strongdm

THE 2026 GUIDE TO MODERNIZING ACCESS

Why Legacy PAM Architectures Fail in the Cloud & AI Era, and How to Fix It.

Contents

The Strategic Imperative for Zero Standing Privilege

This research report outlines the critical architectural shift required to secure modern hybrid infrastructure: moving from static "Vault and Rotate" models to Zero Standing Privileges (ZSP). It exposes why legacy Privileged Access Management (PAM) architectures, heavily dependent on jump hosts and credential vaults, cannot scale for the cloud era and demonstrates how a Protocol-Aware approach eliminates the operational friction that drives Shadow IT.

THE FAILURE OF "VAULT AND ROTATE"

Despite significant investments in vaulting and rotation, static credentials remain the primary attack vector for modern breaches. Legacy PAM treats the symptom (password management) rather than the root cause (Standing Privilege). In a cloud environment where infrastructure is ephemeral and Non-Human Identities (NHI) outnumber humans by a factor of 45 to 1, relying on daily password rotation is a failing strategy. If a standing identity exists, it can be compromised.

THE FRICTION-SECURITY TRADEOFF

Legacy tools force a binary choice Security or Speed. Clunky web portals and resource-intensive "Jump Hosts" create bottlenecks, forcing developers to bypass controls just to do their jobs. Modern security must enforce policy at runtime by authorizing specific actions (e.g., "who ran query X?"), not just initial access, and all that without slowing down engineering velocity.

SCOPE OF ANALYSIS

This document analyzes the architectural limitations of traditional PAM and details how StrongDM's Runtime Authorization resolves these deficits by inspecting protocols, eliminating static credentials, and extending control to the modern stack of machines and cloud-native resources.

The Legacy Identity Crisis

Click on the problem statements below to understand why traditional PAM solutions have been poorly implemented, and to see how the StrongDM approach helps organizations to overcome these challenges.

Top 3 Problems with Legacy PAM

→ PROBLEM 1: WHEN ACCESS IS HARD, WORKAROUNDS BECOME THE FAST PATH

1. User adoption is challenging and people are bypassing the system.
2. Extending PAM controls beyond Windows and Linux has proved challenging due to user pushback and product limitations.
3. Adopting Just-In-Time and Zero Standing Privilege needs to be a priority, yet legacy solutions introduce too much friction and enforce these controls unevenly across environments.

→ PROBLEM 2: AS ORGANIZATIONS SCALE, LEGACY PAM BRINGS OPERATIONAL COMPLEXITY

1. Traditional PAM solutions are complex to manage and require significant operational overhead.
2. Legacy PAM struggles to extend capabilities to modern use cases, particularly across cloud environments, SaaS applications, and non-human identities (NHI).
3. Session recordings are captured en masse but reviewing them is highly inefficient, time-consuming and provides minimal value.

→ PROBLEM 3: AS COST SPAWLS, ROI VANISHES

1. Legacy PAM is unaffordable and untenable.
2. Migrating from Legacy PAM requires significant time, effort, and resources.
3. Justifying further investment becomes difficult when risk reduction is unclear.

PROBLEM 1: WHEN ACCESS IS HARD, WORKAROUNDS BECOME THE FAST PATH

1 USER ADOPTION IS CHALLENGING AND PEOPLE ARE BYPASSING THE SYSTEM.

- Users are forced to retrieve credentials or establish connections via a web portal or a limited set of supported clients.
- Connections to target systems take longer than establishing direct connections.
- Limited project resources are drained by time-intensive user training and account onboarding.
- Inconsistent workflows accessing different devices create frustration and pushback.
- Workflows involving manual approval steps introduce too much friction.

SOLUTION - Tooling developers actually want to use.

StrongDM improves buy in and accelerates adoption, ultimately reducing attempts to bypass your controls and increases the return on your investment.

