Silverfort

CASE STUDY

Leading gaming company extends MFA protection to core legacy applications and bridges on-prem resources to Entra ID with Silverfort

BASED	INDUSTRY	USERS	ENVIRONMENT
Israel	Gaming	1,000+	1,000 Service accounts 38 Domain controllers 10 Core on-premlegacy applications Network infrastructure

THE CHALLENGE:

The gaming company needed to apply end-to-end multi-factor authentication (MFA) protection to all users and core legacy business applications.

CUSTOMER OVERVIEW

About

An international telecommunications provider headquartered in Southeast Asia and operating in over 20 countries. It offers internet service provision, mobile phone networks, and fixed-line telephone services, as well as services such as data and internet solutions, information technology, engineering, and more.

Environment

The telecommunications provider operates with 15 core business homegrown legacy applications integrated throughout its organization. Their suite of legacy applications was developed specifically for their telecommunication needs. One prominent example is their custom CRM system used across the company, enabling employees to access customer data. There are two categories of users accessing these applications regularly: internal users (comprising support teams, IT personnel, and other staff members) and external users from third-party vendors.

Why now

The telecom provider needed to apply end-to-end multi-factor authentication (MFA) protection to their custom legacy telecom applications. When their employees requested access to view customer data from an application, there was no process in place to verify the user.

Finding the right partner

As a result of their growing identity security challenges and the rapidly evolving threat landscape, the company's IT security team sought a scalable solution that would help them comply with PCI DSS MFA requirements, while providing advanced MFA protection and complete visibility into their service accounts.

After meeting Silverfort at a security conference, they ran a demo and proof of concept and quickly identified the Silverfort platform as the most appropriate solution for addressing their MFA protection needs. The deployment took one month, during which they enrolled over 1,000 employees, 1,000 service accounts and 10 critical business applications with the proper security controls.

Challenge 1: Comply with industry regulations

Needed to comply with PCI DSS MFA requirements

The company needed to comply with PCI DSS MFA requirements, which would result in a significant overhaul of its identity security controls. To comply, the organization needed to implement MFA protection and security controls for all users, including administrator accounts, reinforce access controls, and mitigate the risk of unauthorized access. The challenge of PCI DSS compliance was a major initiative for the company.

Achieving PCI DSS compliance with Silverfort

By implementing robust MFA protection across all resources and users, the company significantly bolstered its overall identity security posture. By adding security controls to every user access request for core applications, the company has not only strengthened its security but also streamlined its compliance framework processes. By taking this strategic approach, the PCI DSS compliance requirements were met quickly and easily, underlining the company's commitment to safeguarding sensitive data and maintaining regulatory compliance.

