SILVERFORT | IS4U

Overcoming the Security Blind Spot of Service Accounts

eBOOK

Service Accounts Are a Security Challenge That Must Be Resolved

In today's rapidly evolving cybersecurity landscape, service accounts have emerged as a pressing concern for identity and security stakeholders. These machine-to-machine accounts have proven to be a double-edged sword, as adversaries increasingly use them for lateral movement, particularly in the realm of ransomware attacks. The inherent lack of visibility, coupled with their elevated access privileges and exemption from identity protection measures like Privileged Access Management (PAM) and Multi-Factor Authentication (MFA), renders service accounts a perilous blind spot—a veritable goldmine for attackers.

This eBook examines the factors that make protecting service accounts a hard task and assesses the existing approaches to mitigate this risk and their limitations. We then explore the new approach of Unified Identity Protection, which addresses this challenge by automating service account discovery, monitoring, and protection, providing true coverage to this exposed attack surface for the first time.

Service Accounts 101: The Silent Workers in the Background

In the Active Directory environment, service accounts play a pivotal role in facilitating the seamless functioning of various applications and services. **At their core, service accounts are similar to human user accounts** in that they both possess login credentials and access rights. However, service accounts are specifically designed for system-level automation, operating behind the scenes without the need for human intervention. These are the two most prominent service account use cases:

Automate Repetitive Tasks for Admin

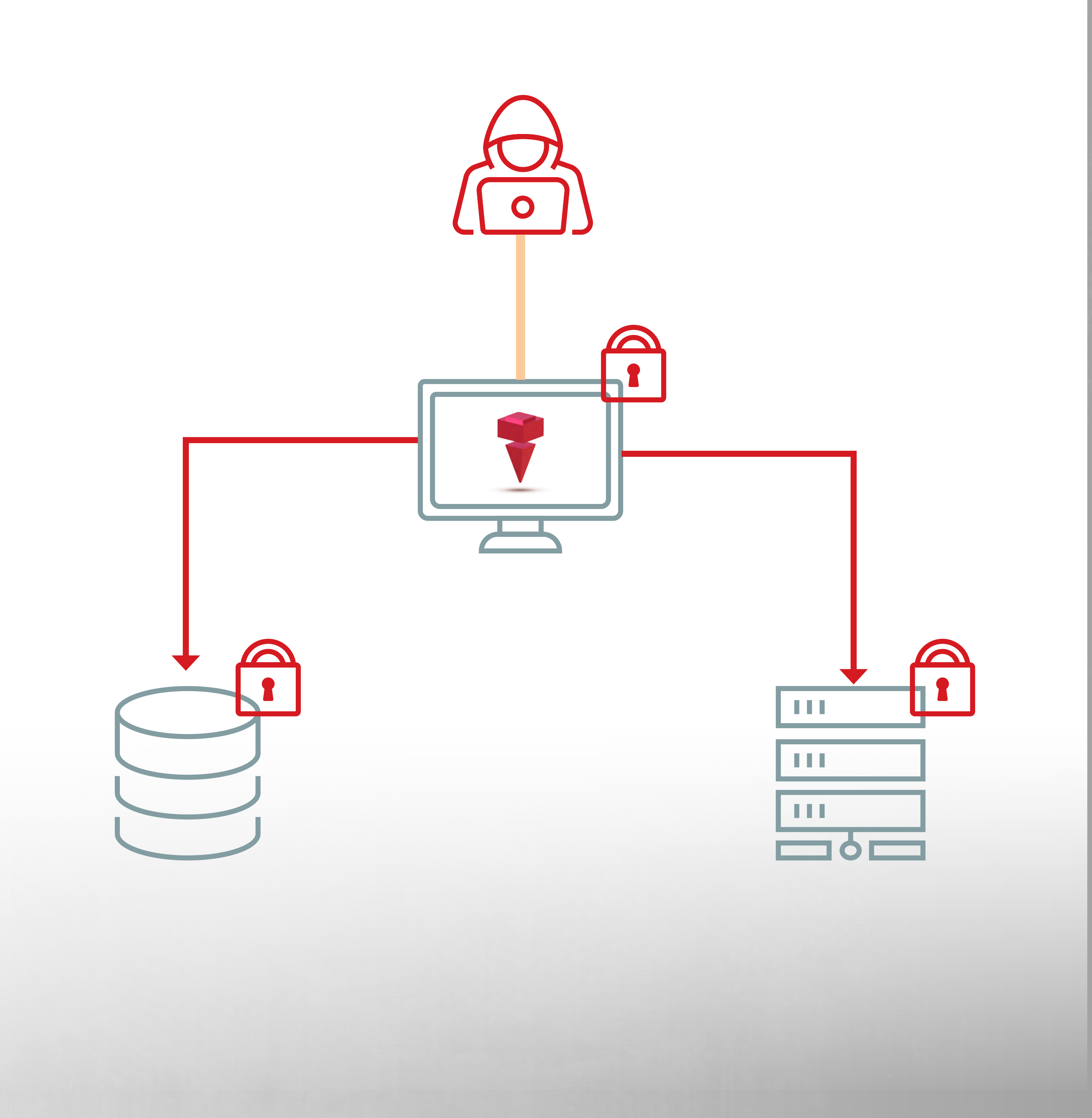
Admins often create service accounts to automate repetitive IT tasks on multiple machines in the environment. Common tasks assigned to service accounts include automated data backups, system monitoring, and scheduled maintenance.

