How to Audit Privileged Access Management

strongdm

Table of Contents

A lineup of **“Pams”** wearing superhero costumes with a message above them that reads **“Audit PAM because some users are not so super.”**

01

How to Audit Privileged Access Management

It's easy to assume that individuals with privileged access will inherently do the right thing, or simply know what they're doing when accessing systems. That isn't always the case. Similarly, how often do you check in on your systems with privileged access to understand what they're up to?

Since privileged access management (PAM) helps you protect critical assets and prevent unwanted changes to your network, it's critical that you include auditing as an essential component of your PAM strategy.

Auditing privileged access management ensures that all users in your network adhere to the PAM policies that your organization has established. It is the process of taking inventory of privileged accounts, understanding each account's access, and analyzing and monitoring each account's activity.

So how do you get started with auditing privileged access management? The auditing approach below will help you **establish a culture of security** within your organization, so you can be confident that your critical assets are safe.

02

Take Inventory | Identify Privileged Users (Human or Otherwise)

First, take an inventory of privileged accounts. Make a note of any users, human or machine, with the ability to modify networks and devices, add and update user profiles and privileges, or access confidential and sensitive data.

These may include:

- Human users with administrative permissions, including the ability to execute commands, make system changes, and grant or revoke access.
- Service accounts with the capacity to interact with an operating system, make changes, and run scheduled tasks.
- Ephemeral infrastructure, including containers, Kubernetes, and serverless frameworks.
- Users outside of your organization, like third-party vendors and contractors.
- Privileged business users with access to sensitive data.

03

Record and Replay | Monitor Privileged Users

After you establish who has elevated access in your organization, you can begin to track and record privileged user activity. When auditing PAM, continuous observation is vital. According to Verizon's 2021 Data Breach Investigations Report, more than fifty percent of security breaches take months to detect. Consistently locating and monitoring privileged accounts helps you discover accidental or malicious handling of your data and critical systems before it becomes a problem.

Session recording and replay tools provide a contextualized understanding of who performed a behavior and when. You can monitor privileged accounts in real time or replay sessions for incident management, training, or compliance.

As a guard rail against access control violations, host your session logs outside of the database they are monitoring, and restrict write access for log admins to ensure that users cannot modify the data from the original input.

When auditing PAM, look for session monitoring tools that:

- Track every keystroke of an SSH or RDP session.
- View kubectl commands, API calls, and other k8s interactions.
- Observe queries from a variety of datasources.
- Record HTTP calls, including the headers and completion time.
- Monitor access gestures such as login attempts, user updates, and role changes.
- Collect and save audit logs from all sessions.

Retain access logs and other session monitoring data according to the regulatory requirements established in your PAM policy. A good rule of thumb is to keep your logs available for search and analysis for 90 days and retain encrypted archives for up to a year.

04

Harness SIEM Tools | Analyze Privileged Account Activity

Next, it's time to analyze your logs. Modern Security Information and Event Management (SIEM) tools use machine learning to detect anomalous behavior and send alerts when user activity falls outside of the norm. These tools aggregate data from multiple sources, allowing you to correlate user access logs with other security events. More-detailed audit logs will yield richer SIEM outputs.

Favor tools that track:

- The addition or suspension of privileged users.
- Access of critical information, including protected or sensitive data.
- Signs of anomalous activity, like large file deletions.
- Updates to user roles or permission levels.
- Administrative changes to databases or servers.

SIEM tools generate a broad view of network activity while keeping a close eye on problems. They perform forensics if a security incident occurs and help prevent attacks by detecting unusual traffic patterns. Additionally, these tools can scan through a large volume of alerts from multiple systems and help you prioritize those with the highest risk to your organization. Not only does this save admins time and frustration, it also helps them determine the next right action to address the threat.

05
Consider the Human Element | Review Privileged User Behavior

The last step in auditing PAM is auditing people.

