Silverfort | onelogin

Bridging on-prem authentication with OneLogin

Extend OneLogin security controls to on-prem resources with Silverfort's bridge, applying access policies across hybrid environments.

Silverfort's OneLogin Identity Bridge enables organizations to implement OneLogin web SSO flows to on-prem applications. Enterprises gain real-time protection against identity-based attacks utilizing compromised credentials to access enterprise on-prem or multi-cloud resources. Silverfort bridge allows organizations to extend authentications with OneLogin, enabling better visibility into their users' and resources' activities across web and on-prem applications.

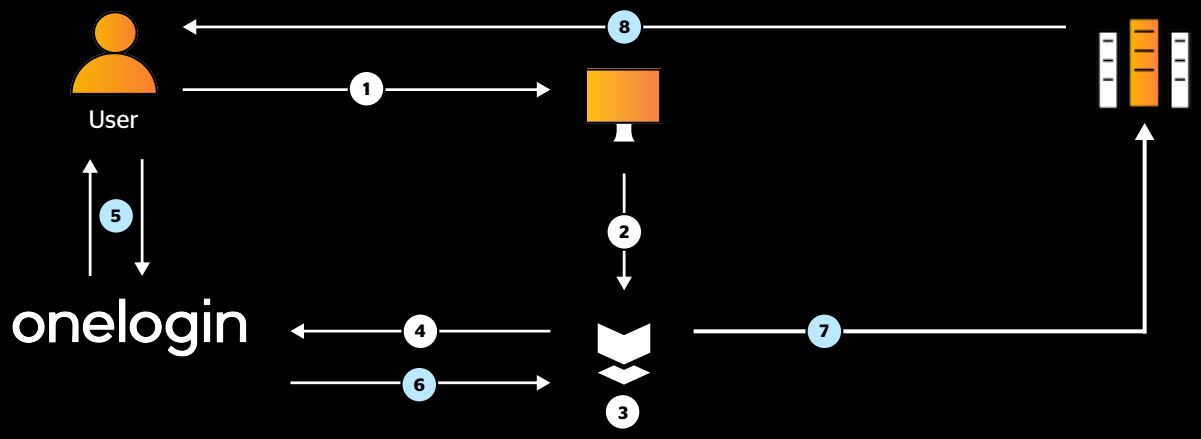
Bridging legacy resources

Silverfort seamlessly bridges any type of authentication (legacy apps, command-line tools, and more) into OneLogin as if it were a modern web application. With Silverfort's OneLogin bridge, customers can create SAML apps for on-prem resources, allowing them to leverage any OneLogin authentication flow. By applying a policy to each bridged on-prem resource, organizations can unify hybrid resource management. Once authentication and access policies are set, Silverfort forwards all access attempts through the bridged application to OneLogin, where they are managed, monitored, and secured.

How does Silverfort's OneLogin bridge work

Silverfort acts as a SAML Service Provider (SP) and seamlessly integrates legacy authentication protocols like Kerberos, NTLM, and LDAPS into OneLogin, allowing them to be treated like a modern web application. Users can define access policies for these bridged applications, leveraging OneLogin security controls and MFA capabilities. By applying policies to each bridged on-prem resource, organizations can unify hybrid resource management. Once authentication and access policies have been configured, Silverfort forwards all access attempts to OneLogin, where they are managed, monitored, and secured.

Enabling the OneLogin 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 OneLogin.
5. OneLogin evaluates the authentication based on set policy and sends the MFA request to the user.
6. After user's identity verification, OneLogin 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 OneLogin 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 OneLogin 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—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.