



Best Practices in Privileged Access Management

www.secureki.com

Challenges and Benefits of PAM Done Well

Privileged access management involves handling highly powerful administrative accounts and rights built into every piece of technology, from the largest servers to the smallest devices. This widespread presence of privileged identities makes them challenging to manage. Additionally, people who need access to these privileges are also everywhere, including administrators, everyday users, contractors, and more. This spreading of privileged identity, sometimes referred to as "access sprawl," complicates efforts to keep intruders out. Today's intruders bypass firewalls and find privileged access waiting for them. Meanwhile, insiders with malicious intentions can retain their administrative access and wreak havoc on the organization. Privileged Access Management (PAM) secures privileged identities while enabling business operations to remain fluid.



When PAM is done well, it reduces risk, enhances efficiency, meets compliance needs, and builds a robust cyber defense behind the firewall. Every unmanaged privileged identity poses a risk not worth taking. PAM mitigates this risk by managing credentials where they reside and controlling who can use them at all times. This management ensures that legitimate access is granted in a predictable, repeatable manner. PAM also ensures you always know who has what power at any time, reducing individual risk for administrators and providing the audit trail every regulated organization needs. Combined, these measures help defeat intruders before they can cause real damage. Whether attackers bypass your perimeter defenses or gain entry as contractors, they seek unsecured privilege to escalate their attacks, and PAM done well stops them in their tracks.

This document outlines how to implement PAM effectively and reap its benefits. We'll start with a quick list of best practices collected from decades of experience helping customers, followed by a detailed dive into each practice to provide practical insights on their implementation.

Quick List of PAM Best Practices

We've categorized these practices into the required, the proactive, and the advanced stages. While the goal may be to implement everything as best as possible, practical constraints often dictate a staged approach.


What's Required for Starting Out with PAM

PAM, like any other initiative, must start somewhere. The success of the initial phase often dictates overall effectiveness. Here are best practices distilled from our most successful customers for starting your PAM journey:

Required:

- Provide safe storage for privileged identities, a "vault," with check-in and check-out capabilities.
- Rotate privileged identity passwords on a schedule to mitigate insider risk and stop attackers before they escalate to cause significant damage.
- Manage service accounts to avoid stale credentials creating risk at the application layer.
- Furnish reporting mechanisms to satisfy auditor requirements.

Proactive:

- Move beyond passwords to other forms of privilege (e.g., SSH keys or group memberships).
 - Use a closed-loop discovery process to ensure new privileged identities are managed quickly and efficiently.
 - Control and record sessions to monitor all actions performed with privileged access.
 - Integrate PAM with SIEM and other threat detection systems for automated responses to suspicious activity.
- 

Advanced:

- Scale up to manage privileges end-to-end across IT systems, including IoT and cloud environments.
- Manage embedded credentials in application configuration files, backup scripts, database connection strings, and other common locations where passwords appear in clear text or with little protection.
- Deeply integrate PAM with Identity Governance and Administration (IGA) and Identity Access Management (IAM) to ensure proper lifecycle management of privileged identities related to governance and personnel events.

Detailed Best Practices for PAM

Provide Safe Storage for Privileged Identities

Safe storage of privileged identities is essential. Moving privileged access from individuals' control to system control is crucial. No one needs to be an all-powerful administrator at all times. Early PAM solutions used a vault metaphor for storing privileged credentials. Modern solutions should be secure yet lightweight and functional, with mobile-friendly check-in/check-out capabilities and automated credential management.

Rotate Privileged Identity Passwords on a Schedule

Rotating privileged passwords regularly enhances security by making it harder for attackers and insiders to exploit them. IT often hesitates to change passwords due to uptime concerns. However, with a competent PAM system, password rotation can be automated without impacting uptime. The goal is to rotate credentials as frequently as possible, ideally daily, to outpace automated attacks.

Manage Service Accounts

Service accounts running critical applications often suffer from poor password practices. These credentials need regular rotation without disrupting application operations. Demand a process that rotates service account passwords without interfering with application functionality. Ensure that credentials embedded in applications are rotated securely and consistently.

