Devolutions

10 Reasons why SMBs should stop using a VPN & start using a Just-in-Time gateway

NOVEMBER 2025

TABLE OF CONTENTS

Discover a practical guide for SMBs to move from fragile VPN tunnels to secure, auditable, just-in-time gateway access that reduces attack surface, simplifies remote operations, and supports employees, vendors, and MSP partners across hybrid environments.

For many small and mid-sized businesses (SMBs), a conventional VPN has been the default answer to a critical question: How do we give employees, contractors, vendors, and other authorized users secure remote access to what they need, when they need it? And for several years, a VPN did the job. However, things have changed. **Today, from a security standpoint, VPNs are increasingly being called out as a potential risk rather than recommended as a best practice.**

What has shifted so dramatically in recent years? It is this: VPNs were designed for a landscape in which a small number of trusted employees connected into a well-defined corporate network. Today, this expectation does not align with the reality for most SMBs that deal with cloud workloads, SaaS, third-party support, hybrid work, and a constant churn of users, devices, and endpoints. **The result is VPN sprawl, over-privileged access, and blind spots that attackers are quick to exploit.** For example:

- The Verizon 2025 Data Breach Investigations Report highlights **credential abuse as the most common initial access vector**, and notes that attacks exploiting vulnerabilities in edge devices and VPNs now account for roughly 20% of all breaches.
- Research on VPN risk found that 56% of organizations were targeted by cyberattacks in the last year that **exploited VPN security vulnerabilities**.
- High-profile incidents involving zero-day flaws in VPN connectors show that these conventional and common appliances **are increasingly vulnerable and attractive targets.**

In this white paper, we dive deeper into this common — and potentially catastrophic — issue for SMBs. Our roadmap covers:

- **The biggest problems and vulnerabilities with VPNs.**
- **How a just-in-time (JIT) gateway works.**
- **10 reasons why SMBs should use a JIT gateway instead of a VPN.**

We wrap up with a look at how **Devolutions can help SMBs establish JIT access and strengthen their IT security posture**, without facing a disruptive implementation, unnecessary complexity, and excessive costs.

PROBLEMS WITH TRADITIONAL VPNS

As we noted a moment ago, VPNs were not designed with today's realities in mind. In many environments, the setup (it cannot truly be called "infrastructure") has been cobbled together over time: a VPN concentrator here, a firewall rule there, a handful of temporary vendor accounts that quietly became permanent. The result is an access model that is fragile, opaque, and risky, especially for lean IT teams in SMBs that must juggle security with day-to-day operations. Common VPN pain points include:

- **Broad, implicit trust once "on the network":** A compromised VPN credential often grants access to far more than a specific user actually needs. As a result, once attackers land on the internal network, they may be able to scan, move laterally, and target high-value systems with relative ease. VPN access is a powerful foothold, not a narrow pathway.
- **Over-privileged and hard-to-clean entitlements:** VPN entitlements tend to grow over time. Users change roles, vendors complete projects, and servers are retired — but the underlying VPN groups and firewall rules often remain. Cleaning up old access requires careful coordination and testing, so many SMBs live with "good enough" policies that often totally disregard the principle of least privilege (i.e., granting users only the access their job or task requires, and for only as long as they need it).

- **Limited visibility into what happens after connection:** VPN logs typically show which user connected, from where, and for how long. However, what those users did inside key systems is much harder to capture. For SMBs facing audits, cyber insurance investigations, or regulatory scrutiny, this lack of session-level evidence creates both compliance and incident-response challenges.

- **A growing attack surface at the edge:** As noted earlier, VPN appliances have become attractive targets. Over the last few years, multiple high-profile vulnerabilities in VPN and remote access devices have been exploited at scale, giving attackers direct entry into internal networks. Keeping these edge systems patched, hardened, and monitored is difficult and can be overwhelming for lean IT teams.

- **Operational friction for users and admins:** Users often need to remember which VPN to connect to, which profile or split tunnel to use, and how to work around performance issues like hair-pinned traffic. Administrators must maintain complex combinations of VPN policies, firewall rules, and routing configurations, and every change risks unintended side effects.

Taken together, these issues create a pattern: VPNs tend to grant too much network access, for too long, with too little visibility. For SMBs, that is the opposite of the desired state: precise, time-bound, and auditable access.

