For over 200 years, Hartmann has focused on “going further for health,” as their tagline proudly states. Headquartered in Germany, the company’s medical and hygiene products are available in over 100 countries and primarily serve three distinct practice areas: wound treatment, incontinence care, and infection prevention. Hartmann shares its intellectual property with business partners and protected health information (PHI) with patients. With either stakeholder, Hartmann must ensure this confidential information is held and shared securely.

Hartmann Guards Data and Proves Compliance with Extensive Controls

Hartmann was approached by a customer who, for GDPR compliance purposes, required some type of secure communications mechanism that encrypted invoices and other data in motion, at rest, and in use. Michael Williams, Hartmann’s Senior Manager for Cybersecurity Management, was unphased by the request. “As soon as I heard their requirements, I knew the only platform that conforms is Accellion.”

A previous experience with Accellion cemented Williams’s confidence. Prior to joining Hartmann, Williams conducted red team and penetration testing services. One of his clients had Accellion installed on a Windows system and, while he was able to get into Windows, he was unable to get through the Accellion content firewall or the data stored inside.

“I told our procurement office, ‘I know there are solutions in the marketplace that provide some encryption capabilities, but they’re missing a key requirement – encryption of data at rest. Accellion is literally the only company I know that protects data on all three layers – in motion, at rest, and in use.’”

Williams suspected there were other use cases. For example, he knew business partners within Hartmann shared sensitive data sets with contractors and other external specialists. The data must be made viewable in order to get work done, but it shouldn’t be downloadable. This distinction was important for protecting intellectual property and patient privacy, but also for demonstrating compliance with GDPR. Secondly, Hartmann is a global company and therefore has unique data sovereignty requirements. Some Accellion competitors only had data centers in the US or in countries where Hartmann didn’t operate. Because the Accellion content firewall lets customers define locations and assign servers and storage, data sovereignty requirements would be a non-issue.

Employees Increase Visibility by Integrating Security into Daily Workflows

Williams has noticed several benefits since deploying the Accellion platform on private cloud.

Business partners across Hartmann utilize the Accellion content firewall to share sensitive data internally and externally. If one of Hartmann’s customers treats a patient for a wound and wants a second opinion on proper treatment, he can securely upload images and notes to Hartmann product specialists. For one department, Williams

“Accellion is literally the only company that protects data on all three layers – in motion, at rest, and in use.”

Michael Williams
Senior Manager of Cybersecurity Management
The Accellion Kiteworks® content firewall prevents data breaches and compliance violations from sensitive 3rd party cyber communications. With Accellion, CIOs and CISOs gain complete visibility, compliance and control over IP, PII, PHI, and other sensitive content across all 3rd party communication channels, including email, file sharing, mobile, enterprise apps, web portals, SFTP, and automated inter-business workflows. Accellion has protected more than 25 million end users at more than 3,000 global corporations and government agencies, including NYC Health + Hospitals; KPMG; Kaiser Permanente; AVL; American Automobile Association (AAA); The Linde Group; Tyler Technologies; and the National Institute for Standards and Technology (NIST).

For more information please visit www.accellion.com or call (650) 485-4300. Follow Accellion on LinkedIn, Twitter, and Accellion’s Blog.

© 2021 Accellion USA LLC. All rights reserved.