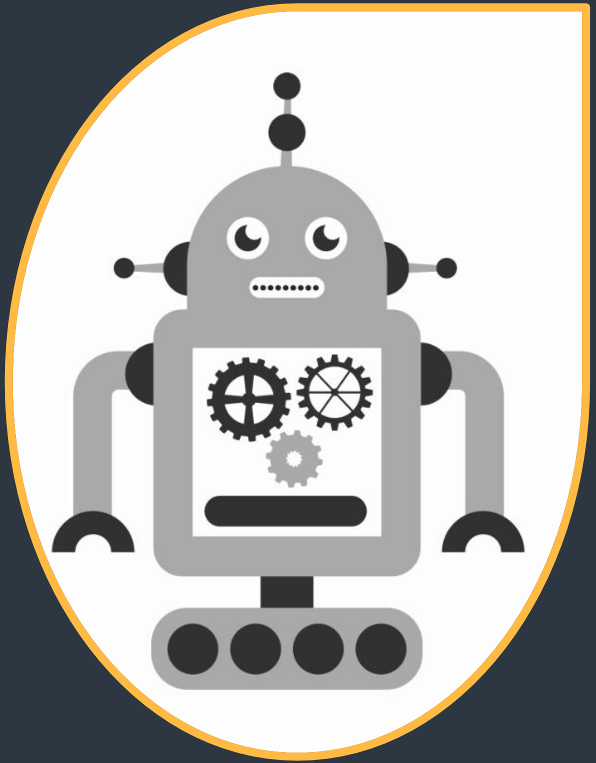
Protecting Service Accounts
Luxury or Critical Necessity?

SILVERFORT

Dr. Shahriar Daneshjoo, VP Central EMEA
Vienna, 09. October 2024

What are Service Accounts?



- Non-human account,
- Communication and interaction between systems, or services,
- Representing the identity and authorization of an application or service.

The Service Account Blind Spot

- Non-human identities are especially difficult to protect
- Password rotation (PAM) at scale takes years & causes operational disruptions

Highly privileged

Can cause large damage when compromised

Unknown Dependencies

Companies don’t know all service accounts

Difficult to Protect

Rotating their passwords often breaks applications

Regularly Abused

Often used outside of their intended purpose

Service Accounts are highly vulnerable and targeted by attackers

> **“We are 2 years into our PAM and password rotation journey, and only 10% deployed”**
> – CISO, large US-based insurance company

The Necessity of Service Account Protection

78% of organizations are not confident in their ability to block malicious access carried out with a compromised service account

Only 5.7% of organizations believe that they have full visibility into service accounts in their environment

"*Osterman Research**, The State of the Identity Attack Surface 2023*"

„Machine accounts are a significant source of **risk** (well, many of us knew that...), AND: machine accounts are a significant vector for breaches, TODAY."

„……..I hope this will open more eyes to the importance of machine IAM and increase the priority and urgency of it".

"***Gartner**, Felix Gaehtgens, Vice President, Analyst, IAM, August 2024* "

According to Silverfort's research data, compromised service accounts were involved in over 70% of the attack attempts that we have prevented or investigated in our customers' environments

Examples of Data Breaches

solarwinds

(2020)
In the SunBurst attack, the Solarwinds service accounts was used for moving laterally and compromising additional systems on-prem and in the cloud

Uber

(2022)
Attackers found a script that contained the credentials of a privileged service account, which allowed them to breach the PAM vault

okta

(2023)
Breaching the customer support system was done with a service account, that was mistakenly saved to an employee's personal Google account

What Next?

