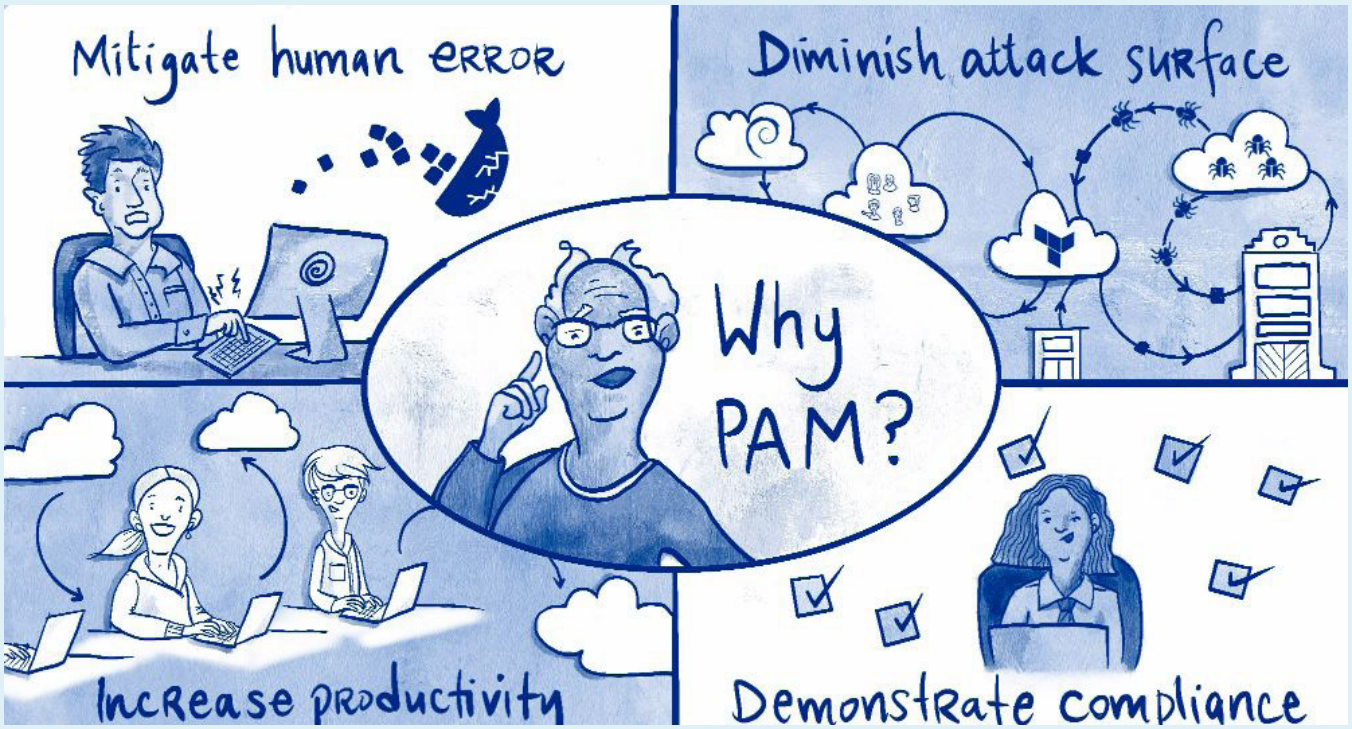
Understanding Privileged Access Management (PAM)

TOOLS AND TECHNIQUES TO HELP SAFEGUARD YOUR CRITICAL ASSETS

strongdm

Table of Contents



TL;DR

In this article, we will take a big-picture look at **Privileged Access Management (PAM)** and how it compares with other access management concepts. You'll learn about the different types of privileged accounts, the risks associated with those accounts when they go unmanaged, and how you can use PAM to mitigate these risks. By the end of this article, you'll have a clearer understanding of how PAM works, the key problems it addresses, and the methods modern businesses use to prevent cyberattacks, improve compliance, and reduce operational complexity.

01

What is Privileged Access Management?

Privileged access management (PAM) encompasses the policies, strategies, and technologies used to control, monitor, and secure elevated access to critical resources for human and service accounts.

PAM strategies enforce the principle of least privilege, restricting account creation and permissions to the minimum level a person requires to do a job. Least privilege helps prevent the spread of malware, decreases your cyber attack surface, improves workforce productivity, and helps demonstrate compliance.