This is where a JIT gateway model comes into play and sets a new, higher standard for security, visibility, governance, and control. Instead of centering on network tunnels, a JIT gateway focuses on per-session access to specific systems and applications, which directly addresses many of the weaknesses outlined above. The next section explains how a JIT gateway works, and why it is so well aligned with SMB realities.

WHAT IS A JIT GATEWAY?

A JIT gateway is a modern remote access model that flips the traditional VPN approach on its head. Rather than creating a persistent tunnel into the network, a JIT gateway brokers short-lived, tightly scoped connections to individual resources, such as RDP servers, SSH endpoints, privileged web consoles, or internal line-of-business applications. At a high level, a JIT gateway introduces three key shifts:

- **From network-level trust to session-level trust:** Access is granted per user, per session, and per resource. Instead of "you're on the network now, have fun!" each connection is explicitly authorized and controlled.
- **From always-on tunnels to time-boxed access windows:** Remote access is opened when needed and automatically shut down when the job is done. This limits the time window that an attacker can exploit stolen credentials or tokens.
- **From opaque activity to built-in observability:** Since sessions are brokered through the gateway, it is much easier to capture detailed logs, as well as full recordings of privileged actions for audits and investigations.

Essentially, a JIT gateway brings the **control, visibility, and precision that SMBs need** — without the heavy complexity of full-scale enterprise zero-trust or SASE projects.

The remainder of this white paper drills into the practical implications of that shift. We compare traditional VPNs and a JIT gateway across 10 concrete dimensions such as attack surface, least-privilege enforcement, vendor access, performance, and cost.

Each factor shows how moving away from legacy VPN tunnels toward a JIT gateway model helps SMBs strengthen security, simplify operations, and deliver a better experience for both internal users and external partners. They also connect to typical SMB realities such as limited staff, budget constraints, and growing compliance expectations.

REASON 1:
REDUCE EXPOSED ATTACK SURFACE

Traditional VPNs effectively put a large sign on the perimeter that says: «Dear adversaries, go ahead and start your attack here.» For SMBs, a single exposed VPN appliance or open port is often the most visible, and sometimes only, path into the internal network. A JIT gateway reduces this exposure by brokering sessions instead of publishing network entry points.

With a JIT gateway, SMBs can:

- **Remove (or drastically reduce) open inbound VPN ports on the internet.**
- **Terminate sessions through a hardened broker instead of exposing internal services directly.**
- **Limit access to individual systems rather than entire network segments.**

For lean IT teams that cannot spend all day chasing perimeter vulnerabilities, this approach reduces the number of high-value targets an attacker can see and probe. The fewer exposed services, the smaller the attack surface and the lower risk of a compromise.

REASON 2:
ENFORCE LEAST PRIVILEGE BY DEFAULT

In many VPN environments, once a user is connected they can see far more of the network than they actually need. Even if firewalls and segmentation exist, they often grow messy over time. A JIT gateway shifts the model so that access starts with the specific resource, not the network.

With a JIT gateway, least privilege becomes the default pattern:

- **Access is granted per user, per session, and per resource.**
- **Policies are defined in terms of who can reach which system or application.**
- **Unnecessary network reach is removed, which limits lateral movement after compromise.**

For lean IT teams, this means fewer sleepless nights about dormant accounts, forgotten vendor access, or over-privileged VPN groups. Users get precisely what they need to do the job and nothing more, which is exactly how things should be.

REASON 3: JIT, TIME-BOXED ACCESS

With VPNs, accounts, groups, and profiles often remain enabled long after projects end or roles change. This gives attackers a large window of opportunity to abuse stolen credentials. A JIT gateway makes time an ally by limiting access to when it is actually needed.

A JIT gateway supports time-boxed access such as:

- **Sessions that are created on demand for a specific task.**
- **Automatic expiry of access when the time window ends.**
- **Temporary rights for emergency or maintenance work that do not linger afterward.**

For SMBs with small teams and no dedicated identity specialists, automatic expiry of access is essential. When access closes itself on schedule instead of depending on manual cleanup and help desk tickets, temporary rights are far less likely to linger and become a long-term risk.

REASON 4: STRONG IDENTITY AND MFA AT THE FRONT DOOR

SMBs are frequently targeted by attacks that involve credential theft, password spraying, and phishing. Shared VPN accounts and static credentials make matters worse, because it is difficult to know who is truly behind a connection. A JIT gateway puts strong identity and multifactor authentication (MFA) at the front door of every session.

