Richard Toropov

Securing Privileged Access: Best Practices for PAM System Implementation

Metropolia University of Applied Sciences

Bachelor of Engineering

Information and Communication Technology

Bachelor's Thesis

11 January 2025

Abstract

Author:	Richard Toropov
Title:	Securing Privileged Access: Best Practices for PAM System Implementation
Number of Pages:	34 pages
Date:	11 January 2025
Degree:	Bachelor of Engineering
Degree Programme:	Information and Communication Technology
Professional Major:	Computer Science
Supervisors:	Janne Salonen

Compromised credentials are a leading cause of modern security breaches, underscoring the urgent need for effective Privileged Access Management solutions. In many organizations, privileged accounts often outnumber standard employee accounts, sometimes by a factor of three. This imbalance significantly heightens the risk of unauthorized access to critical systems and data, making robust PAM strategies essential for safeguarding sensitive resources.
This thesis introduces a comprehensive framework for effectively implementing Privileged Access Management within a corporate environment, aimed at assisting cybersecurity professionals in the strategic planning and implementation of advanced PAM programs. By integrating the right combination of people, technologies, and processes, organizations can build a resilient PAM infrastructure that strengthens their security posture and protects against the misuse of privileged accounts.

Based in a comprehensive review of PAM theory, industry best practices, and expert insights, this thesis provides actionable guidance for effectively deploying PAM in organizational settings. Key topics include strategic planning, criteria for solution selection, integration methodologies, policy implementation, and considerations for ongoing management and optimization.
The theoretical framework of this thesis explores the fundamental principles of Privileged Access Management, emphasizing its critical role, key features, and implementation challenges within the broader scope of Identity and Access Management. By adopting the best practices outlined in this framework, organizations can take a proactive approach to managing privileged access, mitigating security risks, and strengthening overall cybersecurity resilience.

Keywords: privileged access management, implementation guide, best practices, PAM, IAM

Tiivistelmä

Tekijä:	Richard Toropov
Otsikko:	Korkeiden Käyttöoikeuksien Turvaaminen: PAM Implementoinnin Parhaat Käytännöt
Sivumäärä:	34 sivua
Aika:	11.01.2025
Tutkinto:	Insinööri (AMK)
Tutkinto-ohjelma:	Tieto- ja viestintätekniikan tutkinto-ohjelma
Ammatillinen pääaine:	Ohjelmistokehitys
Ohjaajat:	Janne Salonen

Suurin osa tämän päivän tietoturvahyökkäyksistä kohdistuu korkeisiin käyttöoikeuksiin, kasvattaen kriittistä tarvetta tehokkaille Privileged Access Management -ratkaisuille. Yrityksillä voi olla jopa kolme kertaa niin paljon korotettuja käyttöoikeuksia kuin työntekijöitä, mikä nostaa merkittävästi riskiä luvattomasta pääsystä kriittisiin resursseihin.

Tämä opinnäytetyö antaa yleisen viitekehyksen PAM:n tehokkaaseen käyttöönottoon yritysympäristössä, suunniteltuna tukemaan tietoturva-ammattilaisia PAM-ohjelmien suunnittelussa ja toteutuksessa. Tehokkaita resursseja hyödyntämällä organisaatiot voivat luoda vankan PAM-infrastruktuurin, joka parantaa tietoturvaa ja suojaa korotettuja käyttöoikeuksia väärinkäytöltä.

Hyödyntämällä katsausta PAM-teorian parhaisiin käytäntöihin ja alan näkemyksiin, tämä opinnäytetyö tarjoaa käytännön ohjeita PAM:n tehokkaaseen käyttöönottoon organisaatioissa. Avainaiheita ovat strateginen suunnittelu, valintakriteerit, integraatiostrategiat, käytäntöjen toteuttaminen ja jatkuva hallinnointi.

Tämän opinnäytetyön teoreettinen viitekehys syventyy PAM:n taustalla oleviin periaatteisiin, korostaen sen välttämättömyyttä, ominaisuuksia ja toteutusnäkökohtia laajemmassa Identity and Access Management kontekstissa.

Avainsanat: PAM, IAM, pääsynhallinta, perehdytysopas

Contents

List of Abbreviations

ACA: Advanced Configuration and Power Interface. An open standard for controlling the power consumption and configuration of computer systems.

AD: Active Directory. A directory service developed by Microsoft for managing permissions and resources on a network.

AI: Artificial Intelligence. The simulation of human intelligence in machines that are programmed to think and learn.

API: Application Programming Interface. A set of protocols and tools for building software applications that allow different systems to communicate with each other.

DBA: Database Administrator. A professional responsible for managing and maintaining databases, ensuring their availability, integrity, and security.

GDPR: General Data Protection Regulation. A regulation in EU law on data protection and privacy in the European Union and the European Economic Area.

GRC: Governance, Risk, and Compliance. A strategic approach to managing an organization’s overall governance, risk management, and regulatory compliance.

HIPAA: Health Insurance Portability and Accountability Act. A US law designed to provide privacy and security protections for health information.

IaaS: Infrastructure as a Service. A cloud computing model that provides virtualized computing resources over the internet.

ID: Identifier. A unique name or number used to identify an object, user, or system within a database or system.

IAM: Identity and Access Management. The administration of user identities and their associated access rights within an organization.

ISO 27001: International Organization for Standardization 27001. A standard for information security management systems (ISMS) to manage sensitive company information securely.

IT:	Information Technology. The use of systems (especially computers and telecommunications) for storing, retrieving, and sending information.
KPI:	Key Performance Indicator. A measurable value that demonstrates how effectively an individual, team, or organization is achieving a business objective.
MFA:	Multi-Factor Authentication. A security mechanism that requires more than one form of authentication to verify a user's identity.
ML:	Machine Learning. A subset of artificial intelligence that enables systems to learn from data and improve over time without being explicitly programmed.
NIX:	A family of operating systems that include Unix-like systems, such as Linux and macOS.
OS:	Operating System. Software that manages computer hardware and software resources and provides services for computer programs.
PaaS:	Platform as a Service. A cloud computing model that provides a platform allowing customers to develop, run, and manage applications without worrying about infrastructure.
PCI-DSS:	Payment Card Industry Data Security Standard. A set of security standards designed to ensure that companies that process, store, or transmit credit card information maintain a secure environment.
PAM:	Privileged Access Management. A set of security technologies that control and monitor access to critical systems and resources within an organization.
RDP:	Remote Desktop Protocol. A protocol developed by Microsoft that allows users to connect to another computer over a network.
RPA:	Robotic Process Automation. The use of software robots or "bots" to automate repetitive tasks typically performed by human workers.
RBAC:	Role-Based Access Control. A method of managing user access based on their roles within an organization.
ROI:	Return on Investment. A performance measure used to evaluate the efficiency of an investment, calculated as the gain from the investment divided by its cost.

SaaS: Software as a Service. A software delivery model where applications are hosted by a service provider and made available to customers over the internet.

SIEM: Security Information and Event Management. A system that collects, analyses, and responds to security data from various sources within an organization.

SSH: Secure Shell. A cryptographic network protocol used to securely access remote computers.

SSO: Single Sign-On. An authentication process that allows a user to access multiple applications with one set of login credentials.

SQL: Structured Query Language. A standardized programming language used to manage and manipulate relational databases.

SAML: Security Assertion Markup Language. An open standard for exchanging authentication and authorization data between parties, especially between an identity provider and a service provider.

SOX: Sarbanes-Oxley Act. A US law that set new or expanded requirements for all US public company boards, management, and public accounting firms.

TCO: Total Cost of Ownership. The total cost of owning a product or system, including all associated costs such as purchase price, maintenance, and operation.

UBA: User Behavior Analytics. A security process that uses machine learning to identify abnormal behavior patterns among users that could indicate malicious activities.

UAT: User Acceptance Testing. A process in software development where the end users test the software to ensure it meets their needs before it is deployed.

VPN: Virtual Private Network. A technology that allows a secure network connection over the internet, providing privacy and security.

CISO: Chief Information Security Officer. A senior-level executive responsible for managing an organization's information and data security.

KPI: Key Performance Indicator. A measurable value that demonstrates how effectively an individual, team, or organization is achieving a business objective.

AI: Artificial Intelligence. The simulation of human intelligence in machines that are programmed to think and learn.

ML: Machine Learning. A subset of artificial intelligence that enables systems to learn from data and improve over time without being explicitly programmed.

1 Introduction

1.1 Thesis Background

My exploration into the field of PAM (Privileged Access Management) started from my professional interest in cybersecurity and a recognition of the critical role that managing users' rights plays in safeguarding organizational data and assets. During my decade of work experience within the different sectors of IT (Information Technology), big part of my work has always related to actively managing users' rights and access privileges, gaining firsthand insights into the complexities and challenges associated with privileged account management.
Drawing on my professional experience and academic pursuits, I sought to leverage my expertise to develop a comprehensive guide aimed at assisting organizations in effectively protecting their privileged users.

