INFO~TECH
RESEARCH GROUP

IT-Led Privileged Access Management for SMB

Victor Okorie
Senior Research Analyst
Info-Tech Research Group

Executive Summary

Privileged access management has a deployment and usability problem that most vendors have been slow to acknowledge. The platforms built for enterprise security teams are feature-rich, compliance-ready, and genuinely difficult to deploy and operate for an IT generalist managing a small environment. For most SMBs, that trade-off is unacceptable.

Devolutions PAM is built around a different premise: that the primary user of privileged credentials in a small or mid-market IT environment is a technician trying to connect to an asset and get work done, not a security analyst producing compliance reports. The platform integrates natively with Remote Desktop Manager (Devolutions' remote connection management product, which the vendor reports has approximately one million users), making privileged credential use a seamless step in the connection workflow rather than a separate, friction-heavy process.

Devolutions PAM is a strong fit for SMB and mid-market organizations with small IT teams, existing Remote Desktop Manager deployments, and a threat model centered on opportunistic attacks rather than sophisticated adversaries. It is also a practical option for organizations with data sovereignty requirements, given full feature parity between cloud-hosted and self-hosted deployment options as of April 2026. Organizations with mature security operations, endpoint privilege management requirements, or large-scale compliance mandates should look to enterprise PAM platforms rather than treating Devolutions as a scaled-down substitute.

Introduction

PAM adoption among SMBs lags behind what most security frameworks recommend, and the primary barrier is rarely awareness: it is implementation burden. The platforms that dominate the enterprise PAM market were designed for environments with dedicated security teams, extended deployment timelines, and compliance-driven purchasing decisions. Deploying them in a small IT team with a constrained budget typically means weeks of implementation effort for a tool that the team then struggles to use efficiently day to day.

Devolutions approaches this gap by treating PAM not as a security overlay but as an extension of how IT teams already manage their work: connecting to systems, resolving incidents, and administering infrastructure. The platform is explicitly framed by the vendor as "IT-led": a PAM solution operated by IT generalists rather than dedicated security staff. Whether that design philosophy represents the right trade-off depends on the organization's size, security posture, and what they need privileged access management to do for them.

Product Overview

Devolutions PAM is an agentless privileged access management platform available in cloud-hosted and self-hosted deployment configurations. It is tightly integrated with Remote Desktop Manager, Devolutions' remote connection management product, and is organized around four operational phases: account discovery, credential vaulting, access request and approval, and password propagation after session close. Devolutions Gateway, a proxy and recording component, is included with the PAM license and handles session routing and recording without requiring agents on managed endpoints. Both deployment models reached full feature parity in April 2026.

Features and Capabilities

Core Features

- **Account discovery and import.** The platform connects to identity providers (including Active Directory and Entra ID) through a provider configuration and scans for privileged accounts within designated containers or groups. Discovered accounts are displayed in a split view of already-imported and not-yet-imported accounts. Import requires selecting accounts and assigning them to a vault. The process is designed to support incremental onboarding (a single scan and five-account import is a valid starting point) rather than requiring a complete credential inventory before the platform becomes usable.

- **Credential vaulting and access control.** Privileged accounts are stored in vaults within the platform's data layer. For the self-hosted deployment, sensitive fields in the underlying SQL database are encrypted at rest while non-sensitive fields remain readable to support vendor troubleshooting. The cloud-hosted deployment uses a zero-knowledge encryption model under which Devolutions manages the infrastructure but retains no access to stored credential data. Vault assignment controls which users can request access to which credentials, with granular permission schemes that allow audit log visibility to be granted independently of administrative rights.
- **Checkout requests and approval workflows.** Access to privileged credentials is governed through a checkout request process. When a user initiates a connection tied to a PAM account, they submit a request that can require a comment, a ticket reference, or a reason. Approvers receive the request by push notification through the Devolutions mobile client, by email, or directly within the product. Approvers can modify the requested duration and scope before approving, and can assign the request for review by a second approver where dual-approval requirements apply. Access is time-bound by default, and the credential is rotated and propagated back to the vault automatically when the session closes or is checked in.
- **Session recording and live monitoring.** All connections routed through Devolutions Gateway are recorded and available for playback from the activity log. Live session monitoring is available for active privileged sessions with a short delay, enabling real-time oversight. This applies to Remote Desktop Protocol sessions and other supported protocols that do not natively support session shadowing.
- **Clientless privileged remote access.** External contractors and third-party consultants can be granted access through a browser-based session launched from the Devolutions web interface, without requiring a VPN client or software installation on their device. Checkout request and approval workflows apply to these sessions in the same way as internal connections.
- **Audit logging and reporting.** All credential interactions are logged, including which account was used, by which user, on which asset, and with what outcome. Credential events and connection events are captured independently

