Silverfort

What is Silverfort's cyber insurance identity assessment?

Whitepaper

Executive summary

Silverfort's free cyber insurance assessment enables organizations to overcome compliance obstacles by providing comprehensive visibility into all admin and privileged 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 nefarious activity 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 and privileged 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 the activities, authentications, and privileges of all admin and privileged users – including shadow admins you might not be aware of – and the resources they access. It enables you to easily see their existing level of MFA cyber insurance coverage, determine if regular accounts are being used with privileged intent, and – in the case of any gaps – extend this protection to all necessary users and resources.

Image 1. Admin and privileged users visibility

Service account discovery

Another important aspect of cyber insurance eligibility is being able to demonstrate that you can monitor and protect your Active Directory 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.

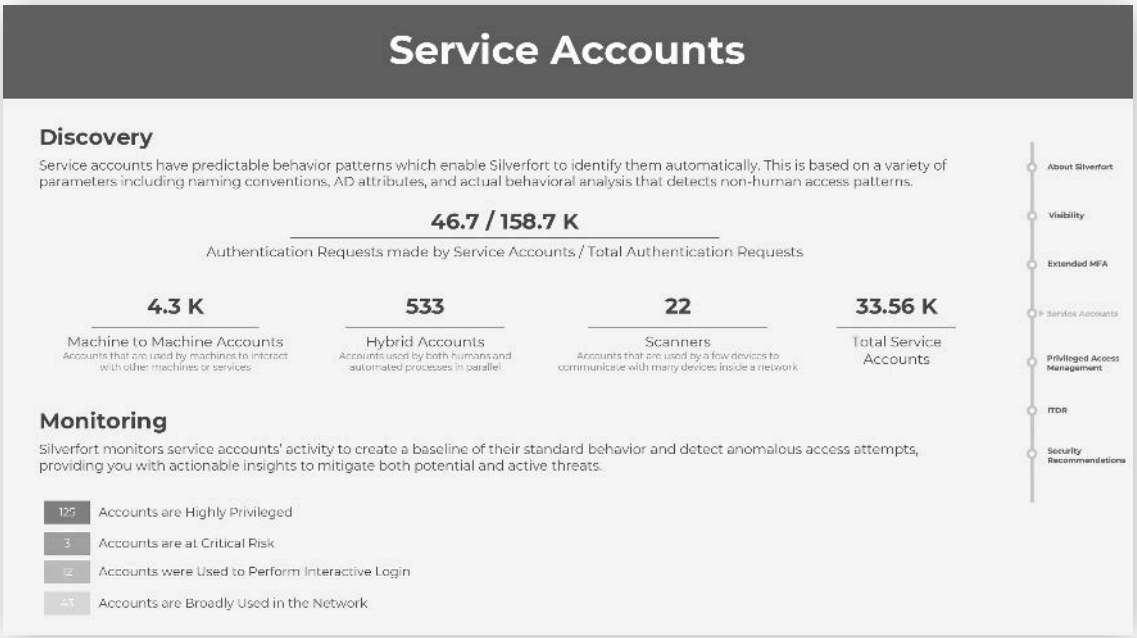

Image 2. Service accounts discovery

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 NTLMv1. Resolving these hygiene issues is a key step in reducing a threat actor's ability to attack your environment.

