

Hartmann Ensures GDPR Compliance by Protecting PHI While Enhancing Staff Efficiency

OVERVIEW



Customer: Hartmann
Industry: Healthcare
Location: Heidenheim, Germany

Kiteworks Capabilities Used:

- Email
- File Transfer
- Automated File Transfer
- File Sharing
- APIs
- Web Forms

Going Further for Health

For over 200 years, Hartmann has focused on “going further for health,” as its tagline proudly states. Headquartered in Germany, the company’s medical and hygiene products are available in over 100 countries with the company primarily serving 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.

“Kiteworks 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

Addressing Content-sharing Compliance Requirements

Hartmann was approached by a customer that required a secure communications mechanism for encrypting invoices and other data in motion, at rest, and in use. This is a requirement of the EU’s General Data Protection Regulation (GDPR). Michael Williams, Hartmann’s senior manager for Cybersecurity Management, was unfazed by the request: “As soon as I heard their requirements, I knew the only platform that conforms is Kiteworks.”

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

Tackling Different Use Cases

Williams knew there were other use cases. For example, he knew business partners within Hartmann shared sensitive datasets with contractors and other external third-party specialists. The data must be viewable, but it cannot be downloadable. This distinction is important for protecting intellectual property and patient privacy. It is also important for demonstrating compliance with GDPR.

Another use case related to the global nature of Hartmann’s business. Some Kiteworks competitors only have data centers in the United States or in countries where Hartmann does not operate. Because the Kiteworks platform allows customers to define locations and assign servers and storage, Hartmann can meet global data sovereignty requirements globally.

At the time, Hartmann was also in the midst of rebuilding its security program using the National Institute of Standards and Technology’s (NIST) Cybersecurity Framework (CSF). As a result, Williams knew that the Kiteworks deployment needed to comply with the NIST CSF framework.

Deploying Unified Content Security

Williams and his team purchased the Kiteworks platform on a private cloud. A private cloud deployment provides the customer the best of both worlds: flexibility, scalability, and cost efficiency on the one hand, and security and control on the other. The cloud provider provides the infrastructure and maintenance, yet the customer has full control of the data—namely, sole ownership of the encryption keys. As a result, the cloud provider does not have access to customer data.

Case Study

Hartmann Ensures GDPR Compliance by Protecting PHI While Enhancing Staff Efficiency

Williams and his team set up policies, standards, guidelines, and control mechanisms. Then, they created a security plan for every application to ensure total alignment with policies and procedures. In addition, they aligned Hartmann with international security and privacy requirements, including GDPR and the California Consumer Privacy Act (CCPA), among others. For one department, Williams leveraged Kiteworks application programming interfaces (APIs) to design email templates for specific use cases involving sensitive information.

For one business unit, Williams used Kiteworks APIs to design secure email templates. A business leader in another department installed the Kiteworks Salesforce plugin to protect customer content in Salesforce.

Realizing Tangible Benefits

Hartmann has experienced numerous benefits using the Kiteworks platform:

Secure File Sharing

Business partners across Hartmann now utilize the Kiteworks platform to share sensitive content internally and externally. If Hartmann's customers treat a patient for a wound and want a second opinion on proper treatment, they can securely upload images and notes to Hartmann product specialists.

Secure Emails

Thanks to the API-designed email templates that were created using the Kiteworks platform, one department now can rest assured that every email they send and receive is compliant with internal and external regulations.

Rapid Adoption

Williams is pleased with the adoption rate and notes it occurred organically or, as he puts it, "grown wings." When end-users discover just how good the platform is, they are more inclined to share the benefits with others. Naturally, word-of-mouth marketing is more effective than trying to force a new tool down people's throats. This organic growth led one business leader to promote Kiteworks over Microsoft SharePoint for enhanced security and visibility of all file activity.

Added Value

The business unit that uses the Kiteworks Salesforce plugin not only protects customer content, but also has realized a reduction in Salesforce spend. In another instance, a business manager now receives a daily report that details what information stored in a critical, frequently used application has been accessed, downloaded, or shared.

Looking to the Future

Based on the reception of the Kiteworks platform, Williams hopes to triple the number of Kiteworks users and eventually provide access to every Hartmann employee. "I would recommend Kiteworks to any CISO who is looking for something that helps with secure communications internally but especially between internal employees and external parties."

Needs

- Encrypt content in motion, at rest, and in use to comply with GDPR and NIST CSF
- Share content with third-party vendors and contractors in view-only format
- Ensure data sovereignty support to keep documents in specific jurisdictions

Kiteworks Solution

- Kiteworks for secure email, file sharing, and APIs, internally and externally
- Kiteworks API for designing secure email templates
- Kiteworks Salesforce Plugin to protect CRM content

Business Impact

- Comprehensive visibility into what, when, and by whom sensitive content is being shared
- Compliance with numerous data privacy requirements, including GDPR and NIST CSF
- Secure emails using API-generated templates
- Protection for customer data in Salesforce
- Reduced Salesforce budget
- Quick adoption by employees due to easy-to-use interface

"I would recommend Kiteworks to any CISO who is looking for something that helps with secure communications internally but especially between internal employees and external parties."

– Michael Williams, Senior Manager of Cybersecurity Management

Kiteworks

Copyright © 2021 Kiteworks. Kiteworks' mission is to empower organizations to effectively manage risk in every send, share, receive, and save of sensitive content. To this end, we created a platform that delivers content governance, compliance, and protection to customers. The platform unifies, tracks, controls, and secures sensitive content moving within, into, and out of their organization, significantly improving risk management and ensuring regulatory compliance on all sensitive content communications.