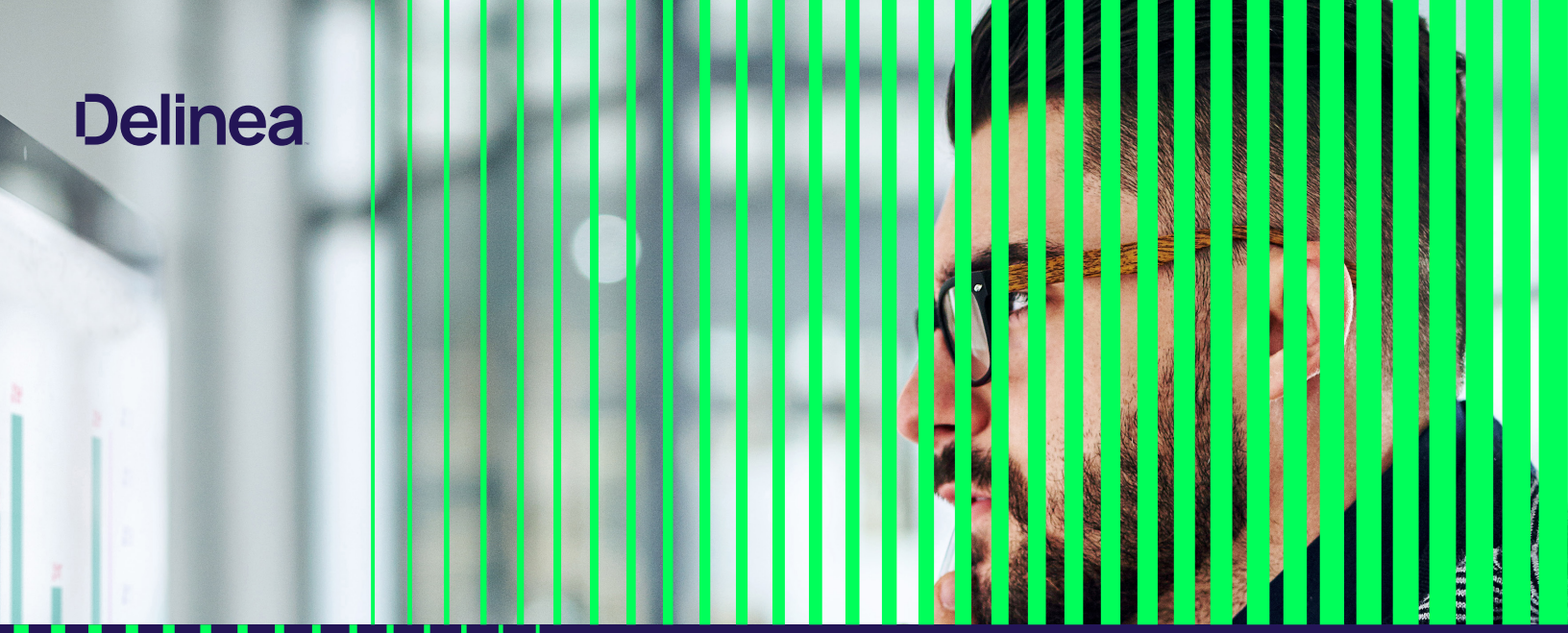
Delinea



Expert's Guide to Privileged Access Management (PAM) Success

WHITEPAPER

Introduction

80% **of breaches involve compromised credentials, making privileged access management (PAM) a security priority for organizations of all types.** Yet, cyberthreats are becoming more persistent and business and technical environments more complex and interdependent. Therefore, proactive enterprises and rapidly growing organizations are going beyond basic PAM security controls to fortify and expand their privilege protection programs.

This best practice framework is designed to help CISOs, IT operations, and cybersecurity professionals plan and execute an advanced PAM program by putting the right people, processes, and technologies in place. It reflects Delinea's experience with more than 15,000 PAM customers worldwide, including half of Fortune 500 enterprises.

Throughout the guide, PAM experts from some of the world's most security-conscious organizations share their experiences implementing advanced privilege account security controls and evolving their PAM strategies.

Becoming a PAM expert isn't simply about becoming a wiz at using software. It's also imperative to develop a coherent PAM strategy and continuous program that works for all stakeholders, including executives, security and IT teams, developers, business users, and third parties. PAM experts manage and collaborate across departments to effectively reduces risk across an entire organization. That means taking a business-first approach and enabling people to stay productive while reducing risks.

In this guide, you'll learn steps to becoming a PAM expert that help you balance the goals of securing access to privileged credentials and endpoints, enhancing productivity and minimizing costs.

