Silverfort | yubico

Silverfort and Yubico integration

Apply YubiKey MFA protection and risk-based authentication to access requests for all on-prem and cloud resources, including those that could not be protected before

It has been proven that Yubico's multi-factor authentication (MFA) is the most effective hardware-based security measure against identity-based attacks. However, it has been difficult to extend YubiKeys to all environments to provide secure access to critical resources such as legacy applications, command line access, file shares, databases, and others. To address this challenge, Yubico and Silverfort offer a native integration to deliver real-time risk analysis and MFA protection.

Yubico + Silverfort extend MFA protection to:

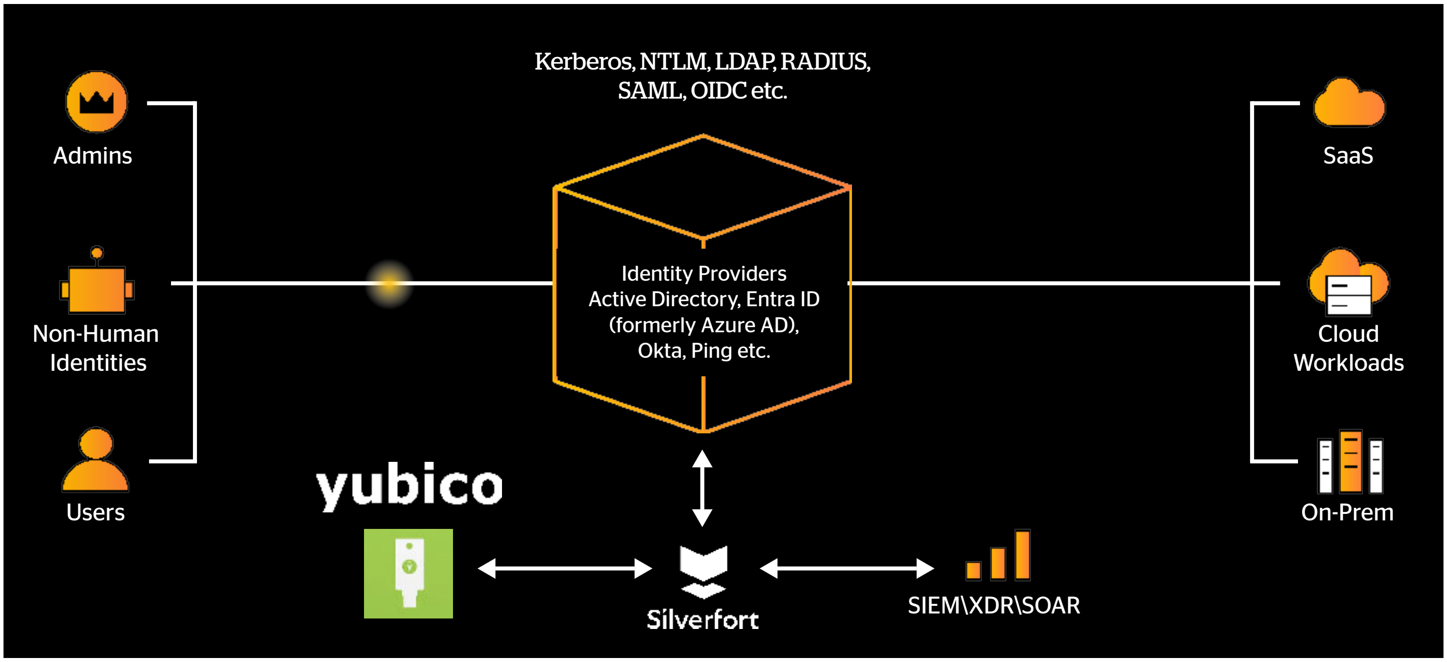
- Legacy applications
- Command line access tools (PowerShell, PsExec, etc.)
- External and internal admin access
- File shares and databases
- IT infrastructure
- Desktop login
- RDP and SSH
- SaaS applications
- And more

Comprehensive coverage with Yubico and Silverfort

By integrating Silverfort and Yubico, users can increase their resilience to identity threats on two fronts. First, customers can extend FIDO2-enabled YubiKey MFA protection to resources they couldn’t protect before. Second, Silverfort enforces adaptive authentication and Zero Trust security policies with the YubiKey to maximize security without disrupting legitimate users. Together, these capabilities enable users to configure adaptive MFA policies triggered only when a risk is detected to optimize users’ experience and avoid MFA fatigue.

How Yubico and Silverfort work together

Whenever a user attempts to access a resource, Silverfort analyzes the context of the user's full on-prem and cloud authentication history to determine whether an MFA step-up is justified. If MFA is required, a push request will be sent to the user's machine, and the user will be prompted to insert their YubiKey to verify their identity and approve the MFA request. Silverfort also leverages its native AD integration to perform a similar risk analysis when a user attempts to access an on-prem resource. If a risk is detected, Silverfort will push a YubiKey MFA notification to this user, extending its coverage to the entire environment.



Key benefits

Extend YubiKey MFA everywhere

Secure access to all resources, on-prem or in the cloud, including those that couldn't be protected until now.

Real-time protection

Detect and prevent advanced identity-based attacks across your entire environment.

No MFA fatigue

Ensure users are only required to respond to an MFA request when Silverfort's risk engine detects irregular activity.

Advanced risk analysis

Evaluate the risk of each access attempt based on the user's full context.

Consistent user experience

Provide users with a single MFA solution when requesting access to any resource, on-prem or on the cloud.

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.