



Qualify for cyber insurance with fast and effective AD security

Accelerate your cyber insurance policy qualification by eliminating identity security blind spots and enforcing security controls across your environment.

Qualifying for cyber insurance is more difficult than ever, with rising ransomware attacks and costly claims forcing tighter cybersecurity requirements. Active Directory (AD) is at the center of these attacks, making it a key driver of cyber insurance claims.

With the lack of built-in MFA and the presence of unmanaged privileged accounts and non-human identities, securing AD environments remains a major challenge. Organizations are required to enforce MFA across all admin access and monitor privileged users, but without a way to properly secure AD, complying with those cyber insurance requirements—and preventing the spread of ransomware—can be a complex task.

With Silverfort, insurance applicants can overcome regulatory barriers by providing comprehensive visibility into all admin and privileged accounts that need MFA protection. It also provides complete visibility into all service accounts, including their privilege level and activities, to protect these accounts at scale with virtual fencing policies.

Here are four key reasons you should choose Silverfort:

1. Leading cyber insurance partners trust Silverfort

Silverfort is trusted by leading cyber insurers to meet strict compliance and insurance requirements. Our partnerships with top carriers, MGAs, and brokers help organizations qualify faster, reduce premiums, eliminate subjectivities, and strengthen their security posture:

- **Recognized by leading cyber insurers**

Many top global insurance providers, including **AIG, Arch, Axis, Beazley Security, Chubb, Sompo, and Travelers**, acknowledge Silverfort's capabilities in securing privileged accounts and enforcing MFA across all resources, simplifying the qualification process.

- **Comprehensive compliance readiness**

Silverfort's automated controls align with insurers' evolving security mandates, reducing the risk of coverage denial or higher premiums.

- **Real-time identity threat protection**

Continuous monitoring and adaptive policies ensure proactive defense against credential-based attacks, reducing claim risks.

2. Solving the most critical identity security problems

Silverfort helps you to address critical gaps in identity security and meet cyber insurance requirements with ease. By automatically discovering all privileged users, non-human identities, and service accounts, Silverfort helps you to continuously monitor all access requests and detect anomalies in your environment to prevent malicious access in real time:

- Discover all privileged users, NHIs, and service accounts to eliminate security blind spots.
 - Enforce specific, granular access policies based on real-time incident alerts.
 - Prevent credential-based attacks to reduce insurance claim risks and premium costs.
-

3. Lightweight architecture

Our unique architecture makes it possible for Silverfort's technology to be integrated with the existing organization's environment. It requires minimal resources and has no impact on critical business operations, so you can demonstrate a step change in security posture to the business within a month:

- Quick deployment that requires minimal resources, accelerating time to value.
 - No impact on Active Directory (AD) performance during the deployment process.
 - Due diligence is run on DC health and certified by Microsoft.
-

4. Quickly and effectively reducing cybersecurity risks

Silverfort can extend MFA protection to all resources and environments, including command-line access, legacy apps, IT infrastructure, and other critical resources that couldn't be protected before.

- MFA protection is extended to all sensitive resources within your organization, ensuring only authorized users can access critical systems and data.
- MFA or access block policies can be enforced on all privileged users, both human admins and non-human identities (NHIs).
- Real-time risk-analysis and adaptive security controls help prevent identity-related attacks such as privilege escalation and lateral movement.

About Silverfort

Silverfort secures every dimension of identity. 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.