Maintenance for On-Prem Software

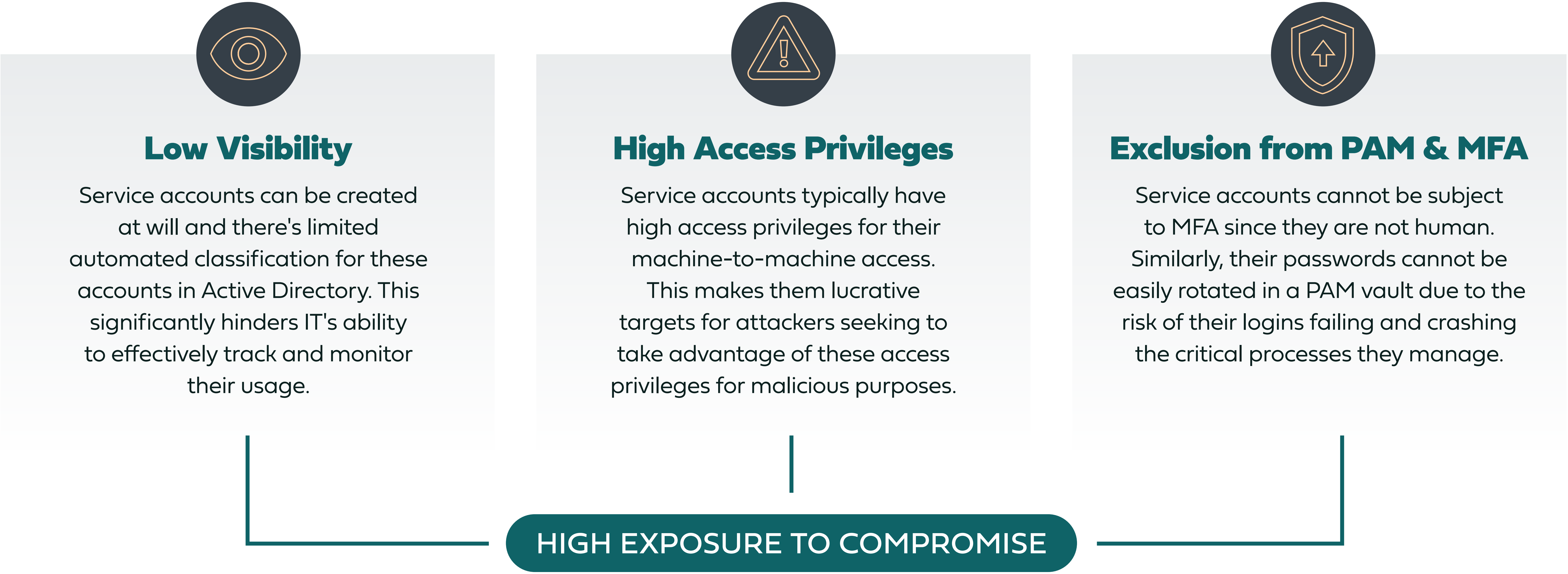
On-prem software applications rely on service accounts to act as intermediaries between the application server and client machines. These accounts manage tasks such as monitoring, updating distribution, and performing health checks.

The Service Account Threat Landscape: The Ultimate Tool for Lateral Movement and Ransomware Spread

In recent years, ransomware attacks have surged, becoming a significant cybersecurity concern for organizations worldwide. Disturbingly, over 80% of these attacks now employ lateral movement as a tactic to escalate their impact and maximize damage. As more and more attacks show, service accounts have become the ideal and most sought-after tool for facilitating lateral movement within compromised environments.



