eBOOK

SILVERFORT

4 Steps to Comprehensive Service Account Security

What are Service Accounts

Service accounts, dedicated non-human accounts used by systems, applications, and services to interact with other systems, are an IT infrastructure basic. They perform scheduled actions automatically and repeatedly in the background, typically going totally unnoticed, and sometimes, forgotten about, by security administrators. There are countless service accounts in any given organization and today, there are more than ever. The rise in Robotic Process Automation (RPA), or the use of AI to configure software "robots" to perform business tasks, that used to require the guidance of humans is increasing their popularity. Today, the number of these non-human accounts used by organizations, and the number of applications that rely on such accounts, is growing each day.

Since service accounts are scattered across the organization and used by various business applications (not by human users), they are typically forgotten about and left unsupervised. This means that nobody is tracking their use or validating that they aren't hijacked and used by malicious actors. What a great opportunity for adversaries! Add to that the fact that domain level service accounts typically require elevated privileges and you make these accounts a prime target. Considering that too often, these accounts are over privileged - a result of the need to quickly implement business processes, makes them very valuable for hackers.

In the end, service accounts are left over-privileged and under-supervised.

You Can't Secure What You're Not Aware of

You might be sensing a problem here.

With hundreds or even thousands of these unsupervised, highly-privileged accounts running, they can become high-risk assets that, if left unchecked, may become a tool that enables threats to propagate throughout the network undetected. So these special accounts present an added set of risks, and in the process, create some very complicated challenges.

Here is a look at some of the problems created by service accounts:

Admins can't keep track of them

Service accounts are used for implementing much needed business processes, often in a haste. This leads to improper documentation of these accounts. Overtime, the lack of documentation and staff turnover leads to lack of awareness of the service accounts in use and their dependencies.

Passwords can be a pain

Service accounts are often left with the same initial password with which they were created. This is obviously a bad security practice - their passwords should be changed regularly. However, that's not always easy to do. Domain service accounts require passwords to be changed at both the domain and application level, which requires a ton of planning, creating additional complexity. In some cases, the passwords are hardcoded into the application code which means you need to change the application code itself.

The fear of unexpected downtime

Often, admins don't remember, or know, what dependencies service accounts have and there is a concern that if changes are implemented incorrectly, applications may break.

Sounds like a recipe for disaster, right?

Leaving service accounts unmanaged and improperly secured allows attackers to make their way deep inside networks, move laterally undetected, and get their hands-on critical data.

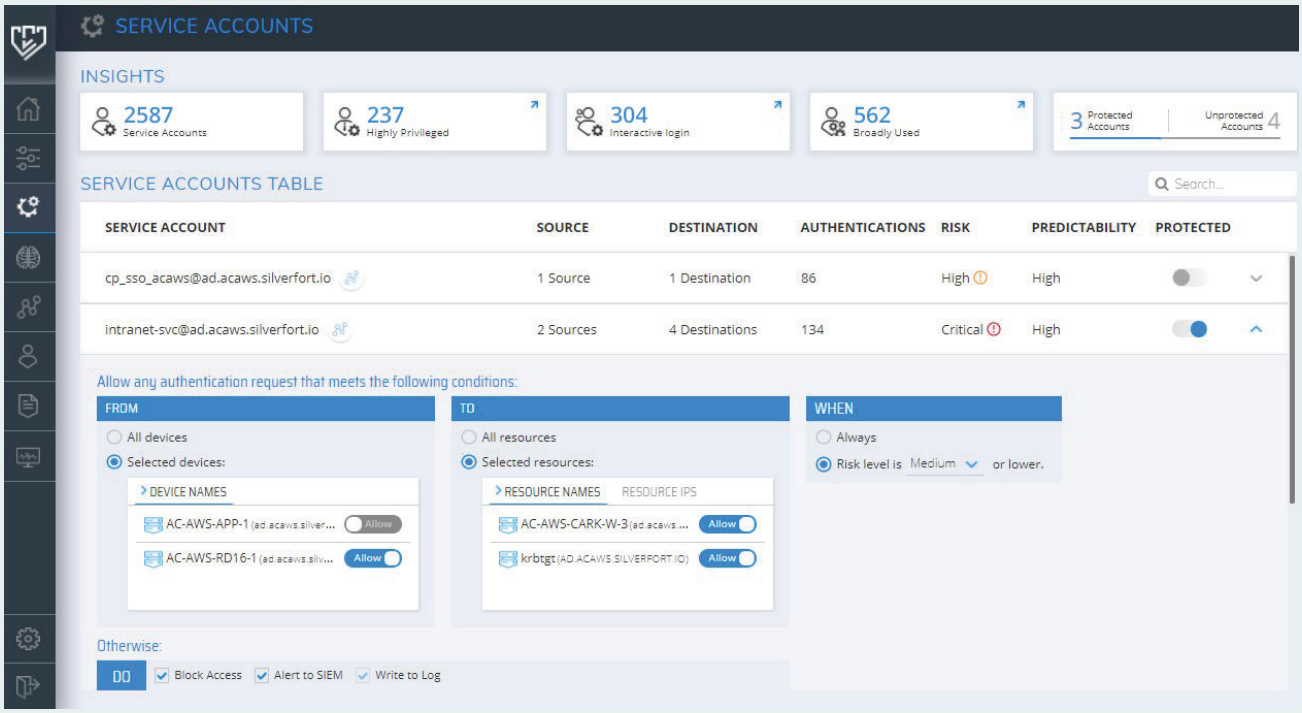
Current Methods of Securing Service Accounts Fall Short

To manage these potential landmines, most vendors are looking to establish strong password rotation policies. But there are some limitations to this approach. For example, it's not always possible to deal with hardcoded passwords, and you might wind up breaking applications with dependencies. Some organizations use password vaults, which securely manage your passwords. But to do this, you need to know which service accounts need to be managed by these solutions. And, in some cases you will need to modify the way your applications use your service accounts, which is not always possible and can be very expensive and time consuming.