in separate log views. Custom reports can be generated by running PowerShell scripts against the logged data, supporting tailored output for compliance or investigation purposes.

- **Just-in-time privilege elevation.** For Active Directory and Entra ID accounts, the platform supports temporary privilege elevation by placing an account into a time-limited group with an automatic time-to-live. This enables time-bounded access without issuing standing privileged roles, and does not require a premium identity license tier from the identity provider to function.

Differentiating Features

- **Connection-native PAM workflow.** The clearest operational advantage Devolutions PAM offers in this category is that credential use and connection establishment occur as a single action within Remote Desktop Manager. For organizations whose primary PAM use case is connecting to infrastructure (servers, domain controllers, network devices), this removes the workflow friction of retrieving a credential from a separate vault, copying it, and initiating a connection in a different tool. The vendor states that this integrated path takes approximately 10 seconds where an equivalent workflow in enterprise PAM platforms can take 5 to 15 minutes; this specific comparison was not independently validated, but the architectural basis for the efficiency gain is credible and consistent with how credential injection through connection managers works in practice.
- **Deployment speed.** The vendor reports cloud-hosted deployment times of approximately 20 minutes and self-hosted deployment times of approximately 35 minutes to first credential import, based on internal testing. These are vendor-stated figures. The agentless architecture is the structural reason: there is no endpoint software to push, no managed dependency chain to validate, and no agent version management after go-live. For IT teams measuring implementation success in hours rather than weeks, this is a material difference from agent-dependent platforms.
- **Cloud and self-hosted at full feature parity.** Many PAM vendors have deprioritized self-hosted deployment in favor of cloud-only or cloud-primary

models. Devolutions maintains full feature parity across both. This is directly relevant to organizations with data residency or sovereignty requirements (particularly in jurisdictions where vendor-managed cloud storage of privileged credentials creates regulatory or contractual complications), who would otherwise have to choose between feature completeness and data control.

- **Enterprise PAM complementation.** For organizations operating enterprise PAM platforms but whose IT teams find the day-to-day connection workflow cumbersome, Devolutions integrates via API to retrieve credentials from those platforms and inject them into Remote Desktop Manager sessions. This positions the product as a usability layer on top of existing PAM infrastructure, a relevant option for mid-market organizations partially committed to an enterprise PAM deployment that their IT staff find difficult to use efficiently for connection tasks.

Analyst Perspective

PAM adoption lags the threat landscape it is meant to address, and the gap is usually attributed to cost and complexity. Both are real barriers. But there is a third factor that receives less attention: most PAM platforms are built for the person who selects them, not the person who uses them day to day. A security architect evaluating a PAM platform and an IT technician using it to connect to a domain controller during an incident are solving different problems. Enterprise PAM platforms optimize for the architect's requirements (policy enforcement, audit completeness, compliance reporting) and treat the technician's experience as secondary.

Devolutions has made the opposite choice, and the integration with Remote Desktop Manager is the most visible expression of that decision. Privileged access management becomes a byproduct of how IT teams already work rather than a separate security workflow they are expected to adopt. In my experience, security tools that add significant friction to daily IT tasks tend to get configured once and quietly worked around. A platform that makes using privileged credentials through an approved, recorded, time-bound workflow faster than using unmanaged credentials addresses the adoption problem at its root.

