

Solving key identity security challenges in SMBs with Silverfort

Small and medium-sized businesses (SMBs) face growing identity-based threats but often with only a handful of IT staff managing everything — from support and system administration to security.

Additionally, both cyber insurance providers and compliance regulators now require stronger security controls, including multi-factor authentication (MFA) enforcement across all the critical systems, but most SMBs struggle to extend their identity security layer beyond the cloud.

With legacy infrastructure and an expanded attack surface from hybrid environments, SMBs are exposed to ransomware and lateral movement attacks. A single breach, often caused by compromised credentials, can disrupt operations, damaging customer trust, and in the end, lead to financial losses that many SMBs may not recover from.

To reduce identity security risks and comply with growing requirements, SMBs must adopt a proactive, identity-first security approach that is both scalable and practical. Just as important, the solution must deploy fast and integrate effectively, minimizing downtime for IT teams already managing a wide range of tools and responsibilities.



What makes SMBs a key target for identity threats?



1. MFA coverage blind spots

Many SMBs use Microsoft Entra ID to enforce MFA for remote desktop access (RDP) and cloud applications, like Outlook and Microsoft 365.

However, they often lack MFA coverage for on-prem resources such as legacy applications, file shares, and command-line tools. These gaps allow attackers to use compromised credentials to gain malicious access and move deeper into the environment.



2. Lack of visibility into non-human identities

Non-human identities (NHIs), including service accounts, scripts, and automated processes, are widely used in SMB environments to run system tasks and connect applications.

NHIs suffer from extremely low visibility, exposing them to compromise and lateral movement. This is especially true for service accounts, which often have excessive privileges and lack of monitoring, making them prime targets for compromise.



3. Manual identity controls and limited capacity

Most SMB IT teams are stretched thin — managing support, infrastructure, and security all at once. Without automation or centralized policy enforcement, access decisions become inconsistent and difficult to audit. These gaps create critical blind spots attackers can exploit through credential compromise or lateral movement.



How Silverfort solves identity security challenges for SMBs

1. MFA for on-prem resources

Silverfort extends MFA protection to all resources and environments, including command-line access, legacy apps, IT infrastructure, and other critical resources that couldn't be protected before.

This ensures consistent enforcement of strong security controls across all access points within hybrid environment and not just cloud infrastructure.

2. Full NHI visibility and security

Silverfort automatically identifies all NHIs within the environment, including on-prem service accounts, and offers the identity and security teams the tools to secure them based on each account's behavior.

By continuously monitoring and enforcing policies on these often-overlooked accounts, Silverfort reduces blind spots and protects against identity-based attacks such as credential compromise and lateral movement.

3. Complete coverage and protection to stay compliant

Silverfort enforces real-time access policies, privileged user monitoring, and continuous MFA coverage across all environments.

By replacing manual process with automated, policy-based controls, Silverfort helps SMBs meet cyber insurance and compliance requirements without adding complexity and operational overhead.

4. Fast deployment and time to value

Silverfort's unique architecture integrates seamlessly with your existing environment. It deploys quickly with minimal resources, doesn't impact Active Directory (AD) performance, and runs due diligence on domain controller health – certified by Microsoft. This allows organizations to significantly improve their identity security posture within days not weeks.

About Silverfort

Silverfort secures every dimension of identity. We deliver end-to-end identity security that is easy to deploy and won't disrupt business operations, resulting in better security outcomes with less work.

Discover every identity, analyze exposures, and enforce protection inline to stop lateral movement, ransomware, and other identity threats.