SILVERFORT

White Paper

What is Silverfort's Cyber Insurance Assessment?

Silverfort's free cyber insurance assessment enables cyber insurance applicants to overcome compliance obstacles by providing comprehensive visibility into all admin accounts that need MFA protection as well as into all service accounts, including their privilege level and activities.

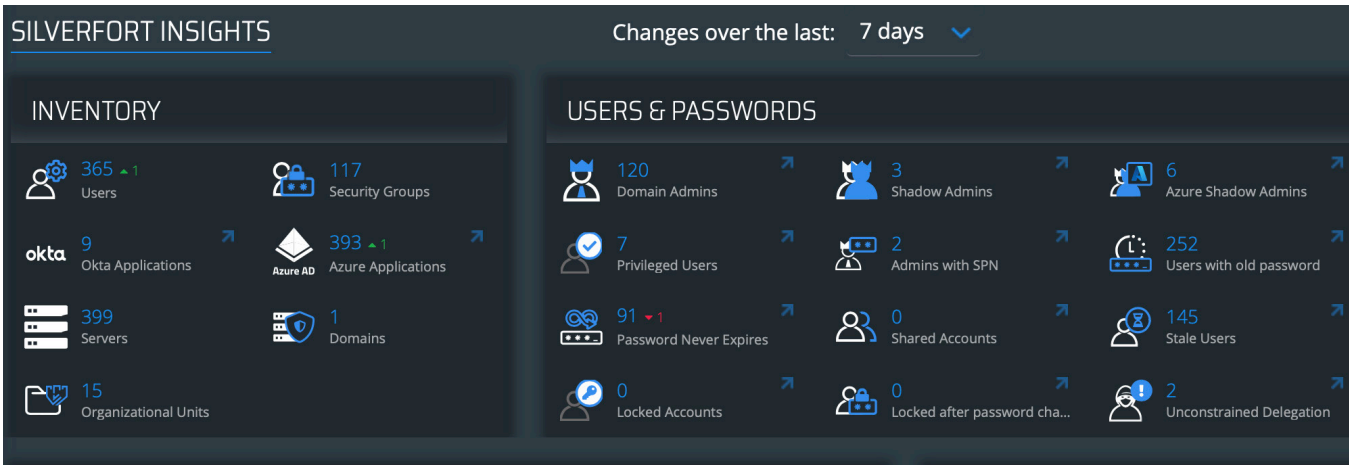
The assessment also uncovers any security hygiene issues that can expose the environment to identity threats while detecting any active ones already underway. With this information in hand, organizations can easily identify the identity security gaps preventing them from aligning with insurers' requirements, so they can resolve them and get the cyber insurance policy they need.

Silverfort's identity security assessment provides you with the following key insights:

Visibility of Admin Users

The most stringent requirement put in place by insurers is to apply MFA protection on all administrative access across various resources in the environment, including directory services, networking infrastructure, and command-line access.

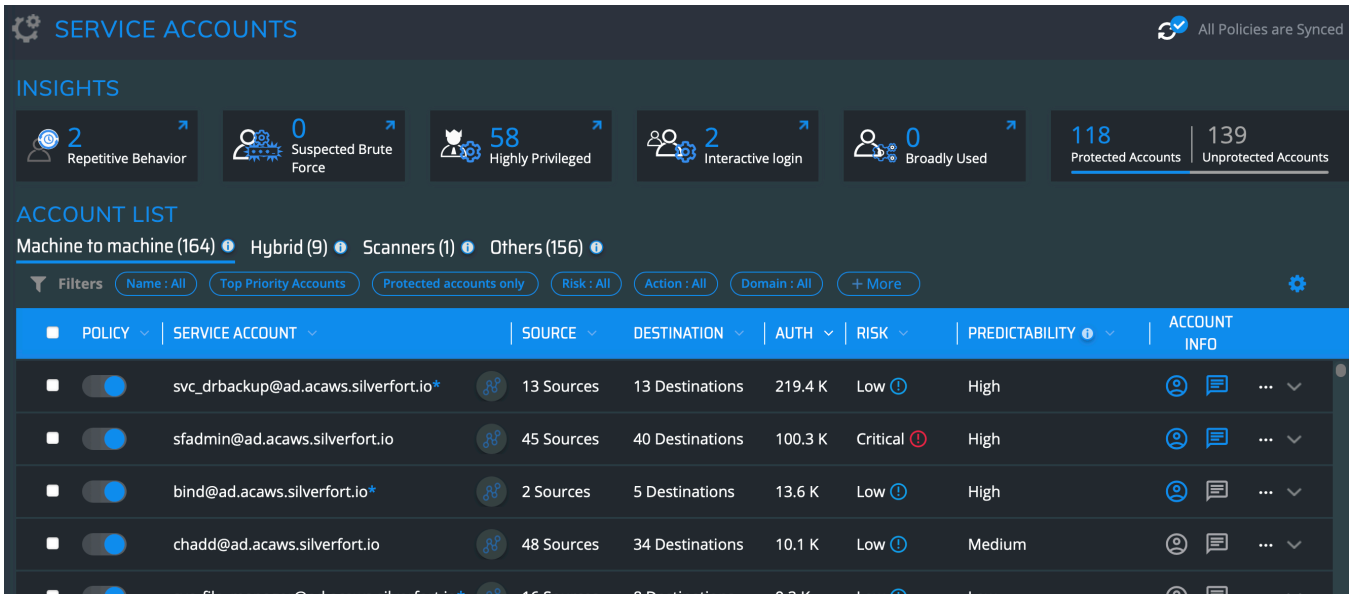
Silverfort's assessment provides complete visibility into all admin users (including shadow admins you might not be aware of) and the resources they access, enabling you to easily see their existing level of MFA cyber insurance coverage and – in the case of any gaps – extend this protection to all necessary users and resources.



