Devolutions

Why your small or mid-sized business needs a secure digital vault

NOVEMBER 2025

TABLE OF CONTENTS

To operate efficiently and effectively, small and mid-sized businesses (SMBs) depend on credentials and corporate secrets such as admin passwords, vendor logins, API keys, certificates, and service accounts. So, what's the problem? **It is this: When these critical assets live in spreadsheets, browsers, or personal tools, then risk climbs, audits get harder, and day-to-day work slows down.**

This white paper explains why a secure digital vault is now a fundamental requirement for SMBs. Our journey will cover:

- **The SMB risk reality:** How credential theft, reuse, and shadow secrets drive breaches, and why remote work and vendor access raise the stakes.
- **Emerging threats facing SMBs:** New risks and challenges that SMBs need to be aware of and avoid — or risk facing a potentially catastrophic breach.
- **What a secure digital vault is:** Understand the essence of a secure digital vault by exploring what it is, who uses it, and what belongs in it.
- **How a vault differs from a basic password manager:** Demystify a common source of confusion by grasping the core differences between a secure digital vault and password manager.
- **Benefits of a secure digital vault:** Key advantages and wins of using a secure digital vault.
- **Must-have capabilities:** What SMBs should look for in evaluating and ultimately choosing a secure digital vault for their environment.

We wrap up our journey with a look at how SMBs can translate their newfound understanding into strategic action with help from Devolutions.

THE SMB RISK REALITY

Even with smaller footprints, SMBs manage a large number of passwords, keys, certificates, and service accounts across SaaS, on-premises systems, and vendor tools. When these live in spreadsheets, browsers, and personal vaults, teams can lose track of who has access, where the truth lives, and whether old credentials were ever cleaned up. **This triggers key risks including:**

- **Credential sprawl:** Secrets left in source code and repos often linger. According to Verizon's 2025 Data Breach Investigations Report (DBIR), the average time it takes to remediate credentials leaked through GitHub repositories is 94 days, which is ample time for attackers to exploit access without being detected.
- **Shadow access from shared or stale accounts:** Third-party breaches rose to 30% of cases in the 2025 DBIR, highlighting how vendor and partner access can become a path into core systems.
- **Remote and vendor access pressure:** Ransomware featured in 44% of analyzed breaches per the Verizon 2025 DBIR, underscoring the need for stricter credential controls and rapid de-provisioning.
- **Password-based attacks dominate:** With more than 97% of identity attacks reported as password-based in the Microsoft Digital Defense Report 2025, SMBs should assume credential abuse is the default threat.

The next section explains the emerging threats that are accelerating these trends, and consequently increasing the risks and stakes for SMBs.

EMERGING THREATS FACING SMBS

Attackers have industrialized tactics and techniques that were once categorized as highly advanced. Automated credential attacks, token theft/abuse, and turnkey infostealer kits now turn small oversights into real incidents. Meanwhile, hybrid work and an expanding vendor ecosystem widen the attack surface faster than most lean teams in SMBs can govern.

Let us take a closer look at some of the emerging threats facing SMBs, which collectively increase the urgency of leveraging a secure digital vault now, not later:

- **Credential stuffing and password reuse at scale:** Based on observed traffic across Cloudflare protected sites, 41% of successful logins used already compromised passwords, which turns reused credentials into quick account takeover. Attackers source these credentials from breach dumps and infostealer logs, then automate attempts across email, VPN, SaaS, and admin portals.
- **Token and session abuse:** A recently disclosed Microsoft Entra ID actor token revealed how a single token class can bypass normal controls and grant Global Admin-level actions until remediated. The issue, tracked as CVE-2025-55241, has now been patched. However, it highlights how token misuse can undermine password and MFA defenses if tokens are not tightly governed and logged.
- **Infostealers harvesting browser secrets:** Infostealer malware continues to vacuum up saved passwords, cookies, and tokens at scale. In June 2025, researchers reported a cache of 16 billion login records, with an estimated 85% sourced from infostealers, which feeds credential stuffing and session hijacking long after the initial infection.
- **Identity attacks are mostly simple password attacks:** Microsoft has reported that identity-based attacks rose by 32% in the first half of 2025. This reinforces the need to remove password exposure wherever possible and to add strong checks at approval points.
- **Web apps remain a prime target for stolen credentials:** The Verizon 2025 DBIR noted that in the Basic Web Application Attacks category, about 88% of breaches involved stolen credentials. This is a direct signal that secrets governance must cover human logins and machine secrets that back web services.

