Silverfort

Best Practices for Service Accounts

Whitepaper

Introduction

Service accounts are dedicated accounts created by administrators, usually in a network directory, to allow systems and applications to interact with each other. These service accounts allow applications and systems to perform automatic, repetitive, and scheduled actions in the background, without human intervention. They help organizations automate important processes such as passing information between systems, backup data, perform security scans and so on.

Although service accounts enable organizations to automate processes and work more efficiently, they lack some basic security best practices making them highly vulnerable to compromise.

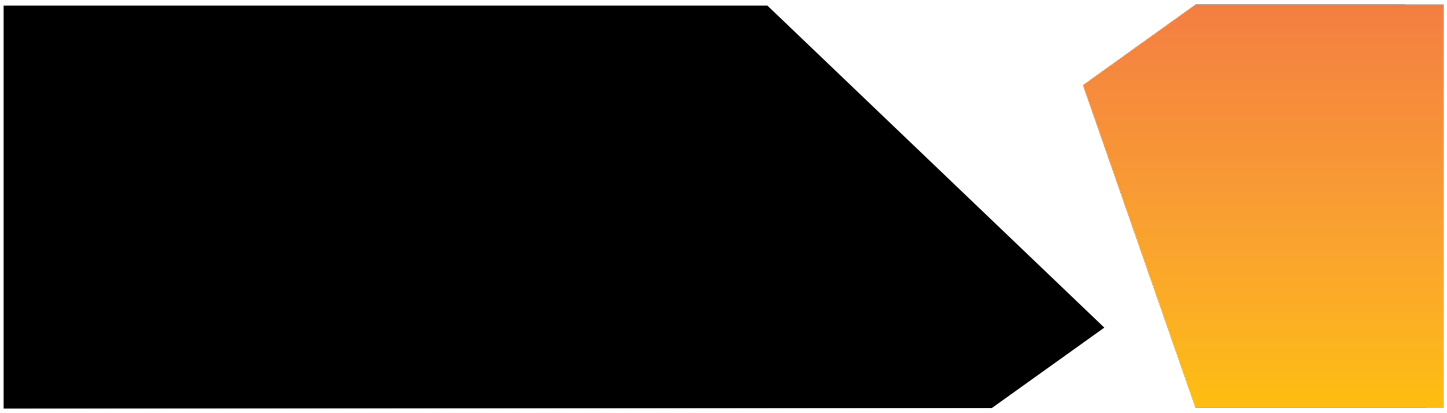
- Poor lifecycle management
- Lack of strong security controls such as strong password policies and MFA
- Lack of documentation and clear ownership

Many administrators are unaware of all the service accounts operating in their network and their activities. This together with the fact that they are usually highly privileged and have access to various often critical systems and data, has made them a prime target for attackers in the last decade.

Silverfort service account protection involves the following steps:

1. Discover all service accounts and their activities
2. Prioritize service account protection
3. Add proactive protection

This document shows how Silverfort can identify all types of service accounts in your network and outlines best practices for securing them.



Protecting Service Accounts

Discover

The first step in protecting your environment is knowing where your data resides.
When it comes to service accounts:

1. What service accounts do you have
2. The total number of service accounts
3. Which assets use those service accounts

When your DCs connect to Silverfort, Silverfort automatically identifies the service accounts, monitors their authentication and behavior, and displays them in the Silverfort user interface. Silverfort identifies service accounts through several different methods:

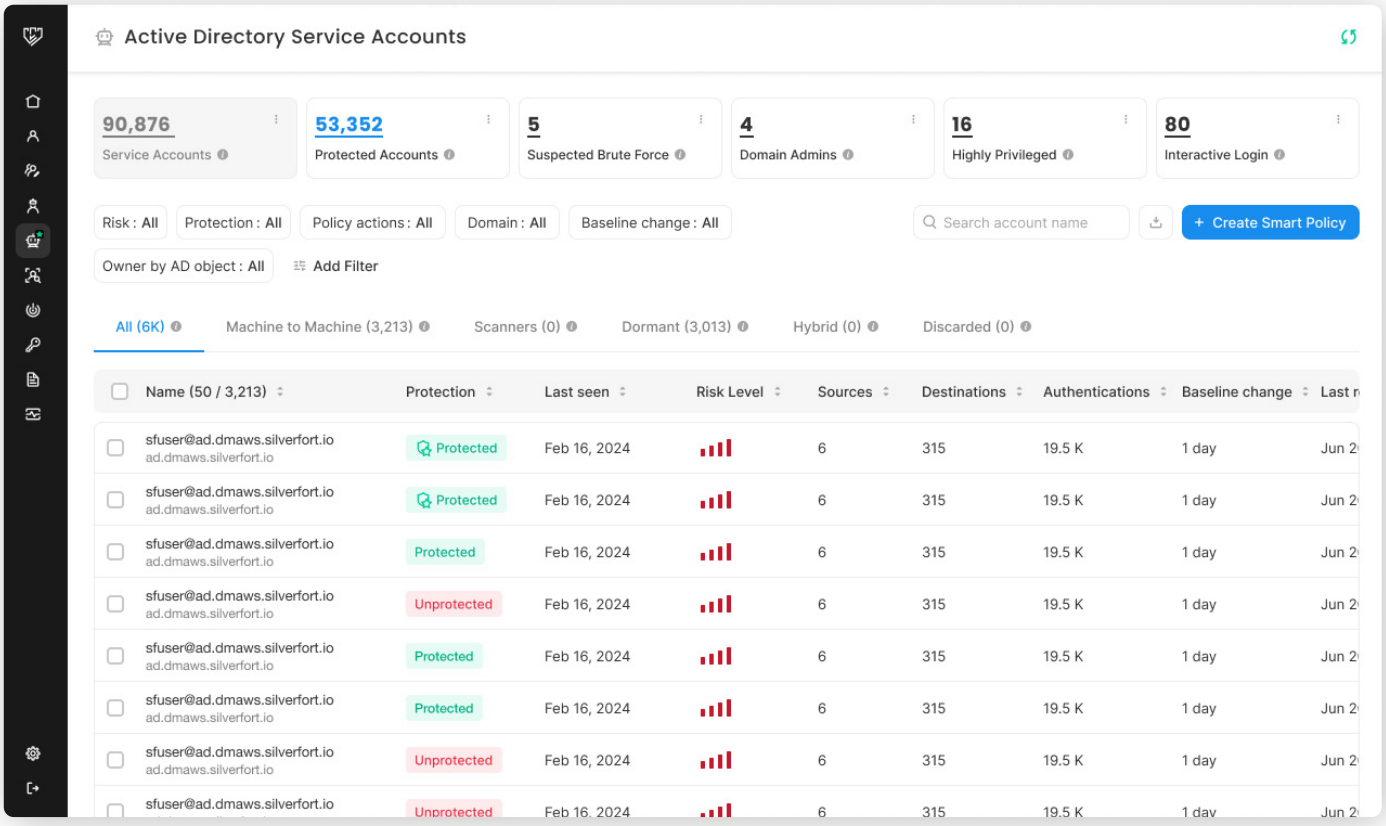
AD configuration — Silverfort checks different attributes of user accounts in AD to find characteristics common to service accounts, such as a password that never expires, or a naming convention typical of service accounts.

Behavioral analysis — Silverfort analyzes each account's behavior to identify repetitive traffic patterns and discover even the most unknown accounts.

Custom insights — Silverfort receives feedback from the admin regarding the management structure of service accounts in the customer environments (like OU, SG, and other naming conventions).

gMSA — The specialized account type in AD used as a managed service account.

Silverfort identifies and categories four types of service accounts:



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

Machine-to-machine — Used by machines and applications to interact with other machines or services (for example, a Web container that communicates with a database container).

Hybrid accounts — Used by users to access machines automatically or according to a schedule (for example, database administrators who run scripts from their user accounts to connect to servers).

Scanners — Used by a few devices to communicate large numbers of devices in a relatively small period inside a network (for example, NAC or inventory platforms)

Dormant service accounts — Service Accounts with zero authentications.

Silverfort automatically monitors and gathers data on every service account's authentication activity. The system identifies and presents all sources, destinations and protocols the service account operates with. It also presents the number of authentications and the latest activity of each.