As I delved deeper into the field, I encountered statistics revealing the significant risk posed by the misuse of privileged accounts in cybercrimes. Studies have shown that up to 76% of cybercrimes involve the exploitation and misuse of privileged credentials, highlighting the urgent need for robust PAM solutions to mitigate such risks. Also, industry recognition, such as Gartner Research's acknowledgment of IAM (Identity and Access Management) security as one of the top cybersecurity trends of 2024, emphasizes the importance of prioritizing PAM within the broader context of IAM. [21; 12]
Gartner's identification of IAM security as a top security trend highlights the evolving landscape of cybersecurity, where an identity-first approach is gaining importance. With organizations increasingly focusing on IAM to enhance cybersecurity outcomes, the importance of fundamental protection and system hardening cannot be overstated. As security leaders strengthen and leverage their identity technologies, the integration of identity threat detection and response becomes critical to ensuring IAM capabilities effectively support the broader security program.

1.2 Objective and Research Approach

The primary objective of this thesis is to address the key steps of PAM implementation within a company environment. Specifically, the research seeks to answer the question, "What are the most critical phases of PAM implementation?"

To achieve this objective, qualitative research methods are used to explore and understand the essential phases of PAM implementation comprehensively.
The research methodology involves the utilization of secondary research methods, focusing on gathering and analysing pre-existing documents related to PAM implementation. These documents encompass a diverse range of sources, including scholarly articles, industry reports, case studies, and best practice guides, providing valuable insights into the critical phases of PAM implementation.

2 Defining Privileged Access Management

2.1 Brief Overview of PAM

The origins of PAM date back to the formative years of computing, when the focus was primarily on fundamental user access management. This early stage involved establishing basic controls over user accounts, implementing password policies, and defining roles and permissions. However, as technological advancements occurred, the cybersecurity landscape faced increasingly sophisticated threats.

By the early 2000s, PAM emerged as a distinct domain within cybersecurity, specifically dedicated to managing access to privileged accounts. This evolution was prompted by a heightened awareness of the inherent risks associated with privileged access, including insider threats, credential theft, and cyber-attacks that exploit such access to compromise sensitive information or disrupt critical infrastructure. Over time, PAM has transformed into a comprehensive framework

of cybersecurity practices, integrating a variety of tools and technologies. Modern PAM encompasses solutions for managing privileged access, enforcing access control policies, implementing MFA (multi-factor authentication), and conducting privileged session monitoring. [13]

Figure 1 below defines some main elements of how PAM is used in a modern company setting.

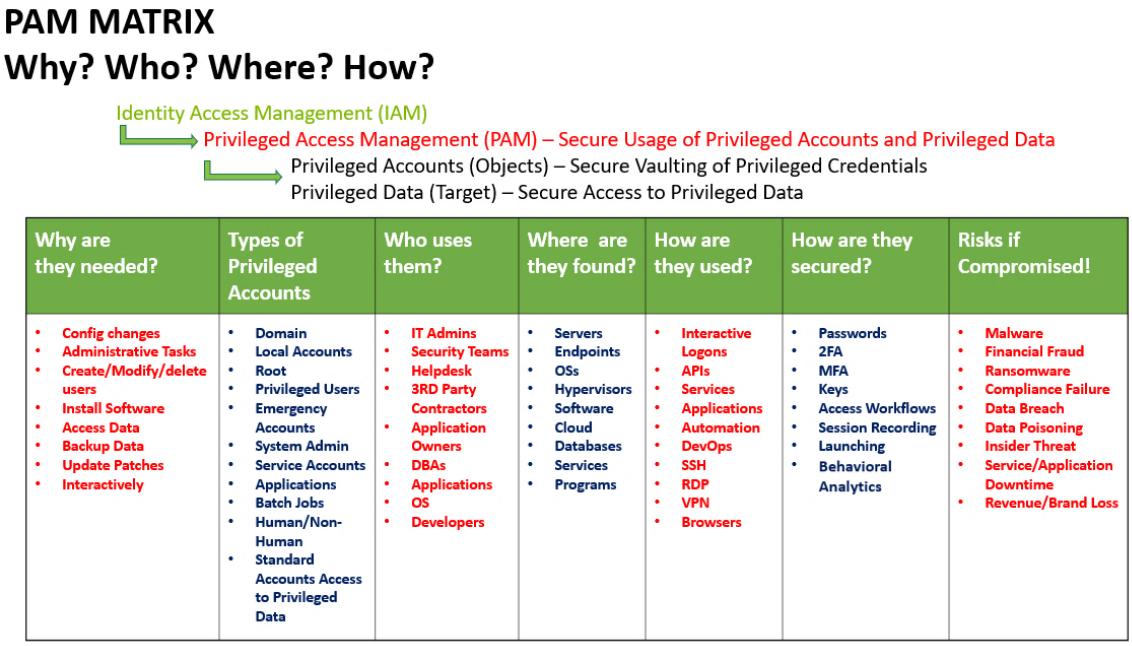

Figure 1: PAM matrix (adapted from Joseph Carson 2019.)

2.2 Privileged Accounts

Organizations can maintain up to three times as many privileged accounts as they have employees. These accounts are crucial for executing various administrative and management tasks and can be found across nearly every connected device, server, database, and application within the organization. In addition to traditional IT environments, privileged accounts extend to corporate social media accounts managed by employees. Typically, a standard user account signifies an individual's identity within a directory service such as AD (Active Directory), with each employee possessing one such account. In contrast,

a privileged account may represent either a human or non-human entity and is often shared among members of the IT team. [8]

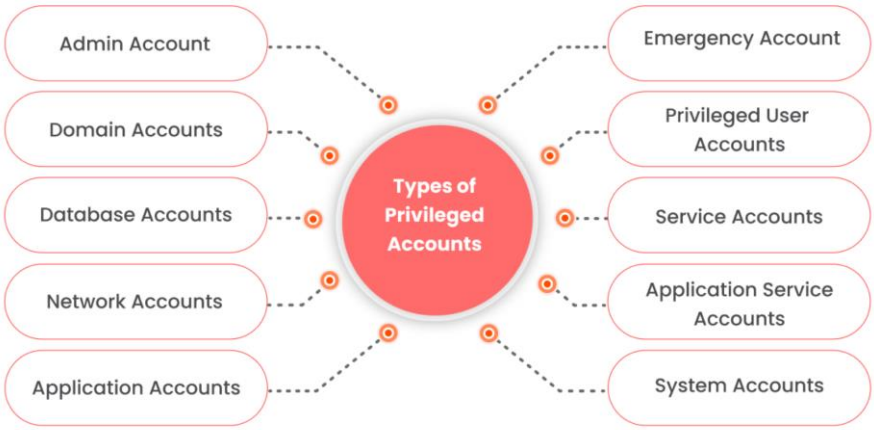

Figure 2: Types of privileged accounts (adapted from miniOrange 2024.)

Organizations utilize various types of privileged accounts, including local administrative accounts, domain administrative accounts, break glass accounts, service accounts, and application accounts. A specific category of privileged accounts includes superuser accounts, which are referred to as "Root" in Unix/Linux systems and "Administrator" in Windows environments. Local administrative accounts grant elevated access only to the local machine, while domain administrative accounts extend permissions throughout the entire domain. Break glass accounts are designated for emergency scenarios, such as disaster recovery situations. Service accounts, which can be either local or domain-based, enable applications or services to interact with the operating system. Application accounts are employed by applications to execute batch jobs, connect to databases, or access other applications. [1]

2.3 What does PAM solve?

Organizations face large challenges in managing privileged accounts, which are often poorly maintained or, in some cases, totally forgotten. These neglected accounts create substantial security vulnerabilities, as they can be exploited by malicious actors, including former employees or external hackers.

PAM addresses this issue by centralizing the management of privileged accounts, ensuring they are regularly reviewed and secured.
A common challenge is the overprovisioning of privileges. End-users are frequently granted excessive permissions, either for convenience or due to a lack of proper oversight. Over time, as roles evolve and new tasks are assigned, users may accumulate an unnecessary number of privileges, increasing the organization's attack surface. PAM enforces the principle of least privilege by restricting access to only what is necessary, reducing the risk of misuse or exploitation. [11]

Another critical problem PAM solves is the management of administrative account credentials. IT teams often share these credentials for convenience, making it difficult to attribute actions to specific users. This lack of accountability can hinder forensic investigations and compliance efforts. PAM eliminates this issue by enabling unique, time-bound access to administrative accounts, ensuring traceability and accountability.
Hardcoded credentials pose yet another significant risk. Many applications and devices ship with default credentials that are often left unchanged, or employees embed credentials directly into scripts or configuration files for ease of use. These practices create easy entry points for attackers. PAM solutions address this by automating password management, enforcing regular credential rotation, and securely storing all sensitive information in encrypted vaults. [17]

In cloud and virtualized environments, managing privileged accounts presents unique challenges. The dynamic nature of these systems allows users to create and manage virtual machines easily, often leading to an explosion of new privileged accounts. Without proper controls, this can result in unchecked access and sprawling attack surfaces. PAM provides robust tools to discover, monitor, and manage these accounts effectively, ensuring that access controls extend seamlessly across hybrid and multi-cloud environments. PAM mitigates the risks associated with excessive permissions, dormant accounts, shared credentials, hardcoded passwords, and the complexities of cloud environments. By implementing PAM, organizations can significantly enhance their security

posture, ensure compliance with regulations, and establish a culture of accountability and control. [11]

2.4 Key components of PAM

Enterprise-class PAM solutions comprise numerous components. These systems act as secure vaults for passwords, capable of discovering network accounts and importing them for centralized control. When multiple users need access to the same privileged account, passwords can be shared using a one-to-many approach. Strong encryption of stored passwords is essential, and many PAM solutions offer automatic password injection for improved user experience.