Looking at all of these emerging threats, the common thread is simple: **Attackers are not always breaking in with novel exploits.** Rather, they are signing in with secrets and tokens that were saved, reused, or left ungoverned. Granted, a secure digital vault will not stop every tactic. **However, it will certainly remove easy wins by centralizing secrets, enforcing use without reveal, adding approvals for sensitive actions, and generating an audit trail.**

The next section looks closer at what a secure digital vault is, who uses it and how, and the ways in which it differs from a password manager.

WHAT IS A SECURE DIGITAL VAULT?

A secure digital vault is a centralized system that stores, protects, and governs access to sensitive credentials and corporate secrets. It gives SMBs one trusted place to keep admin passwords, vendor logins, API keys, certificates, SSH keys, and service account credentials. It also controls who can use each item, records every access, and enables work without exposing the underlying secret.

WHAT SHOULD BE KEPT IN A SECURE DIGITAL VAULT?

A secure digital vault is most effective when it holds every secret that could be abused or lost. Centralizing these items makes them easier to protect, use, and audit. The list below highlights what should be contained and secured in a digital vault, so nothing critical is left on a spreadsheet or a browser.

- **Credentials:** Admin and operator passwords, vendor accounts, finance and HR system logins.
- **Machine secrets:** Service accounts, database credentials, application passwords.
- **Keys and certificates:** SSH keys, API tokens, TLS certificates, and related private keys.
- **Remote connection entries:** Targets and connection settings that pair with stored credentials for secure launch.
- **Documentation with guardrails:** Runbooks and notes that are bound to entries and inherit the same access controls.

WHO TYPICALLY USES A SECURE DIGITAL VAULT & HOW DO THEY USE IT?

A secure digital vault serves multiple teams across an SMB, each with different needs. Admins need fast, safe access to systems. Developers need reliable automation without hardcoding secrets. Security leaders need policy control and clear evidence. Service providers need clean separation between clients. The list below shows who typically uses a vault and how they use it in daily work.

- **IT and ops:** Launch privileged sessions with credential injection, request temporary elevation, and record sessions for high-risk work.
- **Developers and DevOps:** Retrieve tokens and keys through APIs or CLI, rotate secrets automatically, and remove secrets from code and pipelines.
- **Security and compliance:** Set policies, require approvals, and export evidence for audits and customer reviews.
- **Managed service providers:** Segregate client vaults, delegate access safely, and report on usage across tenants.

HOW A SECURE DIGITAL VAULT DIFFERS FROM A PASSWORD MANAGER

Generally, password managers help users store and autofill logins. A secure digital vault goes further by controlling how secrets are used, who can use them, and what evidence is recorded. The goal is to let teams do their work, while keeping the underlying passwords, keys, and tokens out of sight and under policy. The points below cover how a vault differs in practice from a password manager, and why this extra control matters:

- **Use without reveal:** A secure digital vault can inject credentials into RDP, SSH, VNC, web consoles, and scripts so staff complete tasks without seeing any secrets.

- **Granular permissions:** Rights can be set to view, use, modify, or administer at the vault, folder, and entry level. Password tools usually focus on end user convenience rather than enforcing control.
- **Approvals and just-in-time access:** Sensitive actions can require an approval and time-bound access. This reduces standing privilege and limits blast radius.
- **Rotation and propagation:** Secrets can rotate on a schedule or after an event and changes can propagate to dependent systems.
- **Audit and reporting:** Every checkout, approval, and use is logged with who, what, when, where, and why so audits stop being guesswork.
- **Coverage for people and machines:** In addition to human passwords, a secure digital vault manages service accounts, API tokens, certificates, and SSH keys used by apps and automation.