Taking inventory gave you an overview of what to monitor. Session recordings gathered information about your network. And SIEM tools scanned that information to detect anomalous behavior. But PAM is only as effective as the humans who use it.

A 2018 survey by Accenture found that one in five healthcare employees would be willing to sell login credentials and other confidential data to unauthorized parties. Other industries are also at risk.

Thankfully, consistent, high-quality PAM auditing can make a difference. When it comes to security, regular access reviews help to establish collaboration among departments, limiting the negative impact of bad actors and ensuring that any unmanaged accounts are properly deactivated.

06
Privileged User Activity Auditing

When to Review
Audit privileged access at least once a year, plus any time significant changes occur in your organization. Have HR trigger an access review any time an employee leaves or changes roles. Additionally, managers should initiate access reviews after time-limited projects end to ensure that IT revokes temporary access when it is no longer necessary.

Who to Evaluate
Pay close attention to users with elevated privilege or those in high-turnover categories, including:

- **IT admins and developers** who can make system changes and grant or revoke permissions for other users. They pose the greatest risk to your business should they decide to do harm.
- **Contractors and third-party vendors** who require temporary access, increasing the potential risk of forgotten accounts. Left unmanaged, these accounts represent an enticing back door for would-be attackers.
- **New hires, exiting employees**, and current staff who are changing roles within the organization. As roles change, so do access needs. Without proper monitoring, unused systems may go unmanaged and eventually be forgotten.

How to Respond

If any stage in your review reveals unwanted behavior, take action to remedy the problem.

- **Restructure or eliminate shared accounts**. When teams share passwords across multiple systems, accounts become difficult to manage. Replace shared passwords with individual credentials, and educate your workforce about the security risks of account sharing.
- **Revoke privileges or terminate employment.** Depending on the transgression it's necessary to consider restricting access to subsets of data or granting read-only rights. Limiting access in this way adds security to your
- **Decommission any unmanaged accounts.** If you are terminating employment, follow the procedures outlined in your organization's offboarding checklist to ensure a clean break.
- **Revise policies to maintain clarity.** If your audits reveal unmanaged accounts, insufficient education, or a lack of security barriers for your employees, review your mistakes and update your PAM documentation and technologies to better support you moving forward.

07

Conclusion | Auditing PAM with strongDM

Consistently auditing privileged access management will help your workforce adhere to secure access policies and will help you detect and respond to security breaches before they escalate. Manual methods for auditing PAM are inefficient and haphazard, but technology is here to help.

strongDM simplifies your workflow with automated access, session monitoring, and custom tool integrations, so you can be confident that your infrastructure is secure. Here's how:

Happy admins, well-managed accounts. strongDM allows admins to grant and revoke access to your entire infrastructure from a unified control plane. This makes it simple to implement least-privilege access without all the administrative busywork.

Credential leasing is built in. Many organizations fail to rotate passwords, or they attempt to do so using manual techniques like spreadsheets. strongDM delegates secret management to established tools, allowing you to vault and rotate sensitive credentials automatically.

Session monitoring is a given. strongDM tracks every query, keystroke, and access attempt and generates human-readable logs that you can send to your SIEM tools so you always know what is happening in your network.

Offboarding is easy. No more worrying that former employees will walk away with access to critical data and systems. strongDM ties authentication to your existing SSO and allows admins to revoke all access at once.

strongDM simplifies user access, freeing up time and energy for HR, IT, and Security teams alike. After all, auditing PAM is about more than just protecting your data. A clear, consistent strategy provides the peace of mind that your critical assets are safe.

If you want to learn more about how strongDM can simplify privileged access auditing for your organization, contact one of our experts today for a free demo.

strongdm

strongDM's infrastructure access platform gives every business secure access controls in a way folks love to use. Trusted by the Fortune 500 to fast-growing businesses like Peloton, SoFi, Chime, Yext, and Better, strongDM gives businesses the control and visibility they need at the speed they want with one platform that works for every environment. strongDM is intentionally distributed. Head to **www.strongdm.com** to learn more.