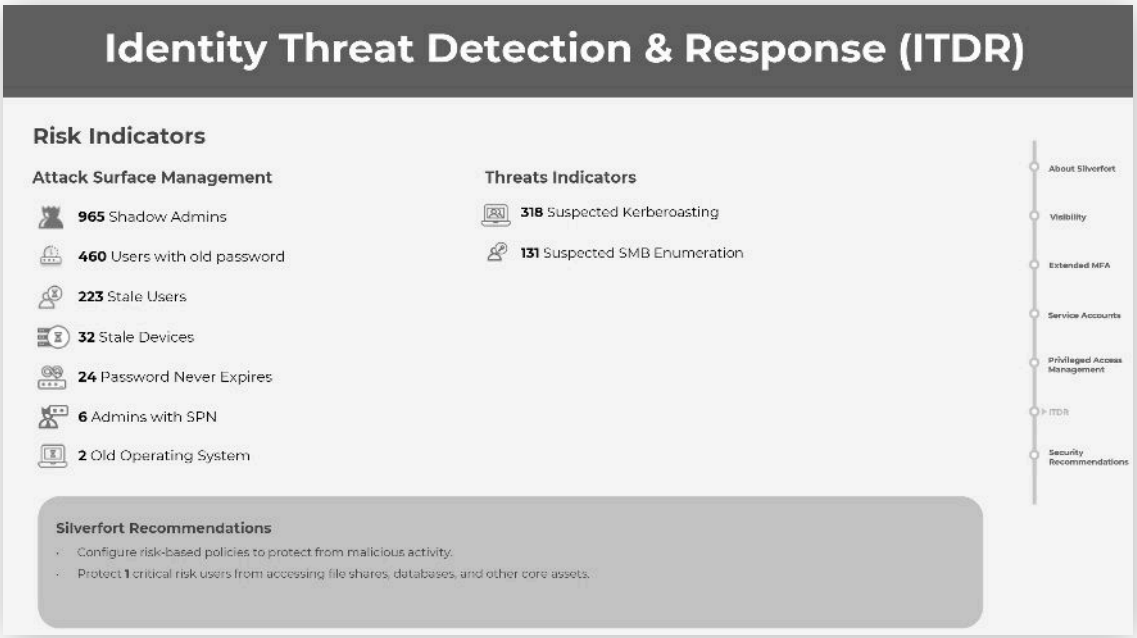

Image 3. Risk indicators (identity security hygiene)

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.

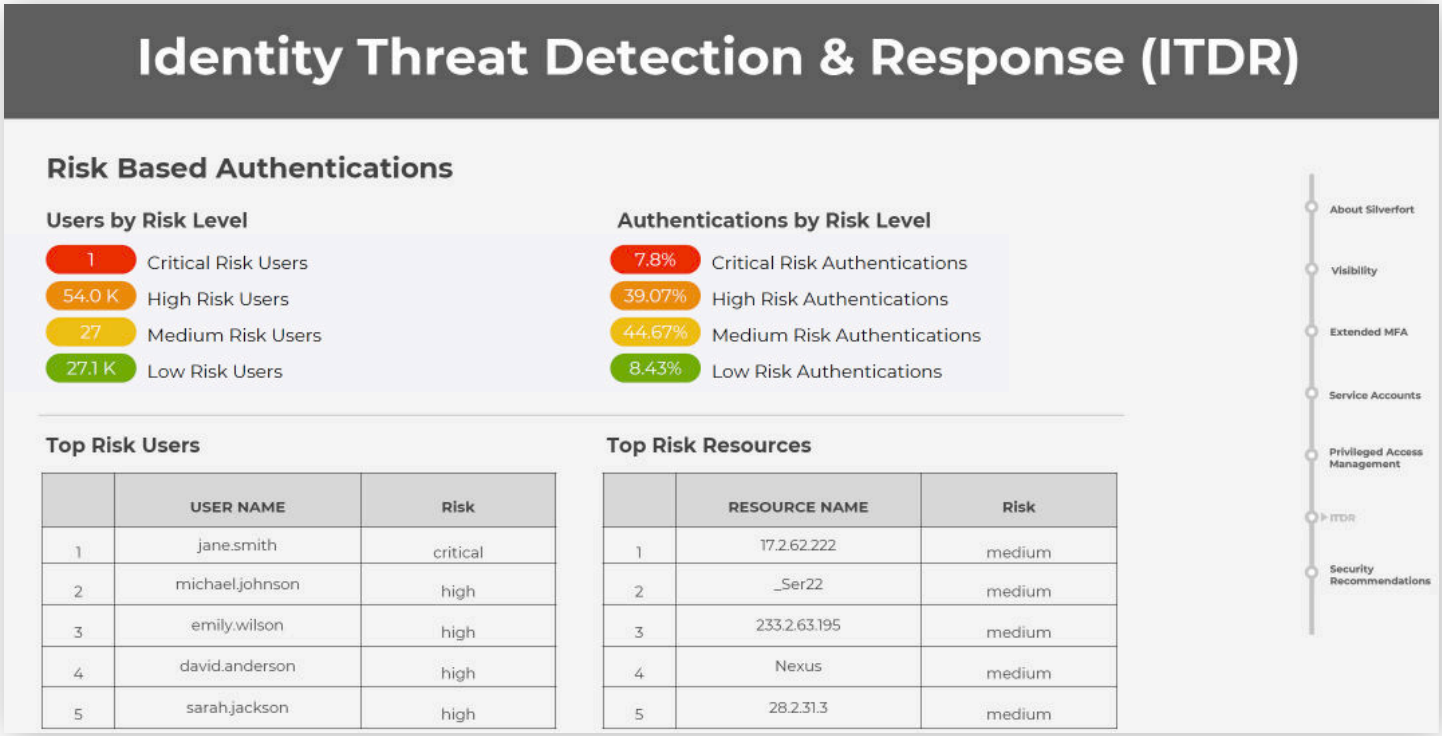

Image 4. Identity threat detection & response (ITDR)

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.

Learn more