CHAPTER 1
Defining "Advanced" PAM

Let's put "advanced" PAM in context of how most organizations implement privilege account security controls as they progress.

Compared with organizations just starting out with PAM, those with PAM expertise have moved from a reactive to a proactive privilege security strategy. For them, PAM is a top cybersecurity priority, with a commitment to continuous improvement of privileged security practices through an ongoing PAM program.

Advanced organizations take continuous improvement to a higher level, integrating leading technologies such as threat intelligence, trust frameworks, machine learning, and advanced automation to collect information and adapt system rules. These organizations fully automate and manage the entire lifecycle of privileged access, from provisioning to rotation to deprovisioning and reporting.

Which privileges does your PAM program address?

Privileged identities can be human or non-human. Some privileged accounts are associated with individuals such as business users, local machines, or domain and network administrators, while others are service accounts used to provide access to networks, databases, and applications, including IoT systems and DevOps toolchains.

Figure 3 below includes various types of privileged accounts, why and how they are used, as well as who uses them, and how they should be secured.

Fig 3: Privileged Access Management matrix: why, who, where, and how

Why are they needed?	Types of privileged accounts?	Who uses them?	Where are they found?	How are they used?	How are they secured?	Risks if compromised?
• Config Changes • Administrative Tasks • Create/Modify/ Delete Users • Install Software • Access Data • Backup Data • Update Patches Interactively	• Domain accounts • Local accounts • Root • Privileged Users • Emergency Accounts • System Admin • Service Accounts • Applications • Batch Jobs • Human/ Non-Human • Standard accounts access to privileged data	• IT Admins • Security Teams • Helpdesk • 3rd-party Contractors • Application owners • DBAs • Applications • O.S. • Developers • Hardware • IoT	• Servers • Endpoints • Operating systems • Virtual • Software • Cloud • Databases • Services • Programs	• Interactive logons • APIs • Services • Applications • Automation • DevOps • SSH • RDP • VPN • Browsers	• Passwords • 2FA • MFA • Keys • Access workflows • Session recordings • Launching • Behavioral analytics	• Malware • Financial fraud • Ransomware • Compliance failure • Data breach • Data poisoning • Insider threats • Service/ application downtime • Revenue/ brand loss

Delinea

CHECKLIST: Get the basics in place first

Before you tackle the more advanced phases of described in this Expert's Guide, make sure you have the basics in place.

You should be able to answer "yes" to these questions.

- [ ] Are you including privileged accounts in your broader IT cybersecurity policy?
- [ ] Are you discovering all the privileged accounts in your organization?
- [ ] Do your privileged accounts utilize automatically generated, complex passwords which are rotated on a regular basis?
- [ ] Are all your privileged credentials stored in a secure vault?
- [ ] Are all your privileged passwords protected with multiple credential verifications?
- [ ] Are security controls (such at two-factor authentication) applied to your privileged accounts?
- [ ] Do you know which compliance mandates are required for your organization?

If you're still working on the basics, the PAM Checklist can help.

CHAPTER 2
PEOPLE: Establish key stakeholder roles and responsibilities

No matter how advanced your technical skills, you can't build a successful PAM program without engaging key stakeholders. You need to align people and technology so PAM can be readily deployed and adopted across your organization.

Your comprehensive PAM program must engage multiple IT and business functions and tap specific people to take on roles and responsibilities, from executive management through system administration. Organizations—even small ones—must identify a person, department or formal team that takes ownership of the program, setting PAM policies and ensuring they are carried out. The Identity and Access Management (IAM) team is typically responsible for a PAM program, with strong ties to both security and risk personnel.

In a smaller organization, getting buy-in for PAM is usually quicker, as it's often one of many security and operations responsibilities within a single IT team. In larger organizations, PAM may be a shared responsibility across different teams: IT Security, IT Risk, Identity and Access Management, IT Operations, Development and Engineering, and so on. These teams typically report up through the CISO or CIO to executive management, who in turn report to the board of directors.

To avoid friction among these groups, PAM experts must prioritize collaboration, transparency, and joint goals across departments. Keep in mind, while cybersecurity teams may set PAM goals and strategy, they're dependent on their IT operations counterparts for help with implementation and ongoing management and reporting.

Additionally, PAM policies impact the workflow of other teams. For example, if your PAM team removes local admin rights from workstations to reduce risk, you'll need to work closely with IT support teams to keep the business running and avoid a backlash from angry users.

Figure 4 illustrates the broad range of stakeholder roles and titles across an organization, along with their responsibilities and involvement in PAM.