- StrongDM allows users to continue using any native client they currently use, without exposing credentials or needing to access a web portal first, while providing continuous runtime authorization.
- The brokered access is light touch and can improve connectivity speeds for users when compared to e.g., VPNs, Bastion servers and traditional PAM jump hosts.
- Ideal for remote access and to ensure third-parties meet their SLAs.
- The same user workflows apply to all device and application types, from legacy databases through to modern cloud management consoles. A consistent experience is key to avoiding user frustration.
- Approval workflows for Just-In-Time access can be integrated into existing ChatOps solutions (e.g., Teams and Slack) to accelerate the time to request and approve access.

2 EXTENDING PAM CONTROLS BEYOND WINDOWS AND LINUX HAS PROVED CHALLENGING DUE TO USER PUSHBACK AND PRODUCT LIMITATIONS.

- Forcing users to launch sessions through a web portal creates a poor user experience and drives resistance to adoption.
- Legacy 'Jump Host' architectures act as terminal servers, rendering a full GUI for every session. This creates a hard bottleneck, capping at 20-30 sessions per server and incurring expensive RDS Client Access Licenses (CALs) for every user. StrongDM replaces this with a Protocol-Aware Proxy that streams bytes, not pixels, eliminating RDS CALs and scaling to thousands of concurrent sessions per node.
- ‘Native’ user experience workflows are limited to a set of supported clients, typically for RDP and SSH only and require users to modify the connection strings in their clients to communicate with an appropriate set of proxy servers. This becomes complex in large environments with multiple proxy pools and complicates the user training and awareness process.
- Underlying proxy mechanisms use shadow users to launch sessions, making it difficult for users who e.g, require their own personal home profile or need to save personal stored procedures for databases.

SOLUTION - Extending beyond Windows and Linux

By handling access at the protocol level and enforcing authorization at runtime, StrongDM is not limited to supporting specific clients that require connectors to be developed. This becomes critical when extending beyond the basics of RDP and SSH access and is necessary for consistent, native user experiences.

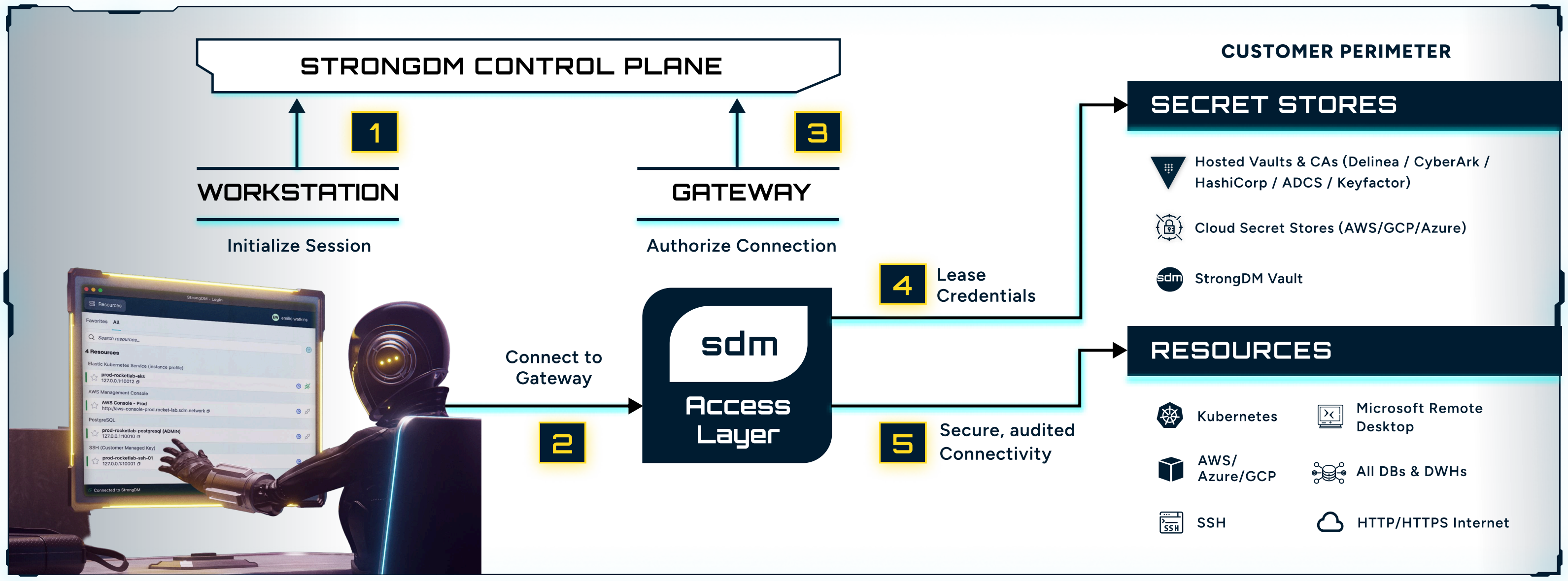
- StrongDM's support at the protocol level means users can continue to access their native tools for a far greater variety of systems than Windows and Linux, this drastically reduces user pushback, simplifies deployment and improves user experience.
- Resource intensive application clients are launched from the users' local machines, removing the dependency on the proxy servers to be heavily scaled.
- The protocol level approach means that a single, lightweight broker is capable of hosting thousands of concurrent sessions regardless of the target system, compared to typically tens or hundreds on significantly heavier infrastructure.
- StrongDM brokers access using a unique, named account per user and launches sessions locally, allowing users to keep their personal settings and configurations without managing credentials.