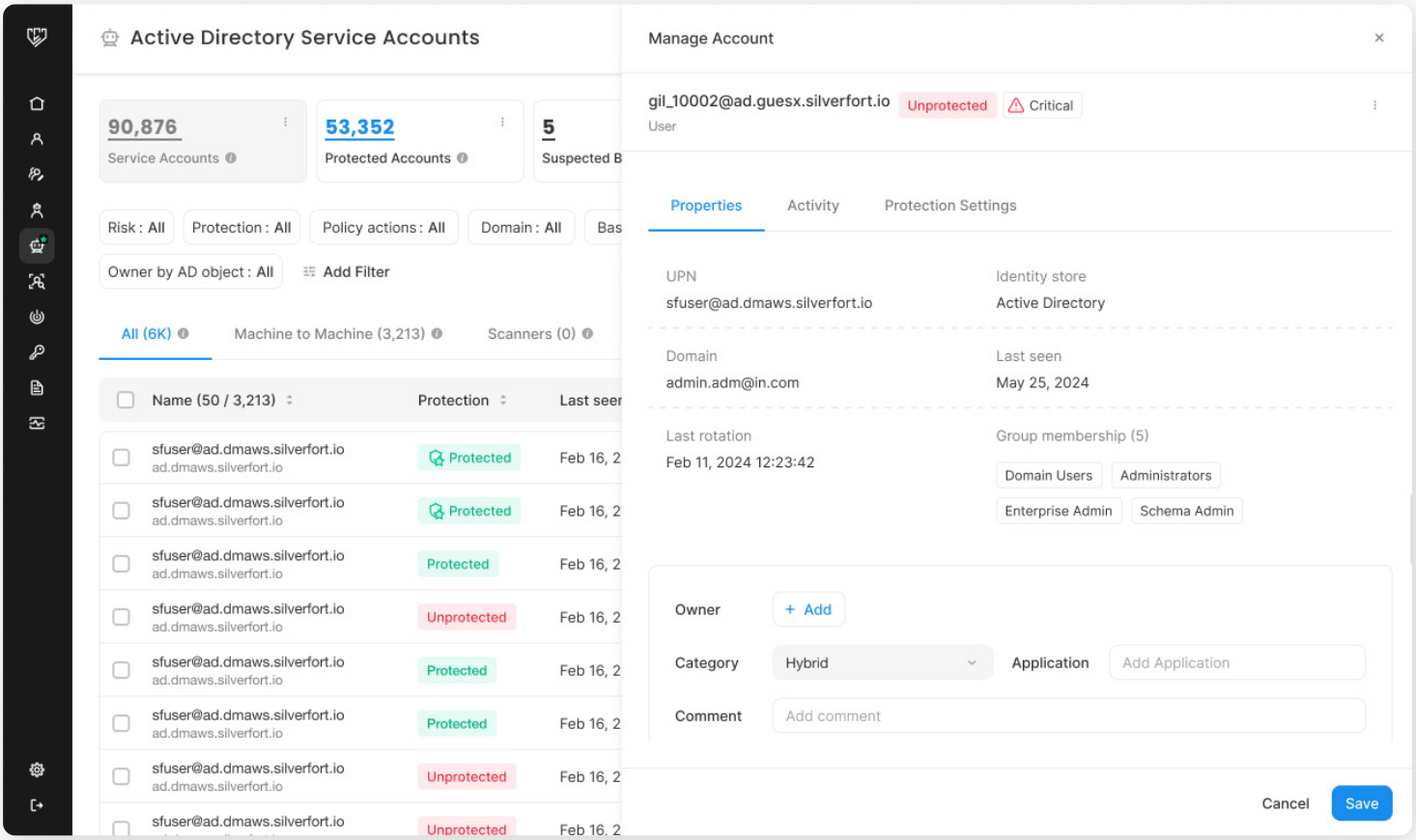
This enables security teams to gain a deeper understanding of the service account's activity. Important points toward improving the security of the service account is as follows:

- Identifying the application owner to validate the proper usage of this service account and applying better controls such as lifecycle management and access reviews
- Identifying the service account dependencies (sources and destinations) to allow password rotations either manually or by ingesting this information into your PAM solution
- Applying a security policy that acts as a "virtual fence" around the actual usage of the service account, detected by Silverfort

Additionally, Silverfort allows administrators to build an inventory of service accounts. Use the comments field per service account to document the service account's purpose, as well as any notes related to its management. Use the owner field to document the service account's owner. In cases where service accounts are managed in a different tool, use Silverfort's REST APIs and ServiceNow integration to automatically build and update the service accounts inventory in Silverfort.

