Delinea

Privileged Access Management Maturity Model

Delinea

Privileged Access Management Maturity Model

A framework to help organizations systematically lower privileged account risk, increase business agility, and improve operational efficiency

Introduction

Privileged access is the primary method that attackers use to gain access to sensitive systems. Protecting privileged access on each system is becoming extremely important to defend against these attacks. The Delinea Privileged Access Management (PAM) Maturity Model is a framework to help you systematically lower privileged access risk, increase business agility, and improve operational efficiency.

The model is based on security industry best practices and Delinea's work with over 10,000 customers of all types, ranging from organizations just beginning their PAM journey to the most experienced and advanced PAM users.

As a leader in the PAM market working to continually improve our customers' security posture and reduce business risks, we recognize the need to update and refine the definition of PAM maturity as the industry evolves. This latest model is multi-dimensional and provides actionable recommendations for step-by-step PAM adoption.

You can apply lessons and guidance from the PAM Maturity Model to your cybersecurity strategy regardless of the size of your company, your industry, or the number and type of systems you need to secure. It will help you navigate your PAM journey based on your own risk drivers, budget, and priorities.

Approach

The PAM Maturity Model outlines four phases:

PHASE 0: Starting Point	PHASE 1: Foundational	PHASE 2: Advanced	PHASE 3: Expert

The more mature you are…
the more your attack surface is under your control

As you progress through the phases of the maturity curve, you expand your protection to include more types of privileged users, sensitive systems, and their privileged accounts.

Most organizations have exponentially more privileged accounts and systems as employees. A by-product of cloud migration is a much larger attack surface due to an exponential increase in privileged accounts and virtual systems. Privileged accounts include domain administrator accounts, local accounts, and non-human service

accounts that run applications, databases, and other communications and data exchanges between systems.

In a mature PAM strategy, the term "privileged user" no longer equals "IT user." It also includes business users who access financial, personal, or other sensitive information from web apps and developers who build products on platforms using AWS, Azure, Google Cloud Platform, or their own cloud.

In each phase of the model, the scope of privileged users and use cases expands. Organizations in the Foundational phase are focused on the administrators using Windows

machines. Those in the Advanced phase incorporate business users, developers, and third parties using their own workstations, as well as non-Windows endpoints such as Unix/Linux. The Expert maturity level encompasses non-human accounts as well.

The more mature you are…
the more dynamic, automated, and integrated
your approach

The meaning of "privileged access" includes not only who can access what, but also what they can do with that access and when they can do it.

PAM maturity begins with static policies and controls and becomes more granular and dynamic with each phase. Native operating controls aren't sufficiently granular. As

you progress along the maturity curve, you add more granular controls and implement conditions and time limits to access. Ultimately, access controls become risk-based and adapt as your risk profile changes.

Intelligence and automation increase as well. Making the jump from manual to automatic password creation and rotation is the first shift. From there, more capabilities are automated, until, ultimately, PAM is continuously learning and adapting as an intelligent system.

Integration with other enterprise tools is a key aspect of automation. As such, as the maturity curve rises, more technologies are integrated, to the point where virtually all privileged users access PAM via another system (their ITSM or IGA tools, CI/CD tooling for DevOps, web browsers, native clients, etc.) making PAM virtually "invisible."

Dimensions of maturity

An important addition to this updated model is a multi-dimensional view of PAM maturity. Each maturity phase is characterized by an organization's approach to PAM along three dimensions, including:

- **Governance, Risk, and Compliance (GRC)** – How strong is the integrity of your system and how much visibility and oversight do you have?

- **Privilege Administration** – How do you create, define, and manage privileges across your organization?

- **Identity and Access Management** – How strong are your authorization controls and how granular are your access controls?

In the detailed description of each maturity phase below, you'll learn how to evaluate your PAM maturity according to these dimensions. It's not unusual for an organization to be more mature in one dimension than another. Once you evaluate your own maturity level, you'll be able to
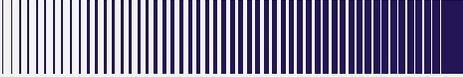
Note that the three dimensions of maturity aren't tied to specific job roles or business functions. "Governance," for example, may be shouldered by people responsible for IT infrastructure or desktop teams, not necessarily by a central GRC function alone.

prioritize security activities so that one dimension doesn't accelerate too rapidly without the support of the others.

Note that the three dimensions of maturity aren't tied to specific job roles or business functions. "Governance," for example, may be shouldered by people responsible for IT infrastructure or desktop teams, not necessarily by a central GRC function alone.

How quickly should you accelerate your maturity?

Acceleration isn't the same for everyone. Your PAM maturity should reflect your risk profile.

For some organizations, protecting access to a small number of critical systems has the greatest impact on their overall risk profile. Based on their risk tolerance, a company might implement PAM capabilities for one department, geography, or type of privileged account, and never roll them out to the full organization.