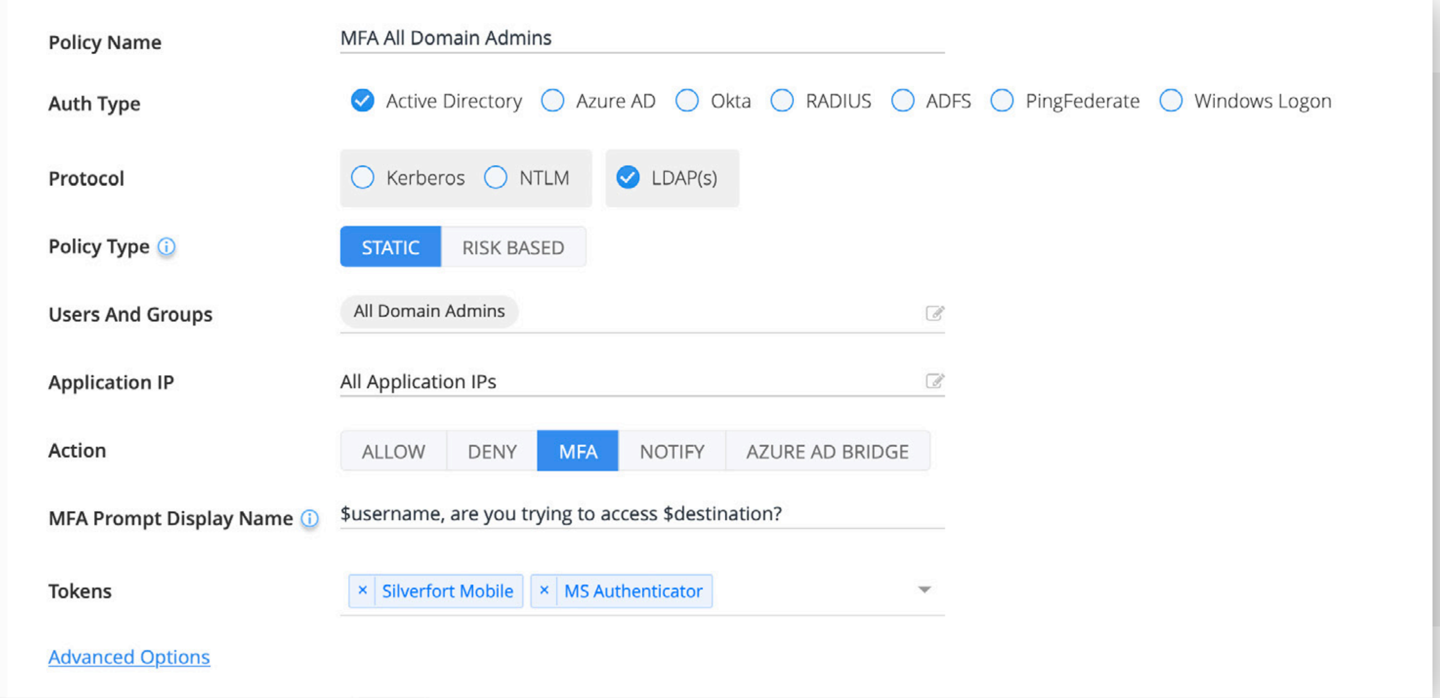
Challenge 2: Protecting privileged admin accounts

Domain admin accounts needed MFA protection

To enhance their security posture, the company needed to implement additional security controls, including MFA protection for their highly privileged domain admin accounts. Since these accounts have elevated privileged access, they frequently interact with critical legacy business applications, making them potential targets for malicious actors. By protecting all domain admin accounts with MFA, the company created an extra layer of security by requiring these admin users to verify their identities more frequently before gaining access to different applications.

Protecting all domain admins with MFA

As a result of the deployment of Silverfort, the company configured and applied a user access policy for all domain administrators. Their Silverfort MFA policy rules would trigger an MFA prompt once an hour to verify the user's identity. This policy was specifically designed to protect domain admin access requests to the company's domain controllers. Once the policy was applied, all domain admin accounts were protected with the appropriate security controls. Following the policy's success, the company began to implement additional policies to protect user access across its systems.



Policy Name	MFA All Domain Admins
Auth Type	● Active Directory ○ Azure AD ○ Okta ○ RADIUS ○ ADFS ○ PingFederate ○ Windows Logon
Protocol	○ Kerberos ○ NTLM ● LDAP(s)
Policy Type ⓘ	[✓ STATIC] RISK BASED
Users And Groups	All Domain Admins
Application IP	All Application IPs
Action	ALLOW DENY [✓ MFA] NOTIFY AZURE AD BRIDGE
MFA Prompt Display Name ⓘ	$username, are you trying to access $destination?
Tokens	× Silverfort Mobile × MS Authenticator

Advanced Options

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.