3 ADOPTING JUST-IN-TIME AND ZERO STANDING PRIVILEGE NEEDS TO BE A PRIORITY, YET LEGACY SOLUTIONS INTRODUCE TOO MUCH FRICTION AND ENFORCES THESE CONTROLS UNEVENLY ACROSS ENVIRONMENTS.

- Introducing JIT necessitates workflows that capture the required time and purpose for performing an activity prior to granting access. Users and approvers have to log into a web portal to request this and it causes frustration and delays.
- The policies and approval workflows differ depending on whether we are connecting to legacy systems or managing access to cloud environments. Features in the PAM solution have been introduced through acquisitions, causing inconsistencies in the way we work.
- Policies and approval workflows vary between legacy systems and cloud environments, creating inconsistent access management practices.
- Some legacy PAM solutions rely on provisioning and deprovisioning for zero-standing access, but this is only supported for a handful of systems.

SOLUTION - Reduce friction for users and approvers by implementing JIT and Zero Standing Privileges without relying on native support from target systems.

- StrongDM integrates with existing ChatOps solutions like Teams and Slack for requests and approvers. Users access systems through the same tools and workflows they already use.
- Access can be requested and granted via existing chat channels, significantly accelerating the time to gain JIT access. Extrapolated across an organization, this drastically increases productivity.
- StrongDM can default to a zero standing access approach regardless of system type, by removing the ability for a user to connect out-of-band and will grant access following a successful JIT approval request.
- True Zero Standing Privilege (ZSP) isn't about faster provisioning; it's about Just-In-Time injection.
- StrongDM issues ephemeral, short-lived certificates or injects credentials at the protocol level only for the duration of the request. When the session ends, the access artifact evaporates. There is no credential left on the device to be stolen.



PROBLEM 2: LEGACY PAM BRINGS OPERATIONAL COMPLEXITY THAT DOESN'T SCALE

1 TRADITIONAL PAM SOLUTIONS ARE COMPLEX TO MANAGE AND REQUIRE SIGNIFICANT OPERATIONAL OVERHEAD.

- Password verifications and rotations fail, requiring troubleshooting and leading to accounts with exclusive usage becoming locked.
- Connectors need developing and maintaining to extend our rotation capabilities beyond traditional infrastructure.