Fig 4: PAM key stakeholder roles and responsibilities

PAM focus and responsibility	Individual roles and titles	What they do and how you can help
Oversight	C-level Executives/ Board of Directors	Executive leadership is held responsible for cybersecurity by customers, auditors, and regulators. Their commitment to a PAM program is essential to approve appropriate resources, time, and budget. Most executives and BODs aren't cybersecurity experts and likely don't understand the requirements of PAM compared with other cyber strategies. To gain support from this key stakeholder group, PAM experts need to build awareness and understanding of the importance of protecting privileged accounts and regularly communicate the impact of their PAM program. Align reports to business priorities to show how PAM enables business innovation and reduces cyber risks.

PAM focus and responsibility	Individual roles and titles	What they do and how you can help
Accountability/ Direction	Chief Information Security Officers	CISOs serve as the "glue" that brings multiple security disciplines together, including application security, network security, incident response, and more. CISOs need to consider how PAM works within their overall security strategy and toolset. They should set high-level goals and measurements for success that are shared across teams. They must reserve appropriate resources and approve timelines. If necessary, they can resolve conflicts and eliminate roadblocks to PAM adoption. Beyond being security guardians, CISOs are increasingly seeking ways to become business enablers, ensuring security tools and policies also make processes more efficient and accelerate business goals.
Governance	Security Administrators	Security administrators handle all aspects of information security and protect the virtual resources of an organization. They're responsible for desktop, mobile, and network security. PAM may be part of a larger Identity and Access Management (IAM) and Identity Governance function, which should consider PAM in the context of Active Directory or other identity management solutions and policies. PAM specialists within this group are responsible for installing, administering, and troubleshooting PAM security solutions, including least privilege policies, application control, and privileged behavior analytics. The PAM governance responsibilities of this group include outlining, confirming, and organizing rules for secrets, permissions, and workflows. They own naming conventions, folder structure, and other foundational aspects of identity governance that keep the PAM program organized and on track.
Compliance	Auditors & Compliance Officers	Like most cybersecurity functions, PAM policies are heavily derived from compliance requirements that may include PCI, NIST, ISO, SOX, HIPAA, and EU GDPR. Because of legal implications, compliance teams should have input into PAM governance, including policy creation, logging, and reporting requirements.
Risk Management	Risk Management Officers	PAM may also fall under IT Risk Management, which is responsible for risk ranking and determines which privileged accounts and use cases represent the highest risk and must be prioritized in a PAM program.
Deployment	IT Operations/ Cloud Managers	IT operations as well as cloud managers are essential to assuring PAM deployment in the context of your organization's IT architecture and hosting policies.
Operations	IT Administrators	IT operations managers, responsible for set up and management of applications, databases, networks, and other IT resources, are key stakeholders for ongoing PAM success. These folks are tasked with day-to-day administration of PAM software. If PAM security policies negatively impact their productivity or create friction for business users, IT admins will feel the pain and may not adopt the solution. Domain administrators may be used to sharing privileged credentials or maintaining them in other ways. The shift to centralized PAM will require their buy-in and willingness to change existing processes.

PAM focus and responsibility	Individual roles and titles	What they do and how you can help
DevOps	Developers	Developers may use open source PAM tools, create their own methods to protect credentials in the development process, or use no PAM controls at all so they can maintain velocity in their aggressive release schedule. In organizations using a DevSecOps model, cybersecurity is integrated into the development process. To incorporate developers in your PAM program, especially in terms of managing privileged credentials via centralized controls, PAM experts need to embed PAM within the DevOps toolchain and match developer requirements for speed and scale.
Business Units	BU Directors	PAM experts need to understand from business units which applications, systems, and users require privileged access and which don't. Business Unit Directors help to ensure PAM adoption and understanding of policies among privileged business users. They may be called on to approve access or elevation requests or to review account activity for people on their teams. Many business units license SaaS applications, with or without permission from IT management. BU Directors must be willing to integrate those tools into an organization's PAM policies and processes.
Human Resources	HR Directors	The assistance of the Human Resources department is essential in raising employee security awareness. HR may also be involved in determining privacy and other policies that relate to employee procedures following a breach of privileged credentials.
Legal	Attorneys	Legal staff may be involved not only in shaping policies around privileged access but also in setting procedures for managing a breach of privileged credentials and the individuals involved. Legal staff reviewing contracts with third-party contractors and vendors should ensure that PAM requirements are included in all agreements. For example, third parties should agree to certain levels of permissions, approval requirements, and session monitoring before they're allowed access to sensitive systems and information. Additionally, any vendors providing software or other technology must confirm in their provider agreements that they have PAM best practices in place.
Managed Security Services	Cloud Partner's SOC Team or Consultants	Managed security service providers (MSSPs) require special attention, with security measures for SOC teams or other consultants spelled out in SLAs.
Incident Response Teams	CISO, Security Admins, Legal, HR, Corporate Communications	The incident response team will likely include many of the individual stakeholders described here. A formal IR team should be established, headed by the CISO, a plan put in place, and regular meetings held to review and discuss IR procedures and evolving threats.