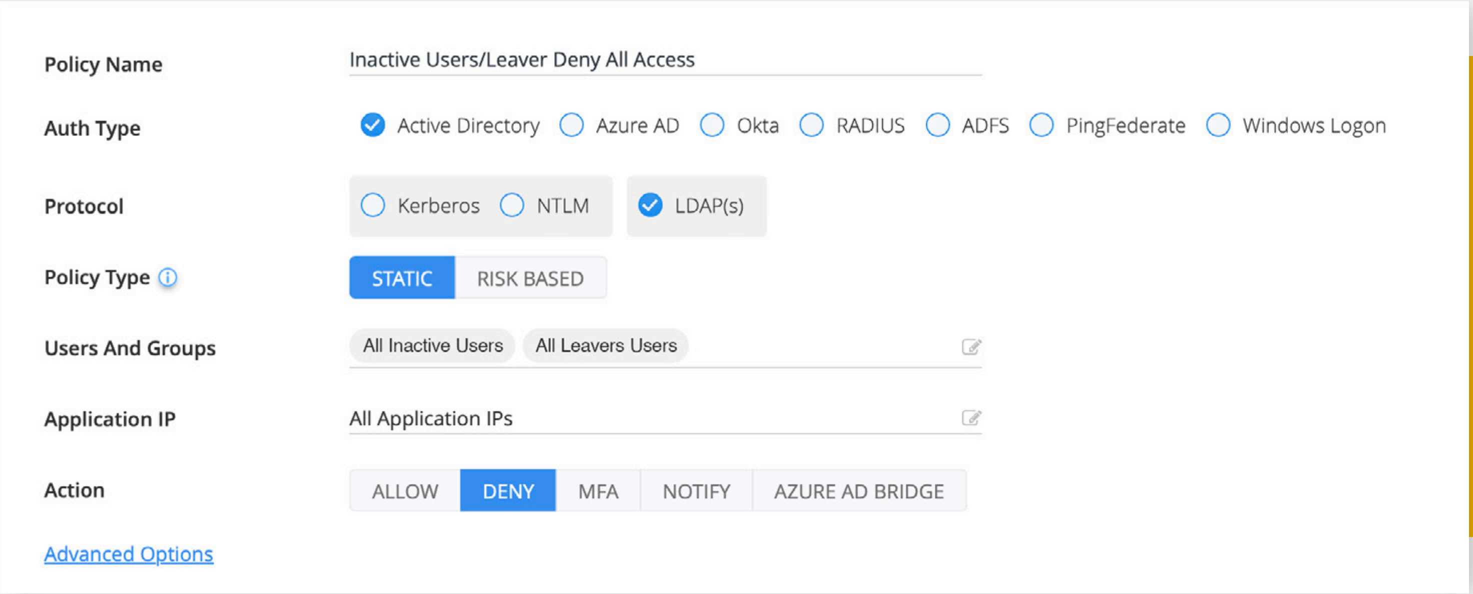
Challenge 3: Denying access to inactive accounts

Preventing access for inactive accounts

The company needed to implement stringent security controls for inactive accounts, particularly those associated with terminated employees who might have access for a short period of time. These accounts should not be able to access or authenticate to any resource. As such, the company must use security controls to ensure they are completely removed and denied access to any resources. If not properly managed, these accounts may pose a security risk, despite their inactive status.

All inactive users are automatically denied access

The company took proactive measures to enhance its security posture by configuring and applying a 'deny access' policy specifically targeted at a group of inactive users. Despite these users typically not having any access privileges, the company recognized the potential risk they could pose if not properly managed. The policy rules were designed to automatically deny any access requests from these users, effectively eliminating the possibility of unauthorized access. This proactive approach served as an additional layer of protection, reinforcing the company's commitment to securing its critical resources and environment.



Policy Name	Inactive Users/Leaver Deny All Access
Auth Type	● Active Directory ○ Azure AD ○ Okta ○ RADIUS ○ ADFS ○ PingFederate ○ Windows Logon
Protocol	○ Kerberos ○ NTLM ● LDAP(s)
Policy Type ⓘ	[✓ STATIC] RISK BASED
Users And Groups	All Inactive Users, All Leavers Users
Application IP	All Application IPs
Action	ALLOW [✓ DENY] MFA NOTIFY AZURE AD BRIDGE

This policy automatically denies access to any inactive account to whom this policy is assigned. If an account under the policy was compromised, it would block any threat actor from using it for malicious access.

