Silverfort

Silverfort Identity Bridge

Unify and extend modern identity security controls to any system, user, or access path across hybrid and multi-cloud environments

Hybrid identity environments are now the new norm for modern organizations – and with them come new security blind spots. Cloud platforms enforce modern security controls such as phishing-resistant MFA, Conditional Access, and Adaptive Access that continuously verify users and detect risk.

In contrast, on-prem resources still rely on legacy authentication protocols, such as NTLM, LDAP(S), and Kerberos, which can't enforce these same controls.

This disconnect leaves organizations exposed. Attackers exploit these legacy gaps to compromise credentials, move laterally, and access sensitive data.

For security and IAM teams, this fragmentated identity landscape creates inconsistent enforcement, limited visibility, and increased risk. Without a unified approach to protect all identities across on-prem and cloud, organizations face persistent challenges:

- → **Siloed identity tools** enforce inconsistent policies and create visibility gaps across hybrid environments
- → **Legacy authentication protocols** can't support modern security controls
- → **Emerging authentication standards** like FIDO2, passwordless, and number-matching MFA can't extend to legacy systems

What is Silverfort Identity Bridge

Silverfort Identity Bridge unifies identity security across hybrid and multi-cloud environments by extending modern authentication controls to on-prem and legacy systems and access interfaces.

Acting as a SAML-based security layer, it bridges legacy authentication protocols such as NTLM, LDAP(S), and Kerberos with modern frameworks. This enables organizations to enforce phishing-resistant MFA, SSO, and risk-based access on any resource – cloud or on-prem.

By integrating previously unprotected systems into a unified policy framework alongside cloud and SaaS applications, Silverfort Identity Bridge delivers consistent enforcement, simplified management, and stronger protection against identity-based threats. Organizations can now extend existing cloud IdP controls to any or all on-prem authentications, closing a long-standing gap that was once considered an accepted risk.

By integrating previously unprotected systems into a unified policy framework alongside cloud and SaaS applications, Silverfort Identity Bridge delivers consistent enforcement, simplified management, and stronger protection against identity-based threats. Organizations can now extend existing cloud IdP controls to any or all on-prem authentications, closing a long-standing gap that was once considered an accepted risk.

How it works

Silverfort Identity Bridge integrates directly with an organization's cloud identity provider (IdP), extending its authentication flows and security policies to all on-prem and legacy resources

Step 1:
Intercept authentication requests

When a user authenticates to an on-prem resource, Silverfort intercepts the authentication request via Active Directory Adapter or another IdP enforcement point and routes it through the Identity Bridge

Step 2:
Extend cloud identity policies

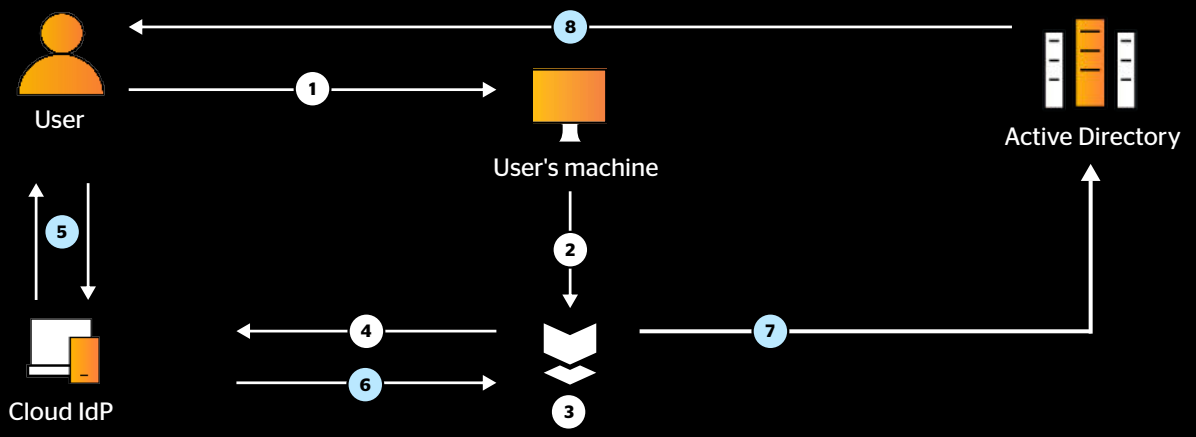
The bridge translates legacy authentication into a modern SAML request and sends it to the existing IdP, which evaluates it against configured access policies and enforces MFA, FIDO2, or other risk-based controls.

Step 3:
Enforce decisions inline

Silverfort enforces the IdP's decision inline in real time, ensuring consistent policy enforcement and providing unified visibility across all authentication activity.

The result: A single, unified layer of identity security across hybrid environments, where modern authentication and risk-based protection extend to every user, system, and access path.

Enabling the Silverfort Identity Bridge



1. User initiates an authentication to on-prem resources (to Active Directory) and sends Active Directory (AD) a request to access the resource.
2. AD forwards the request to Silverfort.
3. Silverfort evaluates the authentication and decides whether to allow, trigger MFA, or block.
4. If Silverfort triggers MFA, Silverfort sends the access request to Cloud IdP.
5. Cloud IdP evaluates the authentication based on set policy and sends the MFA request to the user.
6. After user's identity verification, Cloud IdP forwards the verdict to Silverfort.
7. Silverfort accepts the verdict and forwards it to AD.
8. AD sends the response to the user to either allow the authentication or block it.

Key benefits

Unified Policy Enforcement

Secure on-prem environments and resources with Cloud IdP policies via Silverfort, reducing identity-based risks.

Seamless User Experience

Provide users with a consistent and familiar experience when accessing any resource, both on-prem and in the cloud.

Protect the 'Unprotectable'

Extend Cloud IdP MFA and access policies to any resource, including on-prem servers, legacy apps, IT infrastructure, and command-line tools.

Hybrid Attack Protection

Detect and prevent advanced lateral movement attacks that connect between the on-prem and cloud environments.

About Silverfort

Silverfort secures every dimension of identity—humans or machines across the cloud and on-prem. 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.