PAM solutions do more than store passwords; they manage them through automated tasks such as changing passwords for both human and machine accounts. They ensure compliance with organizational password policies, including requirements for rotation and complexity. A check-in/check-out feature can be used for password retrieval to prevent concurrent account usage. Manual password management is also available for ad-hoc needs, such as during disaster recovery. Managing privileged sessions is another key function of PAM, which includes documenting and controlling user’s access. PAM tools can automatically launch sessions and inject credentials into target systems, providing comprehensive privilege management. Critical features include monitoring, controlling, and terminating privileged access across various platforms, including Windows, macOS (Macintosh Operating System), cloud environments, virtual systems, and network devices. UBA (User Behaviour Analysis) detects threat patterns in user activities, triggering alarms or events as necessary. ACA (Advanced Control and Audit) provides tighter control over hidden commands, ensuring secure execution of applications. [9]

To integrate seamlessly into an organization's workflows, PAM solutions must support multiple system integrations. Connecting to helpdesk and ticketing systems ensures that a ticket is automatically generated when privileged access is initiated. Authentication for PAM should go beyond just a username and

password, integrating with existing SSO (Single Sign-On) and MFA systems for enhanced security. Additionally, if the organization uses SIEM (Security Information and Event Management), all auditing data from PAM should be routed there for better anomaly detection.

PAM solutions must offer detailed auditing and reporting features to meet compliance requirements and support internal audits and monitoring of privileged access risks. Reports should detail who accessed a resource, when it was accessed, and what actions were taken during the access.
Effective PAM governance is crucial, dictating how PAM is implemented in daily operations. Policies should specify who can access which resources, ensuring not all users have access to every resource. Governance also covers the assignment and revocation of privileges, ensuring proper control and oversight. [14]

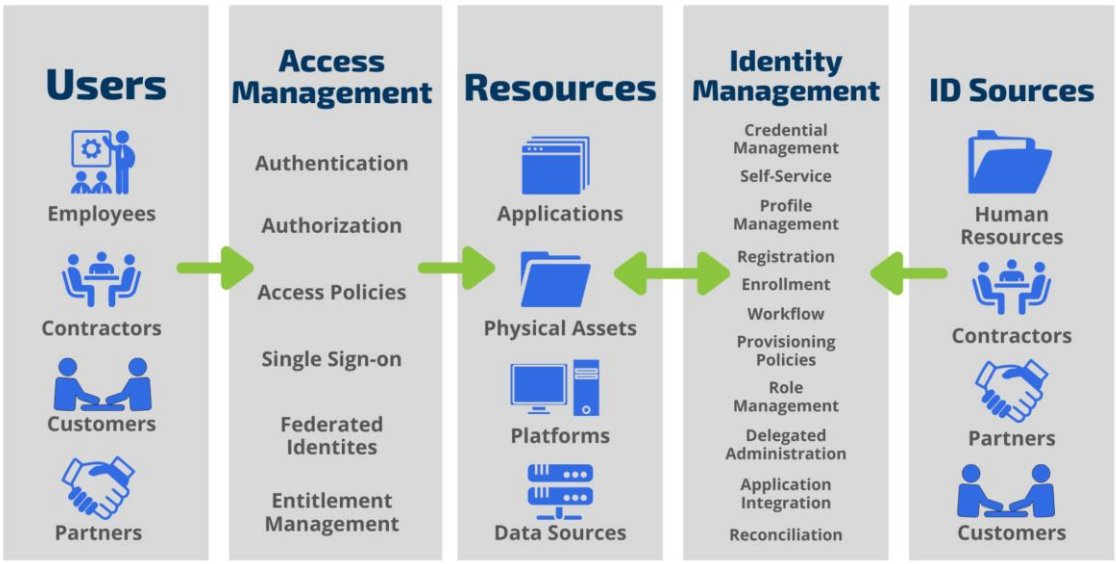

Figure 3: PAM key components (adapted from Braxton-Grant 2022.)

A well-crafted PAM strategy and effective deployment of its components ensure robust management and oversight of privileged accounts. This significantly decreases the risk of accidental or intentional privilege misuse while enhancing the ability to monitor and control access. By reducing the attack surface and

implementing comprehensive auditing, organizations achieve a tightly regulated workflow, as depicted in figure below. [20]

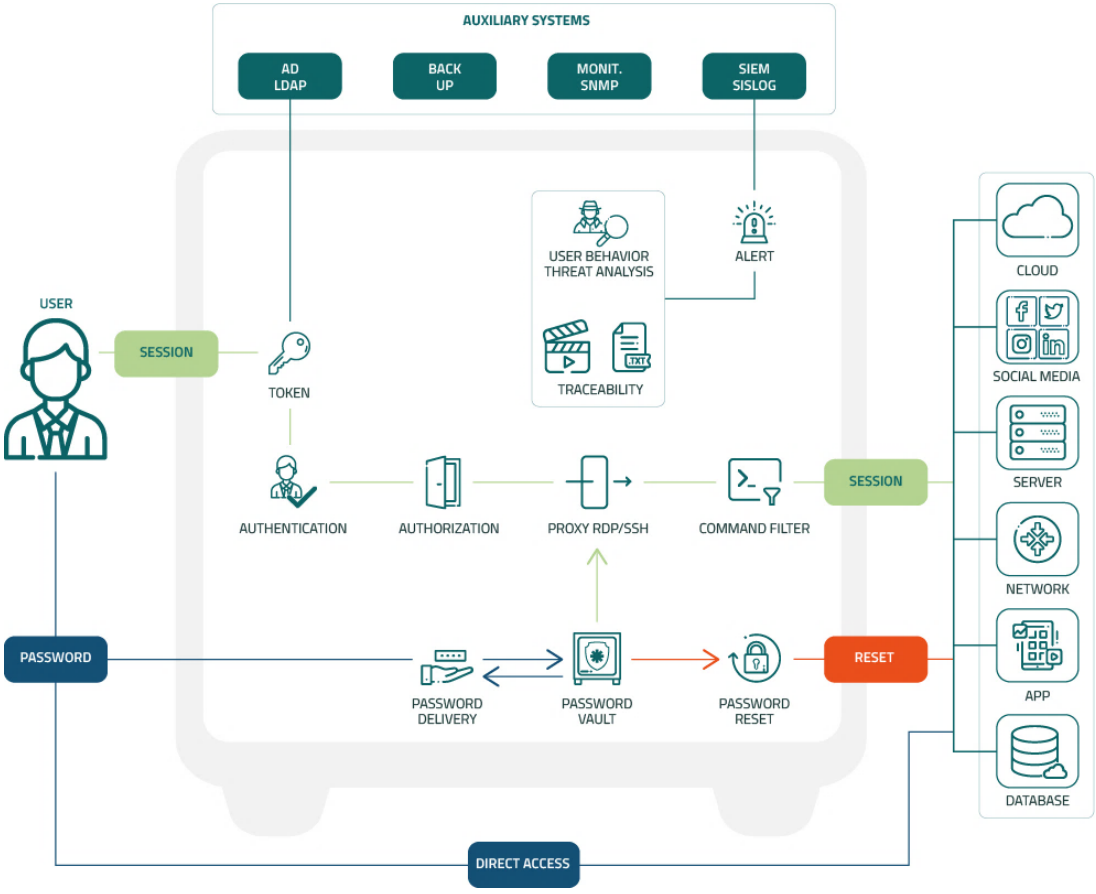

Figure 4: PAM workflow (adapted from Senhasegura 2024.)

2.5 PAM Lifecycle

Effective PAM implementation hinges on careful planning and readiness. Early attention to these aspects can prevent considerable future workload. Initially, precise identification of essential data and user groups is important. Leveraging scanning and discovery tools offered by PAM vendors facilitates investigation, potentially uncovering dormant privileged accounts. Designing and reviewing the data model alongside end-users ensures the selection of suitable PAM technology tailored to organizational needs and use cases. Clear depiction of responsibility and ownership for the PAM solution should be established early on. [15]

Migration to a PAM solution entail defining and implementing necessary policies and security controls across all target systems. Mapping organization applications and assessing PAM integration needs are critical. Modeling different processes, including third-party access and disaster recovery scenarios, is essential. While company-wide PAM implementation yields maximal benefits, prioritizing urgent cases initially is prudent. A well-planned PAM roadmap ensures comprehensive coverage, extending beyond passwords to encompass SSH keys (Secure Shell keys), DevOps (Development and Operations), scripts, and RPA (Robotic Process Automation). PAM solutions typically offers multiple interfaces to cater to diverse requirements. Integrating MFA and SIEM from the outset, along with platform hardening and scenario testing, is imperative. [10]

Post-implementation, ongoing maintenance is required. Regular internal audits ensure correct privilege assignment based on least privilege and segregation of duties principles. Monitoring PAM usage and setting up alerts for suspicious events are paramount. Utilizing both internal PAM monitoring tools and external SIEM solutions is advisable. Keeping PAM technology updated is important to align with evolving company needs. The PAM lifecycle, illustrated in figure 5, underscores the continuous nature of PAM management, emphasizing the need for comprehensive steps to adequately safeguard privileged accounts and resources. [2]

Figure 5: PAM lifecycle (adapted from Joseph Carson 2018.)

