Silverfort | CYBERARK THE IDENTITY SECURITY COMPANY

How Silverfort boosts your CyberArk PAM investment

Privileged accounts carry standing privileges that are always on, in use or not—which is why many organizations invest in PAM solutions to vault and manage them. The explosion of human and non-human identities, as well as AI agents, is outpacing what many PAM programs can scale to cover across today's modern, hybrid environments.

Silverfort Vaultless PAM immediately extends protection to all privileged identities in your environment, whether they are currently vaulted or not. It adds runtime security controls that reach even the identities most vaults can't—such as Tier-2 users and NHIs—helping you accelerate your PAM investment and reduce risk, quickly and at scale.

Due to its light architecture and rapid deployment, Silverfort allows you to focus on making the most of your existing PAM program, while extending and prioritizing protection to the accounts that are still not onboarded.

Silverfort seamlessly integrates with CyberArk to give you clear visibility into your privileged access posture and prioritize controls over those that are yet unmanaged.

Silverfort and CyberArk PAM Integration

Available for: *On-prem PAS*

The Silverfort and CyberArk PAM integration brings CyberArk account data into Silverfort's Privileged Access Security (PAS) module, so privileged access can be managed in one place, without exposing sensitive account details outside the environment.

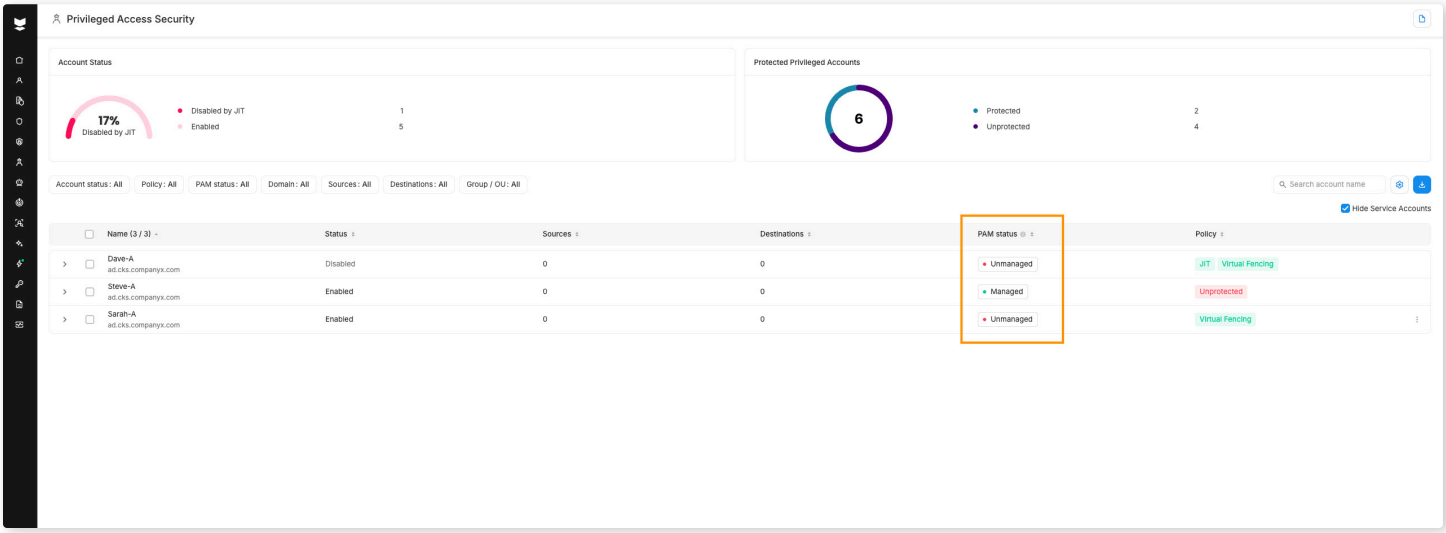
By correlating the accounts vaulted in CyberArk PAM with the privileged identities it discovers across the environment, the integration shows which privileged identities are managed and what protections apply to them, providing full visibility into privileged access coverage.

This gives security teams a regularly updated view of their privileged accounts, including the ability to:

- See a '**Managed**' or '**Unmanaged**' PAM status on every privileged identity Silverfort discovers within their environment
- Filter privileged identities by PAM status to focus on the accounts that aren't covered, and apply security policies and controls
- Keep the status up to date through automated, periodic synchronization with CyberArk

How it works

Silverfort connects to CyberArk PAM over the CyberArk REST API using a least-privileged read-only API user. With PAS deployed on-prem, the connection runs entirely inside the customer environment, so account data never leaves it. On a set interval, it retrieves the accounts vaulted in CyberArk and matches each one to the privileged identities it has already discovered, marking every privileged identity Managed or Unmanaged in the Privileged Access Security page. As accounts are vaulted or removed in CyberArk, the status refreshes automatically, so coverage stays current over time.



Key benefits

Coverage without guesswork

With a Managed or Unmanaged status on every privileged identity, security teams know exactly which of their privileged accounts are vaulted with CyberArk—no guesswork, no manual audits.

Protect at Runtime

Silverfort enforces runtime controls at the moment of access—MFA, virtual fencing, and Just-in-Time access. Even if a legitimate, vaulted credential is exposed, lateral movement and privilege escalation are blocked inline.

Focus on what's exposed

By filtering the privileged identities outside the vault, teams can prioritize the accounts that carry the most risk and bring them into their security strategy at scale, with no additional onboarding projects.

Audit-ready visibility

A current, correlated view of managed privileged accounts gives teams the proof to demonstrate PAM coverage to auditors and the board—without reconciling account lists by hand.

About Silverfort

Silverfort secures every dimension of identity—human, machine, and AI—across on-prem, cloud, and hybrid environments. We are the first to deliver an end-to-end Identity Security platform that is easy to deploy and won't disrupt business operations, resulting in better security outcomes with less work. Discover every identity across every environment, analyze exposures to reduce your attack surface, and enforce security controls inline and at runtime to stop lateral movement, ransomware, and other identity threats.