SILVERFORT

CASE STUDY

STARCO Extends MFA Protection to All Users and Resources While Securing All Service Accounts

STARCO - a KENDA company

STARCO has been a pioneering force in the wheel and tire industry since 1961. STARCO's specialty is low- and high-volume standard and bespoke complete wheels for a wide range of applications in different market segments: Light Transportation; Industrial Vehicles; Utility and Ground Care Vehicles; Agricultural, Trailers & Caravans; Specialized Vehicles; and National Distributors.

STARCO is a part of the KENDA Group, which is one of the world's leading tire and tube, manufacturers with factories around the world and more than 11,000 employees globally.

BASED	**Aarhus, Denmark**
INDUSTRY	**Industrial Machinery Manufacturing**
EMPLOYEES	**Over 600**
ENVIRONMENT	**On-prem workstations and servers, legacy applications, privileged accounts**

The Challenge

- Lack of security controls to protect access to domain controllers via RDP
- Insufficient protection for access requests made by admin users
- Minimal visibility and protection of service accounts

The Results

- Deployed MFA protection across all users and resources in just a few hours
- All admin and privileged users protected with MFA policies
- Fully automated visibility and protection of service accounts

The Challenge

Admin Users and RDP Access Needed MFA Protection

As STARCO scaled its business operations globally, it needed to implement more security controls across its environments. Although Azure MFA was in place for email access, the company did not have the same security controls for their admin users and RDP access.

“If I wanted to gain access to my emails, I needed to verify my identity with MFA, but if I wanted access to our domain controllers via RDP, it’s one click and I am in. It was just too easy for admins to gain access to everything,” explained Fabian Jura, STARCO’s IT Infrastructure Manager.

Without the proper MFA protection across their admin users and core business applications, STARCO had a visibility gap across their manufacturing environment.

> “At the time, we didn’t have a concrete security structure in place to protect our privileged users and RDP access to our on-prem applications."

“This limited us from having the proper visibility into the access requests of each user. We didn’t have the insights or logs into where our users were connecting to and what resources they wanted access to,” Jura said.

Visibility Into Service Accounts

In addition to their need to add MFA protection across their workforce and environments, STARCO was seeking a solution that would help them to gain better visibility into the behavior of their service accounts and also protect them.

“As we are a smaller IT team, we had limited resources that could be allocated to provide the proper attention to understanding the ins and outs of each service account. We needed to understand where this service account was configured and what task is it running. Additionally, we wanted an automated process that would help us protect these accounts from any potential security risks,” said Jura.

Understanding the security risks of identity-based attack methods that are commonly used when targeting admin users and RDP access, STARCO searched for an identity protection solution that would be the answer to their security needs. After reading about Silverfort in a German IT security publication focused on Active Directory security, STARCO investigated Silverfort’s capabilities, and after running a successful POC decided to deploy the Silverfort platform across their environments.

“We initially chose Silverfort for its MFA protection for admin users and RDP, and along the way, we’ve found its service account discovery and protection capabilities extremely useful for our organization.”

> "Additionally, we decided to go with Silverfort as they empowered my team to mitigate any identity-based risk in our on-prem environment. Now we have the time to focus on each risk and solve it accurately without panicking."

“Their key security capabilities answered all challenges at the time, and we decided to deploy the Silverfort solution,” said Jura.

The Solution

Quick Deployment Leading to Secure Admin User and RDP Access

After deciding to adopt Silverfort, quick and efficient deployment was a key factor for STARCO, and they were pleased with how quickly it took to deploy Silverfort into their production environments.

> “It’s amazing how simple it was to implement Silverfort – it took only a few hours. We brought up the virtual machines, and after three or four configuration steps we were fully deployed with Silverfort.”

“The user interface is easy to use and we did not need much training. If you have an IT background, it’s really easy to get into it.” remarked Jura.

After the deployment phase, STARCO was able to achieve visibility across all their admin users’ access requests to all core resources. “Currently, we have 10 highly privileged admin user accounts that are being protected with Silverfort’s MFA. By protecting our admin users who have access to our domain controllers and sensitive resources, Silverfort is helping us to protect our entire environment, including our entire workforce, from incoming identity-based attacks,” said Jura.

Additionally, Silverfort is helping STARCO to protect all its core resources. “We are currently securing over 50 servers with RDP access, which is protected with MFA provided by Silverfort. Silverfort is not only providing MFA protection, they are also giving us actionable insights about threat detection into each authentication request. Additionally, we are protecting our NAS system, where we have some confidential data with LDAP authentication protocols which we are using Silverfort to protect. Securing all our core business resources wouldn’t be possible without Silverfort and, more importantly, we have saved time and had more confidence knowing that our admin users’ access to core resources is secure,” Jura added.

Complete Service Account Protection

When initially seeking out Silverfort, STARCO was looking to protect their RDP access, and once they learned more about the Silverfort platform, they understood Silverfort’s service account capabilities were needed. “Once we saw the functionality of Silverfort’s service account protection, we understood this was a feature we needed as we have 50 service accounts, including a several that are domain admins. We can’t make any changes to them, as we have restricted resources, and doing it manually would’ve taken too much time to find out whether some of these credentials were hardcoded somewhere.”

Since implementing Silverfort’s service account capabilities, STARCO has full confidence in knowing that its service accounts are being continuously monitored and protected.

> “We are protecting 50 service accounts, and Silverfort enables us to limit the source and destination of each service account. Even if the service account has privileged access, we are restricting these machines to running their daily tasks and nothing else.

“Overall, it has been extremely valuable for our overall security strategy to have complete visibility into all our service accounts and how they are configured, especially in our case where we create these accounts for third-party vendors and external staff,” Jura said.

All Rights Reserved © Silverfort 2024