Silverfort

Protect the identities behind every financial transaction

A compromised credential can be a master key to the systems that move money. In financial services, the distance between access to material impact can be measured in minutes , especially in the era of AI-powered attacks.

Yet core banking platforms, mainframes, and legacy systems are unevenly protected and difficult to modernize. The same gap is growing in the cloud, where machine identities, API keys, and AI agents accumulate access without clear ownership.

Silverfort closes Identity Security gaps for financial institutions, before trust becomes impact.

Silverfort prevents compromised credentials from causing damage. Every access request is evaluated in real time at the authentication layer across AD, cloud, and hybrid environments—even for identities and authentication paths beyond the reach of traditional identity tools.

- → Extend MFA to legacy and critical systems, no app changes required
- → Replace standing admin privileges with Just-in-Time access
- → Restrict service accounts to their intended sources, destinations, and protocols
- → Block unauthorized privileged access across remote and administrative pathways
- → Control AI agent actions at runtime before execution

For CISOs

Reduce risk across unvaulted identities, persistent privilege, third-party access, and legacy authentication paths. Contain a compromised identity before it enables fraud, ransomware, or a material security event.

For IAM leaders

Extend MFA, Least Privilege, and access control to the identities your existing IAM and PAM programs haven't reached yet, without a redesign or lengthy deployment.

For Compliance

Continuously demonstrate that access controls are operating across regulated systems and critical functions—not only when the assessment window opens.

Reduce financial, operational, and regulatory risk

Silverfort helps financial institutions reduce the likelihood and blast radius of credential compromise, protect the continuity of critical services, and demonstrate that access controls remain effective across regulated environments.

Protect critical systems without waiting for modernization

Close MFA and access-control gaps across core banking, payment, trading, and legacy systems. Silverfort extends adaptive MFA and policy enforcement across AD authentications such as Kerberos, NTLM, and LDAP.

Enforce control at the speed of financial risk

When compromise can become loss in minutes, detection is not enough, especially in the era of AI-powered attacks.
Silverfort evaluates every access request as it happens and enforces policy inline—before access is granted, not after the fact.

Prevent service accounts from becoming lateral movement paths

Protect the machine identities behind clearing, reconciliation, reporting, and essential financial processes. Silverfort discovers all service accounts and uses Virtual Fencing to restrict them to approved sources, destinations, and protocols without requiring credential rotation or application changes.

Protect privileged access and enforce Least Privilege

Reduce standing privilege and privilege sprawl across your environments. Silverfort discovers all privileged identities and applies Just-in-Time access, MFA on administrator tools, tier-segmentation, Least Privilege and runtime restrictions for each privileged access attempt.

Scale cloud and AI adoption without unmanaged privilege

Maintain ownership, accountability, and Least Privilege as machine identities and AI agents gain access to financial systems and data. Silverfort discovers, classifies, and maps NHIs and AI agents to owners while enforcing policy on AI agent actions at runtime.

Prove that controls remain effective between assessments

Demonstrate that access policies remain enforced across regulated systems and critical financial processes. Silverfort provides ongoing evidence of authentication activity, policy decisions, exceptions, and blocked access, not only a snapshot prepared for the next assessment.

From identity risks to financial resilience

Your policies define who should have access. Silverfort verifies whether that access should still be allowed—every time it is used.