Privileged access control provides security teams with fine-grained governance over sensitive systems and the ability to monitor how privileged company resources are being used. Whether your organization is a three-person startup or an enterprise giant, privileged access management done correctly will protect you against cybersecurity threats and prevent catastrophic user error while improving workflow and policy compliance.

PIM or PAM?

Privileged access security is a jargon-rich category, so let's begin with a quick look at similar and related terms. Although there is a clear difference between IAM and PAM, many of these acronyms overlap. Furthermore, industry leaders sometimes use terms interchangeably, leading to greater confusion. The important thing to understand is not the acronyms but the functionality they represent.

Type	Detail
Identity and access management (IAM)	A term with broad scope, encompassing the processes, policies, and tools involved in authenticating access to ensure that the right users can connect to the right resources at the right time.
Privileged access management (PAM)	A subset of IAM, focused on defining and controlling who or what has the authority to make changes to a network or device. PAM establishes policies and practices to ensure the security of sensitive data and administrative accounts.
Privileged account management (PAM)	A subset of privileged access management, this PAM focuses specifically on managing accounts that you have defined as privileged.
Privileged identity management (PIM)	Often used interchangeably with privileged access management, PIM involves managing which resources privileged users can access. PIM is also the name of a service inthat controls and monitors access to crucial resources.
Privileged session management (PSM)	A feature of good PAM tools, PSM allows administrators to control, monitor, and record privileged access sessions. Privileged session management may include SSH and RDP logging, remote session monitoring, auditing and reporting, and workflow coordination.

This article will focus primarily on the first two terms—namely privileged account management and how it fits into a larger IAM strategy. But first—what qualifies as a privileged account?

02

Types of Privileged Accounts

An effective IAM strategy includes managed access to both privileged and non-privileged accounts. Although it may seem counterintuitive, increasing the number of accounts in your organization can reduce the attack surface. With PAM best practices, even the highest level users will connect with non-privileged access 90% of the time, with IT staff using non-privileged accounts for day-to-day activities and only using privileged accounts to adjust permissions, change critical data, or perform other critical actions.

Non-privileged accounts include:

- **Standard user accounts:** These accounts meet the needs of typical business users: email, web browsing, and word processing, plus role-based access to SaaS tools for communication and project management.
- **Guest user accounts:** These accounts have limited privileges, including basic application access and internet browsing.

Privileged accounts, on the other hand, allow systems administrators to change settings for large groups of users, override or bypass security restraints, and even configure and provision systems, cloud instances, and other accounts. Privileged accounts occur in two broad categories: human (user accounts) and machine (service accounts), and exist in nearly all connected devices, servers, databases, and applications. Let's take a closer look.

Privileged User Accounts:

Type	Detail
Superuser account	Also called root, admin, administrator, or supervisor, this account grants specialized IT employees nearly unlimited privileges over a system. This includes the ability to execute commands, make system changes, create and modify files and settings, and grant or revoke permissions for other users.
Domain administrator account	Also called domain admin, this is a Windows user account that can edit information in Active Directory (AD), including creating and deleting users and changing user permissions.
Local administrator account	A local admin account allows a user to access and make changes to a local Windows machine but lacks the ability to modify information in AD for other users.

Type	Detail
SSH keys	Secure socket shell (SSH) keys are access credentials that provide direct root access to Unix-like operating systems, often over a remote connection. Administrators use them, much like usernames and passwords, to implement single sign-on.
Emergency account	Also called break glass or firecall account, this account allows unprivileged users to bypass the access controls in a secure application in the event of a crisis.
Privileged business users	These are users in finance, marketing, human resources, and other roles who require limited access to sensitive systems.

Privileged Machine Accounts

Type	Detail
Application account	Applications use these highly privileged accounts to access databases, run batch jobs or scripts, and confer access to other applications.
Service account	Among the highest risk privileged accounts, services use these accounts to interact with the operating system, make changes, and run scheduled tasks.
Active Directory service account	Also called domain service account, this type of account enables a service to interact with the operating system, managing users and computers, organizing data, and changing passwords.
SSH keys	Automated processes use SSH keys to gain access to firewalls, routers, and switches.
Secret	Also called privileged credentials, secrets include API keys, passwords, SSH keys, tokens, and certificates that allow both human and service accounts to securely authenticate to privileged systems.

