Silverfort

CASE STUDY

US insurance provider enhances identity security posture with authentication firewall to deny all unauthorized access to critical resources

BASED
South Central US

INDUSTRY
Insurance

USERS
425

ENVIRONMENT
36 Service accounts
6 Domain controllers
10 Core on-prem applications
Azure cloud services

THE CHALLENGE:

The insurance company needed to strengthen its identity security posture by applying deny access policies and improving its visibility into service accounts.

CUSTOMER OVERVIEW

About

The company is a trusted insurance provider and offers solutions to protect customers' most significant financial investments. They combine proven experience with a customer-first approach to ensure seamless and secure transactions for home buyers, sellers, lenders, and commercial customers.

Environment

The company operates in a hybrid IT environment with 10 legacy on-prem critical applications and Azure cloud services. Their environment is distributed between 13 office locations and includes 6 domain controllers, SQL servers, and file shares across their offices. They deploy 20 privileged service accounts to run various application services and automated processes within their environment.

Why now

Leading by the CISO's proactive approach to cybersecurity, the company needed to implement MFA protection across all users and on-prem resources. The company's security team used shared domain accounts as proxy service accounts which caused high security risks which could lead to compromise. Additionally, they needed to apply strict security controls to their users across different locations which would deny access to the allowed resources and permitting them to access only necessary resources.

Finding the right partner

As the company's security team had already used MFA for their cloud operations, they knew they needed a scalable solution with MFA protection capabilities for their on-prem environment. At the same time, the company wanted to get rid of shared domain accounts used as proxy service accounts and get more visibility and logging information for their regular automated tasks and scripts.

The company discovered Silverfort's offering on Reddit. They quickly requested a demo and then proceeded to run a proof of concept with Silverfort. After a successful POC, the company realized the Silverfort platform was the ideal solution for their identity security needs. The deployment took less than one month, during which they enrolled 425 employees, configured 36 service accounts, and set an authentication firewall to deny access unless explicitly allowed.

CHALLENGE 1:

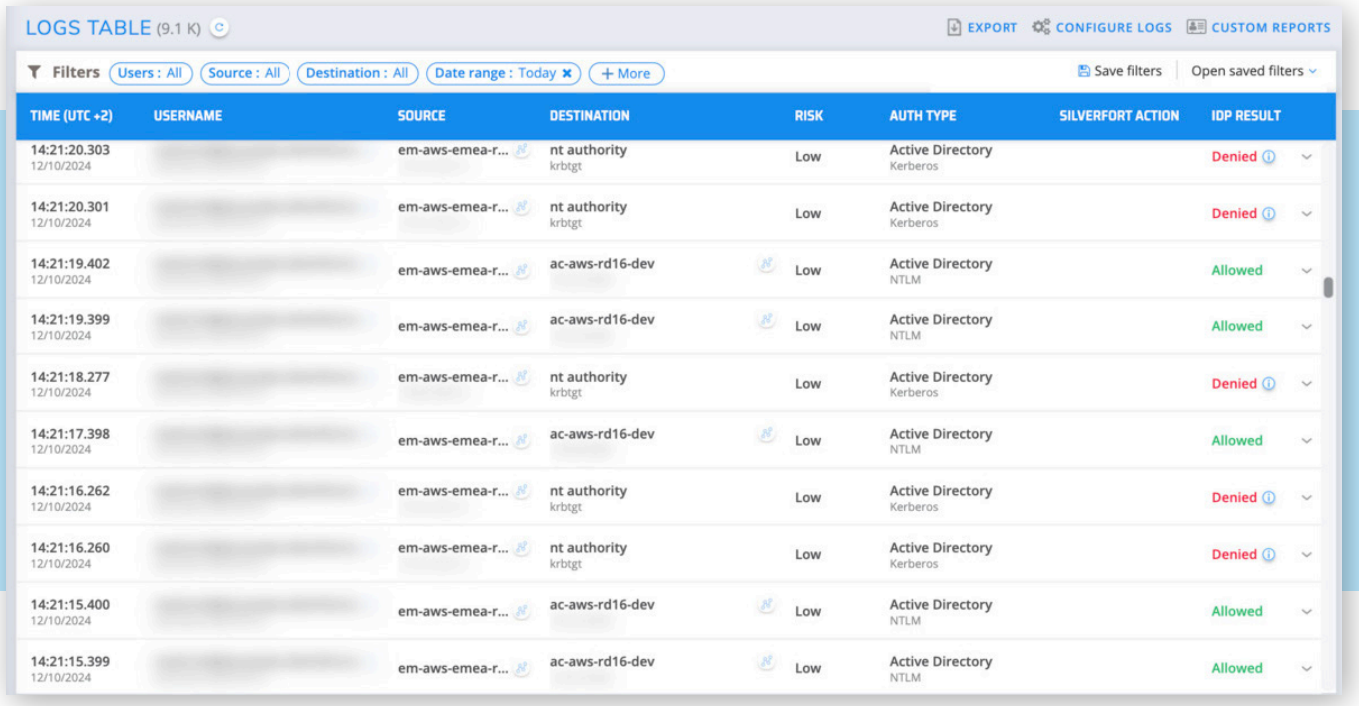
Denying access to critical resources

Preventing unauthorized access to critical resources

The company needed to enable strict security controls for all users, especially privileged accounts. These devices needed to have role-based access to the critical resources. The company wanted to block all access to domain controllers for basic users and to allow them to authenticate to the file server only for shared folder access. Keeping excessive access permissions for these user groups would pose a significant security risk.

Deny access policies with Silverfort's Authentication Firewall

By enforcing Silverfort's authentication firewall, the company quickly configured and applied a set of 40 access policies with allow, deny, and MFA rules based on user identity and real-time authentication analysis. The company enforced least privileged access policies to each user, ensuring they could have only access to the resources they needed and removed any excessive access permissions. By creating strict authentication controls, they enhanced their environment's resilience to identity threats.



The company's authentication logs dashboard in Silverfort, provides full visibility into all user logs, authentication activity and other user insights. If any unauthorized or abnormal behavior is identified, the system can immediately Deny Access. All the details about a denied access event within the environment will be displayed, including last time used, account name, source, destination and risk level.

CHALLENGE 2:

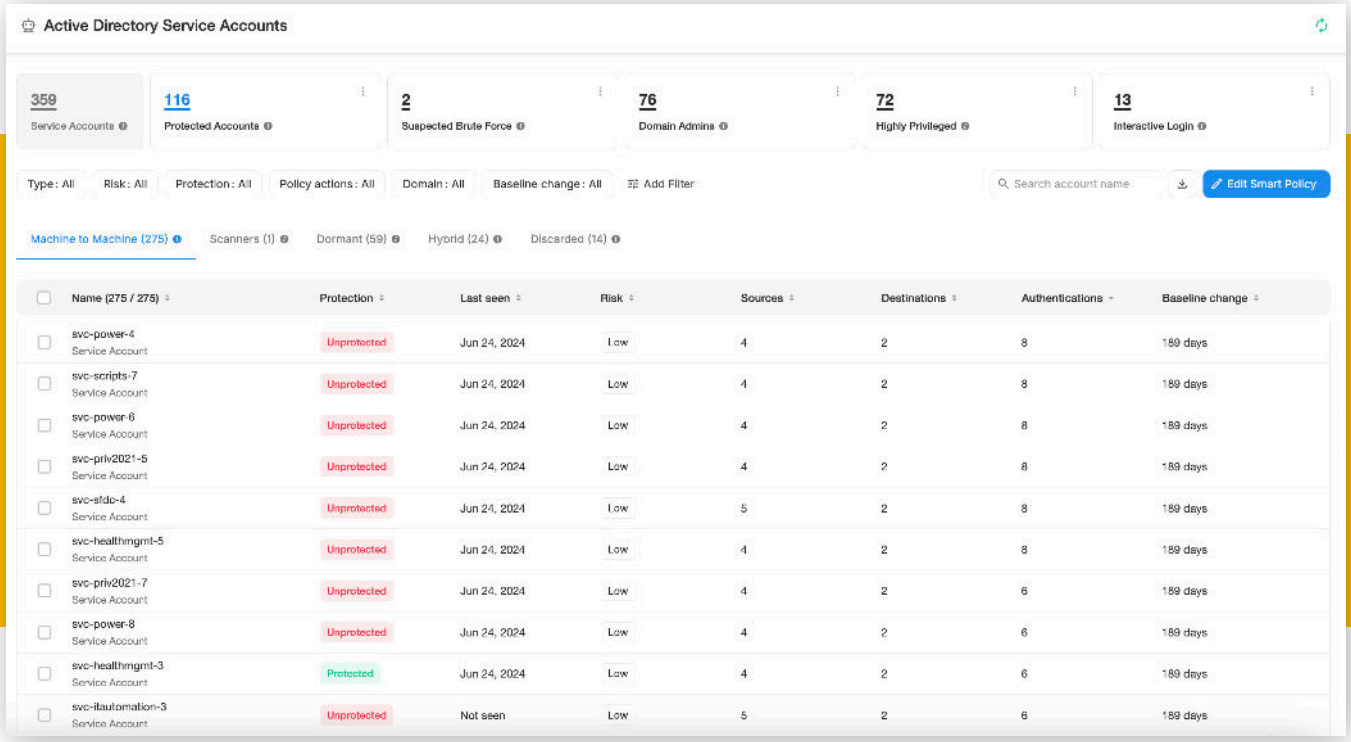
Visibility into service accounts

Limited visibility of service accounts

The company had 20 service accounts, and recognized they had a critical need to have real-time visibility into each service account to effectively mitigate security risks. They had a technical debt of using shared domain accounts as proxy service accounts with elevated privileges to run scripts and perform automated tasks on machines. By understanding the critical security risks of service account misuse, the company needed a solution that would provide full management of service accounts including logging information to get real-time insights into all their activities.

Complete service account protection

With Silverfort, the company gained automated discovery, real-time monitoring and comprehensive visibility into the activities of its 20 service accounts, including source, destination, and last time used. In less than 4 weeks, they were able to delete the over-privileged service accounts and configure a new set of 36 service accounts to run dedicated automated tasks. Additionally, the company vaulted each service account's credentials into their PAM to ensure they are secured. By changing its approach to service account management and protection, the company significantly improved its overall identity security posture.



The company's service accounts dashboard in Silverfort displays all detected service accounts, including name, source, destination, number of authentications, risk score, baseline change and other account info.

CHALLENGE 3:

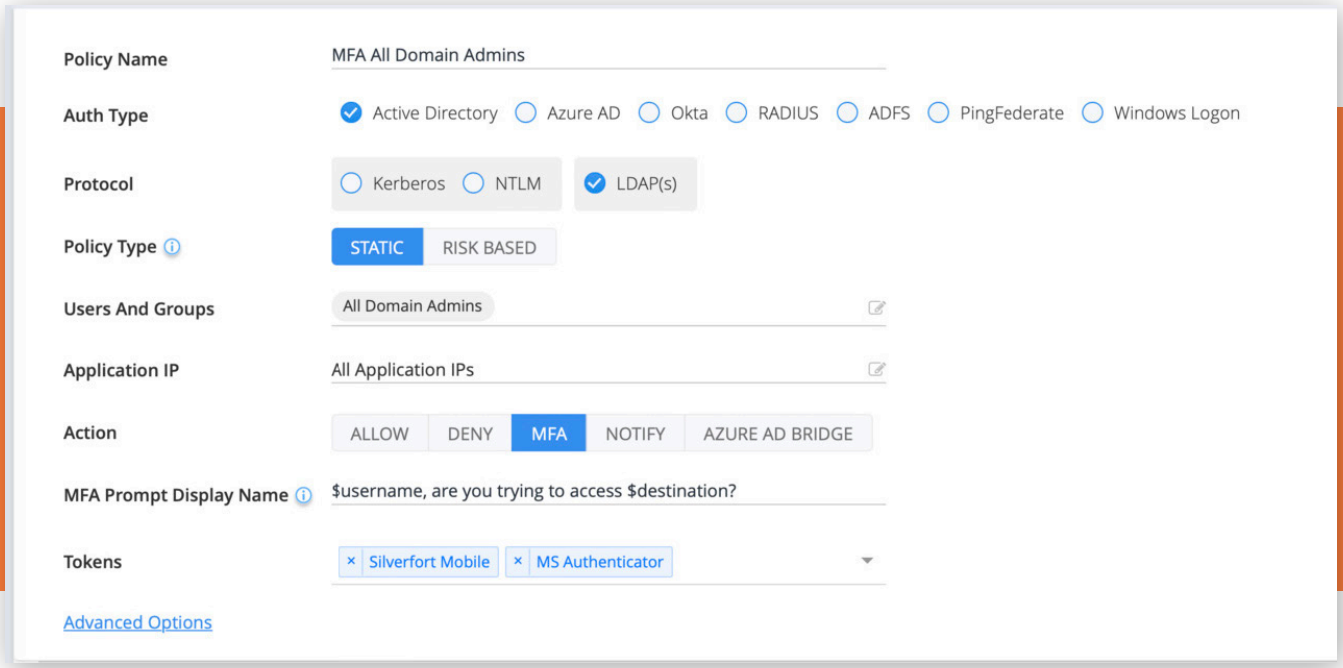
On-prem MFA protection

Needed to secure on-prem resources with MFA

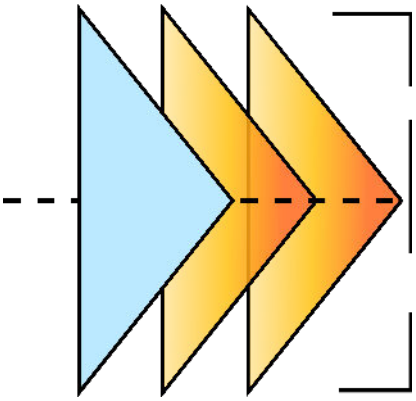
The company needed to apply MFA protection to its on-prem infrastructure and resources. They needed to add MFA protection for all users across 13 different locations, including privileged admin accounts. The main goal was to mitigate the risks of unauthorized access to critical infrastructure like file servers and remote desktop machines through RDP and VPN. This was one of the key use cases and challenges that they needed to solve.

Applied MFA protection to all on-prem resources with Silverfort

By enforcing MFA protection with Silverfort across all on-prem resources, the company improved its overall identity security posture. They configured 10 MFA access policies for their users' identity verification based on a specific office location. When users are trying to gain access into a shared folder on a file server or to log in to a remote machine through VPN, they are now required to be verified with Silverfort's MFA. By adding security controls to every user access request for core on-prem systems and devices, the company extended its cloud services protection to the IdPs that could never have been protected with MFA before.



The company's LDAP protocol policy requires all access requests by domain admin accounts to be verified with MFA. During LDAP authentications, they see which application the admin is trying to access and the IP address of users.



Moving forward

After quickly deploying Silverfort across their hybrid environment, the insurance company successfully implemented authentication firewall capabilities to deny unauthorized access to critical resources. With the enablement of a highly secure policy-driven approach and detailed activities monitoring, the company has gained full visibility to all account authentications, based on specific user roles like privileged accounts.

What began as a project to extend MFA coverage from only cloud resources to hybrid, including on-prem systems, it evolved into an opportunity to eliminate years of technical debt with proxy service accounts with elevated privilege access. By implementing task-specific service account practices, the organization quickly achieved results that exceeded their expectations. With Silverfort in place, the company's IT security team is now equipped with strong security controls to identify and stop identity-based attacks, ensuring their environment is protected against evolving threats.

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