BENEFITS OF A SECURE DIGITAL VAULT

A secure digital vault improves both security and day-to-day operations. The points below summarize the benefits SMBs can expect when a secure digital vault is designed well and fully adopted across the organization:

- **Least privilege:** Users (and systems) get only the access they need, only when they need it.
- **Use without reveal:** Users can launch sessions or scripts without copying secrets into notes or terminals.
- **Separation of duties:** The people who approve are not the same as the people who request or use the access.
- **Tamper-proof logging:** Security activity is recorded in a way that can't be changed or deleted. These records can be sent to a Security Information and Event Management (SIEM) system for monitoring and audits.
- **Resilience and recovery:** Multiple emergency keys, tested break glass procedures, and backup options prevent single points of failure.
- **Simple daily experience:** Fast search, clean policies, and native clients keep adoption high for small teams.

For SMBs, a secure digital vault replaces scattered passwords and ad hoc practices with governed access and clear evidence.

Next, we look at what SMBs should focus on when evaluating and ultimately choosing the right secure digital vault for their environment.

MUST-HAVE CAPABILITIES OF A SECURE DIGITAL VAULT

Choosing a secure digital vault is a strategic decision for SMBs. **The right solution centralizes credentials and secrets, reduces breach risk from reuse and shadow storage, and adds guardrails for privileged work without slowing teams down.**

Below is a checklist that separates mere password managers from full-blown, legitimate secure digital vaults that support today's sophisticated remote access, governance, and audit needs:

- **Strong security fundamentals:** End-to-end encryption, zero-knowledge architecture, hardware-backed key options, configurable data residency, and reliable backup/restore with point-in-time recovery.
- **Deployment choice:** Cloud, on-premises, or hybrid, with a straightforward path to move between models as needs change.
- **Identity integration:** Single sign-on (SSO) and multi-factor authentication (MFA) with major identity providers, conditional access, and group-based provisioning to keep onboarding and off-boarding tight.
- **Granular role-based access control (RBAC) and policy templates:** Roles, fine-grained permissions, and reusable policies for teams, vendors, and contractors to prevent over-privilege.
- **Privileged access workflows:** Check-out with approval, time-boxed access, and just-in-time elevation for sensitive accounts.
- **Rotation and propagation:** Automated password/key rotation on schedules and events, with change propagation to dependent systems and services.

- **Secret injection without reveal:** Inject credentials into RDP, SSH, VNC, databases, and web consoles so users never see or copy secrets.
- **Remote access brokering:** Gateway-based session brokering that avoids exposing ports and supports audited, proxied connections from anywhere.
- **Session recording and privacy controls:** Capture privileged sessions with redaction options, access controls, and immutable retention for investigations.
- **Audit, reporting, and SIEM export:** Tamper-evident logs, built-in compliance reports, and easy export to your SIEM for monitoring and attestations.
- **Vendor and third-party access:** Scoped, temporary access for suppliers with required approvals, automatic expiration, and clear audit trails.
- **Break-glass readiness:** Multiple emergency recovery keys, testable procedures, and the ability to create new keys without invalidating existing ones.
- **Broad secret coverage:** Passwords, keys, certificates, API tokens, connection strings, and infrastructure secrets in one system, with expiration tracking.
- **Cross-platform clients and extensions:** Native apps for Windows, macOS, Linux, iOS, and Android, plus browser extensions for web apps.
- **Automation and API:** Well-documented APIs, CLI/PowerShell modules, and event hooks to integrate with ITSM, CI/CD, and configuration management.
- **Usability for lean teams:** Clear UX, role-based folders, bulk import/migration, and productivity features like templates and search that reduce admin overhead.
- **Scalability and performance:** Proven support for thousands of secrets and concurrent sessions without slowdowns, plus horizontal growth options.
- **Transparent pricing and support:** SMB-friendly pricing, simple and varied licensing/subscription options, expert guidance for deployment, and fast support.

