Privileged Access Management (PAM) Best Practices

Sechard.com

Embracing Privileged Access Management (PAM)

SECHARD
Complete Zero Trust

In an era where data breaches and cyberattacks have become rampant, Privileged Access Management (PAM) stands as a critical defense mechanism in an organization's cybersecurity framework. PAM is more than just a technology; it's a comprehensive strategy and a set of practices that meticulously manage, control, and monitor account and data access rights within an organization.

The core objective of PAM is to ensure that individuals and systems have the appropriate level of access to critical resources when required, and nothing more. It targets the often-overlooked concept of privileged access, including human access (employees, vendors, or contractors) and non-humans (applications, systems, or connected devices).

The sophistication of modern cyber threats necessitates a solution that extends beyond traditional perimeter-based security models. PAM, therefore, provides a granular level of control that helps protect sensitive information and critical systems by restricting access based on necessity and relevance. Moreover, PAM acts as a safeguard against external threats and significantly mitigates insider threats. By meticulously managing privileged access, PAM helps minimize the risk of data leaks, misuse of privileges, and unauthorized access, ensuring a robust security ecosystem within the organization.

As we step further into the digital age, where the proliferation of cloud-based solutions, remote work, and digital transformation initiatives continue to grow, the role of PAM in enhancing an organization's security posture becomes more critical than ever before. It's time for organizations to embrace PAM as an essential part of their cybersecurity strategy.

Sechard.com

SECHARD
Complete Zero Trust

PAM BEST PRACTICES

Privileged Access Management (PAM) Best Practices

SECHARD
Complete Zero Trust

1 Employ Temporary Privilege Escalation

Security vulnerabilities often arise from granting users excessive access rights. A wise way to reduce these vulnerabilities is to use temporary privilege escalation, where admin rights are granted only when necessary. This strategy allows organizations to avoid unnecessary exposure and effectively manage insider threats, thus lowering the risk of both internal and external attacks.

2 Keep Track of Assets and Privileges

Visibility into your digital assets and corresponding privileges is key to managing them effectively. By maintaining a clear inventory of your digital assets, you can understand which privileges are redundant, obsolete, or potentially risky. This proactive approach ensures your organization stays on top of its asset management, helping avoid any unforeseen security challenges.

Privileged Access Management (PAM) Best Practices

SECHARD
Complete Zero Trust

3 Deploy Attribute-Based Access Control

Attribute-Based Access Control (ABAC) adds another level of security to your organization. It uses a combination of user, device, and environmental attributes to make access decisions. This comprehensive approach enhances your security posture by giving you more control and flexibility in defining who can access what, when, and under what circumstances.

4 Monitor Assignment of Privileges Versus Usage

The privileges granted to a user or role may not always align with their actual usage. Regularly reviewing the assigned privileges versus actual usage can uncover unused privileges that could pose potential security risks. This active monitoring helps organizations maintain a lean, efficient, and secure access management strategy.

Privileged Access Management (PAM) Best Practices

SECHARD
Complete Zero Trust

5 Deploy Zero Trust, Everywhere

The Zero Trust model assumes breach, meaning it doesn't automatically trust anything inside or outside its perimeters. It verifies every access request as though it originates from an open network. This rigorous strategy enhances security by requiring complete authentication, authorization, and encryption for every request, regardless of origin.

6 Record and Audit

Record-keeping and regular audits are critical for maintaining a healthy PAM strategy. An audit trail of all privileged activities aids in identifying unusual patterns and supports forensic investigations. Regular audits also ensure your organization stays compliant with regulatory requirements, making it a vital practice in effective PAM.

Privileged Access Management (PAM) Best Practices

SECHARD
Complete Zero Trust

7 Monitor and Alert

Implementing real-time monitoring and alerting systems significantly enhances your organization's ability to detect unusual or potentially harmful activities. Quick detection can either prevent potential breaches or minimize their impact, thereby helping maintain your organization's cybersecurity integrity.

Adopting these best practices for Privileged Access Management can significantly improve an organization's security posture. Not only does a robust PAM strategy protect your critical assets, but it also supports compliance, boosts operational efficiency, and fuels business growth, making it a valuable component of your overall business strategy.

SecHard Privileged Access Manager

SECHARD
Complete Zero Trust

SecHard Privileged Access Manager is packed with advanced features and is engineered to offer unbeatable protection for your organization's privileged accounts.

From an encrypted password vault that securely stores all your critical credentials and comprehensive session recording capabilities that provide in-depth visibility into user activities to 2FA authentication, ensuring extra layers of security, SecHard Privileged Access Manager is your ultimate defense against cyber threats.

But that's not all - our solution is more than just a security tool. It's designed to enhance operational efficiency too. By automating routine tasks, reducing the potential for human error, and providing tools for seamless policy enforcement, SecHard Privileged Access Manager helps your organization save valuable time and resources.

Contact us today to learn more about how Sechard can help you achieve your cybersecurity goals!

sales@sechard.com