Silverfort's PingFederate Bridge

Silverfort's PingFederate Bridge enables organizations to implement PingFederate web SSO flows to on-prem applications within their PingFederate environment and apply security controls to these resources. 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 PingFederate, enabling better visibility into their users' and resources' activities across web and on-prem applications.

Bridging Legacy Resources

PingFederate security controls can be extended using Silverfort bridging, while access policies can be applied to any resource on-prem or in multi-cloud environments. This enables organizations to apply strong modern identity security controls to all resources. By enforcing new security measures with Silverfort, organizations can take proactive measures against incoming cyber threats such as lateral movement attacks.

How Does Silverfort's PingFederate Bridge Work

Silverfort seamlessly bridges any type of authentication (legacy apps, command-line tools, and more) into PingFederate as if it were a modern web application. With Silverfort's PingFederate bridge, customers can create enterprise application objects representing the on-prem resource in PingFederate and views this object as a SaaS app like any other cloud-based application. In PingFederate, configure an access policy for the application object that can utilize PingFederate's security controls and PingID MFA. By creating and applying the policy to each bridged on-prem resource, organizations will consolidate hybrid resources. Once the authentication and access policies have been configured, Silverfort monitors and protects attempts to access resources. All bridged applications can now be managed, monitored, and protected in PingFederate.

1. User sends Active Directory (AD) a request to access resource.
2. AD forwards the request to Silverfort.
3. Silverfort sends the access request to PingFederate.
4. PingFederate evaluates authentication based on its policy and makes a verdict if to allow/MFA or block.
5. PingFederate forwards the verdict to Silverfort.
6. Silverfort accepts the verdict and forwards it to AD.
7. AD sends the response to the user to either allow the authentication or block it.
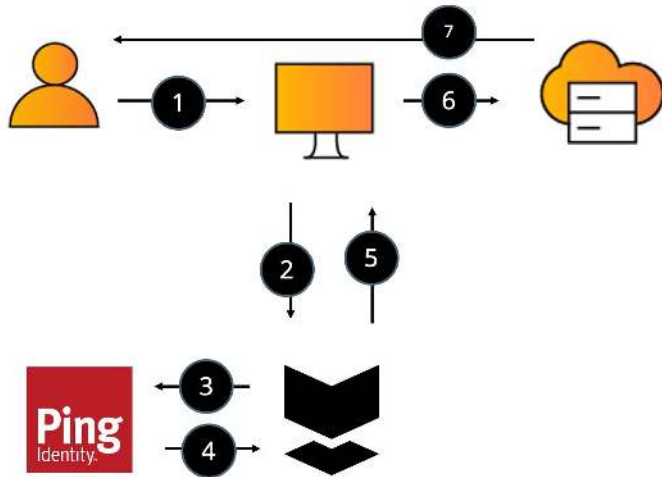
*A similar flow would apply upon attempting to access any other resource – the only change is the respective directory.

KEY BENEFITS

Unified Policy Enforcement
Secure on-prem environments and resources with PingFederate policies via Silverfort, reducing identity-based risks.

Protect the 'Unprotectable'
Extend PingID 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 traverse between the on-prem and cloud environments.