SMBs should shortlist solutions that deliver strong security, clean integrations with identity and remote access, and practical automation that lean teams can run confidently. Ultimately, the right solution unifies secret governance and privileged access into one controlled workflow, not a patchwork of tools.

DEVOLUTIONS: DELIVERING A COMPLETE SECURE DIGITAL VAULT FOR SMBS

Devolutions gives lean IT teams in SMBs an end-to-end platform that combines a hardened digital vault with privileged access, remote session brokering, and audit-ready evidence — all without costly or complex enterprise overhead.

Cloud, on-prem, and hybrid options let SMBs start fast and stay in control as they scale, while features like credential injection, rotation, just-in-time (JIT) elevation, and session recording turn policy into day-to-day practice. Here is an overview of how the pieces work and fit together:

- **Devolutions Hub Business (cloud vault):** Zero-knowledge, client-side encryption; centralized secrets (passwords, keys, tokens, certs); granular RBAC; tamper-evident audit logs with SIEM export; multiple emergency recovery keys; APIs/automation.
- **Devolutions Server (on-premises vault):** Self-hosted credential and secrets governance with data residency control; RBAC and policy enforcement; centralized storage of session recordings; detailed auditing and reporting.
- **Remote Desktop Manager:** Secret injection into RDP/SSH/VNC/databases/web consoles (no secret reveal); policy templates; session recording capture; tight integration with Hub/Server for vault-backed launches.
- **Devolutions PAM:** Privileged account discovery; scheduled and event-based rotation; password-change propagation; approval-based check-out; just-in-time (JIT) elevation with full audit trails.
- **Devolutions Gateway:** Brokered remote/vendor access without exposing inbound ports; proxied, auditable sessions that inherit vault and PAM policies.
- **Devolutions Web Login (browser extension):** Vault-backed, policy-controlled credential use in web apps without copy/paste; domain rules and audit visibility.
- **Devolutions Workspace (desktop & mobile):** Unified client experience across products to standardize workflows for lean teams; cross-platform support for Windows, macOS, Linux, iOS, and Android.

AUTOMATION & INTEGRATIONS

SMBs can also leverage automation and integration layers across Devolutions' products to increase productivity, security, control, and governance:

- A well-documented REST API, CLI, and PowerShell module handle bulk provisioning, folder/role management, and policy changes as code.
- Rotation jobs and check-out approvals can trigger scripts or webhooks to update tickets, notify chat channels, or kick off remediation workflows.
- CI/CD pipelines can request short-lived secrets at build time (no hard-coded credentials).
- ITSM integrations gate privileged access behind a ticket or change record.
- Session, audit, and configuration data can be exported to monitoring and SIEM platforms for detection and compliance reporting.
- Identity integrations (SSO/MFA/conditional access) keep automation aligned with existing IdP policies.

The result is repeatable, auditable workflows that reduce admin toil and fit small-team realities.

PURPOSE BUILT FOR SMB BUDGETS AND REALITIES

Every Devolutions product is designed to be affordable and practical for SMBs through:

- **Transparent, predictable licensing with no hidden costs**
- **Modular adoption so teams can start small and expand**
- **Minimal services overhead thanks to guided setup, pre-set defaults, and rich documentation**

SMBs can begin with the essentials — typically centralized vaulting and credential injection — and then add automated rotation, approvals, JIT elevation, and session brokering as needs grow. **This phased approach avoids excessive initial costs, reduces change-management friction, and delivers measurable security gains early.**

NEXT STEPS: PUT A SECURE DIGITAL VAULT TO WORK

SMBs can validate a secure digital vault quickly and safely in their own environment. Start with a free trial to centralize secrets, enable credential injection, and see audit-ready evidence in action. **Free trials are available for all of Devolutions' products and solutions noted earlier in this white paper.**

Prefer a guided path? Book a live demo or run a 30–90 day proof of concept (POC). During the POC, Devolutions' experts will map roles and systems, configure vault and access policies, and define clear success metrics such as time to connect, audit readiness, and measurable risk reduction — so your teams move from baseline to execution with clarity, confidence, and control.