Various use-cases significantly influence the optimal implementation of PAM. Additionally, the resource location, whether in the cloud, on-premises, or in a hybrid model, plays a crucial role in determining the most suitable approach. Nevertheless, referring to table 1 below aids in measuring the maturity level of PAM implementation within an organization, while also offering insights to enhance the existing setup.

Privileged Access Management Maturity Model

	Level 0	Level 1 Ad Hoc / Manual	Level 2 Baseline	Level 3 Managed	Level 4 Advanced
Privileged User/Shared Accounts	Not managing or rotating credentials	Manual Controls For Privileged Accounts	Basic Vault Structured Controls Account Inventory SDLC Integration	Credential Vault w/ RBAC Central Password Policies Account Discovery MFA	Password-less (SAML/OAUTH/TGS) Cloud/SaaS/SDN & HSM Integration
Service & Application Accounts	No knowledge of Application accounts	Ad Hoc Application Account Management Hard Coded Passwords	Manual Application Account Management	Centralized A2A Mgmt. No Hardcoded Creds. REST API Integration	Governed A2A DevOps Integration
Monitoring & Threat Detection	No monitoring of account usage	Ad Hoc Audit & Controls Activity Monitoring	Decentralized logging	SIEM Integration Account Attribution SNMP Alerting Session Recording	Meta-Data Service Desk Workflow & Analytics Integration
Identity Management Integration	Manual provision, no certification or accreditation	Manual Process For Privileged Access	Automated Privileged Identity Mgmt.	Integrated Privileged Access Requests Basic Governance	Fully Delegated Administration Governed Privileged Access w/SoD
Fine-grained Controls/SoD	Non existent	Open Source Tools and Scripts	Decentralized Tools (Silos)	Command Filtering Restricted Shell Leap Frog Prevention	Centrally Managed Kernel Interceptor with Cred Vault Integration

Table 1: PAM maturity model (adapted from Haber & Hibbert 2018.)

3 7 Keys to implementing PAM

3.1 Define and Discover

Establishing a baseline of privileged credentials is the number one step, as you can't protect what you're unaware of. Understanding the current state of privilege within your enterprise is key to safeguarding organizational privileges. This involves taking stock of assets across your operating environment and identifying the countless privileged accounts supporting them. Privileged accounts and credentials are ubiquitous, spanning Active Directory, IaaS (Infrastructure as a Service), PaaS (Platform as a Service), SaaS (Software as a Service), SQL (Structured Query Language), and various other IT, OT (Operational Technology), and business services. Regularly scanning systems across your network and cloud providers is crucial for uncovering privileged accounts, credentials, entitlements, and misconfigurations that may pose risks.

The data gleaned from this inventory process enables risk assessment based on your PAM framework and informs target-setting and prioritization for implementation schedules. Gathering real numbers of Windows domain admin accounts or Windows Server local admins, not only shapes remediation strategies but also establishes baseline metrics for future comparisons.
Integrating your PAM solution with vulnerability management and discovery technologies from vendors like Rapid7, Forescout, and Tenable is a best practice. This not only secures privileged credentials used to access sensitive infrastructure environments but also yields insights into asset and credential-based information, informing migration strategies.

Identifying privileged accounts involves a systematic process of discovering and cataloguing all accounts within an organization that possess elevated access rights or privileges. This encompasses various types of accounts, including user accounts assigned administrative privileges, service accounts utilized by

applications or system services, and application accounts used for specific software functions. The process begins with conducting thorough inventorying across the IT infrastructure, including servers, databases, applications, and network devices, to identify all potential sources of privileged access. Automated discovery tools may be employed to scan the network and identify accounts with privileged permissions. Collaboration with different departments and stakeholders helps in uncovering accounts that may have been created for specific purposes but are not adequately documented.

Once identified, these privileged accounts are catalogued and classified based on their level of access and function. This involves documenting pertinent details such as account names, associated users or services, the scope of access, and any dependencies. It's crucial to establish a centralized repository or database to maintain this catalogue for ongoing management and monitoring.
Also organizations should implement mechanisms to continuously monitor and update the catalogue of privileged accounts, as new accounts may be created, existing accounts may be modified, or accounts may become obsolete over time. Regular audits and reviews help ensure the accuracy and completeness of the catalogue, enabling organizations to maintain a comprehensive understanding of their privileged account landscape and effectively manage associated risks.

The process of identifying privileged accounts involves a comprehensive approach that combines automated discovery tools, collaboration with stakeholders, documentation, and ongoing monitoring to establish a thorough catalogue of accounts with privileged access rights within the organization's IT environment. This serves as a foundational step in implementing effective Privileged Access Management practices and mitigating cybersecurity risks. [6]

3.2 Solution Evaluation

Selecting a PAM solution should commence with an evaluation of its alignment with the organization's overarching security and compliance requirements. The

ideal PAM software seamlessly integrates within the existing security and compliance framework, rather than imposing an arbitrarily chosen solution onto the respective teams. Additionally, assessing the complexity of the privileged account landscape within the organization is crucial. For instance, if privileged users are predominantly employees and the system architecture is straightforward, a PAM solution with a limited feature set may suffice. Conversely, if privileged users are dispersed across various entities and regions, managing intricate, interdependent systems, a PAM solution offering comprehensive monitoring capabilities becomes imperative to maintain oversight.

Compliance mandates such as GDPR (General Data Protection Regulation), PCI-DSS (Payment Card Industry Data Security Standard), or ISO 27001 (International Organization for Standardization 27001) necessitate robust privileged access management solutions. Organizations bound by these regulations require deeply featured, highly automated PAM solutions, with particular emphasis on audit logging and reporting functionalities to facilitate compliance and internal audit processes effectively. Additionally, IT factors such as infrastructure nature and PAM solution architecture play pivotal roles in the selection process. The adaptability of the solution to hybrid cloud/on-premises environments and its architecture, preferably agentless, should be carefully evaluated to ensure seamless integration and operational efficiency. From a business and organizational perspective, factors like solution adaptability, ease of use, and organizational structure influence the choice of PAM solution. Cumbersome solutions can disrupt IT operations and hinder business agility, while overly complex technologies risk being disregarded altogether, leading to financial waste and compromised security posture. Furthermore, organizations operating through partnerships or across multiple countries with distinct data privacy regulations should opt for PAM solutions tailored to their unique organizational structures and regulatory landscapes. [16]

To effectively compare different PAM solutions, organizations should employ a structured framework that considers various factors. The framework should include the following key components:

Deployment Flexibility: Evaluate whether the solution offers flexible deployment options, such as on-premises, cloud-based, or hybrid models, to align with the organization's IT strategy and requirements.

Ease of Use: Assess the user interface and administrative tools to determine the solution's ease of use and manageability, ensuring that it can be effectively implemented and maintained by IT staff.

Features: Examine the features offered by each PAM solution, such as MFA, password management capabilities, session recording, privilege escalation controls, and integration with other security tools.

Vendor Reputation: Research the reputation and track record of PAM solution vendors, including their experience, reliability, and customer satisfaction ratings, to gauge the credibility and trustworthiness of the offerings.

Support Services: Consider the availability and quality of vendor support services, including technical support, training programs, and documentation, to ensure prompt assistance and effective resolution of any issues or challenges.

Cost-effectiveness: Evaluate the TCO (Total Cost of Ownership) of each PAM solution, including initial licensing fees, implementation costs, ongoing maintenance expenses, and potential savings or ROI (Return on Investment) resulting from improved security and operational efficiency. [16]

3.3 Roadmap

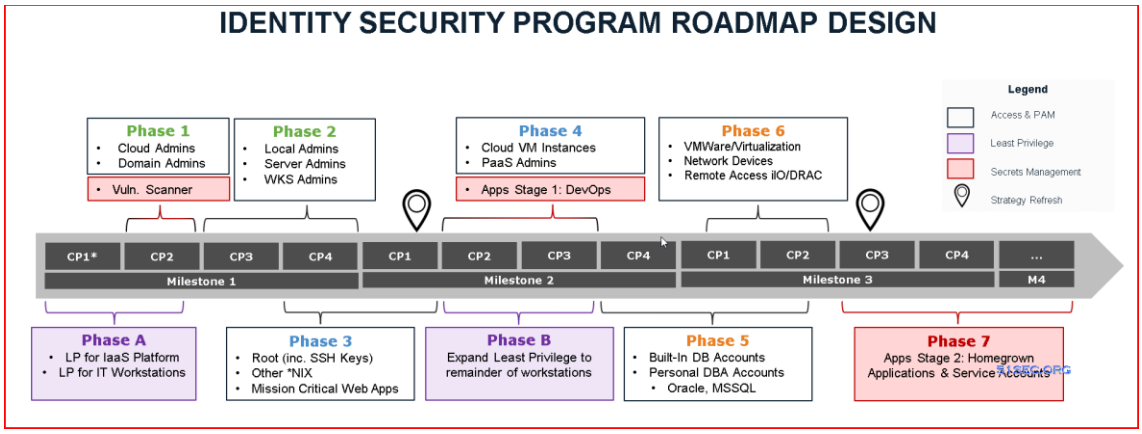

Figure 6: Example of Roadmap (adapted from CyberArk 2024.)