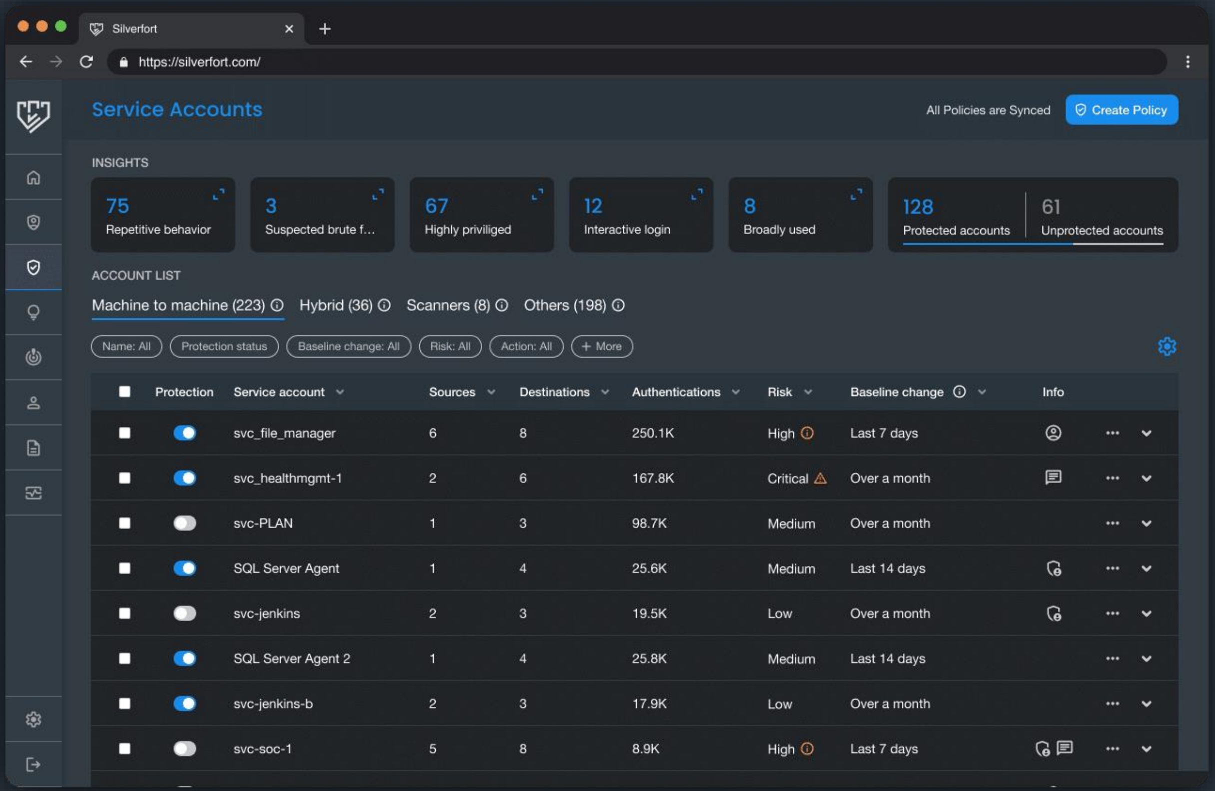
1. Discover

2. Protect

3. Automate

Discover

- Group memberships
- Naming conventions
- Behavior-based discovery (ML)