Prioritize

In the Silverfort service account screen, admins are provided with actionable insights and the total risk level for each service account. This enables security teams to understand better the different risks associated with their service accounts in this manner.



Continuously monitor service accounts in real-time, tracking usage patterns and behaviors with precise anomaly detection to alert on deviations.

Use Silverfort's insights to prioritize service accounts which are:

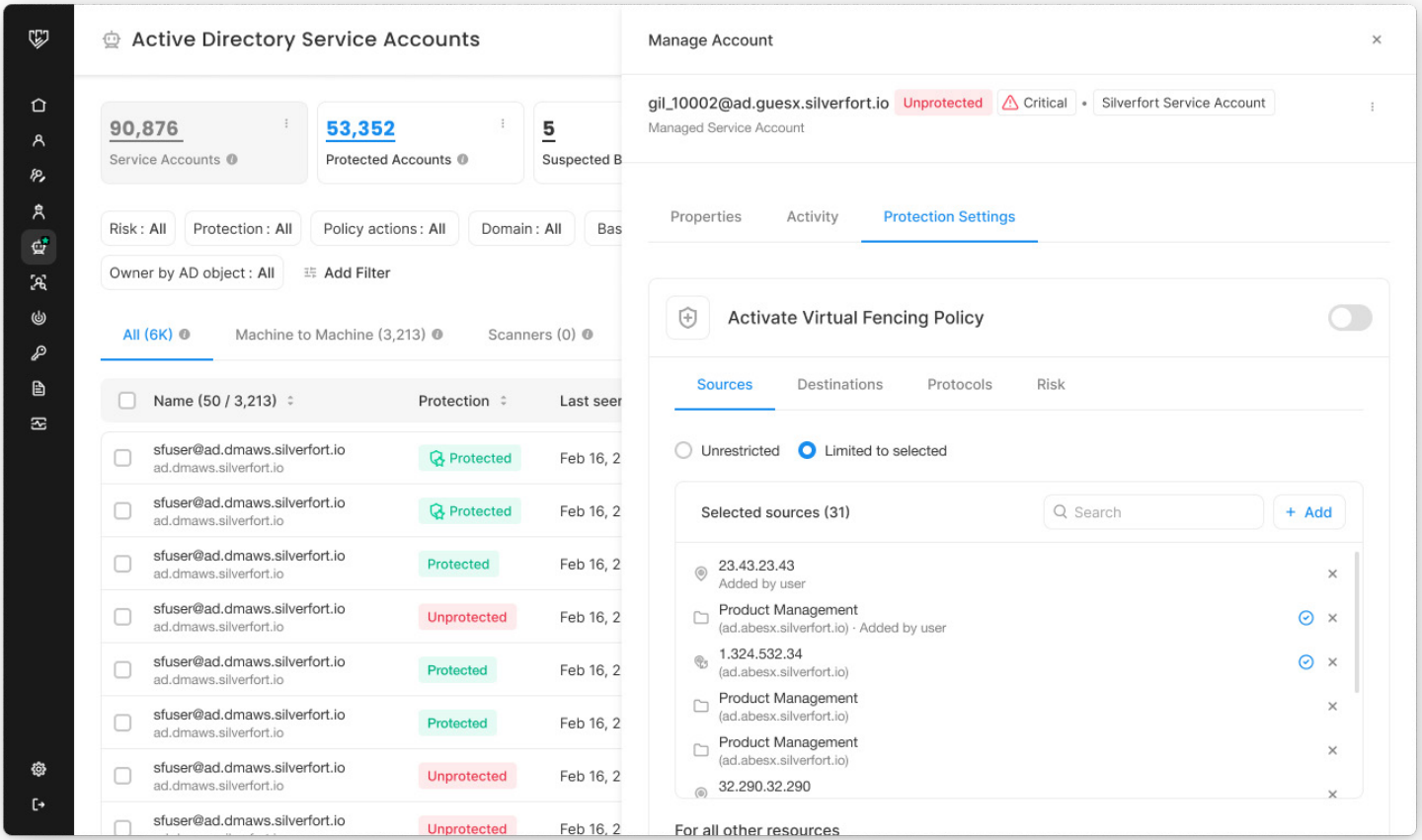
1. Used by or connected to your crown jewels applications
2. With very high permissions
3. With critical or high-risk levels (from the risk levels provided by Silverfort).
4. Suspected to be brute forced
5. Used interactively

On the Investigate page, you will be able to view more information about the service account and its authentications and risk indicators that have an impact on the reported risk level.