The development of a PAM roadmap is shaped by several factors, encompassing the status of existing controls, identified critical assets, internal agendas (audit, regulatory, security incidents, leadership priorities), and individual goals and objectives. A roadmap usually divides tasks into distinct phases and may involve various technologies and security measures. Phases might also intersect partially. For instance, consider an organization with an audit finding concerning least privilege on workstation computers, prioritizing this over other issues. [6]

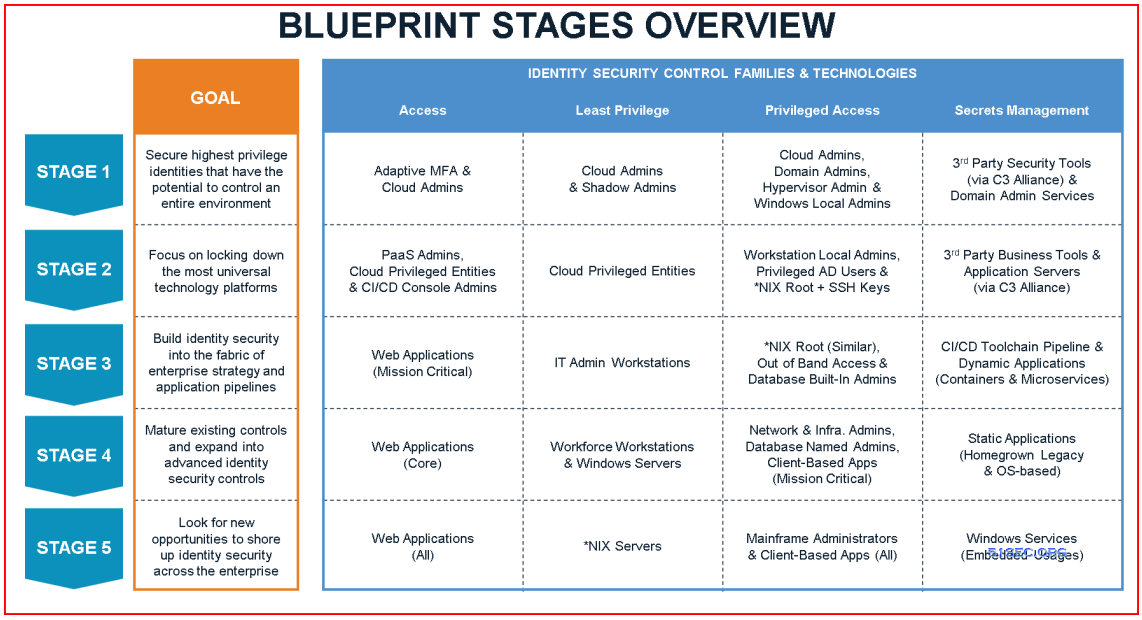

Figure 7: Example of PAM Phases/Stages (adapted from CyberArk 2024.)

This section outlines a high-level view roadmap for implementing a PAM program within organizations. It provides an example of five phase framework that includes recommendations for risk assessment, identification of critical controls, program scoping and planning, rapid risk mitigation, program execution, and ongoing development.

By following this structured approach, organizations can establish a robust and scalable PAM program that evolves into a mature and effective security framework for managing privileged accounts.

Phase 1 (Discovery and Initiation):
The first phase focuses on identifying the organization's business and security requirements, analysing risks, defining critical controls, and mapping out high-level timelines. A significant challenge during this phase is determining the organization's most sensitive systems and data, often referred to as the "keys to the kingdom." Instead of attempting to secure everything immediately, organizations should consult with internal or external experts to leverage proven methodologies and real-world experiences. These efforts provide a solid foundation for planning the program.

Phase 2 (Definition and Planning):
In this phase, the scope of the project is clearly defined. It is recommended to start with a smaller, more manageable scope, as attempting to address everything simultaneously can jeopardize the project's success. The goal is to create a repeatable process, focusing on critical privileged accounts first. By mapping out use cases and critical controls, organizations can establish a clear roadmap for execution and ensure that each step contributes to the overarching program goals.

Phase 3 (Launch and Execution):
Once the team, scope, project objectives, and timeline are in place, a kick-off meeting should be conducted to align stakeholders, set expectations, and define accountability. This phase involves preparing for the deployment of the PAM

solution by addressing prerequisites, installing and configuring the tools, and ensuring system stability. The focus here is to enable secure access to sensitive systems while maintaining operational stability and minimizing disruptions to existing workflows.

Phase 4 (Rapid Risk Mitigation):

During this phase, organizations roll out the PAM solution incrementally. A small group of privileged accounts is selected for initial implementation as part of a pilot program. This allows the organization to identify and address any issues early on while refining the rollout plan. By testing the solution with a controlled subset of accounts, organizations can ensure that broader implementation is smoother and more effective.

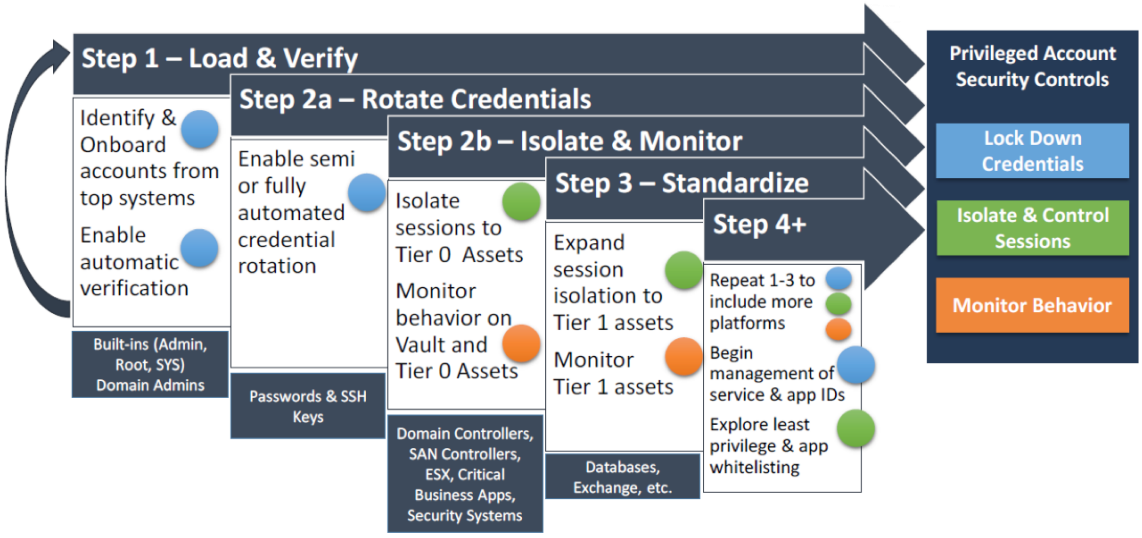

Figure 8: Example of risk mitigation (adapted from CyberArk 2024.)

Phase 5 (Program Maturity):

The final phase involves scaling the PAM solution across the organization. This includes onboarding additional privileged accounts, rotating credentials, implementing session isolation, and monitoring privileged user behaviour. By continuously improving controls and refining processes, the organization enhances its overall security posture. Regular reviews, monitoring, and training ensure that the PAM program remains aligned with organizational goals, adapting to new challenges and growth. [6]

3.4 Policy Definition

At the core of PAM lies the principle of least privilege. This principle dictates minimizing the rights of an agent, be it a human user or a non-human account within a system to the bare minimum necessary for operational functionality and task completion. Designers and managers must meticulously determine the appropriate access level for each user, adjusting access only when essential. However, enforcing this principle necessitates a delicate equilibrium between operational efficiency and security.