Service Accounts

All Policies are Synced

Create Policy

INSIGHTS

75 Repetitive behavior

3 Suspected brute f...

67 Highly priviliged

12 Interactive login

8 Broadly used

128 Protected accounts

61 Unprotected accounts

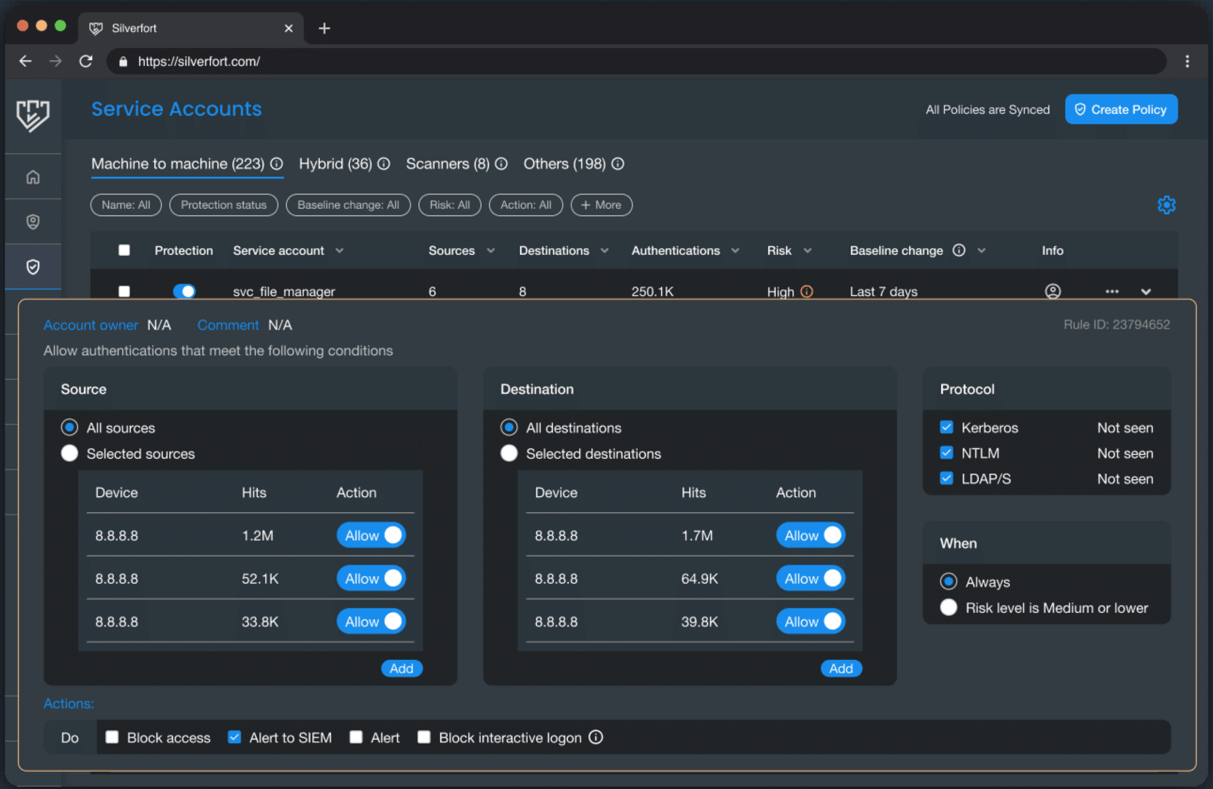
ACCOUNT LIST

Machine to machine (223) | Hybrid (36) | Scanners (8) | Others (198)

Name: All | Protection status | Baseline change: All | Risk: All | Action: All | + More

□	Protection	Service account	Sources	Destinations	Authentications	Risk	Baseline change	Info
□	●	svc_file_manager	6	8	250.1K	High ⓘ	Last 7 days	
□	●	svc_healthmgmt-1	2	6	167.8K	Critical ⚠	Over a month	
□	○	svc-PLAN	1	3	98.7K	Medium	Over a month	
□	●	SQL Server Agent	1	4	25.6K	Medium	Last 14 days	
□	○	svc-jenkins	2	3	19.5K	Low	Over a month	
□	●	SQL Server Agent 2	1	4	25.8K	Medium	Last 14 days	
□	●	svc-jenkins-b	2	3	17.9K	Low	Over a month	
□	○	svc-soc-1	5	8	8.9K	High ⓘ	Last 7 days	

Protect



Service Accounts

All Policies are Synced

Machine to machine (223) | Hybrid (36) | Scanners (8) | Others (198)

Name: All | Protection status | Baseline change: All | Risk: All | Action: All | + More

□	Protection	Service account	Sources	Destinations	Authentications	Risk	Baseline change	Info
□	●	svc_file_manager	6	8	250.1K	High	Last 7 days	

