

# 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.

TIME (UTC +3)	USERNAME	SOURCE	DESTINATION	RISK	AUTH TYPE	SILVERFORT ACTION	IDP RESULT
15:50:28.485 05/07/2024	David.a@ad.acaws.sampleco... acaws.silverfort.io	Labtop-admin 8	ac-aws-dc2	Medium	Active Directory	MFA	Allowed
15:50:28.485 05/07/2024	Jon.r@ad.acaws.sampleco... acaws.silverfort.io	Labtop-223	app-support-34	Low	Active Directory	Allow	Allowed
15:50:28.484 05/07/2024	bob.i@ad.acaws.sampleco... acaws.silverfort.io	laptop-admin32	ac-aws-dc89	Medium	Active Directory	MFA	Allowed
15:50:28.483 05/07/2024	sara.p@ad.acaws.sampleco... acaws.silverfort.io	Labtop-45	ac-aws-rd67	Low	Active Directory	Allow	Allowed
15:50:28.482 05/07/2024	kevin.s@ad.acaws.sampleco... acaws.silverfort.io	laptop-admin4	app-accounting-12	Medium	Active Directory	MFA	Allowed

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.

**INVESTIGATION**

User Principal Name: sfadmin  
 Domain: Admins  
 MFA Enrollment: No  
 SAM Account: sfadmin  
 Email: [redacted]

5 Risk Indicators | 5 Sources | 8 Destinations | 6 Active Policies

05/16/2024 11:11:43 ✓ Accessed svc\_file\_manager 1 from svc\_file\_manager  
 05/15/2024 11:11:43 ✓ Accessed svc\_file\_manager 1 from svc\_file\_manager  
 05/14/2024 11:11:43 ✓ Accessed svc\_file\_manager 1 from svc\_file\_manager

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 INSIGHTS** Changes over the last: 7 days

INVENTORY: 363 Users, 117 Security Groups, 9 Okta Applications, 390 Azure Applications, 399 Servers, 1 Domains, 15 Organizational Units

USERS & PASSWORDS: 119 Domain Admins, 3 Shadow Admins, 6 Azure Shadow Admins, 7 Privileged Users, 2 Admins with SPN, 251 Users with old password, 90 Password Never Expires, 0 Shared Accounts, 145 State Users, 0 Locked Accounts, 0 Locked after password c..., 2 Unconstrained Delegation

SERVICES & DEVICES: 4 Shared Devices, 1 Old Operating System, 12 State Devices, 2 Log4Shell exploit attempts

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.

**Service Accounts** All Policies are Synced Create Policy

INSIGHTS: 75 Repetitive behavior, 3 Suspected brute f..., 67 Highly privileged, 12 Interactive login, 8 Broadly used, 128 Protected accounts, 61 Unprotected accounts

Protection	Service account	Sources	Destinations	Authentications	Risk	Baseline change	Info
On	svc_file_manager	6	8	250.1K	High	Last 7 days	...
On	svc_healthmgmt-1	2	6	167.8K	Critical	Over a month	...
Off	svc-PLAN	1	3	98.7K	Medium	Over a month	...
On	SQL Server Agent	1	4	25.6K	Medium	Last 14 days	...
Off	svc-jenkins	2	3	19.5K	Low	Over a month	...

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.

**INVESTIGATION**

User Principal Name: svc\_file\_manager  
 Domain: Users  
 MFA Enrollment: No  
 SAM Account: svc\_file\_manager  
 Email: [redacted]

5 Risk Indicators | 6 Sources | 8 Destinations | 6 Active Policies | 0 Cloud Applications | 0 AD Roles

05/16/2024 11:11:43 ✓ Accessed svc\_file\_manager 1 from svc\_file\_manager  
 05/16/2024 11:11:43 ✓ Accessed svc\_file\_manager 1 from svc\_file\_manager  
 05/17/2024 11:11:43 ✓ Accessed svc\_file\_manager 1 from svc\_file\_manager  
 05/18/2024 11:11:43 ✓ Accessed svc\_file\_manager 1 from svc\_file\_manager  
 05/19/2024 11:11:43 ✓ Accessed svc\_file\_manager 1 from svc\_file\_manager

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