Devolutions

Why essential SMB cybersecurity preparation must include PAM

OCTOBER 2025

TABLE OF CONTENTS

Small and mid-sized businesses (SMBs) run on a small set of people and systems that hold the keys to everything important: domain controllers, cloud consoles, payment systems, source code, and customer data. These keys are privileged access. When the right person has the right privilege at the right time, work flows. **But when privilege is unmanaged, outages take longer to resolve, audits become harder, and attackers get a shortcut to the "crown jewels."** That is where privileged access management (PAM) enters the picture.

PAM is a simple idea with outsized impact: keep elevated access rare, short-lived, and well governed. PAM centralizes secrets in a vault, issues access just in time rather than leaving standing admin rights, records sensitive sessions, and automates password and key rotation. **When done properly, PAM shrinks the blast radius of mistakes and attacks, and it gives executives clear, confident answers to board, customer, and insurer questions about how sensitive access is controlled.**

In this white paper, we dive into the PAM-SMB landscape and:

- **Define privileged access** in practical SMB terms and explain how PAM complements broader identity and access management.
- **Diagnose the most common security** and administrative problems around privileged access in smaller environments, including shared accounts, tool sprawl, and limited visibility.
- **Examine emerging threats** that raise the stakes for privileged misuse, from large-scale password reuse to attacker automation and supply chain pivots.
- **Present a pragmatic roadmap** for implementing or maturing PAM, with quick wins, policy patterns, and measurable success criteria.

We wrap things up with a look at how multiple Devolutions' solutions help operationalize PAM in SMBs in a way that is streamlined, easy-to-manage, and affordable.

THE CRITICAL SECURITY & ADMINISTRATIVE PROBLEMS SMBS FACE AROUND PRIVILEGED ACCESS

Privileged access is where everyday friction meets significant risk. In smaller environments, a few people perform sensitive work using tools and processes that grew organically over time. Often, this leads to recurring problems that slow teams down and create openings for attackers.

Here are some of the most common and dangerous security and administrative problems that SMBs face around privileged access:

- **Shared, static, and sprawling secrets:** Many SMBs still manage administrator passwords, SSH keys, API tokens, and database credentials in wikis, spreadsheets, or personal password tools. Secrets end up copied into scripts, tickets, and cloud notes. Rotation is inconsistent (if done at all). When an employee leaves or a vendor changes, teams scramble to update dozens of places by hand. This becomes a direct path to misuse and leakage. The latest Verizon Data Breach Investigations Report highlights **how stolen credentials remain a dominant entry point**, and analysis by Cloudflare shows that **41% of successful logins across sites it protects used passwords that had been compromised.**
- **Always-on admin rights:** Standing privileges are convenient for busy admins, but they dramatically increase the blast radius when an endpoint is phished or a token is harvested. **In many SMBs, default credentials and never-changed device passwords still appear on network gear, IoT, and lab systems.**
- **Limited visibility into privileged work:** When elevated sessions are launched from admins' laptops with locally stored credentials, it is difficult to answer basic questions like: Who did what? Where did they do it from? What commands did they use? This lack of intel makes audit prep more difficult and slows incident response – which can lead to a much higher price tag. The IBM Cost of a Data Breach 2025 study **tied longer investigations and delayed containment to higher breach costs.**

- **Tool sprawl and inconsistent process:** Privilege workflows touch remote connection tools, vaults, multi-factor authentication (MFA), ticketing, logging, and change control. In many SMBs, these systems are disconnected, which forces admins to juggle multiple consoles and browser tabs. **This slows troubleshooting and leaves gaps where policy should be enforced.**

- **Third-party and vendor access that is hard to govern:** Vendors often need elevated access to fix line-of-business apps, maintain ERP or POS systems, or support cloud workloads. As a result, they often receive shared credentials, broad VPN access, or standing accounts that are difficult to monitor and hard to revoke. Guidance on software supply chain and third-party risk from organizations like NIST and CISA stress granular, auditable controls for external access. **However, many SMBs still lack the tooling and workflows to enforce them.**

- **Service accounts and automations that never expire:** Batch jobs, integration connectors, CI pipelines, and monitoring agents often run with broad, permanent permissions. Their secrets live in configuration files and repositories and can go years without rotation. **Adversaries actively hunt for these machine identities because they can move laterally without user interaction or MFA prompts.** Modern identity security guidance per NIST SP 800-53 calls for scoping, rotating, and monitoring non-human accounts with the same rigor as human admins.