- Application clients deployed to PAM proxy servers need updating and maintaining across multiple servers.
- The solution requires manual interaction to perform upgrades, failovers and fallbacks.
- Approvers are continuously having to log into a web portal to approve requests for access.
- Connectors to web portals are breaking when the application is updated.

SOLUTION - StrongDM minimizes administrative effort allows users to focus and resources on continued expansion and adoption of the solution.

- StrongDM not only acts as a standalone solution, but is vault-agnostic and allows you to integrate with existing vaulting solutions. This allows you to gradually phase out the reliance on password management in favour of ephemeral access, e.g. short-lived certificates, orchestrated by StrongDM.
- By operating at the protocol level, we remove the need to build and maintain connectors for specific application clients.
- Access to web-based applications remains stable even when the user interface changes.
- Approvals for access requests can be made natively within existing ChatOps applications like Slack or Teams.
- The infrastructure installation and configuration is fully automatable, can be auto-scaled and handles its own failover mechanisms, significantly reducing the overhead associated with upgrades, maintenance and resiliency.

2 LEGACY PAM STRUGGLES TO EXTEND CAPABILITIES TO MODERN USE CASES, PARTICULARLY ACROSS CLOUD ENVIRONMENTS, SAAS APPLICATIONS, AND NON-HUMAN IDENTITIES (NHI).

- Machine identities now outnumber humans 45:1. Legacy vaults cannot manage the velocity of automated CI/CD pipelines or autonomous AI agents that require instant, high-frequency access to infrastructure.
- Traditional PAM solutions were designed to manage relatively static infrastructure, primarily hosted on-premise. Extending these capabilities to the cloud often requires bolting on additional modules.
- User experience in a developer-driven world is more critical than ever as velocity is key. Developers do not want to use PAM web portals or a limited subset of tools to do their jobs.
- SaaS PAM solutions often require sensitive data to traverse the internet back to their cloud-hosted backend and introduces challenge for data residency.
- Role-based policies are not dynamic enough to handle real time access to short-lived target systems.
- Additional infrastructure is required to support specific types of target systems, increasing operational overhead and underlying costs.
- Support for web consoles is unreliable because frequent interface updates can disrupt how PAM solutions inject credentials into the correct user fields.

SOLUTION - StrongDM was built natively for cloud and hybrid infrastructure, eliminating the need to retrofit legacy architectures for modern environments. It delivers a unified identity-centric control plane across on-prem and cloud resources alike—applying the same runtime authorization, policy enforcement, and seamless user experience to static infrastructure and dynamic cloud environments.

- StrongDM acts as the unified access layer for humans and machines, applying Zero Trust policies at runtime. This eliminates secret sprawl and ensures consistent authorization and auditability for every identity, regardless of the application type across any modern environment.
- Privileged users, including developers who primarily leverage CLIs, can use the tools they would use natively from their desktop to interact with target systems. StrongDM focuses on the protocols and not the application clients or fields on a web interface.
- As a hybrid SaaS solution, data storage can be configured granularly to ensure data residency requirements are met and secrets/credentials can be kept within an organization's own environment if preferred.
- StrongDM can be used to extend the capabilities of an existing PAM solution to enable seamless access for modern use cases.
- There is no need for multiple connector types, HTML gateways and remote access portals. The infrastructure is lightweight, automatable, scalable, consistent and suitable for all use cases.

3 SESSION RECORDINGS ARE CAPTURED EN MASSE BUT REVIEWING THEM IS HIGHLY INEFFICIENT, TIME-CONSUMING AND PROVIDES MINIMAL VALUE.

- Internal policies and external regulations require privileged sessions to be recorded and retained. Storing these recordings demands significant storage capacity, increasing overall total cost of ownership.
- Random or sample-based session reviews rarely deliver meaningful insight. During incident investigations, correlating the target system's user ID with the actual end user who accessed the account is time-consuming and inefficient.
- Geographically distributed operations must comply with multiple local data residency regulations. Legacy PAM solutions make it difficult to segregate session recordings at a granular level without deploying additional instances, increasing complexity and cost.