Instead of a generic VPN credential, a JIT gateway typically:

- **Integrates with an existing directory or identity provider.**
- **Requires users to authenticate with MFA for sensitive access.**
- **Ties each session to a unique, named identity for accountability.**

This identity-centric approach helps SMBs move away from shared accounts and generic VPN logins toward individual responsibility. When every privileged session is tied to a real person and backed by MFA, it becomes much harder for attackers to blend in as legitimate users.

REASON 5: APPLICATION-LEVEL ACCESS INSTEAD OF NETWORK-LEVEL TUNNELS

VPNs are built around network-level tunnels. Users connect and are effectively «dropped» into the environment; even if they only need to reach a single internal application or admin console. A JIT gateway reverses this by providing application-level access without granting broad network reach.

With a JIT gateway, remote access can:

- **Go directly to a specific RDP server, SSH endpoint, or web console.**
- **Avoid exposing file shares, internal subnets, and unrelated systems.**
- **Align more naturally with cloud and SaaS workloads that are already application-centric.**

For SMBs that are steadily moving to hybrid or cloud-first environments, this model fits how systems are actually deployed today. SMBs are no longer forced to extend the network everywhere just to let a user reach a single tool or management interface.

REASON 6: BETTER VISIBILITY AND AUDITING OF REMOTE SESSIONS

VPN logs show who connected, from where, and when. However, they generally do not show what a user actually did once inside a critical system. For SMBs under pressure from customers, auditors, and cyber insurers, this lack of business intelligence can be a serious problem. A JIT gateway makes visibility and auditing part of the design instead of an afterthought.

Typical JIT gateway capabilities include:

- **Per-session logging tied to identity and target system.**
- **Optional session recording for high-risk or highly regulated activities.**
- **Clear reports that show who accessed what, when, and for how long.**

This level of observability helps SMBs respond faster to incidents, demonstrate control to auditors, and provide better reporting to customers (which is absolutely critical if they operate as an MSP). Instead of piecing together clues from multiple logs, SMBs have a clean, session-centric trail of activity.

REASON 7: SIMPLER OPERATIONS FOR SMALL IT TEAMS

Running a traditional VPN often involves juggling multiple components: concentrators, firewalls, routing rules, split tunneling, client distributions, and device compatibility issues. For lean IT teams, keeping everything stable and secure is time-consuming and exhausting. A JIT gateway offers a more focused operational footprint.

A well-designed JIT gateway will:

- **Reduce the number of moving parts compared to VPN plus complex firewall rules.**
- **Centralize access policies in one place instead of scattering them across devices.**
- **Provide a consistent workflow for different protocols and environments.**

For SMBs, this translates into fewer configuration surprises and less firefighting. The team can spend more time on strategic improvements and less time troubleshooting tunnels, profiles, and connectivity issues that frustrate users and consume scarce support hours.

REASON 8: EASIER, SAFER VENDOR AND CONTRACTOR ACCESS

With a VPN, granting external access often means creating new accounts, adding people to internal groups, and then remembering to remove them later. A JIT gateway makes third-party access more controlled and easier to manage.

WITH A JIT GATEWAY, SMBS CAN:

- **Grant vendors access only to the specific systems they support.**
- **Use time-bound, project-specific access windows.**
- **Require approvals and extra verification for sensitive sessions.**

This helps SMBs work confidently with external partners without diluting their security posture. Instead of either over-trusting vendors or blocking them entirely, SMBs can strike a practical balance: just enough access, only when required, with a clear record of what happened.

REASON 9: IMPROVED PERFORMANCE AND USER EXPERIENCE

Centralized VPN concentrators can become bottlenecks, especially when traffic is hair-pinned through a single site. Remote users may experience slow file transfers, laggy sessions, or dropped connections – all of which lead to frustration and lost productivity. A JIT gateway minimizes these issues by connecting people closer to the resources they need.

A JIT gateway can improve the experience by:

- **Reducing unnecessary routing and backhauling through a single VPN hub.**
- **Allowing gateways to be placed closer to workloads or regions.**
- **Providing a more stable experience for protocols like RDP and SSH.**

For SMBs that cannot afford to overbuild their network just to support remote access, these gains are compelling and valuable. A smoother, faster experience keeps employees productive and reduces the number of remote access complaints landing in the IT queue.