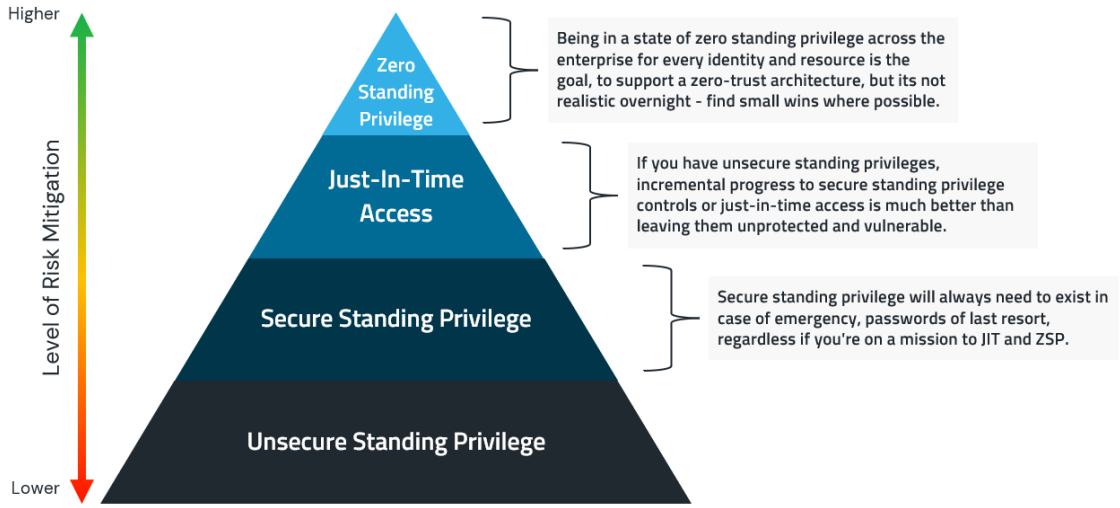

Figure 9: Privileged Access Hierarchy (adapted from CyberArk 2024.) [5]

Unsecure standing privilege represents the highest risk, where identities are granted freestanding, persistent access to enterprise systems with minimal security controls, leaving them vulnerable to identity compromise, lateral or vertical movement, and privilege escalation. Secure standing privilege improves security by applying intelligent controls such as MFA, credential vaulting, session protection, and threat detection to mitigate these risks, though the privilege remains perpetually granted. Just-in-time access further reduces risk by ensuring access is granted only when needed, coupled with intelligent controls, eliminating continuous freestanding access and further protecting against identity compromise and privilege abuse. Finally, zero standing privilege is the most secure model, where both access and entitlements are granted only at the time

of need, with all access controlled by MFA, session management, auditing, and threat detection, and sessions being time-bound, significantly reducing the risk of privilege escalation and misuse. [5]

Consider the scenario where granting an individual full administrative or root access boosts operational efficiency but entails unrestricted system access. Conversely, revoking all privileges and mandating access requests on a case-by-case basis represents the most stringent adherence to the principle of least privilege. Striking a balance between these extremes requires rigorous scrutiny to uphold operational efficiency while mitigating risk. This scrutiny entails conducting a risk assessment of privileges, data, code, files, and resources accessed, along with evaluating frequency of use and impact on system operation. For instance, if an individual needs daily file updates, requiring daily access requests might prove cumbersome. Alternative solutions could involve granting the user the ability to modify the file without approval if the risk is low, assigning the update task to a more privileged user, or system redesign.

Common industry approaches to least privilege include implementing RBAC (Role-Based Access Control), where individuals sharing common roles or responsibilities are grouped together based on logical access attributes. Another solution involves integrating privileged access tools to enable partially or fully automated decisions regarding privileged access, based on predefined criteria. [2]

Dual Approval: Implement a dual approval system for creating or modifying privileged user accounts. Both the System Owner and a member of the IT team should authorize any operational changes to privileged accounts.

Traceability: Ensure that all privileged user IDs (Identification) uniquely identify specific individuals. Avoid creating generic user IDs based on job functions, roles, or projects. Additionally, establish clear naming conventions for service or application accounts to enhance traceability in the event of a security incident.

Expiration Dates: Set expiration dates for all non-employee or third-party privileged user IDs. These dates can be project-specific or default, but it's crucial to revoke high-level rights when they are no longer necessary.

Centralization: Manage all privileged accounts through a centralized system with auditing capabilities. This system should track additions, changes, and deletions to privileged accounts.

Authentication Security: Enforce multi-factor authentication for all privileged accounts to enhance security.

Regular Reassessment: Regularly reassess your inventory of privileged accounts, at least four times a year or more frequently if possible. Look for new, changed, or inactive accounts, and revoke privileges or disable unused superuser accounts accordingly. Adjust expiration dates to align with your organization's workflow and specific needs.

Separate Accounts: Avoid using default admin accounts for production applications requiring privileged access. Instead, create specific privileged accounts for each application to improve traceability and auditing.

Password Security: Never hard-code passwords into the software developed by your organization's employees.

Logging: Log all privileged activities, including user ID creation, deletion, and privilege changes executed by Systems Administrators and other privileged users. Employ session and keystroke recording to capture all activity on privileged accounts. [2]

3.5 Testing and Validation

Testing a PAM system is a critical process that ensures the system's security, functionality, and compliance with organizational policies. This comprehensive plan outlines a structured approach to effectively test a PAM system, covering preparation, functional and security testing, performance evaluation, and continuous monitoring.

Preparation and Planning: The initial phase involves setting clear objectives and developing detailed test plans. Objectives should encompass security, functionality, and performance goals. Creating thorough test plans helps in systematically addressing all potential scenarios that need testing. Preparation ensures the test process is focused and organized.

Environment Setup: Setting up a separate test environment that replicates the production environment is crucial to avoid any disruptions. Using realistic test data that mirrors actual organizational data provides accurate insights into how the PAM system performs under real-world conditions.

Functional Testing: Functional testing verifies that the PAM system performs essential tasks effectively. This includes testing the system's ability to discover privileged accounts across various environments such as Active Directory, *NIX (Unix-like Operating Systems), and cloud platforms. Access control measures are scrutinized to ensure they enforce the principle of least privilege, granting access only to authorized users. The system's password management capabilities are tested to ensure secure storage, rotation, and management of passwords. Additionally, session management features, including session initiation, monitoring, and termination, are evaluated to ensure comprehensive auditing and security. MFA enforcement and the proper assignment of user roles and permissions are also verified.

Security Testing: Security testing involves conducting vulnerability scans and penetration tests to identify potential weaknesses. This phase aims to simulate attacks and assess the system's response to unauthorized access attempts. Testing for common misconfigurations and ensuring audit logs are tamper-proof and accurately recorded are essential components of this phase.

Performance Testing: Performance testing evaluates how the PAM system handles high load and stress conditions. Load testing measures the system's performance under normal and peak conditions, while stress testing assesses its

stability under extreme scenarios. Response time measurements for various operations ensure the system meets acceptable performance thresholds.

Compliance Testing: Compliance testing ensures the PAM system adheres to relevant regulations and standards, such as GDPR, HIPAA (Health Insurance Portability and Accountability Act), and SOX (Sarbanes-Oxley Act). It also verifies that the system enforces organizational security policies, ensuring a consistent and compliant security posture.

Integration Testing: Integration testing examines how well the PAM system integrates with other security tools like SIEM, IAM, and vulnerability management systems. Testing APIs (Application Programming Interface) used by the PAM system ensures they function correctly and securely, facilitating seamless integration and communication with other systems.

User Acceptance Testing (UAT): End-user testing is conducted to ensure the system meets the needs and expectations of actual users. Collecting feedback during this phase helps identify any issues or areas for improvement, ensuring user satisfaction and system effectiveness. [22]

Documentation and Training: Reviewing documentation ensures that user manuals and operational documents are accurate and complete. Validating training programs ensures they effectively educate users on how to use the PAM system, promoting proper usage and adherence to security protocols.

Review and Reporting: Tracking issues discovered during testing and compiling a comprehensive report detailing the testing process, findings, and recommendations are essential for transparency and accountability. This phase ensures all stakeholders are informed and aligned on the PAM system’s status and any necessary improvements.

Continuous Monitoring and Improvement: Implementing continuous monitoring helps detect and respond to new threats and issues in real time. Regular audits

ensure the PAM system continues to meet security and operational requirements, maintaining a robust and secure environment. [18]

3.6 Steps of PAM Configuration

Let’s delve into the specific technical settings and steps during the implementation phase, the following tasks will be broadly addressed: It's crucial to recognize that the order will widely fluctuate based on factors such as organization size, complexity, types of IT assets, network segmentation, access patterns, unified PAM requirements, and resource availability.

The figure below is to show the general components that need to be configured for the implementation of PAM system. Consistent communication and collaboration among stakeholders, IT teams, security teams, and business units is crucial throughout this process. [15]

General Settings
Mail Server Settings
Proxy Server Settings
Securden Server Connectivity & Starting the PAM Server
User Onboarding
Integration with AD/Azure AD/LDAP for user provisioning and authentication
User Import Options
Add Users Manually
Assigning Roles to Users
Custom Roles
User Reports

Details
User Groups
Import Groups Options
Group Settings
Basic Configurations
Integration with multiple AD domains / Azure AD
Integration with SAML 2.0 based Single Sign On Solutions
Multi Factor Authentication Setup

Account Management
Automatic discovery of IT assets and privileged accounts
Importing Accounts - Flexible import options to build inventory
Secure, Centralized Repository of Accounts
Storing SSH keys, documents, files, images, digital identities
Organizing data as folders for bulk management
Optional personal vault within organization's vault
Manage Shared Admin Passwords
Granular Sharing and Controls
Secure sharing with third-parties
Option to allow access without showing the password
Periodically synchronizing assets and accounts
Windows service accounts and dependencies management

Password Management
Automated, periodic remote password resets
Self-supporting any SSH-enabled device for password resets
Password release control workflow for just-in-time access
Password policy creation and enforcement
Role based access controls
Remote Access and Session Management
Support for one-click remote session initiation - RDP, SSH, SQL, HTTPS etc.
Web-based remote connection launching
Remote connection through native tools for RDP, SSH, SQL
Session access without disclosing password