- **Ransomware pressure and extortion:** Weak control of privileged access makes it easier for attackers to disable protections, spread quickly, and extract high-value data for leverage. **This is shockingly easy and fast when baseline defenses are missing, such as least privilege, MFA on admin accounts, and rapid credential rotation.**

- **Gaps in basic hygiene at the edge:** Branch offices, labs, and remote endpoints often lag behind servers and core cloud resources. Local admin rights persist, MFA is inconsistent on privileged actions, and break-glass procedures are either ad hoc or untested. **These edge gaps can become the automated entry points for attackers and the choke points that slow recovery after an incident.**

The theme is clear: **Decentralized secrets, permanent privileges, scattered tools, and poor session visibility combine to create operational drag and elevated breach risk.** Next, we will examine emerging threats that amplify these weaknesses and raise the stakes for SMBs.

EMERGING THREATS AND RISKS THAT RAISE THE STAKES FOR PRIVILEGED ACCESS IN SMBS

Attackers move fast, automate relentlessly, and aim straight for the access that matters. A new wave of tactics is changing how privilege is abused and how quickly an intrusion becomes business disruption. These include:

- **Industrial-scale credential theft via infostealers:** The economics of credential abuse have shifted. Infostealer malware quietly harvests browser-saved passwords, cookies, and tokens, then dumps them into criminal markets where they are packaged and resold within hours. **More than 1.8 billion credentials were exposed in the first half of 2025**; an eight-fold increase over prior periods, driven largely by stealer malware campaigns. For privileged access, that means stolen admin logins and service credentials are available at volume and at low cost, which accelerates initial access and lateral movement.

- **Post-authentication attacks: session hijacking and consent abuse:** Even when passwords are protected, attackers increasingly target what happens after login. Adversary-in-the-middle kits and token theft let criminals replay session cookies to bypass authentication and many second factors. In parallel, consent phishing and malicious OAuth app abuse grant persistent API-level access without ever stealing a password. Microsoft's 2024 Digital Defense report highlights how post-authentication techniques such as token theft and consent phishing are now central to intrusion chains.

- **MFA fatigue and phishing-resistant authentication gaps:** Push notification fatigue, SIM swap, and adversary-in-the-middle techniques continue to defeat weak MFA factors. Real-world incidents keep showing that attackers do not need to break cryptography to win: **they only need to subvert the user flow and hijack sessions.**

- **Ransomware fragmentation and data-theft-first playbooks:** The ransomware ecosystem is expanding and splintering. Current tracking shows a **record number of active groups in Q3 2025**, and continued emphasis on double extortion, where sensitive data is stolen first to maximize leverage. Payment rates remain troubling, and many victims still do not fully recover their data even after paying. **For SMBs, this means attackers will monetize any privileged foothold quickly by disabling defenses, stealing high-value data, and only then encrypting.**

- **Attack paths are short and frequently lead to sensitive users:** Modern environments contain many potential chains from an exposed asset to a privileged identity. Most organizations have multiple viable attack paths; **a significant share of which lead directly to sensitive users in only a few steps.**
- **Supply chain and third-party pivots:** Suppliers, managed service platforms, and SaaS connectors remain a frequent route into downstream customers. When a third-party tool or identity integration is compromised, **attackers inherit trust and often gain broad API scopes or remote management privileges.**
- **Rapid change in authentication standards:** Passkey adoption is gaining momentum, which is good news for reducing password theft. The transition period, however, creates mixed environments where employees use a blend of device-bound and synced passkeys alongside passwords and legacy MFA. **Admin actions that still allow weak factors remain prime targets.**
- **Social engineering at scale, boosted by AI:** Attackers are weaponizing automation to personalize lures, clone voices, and sustain long-running operations that blend phishing with business process compromise. Microsoft's 2025 Digital Defense Report **revealed that financially motivated cybercrime now dominates the threat landscape.**

The takeaway for SMBs: These emerging threats and risks do not only increase the probability of an incident. **They compress the timeline from compromise to impact.** The right countermeasure is disciplined privileged access. We look closer at this in the next section.

PRACTICAL AND STRATEGIC WAYS FOR SMBS TO MANAGE PRIVILEGED ACCESS AND EMBRACE PAM

The goal for SMBs is a program that is lightweight to run, easy to prove in audits, and resilient under pressure. Start with quick wins that reduce risk immediately, then build toward a repeatable operating model with clear owners, workflows, and metrics. Key actions on the roadmap include:

- **Centralize and automate secrets management:** Place administrator passwords, SSH keys, API tokens, and database credentials in a vault where they are encrypted at rest, brokered through policy, and rotated automatically. Secrets should be injected into sessions at runtime so technicians never see the raw values. This limits accidental disclosure, curbs reuse, and shortens investigations.

