Silverfort

Silverfort Universal MFA

Extend MFA protection to every resource and application across on-prem, multi-cloud and hybrid environments

The Challenge: **Incomplete MFA coverage leaves identities exposed**

While MFA adoption has become widespread, most organizations struggle to achieve full coverage across all users and access paths. Traditional MFA tools are limited to cloud and web-based applications, leaving critical gaps across on-prem, legacy, and OT systems that don't natively support modern MFA methods. These blind spots are exploited for lateral movement, ransomware propagation, and credential-based attacks.

At the same time, cyber insurance and compliance frameworks now mandate MFA protection for every user, system and access path, not just cloud or privileged accounts.

For IAM and security teams, achieving this level of consistency remains a major challenge:

- **MFA fragmentation** creates inconsistent enforcement and visibility gaps across multi-cloud, on-prem, and hybrid environments
- **Legacy blind spots** leave on-prem and OT systems unsecured, exposing them to credential-based attacks
- **Compliance pressure** makes it harder for organizations to meet strict MFA requirements across all users and access paths, while staying audit- and insurance-ready

Universal MFA: Extend adaptive MFA to every user and access path

Extend MFA protection to every resource and access path, including homegrown applications, legacy systems, OT, and SaaS apps, by enforcing MFA directly at the authentication layer. Eliminate blind spots and secure every authentication flow with no infrastructure changes.

Deliver adaptive, risk-based authentication through rule-based and contextual MFA triggers that respond in real time to user, device, and behavioral risk. Prevent lateral movement with MFA protection that activates the moment suspicious authentications or credential compromise are detected.

Unify and simplify MFA management across on-prem, cloud, and hybrid environments with centralized policy control and consistent user experience. Consolidate fragmented MFA tools into a single platform that enhances visibility, strengthens identity security, and ensures full compliance coverage across all systems

How it works

Silverfort extends MFA protection across every authentication flow across cloud, on-prem, and hybrid environments by integrating directly with Active Directory and enforcing adaptive MFA policies in real time:

Step 1: Connect directly to Active Directory

Silverfort integrates natively with AD and monitors all authentication traffic across cloud, on-prem, and hybrid environments, without any infrastructure or application changes.

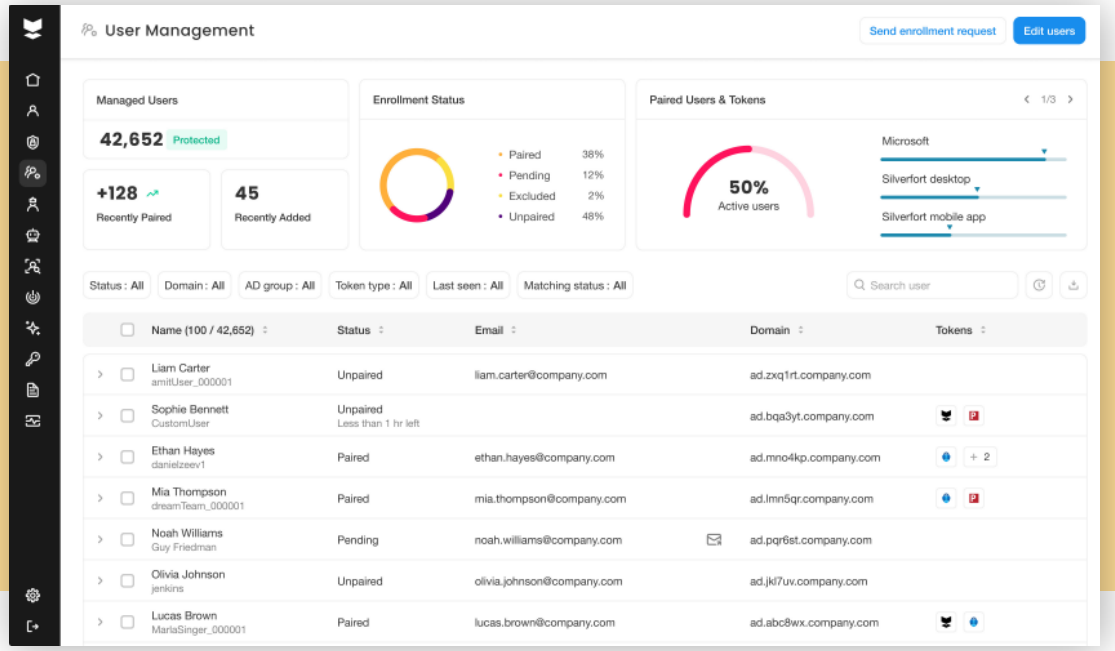
Step 2: Evaluate and enforce in real time

Every authentication request is analyzed and enforces static and risk-based MFA policies instantly when anomalous or risky behavior is detected.

Step 3: Protect every access path

Silverfort applies MFA at the authentication protocol layer (Kerberos, NTLM, LDAP) to prevent credential-based attacks and lateral movement across hybrid environments.

The result: Organizations achieve complete MFA coverage across hybrid environments, stop credential-based attacks in real time, and meet compliance requirements without changing infrastructure



About Silverfort

Silverfort secures every dimension of identity—humans or machines across the cloud and on-prem. 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.