Silverfort and Microsoft AD FS Integration

Apply MFA for Active Directory Federation Services (AD FS) to critical resources without modifying them and gain real-time visibility into all user access requests

Identity-based attacks that utilize compromised credentials to access targeted resources are increasing in scope and sophistication. While Multi-Factor Authentication (MFA) for AD FS has proven itself as the ultimate security measure against such attacks, it cannot be applied to core enterprise resources such as such as legacy applications, on-prem servers, and more. Microsoft 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.

Microsoft AD FS + 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

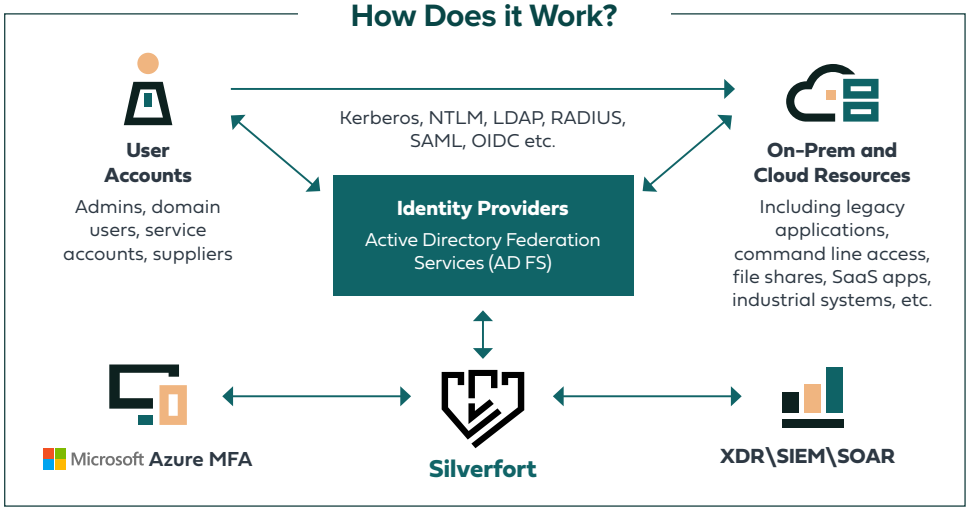
End-to-End Identity Protection with Microsoft AD FS and Silverfort

Silverfort and Microsoft AD FS integration enable users to increase their resilience to identity threats in two aspects. First, customers can extend Azure MFA protection for Active Directory Federation Services (ADFS) 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 Microsoft AD FS and Silverfort Work Together

When a user attempts to access an on-prem resource, Microsoft AD FS 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 Azure 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 an Azure MFA notification, thus extending its coverage to the entire environment.

How Does it Work?



KEY BENEFITS

Extend MFA Protection Everywhere
Secure access to all resources, on-premises or in the cloud, including those that couldn't be protected until now.

Superior 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.

Eliminate 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 lateral movement attacks that traverse between the on-prem and cloud environment.