Service Account Security Challenges: Invisible, Highly Privileged, and Unprotectable



Low Visibility

Service accounts can be created at will and there's limited automated classification for these accounts in Active Directory. This significantly hinders IT's ability to effectively track and monitor their usage.

High Access Privileges

Service accounts typically have high access privileges for their machine-to-machine access. This makes them lucrative targets for attackers seeking to take advantage of these access privileges for malicious purposes.

Exclusion from PAM & MFA

Service accounts cannot be subject to MFA since they are not human. Similarly, their passwords cannot be easily rotated in a PAM vault due to the risk of their logins failing and crashing the critical processes they manage.

HIGH EXPOSURE TO COMPROMISE

The Three Approaches to Protecting Service Accounts

Manual Discovery and Monitoring

How: Investigating directories and machines to identify service accounts and their associated scripts.

Pros: Doesn't require a dedicated solution or skill.

Cons: Resource consuming, partial results, prone to human error.

No visibility or protection against malicious access

Alerting on Anomalous Activity

How: Utilizing Security Information and Event Management (SIEM) or Endpoint Detection and Response (EDR) platforms to alert when deviations from normal behavior occur.

Pros: Automated alerting.

Cons: Allows malicious activity to continue while investigation takes place, requires highly skilled security team, prone to alert fatigue.

Retroactive visibility without preventing malicious access

Unified Identity Protection Platform

How: Automated discovery, monitoring and protection for all service accounts.

Pros: Full coverage, zero manual effort, automated blocking of malicious activity.

Cons: Need to manually enable policies.

Real-time blocking of the compromised service accounts' malicious accesss

What is a Unified Identity Protection Platform?

Unified Identity Protection is a new category of security products purpose-built to deliver real-time protection of the identity attack surface via continuous monitoring, risk analysis, and access policy enforcement on every incoming authentication and access request, both on-prem and in the cloud. It achieves this by integrating with the Identity Providers (IDP) in the environment. This integration enables the platform to gain visibility into 100% of user authentications within the environment.

In the context of service accounts, a Unified Identity Platform leverages its visibility into every incoming access request to Active Directory to **identify** the accounts that feature a predictable and repetitive behavior, classify them as service accounts, and **protect them with access policies.**

How Does a Unified Identity Protection Platform Secure Service Accounts?

At the core of the Unified Identity Protection platform is its integration with the identity providers – in this case it's Active Directory. With this integration, the platform becomes a native part of the authentication flow:

1 → 2 → 3 → 4

1 See All Authentications

AD forwards every incoming account access attempt to the Unified Identity Protection platform.

2 Learn Account Behavior

Within a defined learning period the platform classifies the accounts that feature a repetitive and predictable behavior and classifies them as service accounts.

3 Identify Service Accounts

The platform associates each service account with its mapped standard behavior that becomes its baseline.

4 Generate Policy

A policy is generated to block or alert when a service account or group of service accounts deviates from their standard behavior.

From now on every access attempt of the service account is evaluated against the policy, allowing normal access and blocking any deviation.

The Silverfort Way: Fully Automated Service Account Protection

Silverfort's Unified Identity Protection automates the entire service account life cycle:

Automated Discovery

Automatically discover all service accounts within the environment and map their sources, destinations, privilege levels and common usage patterns.

Activity Monitoring

Continuously monitor service account activity in real time. This includes tracking and the usage patterns, access requests, and behavior of each service account. Any deviation from the service account's standard behavior is immediately identified.

Real-Time Protection

Set access policies that alert or block access for single or multiple accounts whenever they deviate from their standard behavior. This prevents adversaries from using service accounts for malicious access, even if they have compromised them.

In this manner, all service accounts within the environment are visible and protected with almost no manual effort from the identity and security teams.

About Silverfort

Silverfort has pioneered the first-ever Unified Identity Protection platform, which protects enterprises against identity-based attacks that utilize compromised credentials to access enterprise resources. Using innovative agentless and proxyless technology, Silverfort natively integrates with all existing IAM solutions, to extend secure access controls such as Risk-Based Authentication and MFA across all on-prem and cloud resources. This includes assets that could never have been protected in this way before, such as homegrown/legacy applications, IT infrastructure, file systems, command-line tools, machine-to-machine access, and more. Silverfort continuously monitors all access attempts by users and service accounts and analyzes risks in real time using an AI-based engine to enforce adaptive access policies.

For more information, visit silverfort.com