REASON 10: RIGHT-SIZED COST AND SIMPLICITY FOR SMBS

Many SMBs look at large enterprise VPN, SASE, or zero trust projects and conclude that they are too expensive, too complex, or both. At the same time, trying to hold onto an aging VPN stack clearly carries growing risk. A JIT gateway offers a practical path forward that aligns with SMB budgets and capabilities.

In a right-sized JIT gateway approach, SMBs can:

- **Start with a small set of critical systems and expand gradually.**
- **Avoid large up-front hardware investments in favor of more flexible deployment options.**
- **Gain meaningful security and compliance improvements without needing a large security engineering team.**

For SMBs, the goal is not to mimic a global enterprise architecture. It is to achieve strong, practical control over remote access with tools that are manageable day-to-day. A JIT gateway fits that reality. It lets SMBs move beyond the limitations of traditional VPNs and adopt a model that delivers better security, clearer visibility, and more predictable costs without overwhelming the people who have to run it.

HOW DEVOLUTIONS HELPS SMBS ADOPT A JIT GATEWAY MODEL

A JIT gateway approach is only useful if it can be implemented and operated in the real world by SMBs that typically have lean teams, limited budgets, and no tolerance for over-complex tools or disruptive deployments. **This is where Devolutions comes in.**

Devolutions Gateway is a secure, easy-to-manage alternative to traditional VPNs and RD Gateway. It grants authorized, session-based access to internal resources in segmented networks, and only forwards traffic to a target system after authentication and authorization have succeeded. This reduces the risk of exposing internal systems

on the internet, while still giving users fast and responsive remote sessions for RDP, SSH, VNC, ARD, Telnet, PowerShell, and web applications.

When combined with Devolutions' Remote Desktop Manager and either Devolutions Server or Devolutions Hub Business, Devolutions Gateway gives SMBs a practical JIT remote access stack. Devolutions Gateway acts as the secure bridge, while Devolutions Server or Hub control who can reach what, and Remote Desktop Manager provides the single pane of glass that IT pros and MSPs use to launch sessions. Authorized connections are brokered through Devolutions Gateway and logged centrally, so access is just in time, auditable, and no traditional VPN is required.

Just as importantly, this ecosystem is shaped around SMB realities. Deployment options include on-premises and cloud, policies are managed in familiar tools, and the same platform can cover multiple use cases: internal admins, remote workers, and external vendors or MSP technicians. **And for SMBs that also need privileged account discovery and rotation, Devolutions PAM adds password vaulting and credential injection to the same environment, so that sensitive credentials never have to be revealed to end users.**

The table below connects each of the ten reasons to move away from VPNs with the specific Devolutions capabilities that support that outcome.

Reason to choose a JIT gateway instead of a VPN	How Devolutions Gateway and the Devolutions ecosystem help	Related Devolutions products
Reduce exposed attack surface	Devolutions Gateway brokers JIT sessions to internal resources and only forwards traffic after authentication and authorization, which limits direct exposure of RDP, SSH, and web services on the internet. Static VPN and firewall rules can be replaced with dynamic, session-based access policies.	Devolutions Gateway; Devolutions Server; Devolutions Hub Business

Enforce least privilege by default	Access is defined per user or group to specific entries in Remote Desktop Manager and is authorized by Devolutions Server or Hub. Gateway then connects only to the approved target, which makes least privilege the normal pattern instead of a special case.	Devolutions Gateway; Remote Desktop Manager; Devolutions Server; Devolutions Hub Business
Just-in-time, time-boxed access	Gateway supports session-level JIT access so systems do not need permanent open access paths. Devolutions Server or Hub can require approvals and define how long access is valid, after which the session ends and the path is closed without manual cleanup.	Devolutions Gateway; Devolutions Server; Devolutions Hub Business
Strong identity and MFA at the front door	Authentication and authorization decisions are handled by Devolutions Server or Hub, which integrate with directories and identity providers. This allows SMBs to enforce multifactor authentication and identity-centric policies before Gateway forwards traffic to an internal resource.	Devolutions Gateway; Devolutions Server; Devolutions Hub Business
Application-level access instead of network-level tunnels	Instead of dropping users onto a network, Remote Desktop Manager launches RDP, SSH, VNC, ARD, or web sessions through Gateway directly to a given host or service. Internal networks remain hidden while technicians still reach the tools they need for daily work.	Devolutions Gateway; Remote Desktop Manager