Furnish Reporting Mechanisms for Auditors

Strong cyber defense behind the firewall produces valuable audit information. While compliance shouldn't overshadow security goals, ensure your PAM system offers adequate out-of-the-box reports and supports extensive data mining. This balance allows auditors to obtain necessary reports without overburdening security teams.

Making PAM a Proactive Defense

Checking off required items establishes a foundational PAM program. For real success, evolve into a proactive defense by addressing internal and external threats through the following practices:

Furnish Reporting Mechanisms for Auditors

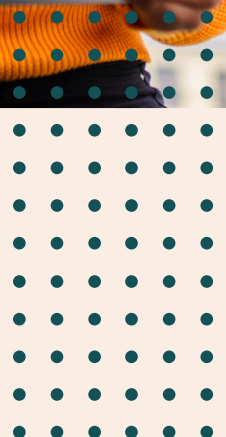
Strong cyber defense behind the firewall produces valuable audit information. While compliance shouldn't overshadow security goals, ensure your PAM system offers adequate out-of-the-box reports and supports extensive data mining. This balance allows auditors to obtain necessary reports without overburdening security teams.

Move Beyond Passwords

Passwords are only part of the risk landscape. Manage other forms of privilege, such as SSH keys, AD group memberships, and Sudo access. Bringing all methods of privilege use under PAM management enhances overall security.

Use a Closed-Loop Discovery Process

Ensure continuous discovery and management of privileged identities. Automated discovery and integration with other IT systems, like CMDB, can keep your PAM system current and responsive to changes.



Control and Record Sessions

Providing administrators with fully formed, recorded sessions for routine tasks minimizes the risk of direct privilege misuse. Session recording also serves as a deterrent, as people tend to behave better when they know they are being monitored.

Integrate PAM with SIEM and Threat Detection

PAM should also function as a reactive control. Integrating PAM with SIEM and threat detection systems allows for automated responses to suspicious activity, such as rotating critical credentials during an active threat.

Advanced PAM Best Practices

For mature PAM programs, implement the following advanced practices to enhance security further:

Scale Up to IoT and Cloud Environments

Extend PAM across all IT systems, including IoT devices and cloud environments. Ensure your PAM solution can handle large-scale deployments and test it thoroughly before full implementation.

Manage Embedded Credentials

Embedded credentials in application files, backup scripts, and database connection strings need secure management. Advocate for secure credential storage and rotation methods that do not disrupt operations.

Integrate PAM with IGA and IAM

Privileged identities should be integrated with IGA and IAM systems to ensure proper lifecycle management. Business-driven policies should govern access to privileged identities, and these policies should be enforced through PAM.

Conclusion

As Oscar Wilde said, "The only thing to do with good advice is to pass it on. It is never of any use to oneself." These best practices, derived from the experiences of our customers, are intended to guide you in implementing a robust PAM program. While no organization may implement all practices at once, aspiring to adopt them will strengthen your cyber defense and help you win battles in the ongoing cyberwar.

About SecureKi

SecureKi is a leading cybersecurity company specializing in securing and managing credentials. Our solutions empower customers to prevent targeted attacks, mitigate insider threats, achieve compliance, enhance operations, and secure their hybrid enterprises.

Trusted for our innovative and forward-thinking security technologies, SecureKi designs and develops solutions that enable organizations to manage their enterprise passwords effectively and automatically. Our cutting-edge technology has revolutionized enterprise password management, introducing a new paradigm in credential security.

With our automated password policy workflow, SecureKi eliminates the tedious and time-consuming task of manually changing passwords, significantly reducing administrative overhead. As a future-oriented company built on trust and credibility, our mission is to help customers secure and efficiently manage their enterprise passwords. SecureKi — Where Identity Meets **Security**.



SecureKi Sdn Bhd (1143453-U)

C-13-09, Sunway Nexis, No 1, Jalan PJU
5/1, Kota Damansara, 47810 Petaling Jaya,
Selangor.

Tel: +603-7652 1099

Sales@secureki.com

www.secureki.com