

Privileged Accounts Protection Reborn with Silverfort



Privileged Account Protection in the Past

Traditionally, entrusting the credentials for these accounts in a PAM vault was the only way to protect against their compromise. Identity and security teams accepted the long and complex deployment process, the need for dedicated customizations, and network segmentation dependency PAM solutions entail, because that was the only reliable alternative to protect against a privileged account's compromise scenario. However, this is no longer the case.

Silverfort Brings Comprehensive MFA Protection to Active Directory Environments

MFA is known to reduce by 99% percent the probability of account takeover. While so far, this capability has been limited to SaaS and modern web applications, Silverfort brings it to every user and resource in the AD environment. This includes all authentication protocols like LDAP, Kerberos and NTLM, as well as command line access tools like PsExec, PowerShell and others that could never have been protected in that manner before.

Privileged Accounts: Off the Vault and into MFA

The Security Aspect

Applying MFA to privileged accounts provides them iron-clad protection against the vast majority of lateral movement and ransomware propagation attacks.

The Operational Aspect

Applying an MFA policy is a simple and straightforward process. While PAM full deployment can be a months-long process, Silverfort MFA policies are operational within minutes of initial installation.

Key Benefits

- ✓ **Rapid Time to Value**
Once Silverfort is installed in the environment, you can create MFA policies for all your privileged accounts within minutes
- ✓ **Minimal Overhead**
Silverfort protects all your machines without requiring any dedicated plugins or customizations
- ✓ **Consistent Protection**
Continuous and consistent protection vs the typical PAM 30 days timeframe that attackers can abuse
- ✓ **No Segmentation Required**
Silverfort's protection is fully effective regardless of east-west segmentation
- ✓ **Service account protection with no password rotation**
Automated discovery, monitoring and policy enforcement on all enterprise service accounts
- ✓ **Lateral movement prevention**
Eliminate lateral movement by enforcing MFA on remote access command line tools

Can Silverfort Complement my PAM Solution?

Definitely. PAM is ideal for local computer accounts, and this is where your vaulting efforts would yield the best results. Silverfort, on the other hand, is best suited for your domain accounts (shared, personal and service accounts), which are the prime target in lateral movement attacks and ransomware propagation. The table to the right summarizes how the two solutions can jointly operate to ensure your environment is protected.

	PAM Vault	Silverfort MFA
Local computer Accounts	●	○
Shared Interactive Domain Accounts	○	●
Personal Domain Accounts	○	●
Service Accounts	○	●

Silverfort Privileged Account Protection in Action

The flow below shows how Silverfort MFA policy mitigates the common attack pattern of compromising admin credentials for malicious access to target resources.

