Silverfort | JARVISS When Your OT & IT Security Get Personal

CASE STUDY

Securing Belgium's rail freight operations: How Lineas gained control over AD and service account risks

BASED	INDUSTRY	USERS	ENVIRONMENT
Brussels, Belgium	Transportation	1,000+ employees	Active Directory Entra ID, Okta Homegrown legacy applications for railways operations

LINEAS

Lineas is the largest private rail freight operator in Europe. Headquartered in Belgium, the company provides premium rail logistics services across the continent, helping customers shift freight from road to rail and reduce their carbon footprint. As a core player in Europe's supply chain, Lineas plays a vital role in supporting sustainable, uninterrupted freight movement across key industrial corridors.

THE CHALLENGE:

Restricting access and gaining control over AD to prevent operational disruption

- Limited ability to enforce a second layer of risk-based MFA protection for privileged access, including RDP
- Lacked visibility into service account activity and potential misuse across AD
- Couldn't monitor or control AD authentication activity across legacy systems

THE SOLUTION:

Improved privileged access security and reduced service account exposure

- Enforced MFA protection on RDP access and cleaned up excessive privileged access paths
- Identified over 60% of inactive service accounts and began cleanup efforts
- Reduced failed login attempts and lowered domain controllers' overload

The challenge: Limited MFA options and hidden service account risks increased ransomware exposure

As Belgium's primary rail freight operator, Lineas plays a vital role in the country's transportation system. As a designated critical infrastructure provider, even a brief operation disruption could create collapse across national logistics. From day one, the cybersecurity strategy at Lineas prioritized operational continuity, making identity security a top concern.

While Lineas had a mature security stack in place, including SIEM and SOC solutions, the team lacked real-time visibility into AD authentications and couldn't enforce controls beyond the perimeter.

> "We had a good SIEM but still lacked the ability to interfere with AD authentication traffic. That's the capability we needed. You can collect logs all day, but if you can't act on them in real-time, especially for internal traffic, you're missing a critical layer of defense."
>
> Christophe Rome,
> Cybersecurity Strategy Lead at Lineas

Two priorities emerged: enforcing a second layer of risk-based MFA protection for privileged access, including RDP, and restricting the access of service accounts to only the systems they needed access to. With high dependency on homegrown rail software and legacy authentication protocols, Lineas faced added complexity in implementing effective privileged access security controls.

Finding the right privileged access security platform

Lineas had been aware of its identity security gaps for some time. They knew they needed a solution that could secure privileged access and offer visibility and control over service account activity, without introducing unnecessary complexity.

To validate the solution fit internally, Lineas launched a POC with support from Jarviss, their trusted integration partner. The POC clearly demonstrated Silverfort's effectiveness in both key use cases: protecting privileged access and gaining end-to-end visibility into service account activity.

> "I've known about Silverfort for quite a while. It solves a very specific problem with a unique capability. There's nothing else I know of that can intercept AD authentication traffic the way Silverfort does."
>
> Christophe Rome,
> Cybersecurity Strategy Lead at Lineas

"This isn't a tool you install at the beginning of your journey. It fits when you've already reached a certain level of identity maturity. That's why we waited for the right moment – and the right budget. The POC helped us sell the value internally. Jarviss supported us every step of the way, and the rollout went smoothly," said Cristophe.

The solution: Enforcing MFA for privileged access and reducing internal exposure

After a successful POC, Lineas moved quickly to deploy Silverfort across its hybrid environment. The team focused first on enforcing MFA protection for privileged access within the internal network, applying risk-based policies to RDP connections and other high-risk access paths.

"For us, any kind of RDP access is privileged. If someone connects to a server, they now get hit with MFA — no exception. Once we enforced that, we started looking at RDP usage more broadly and realized we had a lot of existing accesses that needed to be cleaned up. That was a great side effect of the project," said Christophe

MFA protection enforcement also triggered a broader access hygiene initiative for Lineas. As Silverfort provided authentication patterns across the entire hybrid environment, the team discovered excessive access rights and repeated failed authentications, prompting a comprehensive clean-up.

> "Installing Silverfort made us reevaluate everything – accesses we didn't know existed, failed logins, over-permissioned accounts. We started tidying it all up. The visibility helped us to reduce authentication traffic as a whole, which in turn eased the load on our domain controllers. That wasn't part of the original goal, but it was a very welcome result."
>
> Christophe Rome,
> Cybersecurity Strategy Lead at Lineas

Extending visibility and control over service accounts

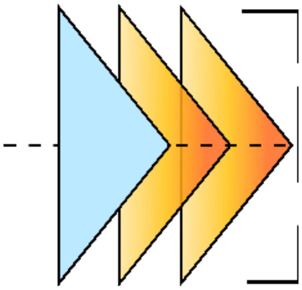
With privileged access enforcement in place, Lineas turned its attention to AD service accounts. While the team had long suspected some account sprawl, Silverfort provided the visibility into just how widespread the issue was.

Instead of immediately setting baseline behavior for service accounts, Lineas prioritized human accountability. They worked to assign ownership, map access needs, and understand each account's true role, especially those tied to legacy applications or used during year-end or recovery processes.

> "With Silverfort we found more than 60% of our service accounts to be inactive. That gave us the insights we needed to start a proper clean-up, focused on ownership, least privilege, and long-term hygiene.."
>
> Christophe Rome,
> Cybersecurity Strategy Lead at Lineas

"We've started identifying owners, understanding how accounts are used, and applying least privilege again. It's a difficult process, but one that Silverfort made possible. You can't just baseline activity and assume it's safe. Some accounts only run once a year. You need ownership first. That's what we're building now," said Christophe

Looking ahead: Building long-term identity access management with visibility and ownership



With Silverfort now fully integrated into its identity strategy, Lineas continues to evolve its approach to securing privileged access and service accounts. The next phase of the project focused on refining AD protections even further – beyond authentication enforcement.

"For me, Active Directory security is number one on the list in terms of risk reduction. Silverfort helped us take the next step, but there's still more we want to do – especially around misconfigurations and attack path visibility," – said Christophe

Lineas is working to ensure account ownership becomes a consistent practice across teams, and that policy enforcement is supported by clear accountability and refined procedures. This effort is already improving operational hygiene while reducing the risk of misuse or misconfiguration.

> "Silverfort gave us the visibility and control we were missing. It's what allowed us to finally align our tooling with ownership and processes – and that's where the real progress happened."
>
> Christophe Rome,
> Cybersecurity Strategy Lead at Lineas

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 Jarviss

Jarviss an integrator and managed security service provider, delivering expert solutions in cybersecurity and data networking. Founded in 2020, we operate across two countries and three locations, with a dedicated team of 30+ specialists. We focus on select, proven technologies to safeguard our customers' operations, ensuring security, resilience, and business continuity all with a personal approach.