Account owner N/A Comment N/A Rule ID: 23794652

Allow authentications that meet the following conditions

Source

● All sources
○ Selected sources

Device	Hits	Action
8.8.8.8	1.2M	Allow
8.8.8.8	52.1K	Allow
8.8.8.8	33.8K	Allow

Add

Destination

● All destinations
○ Selected destinations

Device	Hits	Action
8.8.8.8	1.7M	Allow
8.8.8.8	64.9K	Allow
8.8.8.8	39.8K	Allow

Add

Protocol

☑ Kerberos	Not seen
☑ NTLM	Not seen
☑ LDAP/S	Not seen

When

● Always
○ Risk level is Medium or lower

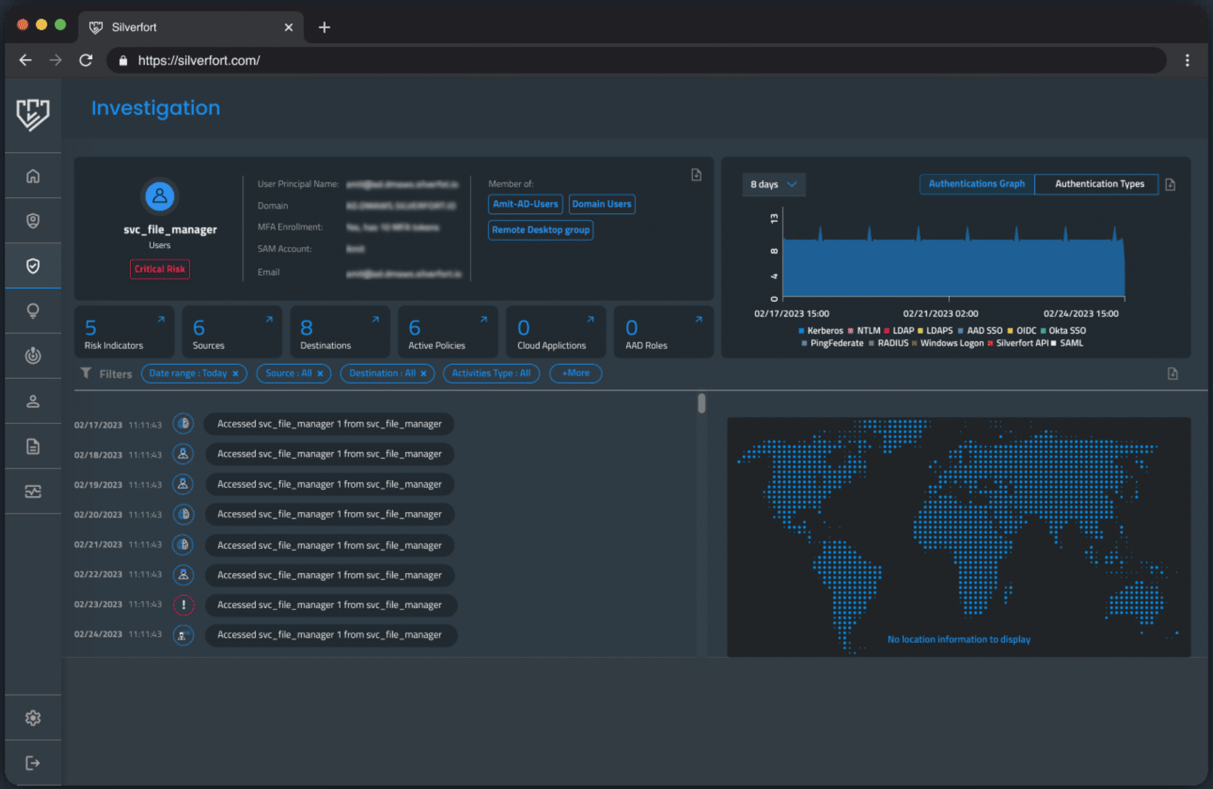
Actions:

Do □ Block access ☑ Alert to SIEM □ Alert □ Block interactive logon

- learn the access pattern
- Enforce ‘virtual fencing’
- Use real-time enforcement
- Block and/or alert on unauthorized access
- Notify application owners

Automate

- Option 1: Smart policies that move each account automatically
- Option 2: Integration with the CMDB and other IT tools New service accounts should be
- Protected from day 1, as part of their creation process



svc_file_manager
Users
Critical Risk

User Principal Name: [redacted]
Domain [redacted]
MFA Enrollment: [redacted]
SAM Account: [redacted]
Email [redacted]

Member of: Amit-AD-Users Domain Users Remote Desktop group

5 Risk Indicators
6 Sources
8 Destinations
6 Active Policies
0 Cloud Applictions
0 AAD Roles

Filters: Date range : Today, Source : All, Destination : All, Activities Type : All, +More

```
02/17/2023 11:11:43  Accessed svc_file_manager 1 from svc_file_manager
02/18/2023 11:11:43  Accessed svc_file_manager 1 from svc_file_manager
02/19/2023 11:11:43  Accessed svc_file_manager 1 from svc_file_manager
02/20/2023 11:11:43  Accessed svc_file_manager 1 from svc_file_manager
02/21/2023 11:11:43  Accessed svc_file_manager 1 from svc_file_manager
02/22/2023 11:11:43  Accessed svc_file_manager 1 from svc_file_manager
02/23/2023 11:11:43  Accessed svc_file_manager 1 from svc_file_manager
02/24/2023 11:11:43  Accessed svc_file_manager 1 from svc_file_manager
```

8 days
Authentications Graph
Authentication Types
13
8
4
0
02/17/2023 15:00
02/21/2023 02:00
02/24/2023 15:00
Kerberos NTLM LDAP LDAPS AAD SSO OIDC Okta SSO
PingFederate RADIUS Windows Logon Silverfort API SAML
No location information to display

SILVERFORT

Thank You

www.silverfort.com

shari.daneshjoo@silverfort.com