Centralized PAM for a holistic, integrated strategy

As your PAM program advances, you'll bring more departments into the fold. Rather than having multiple, overlapping PAM solutions operating in departmental silos, an advanced PAM program centralizes all PAM policies and processes for comprehensive, efficient management and oversight.

Make sure people from different departments have input into the process and receive the training they need to support PAM.

"Having a product that everyone agrees on makes people a lot more productive," advises Michael Somerville, University of San Diego. Everyone should share the same policies, metrics, and goals for success."

CHAPTER 3

PROCESS: Process and scope of the PAM lifecycle

To move beyond the basics, you must plan and implement PAM in the context of an ongoing, evolving program.

The Privileged Access Management Lifecycle approach provides a framework to help PAM experts manage privileged access as a continuous process rather than a one-and-done project.

Define

The definition stage of a PAM program may be the most time-consuming and involve the most stakeholders as it sets the foundation for all that follows. You likely won't have the resources to protect every data asset, therefore you must prioritize where the most critical keys to your kingdom reside, who uses them, when and for what purpose. This isn't strictly a security or IT department exercise but must involve executives and business unit managers and data owners to fully understand what mix of privileged access is appropriate for your organization.

You may have already conducted a basic risk assessment. To be a PAM expert, however your risk assessment processes must be continuous, integrated, and automated.

Start by defining what 'privileged access' means, identify what a privileged account is for your organization and define governance policies. These decisions are different for every company so it's crucial you map out what important business functions rely on data, systems, and access. Gaining understanding of who has privileged account access and when those privileged accounts are used is essential to managing the scope and complexity of your PAM program.

Discover

Once you identify your privileged accounts, you'll need more granular insights into the security elements of privileges. For example, you'll want to discover service accounts and dependencies, AWS entitlements, shadow IT instances, as well as local users and applications.

Discovery isn't a once and done event. You need continuous discovery to reveal the extent of the attack surface and your associated risk. Ideally, discovery should be automated and reviewed on a weekly basis at a minimum.

Manage & Protect

Secure access to systems and services that reside on-premise and in the cloud, including IaaS, PaaS, and SaaS. For IT administrators and privileged account users, you must control access to workstations, servers, containers, and cloud platform consoles at a granular level.

Automated controls are the only way to practically manage and protect privileged accounts at scale.

Control privileged account access through password rotation and multi-factor authentication requirements at login and privilege elevation.

Implement proactive service account governance to prevent service account sprawl,

Implement privilege elevation and delegation management (PEDM) to prevent attackers from escalating privilege, running malicious applications, remote access tools, and commands, and moving laterally. Your approach to privilege elevation should be based on risk perspective and use case.

- For users who want to access applications via workstations, rather than giving them local admin rights which increase risk, you can elevate the process, such as application privileges, rather than the actual user. This approach to PEDM increases the number of steps an

attacker must take to access administrative rights. Least privilege policies and application control solutions enable seamless elevation of approved applications while minimizing the risk of running unauthorized applications.

- When you have greater risk, but greater trust, such as when administrative users need access to servers. You may choose to elevate the user.
- In the case of a third party administrating a firewall or application, you may instead choose to grant time-bound, non-persistent privileges that provide administrative rights to a certain application but nothing else.

Once security controls are in place, monitor how they are used to ensure they are operating as expected.

Monitor Activities

Monitor and record all privileged account activity at a fine-grained, granular level.

By increasing oversight, monitoring can enforce proper behavior. It can also help you determine if an account has been compromised. If a breach does occur, monitoring helps digital forensics identify the root causes and identify critical controls that can be improved to reduce your risk of cybersecurity threats.

Specifically, implement session recording at the vault level and/or the host level, which is useful if your vault is bypassed.

Additionally, integrate monitoring as part of session launchers which admins use to open remote connections.

For a virtual private cloud, or cloud platform like AWS, you should make sure that your IP address is the only trusted path into your network and confirm that the connection originated through the proxy.

Detect

With monitoring in place, you have the opportunity to spot privilege abuse and account compromise. However, no IT person has time to look at logs of privileged account activity, searching for a needle in a haystack.

How can you detect people who are working around your security controls? Behavioral analytics solutions help you understand indicators of compromise. They determine baselines for normal privileged activity such as including user activity, password access, similar user behavior, and time of access.