Screenshot 1: Visibility of admin users

Service Account Discovery

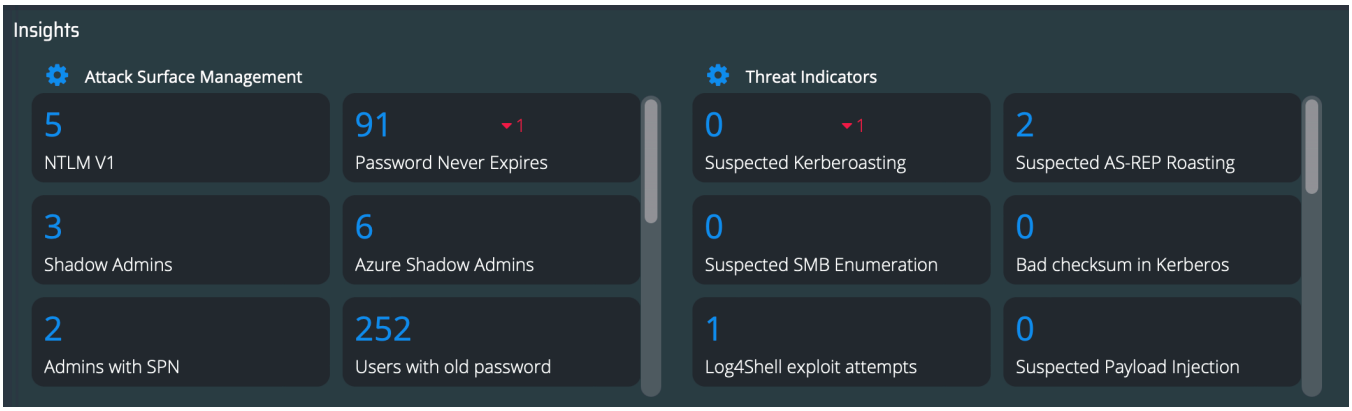
Another important aspect of cyber insurance eligibility is being able to demonstrate that you can monitor and protect your service accounts. Silverfort's assessment provides you with a complete service account inventory while showing you their privilege levels, source and destination, and the overall activity of each account. Most importantly, this assessment enables you to determine whether any of these accounts are at risk or behaving in an anomalous way that could indicate compromise.



