Silverfort | T2KEN

Silverfort and Token2 integration

Apply Token2 FIDO2 MFA protection and risk-based authentication to access requests for all on-prem and cloud resources, including those that could not be protected before.

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, Token2 and Silverfort offer a native integration to deliver real-time risk analysis and MFA protection.

Token2 + 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
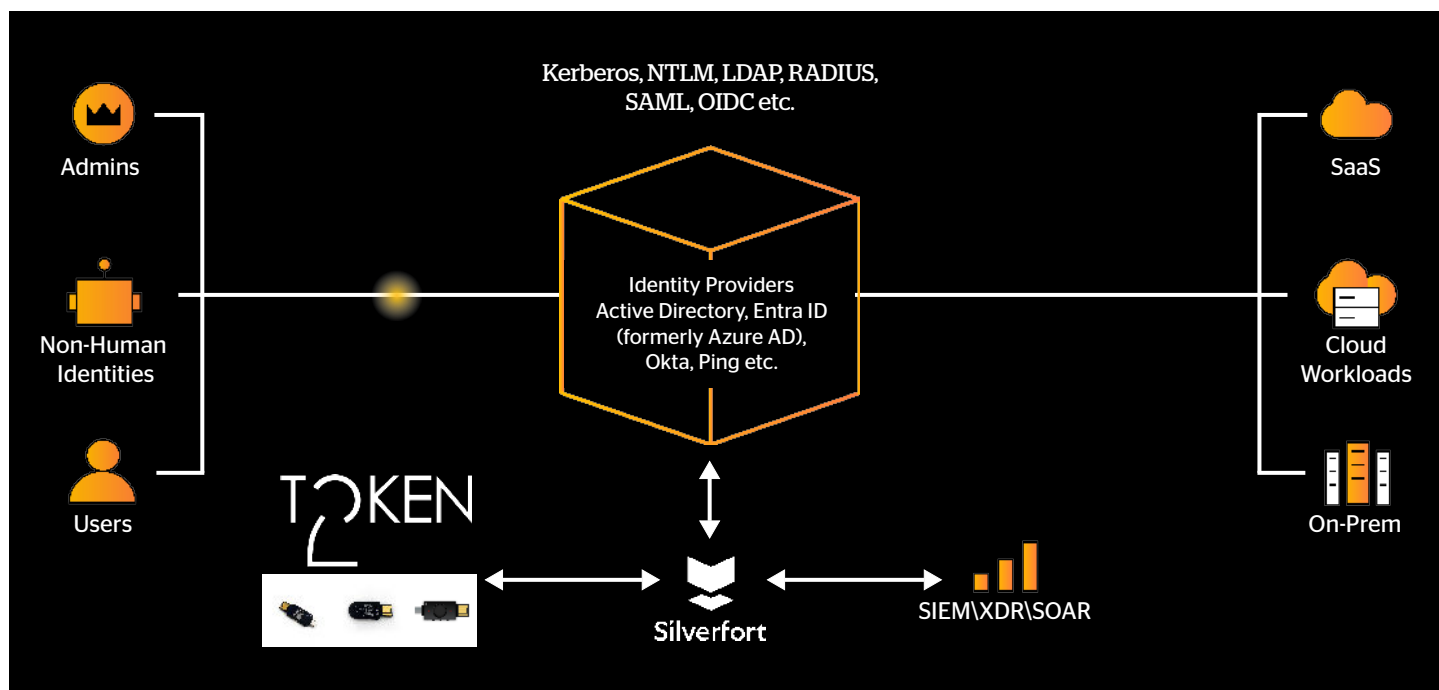- RDP and SSH
- SaaS applications
- And more

Comprehensive coverage with Token2 and Silverfort

By integrating Silverfort and Token2's Pin + Series (which is open-source and has undergone a public security assessment), users can increase their resilience to identity threats on two fronts. First, customers can extend FIDO2-enabled MFA protection to resources they could not protect before. Second, Silverfort enforces adaptive authentication and Zero Trust security policies with Token2 FIDO2 keys 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 Token2 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 Token2 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. When a risk is detected, Silverfort will send a Token2 FIDO2 MFA notification to the user, thus extending its coverage to the entire environment.

Kerberos, NTLM, LDAP, RADIUS, SAML, OIDC etc.

Admins

Non-Human Identities

Users

T2KEN

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

SaaS

Cloud Workloads

On-Prem

Silverfort

SIEM\XDR\SOAR

Key benefits

Extend Token2 FIDO2 MFA everywhere

Secure access to all resources, on-prem or in the cloud, including those that could not 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.

No MFA fatigue

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

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.

Silverfort