03

Defining Privileged Accounts for Your Organization

Ultimately, defining privileged accounts is the responsibility of each organization. Activities typically requiring privileged access include:

- granting and revoking access for other users
- connecting to sensitive data, and
- configuring, provisioning, and managing infra-structure

Which accounts require privileged access will vary by organization and by industry.

Begin by defining roles for users and outlining required privileges and access rights for those roles. Remember to limit access by scope as well as time. DevOps admins need different permissions than summer interns, and privileges change when people leave or change roles within the company.

Next, consider which systems you would need to recover first in the event of an attack—those containing sensitive data, high-level permissions, and the ability to configure and access other systems. Remember that these may be human or service accounts.

Finally, review the access needs of third-party vendors. In the massive 2013 Target breach, hackers gained access to sensitive data through an HVAC contractor. Privileged access should be limited to vendors who need it and revoked when they finish the job.

Taking these steps will help you limit or even eliminate one of the most common weak points organizations face: unmanaged privileged accounts.

04

Why Privileged Accounts Go Unmanaged

In an effort to increase uptime and reduce complexity, IT admins may over-provision users. Employees may retain access when they leave or change roles within the company. And devices and services may retain default privileged access. Furthermore, security blind spots, poor secrets hygiene, and lack of visibility can result in broad, unmanaged access to sensitive assets and data.

Some reasons privileged accounts go unmanaged:

Type	Detail
Too much access	Restrictive access controls can disrupt user workflow. As a result, overworked admins may attempt to improve productivity and reduce frustration among users by granting too much access. Over-provisioned accounts are then forgotten or unmonitored, opening the door to risk.
Privilege creep	When employees receive promotions or change roles within a company, they often retain access to systems they no longer need. Admins often add access based on the new or expanded role without revoking access to systems the employees no longer use. Without monitoring, these systems go unmanaged and may eventually be forgotten.
Zombie accounts	Also called orphaned or abandoned accounts, these result when an employee leaves the company and privileged access is not disabled. Additionally, some accounts may be utilized less often until they become obsolete or forgotten.
Unchanged defaults	Service accounts often possess privileged access by default. Such applications, systems, and devices commonly ship with embedded credentials that are easy to guess and represent prime targets for malicious actors.
Static credentials	Rotating and updating privileged credentials can be manually intensive and error-prone, resulting in default passwords that are never disabled and static passwords that are not rotated or have no expiration date.

Type	Detail
Password sharing	When the same admin account manages multiple service accounts or IT teams share passwords across multiple systems, it becomes difficult to audit and manage privileged accounts. Additionally, phishing schemes, re-used passwords, and easy-to-guess passwords can also open the door to account mismanagement.
Lack of monitoring	A final note here: although insufficient oversight will not create unmanaged accounts, it certainly compounds the issue. You can't correct what you can't see. As a result, unmanaged accounts may linger, becoming threat vectors that open the door to attack.

05

Why is Privileged Access Management Important?

PAM Security matters. Whether through malice or mistake, unmanaged accounts present many privileged risks to your organization.

When admins provide too much access in an effort to reduce friction, users who lack the proper expertise may accidentally mistype a command or delete an important file—causing catastrophic damage to your organization. Too much access may take the form of unnecessary privileges for a single user. It may also result from password sharing, with multiple people using the same privileged account. Additionally, admins may try to simplify network access by allowing a single account within your organization to operate multiple services or applications. A mistyped command on such an account could cause far-reaching damage, impacting systems across your network.

Beyond human error, disgruntled former employees who retain privileged access or cybercriminals who uncover forgotten credentials may gain control over sensitive data, privileged information, and powerful systems. Bad actors can use stolen credentials to gain access to your network and then move laterally, progressively searching for the key data and assets they can use to damage your operations.
Even privilege creep poses a security risk. An

employee may change roles and retain unneeded access, gradually accumulating rights beyond what is required. Such employees may connect to an unmanaged account and perform unauthorized tasks, whether in error or intentionally. Privilege creep, especially among bad actors with insider know-how, can cause incalculable harm.

Because privileged account holders can make administrative-level changes to your network, and because they can access confidential and sensitive data, they represent an elevated threat vector for your organization. A comprehensive PAM policy will help limit this vulnerability.