SOLUTION - Reduce costs by capturing session recordings efficiently and use the access broker to proactively prevent malicious activity.

- Session audits are captured in a storage-efficient format optimized for each protocol. For example, RDP sessions are recorded as byte streams rather than large AVI or MP4 video files. Text-based activity can be reconstructed into a video-like playback experience, providing intuitive review without the storage burden of traditional screen recordings.
- Reduce audit storage costs by up to 90 percent while making session data fully searchable.
- A modern approach captures the underlying protocol stream—text and commands instead of pixels —transforming what would be a 500 MB video file into a roughly 50 KB text log. The result is audit data that can be searched instantly using tools such as grep or a SIEM to identify specific commands.
- If data residency requirements apply, a distributed architecture enables session recordings to be stored locally within each region. Recordings can be retained on regional brokers or directed to approved storage services such as Amazon S3 buckets.
- If data residency is not a concern, StrongDM will host recordings for 13 months for no additional charge.
- The StrongDM broker continuously evaluates the context of a session, allowing additional friction to be applied where necessary including the termination of a session, prompting for additional authentication or even preventing specific database commands. This reduces the dependency on session reviews that focus on specific commands or signals, or allows admins to easily identify conflicts against policy using built-in reports.

PROBLEM 3: AS COSTS SPRAWL, ROI VANISHES.

1 LEGACY PAM IS UNAFFORDABLE AND UNTENABLE.

- Vault-based architectures require manual discovery, onboarding, and credential rotation for each account—an operationally heavy process that breaks legacy workflows.
- Organizations typically vault only Tier 0 assets, leaving thousands of local admin, service, and cloud accounts unmanaged because onboarding them is too complex and resource-intensive.
- Additional RDS CAL and/or SQL Cluster licensing costs for brokering and resiliency purposes are expensive.
- Session recordings, particularly for graphical interfaces like Windows uses a considerable amount of storage.
- The proxy servers are resource-intensive and require scaling both horizontally and vertically to manage concurrent sessions.
- Multiple types of connector and proxy servers need to be deployed and maintained to handle access to varying target systems.
- Third-party load balancing and higher-availability solutions are required to provide resiliency.
- Additional PAM licensing is required to support different personas and interactive use cases.
- Reviewing access and preparing audits takes a considerable amount of time and resource as reports are outdated and provide limited information.
- Time spent granting system access is time diverted from driving business productivity.

SOLUTION - Leverage a lightweight, modern platform that minimizes reliance on third-party licensing, reduces compute and storage costs, and lessens time spent on repetitive tasks.

- StrongDM provides built-in resiliency and failover mechanisms, eliminating the need for third-party clustering licences or load balancing solutions.
- Session audits and recordings are captured efficiently, reducing storage requirements against traditional PAM solutions by approximately 70%.
- The StrongDM tunneling approach does not require RDS CAL licensing or any other third-party licenses to proxy connections.
- StrongDM covers modern use cases, including cloud and SaaS applications requires no additional features to be licensed or deployed.
- Modern, extensive reporting and dashboard capabilities allow internal teams to rapidly obtain the information they need to prepare for audits and for security teams to improve their JIT/ZSP posture.

2 MIGRATING FROM LEGACY PAM REQUIRES SIGNIFICANT TIME, EFFORT, AND RESOURCES.

- Years of maturing access controls and auditing standards have created a rigid policy framework that is difficult and time-consuming to translate into a new platform.
- Extensive manual effort was invested in building custom connectors for legacy infrastructure, creating a significant engineering hurdle to replicate in a modern tool.
- The entire workforce, from administrators to end-users, is specialized in the current system, making the cost and time of enterprise-wide retraining appear insurmountable.
- Existing access is brokered through complex proxy server pools and hard-coded firewall rules, requiring a high-risk, massive network re-architecture to change.
- Many accounts were engineered specifically to fit the current solution's onboarding workflow, and there is no organizational appetite for the mass re-engineering required to move them.
- Subscription and maintenance renewal cycles rarely align with migration timelines, creating a perpetual "wrong time to move" loop that stalls decision-making.
- The financial burden of paying for the legacy subscription while simultaneously funding a new implementation is considered budget-prohibitive.

