Liebherr Iberica Case Study

CASE STUDY | Industrial Machinery

PROFILE

Industry

Industrial Machinery

The Challenge

Managing insider threats and closely monitoring employee activity related to data transfers, while meeting compliance requirements of data protection regulations such as the GDPR.

The Solution

Endpoint Protector

Why Endpoint Protector?

Liebherr Iberica has chosen Endpoint Protector because the solution is easy to deploy and user-friendly, and it adapts to their national data protection regulations.

About Liebherr Iberica

Liebherr Ibérica, S.L. is the subsidiary of the Liebherr Group responsible for both the marketing and after-sales service in Spain of mobile cranes, port cranes, crawler cranes, earthmoving and mining machines, as well as concrete mixers produced by Liebherr.

Based in Azuqueca de Henares and Chiloeches, both near Madrid, the company distributes new and used machines in close cooperation with the production plants. It is also responsible for customer service and the supply of spare parts in Spain and Portugal.

The Challenge

Liebherr Iberica needed a product that helps to manage insider threats and close monitoring of employee activity related to data transfers.

With previously registered data losses, they were also searching for a DLP solution as an additional layer for data security.

Another important aspect for the company was meeting the compliance requirements of data protection regulations such as the GDPR.

"We had a good experience with Endpoint Protector because it suited our needs. We consider that the Device Control module is very useful because we can have a remote control for external devices which is very important to us."

Mr. Victor Delgado,
IT

About Endpoint Protector

Endpoint Protector is an enterprise-grade DLP software for Windows, macOS, and Linux computers, Thin Clients, and Desktop-as-a-Service (DaaS) solutions. It is an ideal choice for companies running on multi-OS networks, and the solution's modular format allows them to mix and match the right tools to serve specific needs. The solution puts an end to data loss, data theft, and data leaks by monitoring and blocking all data transfers to cloud-based services and applications such as web browsers, email, or Skype. It also monitors the use of portable storage media such as USB sticks, memory cards on endpoints running Windows, macOS, and Linux operating systems. Strong security policies prevent data from leaving the company unlawfully or accidentally.

The Solution

Liebherr Iberica is using our Device Control module.
Endpoint Protector's Device Control module allows the company to monitor and control USB and peripheral ports, thus preventing unauthorized data transfers and the use of unauthorized devices.

"The most required features for our organization were managing insider threats by close monitoring of employee activity related to data transfers. It's very easy to use and deploy, and it helps us to be compliant with our internal regulation." , said Mr. Victor Delgado.

For the company, it is very important to have a remote control for external devices. The functionality they most use is the Offline Temporary Password (OTP), which grants access rights for a limited time. OTPs can lift all restrictions for specific devices, users, or computers and can be used even remotely or when a computer is not connected to a network.

Endpoint Protector comes equipped with features that allow you to change the Master Password because this password should only be used very exceptionally and on urgent occasions. Every time this password is used, the IT department changes it to not allow users to use it continually. After changing the Master Password, if they share it with the team leaders and they decide if the share with employees who are working after hours and with those who are traveling outside of Spain. Generally, employees who work outside the business hours are in South America and due to the time difference, need to have this control over the devices used by the employees of this region.

Liebherr Iberica created a specific allowed device for each user, within the Device Control module, using the functionality that allows creating specific devices to use. They offer to each mechanic engineer a specific USB and register that device in Endpoint Protector, in order to offer permission only for those specific devices.

Liebherr Iberica rated Endpoint Protector's features, granularity as good, support and updates, ease of installation, and staff availability when calling or asking for assistance as very good.

	Endpoint Protector GmbH	CoSoSys Ltd.	CoSoSys USA
E-Mail	info@endpointprotector.de	sales@cososys.com	sales.us@cososys.com
Tel	+49 7541 978 26730	+40 264 593 110	+1-888-271-9349
Fax	+49 7541 978 26279	+40 264 593 113	