Silverfort | protea networks

CASE STUDY

Meeting TISAX compliance: How ASAP Holding secured legacy file access and service accounts

BASED
Gaimersheim, Germany

INDUSTRY
Automotive

USERS
1,600

ENVIRONMENT
Active Directory
Entra ID, Microsoft Authenticator
Legacy applications (SQL, SSH, CIFS)

ASAP Part of HCLTech

ASAP Holding GmbH is a German engineering service provider that delivers engineering and technology solutions to major car manufacturers across Europe. As a TISAX- and ISO-certified organization, ASAP Holding supports its clients with high-compliance design, development, and production services, operating at the forefront of secure automotive innovation.

THE CHALLENGE:

Comply with TISAX requirements across legacy systems and service accounts

- Enforce access controls and MFA protection to meet TISAX 6.0 and ISO 27001 mandates
- Replace legacy MFA tools and secure access to legacy file servers, homegrown apps, and critical authentication protocols
- Discover and protect unmanaged service account activity across on-prem AD

THE SOLUTION:

Quick deployment and strong access controls led to compliance

- Complied with TISAX 6.0 and ISO 27001 mandates to enforce strict controls on AD
- Enforced MFA protection on legacy on-prem systems, including RDP, Domain Admin access, and sensitive file data
- Gained visibility and protected service accounts, including shadow IT and misused user accounts

The challenge: Meet strict automotive compliance standards by securing legacy infrastructure and service accounts

ASAP Holding operates in a highly regulated automotive vertical, where identity security is critical to maintaining trusted partnerships with global manufacturers. They have a hybrid IT environment, with approximately 95% of workloads on-prem, including file shares, domain controllers, and legacy systems that support critical operations.

As part of compliance mandates under TISAX 6.0 and ISO 27001, ASAP needed to enforce strict access controls on sensitive file data and gain full visibility into who could access what and how.

> "We used to rely on a legacy file encryption and MFA tool with physical tokens to protect our file shares. But after we migrated our domains, the setup became fragile and complex to maintain. It no longer scaled with our environment or operational needs."
>
> Sven Nosse, Head of IT and Information Security at ASAP Holding

With the domains migration and hybrid environment scaling up, ASAP Holding noticed growing service account activity that became hard to manage. While maintaining strict naming conventions, they discovered that some user accounts were being misused as shadow service accounts, adding risk to their compliance posture.

As part of compliance mandates under TISAX 6.0 and ISO 27001, ASAP needed to enforce strict access controls on sensitive file data and gain full visibility into who could access what and how.

Finding the right identity security platform

ASAP Holding began its search with a clear objective: find a solution that could deliver fast protection for their on-prem systems, including security for legacy authentication protocols like CIFS, RDP and SSH.

ASAP Holding was introduced to Silverfort by their long-time IT security partner Protea Networks. Hannes Kuffner, Managing Director of Protea Networks, recommended the platform as a lightweight alternative to traditional identity security tools.

> "We looked at traditional PAM tools, but they were too heavy to deploy. We needed something that gave us control fast. Once we saw Silverfort's demo presented by Protea, it fulfilled my expectations straight out of the box. It was exactly the kind of simple, effective solution we needed to meet the new certification requirements."
>
> Sven Nosse, Head of IT and Information Security at ASAP Holding

The solution: Rapid deployment and real-time enforcement across legacy systems

Following internal approval, the ASAP Holding team began rolling out Silverfort across their hybrid environment. Within one week, they were fully deployed in production, securing access to legacy servers, RDP, SSH, and homegrown applications without rewriting code or disrupting operations. As part of compliance mandates under TISAX 6.0 and ISO 27001, ASAP needed to enforce strict access controls on sensitive file data and gain full visibility into who could access what and how.

> "It was a walk in the park. We set up servers, installed the engines and were up and running in a week. The documentation was solid, and we barely needed help."
>
> Sven Nosse, Head of IT and Information Security at ASAP Holding

The team focused first on enforcing MFA protection for high-risk access paths, applying policies to legacy systems and critical infrastructure. With Silverfort's Authentication Firewall, ASAP Holding blocked unauthorized access attempts and met the technical controls outlined in both TISAX and ISO 27001.

"Silverfort acts like an Active Directory Authentication Firewall. It secures everything that talks to the domain controller with MFA, group access policies, or deny rules. That's how we locked down SSH, file shares, and more," said Nosse

Extending visibility and control over service accounts

From there, ASAP Holding shifted their focus to protecting their service accounts. Although the team had strong naming conventions in place, Silverfort uncovered 244 accounts behaving like service accounts, including several standard user accounts being misused in automated processes. With this complete visibility, ASAP Holding built behavioural baselines and fenced access where appropriate.

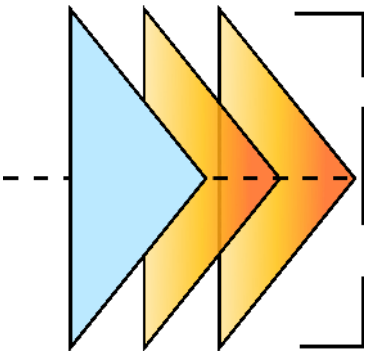
> "Silverfort gave us transparency. We could clearly see which accounts were acting as shadow IT and either restrict or replace them properly."
>
> Sven Nosse, Head of IT and Information Security at ASAP Holding

To complete the deployment, ASAP Holding integrated Silverfort with their Splunk SIEM solution, so identity-based events, including blocked authentications, legacy protocol use, and privilege changes, flowed directly into their detection and response workflows for faster remediation and higher confidence.

Looking ahead: Building long-term identity control with zero complexity

ASAP Holding now treats Silverfort as a core part of their identity security architecture, especially in place of a traditional PAM tool.

> "We were asked to implement a PAM tool for securing network devices, but we pushed back. We didn't need to record everything, just prove who was accessing what. Silverfort already gave us that."
>
> Sven Nosse, Head of IT and Information Security at ASAP Holding



The team also extended MFA protection to SSH-based infrastructure. Silverfort now protects not just user access, but machine-level authentications tied to production systems.

Looking ahead, ASAP Holding plans to continue evolving its identity strategy as more workloads shift to the cloud. For now, their focus remains on maintaining strong coverage across on-prem, resources, and preserving full control over how data is processed - a key requirement in the European automotive sector.

"One of Silverfort's biggest strengths is that everything is processed on-prem. No data leaves our environment. That's critical for us, and we appreciate how the platform is designed with that in mind," said Nosse.

About Silverfort

Silverfort secures every dimension of identity. We are the first to deliver an end-to-end identity security platform that is easy to deploy and won't disrupt business operations, resulting in better security outcomes with less work. Discover every identity across every environment, analyze exposures to reduce your attack surfaces, and enforce security controls inline to stop lateral movement, ransomware, and other identity threats.

About Protea

Protea Networks was founded in Munich in 2004. Today, Protea stand for top-tier IT security services and tailor-made security solutions – built on more than 20 years of deep industry expertise, technical excellence, and a strong network of cutting-edge technology partners, such as **Silverfort**, where Protea is proud to be a **Platinum Partner**.