roles, and security configuration files to ensure visibility and simplify access (including MFA) based on their sensitivity and importance.
		Automatically discover service/application accounts across Identity and Cloud Service Providers for visibility.
		Upon discovering a new/unmanaged asset, automate the process of bringing it under centralized management, deploying PAM controls, enforcing baseline PAM policies, and vaulting local privilege accounts.

Privilege Administration	Password management	Enable automatic rotation of vaulted passwords. Password complexity rules can be configured. Frequent rotation and password complexity contribute to password entropy and reducing the window of opportunity for password cracking.
	Secrets vaulting and management	Vault the most privileged accounts within the environment, those that can create other accounts, move laterally to access multiple systems, and that have full control within your trust fabric (AD and AAD). Enable access only in emergency situations.
		Focus on the most privileged groups within the environment, those membership grant permission to create other accounts, move laterally grant full control within your trust fabric (AD and AAD).
		Manage admin groups, roles, and security configuration files that might grant privileges across all assets.
	Secure PAM	Enable use of a bastion/jump host to proxy connections to servers in private networks that don't expose public IP addresses. Target servers are configured to only permit inbound sessions from the trusted jump hosts.
	Access control	Support dual authorization for privileged operations on critical or sensitive secrets and assets. For example, requiring just-in-time privileged access approval or doublelock to provide an extra layer of security for accessing secrets.
		Support just-in-time access request for elevated permissions to run privileged commands and applications on workstations and servers.
		Control application launch with local controls enforcing privilege elevation policies on Windows and Mac workstations.
		Minimize local privileged accounts on Linux and UNIX to reduce the attack surface and align with the Principle of Least Privilege and zero standing privileges.
		Prohibit privileged access by any client that is unknown, not secured, and untrusted.
	Secure remote access	For remote sessions, obtain necessary credentials from the vault without exposing to the user.
		Leverage vaulted credentials to automatically launch login sessions to targets other than servers and websites. Extend credential and session security to any target that has a suitable API such as PowerShell, PuTTY, SQL Server, and Notepad.
		Enable browser-based remote server sessions to Windows, Linux, and UNIX servers. Ideal for vendors and other remote users, this reduces the risks associated with VPN-based remote access, increases user productivity, and reduces helpdesk calls.
		Expand remote access beyond remote employees to third-party vendors and contractors. Ensure a stricter degree of security leveraging VPN-less remote access since you have less control over these users.
	DevOps	Replace plaintext, hard-coded credentials and sensitive configuration data from source code, configuration, and script files. Replace with programmatic calls to the vault to obtain secrets and credentials. This prevents adversaries from harvesting sensitive data on the disk.
	Just-in-time access request	Integrate with IT Service Management tools (such as ServiceNow) to drive access control request workflows tied to help desk tickets.

Identity and Access Management	Identity governance	Ability to establish policies around secret checkout and session launching. Self-service request workflows built-in to the PAM platform or via integrations with third party workflows such as ServiceNow, allow the user to request additional access. This helps align with best practices such as zero standing privileges.
		Enable creation of basic elevation policies to run privileged applications on workstations (Windows, Mac) and servers (Windows, Linux) to support least privilege.
		Support granular policies for privilege elevation to have tighter control over access. Enforce just-enough privilege to avoid granting excessive privileges that are not required for the task at hand.
		Integrate with Identity Governance and Administration tools (such as SailPoint) for attestation reporting and risk-based approvals.
	MFA at Depth	Enforce MFA policies for all employee logins to eliminate passwords and increase identity assurance.
		For all admin users who log in to the vault, enforce MFA to ensure the user is the legitimate owner of the credential.
		Enforce MFA when checking out a secret to ensure the user is the legitimate owner of the credential.
		Enforce MFA when initiating a remote login session to a server to ensure the user is the legitimate owner of the credential.
		Enforce MFA at workstations and servers for direct login and privileged command and application execution.

Delinea is Your Partner for PAM Maturity

The PAM Maturity Model

Dimensions, categories, and security objectives are part of the PAM Maturity Model. The model is based on security industry best practices and Delinea's work with companies ranging from organizations just beginning their PAM journey to the most experienced.

As you progress along the PAM maturity curve:

- Scope expands to include more types of privileged users, systems, and accounts.
- Controls become more granular and dynamic to govern, validate, and automate access.
- Intelligence and automation increase so your PAM system is continuously learning and adapting.
- Integrations embed PAM in your workflows so PAM becomes virtually invisible to most users.

We're here to help you build a PAM maturity roadmap that suits your organizational priorities and risk.

Learn more about PAM maturity and how organizations like yours are assessing their maturity posture »

Talk with a PAM expert to develop a personalized plan »