Protect

With the authentication data, Silverfort automatically gathers all the details for each service account in order to enforce a security policy that only permits the sources, destinations, and protocols that the service account is actually using. It is possible to activate such policies for multiple service accounts at the same time in Silverfort.

In essence, the security policy acts as a "virtual fence" around the service account, permitting only access necessary for the service to be operated, even if the account is entitled to more access. Any access that deviates from that is blocked and logged, to prevent malicious actors from fully exploiting this service account and moving freely in the network, and quickly investigate the reason for that deviation.



Silverfort's service accounts policy creation screen displaying how to enable the policy and which action the admin should assign to this policy.

These are the best practices of protecting service accounts per category:

Machine-to-machine — Configure and apply a notify policy that monitors and adjusts as needed until moving forward to deny. This is where Smart Policy kicks in since it performs this automatically

Hybrid — Trace the service-like repetitive behavior being performed by a human user and remove this bad practice by contacting the user and potentially suggesting the creation of a dedicated service account

Scanners — If the scanner is running from a few sources to scan a large volume of destinations such as workstations or servers, create a policy that restricts the sources, or vice versa

Dormant — Enable a security policy that allows no authentications to be performed by these accounts (can be performed in bulk) and monitor them for a certain period to eventually disable them or remove them entirely from AD

Silverfort also displays the last time a change in the detected sources, destinations, or protocols was detected for each service account in the Baseline Change column. Utilize this data to identify service accounts with consistent activity over time. It will be considered safe to activate a security policy on service accounts with long periods of consistent activity. This will significantly reduce the chances of disrupting service operation.

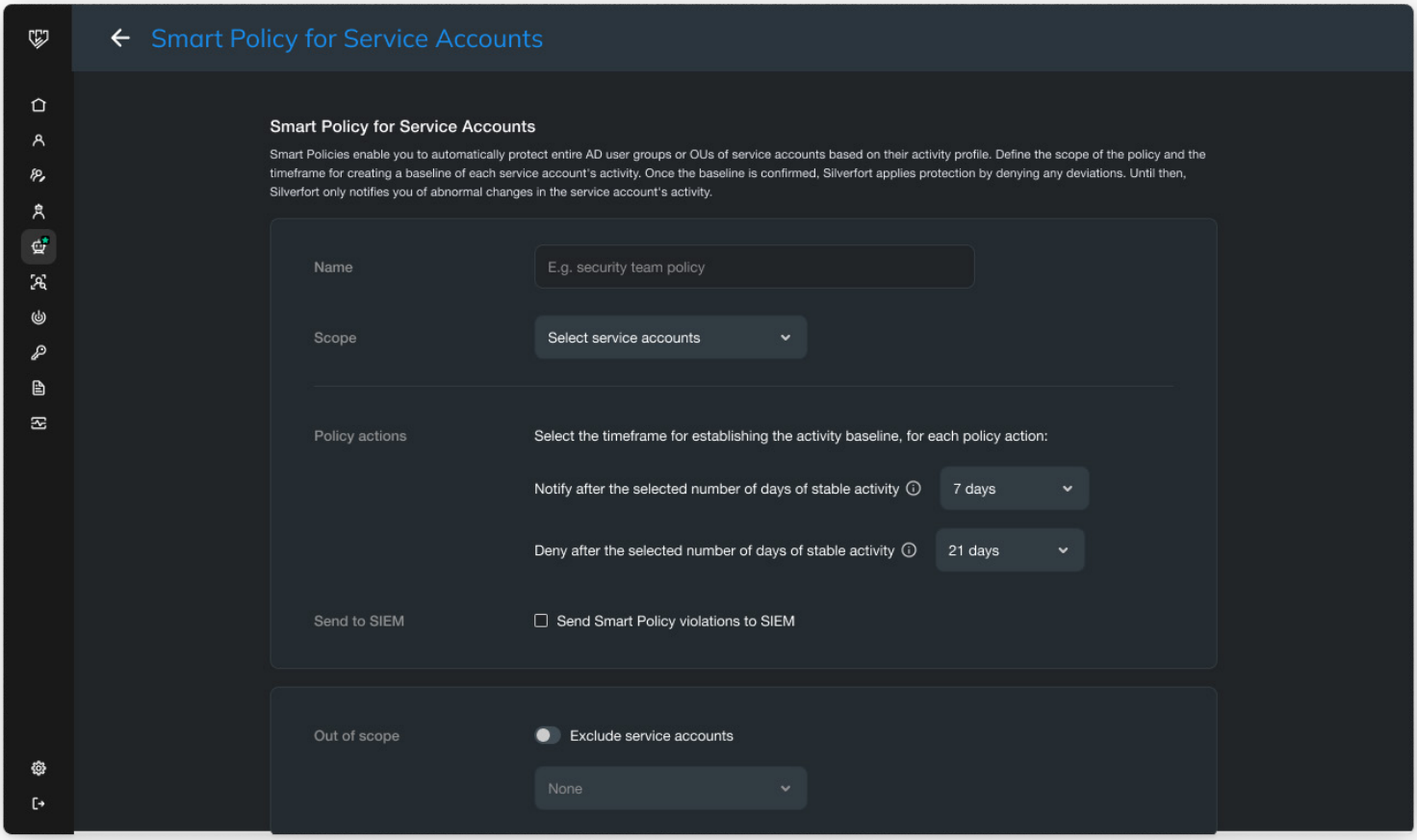
As an extra safety measure, you may want to consider a Notify policy to track policy violations without blocking traffic to allow an additional monitoring period for policy adjustments to take place.