As organizations begin to scale and migrate more workloads to the cloud, however, security risk increases so PAM maturity must keep pace. For example, when organizations grow business functions, they may not decide to — or may not be able to — hire experienced IT staff, which means that the same number of people are stressed to manage a broader, more diverse range of IT operations and security. The demand for IT automation may hasten their acceleration along the maturity curve.

Similarly, rapidly growing organizations tend to work with more vendors, partners, and contractors as they expand into new markets and provide more offerings. Organizations with substantial third-party risk will need to accelerate along the maturity curve faster than others.

Commonly, organizations undergoing digital transformation will likely have more services in the cloud and will need mature privilege management of cloud-based servers, DevOps tools and service accounts.

Those bound by regulatory and compliance mandates will likely prioritize implementing least privilege policies, Multi-Factor Authentication, and session monitoring ahead of other capabilities. As they become more mature, they will need to easily customize and share reports with executives and auditors.

The four PAM maturity phases

The controls associated within each phase of maturity reflect the order Delinea recommends for organizations to roll out their PAM strategy. This step-by-step method of PAM adoption helps you build a strong foundation that supports you as you scale.

PHASE 0: Starting point

The key for organizations in Phase 0 of PAM maturity is to recognize their risk and plan for action.

Organizations in this phase secure their privileged accounts in a limited way, if at all. They typically set up privileges manually and may keep track of them via spreadsheets. As a result, they often provide excess privileges to people who don't need them, share privileges among multiple administrators, and neglect to remove privileges when users leave the organization or change roles.

They tend to have minimal complexity requirements for password creation and only single-factor authentication, which opens the door to password hacking.

Service accounts are created "in the wild," leading to poor documentation, poor mapping to applications or core services, and "re-usage," where a single account is used repeatedly for numerous services.

It's also common in Linux/UNIX environments that administrators create their own local privileged accounts since they don't have a single/unified account (like an Active Directory account) to log in across them all. This makes the attack surface very big.

Security and operations teams are typically unaware of the breadth of web applications in use and allow users to make independent decisions regarding privileged access and permissions.

These organizations have a high degree of cyber risk. If an external attacker or malicious insider has access to privileged accounts, they can steal confidential information, disrupt IT infrastructure — even shut it down — and cost millions.

Dimensions of PAM Maturity	Typical Characteristics
Governance, Risk, and Compliance	• No PAM vault. • No centralized inventory of all assets in the environment. • No easy way to report on user access permission and privileges. • No easy way to reconcile who has access to what, who did what, and who approved access. • Failed audits.
Privilege Administration	• Managing administration for Windows servers using Domain Admin Group membership. • Managing local accounts on each Unix/Linux system and editing local /etc/ sudoers files. • Users are often admins of their own workstations.
Identity and Access Management	• No centralized access controls. • Identity management is not centralized. • Admins access using local admin accounts. • Hard to tell who has access and what privileges they have.

PHASE 1: Foundational

The key for organizations in Phase 1 of PAM maturity is to gain visibility over their attack surface and begin to reduce it.

Once their eyes are opened, organizations begin to take control by vaulting shared privileged accounts. They focus first on privileged accounts managed by domain administrators and other IT users.

Although organizations at this stage are more mature, they continue to operate in a reactive mode. They often have numerous, disconnected tools and practices rather than an integrated system that is centrally managed and controlled by policies. They don't differentiate access based on roles, don't have sufficient visibility over account usage, and can't easily or automatically produce reports or compliance documentation.

Organizations in this stage must make periodic pushes to rediscover new accounts across the network. Occasionally business-critical applications experience downtime or fail

because new usages of service accounts have not been associated with the corresponding service account managed in the PAM solution. This can lead to a breakdown in business operations, negative customer experiences, and an atmosphere of mistrust between teams, making full adoption of a PAM solution difficult.

Dimensions of PAM Maturity	Typical Characteristics
Governance, Risk, and Compliance	• Establish an accurate inventory of administrative privileged accounts and passwords. • Classify credentials and secrets.
Privilege Administration	• Vault and automate periodic rotation for all administrative accounts. • Vault Active Directory and Azure privileged accounts and manage privileged account Groups. • Discover and vault local administrative accounts. • Establish a secure administrative environment for both local and remote sessions. • Establish initial privileged access workflow.
Identity and Access Management	• Enforce MFA for access to vault, including secret check out and remote session initiation. • Establish Alternative Admin accounts to prevent using public identities. • Enforce Alternative Admin and MFA for remote access.

PHASE 2: Advanced

The key for organizations in Phase 2 of PAM maturity is to expand PAM policies to reduce the number of overprivileged users. This is a combination of normalization — reducing excessive privileges — and consolidation — removing additional local privileged accounts for admins so they have only a single (AD) account for access.

