Silverfort | PingIdentity

Silverfort and Ping Identity Integration

Apply PingID MFA protection and risk-based authentication to access requests for all on-prem and cloud resources, including those that couldn't be protected before

Identity-based attacks that utilize compromised credentials to access targeted resources are increasing in scope and sophistication. While Ping Identity's Multi-Factor Authentication (MFA) has proven itself as the ultimate security measure against such attacks, it cannot be applied to core enterprise resources such as legacy applications, on-prem servers, and more. Ping Identity and Silverfort have partnered to address this identity protection challenge by delivering an integration that deploys advanced risk analysis and MFA protection to all resources.

Ping Identity + Silverfort extend MFA protection to:

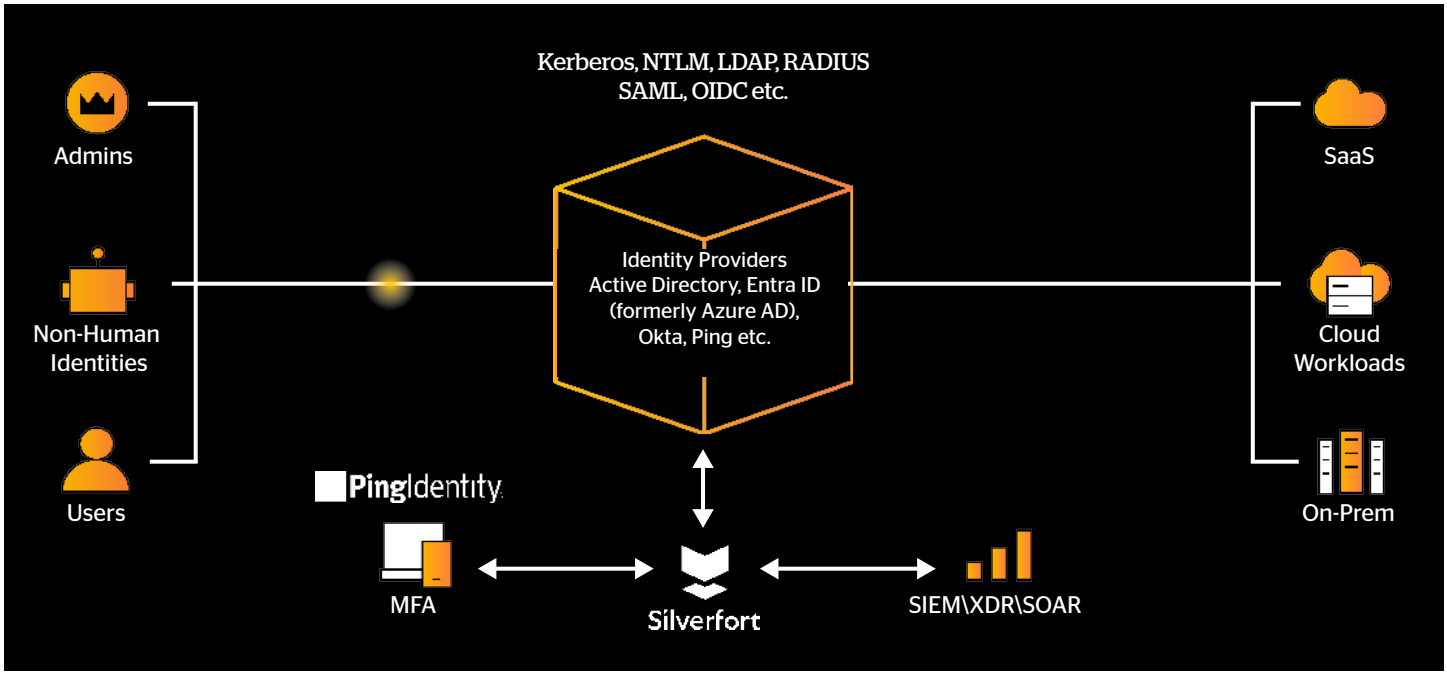
- Legacy applications
- Command line access tools (PowerShell, PsExec, etc.)
- External and internal admin access
- File shares and databases
- IT infrastructure
- Desktop login
- RDP and SSH
- SaaS applications
- And more

End-to-end identity protection with Ping Identity and Silverfort

Silverfort and Ping Identity integration enable users to increase their resilience to identity threats in two aspects. First, customers can extend PingID MFA protection to resources that they couldn't protect before. Second, they can achieve high-precision identity threat detection by analyzing the full context of each incoming access request in Silverfort's risk engine. Together, these capabilities enable users to configure adaptive MFA policies triggered only when a risk is detected to optimize users' experience and avoid MFA fatigue.

How Ping Identity and Silverfort work together

When a user attempts to access a federated app or an on-prem resource, Ping Identity forwards the request to Silverfort which analyzes it based on the full context of the user's on-prem authentication trail, to determine if the level of risk it introduces justifies an MFA step-up. Silverfort leverages its native AD integration to perform a similar risk analysis when a user attempts to access cloud resources as well, and if a risk is detected Silverfort would push this user a PingID MFA notification, thus extending its coverage to the entire environment.



Key benefits

Extend Ping Identity everywhere

Secure access to all resources, on-prem or in the cloud, including those that couldn't be protected until now.

No MFA fatigue

Ensure users are required to provide MFA only when a clear risk is present as detected by Silverfort's risk engine.

Hybrid attacks protection

Detect and prevent advanced identity-based attacks across your entire environment.

Advanced risk analysis

Evaluate the risk of each access attempt based on the user's full context.

Full coverage

Unified identity protection for all on-prem and multi-cloud workloads.

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.