Silverfort | KEYLESS

Bridging on-prem authentication with Keyless Security

Extend Keyless security controls to on-prem and SaaS resources with Silverfort's bridge.

Keyless is a biometric authentication solution that enhances workforce security with privacy-preserving facial biometrics. As Silverfort's only biometric solution, Keyless seamlessly extends to both on-prem and SaaS environments and can authenticate employees in-app across both mobile and desktop. With Keyless policies and workflow, you can enforce modern identity security controls to all critical resources in your hybrid environment and get real-time protection against identity-based attacks.

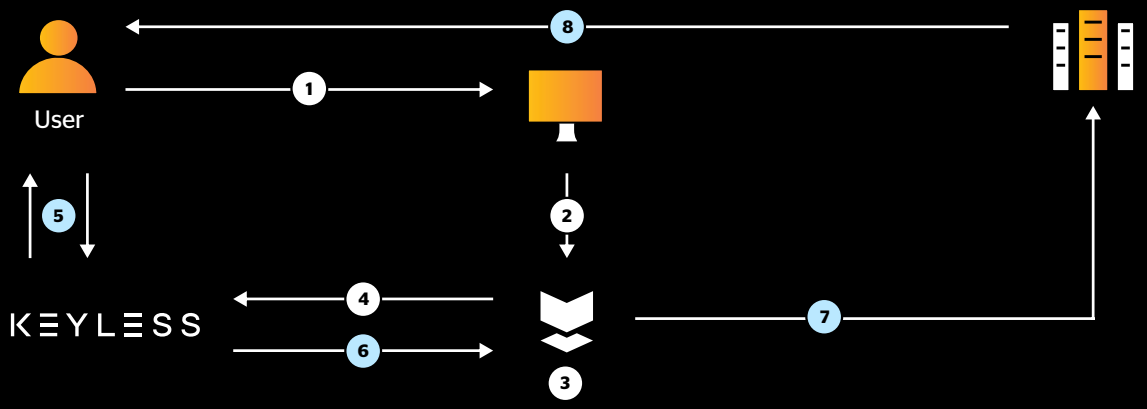
Bridging legacy resources

With our bridging capabilities, Silverfort extends Keyless phishing-resistant MFA to any resource in on-prem or multi-cloud environments, so you can deploy proactive measures against incoming cyber threats, such as lateral movement attacks. You'll also get end-to-end visibility into all users' and resources' activities across web and on-prem applications.

How does Silverfort's Keyless bridge work?

Silverfort bridges any type of authentication into Keyless as if it were a modern web application. Keyless can then view and support all authentications, even on-prem, like any other cloud-based or SaaS application. Users can configure an access policy for the application object to use Keyless' security controls and MFA capabilities. By applying the policy to each bridged on-prem resource, organizations can easily consolidate their hybrid resources. Once the authentication and access policies have been configured, Silverfort monitors and protects attempts to access resources.

Enabling the Keyless 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 Keyless.
5. Keyless evaluates the authentication based on set policy and sends the MFA request to the user using facial recognition.
6. After user's identity verification, eyless 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.

Enabling the Keyless bridge

Unified policy enforcement

Secure on-prem environments and resources with Keyless 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 Keyless 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 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.