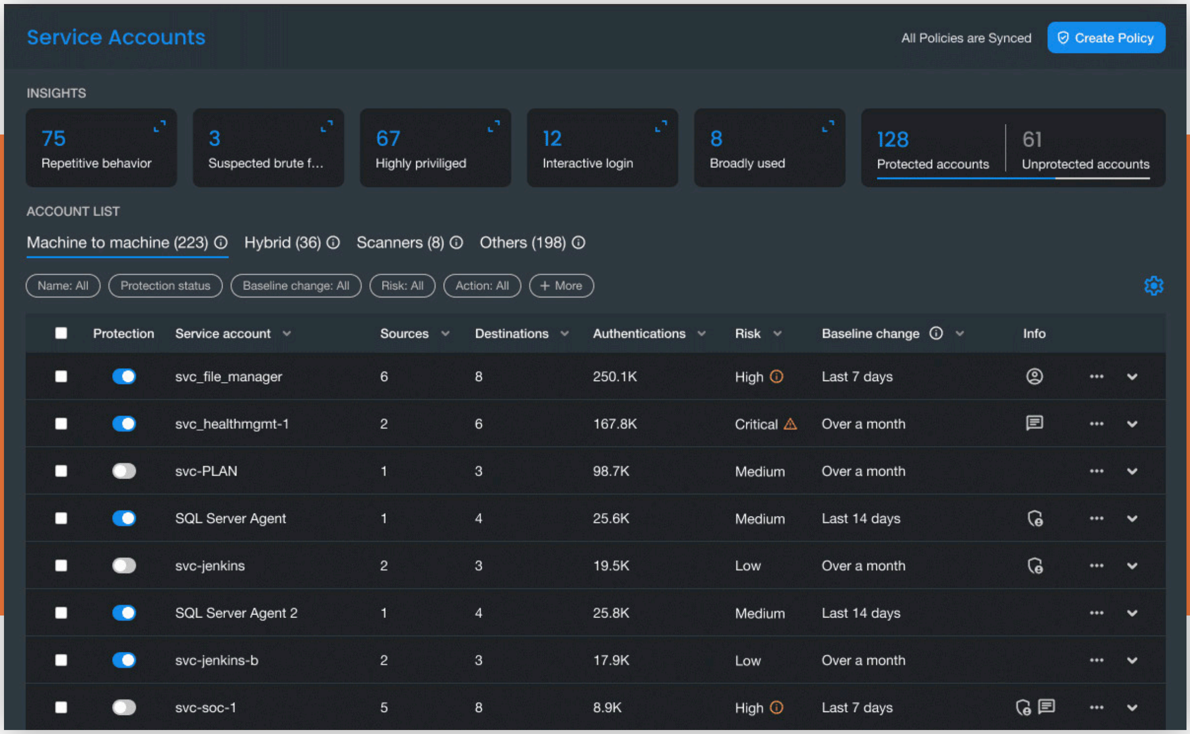
Challenge 4: Visibility into service accounts

Limited visibility of service accounts

With approximately 1,000 service accounts, the company knew they needed enhanced visibility into their activities. Due to their critical operational role as well as the potential security risks associated with these accounts, the organization sought real-time insights into the activity of the accounts to enhance security measures. The company aimed to monitor and understand their service accounts' behavior, particularly those interacting with critical systems and data.

Complete service account protection

With Silverfort, the company gained real-time monitoring and comprehensive visibility into the activities of its 1,000 service accounts, including source, destination and last used. Additionally, the company has placed virtual fencing around each service account to ensure they are protected. These are complemented by access policies unique to each service account. Taking a proactive approach to service account security helped the company to monitor all service account activities in real time, providing a clear and detailed view of their behaviors.



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	🛡 💬	···	⌄

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.

