Logistics leader Simon Hegele secures mobile endpoints and establishes GDPR compliance on mobile

Customer Profile

German-based logistics leader Simon Hegele offers international procurement, production, and packaging solutions, as well as spare parts logistics and supply chain security management in the retail, healthcare, and IT/communication industries.

Industry: Logistics

Mobility Policy: COPE

EMM solution: MobileIron

The Solution: Lookout Mobile Endpoint Security

The Results: Conform to GDPR requirements, riskless use of company data

The Challenge

Global logistics service provider Simon Hegele has come a long way since its inception in 1920. Founded on the backs of two horses and a car, the former furniture transportation company has grown into a worldwide leader offering highly specialized value-added services tailored to its customer processes. With 2500 employees spread across 49 locations around the world, the organization itself has its own unique challenges—including how to keep its mobile workforce and enterprise data protected and compliant.

Facing new GDPR compliance regulations, increasing mobile-based risks, and the complexities of supporting a corporate-owned mobility policy, company leaders sought an all-inclusive mobile security solution.

Security Challenges

- Achieve real-time protection and support for mobile endpoints across an Android and iOS environment
- Protect enterprise data from compromised mobile endpoints
- Comply with new General Data Protection Regulation (GDPR) regulations

Simon Hegele credits its success over the past 90 years to the commitment, dedication, and passion of its employees. A solution with restrictive policies or time-consuming and complex requirements was not acceptable. “Our trusted partner, anyplace IT GmbH, recommended Lookout as the answer we needed to solve our growing mobile security needs while seamlessly integrating with our existing MobileIron EMM platform and not putting additional demands on our employees,” explains Christian Jösch, Network Administrator at Simon Hegele.

The Solution

To address its mobile security needs, the company chose Lookout Mobile Endpoint Security. The approach to deployment was to use the MobileIron EMM platform to push the Lookout for Work app to employees' mobile devices. "The deployment went very smoothly," shares Jösch. "Now all devices within our mobile fleet are protected against threats and risks, such as Man-in-the-Middle attacks, sideloaded apps, and malware."

With Lookout mobile endpoint security, employees can now securely connect to corporate resources from any location around the world. Moreover, with access to customizable privacy control features, complying with GDPR user data handling requirements becomes a simple and intuitive process.

"Securing mobile endpoints is definitely a priority for us. We see Lookout as a critical layer of protection, both to prevent compromise of our corporate data, and to maintain compliance with all privacy laws," said Jösch.

Solution Criteria

- Must be able to protect Android and iOS devices from network- and app-based threats, including malware and riskware
- Must allow the company's global workforce to connect securely to its corporate network
- Must integrate seamlessly with MobileIron, the organization's EMM platform, and be easy for employees to use
- Must offer real-time device scanning to protect the security and privacy of employees as well as corporate data

The Results

Immediately upon deployment, Lookout Mobile Endpoint Security delivered some unexpected results. "We were surprised," explains Jösch, "by the amount of threats, including riskware and man-in-the-middle attacks, detected on our employees' devices that also included corporate data. With real-time scanning and the benefit of the unique Lookout mobile dataset, we've remediated these threats and now have the complete visibility into new threats we were seeking."

Importantly, the company has gained the ability to comply with new, more stringent privacy regulations. While many organizations have been preparing traditional endpoints to conform to GDPR requirements, mobility presents unique and complex security challenges. Because today's employees have the ability to choose devices, apps, and networks from which they access corporate data and applications, the spectrum of mobile risk increases significantly. With Lookout Mobile Endpoint Security, Simon Hegele is able to definitively guard against data compromise due to malicious attacks and non-malicious data leakage, as well as extend its mobile security controls to protect personal data.

As a result of the collaboration, the company achieved all of its mobile security and compliance goals. With integrated mobile endpoint security, built-in and customizable GDPR compliance features, and real-time device scanning of new apps and app versions, the company is equipped to confidently continue its historic growth by providing world-class service and solutions to its customers.

> "The deployment went very smoothly... Now all devices within our mobile fleet are protected against threats and risks, such as Man-in-the-Middle attacks, sideloaded apps, and malware."
>
> **Christian Jösch,**
> Network Administrator
> Simon Hegele