Details
Session Recording, Playback, Live Remote Session Monitoring, Concurrency Controls
Custom connector for launching any application - Custom Application Launcher
Remote gateways to manage distributed networks
Application-to-Application Password Management
APIs for managing machine identities, application identities, secrets, keys
Eliminate embedded credentials on script files, applications
Privilege Elevation & Delegation
Remove admin rights across Windows endpoints, servers
Configure Applications and commands for privilege elevation
Elevate applications for standard users on-demand
Configure policy-based application control
Provision for granting temporary admin rights
Support for command filtering and controls on Unix
Technician Access - (/Third Party Access)

Audit, Reports and Notifications
Explore comprehensive auditing & reporting
Searchable text-based audit trails
Filtering audit trails to create custom reports
User access and activity reports
Policy compliance reports
Password expiration reports
Micro reports for specific requirements
Breached passwords identification and notification
Password security analysis report
Provision to trigger automated follow-up actions upon events
Password event notifications (real-time and periodic)
Advanced Settings, High Availability, and Architecture
On-prem, private cloud deployments
Distributed server deployment architecture

Details
Database backup for disaster recovery
High-availability
Option to use Always-on MS SQL clusters, Amazon Aurora
Best Practices, Security Hardening, Miscellaneous
Configure ticketing system integration
Configure cloud storage integration
Provision web-based access to end users
Enforce security settings and controls (IP restrictions, enabling/disabling access)
Provision for restricted access over the internet
Explore browser extensions
Cross-platform access
Mobile Apps
Secure offline access
User Acceptance Testing
Delivery and closure

Figure 10: An Example of Implementation Steps (adapted from Securden. 2024) [15]

3.7 Reporting, Communicating and User Training

Your reports serve as the narrative that communicates the significance of the program to leadership and oversight communities. They highlight progress, address issues, and quantify risk mitigation due to implemented controls. Tailor these concise and informative messages to your audience using various formats such as scorecards, dashboards, presentations, and open communications. Effective reporting sets the tone for your program, so understanding your audience and their informational needs is crucial for formalizing communications.

Utilize a variety of built-in reports, like inventory, entitlement, and compliance reports, to create comprehensive scorecards and dashboards. Automate these processes to save time and export data to business analytics and intelligence tools like Splunk, Tableau, and PowerBI. Enhance this data with inputs from other inventory tools, entitlement databases, and compliance reports for richer context. Ensure your reporting feeds into your GRC (Governance, Risk, and Compliance) tools to provide a real-time view of the organization's risk and control landscape. Leverage your existing technology to maximize efficiency and effectiveness.

Figure 11: An Example of PAM Adoption Program (adapted from CyberArk 2024.)

Schedule Executive Review Sessions. Reporting is ineffective without sharing and presenting the data to the appropriate audience. Schedule regular review sessions with executive leaders or leadership teams to update them on the progress, updates, and challenges of your PAM program. Key executive audiences may include the IAM director, steering committee, CISO, and board of directors. Perception shapes reality in reporting strategies. Understand your audience and provide meaningful, transparent, and clear communications to set the appropriate tone. If you fail to do so, your reporting committees will form their own conclusions and define the narrative for you.

PAM steering committees typically include representatives from IAM leadership, partner practices, information security, technical departments, audit, IT risk, and human resources to ensure comprehensive organizational representation. Schedule Regular Business Reviews. Successful PAM programs achieve alignment not only with internal executives but also with external stakeholders. Work with your Account Team or relevant external advisors to schedule regular business review meetings. While the content may vary, typical agenda topics include reviewing existing program objectives and progress, aligning on future goals, and discussing relevant updates and product improvements.

Attendees generally include a technical representative from the PAM Team (Vault Admin), Product Owners, Director of IAM, CISO (Chief Information Security Officer), Account Team, and Executive Management.

Coordinate with your Account Team or advisors to establish a regular review cadence, review the relevant agenda, and determine the appropriate participants to ensure comprehensive and productive discussions. [6]

4 Post Deployment

4.1 Post Deployment Review

After the deployment, the first task is to validate the system’s functionality. This includes confirming that privileged accounts are properly managed, automated tasks like password rotation and session monitoring are working, and that integrations with systems such as SSO, MFA, and SIEM are seamless. Additionally, UAT helps identify any usability concerns, ensuring that both users and administrators are satisfied with the system's functionality.

Monitoring and auditing the system’s performance in the live environment is also critical. This involves reviewing access logs to ensure compliance and detecting any suspicious activities. Regular audit reports should also be generated to confirm that internal policies and regulatory standards are being met. Furthermore, ensuring the PAM system can handle the organization’s workload without any performance bottlenecks is vital for long-term effectiveness. Security assessments, such as penetration testing and vulnerability scanning, are necessary to identify any overlooked weaknesses and address them promptly. This phase also includes analysing user behaviour to detect unusual activities within privileged accounts, helping to reinforce the security posture of the system.

Engaging stakeholders is a key aspect of the post-deployment process. Continuous feedback from end-users, the IT team, and executives helps refine

workflows and ensures the system meets the broader IT strategy. Executives should be updated on KPIs (Key Performance Indicators), such as security improvements or compliance gains, while IT staff can provide insights on technical challenges or potential enhancements.
Refining access control policies and governance frameworks is another crucial step. This involves adjusting policies based on actual usage patterns and ensuring that privileged accounts are regularly reviewed in line with the principle of least privilege. Strengthening governance structures will help maintain oversight of PAM operations, ensuring accountability and security.

Continuous improvement is needed for maintaining the effectiveness of the PAM system. Regular software updates and patches should be applied to address vulnerabilities and enhance features. Scalability planning is also important to ensure the PAM solution can accommodate future growth, such as cloud migrations or the addition of new business units. Ongoing training for users and administrators ensures they remain equipped to utilize the system effectively, keeping the organization secure as cybersecurity challenges evolve. Measuring the success of a PAM deployment is done by tracking several metrics, such as reductions in security incidents, improvements in audit compliance, and the overall utilization of the system. These metrics help determine whether the PAM solution is achieving its goals and delivering value. [7]

5 The Future of AI in PAM

5.1 AI and Machine Learning

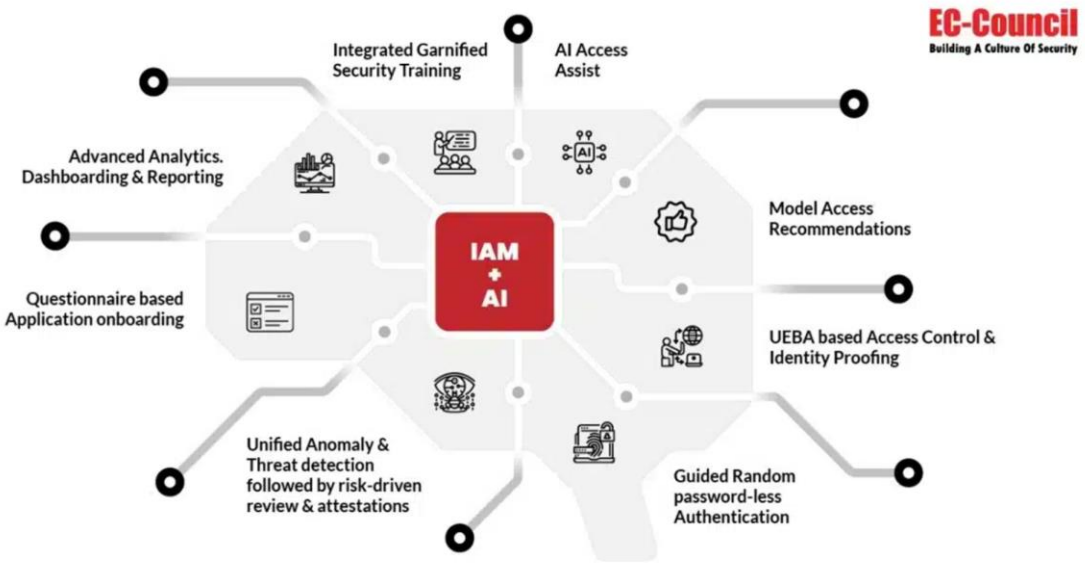

Figure 12: An Example of AI + IAM Integration (adapted from EC-Council 2024.)

As cybersecurity threats become increasingly complex, traditional reactive security measures are no longer sufficient. PAM plays a crucial role in protecting high-level access to sensitive systems, but the integration of AI (Artificial Intelligence) and ML (Machine Learning) is transforming PAM into a proactive, predictive security tool. Machine Learning enhances PAM's anomaly detection capabilities by continuously analysing user behaviour, access patterns, and system logs to establish a baseline of normal activity. This allows ML algorithms to flag unusual behaviour, such as accessing systems from unfamiliar locations or during odd hours, which could indicate compromised credentials or insider threats. Over time, the system learns to reduce false positives, refining its detection accuracy as it adapts to evolving behaviour patterns.

Artificial Intelligence further strengthens PAM by introducing predictive analytics, which leverages historical data to forecast potential security threats. By analysing past breaches, attack vectors, and system vulnerabilities, AI can identify patterns that indicate emerging risks. This predictive capability enables PAM systems to

adjust access controls pre-emptively, restricting sensitive actions or access to critical systems before an attack can materialize. In this way, AI shifts PAM from a reactive to a proactive security solution, identifying and mitigating threats before they can cause significant harm.