Organizations in this phase include business users, developers, and vendors in addition to domain administrators in their definition of privileged users that should be managed. In addition to implementing a central vault, they expand granular PAM controls to endpoints, including servers and workstations. To address the challenges of securing web and SaaS applications, they start to manage access to these apps centrally and apply granular, role-based access control (RBAC) to user permissions.

During this phase and the next, PAM becomes a top priority within an organization's security strategy. Organizations at this level are committed to the continuous improvement of privileged security practices.

Dimensions of PAM Maturity	Typical Characteristics
Governance, Risk, and Compliance	• Discover, classify, and manage local accounts, servers, Groups, roles, and security configuration files that might grant privileges across all assets. • Implement real-time session monitoring and security access control policies for endpoints. • Enforce host-based session, file, and process auditing with integration to SIEM. • Integration with ITSM to drive access control request workflows tied to help desk tickets.
Privilege Administration	• Establish basic privilege elevation policies for all endpoints (workstations and servers). • Establish just-in-time, just-enough privileges. • Vault Linux and local administrative credentials (passwords and SSH keys). • Expand remote access control to vendors and contractors without creating AD accounts.
Identity and Access Management	• Enforce Multi-Factor Authentication at endpoints for direct log-in and privilege elevation. • Eliminate local accounts via identity consolidation for Unix and Linux. • Remove hardcoded credentials and config data from applications and scripts. • Automate privilege security in DevOps workflows and tooling.

PHASE 3: Expert

The key for organizations in Phase 3 of PAM maturity is to increase automation and intelligence, taking the concept of continuous improvement to a higher level.

As such, they fully and automatically manage the entire lifecycle of a privileged account, from provisioning to rotation to deprovisioning and reporting. At this stage, PAM systems are fully integrated for an automated defense-in-depth security strategy. PAM controls are layered to break the attack chain at multiple points. If an attacker gets past one, they will hit another. Continuous monitoring automatically identifies anomalous privileged account behavior and kicks off appropriate incident response activities.

The most mature PAM programs achieve a holistic security culture. They don't keep PAM practices within the silo of the security or IT operations team but instead integrate PAM seamlessly into other areas of IT and software development, even within a high-velocity DevOps environment. They consider every account a privileged account and have a consolidated view of all accounts, credentials, access, and user permissions, for all types of privileged accounts throughout the organization.

Service account discovery, governance, and automation

It isn't until the Expert stage of maturity that most organizations get an accurate picture of privileged service accounts and their dependencies.

Following discovery and automation activities, governance is extended to the provisioning of new service accounts

seamlessly and automatically. This can be managed centrally in Active Directory or through a PAM SaaS platform to increase efficiency and oversight. Accounts are also decommissioned automatically based on policies without causing disruption to critical services or business processes. Organizations establish workflows requiring approval prior to creation of new service accounts. Enforced certification and entitlements for service accounts ensure accountability and ownership. Failed attempts to update new credentials result in automatic rollback to previous credentials.

Dimensions of PAM Maturity	Typical Characteristics
Governance, Risk, and Compliance	• Integrate with Identity Governance and Administration (IGA) tools for attestation reporting and risk-based approvals. • Leverage audit data, machine-learning, behavioral analytics, and automation to detect, track, and alert to any threats. • Integrate with User and Entity Behavior Analytics tools (UEBA). • Discover and classify service accounts. Implement service account discovery, provisioning, and governance across identity and cloud service providers. • Harden operating systems and application components.
Privilege Administration	• Establish more granular policies for privilege elevation. • Automate onboarding of new managed assets.
Identity and Access Management	• Ensure all connections required for privileged operations must be mutually authenticated with cryptographic credentials. • Increase MFA from NIST Authenticator Assurance Level 1 (authenticating with an ID and password) to NIST Authenticator Assurance Level 2 (AAL2). AAL2 has more identity assurance due to the presence of a second factor. • Restrict privileged access to registered and company-owned endpoints. • Prohibit privileged access by any client system that isn't known, authenticated, properly secured, and trusted. • Require dual authorization for privileged operations on critical or sensitive systems.

How Delinea can help

As you progress on the maturity path, Delinea gives you the tools, resources, and expert advice you need every step of the way.

We know that PAM isn't a simple fix and the approach to PAM isn't the same for every organization. We meet you where you are in your PAM maturity and help you accelerate your progression. Our modular security solution is built to scale with you.

Our mission is to make you a self-sufficient security champion so you can own your own PAM journey.

Delinea.

Defining the boundaries of access

Delinea provides seamless security based upon the principles of zero trust, least privilege, and just-in-time privilege elevation. If you're considering a migration to the cloud or worried that your existing cloud resources aren't properly protected, talk with one of cloud experts about PAM for the cloud.

Learn more about Delinea's solutions at **delinea.com.**