Silverfort and Thales FIDO2 Integration

Apply Thales FIDO2 Multi-Factor Authenticators protection and Silverfort risk-based authentication to access requests for all on-prem and cloud resources

Multi-factor authentication (MFA) is the most effective hardware-based security measure against identity-based attacks. However, extending FIDO2 MFA keys to all environments to provide secure access to critical resources has proven difficult. To address this challenge, Thales and Silverfort offer a native FIDO2 integration to deliver real-time risk analysis and MFA protection to users' authentication journey.

Thales + Silverfort Extend MFA Protection to:

- Legacy applications
- Command line access tools (PowerShell, PsExec, etc.)
- IT Infrastructure
- External and internal admin access
- File shares and databases
- Desktop login
- RDP and SSH
- SaaS applications
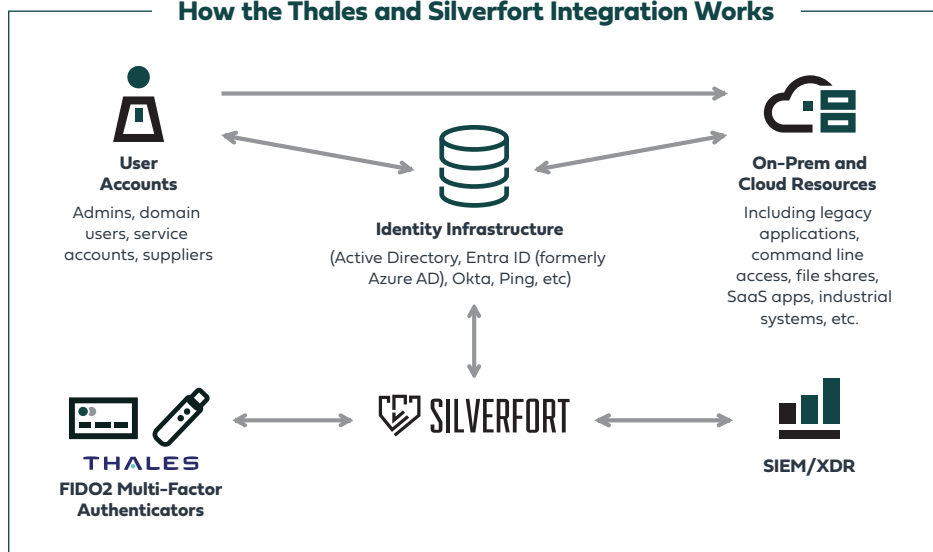- Multiple Devices (Laptops, Desktops and Mobile)

Complete Coverage with Thales and Silverfort

By integrating Silverfort and Thales, customers can increase their resilience to identity threats on three fronts. First, customers can extend Thales' FIDO2 smart cards and USB tokens for MFA protection to resources they couldn't protect before. Second, Silverfort enforces adaptive authentication and Zero Trust security policies to maximize security without disrupting legitimate users. Third, Thales provides FIDO2 smart cards and USB tokens in various form factors that make them compatible with various devices. With these capabilities, customers optimize users' experience and prevent MFA fatigue.

How Thales and Silverfort Work Together

Whenever a user attempts to access a resource, Silverfort analyzes their full on-premises 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 Thales FIDO2 key 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 Thales FIDO2 MFA notification to the user, extending its coverage to the entire environment.

How the Thales and Silverfort Integration Works

User Accounts
Admins, domain users, service accounts, suppliers

Identity Infrastructure
(Active Directory, Entra ID (formerly Azure AD), Okta, Ping, etc)

On-Prem and Cloud Resources
Including legacy applications, command line access, file shares, SaaS apps, industrial systems, etc.

THALES
FIDO2 Multi-Factor Authenticators

SILVERFORT

SIEM/XDR

KEY BENEFITS

Extend Thales FIDO2 Smart Cards and USB Tokens Everywhere
Secure access to all resources, on-prem or in the cloud, including those that couldn't be protected until now.

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

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

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

Meet High Security Standards
Comply with your market regulation by using authenticators compliant with the highest security standards (FIDO2, FIPS, Common Criteria).