06

How Privileged Access Management Works

A privileged management system secures your network and enhances visibility while reducing operational complexity.

Type	Detail
Managing access privileges increases security	at the most basic level by limiting the opportunities for user error and malicious attacks. PAM allows organizations to prevent and respond to external and insider threats. It reduces the cyber attack surface by establishing least-privilege access for humans, processes, and applications. This diminishes the routes and entries an attacker can use to gain a foothold and limits the scope of damage should a breach occur.
Centralizing administrative access reduces operational complexity.	As we've seen, granting broad access to privileged accounts could result in security breaches and major disruptions. PAM takes a more holistic approach to improving workflow. Without PAM, administrators may follow a different protocol for each system, often across multiple networks. With an effective privileged access management framework in place, admins manage critical accounts from a central location. Additionally, users access the systems they need without having to remember multiple passwords using single sign-on integration. This leads to greater productivity and reduced frustration.
Privileged activity monitoring enhances visibility across your network.	With privileged session management, the superuser can easily identify and respond to problems in real time. Admins can observe the activity of every privileged user—from employees to devices to third-party vendors—from beginning to end. Privileged session management improves more than just security. With monitoring tools in place, a comprehensive PAM solution simplifies auditing and compliance requirements, helping your organization comply with regulations like SOC 2, ISO 27001, GDPR, HIPAA, and DSS.
Privilege Management secures cloud-forward and hybrid remote access.	Distributed and even fully-remote workforces are becoming the norm—this means more software as a service (SaaS) applications, infrastructure automation tools, and service accounts connecting from multiple locations. With these privileged accounts increasingly outnumbering humans in an organization, companies require something more granular than a VPN to secure access to cloud and hybrid environments.

07

Privileged Access Management Requirements

So far, we've taken a zoomed-out look at PAM. We identified a few important terms, including the definition of privileged access management as well as IAM, PIM, and PSM. Next, we summarized different types of privileged accounts, common threat vectors, and the benefits of privileged access management for organizations of any size.

The next few sections will dig deeper into the requirements and best practices for your privileged access management solution and cover strategies for implementing them, with a special focus on the important features of PAM tools.

Specific Criteria

Type	Detail
Write a formal policy for privileged accounts	defining roles within your organization and outlining required privileges and access rights for each role. Take a look at the privileged account types we defined in this article. Which of these do you have in your organization? Who needs access to them and for how long? Can you segment networks and systems to make it easier to contain a breach should one occur?
Change or remove embedded credentials	default IDs, and passwords for privileged service accounts and devices. Remember, machine accounts often ship with excessive privileges and easy-to-guess passwords. Take an inventory of all such systems and update privileges and credentials to match the needs of your organization.
Educate your workforce	about security best practices to ensure strong passwords, guard against phishing, and eliminate password sharing. Regularly rotate credentials, implement multi-factor authentication, and use SSO to keep passwords hidden. Empower your users to be proactive when it comes to security.
Enforce the principle of least privilege	for both human and machine accounts. Restrict account creation and permission levels to the exact resources a person or system needs to fulfill a defined role. When appropriate, set a date when privileged access will expire. Pay special attention to PoLP with onboarding and termination, or when current employees shift roles in the organization.

Type	Detail
Inventory cloud applications, SaaS accounts, and other third-party systems	Be sure employees follow the same strict PAM policies with both internal and external resources. Pay special attention to the way contractors and third-party vendors access your network to ensure no privileged accounts go unmanaged.
Vault, rotate, and manage secrets	for privileged accounts in the cloud and on premises—including containerization services, machine learning environments, and infrastructure automation platforms. By limiting the lifespan of passwords and other sensitive credentials, you reduce the risk and impact of an attack.
Monitor, audit, and analyze privileged session activity	Increase visibility into your network so you can detect and correct catastrophic user errors and malicious activity before the problem spreads. Have resource owners perform privileged access reviews yearly, or follow specific regulatory schedules.
Revisit your policies on a regular basis	and ensure that your best practices are up to date. As your organization scales, restructures, or adopts new technologies your security and risk-management needs may change.

08

How to Implement PAM

Today, organizations must manage access in a fast-moving technical landscape comprising multi-cloud and hybrid environments, a distributed workforce, reliance on contractors and third-party vendors, and rapid technological innovation. While these changes lead to enhanced productivity, collaboration, and growth, they also increase the number of security weak points that you may overlook.

