Silverfort | PingIdentity.

Bridging on-prem authentication with PingAM and PingOne Advanced Identity Cloud (AIC)

Extend PingAM and PingOne Advanced Identity Cloud (AIC) security controls to on-prem resources with Silverfort's bridge, applying access policies across hybrid environments.

Silverfort's PingAM and PingOne AIC Bridge enables organizations to implement PingAM and PingOne AIC 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 PingAM and PingOne AIC, enabling better visibility into their users' and resources' activities across web and on-prem applications.

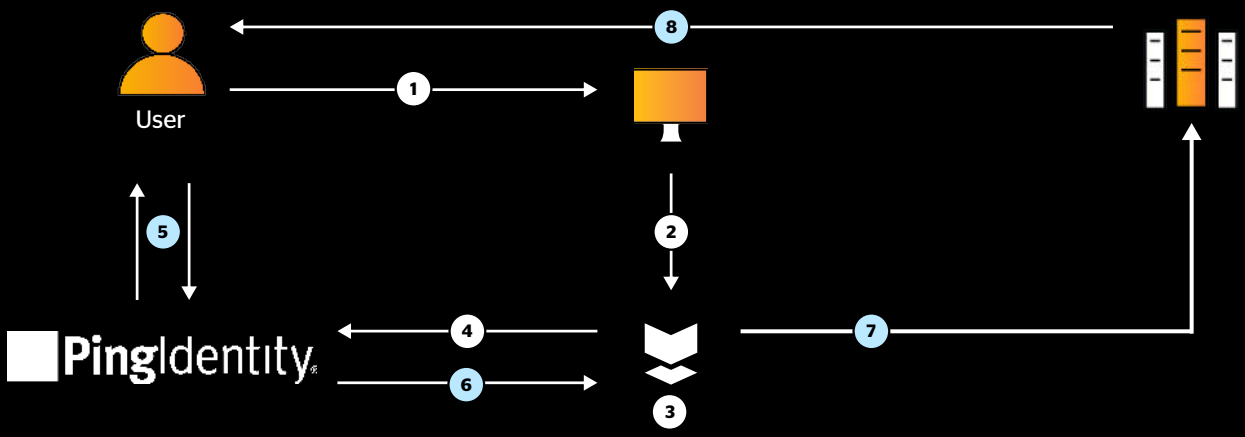
Bridging legacy resources

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

How does Silverfort's PingFederate bridge work

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

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