When unusual privileged account activity is detected, behavioral analytics systems can send you alerts. Then you can determine what action to take.

Respond

How you choose to respond depends on the level of compromise and level of risk.

For example, if a service account is compromised, rotating passwords may be sufficient. You may also want to investigate all activities associated with a particular account. While inside, hackers could have installed malware and even created their own backdoor privileged accounts.

However, if a domain administrator account gets compromised, rotation isn't sufficient. In that case, you should assume that your entire Active Directory is impacted and you may need to rebuild to an attacker can't easily return.

Review & Audit

AI-driven alerts and easy to consume reports help track the cause of security incidents as well as demonstrate compliance with policies and regulations. Auditing privileged accounts will also give you metrics that provide executives with vital information to make more informed business decisions.

Virtually all cybersecurity regulations worldwide call for PAM security controls such as access control, password complexity and rotation, and least privilege policies. Even organizations not beholden to industry or location-based requirements benefit from following best practice security frameworks such as NIST and CIS controls.

Some regulations are highly prescriptive while others give you broad guidelines but leave the detailed decisions up to you. As a PAM expert, your judgment is essential so that you don't approach compliance as a "check the box" exercise but a process to strengthen your security posture.

Internal audits, planned and unplanned, help teams prepare for external ones. As part of your audit process, map your PAM practices to security controls outlined in the laws that apply to your organization and make sure you know the deadlines for compliance.

CHAPTER 4
TECHNOLOGY: Implement and integrate PAM security controls

Once you've engaged the proper stakeholders and created PAM processes, you can begin to implement and refine PAM solutions that fit your specific business model and your industry. Implementing PAM successfully throughout your organization depends on choosing the right technologies to automate and control privileged access across diverse environments and ecosystems.

The following table provides actionable guidance with prescriptive technical recommendations for PAM experts. These controls help to establish PAM security across the PAM Lifecycle and build a strong foundation that can scale as your PAM program grows in maturity.

Fig 6: PAM security controls mapped to lifecycle

PAM lifecycle stage	Security technology control	How to put the control in place
Define	Policy & Governance	PAM governance includes system installation, organization, and implementation across business units and functional areas. Large or diverse organizations may choose to onboard a few business units or locations first, and then roll out PAM throughout the organization, segment by segment. You'll need to decide if you protect high impact systems first as they represent the most risk, or test PAM first on low impact systems with fewer dependencies. Your governance requirements guide how you set up privileged identities, workflow, permissions, and reporting within your PAM solution. Take the time to set policies for naming conventions, plan your permission folder structure according to departments or teams, set rules for sharing secrets, and define a chain of approvals that match the structure of your organization. Then, configure your PAM solution to match. Determine if you plan to manage and configure your PAM solution in-house or work with a PAM provider for managed or professional services. Confirm requirements for your internal IT environment and policies such as expectations for High Availability and SLAs with other departments. This information will help to define the underlying architecture you'll need for an on-premise PAM implementation or may guide your choice toward a cloud-based option. If you're installing your PAM system in-house, set up and test distributed engines, databases, firewalls, routers, failover and test sites. Identify SQL admins, AD admins, IIS admins and any other key stakeholders who will be managing your PAM solution.
Discover	Discovery & Automation	Run discovery processes to find all accounts that require privileges, including human accounts, service accounts, local admin accounts on endpoints, and applications.

PAM lifecycle stage	Security technology control	How to put the control in place
Discover (Cont'd)	Discovery & Automation	Discovery should include Windows, Mac, Unix, and VMware ESX/ESXi accounts as well as cloud platforms such as AWS and Azure. For additional discovery of legacy or custom technology, PowerShell scripts can help ensure you have visibility into all potential vectors of attack. Don't forget privileged accounts used by scheduled tasks and application pools, and all dependencies between systems. It's important to set up continuous discovery processes so information stays up to date as people come and go and systems change. Based on your discovery, you can determine how many people have Domain Admin rights currently at your organization and identify opportunities where those could be reduced or shared. For example, you can replace individual named accounts with shared accounts and remove named accounts from the DA group. Or, you can configure your PAM solution to have it temporarily belong to the DA group only when utilized.
Manage and Protect	Access Security	The core of PAM, access security, includes vaulting, delegation, and elevation of privileged credentials, in accordance with the principle of least privilege. This balances protection of privileged accounts with protection of your business-critical applications and data that resides on workstations and servers on-prem and in the cloud. Privileged account passwords, certificates, and keys are stored and managed in a secure repository – an encrypted vault – with very restrictive permissions, ideally requiring MFA to access. When users or systems "check out" secrets, PAM establishes single user accountability for a specific time period. You can automatically establish interactive administrator login sessions by injecting vaulted credentials transparently, without exposing the password to the user. An advanced PAM solution can serve as a proxy through which an administrative session is performed and automatically relay the privileged account password from its vault to the target device or application. Advanced PAM programs identify and remove embedded/hard-coded passwords and replace them with API calls that inject passwords into applications or config files. Instead of being on-disk where an attacker can discover them, they are replaced with API calls to fetch the passwords from the vault at run-time. You can rotate credentials regularly – and on demand - without impacting dependent applications. You can randomize and rotate service accounts and local accounts on controlled endpoints as well. As your program expands to more systems and departments, you can set up custom password changers for any system credentials that aren't connected out of the gate. You can also create templates that give you ultimate control over password complexity and include custom fields for impact ratings that can be used to determine access levels.