Automated Protection For All Your Service Accounts

With Silverfort's Unified Identity Protection Platform, you can stop rolling out the red carpet for attackers by leaving your service accounts unsupervised, and instead, adopt an approach that's practical and simple. Silverfort enables you to detect and protect all your service accounts, without modifying them, and without requiring software agents, proxies or password changes.

No Need to Modify Service Account Passwords!



4 Steps to Comprehensive Service Account Security

DISCOVERY

Silverfort monitors all the authentication activity, of both human and non-human accounts in the network, providing unprecedented visibility into their behavior patterns. Service Accounts have predictable behavior patterns, which allows Silverfort to automatically identify and categorize them. Silverfort leverages and AI driven risk-engine that easily detects repetitive and predictable authentication patterns that may not be obvious to a human observer. To strengthen the AI-engine, Silverfort also looks for accounts that follow popular service accounts naming conventions, as well as custom naming conventions that may be used by the organization. As Silverfort detects Machine-like behavior patterns, it can also detect if an account is also used by a human user, and alert on this bad practice. Silverfort detects the erratic patterns associated with human user activities that do not match the machine behavior patterns, so if someone associated an application to their own personal user account, you would know about it.

> **With the in-depth visibility Silverfort provides, you can finally be aware of all your service accounts and their dependencies, allowing you to take the next steps required to secure their usage.**

MONITORING

Auditing, and Threat Detection - Now that you are aware of all your service accounts, and have visibility into their behavior, Silverfort continues to monitor and audit their use. By continuously monitoring and auditing authentication and access activity, Silverfort assesses the risk of every authentication attempt, and detects any suspicious behaviors or anomalies, providing SOC teams with deep insight to make intelligence-driven decisions.

AUTOMATIC POLICY SUGGESTIONS

Okay, now you've got this vastly deep visibility into all your service account behavior—how should you go about applying granular access control and Zero Trust policies across these non-human accounts and services? Silverfort is here to help. Silverfort automatically recommends specifically tailored policies for each service accounts, based on their actual behavior patterns: Silverfort has 3 basic types of authentication policies: Allow Access, Deny Access or Require MFA. For obvious reasons, implementing MFA for service accounts doesn't make much sense – after all, there is no human monitoring these accounts to address the MFA request. However, Allow and Deny access policies can be leveraged to automatically secure the use of service accounts. Silverfort's recommended policies simply allow service accounts to continue operating according to the same predictable authentication behavior that has been observed previously, while denying any authentication attempt outside these bounds. Therefore, even if a service account is over privileged, and can access other computers, it won't be able to properly authenticate. So now you can review these recommendations, tune the policies if needed, and turn them on when ready.

PROTECTION AND RESPONSE

The last step is to enforce the policies. With an easy flip of a button, you can actively enforce these policies across all your service accounts - without making any changes to your applications, without changing passwords and without requiring any proxies.

> **Silverfort can alert in real-time, or block access, of any attempts that are outside the expected behavior of each service account, (as was determined by Silverfort's AI engine). This allows you to limit service accounts to their intended purpose and enables automated response to any unauthorized access attempt.**

Conclusion

With Silverfort's Unified Identity Protection Platform, you can finally see what you've been missing. Discover all your service accounts, find the threats and blindspots you need to address, and increase your overall security posture - all without the need to modify or change anything. To find out more about setting up optimal, automatic security for your service accounts, reach out to a Silverfort Rep today.

Benefits of Silverfort's No-Modifications-Needed Security

Establish non-intrusive security without disruptions to business processes
Make securing service accounts simple and sustainable, without the need to change applications, implement software agents or proxies, or any password changes.

Drastically reduce organizational risk
Limit your attack surface and cut down on risk, by automatically discovering and securing all service accounts.

Get automatic, intelligent policy suggestions
Make optimal decisions regarding each account's behavior and risk with automatic suggestions.

AI-based detection of threats in real-time
Leverage an AI-based risk engine to detect threats and prevent them from spreading laterally across your networks.

Lower your security spend
Reduce setup and maintenance efforts and keep security costs low, so you can use your budget for supporting the growth of your business.

About Silverfort

Silverfort is a Unified Identity Protection Platform that consolidates security controls across corporate networks and cloud environments to block identity-based attacks. Using innovative agentless and proxyless technology, Silverfort seamlessly integrates with all existing IAM solutions, extending their coverage to assets that could not be protected until today, such as homegrown/legacy applications, IT infrastructure, file systems, command-line tools, machine-to-machine access and more. It continuously monitors all access of users and service accounts across both cloud and on-premise infrastructure, analyzes risk in real time using an AI-based engine, and enforces adaptive authentication and access policies. Silverfort allows organizations to prevent data breaches, achieve compliance, reduce costs and simplify cloud migration.

To learn more schedule a meeting at:
www.silverfort.com/request-a-demo