Silverfort

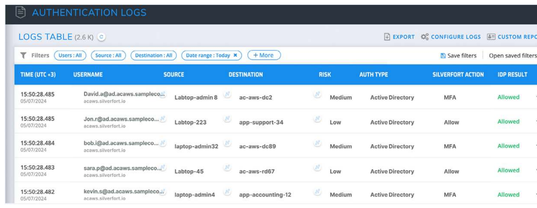
Gain End-to-End Visibility across Your Environment with Silverfort

Real-time visibility into all identity traffic and authentication activities in one place

Continue reading

Security starts with visibility. If you don't have full visibility across your environments, you are essentially operating in the dark. Without clear insight into user and authentication activity, access permissions, risky identities, authorized applications, and the potential identity security risks in your organization, you cannot make informed decisions. As a result, you could be leaving critical identity security gaps without even being aware of them.

The moment Silverfort is deployed into your environment, it will detect and monitor all user accounts and offer real-time insights into their activity and associated risks, providing instant benefit to your security operations. Silverfort's native integration with Active Directory enables it to log every authentication request. This allows you to gain a unified view of all activity across all users and resources within your organization. As each user is detected, their details are displayed in the Log screen by username, risk level assigned by Silverfort, authentication type, Silverfort's authentication action, and the identity provider result.

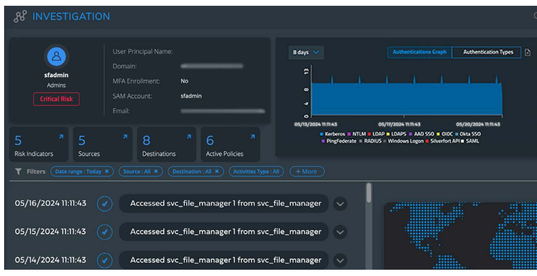


Silverfort's authentication logs screen provides full visibility into all user logs, authentication activity, and risk indicators.

Additionally, you can filter users' logs according to account type or risk indicator, as detected and assigned by Silverfort's risk engine. Silverfort supports a wide range of risk indicators, including NTLMv1, kerberoasting, brute force, MFA bombing, abnormal MFA activity, failed authentications, and many others. Filtering by risk enables you to gain complete visibility and insights into your risky users so you can begin the remediation process.

Investigate Quickly and Efficiently

You can gain more actionable insights by analyzing the details of a user's logs authentication activity, and risk indicators. These details provide a more granular understanding of each user and their authentication activity.



Silverfort's user investigation screen provides a detailed review of the authentication activities of a selected user to display their access requests in your environment.

Identity Security Posture Management

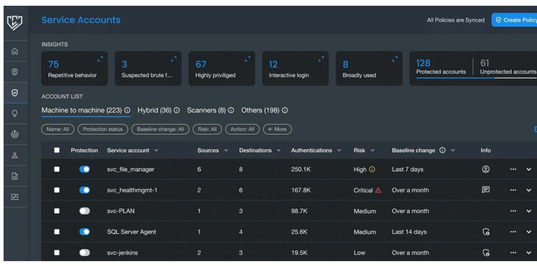
Silverfort provides an identity inventory of your environment in the Insights screen of the console, including users, resources, risky users, and more.

Silverfort's Insights screen offers insights into users, servers, applications, and devices protected by Silverfort.

Silverfort displays the types of users and resources in your environment as well as any weaknesses in your security that adversaries could abuse to launch identity threats. Among these are shadow admins, admin users with SPNs, accounts with passwords that do not expire, and many more. With actionable insights into the security posture of your environment, you will be able to resolve many security issues, making it significantly more difficult for threat actors to gain access to your network.

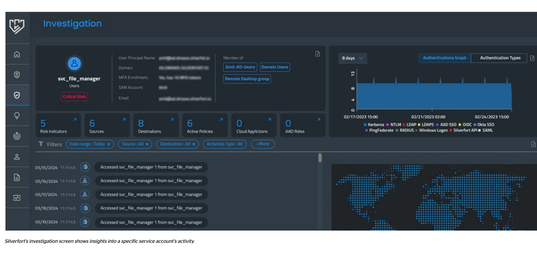
Visibility and Monitoring of Service Accounts

Silverfort identifies all service accounts based on the repetitive behavior that sets them apart from human users. Silverfort categorizes all detected service accounts into three main types: machine-to-machine (M2M) accounts, hybrid accounts, and scanners. Silverfort also supports Group Managed Service Accounts (gMSA) and offers a filter that allows you to see every gMSA in your system. Each gMSA will be detected and treated the same as any service account.



Silverfort's Service Accounts screen displays the service account name, source, destination, number of authentications, risk score, baseline change and account info.

Once all migrated service accounts have been detected, you can monitor service account activity and associated risks. Silverfort provides real-time insights and visibility into all service account details and behavior, and continually monitors and audits their use. This allows Silverfort to assess the risk of every authentication attempt and detect any suspicious behaviors or anomalies.



Silverfort's investigation screen shows insights into a specific service account's activity.