PAM lifecycle stage	Security technology control	How to put the control in place
Manage and Protect	Session Protection	Particularly important for organizations that allow third-party access to privileged accounts, advanced PAM programs include monitoring and recording privileged session activity as well as workflows that allow for multiple levels of approvals to grant or deny exceptional access to sensitive data or critical systems. Add MFA for extra identity assurance, not only on vault login, secret checkout, session establishment, but also at the server, during login and privilege elevation.
Monitor	Audit/Monitoring	Session monitoring increases oversight of privileged account use and allows for in-depth analysis of privileged session activity in real time or after the fact. With "four-eyes" capability you can tune in live to watch sessions, oversee remote connections, modify privileges, or even terminate connections.
Detect	Behavioral Analytics	Certain activities, systems, applications, cloud services, containers, etc. represent relatively low risk, while others are responsible for sensitive data or business-critical operations and thus represent higher risk. Advanced PAM programs integrate threat analytics and risk rankings from your SIEM solutions or other risk criteria to help guide decisions. In addition, behavioral analytics can track privileged account activity, recognize patterns, and identify suspicious behavior, automatically denying access or prompting the user for a second factor to prove their identity.

TREND MICRO™

TrendMicro

Continuous discovery allows TrendMicro's team to scan its network and find all service accounts and dependent services, tasks, and app pools, determine where each service account is being used (including new usage since last scan), and import all service accounts into its central PAM tool for ongoing management and auditing.

Their process eliminates manual errors managing service accounts, sets up an audit trail, and increases accountability. The team set up permissions and powerful security control features such as Request Access to monitor and approve users who are trying to access privileged accounts. They record privileged sessions users launch using service accounts and keep track of any keystrokes during those sessions.

CUSTOMER SPOTLIGHT

PAM lifecycle stage	Security technology control	How to put the control in place
Respond	Event response & Recovery	Based on the analytics you set up, you can trigger alerts or perform automatic responses. For example, when alerted of suspicious behavior, administrators may wish to rotate credentials immediately or terminate or suspend sessions. Once the event is investigated and cleared, administrators can reset to baseline. When configured for geo-redundancy and High Availability, advanced PAM systems have redundancy and failover built in.
Review & Audit	Audit/ Monitoring	Advanced PAM programs include logging privileged activities with an immutable audit log that supports saved searches, ad-hoc queries, reports, playback for visual investigation, auditing, and event forensics. In your log, ensure employees are entering a comment as to why they need access to a privileged account. This can help determine if a particular task can be delegated. Set up alerts or emails to managers, team leads, or InfoSec when Domain Admin membership group and other privileged groups change. Forward your log to a SysLog server or, if logging in AD, use Windows Event Forwarding. Automate and share reports to increase visibility and continuously improve your PAM program.

Putting PAM in context - Multi-dimensional PAM

The controls list highlights the main activities to implement over the PAM lifecycle, but it's not until you can implement those activities at scale that you're truly a PAM expert. It's important to consider how your PAM program secures privileged credentials in different states, across your entire attack surface, and in the context of different environments.

- State of your credentials, systems, and workloads.
- Scale of your attack surface.
- Context of your IT environment.

Unlike consumer password vaults that store credentials at rest, enterprise credentials move throughout the organization—in memory or in a token—and are used to authenticate and authorize privileged activity¬. To do so securely, privileged credentials should be encrypted and use multi-factor authentication (MFA).

You can also monitor credentials when they are in use, during a privileged session or an API call.

Enterprises may have thousands or hundreds of thousands of privileged accounts, including service accounts for servers, databases, applications, and network devices (Windows, Mac, Linux/Unix and proprietary). Many privileged credentials are shared among people and/or systems and can easily fall off your radar. As your PAM program expands, especially to multi-cloud platforms ,you'll discover, enroll, and manage more platforms.