- **Adopt phishing-resistant authentication for admin actions:** Push fatigue, SIM swap, and adversary-in-the-middle techniques continue to defeat weak factors. Use phishing-resistant methods for break-glass accounts, directory and cloud admins, and PAM administrators. As noted earlier in this white paper, FIDO-based passkeys are gaining momentum in the workforce, with recent research indicating that 87% of surveyed enterprises now deploy passkeys for employee sign-ins.

- **Eliminate default credentials and reduce standing privileges:** As discussed earlier in this white paper, default passwords and always-on admin rights expand the blast radius of routine phishing and malware events. Remove defaults, require unique credentials, and favor just-in-time elevation that is time-bound and approval-based.

- **Treat service accounts and automations as first-class identities:** Backups, CI pipelines, integration connectors, and monitoring agents should have scoped permissions, automated rotation, and continuous monitoring. Store keys in a vault and inject them at runtime instead of embedding them in configuration files or repositories.

- **Broker vendor and third-party access through controls:** Vendors often need privileged access to line of business systems and cloud workloads. In such cases, provide time-bound, request and approval-based access that is recorded, source restricted, and scoped to the systems they actually maintain. Set these expectations in contracts and supplier risk reviews and align them to CISA's supply chain risk guidance and NIST SP 800-161.

- **Design privileged work as a single flow:** Privileged tasks should follow one coherent path. An authorized user launches a connection, receives credential injection from the vault, completes the task, and has the session recorded and logged to the SIEM. Approvals, change tickets, and emergency elevation should be part of the same flow, so that steps are not skipped.

- **Plan for post-authentication threats:** Modern intrusions frequently begin after the user has authenticated. Protect tokens and sessions, enforce conditional access that restricts where privileged sessions can originate, and monitor for risky consent grants to third-party apps.
- **Strengthen staff training and practice the workflows:** End users remain central to both success and failure. Provide short, focused training for technicians and vendors on how to request elevation, launch brokered sessions, approve access, handle break glass procedures, and report anomalies. Supplement classroom or computer-based training with short runbooks and quick reference guides that show the exact steps. Reinforce learning with monthly tabletop exercises that simulate a privileged incident, then use the lessons to improve policy language and tighten tooling.
- **Measure what matters:** Choose metrics that link privileged controls to business outcomes. Examples include percent of privileged accounts protected by phishing-resistant authentication, percent of privileged sessions with complete recordings and logs, median time to approve or deny privileged requests during business hours, and time to rotate all privileged secrets after a personnel or vendor change.

The takeaway? Effective PAM for SMBs requires tools that map real-world risks to simple, repeatable controls. Next, we outline how Devolutions delivers this through a suite of solutions, along with use case examples.

HOW DEVOLUTIONS HELPS SMBS OPERATIONALIZE PRIVILEGED ACCESS

Devolutions provides multiple solutions for operationalizing privileged access that fit how smaller teams work: one place to launch secure connections, inject credentials without exposing them, elevate privilege just in time, record sensitive activity, and rotate secrets on schedule. The products work together, so you can start small and add depth as needed.

Remote Desktop Manager: One source and console for privileged access

Remote Desktop Manager (RDM) centralizes remote connections and secrets so users can access privileged accounts and carry out their tasks, but without ever seeing a password. RDM stores administrator passwords, SSH keys, and other secrets in vaults and injects them at session launch, which reduces reuse and prevents copy-paste sprawl. It is also possible to link a single credential to many sessions, change it once in the vault, and have every dependent connection pick up the new value automatically. RDM also records privileged sessions for audit and incident review, and ties recordings to the relevant entry to clearly see who did what, when, and for how long.

RDM use case example: Your help desk needs to patch line-of-business servers after hours. Your admins select the server entry, RDM injects the vaulted credential into the RDP or SSH session, and the entire session is recorded. Nobody sees or types the password, and the recording is automatically associated with the entry for audit. The same setup works for cloud consoles and web admin panels through RDM's browser-based sessions.

Devolutions PAM: Rotate, approve, and elevate on-demand

Devolutions PAM adds purpose-built privileged functions that go beyond vaulting. It discovers privileged accounts, rotates passwords automatically and on schedule, propagates password changes, enforces check-out with approval, and supports just-in-time (JIT) elevation with detailed audit and reporting. In addition, admins can find, edit, rotate, and reset privileged accounts from within RDM. They don't have to waste time or effort switching tools.