Better visibility and auditing of remote sessions	Because sessions are brokered through Gateway and controlled by Devolutions Server or Hub, SMBs get detailed audit logs of who connected to which system, when, and for what duration. Session recording features provide additional evidence where required by policy or regulation.	Devolutions Gateway; Devolutions Server; Devolutions Hub Business; Remote Desktop Manager
Simpler operations for small IT teams	Devolutions Gateway is positioned as a VPN replacement inside a focused remote access management solution. Policies are centralized, integrations with Remote Desktop Manager reduce one-off scripts and profiles, and updates are delivered through regular product releases rather than piecemeal device management.	Devolutions Gateway; Remote Desktop Manager
Easier, safer vendor and contractor access	External technicians can be given controlled access to specific customer environments through Devolutions Gateway without handing out generic VPN credentials. Role-based access controls in Devolutions Server or Hub restrict which entries they see, while all activity is logged and can be recorded for MSP reporting and customer audits.	Devolutions Gateway; Remote Desktop Manager; Devolutions Server; Devolutions Hub Business

Improved performance and user experience	Devolutions Gateway only forwards the traffic of the requested service instead of routing all network traffic through a central VPN concentrator. This helps maintain near-native performance for remote sessions and reduces bottlenecks, which is especially valuable for SMBs that cannot overbuild network capacity.	Devolutions Gateway
Right-sized cost and complexity for SMBs	Devolutions provides packages that combine Devolutions Gateway, Remote Desktop Manager, and vaulting products so SMBs can start small and expand on a single platform. By replacing VPN appliances and complex firewall setups with a just-in-time gateway model, organizations gain better control without committing to an oversized zero trust or a large, expensive and complex SASE project.	Devolutions Gateway; Remote Desktop Manager; Devolutions Server; Devolutions Hub Business; Devolutions PAM

THE FINAL WORD

Remote access is now a core element of operational resilience for SMBs; not a background utility that can be set once and forgotten. It sits directly between external threats and the systems that support and drive day-to-day operations. **As the research shows, VPNs have gone from being good enough, to representing a potentially vulnerable entry point.** Always on tunnels, broad network reach, and limited auditability make it very hard for lean IT teams to control who can do what, where, and when.

A JIT gateway model offers a different and categorically superior approach path:

- **Instead of expanding the network perimeter, it narrows it.**
- **Instead of granting standing access, it creates short-lived, purpose-built sessions.**
- **Instead of relying on coarse network logs, it produces evidence tied to identity and specific systems.**

A JIT gateway infrastructure built on Devolutions Gateway and augmented by one or multiple additional Devolutions' solutions — Remote Desktop Manager, Devolutions Server, Devolutions Hub Business, and/or Devolutions PAM — meets these critical objectives in a way that real-world SMB teams can actually deploy and run. It replaces fragile VPN sprawl with a controllable, auditable, and right-sized model that aligns with how people work today, whether they are internal admins, remote employees, MSP technicians, or external vendors.

Moving to a JIT gateway is not about chasing the latest trend. It is about taking a practical, achievable step toward stronger control over remote access, clearer visibility, and reduced risk. **With Devolutions Gateway and the broader Devolutions ecosystem, SMBs can move away from legacy VPN constraints at their own pace, starting with a few critical workflows and expanding as results come in.** The outcome is a remote access model that actively supports growth and resilience, while giving the people who support it the confidence that they have a secure, modern, and sustainable foundation in place.

NEXT STEPS

Moving from a traditional VPN to a JIT model is not an all-or-nothing decision. You can move at your own pace, starting small and expanding as your confidence grows. There are three practical and free ways to get started:

Free trial: Explore and experience Devolutions Gateway and related Devolutions' solutions in your environment, including Remote Desktop Manager, Devolutions Server, Devolutions Hub Business, and Devolutions PAM. A single evaluation key unlocks the full suite of IT productivity tools, so you can test secure remote access, credential management, and privileged access management together, and see how they integrate.

Live guided demo: These sessions are led by Devolutions experts who walk through how to manage secure, JIT remote access to segmented or isolated networks, and how the platform supports privileged access management in practice. A demo is also the ideal opportunity to get detailed answers about things like integrations, architecture, licensing, and deployment options.

Guided proof of concept: This expert-led program (30-90 days; minimal time investment) enables you to test secure remote access, password management, and connection management in a realistic setting, with clear milestones and ongoing support along the way.

Contact Devolutions at sales@devolutions.net to get started.