SILVERFORT

Privileged Access Security (PAS)

Discover, classify, and enforce least privilege and Just-In-Time (JIT) access policies for all your privileged users

Challenge: Limitations of Traditional PAM Solutions

Managing privileged accounts is the cornerstone of protecting an organization's most valuable resources. However, traditional PAM solutions have inherent blind spots that prevent them from providing security to all privileged users. These solutions often entail lengthy and complex deployment cycles and rely on manual account discovery which makes it difficult to quickly identify all privileged users. Additionally, they cannot enforce least privilege access, prevent admins from bypassing the PAM, or eliminate privileged access abuse, leaving critical security gaps in place.

Solution: Silverfort's Privileged Access Security (PAS)

Silverfort offers a new approach to overcoming the limitations of traditional PAM solutions through its unique architecture, which integrates directly with Active Directory. This allows for the instant discovery and classification of privileged accounts, so that no account goes unnoticed. Silverfort provides comprehensive security capabilities designed to protect privileged users from being compromised. Whether used alongside existing PAM solutions for full coverage or as a standalone solution, Silverfort enhances organizational resilience by closing critical security gaps and simplifying the protection of privileged access.

Automated Discovery and Classification

Automatically detect and classify all privileged accounts to different tiers based on the actual privileges they use and determine if regular accounts are being used with privileged intent.

Seamless Just-In-Time Access

Enforce JIT access policies on domain privileged accounts with a single click, to decrease unnecessary access and reduce the identity attack surface.

Virtual Fencing

Allow admin accounts to only access resources that require admin access while blocking access to all other resources.

Non-Intrusive Security

Eliminate the dependency of vaulting and password rotation, with inline protection on the authentication itself.

Your PAS Journey Made Simple with Silverfort

Discover
Automatically discover privileged accounts based on their authentications.

Classify
Prioritize and implement security controls based on privilege tiers.

Fence
Apply least privilege policies by fencing privileged accounts based on access permissions

Just-In-Time (JIT)
Remove standing privileges with JIT policies by granting access rights only when necessary.

How Does it Work

Silverfort automatically discovers and classifies all privileged accounts based on user authentications. This enables organizations to gain comprehensive visibility into all privileged accounts, cross-tier authentications and access requests to identify whether highly privileged accounts are connecting to vulnerable resources in lower tiers. Just-in-Time (JIT) policies can be applied to privileged accounts, so the user only receives permissions as needed and for a limited duration, further reducing the scope of identity attacks.

Kerberos, NTLM, LDAP

Privileged Accounts

Admin, domain admins, app admin, IT Helpdesk and more

Active Directory

AD Managed Resources

including command line access, file shares, and RDP

Silverfort

Discovery and Classification

Policy Configuration

Enforcement Allow/Block/MFA/ JIT