AI enables PAM systems to trigger automated responses when a threat is detected. For instance, when an unauthorized access attempt is identified, the AI system can automatically revoke access permissions, initiate multi-factor authentication, or even isolate affected network segments to contain potential breaches. These automated responses occur in real-time, minimizing the delay between detection and action, which is critical in preventing the escalation of security incidents. The continuous learning capabilities of AI and ML ensure that PAM systems evolve alongside changing attack tactics. As new threats emerge, these systems automatically adjust their detection models and responses based on the latest data. This adaptability helps organizations stay ahead of attackers who continuously refine their strategies.

One of the most valuable applications of AI in PAM is its use in behavioural analytics. AI-driven systems analyse not only external threats but also internal behaviours, identifying deviations from established norms. By monitoring how users interact with systems and data, AI can detect early signs of insider threats, whether malicious or unintentional. This heightened awareness allows organizations to respond to potential risks much earlier, often before significant damage can occur.

The integration of AI and ML into PAM systems also contributes to greater operational efficiency. Routine tasks such as monitoring access logs, classifying security incidents, and managing access rights can be automated, freeing up security personnel to focus on more complex analysis and strategic decision-making. This not only reduces human error but also allows security teams to prioritize critical threats more effectively.

AI and ML are expected to bring further advancements to PAM. One significant trend is the development of autonomous incident response, where PAM systems

will be able to independently handle security incidents by analysing context, selecting appropriate responses, and executing actions. This will streamline incident management and reduce the reliance on human intervention. Additionally, AI will continue to integrate with external threat intelligence platforms, keeping PAM systems updated on global cybersecurity trends and emerging threats, ensuring that organizations are always aligned with the latest security protocols.

AI and Machine Learning are revolutionizing the way PAM systems operate, moving beyond traditional reactive methods to provide proactive, predictive security. These technologies enhance the accuracy of threat detection, automate response actions, and enable systems to adapt in real-time to new attack methods. As the cybersecurity landscape continues to evolve, the integration of AI and ML into PAM will be essential for staying ahead of increasingly sophisticated threats. [19]

6 Conclusions

In this PAM implementation guide we have gone through a high-level view on how to implement PAM system within an organizational setting. After the initial background of the thesis along with a brief history of PAM, the implementation process was compressed primarily into 7 key topics: Define and Discover, Solution Evaluation, Roadmap, Policy Definition, Testing and Validation, Steps of PAM Configuration and Reporting, Communicating and User Training.

To tie everything together, a successful PAM implementation requires a structured and carefully planned approach that begins with the discovery and mapping of systems and privileged accounts. This foundational step ensures a comprehensive understanding of access points to sensitive data and lays the groundwork for an effective PAM strategy. Evaluating potential PAM solutions and selecting those that align with the organization's specific infrastructure and security requirements is critical. Collaboration with key stakeholders, IT teams, security professionals, and business users, ensures that the selected solution addresses both technical and operational needs. Clear policy definition and

continuous testing is required for establishing secure privileged access, achieving compliance, and mitigating risks before full deployment. When implemented, PAM systems demand continuous oversight to remain effective. Regular monitoring, periodic reviews, and the adaptation of policies and configurations are needed for addressing emerging threats and evolving organizational needs. Ongoing training and awareness programs are important to ensure that users adhere to best practices, maximizing the PAM system's long-term success.

Looking into the future, the integration of AI into PAM systems is set to redefine their capabilities. AI-driven features such as real-time threat detection, anomaly detection, predictive analytics, and automated responses offer enhanced protection against sophisticated cyber threats. By using AI, organizations can improve their ability to detect and mitigate risks, making their PAM systems more resilient and adaptive. Implementing and managing a PAM solution is not a one-time project but a continuous process of refinement and improvement. It is an integral component of a critical security strategy, protecting privileged accounts while ensuring compliance and reducing the risk of security breaches. The future of PAM will undoubtedly be shaped by advancements in AI, reinforcing its role as a cornerstone of cybersecurity in an ever-evolving threat landscape.

References

1 Burnis A. 7 types of privileged accounts, service accounts, and more [Internet]. CyberArk; 2017 Nov 1 [cited 2024 Dec 27]. Available from: https://www.cyberark.com/resources/blog/7-types-of-privileged-accounts-service-accounts-and-more

2 Carson J. Privileged access management best practices. Delinea [Internet]. 2022 [cited 2024 Dec 28]. Available from: https://delinea.com/blog/privileged-access-management-best-practices

3 Carson J. The evolution from password managers to Privileged Access Management. Which is right for you? Delinea [Internet]. 2019 [cited 2024 Dec 27]. Available from: https://delinea.com/blog/privileged-access-vs-account-management

4 Carson J. The Privileged Access Management lifecycle and path to maturity. Delinea [Internet]. 2019 [cited 2024 Dec 27]. Available from: https://delinea.com/blog/privileged-access-management-lifecycle-path-to-maturity

5 Creamer J. Understanding risk, access and privilege controls with the CyberArk blueprint [Internet]. 2024 Oct 21 [cited 2024 Dec 30]. Available from: https://community.cyberark.com/s/article/Understanding-Risk-Access-and-Privilege-Controls-with-the-CyberArk-Blueprint

6 CyberArk. Implementation program. CyberArk [Internet]. 2024 [cited 2024 Dec 28]. Available from: https://docs.cyberark.com/pam-self-hosted/14.0/en/content/imp-program/imp-program-lp.htm?tocpath=Get%20Started%7CImplementation%20Program%7C___0

7 Delinea. Validating operations after deploying [Internet]. 2024 [cited 2024 Dec 30]. Available from: https://docs.delinea.com/online-help/server-suite/install/deployment/validating/index.htm

8 Delinea. What is a privileged account? Delinea [Internet]. 2024 [cited 2024 Dec 27]. Available from: https://delinea.com/what-is/privileged-account

9 Delinea Team. 10 features every PAM solution must have [Internet]. 2024 [cited 2024 Dec 28]. Available from: https://delinea.com/blog/10-features-a-privileged-access-management-solution-must-have

10 Delinea Team. Centrify continues to modernize privileged access management for DevSecOps with SSH key management. Delinea [Internet]. 2020 Aug 26 [cited 2024 Dec 28]. Available from: https://delinea.com/news/centrify-continues-modernize-privileged-access-management

11 Delinea Team. Rising to the modern PAM challenge [Internet]. Delinea; 2020 [cited 2024 Dec 27]. Available from: https://delinea.com/blog/rising-to-the-modern-privileged-access-management-pam-challenge

12 Gartner. Gartner Identifies the Top Cybersecurity Trends for 2024 [Internet]. Stamford, CT: Gartner; 2024 [cited 2024 Dec 25]. Available from: https://www.gartner.com/en/newsroom/press-releases/2024-02-22-gartner-identifies-top-cybersecurity-trends-for-2024

13 Morimanno D. What is Privileged Access Management (PAM)? [Internet]. Integral Partners; 2023 [cited 2024 Dec 25]. Available from: https://www.integralpartnersllc.com/what-is-privileged-access-management-pam/

14 Okta. Privileged access management solutions: Securing critical assets [Internet]. 2024 Oct 31 [cited 2024 Dec 28]. Available from: https://www.okta.com/Identity-101/privileged-access-management-solutions/

15 Securden. Unified PAM Implementation Guide [Internet]. 2024 [cited 2024 Dec 25]. Available from: https://www.securden.com/privileged-account-manager/docs/pam-implementation-guide.pdf

16 Senhasegura. Privileged Access Management (PAM): A Complete Guide. Senhasegura [Internet]. 2024 Nov 19 [cited 2024 Dec 27]. Available from: https://senhasegura.com/post/privileged-access-management-pam-a-complete-guide

17 Shaji A. 5 common challenges associated with privileged access [Internet]. StickmanCyber; 2021 Jul 5 [cited 2024 Dec 27]. Available from: https://www.stickmancyber.com/cybersecurity-blog/privileged-access-management-challenges

18 SSH. Integrating PAM with SIEM for comprehensive threat monitoring [Internet]. 2024 [cited 2024 Dec 30]. Available from: https://www.ssh.com/academy/pam/integrating-privileged-access-management-with-siem-for-comprehensive-threat-monitoring

19 SSH. Leveraging Machine Learning and AI in PAM for Predictive Security [Internet]. 2024 [cited 2024 Dec 25]. Available from: https://www.ssh.com/academy/pam/leveraging-machine-learning-and-ai-in-privileged-access-management-for-predictive-security

20 Tornikoski E. How to do a Privileged Access Management Audit? [Internet]. SSH; 2024 May 17 [cited 2024 Dec 28]. Available from: https://www.ssh.com/blog/how-to-do-privileged-access-management-audit

21 Verizon. 2024 Data Breach Investigations Report [Internet]. Basking Ridge, NJ: Verizon; 2024 [cited 2024 Dec 25]. Available from:

https://www.verizon.com/business/resources/Tc80/reports/2024-dbir-data-breach-investigations-report.pdf

22 Walker J. Best practices for privileged access management for the cloud [Internet]. 2024 Mar 3 [cited 2024 Dec 30]. Available from: https://www.conductorone.com/guides/best-practices-for-privileged-access-management-for-the-cloud/