How you manage privileged accounts matters. Manual solutions for implementing PAM best practices are insufficient in a modern environment. Even well-intentioned humans are error-prone and may fail to enforce all written policies. Spreadsheets can only track passwords when kept up to date, and they make credential rotation difficult. Moreover, session monitoring and recording—an essential task when auditing privileged access management—must be done on an ongoing basis. Manual auditing enforcement of PAM protocols is inefficient, and may even become impossible in the long term.

This is why businesses of all sizes include PAM tools as part of a privileged access management architecture. Using tools for PAM control allows admins to grant and revoke least-privilege access without disrupting workflow; record privileged sessions; ensure credentials are well handled; and monitor sessions to assist with auditing and compliance.

So, what exactly does a PAM tool do?

7 Essential Capabilities of a PAM Tool

1. SSO integration—Improves user workflow by centralizing access to multiple accounts while keeping passwords hidden.
2. Automation—Replaces cumbersome manual tasks with automated processes to remove administrative busy-work for DevOps and improve policy adherence.
3. Credential management—Vaults and rotates passwords and other credentials to shorten the window of time in which they remain valid.
4. Role-based access control (RBAC)—Restricts network access to authorized users based on their role within the organization, helping to enforce PoLP and avoid privilege creep.
5. Auditing—Records and monitors privileged session activity and provides a clear audit trail.
6. Compliance—Helps your organization comply with regulations like SOC 2, ISO 27001, GDPR, HIPAA, and DSS.
7. Convenience—Secures your infrastructure without disrupting workflow. After all, a tool is only effective if you can actually use it

PAM tools provide a centralized, secure, and observable platform to manage the most sensitive access. They come in many forms. Ultimately, it is up to you to discover which tool is right for your organization.

A quick side note: Some readers have asked if Active Directory is a privileged access management tool. The answer is no—at least, not on its own. Active Directory allows administrators to manage permissions and control access to network resources, but you will need additional support to implement a comprehensive PAM strategy. Fortunately, with the right tool, you can integrate Active Directory with privileged systems and streamline access management for your organization..

09

Using Tools to Expand Your IAM Strategy

As we've seen, managing access in the cloud presents many challenges. The right tools will help your organization control and audit access for all users with confidence, integrating the robust features of PAM within the wider framework of your IAM strategy. A centralized control plane expands on PAM to help you:

Type	Detail
Manage access for all users	A control plane manages access for privileged and non-privileged users, including both humans and service accounts.
Automate user provisioning	Integrate with your preferred identity provider to centralize access to servers, databases, web apps, and Kubernetes. This allows you to provision database credentials, ssh keys, and VPN passwords with ease.
Establish role-based access	Enforce your PAM strategies with built-in user and role management. Give each user just-right access for the correct amount of time to limit the risk of unmanaged accounts.
Audit wisely	Capture every SSH session, database query, and kubectl command with logs a human can actually read. Monitor sessions across your infrastructure in real time, or send them to storage, analytics, and SIEM tools to gain deeper insight.
Offboard with ease	Suspend access to databases, servers, and applications from a central interface simply by revoking SSO. Reduce the risk of zombie accounts while easing the administrative burden for DevOps.
Reduce friction for your distributed workforce	Utilize a control plane to keep track of access for remote workers, vendors, and contractors.

Increase peace of mind. Diminish operational complexity from onboarding to termination, and know that users have exactly the access they need—no more, no less.

10

Conclusion

Many factors threaten the security of your operations—from privilege creep and insufficient offboarding to unchanged default credentials. Accounts left unchecked may create entry points for bad actors or simply open the door to user error.

Thankfully, by outlining security strategies and enlisting the help of PAM tools, you can strengthen your network while smoothing access for privileged users.

And with a comprehensive identity and access management strategy, PAM and IAM work together to ensure all users have the right access when they need it.

Want to learn more? Get a free demo of strongDM.

11

More PAM Resources

- What is the Principle of Least Privilege?
- Migrating PAM to the Cloud
- VPN Alternatives You Need to Know About
- How to Replace Your VPN with strongDM
- Technical Staff Offboarding Checklist
- How to Audit Privileged Access Management
- Rise of the Zombie Accounts: 8 Tips to Protect Your Assets
- IAM vs PAM Key Differences & How They Relate

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.