



Estudio de caso de Liebherr Ibérica

CASE STUDY | Maquinaria Industrial

PERFIL

Industria

Maquinaria Industrial

El reto

El manejo de amenazas internas y el monitoreo cercano de la actividad de los empleados relacionada con la transferencia de datos y al mismo tiempo cumplir con los requerimientos de las regulaciones de protección de datos como GDPR.

La solución

Endpoint Protector

¿Por qué Endpoint Protector?

Liebherr Ibérica eligió Endpoint Protector porque la solución es fácil de implementar y fácil de usar y se adapta a sus regulaciones de protección de datos nacionales.

Sobre Liebherr Ibérica

Liebherr Ibérica, S.L. es la filial del Grupo Liebherr responsable tanto de la comercialización como del servicio postventa en España de grúas móviles, grúas portuarias, grúas sobre orugas, máquinas para movimiento de tierras y minería, así como hormigoneras fabricadas por Liebherr.

Con sede en Azuqueca de Henares y Chiloeches, ambas cerca de Madrid, la empresa distribuye máquinas nuevas y usadas en estrecha colaboración con las plantas de producción. También es responsable del servicio al cliente y del suministro de repuestos en España y Portugal.

El reto

Liebherr Ibérica necesitó un producto que los ayudara a manejar las amenazas internas y tener un monitoreo cercano de la actividad de los empleados relacionada con la transferencia de datos.

Con pérdidas de datos previamente registradas, también estaban en búsqueda de una solución de DLP como una capa adicional para la seguridad de datos.

Otro aspecto importante para la empresa fue el cumplimiento de los requerimientos de las regulaciones de protección de datos como GDPR.

„Hemos tenido una buena experiencia con Endpoint Protector porque se adaptó a nuestras necesidades. Consideramos que el módulo de Control de Dispositivos es muy útil porque podemos tener un control remoto de los dispositivos externos, lo que es muy importante para nosotros.”

Mr. Víctor Delgado,
IT

Sobre Endpoint Protector

Endpoint Protector es un software de DLP de nivel empresarial para equipos Windows, macOS y Linux, Thin Clients y soluciones de Desktop-as-a-Service (DaaS). La solución es una opción ideal para las empresas que operan con redes multiplataformas y tiene un formato modular que permite mezclar y combinar las herramientas adecuadas para satisfacer necesidades específicas. La solución pone fin a la pérdida de datos, al robo de datos y a las fugas de datos al monitorear y bloquear todas las transferencias de datos a servicios y aplicaciones basados en la nube, como navegadores web, correos electrónicos o Skype. También supervisa el uso de medios de almacenamiento portátiles, como memorias USB, tarjetas de memoria en terminales que ejecutan sistemas operativos Windows, macOS y Linux. Las sólidas políticas de seguridad evitan que los datos salgan de la empresa de manera ilegal o accidental.

La solución

Liebherr Ibérica está utilizando nuestro módulo de Control de Dispositivos. Este módulo de Endpoint Protector permite a la empresa a monitorear y controlar los dispositivos USB y puertos periféricos, evitando así transferencias de datos no autorizadas y el uso de datos no autorizados.

“Las funcionalidades más requeridas por nuestra organización fueron las que permitían manejar las amenazas internas mediante el seguimiento de cerca de la actividad de los empleados relacionada con la transferencia de datos. Es muy fácil de usar e implementar y nos ayuda a cumplir con nuestra normativa interna.”, mencionó Mr. Víctor Delgado.

Para la empresa, es muy importante disponer de un mando a distancia para los dispositivos externos. La funcionalidad que más utilizan es la Contraseña Temporal Offline (OTP), que otorga derechos de acceso por un tiempo limitado. Las OTP pueden eliminar todas las restricciones para dispositivos, usuarios o equipos específicos y se pueden usar incluso de forma remota o cuando un equipo no está conectado a una red.

Endpoint Protector viene equipado con características que permiten cambiar la Contraseña Maestra debido a que esta contraseña solo debe usarse de manera muy excepcional y en ocasiones de urgencia. Cada vez que se usa esta contraseña, el departamento de IT la cambia. Para no permitir que los usuarios la usen continuamente. Tras cambiar la Contraseña Maestra, la comparten con los jefes de equipo y estos deciden si la comparten con los empleados que están trabajando fuera de horario y con los que están viajando fuera de España. Por lo general, los empleados que trabajan fuera del horario laboral se encuentran en América del Sur y, debido a la diferencia horaria, necesitan tener este control sobre los dispositivos que utilizan los empleados de esta región.

Liebherr Ibérica creó un dispositivo permitido específico para cada usuario, dentro del módulo de Control de Dispositivos, utilizando la funcionalidad que permite crear dispositivos específicos para su uso. Ofrecen a cada ingeniero mecánico un USB específico y registran ese dispositivo en Endpoint Protector, con el fin de ofrecer permiso solo para esos dispositivos específicos.

Liebherr Ibérica calificó como buenas las características y la granularidad de Endpoint Protector y como muy buenas el soporte y las actualizaciones, la facilidad de instalación y la disponibilidad del personal al llamar o pedir ayuda.

Endpoint Protector GmbH

E-Mail info@endpointprotector.de
Tel +49 7541 978 26730
Fax +49 7541 978 26279

CoSoSys Ltd.

sales@cososys.com
+40 264 593 110
+40 264 593 113

CoSoSys USA

sales.us@cososys.com
+1-888-271-9349