Automate

The Silverfort team understands the importance of securing service accounts in an automated and scalable manner. Therefore, we recommend the implementation of our Smart Policy for Service Accounts, Service Accounts APIs, and the ServiceNow integration.

Smart Policy

Use the Smart Policy to completely automate the process of monitoring, adjusting and eventually enforcing a deny policy for service accounts. The Smart Policy is configured with a scope of accounts, security groups and organizational units containing service accounts, and the desired periods of consistent activity for enabling a Notify or Deny policies. Including groups and OUs will allow the automatic protection of newly created service accounts.



Smart Policy enables organizations with many service accounts to apply security policies in bulk.

Integration with Service Account APIs

A different approach to more automated and consistent service account policy management is building an automated correlation between Silverfort's Service Account Policy and a third-party service.

Service Account Protection Policy integrations make use of our Service Account API which allows full visibility and control over the service accounts and their security policies. From an automation perspective, this can all be read and controlled via the API.

ServiceNow Integration

Silverfort understands the need for automated and scalable service account protection capabilities, and therefore developed a ServiceNow application that specifically focuses on leveraging the ServiceNow CMDB data with the Silverfort Service Account Policy.

The integration delivers automated enforcement of our Service Account Policy capabilities without any interaction of security admins. This happens in real-time based on CMDB application and services data. By using the Silverfort service account protection application on your ServiceNow CMDB instance, you enable:

Scalability — Scale service account protection by leveraging the CMDB as a single source of truth and enforce service account protection policies in real-time.

Team collaboration — Leverage the integration for easy cross team collaboration on security enforcement. Application teams updating CMDB application information directly adjust the security policies for these applications without any manual intervention of security teams.

Minimizing human errors — Mistakes are easily made by humans, but not by automation. Source data reflects immediately in corresponding policies with the right data in the right spot.

The integration can be installed through the ServiceNow Store and can be found here.

Conclusion

In most cases, service accounts are privileged, passwords are rarely changed, and MFA is not applicable. This makes them a prime target for attackers, allowing them to move laterally and elevate their privileges. Many organizations do not know who their service accounts are, and those who do have no visibility into their activity and resources face the challenge of protecting them.

When companies gain comprehensive knowledge of service account behavior and activities, they can apply security policies that:

1. Allow only the required authentication flows
2. Reduce risk levels
3. Block network lateral movement
4. Protect previously undetected IT assets

By gaining complete visibility into service accounts and proactively protecting them with the proper security controls, organizations are equipped to reduce the attack surfaces of service accounts.

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