SILVERFORT

5 Ways to Step Up Your AD Hygiene with Silverfort

Active Directory (AD) is the backbone of your organization's network, managing access and authentication for users, devices, and applications. Ensuring its cleanliness and security is vital because a compromised AD can serve as a gateway for attackers to gain unauthorized access to sensitive data.

Here are 5 ways Silverfort can help you strengthen your AD hygiene posture management.

1. Detect Shadow Admins

Shadow admins are users who have admin capabilities that you may not be aware of due to ACLs or nested groups.

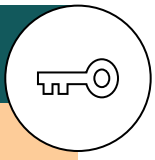
How does Silverfort detect shadow admins?

Silverfort identifies shadow admin accounts based on their privileges and the permissions they have been granted, in both on-prem and cloud environments.

Customer Example:

At a Fortune 500 financial company, Silverfort detected 109 new shadow admins created by a single AD misconfiguration. By detecting and removing the privileges of these admin accounts, the customer decreased their attack exposure.

2. Reducing NTLMv1 Usage



NTLMv1 is inherently insecure due to its use of weak encryption (DES) to encrypt the session key. This encryption type can be easily broken, and the user's password can be extracted.

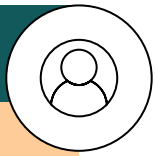
How does Silverfort detect NTLMv1?

Silverfort monitors all authentications processed by Active Directory without using event logs. It identifies which devices are sending NTLMv1 authentication requests and sends alerts to the logs screen inside the Silverfort platform.

Customer Example:

In a leading global manufacturer's environment, Silverfort discovered that around 5-8% of admin users still authenticate with NTLMv1 protocol, which was exposing their user passwords to compromise. Weekly reports are now sent to the team so they can reduce and ultimately eliminate the use of NTLMv1.

3. Discover Stale Users



Stale users are accounts that have not been used for a while; for example, former employees' accounts that have not been disabled. Certain types of stale accounts are difficult to identify unless you are able to monitor their authentication activity. As an example, identifying service accounts is difficult since their information is not available natively.

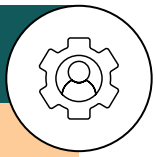
How does Silverfort detect stale users?

Silverfort automatically identifies and discovers stale users based on a lack of user activity data and information gathered from logs and other sources.

Customer Example:

At a leading US retail company, Silverfort detected that 13% of user accounts were stale users that had not performed any recent activity. This helped the company to clean up its Active Directory by disabling/removing the unused accounts, which ultimately helped decrease licensing and minimize costs.

4. Disable Admins with SPN



Having a **Service Principal Name (SPN)** associated with an admin account can expose it to a Kerberoasting attack, where an attacker requests the Kerberos ticket and obtains a payload encrypted by the user's password hash. Attackers can then brute force this payload to expose the credentials and compromise the account.

How does Silverfort detect Admins with SPN?

Silverfort detects these types of accounts by monitoring authentication events involving Service Principal Names (SPNs) within the network. It utilizes behavioral analytics and user behavior profiling to identify deviations from normal patterns, such as unusual access requests or privilege escalation attempts associated with admin privileges.

Customer Example:

In a large healthcare provider's AD environment, Silverfort discovered 8 admins with SPN that the customer was not aware of. This helped the customer to limit their exposure to potential Kerberoasting attacks and decrease their attack surface exposure.

5. Removing PrintNightmare

PrintNightmare is a critical security vulnerability affecting Windows' Print Spooler service that allows remote code execution and could lead to unauthorized access or system compromise.

How does Silverfort detect bad authentications from patched Print Spooler services?

Silverfort detects PrintNightmare by analyzing authentication events and abnormal service behavior and triggering alerts for further investigation and mitigation. Microsoft explains how to fully mitigate PrintNightmare but with Silverfort you can completely skip the problematic network packet capture as it will alert on all the bad Print Spooler authentications.

Customer Example:

A large US school district detected PrintNightmare in their environment thanks to Silverfort. With Silverfort they fixed this issue and reduced the number of unnecessary authentications in their environment by about 70%.