Silverfort

Silverfort for Active Directory: Close identity security gaps, contain lateral movement

For more than 90% of organizations, Active Directory (AD) remains the core system managing authentication and access. Yet after decades of group sprawl, acquisitions, and inconsistent practices, most AD environments carry significant identity tech debt: layers of outdated configurations, over-permissioned users, shadow admins, and unmanaged accounts that attackers know how to exploit. As organizations move to hybrid identity models, this legacy complexity extends to cloud IdPs and expands the attack surface even further.

Without a proactive approach to securing AD, organizations face persistent challenges:

→ **Lack of visibility across all AD accounts, including human, service, and shared accounts,** creates blind spots that attackers exploit for lateral movement and privilege escalation

→ **Reliance on legacy protocols and misconfigurations** (e.g. Kerberos-to-NTLM fallbacks, **NTLMv1/NTLMv2 usage**), combined with the lack of native MFA support, leaves critical on-prem resources and legacy applications exposed

→ **Accumulated identity tech debt,** including stale accounts, shadow admins, long-lived secrets, and no clear ownership, increases licensing costs, drives audit failures, and introduces hidden risks

→ **Fragmented controls** designed for provisioning, not live authentication, leave gaps between detection and enforcement, limiting the ability to respond to threats in real time

How Silverfort helps to close the identity security gaps in AD

The Silverfort Identity Security Platform solves AD blind spots with real-time visibility, control, and protection beyond the reach of traditional tools:

- **See every AD authentication in real time.** Monitor **Kerberos, NTLM, LDAP** across users, service accounts, devices, and servers; detect **Kerberos-denied to NTLM fallbacks** and other risky authentication patterns as they occur.

- **Strengthen AD hygiene at scale.** Automatically classify all accounts, including human, service, shared, and admin accounts, to uncover **shadow admins, stale users, and unmanaged identities.** Map where service accounts actually authenticate to establish ownership and remediate safely.

- **Enforce adaptive security controls in real time.** Deny risky access or apply **MFA protection** instantly. Use **virtual fencing policies** to restrict service and privileged accounts so they can only authenticate between approved sources and destinations.

- **Modernize authentication protocols without disruption.** Identify where Kerberos can replace legacy authentication, prioritize **NTLMv1 elimination**, and enforce **policy-based controls for NTLMv2** to advance protocol security without any infrastructure changes.

How it works

Step 1: Gain end-to-end visibility into AD authentications

Silverfort integrates directly with the existing organization's environment to continuously monitor every AD authentication (Kerberos, NTLM, LDAP) and activity across all users, service accounts, and legacy protocols, with no impact on performance. Spot Kerberos-denied to NTLM fallback and misconfigured SPNs immediately.

Step 2: Discover risks and improve identity security posture

By analyzing AD authentication activity, Silverfort uncovers identity exposures including shadow admins, stale users and unmanaged service accounts, enabling security teams to close critical posture gaps.

Step 3: Enforce adaptive protection and least privilege

With complete visibility in place, Silverfort extends MFA protection and granular access-based controls to AD resources and legacy systems—including service accounts and privileged users—to prevent lateral movement and privilege escalation in real time.

Key benefits

Reduce the risk of ransomware and lateral movement

Proactively stop attackers from exploiting AD blind spots to escalate privileges or spread ransomware.

Simplify identity security operations

Extend MFA and least privilege controls seamlessly across AD and legacy systems, reducing complexity and operational overhead.

Lower costs and accelerate audits

Discover and remediate stale accounts, shadow admins, and unused service accounts to reduce licensing spend and streamline compliance reporting.

Strengthen compliance readiness

Extend security controls across all AD identities and resources, with complete visibility and privileged access security to meet compliance requirements.

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.