Are privileged credentials in your organization used within a DevOps toolchain, to connect cloud-based systems, files within scripts, or as part of an integrated IoT environment that passes data back and forth? These environments are highly dependent and changeable. Breaking connections in these instances could result in shutting down operations and thus carries more risk. Extending PAM to these types of emerging environments is an important step in the advancement of your program.

Customizing PAM to match your organization

PAM programs typically begin with changing default or out-of-the-box passwords for common products and devices. However, every organization is different and may have custom-built or legacy systems and applications that also need to be protected. These unique applications require granular testing to identify where in-code password changes may be failing. Advanced PAM programs extend privileged protection to unique applications with custom password changers.

Similarly, PAM programs begin by tapping into basic discovery sources such as Active Directory, Unix, and VMware. Your organization, however, may need to go beyond these sources to find and manage privileged accounts from Cisco, Oracle, SQL Server, or MySQL databases. As a PAM expert, you can discover and automate the management of those credentials as well, by creating rules to pull in those accounts and turn credentials into secrets that can be generated and changed automatically.

Expert integrations improve collaboration and efficiency

IT operations, security, and development teams must form a united front to protect against cyberattack. The better coordinated these teams, the fewer gaps you leave in your attack surface and the more quickly you can respond if an incident does occur.

Just as PAM operations can't exist in a silo, neither can the tools that support them. PAM programs are most successful when PAM controls are integrated with other IT and security solutions. With tight integration, information stays up to date, reports take less time to create, and decisions can be made more quickly. Your PAM program gains more visibility throughout the organization and with executives and board members.

PAM solutions may offer out-of-the-box integration with third-party tools and provide access to APIs and scripts, which you can customize to match your own solution and workflow.

CUSTOMER SPOTLIGHT

IPC Subway

To harden thousands of servers, IPC Subway relies on its PAM solution to ensure two-factor authentication and changes passwords weekly, with alerts to ensure the changes happen correctly. To ensure availability and mitigate risk, each service on each server has a unique password.

Improve Governance Throughout the PAM Lifecycle
PAM + IAM/IGA

While PAM secures access to key system and admin accounts, Identity & Access Management (IAM) is for every user account in your organization. IAM enables the right individuals to access the right resources at the right times for the right reasons. For example, IAM allows you to provide a salesperson with access to his or her account and provides higher level access for certain individuals to log into sensitive systems, such as finance and Human Resources, that require elevated privileges.

An integrated IAM/PAM system will help track user account ownership, flag user accounts that aren't being used, automate the provisioning of new user accounts, simplify the assignment of privileged accounts, and make it possible to regularly prune access. Integration will enable you to meet compliance and regulatory reporting requirements efficiently and with minimal overhead.

Some IAM solutions, such as Identity Governance and Administration (IGA), provide monitoring and reporting capabilities that are required for a compliance program. These solutions are helpful in ensuring broad compliance with security policies and identifying outliers. They help with segregation of duties, access request handling, and recertification of access (continuous or trigger-based recertification throughout a lifecycle, rather than requiring manual periodic review). When entitlements are adjusted using an IGA solution such as SailPoint IdentityIQ, IGA workflow integrated with PAM can automatically fulfill the changes, resulting in the PAM solution provisioning new roles and deprovisioning existing roles.

CUSTOMER SPOTLIGHT

State of Indiana

The State of Indiana has developed a highly advanced PAM implementation. By integrating its PAM solution with Active Directory, the State of Indiana ensures service accounts are set up correctly, with appropriate privileges, and are managed securely from Day One.

"We've eliminated all kinds of mistakes by centralizing and automating PAM, and not having six different people creating accounts in Active Directory by hand and possibly making mistakes."

The State has expanded its use of PAM from managing service accounts to protecting applications used by third parties and software developers. According to the State's PAM expert, "We used to have shadow sessions that could take four or five hours. There were times in the middle of the night where we had to get up and share our screen with a developer so they can fix a problem in production. Now I'm able to go in and elevate applications using their user group and it just automates the process."

Save time with controlled authentication

PAM + Active Directory

Privileged user accounts are typically located in a central authentication system running in Active Directory (Windows) or in another central identity and authentication system that manages accounts, groups, and permissions for employees. Password changes can be challenging in one system; when you attempt to keep multiple systems in sync, there's a very high chance that errors will fall through the cracks.

It's important that your account management process, from creation to rotation and deprovisioning, stays coordinated every step of the way.

In addition, a PAM integration can leverage Active Directory as a central policy engine for PAM and MFA policies across Windows, Linux, and Unix systems.