That design philosophy has a defined scope. Devolutions PAM does not currently offer endpoint privilege management: once a user has access to a machine, it is admin or nothing, with no mechanism to restrict what an elevated user can do once there. Organizations that have moved past opportunistic threat models, or that operate environments where granular endpoint privilege control is a compliance requirement, will find the platform insufficient for those requirements.

The just-in-time elevation capability deserves specific attention for organizations running Microsoft identity infrastructure. Time-bounded privilege elevation using native Active Directory and Entra ID group mechanisms (without requiring a premium identity licensing tier to access equivalent functionality) closes a real capability gap for budget-constrained SMBs on standard Microsoft licensing. For small IT teams that have been told they need to upgrade their identity licensing to get JIT elevation, this is worth evaluating directly.

Conclusions and Fit Guidance

Strong Fit

- **SMB and mid-market organizations with small IT teams** are the clearest target customer. The design assumptions built into the platform (fast deployment, no agents, technician-centric workflow, mobile approvals) map directly to environments where the person managing PAM is also managing helpdesk, patching, and infrastructure. The platform's ability to go from zero to first credential import in under an hour is a practical advantage that enterprise PAM platforms cannot approach.
- **Organizations already running Remote Desktop Manager** face the lowest adoption friction of any buyer profile. PAM capabilities surface directly within the existing connection workflow, and the path from unmanaged privileged credentials to PAM-governed, recorded, time-bound access does not require users to learn a new tool or change how they connect to systems.

- **Organizations with data sovereignty or residency requirements** benefit from the self-hosted deployment option at full feature parity. This is particularly relevant for organizations operating in European jurisdictions where sending privileged credential data to a vendor-managed cloud environment creates regulatory or contractual complications, and where self-hosted alternatives from other vendors typically sacrifice feature completeness to maintain on-premises support.
- **IT teams managing distributed environments or external contractor access** benefit from the clientless remote access capability. Granting a third-party contractor time-bound, recorded, approval-governed access to specific assets through a browser session (without VPN configuration or client installation) reduces both administrative overhead and the persistent access exposure that follows contractor engagements.

No-Fit or Requires Augmentation

- **Enterprises with mature security operations or insider threat programs** will find Devolutions PAM undersized. Continuous endpoint privilege monitoring, statistical behavioral anomaly detection, and the policy depth those environments require are not part of the current production feature set. For those organizations, Devolutions PAM can function as a connection efficiency layer on top of a primary enterprise PAM platform, but it should not be the primary control.
- **Organizations requiring endpoint privilege management** should look closely at how Devolutions approaches it today. Privileged elevation and delegation management (PEDM) is part of the platform, but it is largely local in its current form, so teams accustomed to centrally managed endpoint privilege policy will find the model narrower than a dedicated endpoint privilege management platform. Access on the endpoint is not simply admin or nothing, however: what a user can do on a machine follows from the identity used to connect, which remains in the customer's hands, and from the permissions carried by that account when just-in-time (JIT) elevation is used. Where fine-grained restriction of application privileges is a compliance requirement or a security control you can't compromise on, it is worth mapping those requirements against the current model and deciding

whether a complementary solution is warranted in the interim. Devolutions has confirmed that PEDM is an area of renewed emphasis on the roadmap, though no timeline is available yet.

- **Large enterprises with complex compliance automation requirements** will encounter limits. The platform supports custom PowerShell-based reporting against its logs, which provides flexibility, but it is not a substitute for enterprise-grade GRC integrations, automated evidence packaging, or multi-tier approval workflows designed for large administrative user populations.

The right question is not whether Devolutions PAM handles every PAM use case (it does not), but whether it handles the use cases that actually matter for a small IT team operating without a dedicated security function. For organizations in that profile, the platform closes the most significant privileged access gaps at a deployment speed and total cost that enterprise platforms cannot approach. For organizations whose security posture has matured past that profile, it belongs at most as a usability layer within a broader PAM architecture, not as a standalone control.