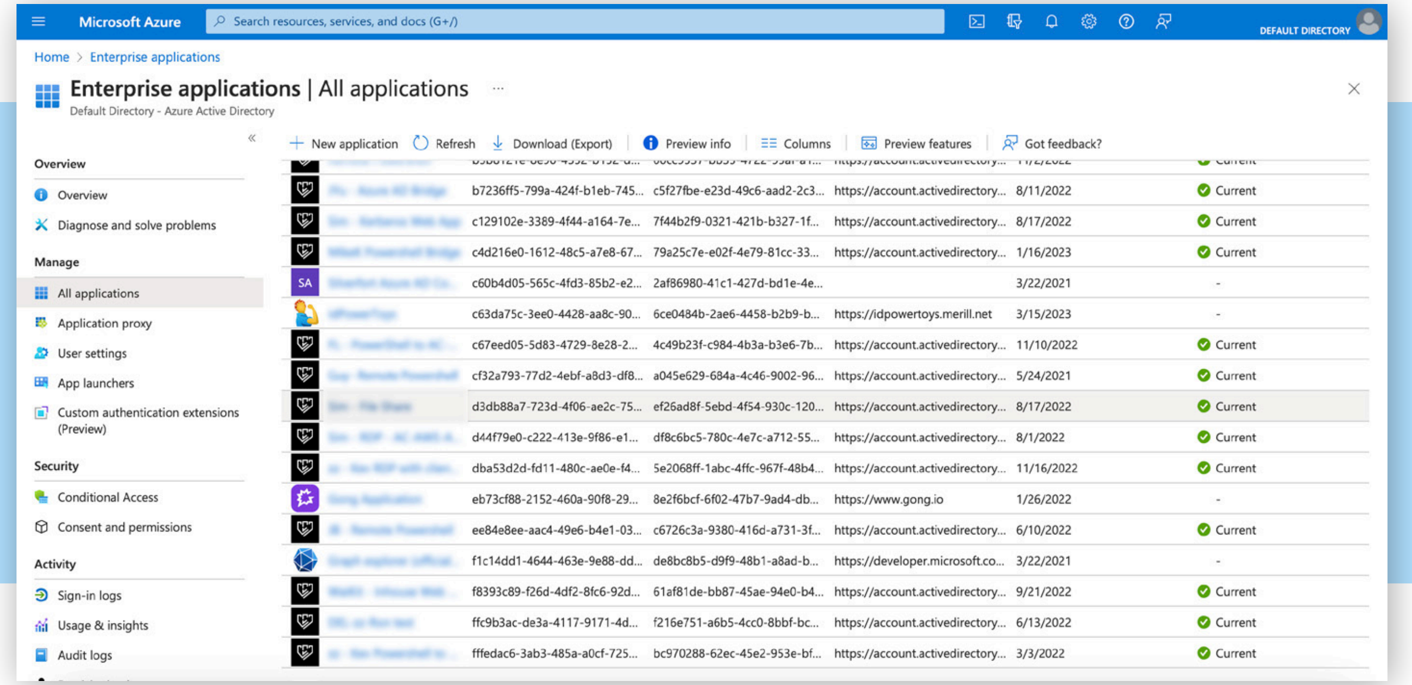
Challenge 5: Extending Entra ID controls to on-prem

On-prem environment did not support Entra ID security controls

The company wanted to extend its Entra ID security controls uniformly to all on-prem resources and policies in its entire environment. While Entra ID effectively protected the company's cloud environment with conditional access and MFA capabilities, extending this protection to their on-prem environment was a challenge. As a result, the company's security team faced a critical gap because the existing authentication protocols used by these on-prem resources did not inherently support Entra ID. The company recognized how important it was to close this gap by extending Entra ID's security controls across its hybrid environment to ensure comprehensive user protection and streamlined authentication processes.

Bridging on-prem resources to Entra ID

The company used Silverfort to bridge three on-prem applications and extend their Silverfort policies to Entra ID. This integration allowed the company to apply Entra ID's robust security controls to these on-prem resources, thereby enhancing their overall security posture. The company was very happy with the manual bridging process and the resulting unified sign-in method for both on-prem and cloud resources. This integration not only simplified the authentication process for their users but also ensured a consistent level of security across all resources.