An advanced integration, such as AD bridging, can also go further by extending many of Active Directory's capabilities to non-Windows platforms, such as Kerberos-based single sign-on, group policies, and smart card support for Linux login.

PAM + Connection Management

Privileged credentials used when making vault-initiated remote desktop connections, such as logging into systems and workloads directly, and elevating privileges, provide access to critical infrastructure, data, and applications. When configuring remote sessions, IT teams must navigate complex networks, cloud services, and user needs. They typically have multiple sessions active at once, using different connection protocols and a variety of privileged accounts.

Integrated connection management solutions provide a unified environment to manage and interact with multiple remote sessions for both Remote Desktop Protocol (RDP) and Secure Shell (SSH).

As a result, IT teams save time and lower risk. Admins can launch remote connections using multiple protocols, authenticate, and gain access to critical resources with appropriate permissions. Additionally, they can monitor and record multiple, simultaneous remote sessions to increase accountability and provide an audit trail to demonstrate compliance.

Improve visibility and workflow between security and IT Ops

PAM + IT Service Management

Consider the numerous service management systems your organization has in place to support workflow and IT processes. A PAM program will be implemented more quickly and completely – and will be more sustainable over time – if it shares information back and forth with the systems IT operations relies on to do their jobs.

For example, asset management systems track approved workstations and applications in use throughout the organization. As you roll out your least privilege and application control policies, connecting with these systems will improve your discovery process and help you keep your inventory up to date. You can set up a least privilege policy rapidly for new workstations by integrating with solutions IT uses for configuration and deployment of new devices. Additionally, you can integrate application control with helpdesk ticketing systems IT operations uses to address user requests for applications and support.

Application elevation requests can be managed directly in the system, so there is continuous communication and event tracking. Finally, integration with ServiceNow and other IT Operations Management (ITOM) tools avoids configuring hard-coded account passwords, allowing ITOM apps to obtain credentials programmatically, from the vault as an external credential provider.

Identify design flaws more rapidly and accurately
PAM + Vulnerability Scanning

PAM integration with vulnerability testing and management solutions provides credentials to scan systems for missing patches and make sure patches are installed correctly.

This deep credential scan allows for a more thorough vulnerability assessment than you would be able to achieve with penetration testing alone.

Automatically add known malware to application control policies
PAM + Threat Analytics

Integrating PAM solutions with threat analytics helps you keep pace with cybercriminals as they develop new malware and advanced strategies for attack.

Threat intelligence databases such as VirusTotal form deny lists you can build into your PAM solutions to block known malicious applications from running. Artificial intelligence and machine learning from solutions like Cylance help you anticipate and detect malicious activity.

CUSTOMER SPOTLIGHT

IT'S HOW WE CONNECT

Telstra

Telstra's CI/CD platform connects to its PAM tool via API to pull privileged credentials at runtime, while reducing the impact when passwords need to change. For example, Telstra stores SSL certificates as secrets in its PAM vault, setting expiry and alerts to ensure the appropriate governance.

Log events, aggregate cybersecurity data, and trigger alerts
PAM + SIEM

Many IT and security teams rely on Security Information and Event Management (SIEM) and log management solutions, such as ArcSight, Splunk, and LogLogic, for centralized reporting and coordinated incident response. As part of a risk-based approach, use these solutions to classify and score a wide range of events to prioritize business and technical risk.

CHAPTER 5
CONCLUSION AND NEXT STEPS: The ongoing PAM journey

Even the most mature PAM deployments are on a journey of continuous improvement.

As privilege is recognized as the new perimeter, everyone in the organization must become a PAM "expert" to some degree. That will require ongoing education.

Your organization will grow and evolve, which means business and technical requirements will change. For example, new development processes or cloud-first policies may generate new types of privileged accounts that need to be protected. Or, you may acquire or merge with another company and need to integrate new people and systems quickly and securely.

You can be ready for these new situations by choosing an extensible solution that can adapt to new situations and grow with you.

There is no doubt that cybercriminals will become more sophisticated and develop new strategies to achieve their goals. With the fundamentals in place, you'll be able to build from a position of strength to keep pace with changing threats, tighten your attack surface, and reduce risk for your organization.

CUSTOMER SPOTLIGHT

AMERICA FIRST CREDIT UNION

AmericaFirst

Integrating PAM with AmericaFirst's vulnerability tools provided a more accurate understanding of the organization's network's security.

For example, with unauthenticated scanning on a PC test system QualysGuard found no network vulnerabilities. After adding authenticated scanning using PAM, QualysGuard returned 33 vulnerabilities that the InfoSec team took action to address.

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.**