

Comprehensive Guide to Secure and  
Compliant Privileged Account Management

# PAM – Complying with GDPR

Deep InfoSec

Pr. Nsiangani, CEO

Expert AI - Information Security & Cyber Defense

---



# Introduction

Identity and access management (IAM) is a critical component of any organization's cybersecurity strategy. Privileged accounts, such as administrator or root accounts, are essential for the operation of an organization, but they also present a significant security risk if not properly managed. According to the 2020 Verizon Data Breach Investigations Report, 63% of data breaches involve the use of stolen credentials, making strong password management and access controls essential for preventing cyber attacks.

In addition to the security risks associated with privileged accounts, organizations must also consider compliance with relevant laws and regulations, such as the General Data Protection Regulation (GDPR). Non-compliance with GDPR can result in significant fines, up to 4% of a

company's global annual revenue or €20 million (whichever is greater), as well as reputational damage.

Given the importance of IAM for both security and compliance, it's essential that organizations have a robust strategy in place for managing privileged accounts.

In this paper, we will explore the challenges associated with privileged account management and provide practical guidance on how organizations can effectively manage these accounts in a secure and compliant manner.

## Challenges of Privileged Account Management

One of the main challenges of privileged account management is balancing the need for access with the need for security. On the one hand, privileged accounts are necessary for the operation of an organization, and

employees need access to these accounts in order to perform their job duties. On the other hand, granting access to privileged accounts also increases the risk of unauthorized access and potential security breaches.

Another challenge is ensuring compliance with relevant laws and regulations. As mentioned previously, GDPR requires that organizations have documented policies and procedures in place for data processing activities, including access to privileged accounts (Article 30). In addition, GDPR requires that organizations have appropriate technical and organizational measures in place to ensure the security of personal data, including measures to prevent unauthorized access to privileged accounts (Article 32).

Another challenge is ensuring compliance with relevant laws and regulations. As mentioned previously, GDPR requires that organizations have documented policies and procedures in place for data processing activities, including access to privileged accounts (Article 30). In addition, GDPR requires that organizations have appropriate technical and organizational measures in place to ensure the security of personal data, including measures to prevent unauthorized access to privileged accounts (Article 32).

# Practical Steps for Secure and Compliant Privileged Account Management

Despite the challenges associated with privileged account management, there are steps that organizations can take to effectively manage these accounts in a secure and compliant manner. These steps include:

Establish a clear and GDPR-compliant process for requesting and granting access to privileged accounts. To ensure that access to privileged accounts is granted only to those who need it and for legitimate purposes, it is important to establish a clear process for requesting and granting access that is compliant with GDPR. This process should include defined roles and responsibilities, as well as a system for tracking and documenting access requests and approvals.

Use a privileged access management (PAM) tool to securely store and manage privileged accounts. A PAM tool, such as a password vault, allows you to securely store and manage privileged accounts in a central location. This not only helps to prevent unauthorized access, but also makes it easier to manage and track access to these

accounts, which can be crucial for demonstrating compliance with GDPR.

One practical solution for secure and compliant privileged account management is the use of a password vault or privileged access management (PAM) tool. A password vault allows organizations to securely store and manage privileged accounts in a central location, helping to prevent unauthorized access and simplifying the management and tracking of access to these accounts.

There are several password vaults on the market, including CyberArk, Thycotic, and Centrify. Each of these products offers a range of features, such as the ability to set expiration dates for passwords, require regular password updates, and track when and by whom passwords are accessed. It's important for organizations to carefully evaluate their needs and choose a password vault that meets their specific requirements.

Implement multi-factor authentication (MFA) for privileged accounts. MFA adds an extra layer of security by requiring users to provide additional information beyond a username and password to verify their identity. This can include a code sent to a phone or a biometric scan. Implementing MFA for privileged accounts helps to

prevent unauthorized access and protect against potential security threats.

Regularly review and audit access to privileged accounts. To ensure that privileged accounts are being used appropriately and that access controls are effective, it's important to regularly review and audit access to these accounts. This can include checking for any unauthorized access, evaluating the strength of passwords, and reviewing access controls.

Regularly review and audit access to privileged accounts. To ensure that privileged accounts are being used appropriately and that access controls are effective, it's important to regularly review and audit access to these accounts. This can include checking for any unauthorized access, evaluating the strength of passwords, and reviewing access controls.

This can be done through using a PAM monitoring solution to track and alert on suspicious activity related to privileged accounts. PAM monitoring solutions can help organizations identify potential security risks and take timely action to mitigate them.

There are several PAM monitoring solutions available, including StealthINTERCEPT, eGrc Cloud, and Alsid.

These products offer a range of features, such as the ability to monitor for unusual activity related to privileged accounts, alert on potential security risks, and provide detailed logs for auditing purposes. As with password vaults, it's important for organizations to carefully evaluate their needs and choose a PAM monitoring solution that meets their specific requirements.

Implement training and awareness programs for employees. To help prevent accidental or intentional misuse of privileged accounts, it's important to provide employees with training and awareness programs. This can include educating them on the importance of secure password practices, the risks of sharing passwords, and the consequences of unauthorized access to privileged accounts.

By following these steps, organizations can effectively manage privileged accounts in a secure and compliant manner. By taking a proactive approach to privileged account management, organizations can protect themselves and their stakeholders from potential security threats and the risk of fines and reputational damage under GDPR.



# Conclusion

Effective management of privileged accounts is essential for the security and compliance of any organization. While the challenges of privileged account management, including the need to balance access with security, the complexity of managing multiple accounts, and the need for compliance with relevant laws and regulations, can be daunting, there are practical steps that organizations can take to effectively manage these accounts in a secure and compliant manner.

By establishing a clear and GDPR-compliant process for requesting and granting access, using a PAM tool to securely store and manage privileged accounts, implementing MFA for added security, regularly reviewing and auditing access, and providing training and awareness programs for employees, organizations can effectively manage privileged accounts and protect themselves and their stakeholders from potential security threats and the risk of fines and reputational damage.

It's important to note that privileged account management is just one aspect of a comprehensive data protection strategy. In addition to managing privileged accounts,

organizations should also consider other measures such as implementing robust network security, conducting regular risk assessments, and regularly reviewing and updating their data protection policies and procedures.

Implementing a password vault and PAM monitoring solution can help organizations effectively manage privileged accounts and protect themselves from potential security threats. However, it's important to note that these tools are only one aspect of a comprehensive data protection strategy. In addition to using a password vault and PAM monitoring solution, organizations should also consider other measures such as implementing robust network security, conducting regular risk assessments, and regularly reviewing and updating their data protection policies and procedures.

It is also essential for organizations to regularly review and audit their use of privileged accounts, as well as provide training and awareness programs for employees to promote secure and compliant practices. By taking a holistic approach to data protection, organizations can ensure that they are well-equipped to protect sensitive data and systems from potential security threats.

By taking a holistic approach to data protection, organizations can ensure that they are well-equipped to

protect sensitive data and systems from potential security threats.