Silverfort | CYBERARK THE IDENTITY SECURITY COMPANY

Bridging On-Prem Authentication with CyberArk Identity

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

Silverfort's CyberArk Identity Bridge enables organizations to implement CyberArk 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 cloud resources. Silverfort bridge allows organizations to extend authentications with CyberArk Identity, enabling better visibility into their users' and resources' activities across web and on-prem applications.

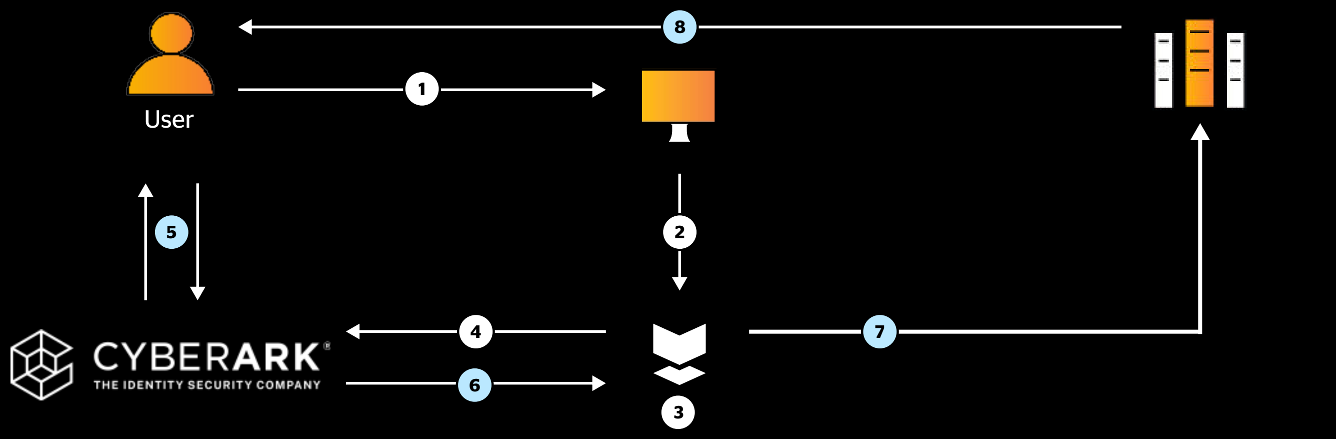
Bridging legacy resources

Silverfort seamlessly bridges any type of authentication (legacy apps, command-line tools, and more) into CyberArk Identity as if it were a modern web application. With Silverfort's CyberArk Identity bridge, customers can create SAML apps for on-prem resources, allowing them to leverage any CyberArk Identity 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 CyberArk Identity, where they are managed, monitored, and secured.

How does Silverfort's CyberArk Identity bridge work

Silverfort acts as a SAML Service Provider (SP) and seamlessly integrates legacy authentication protocols like Kerberos, NTLM, and LDAPS into CyberArk Identity, allowing them to be treated like a modern web application. Users can define access policies for these bridged applications, leveraging CyberArk Identity's 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 CyberArk Identity, where they are managed, monitored, and secured.

Enabling the CyberArk 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 CyberArk.
5. CyberArk evaluates the authentication based on set policy and sends the MFA request to the user.
6. After user's identity verification, CyberArk 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 CyberArk Identity policies via Silverfort, reducing identity-based risks.

Protect the 'Unprotectable'

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

Seamless User Experience

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

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. 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.