



5 Ways to step up your AD hygiene with Silverfort

Active Directory (AD) still runs authentication and access for most enterprises, and it's one of attackers' favorite targets. They rarely break in; they log in and move through identity using the legacy protocols, over-permissioned accounts, and forgotten credentials already in place, and AI-powered attacks make that faster than ever. Staying ahead of them means reducing the attack surface before someone else finds it.

Here are five ways Silverfort helps you strengthen your AD hygiene.

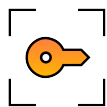


1. Detect shadow admins

Shadow admins hold admin-level privileges no one intended to grant, usually through Access Control List (ACL) inheritance or nested group membership, so they rarely show up in a standard access review.

How Silverfort helps: Silverfort's Identity Security Posture Management (ISPM) automatically detects shadow admins across on-prem and cloud as a prioritized exposure, so you can remove the excess rights or document the access.

Customer example: [NHS Blood and Transplant](#) used Silverfort to surface shadow admins and unusual authentication patterns across its 7,000-user AD, bringing them under management for DSPT and CAF compliance.



2. Reduce weak encryption and legacy protocols

Weak authentication runs quietly on systems no one has touched in years. **NTLMv1** uses weak DES encryption that cracks in seconds, and NTLM relay lets an attacker authenticate as a user without their password, and many teams believe it's disabled while misconfigured apps keep it alive. **RC4 in Kerberos** is just as dangerous: RC4-encrypted tickets are open to Kerberoasting, and with Microsoft now phasing RC4 out, any dependency you haven't mapped will start causing authentication failures.

How Silverfort helps: ISPM flags weak Kerberos encryption and legacy protocol use as prioritized exposures, and Authentication Logs confirm exactly where it's happening, down to the account, source, and service, so you can drive it out without capturing a single packet.

Customer example: [University of the Pacific](#) used Silverfort to detect and retire legacy authentication protocols across its four AD domains, cutting the technical debt tied to outdated infrastructure.



3. Find stale accounts and unrotated passwords

Stale accounts (dormant users, orphaned service accounts, former employees never disabled) are easy to miss without authentication monitoring, and the most dangerous ones still carry admin rights or passwords that never rotate.

How Silverfort helps: Silverfort continuously analyzes authentication activity to surface stale accounts, unrotated passwords, and dormant accounts that still hold privileged access.

Customer example: Encora used Silverfort to surface dormant accounts, unrotated passwords, and unmanaged identities across its decentralized AD, giving the security team a prioritized cleanup list for the first time.



4. Disable admins with SPN

An admin account with a **Service Principal Name (SPN)** is exposed to Kerberoasting: an attacker requests its Kerberos ticket, brute-forces the password hash offline, and recovers a privileged credential, faster still if the ticket is RC4-encrypted.

How Silverfort helps: Silverfort flags Kerberoastable accounts as an exposure and catches abnormal SPN activity in real time, so you can lock them down or migrate them to group Managed Service Accounts (gMSAs).

Customer example: In a large healthcare provider's environment, Silverfort surfaced eight admin accounts with SPNs the customer didn't know existed, cutting exposure to Kerberoasting.



5. Remove PrintNightmare

PrintNightmare is a critical vulnerability in the Windows Print Spooler service. Even after patching, affected systems can keep generating noisy, malformed authentications that are easy to miss.

How Silverfort helps: Silverfort surfaces these bad Print Spooler authentications automatically, so you can apply Microsoft's mitigation and clear the noise, without the manual packet capture the fix otherwise requires.

Customer example: A large US school district surfaced PrintNightmare-related authentication issues through Silverfort, cutting unnecessary authentications by about 70%.

Ready to see where your AD is exposed? [Schedule a call](#) with one of our experts.

About Silverfort

Silverfort secures every dimension of identity—human, machine, and AI—across on-prem, cloud, and hybrid environments. We are the first to deliver an end-to-end Identity Security platform that is easy to deploy and won't disrupt business operations, resulting in better security outcomes with less work. Discover every identity across every environment, analyze exposures to reduce your attack surface, and enforce security controls inline and at runtime to stop lateral movement, ransomware, and other identity threats.