Screenshot 2: Service account discovery

Identity Security Hygiene

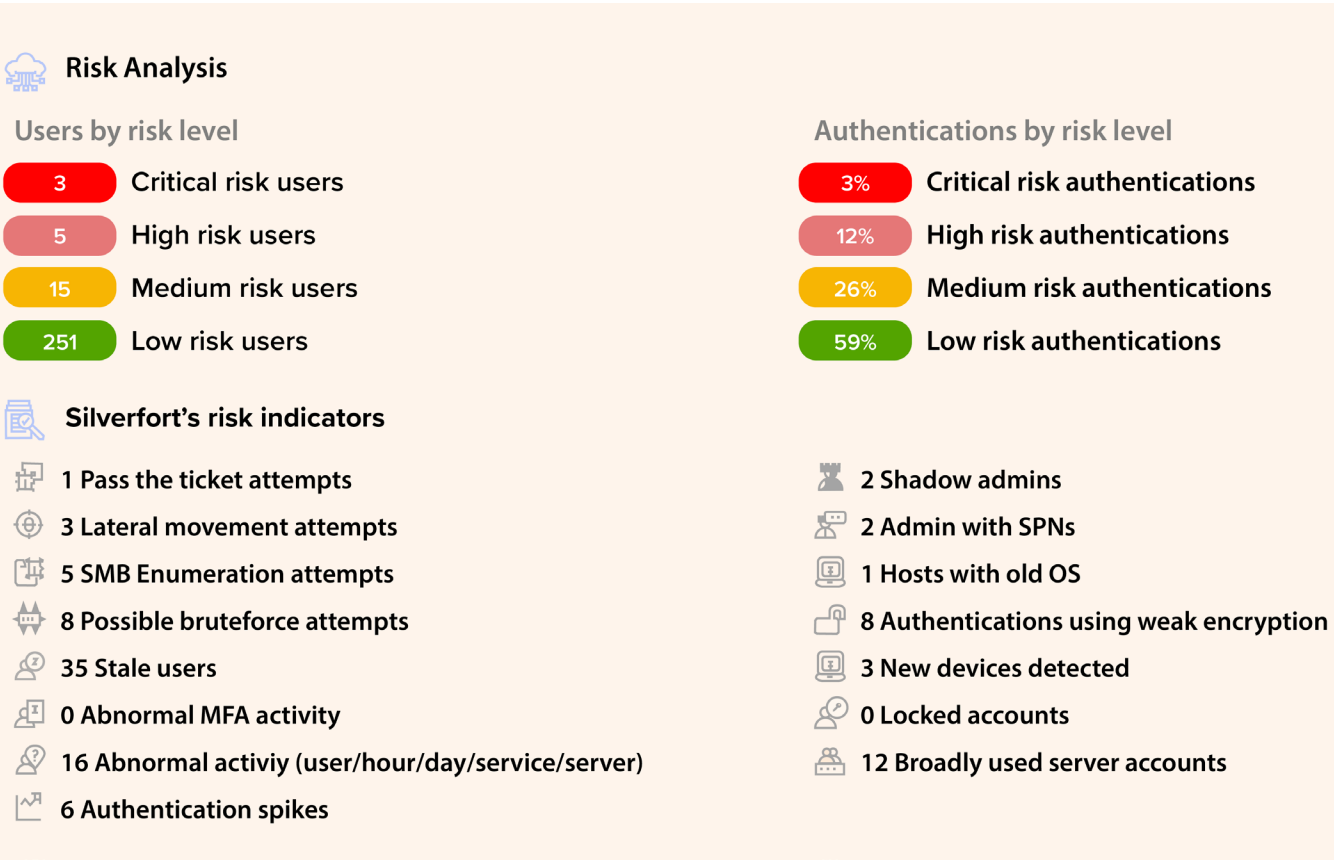
Silverfort's assessment tool can also identify security weaknesses in your environment that reduce its resilience to identity threats and expose it to various attack methods. Examples of these include stale passwords in use, accounts with passwords that never expire, admin users with SPN (making them vulnerable to Kerberoasting attacks), as well as the use of any weak protocols like NTLM and NTLMv1. Resolving these hygiene issues is a key step in reducing a threat actor's ability to attack your environment.



Screenshot 3: Identity security hygiene

Active Identity Threats

Silverfort's risk assessment can also spot any live identity threats active in the environment at the time of the assessment. These include common lateral movement techniques (Pass-the-Ticket, Pass-the-Hash, etc.), credential capture such as Kerberoasting, brute force attempts, and others that involve the compromise and use of credentials for malicious access. These techniques enable ransomware actors to spread within a targeted environment and escalate the impact of their attacks from a single machine to an entire network.



Screenshot 4: Active identity threats

Take the Next Step with Your Identity Security

Complying with all new requirements for a cyber insurance policy can be a challenge, especially if you don't have full visibility into your environment. Thanks to Silverfort's free identity risk assessment, organizations can meet this challenge head-on. Uncover your security gaps, qualify for cyber insurance, and eliminate the threat of ransomware.

About Silverfort

Silverfort has pioneered the first-ever Unified Identity Protection platform, which protects and secures enterprise service accounts against identity-based attacks that utilize compromised credentials to access enterprise resources. Using dedicated access policies for service accounts for lateral movement, Silverfort extends secure access controls such as Risk-Based Authentication and MFA across all on-prem and cloud resources. This includes assets that could never have been protected in this way before, such as homegrown/legacy applications, IT infrastructure, file systems, command-line tools, machine-to-machine access, and more. Silverfort continuously monitors all access attempts by users and service accounts, and analyzes risks in real-time using an AI-based engine to enforce adaptive access policies.

To learn more, visit www.silverfort.com