Devolutions PAM use case example: Your finance database admin passwords must rotate monthly and immediately after staff changes. Devolutions PAM schedules the rotation, updates dependent systems through change propagation, and requires a check-out request with approval for any human use.

Devolutions Server and Devolutions Hub Business: The shared vault and policy backbone

Many SMBs prefer a self-hosted backbone for secrets and policy, while others want a cloud service. Devolutions Server provides a self-hosted shared account and credential management platform with single sign-on, role-based access control (RBAC), multi-factor authentication, conditional access, and detailed logs and reporting. Devolutions Hub Business offers a cloud-based deployment. Both integrate with RDM and Devolutions PAM, so policies, approvals, and audits are consistent across desktop and cloud.

Devolutions Server/Hub Business use case example: You want to restrict privileged sessions to business hours and specific geographies. An admin configures conditional access and MFA in Devolutions Server or Hub Business, assigns role-based permissions to the PAM vault, and lets RDM enforce those policies at session launch. Audit and reports remain in one place for compliance.

Devolutions Gateway: Secure access without a VPN

Devolutions Gateway brokers inbound access to internal resources without exposing VPNs. Admins and vendors can reach RDP, SSH, and other services through the gateway with time-bound, approval-based access, while servers remain unreachable from the public internet. Devolutions Gateway integrates with RDM and Devolutions PAM, so credential injection, check-out, session recording, and elevation all run through the same path.

Devolutions Gateway use case example: A supplier needs temporary access to your point-of-sale servers. You create a vendor profile in Devolutions Server or Devolutions Hub Business, require strong MFA, and grant a two-hour access window through Devolutions Gateway. The vendor launches a session through RDM, receives credential injection from the vault, and the session is recorded. When the window closes, access expires automatically, and the password rotation job runs.

Starter pack: Full platform power, sized up to five users

For small teams or a focused pilot, the Devolutions Starter Pack bundles password, remote connection, remote access, and privileged access features for up to five users with no feature restrictions. It brings RDM, Devolutions PAM, Devolutions Gateway, and the back-end vault (Devolutions Server or Devolutions Hub Business) together. Adoption is straightforward, and the platform meets SMBs where they are and scales as maturity grows.

Starter pack use case example: In day-to-day use, an admin opens RDM, selects a system, and launches a session. RDM injects credentials that are vaulted in either Devolutions Server or Devolutions Hub Business. If the account is governed by PAM, RDM initiates a check-out and approval, and PAM provides just-in-time elevation. If the connection is external, it is brokered through Gateway without a VPN. The session is recorded and logged. Rotation jobs run on schedule or on demand.

Separately or even better together, Remote Desktop Manager, Devolutions PAM, Devolutions Server, Devolutions Hub Business, and Devolutions Gateway transform privileged access from a collection of risky workarounds into a single, governed workflow. Credentials are vaulted and injected at launch, elevation is time-bound and approval-based, vendor access is scoped and recorded, and rotation happens on schedule or on demand. The result is privileged access as a tightly controlled and managed workflow, which is exactly what auditors, customers, and insurers expect and demand to see.

THE FINAL WORD

SMBs must reduce standing privileges, centralize and rotate secrets, enforce phishing-resistant authentication, and treat privileged work as a single auditable flow.

Most of all, SMBs need to start viewing privilege as a workflow, not a static entitlement. This shift turns privileged access from today's highest-value target into tomorrow's competitive advantage: faster operations, cleaner audits, and a security posture that keeps pace with the business.

NEXT STEPS

Turn the insights and advice in this white paper into a working blueprint in your environment. Free trials are available of all of the following solutions:

- **Remote Desktop Manager:** Centralize connections and inject vaulted credentials at launch.
- **Devolutions PAM:** Explore purpose-built privileged controls that rotate secrets, enforce check-out with approval, and provide just-in-time elevation.
- **Devolutions Server and Devolutions Hub Business:** Establish your policy backbone (self-hosted or cloud). Establish robust and reliable single sign-on, RBAC, MFA, conditional access, and reporting.
- **Devolutions Gateway:** Broker secure access to internal resources without a VPN, and keep vendor sessions scoped, time-bound, and recorded.
- **Devolutions Starter Pack:** Pilot the full stack with up to five users and no feature limits. Validate workflows from credential injection to session recording and rotation.

Prefer a guided path? Book a live guided demo or start a proof-of-concept project (30-90 days; minimal time investment) that focuses on your privileged workflows. Our experts will map roles and systems, configure policies, and show your teams how to measure time-to-connect, audit readiness, risk reduction, and more.