SOLUTION - Migration can be phased and cost effective if the platform you move to can augment your existing investment.

- StrongDM integrates with existing PAM solutions, preserving established access controls and credential rotation policies while enabling users to shift away from passwords wherever possible over time.
- By acting as the access layer, organizations can seamlessly improve the user experience by migrating individual teams to StrongDMs native ways of working.
- Resource intensive infrastructure can be deprecated in place of lightweight StrongDM gateways, saving on compute and storage costs in the short term.
- Migrating specific teams and business functions allows you to reduce the licensing dependency on the existing PAM solutions.
- Adopt a 'Cap and Grow' strategy. Don't rip and replace immediately. Keep your legacy Vault for 'break-glass' root accounts, but migrate all high-volume, day-to-day human and machine access to StrongDM. This delivers immediate user experience wins without the trauma of a full migration.

3 JUSTIFYING FURTHER INVESTMENT BECOMES DIFFICULT WHEN RISK REDUCTION IS UNCLEAR.

- Many solutions focus on onboarding, vaulting and rotating credentials, so it's natural to use these figures as metrics to determine adoption, but this is not an accurate way to measure risk reduction.
- When passwords can be viewed, it becomes very difficult to measure the efficacy of PAM controls unless the admin also tracks access outside of the intended brokering mechanism.
- Standing access creates a significant attack surface that can be exploited for lateral movement or privilege escalation, regardless of periodic rotation of credentials
- Traditional solutions attempt to verify trust at the point of a user connecting to a session, but do not continuously evaluate the context afterwards.
- In instances of malicious activity, reactive controls like feeding events to a SIEM are not enough. Security operations teams are inundated with alerts and the time to respond is usually greater than the time it takes an attacker to establish a level of persistence.

SOLUTION - Pivot metrics from 'Vaulted Accounts' to 'Controlled Interactions' by adopting universal privileged access authorization and implementing proactive prevention rather than reactive detection.

- Stop measuring success by how many passwords you rotated. Measure success by reduction in standing privileges and the percentage of sessions that are inspected in real-time.
- Not all accounts are equal, align the weighting of risk reduction against the sensitivity/criticality of the account. Use a tiering model as a foundation and apply your own business logic to refine this further.
- The ability to measure access to accounts that are not onboarded is critical, and is unlikely to be addressed by PAM alone. Introduce preventative measures to reduce the likelihood of out-of-band access using ephemeral access where possible, for example - only allowing interactive access via short-lived certificates that are managed or orchestrated by StrongDM.
- StrongDM provides built-in reporting capabilities that focus on Zero Trust principles including Just-In-Time and ephemeral access control adoption.
- Use StrongDM to continuously verify the context of all active sessions. Integrate with EDR tooling to enhance the intelligence of signals being evaluated.
- Leverage StrongDM policies to prevent specific malicious activities from occurring, and use the built-in reporting to identify instances where these actions have been blocked.

strongdm

StrongDM is the universal access management company reimagining privileged access management. Built for enterprises managing explosive growth in both human and machine identities, StrongDM provides real-time authorization enforcement that governs privileged actions across infrastructure, applications, and cloud environments — not just initial access. The platform unifies traditional PAM capabilities with advanced authorization controls, evaluating identity, context, and policy to authorize or block every privileged operation. Security teams gain action-level visibility and control, while end users experience frictionless access. StrongDM enables organizations to evolve toward continuous, context-aware identity governance.

STRONGDM.COM