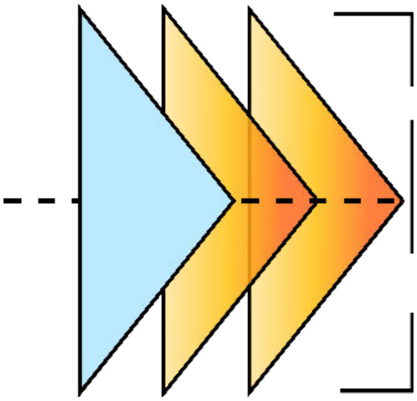
Enterprise applications | All applications

Default Directory - Azure Active Directory

	[redacted]	b7236ff5-799a-424f-b1eb-745...	c5f27fbe-e23d-49c6-aad2-2c3...	https://account.activedirectory...	8/11/2022	✓ Current
	[redacted]	c129102e-3389-4f44-a164-7e...	7f44b2f9-0321-421b-b327-1f...	https://account.activedirectory...	8/17/2022	✓ Current
	[redacted]	c4d216e0-1612-48c5-a7e8-67...	79a25c7e-e02f-4e79-81cc-33...	https://account.activedirectory...	1/16/2023	✓ Current
SA	[redacted]	c60b4d05-565c-4fd3-85b2-e2...	2af86980-41c1-427d-bd1e-4e...		3/22/2021	-
	[redacted]	c63da75c-3ee0-4428-aa8c-90...	6ce0484b-2ae6-4458-b2b9-b...	https://idpowertoys.merill.net	3/15/2023	-
	[redacted]	c67eed05-5d83-4729-8e28-2...	4c49b23f-c984-4b3a-b3e6-7b...	https://account.activedirectory...	11/10/2022	✓ Current
	[redacted]	cf32a793-77d2-4ebf-a8d3-df8...	a045e629-684a-4c46-9002-96...	https://account.activedirectory...	5/24/2021	✓ Current
	[redacted]	d3db88a7-723d-4f06-ae2c-75...	ef26ad8f-5ebd-4f54-930c-120...	https://account.activedirectory...	8/17/2022	✓ Current
	[redacted]	d44f79e0-c222-413e-9f86-e1...	df8c6bc5-780c-4e7c-a712-55...	https://account.activedirectory...	8/1/2022	✓ Current
	[redacted]	dba53d2d-fd11-480c-ae0e-f4...	5e2068ff-1abc-4ffc-967f-48b4...	https://account.activedirectory...	11/16/2022	✓ Current
	[redacted]	eb73cf88-2152-460a-90f8-29...	8e2f6bcf-6f02-47b7-9ad4-db...	https://www.gong.io	1/26/2022	-
	[redacted]	ee84e8ee-aac4-49e6-b4e1-03...	c6726c3a-9380-416d-a731-3f...	https://account.activedirectory...	6/10/2022	✓ Current
	[redacted]	f1c14dd1-4644-463e-9e88-dd...	de8bc8b5-d9f9-48b1-a8ad-b...	https://developer.microsoft.co...	3/22/2021	-
	[redacted]	f8393c89-f26d-4df2-8fc6-92d...	61af81de-bb87-45ae-94e0-b4...	https://account.activedirectory...	9/21/2022	✓ Current
	[redacted]	ffc9b3ac-de3a-4117-9171-4d...	f216e751-a6b5-4cc0-8bbf-bc...	https://account.activedirectory...	6/13/2022	✓ Current
	[redacted]	fffedac6-3ab3-485a-a0cf-725...	bc970288-62ec-45e2-953e-bf...	https://account.activedirectory...	3/3/2022	✓ Current

The company can view all its applications in its Entra ID console, including the applications they have bridged with Silverfort. The bridged applications are marked with the Silverfort logo.

Moving forward



In the years since Silverfort has been deployed, the company has continued to improve its security posture. From deploying MFA protection to more users, enhancing security controls and monitoring service accounts in real-time, to bridging more on-prem applications to Entra ID, the company was delighted with Silverfort's identity security platform. Since deployment, the company and Silverfort have also worked together to enhance the Silverfort offering. As part of its partnership with Silverfort, the company provides product feedback and participates in internal and customer workshops.

Implementing the right identity security controls involves careful planning, but as we've seen in this case study, the results will benefit all stakeholders. Although this project with Silverfort was initiated for compliance reasons, it quickly became clear that its objective was to solidify the identity aspects of its security posture. In addition to having established a robust set of security measures to mitigate any identity threats they may encounter, they also now have a solution that protects their entire user base, which allows them to be more efficient in their work.

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