

Kiteworks

Kiteworks Private Data Network

Customer Storybook

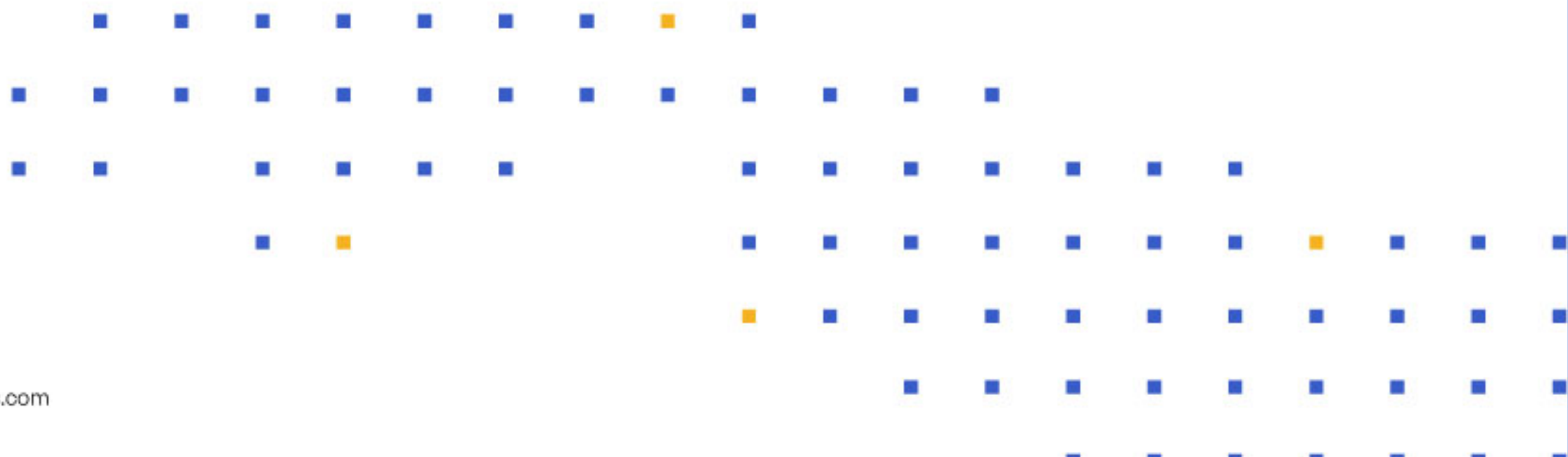




Zero Visibility. No Control. High Risk.

Every day, organizations risk data breaches and compliance violations when they share intellectual property (IP), personally identifiable information (PII), protected health information (PHI), and other sensitive data with customers, suppliers, and partners, using applications designed for expediency over security. But complex digital supply chains and IT infrastructure make it very difficult to protect these risky third-party communications from today's sophisticated, persistent threat actors that are patiently searching for your weakest link.

The Kiteworks platform helps organizations lock down the exchange of confidential enterprise information with digital supply chain partners by unifying security and compliance across siloed third-party communication channels, including email, file sharing, mobile, chat, web forms, managed file transfer, and Secure File Transfer Protocol (SFTP). Thousands of global chief information officers (CIOs), chief data officers, and chief information security officers (CISOs) trust the Kiteworks platform to provide their organizations with protection, privacy, and peace of mind.



How the Kiteworks Platform Works

01

CONSOLIDATE RISKY COMMUNICATIONS

Consolidate and Control Risky Third-party Communications

across email, file sharing, managed file transfer, web forms, and application programming interfaces (APIs) by routing each channel through the Kiteworks platform. Protect your sensitive data more simply, centrally, and uniformly with every channel you add. Save money while securing your business by eliminating legacy apps.

02

SEE SENSITIVE DATA COMING AND GOING

Monitor Sensitive Files Shared With Customers, Suppliers, and Partners

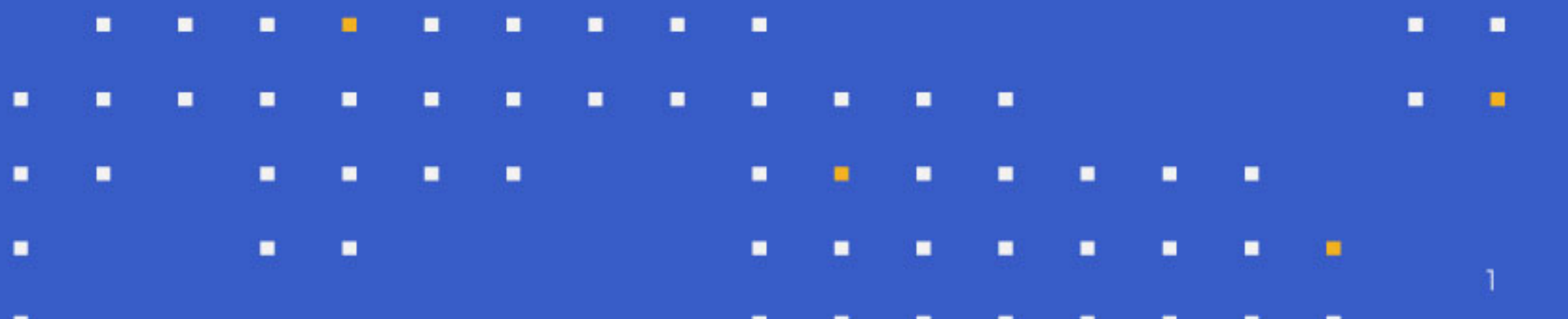
on the CISO Dashboard or on your SIEM. Get a full picture of what content is being shared, where it is going, who is accessing it, when it happens, and how it is done. The Kiteworks platform produces a single, normalized syslog that lays the foundation for threat detection, response, and forensics.

03

SIMPLIFY SECURITY AND COMPLIANCE

Protect Data With Uniform Security and Compliance

across communication channels. Define policies centrally for the Kiteworks platform to enforce as it inspects each transaction. Send each data exchange down a gauntlet of security, including SSO, MFA, AV, ATP, and DLP, with a single point of integration. Prove compliance with a detailed audit trail.



Hospital System Securely Onboards Acquired Clinics

Avoids HIPAA Violations During Complex, Risky Business Integrations

This billion-dollar U.S. hospital system had a growth strategy of acquiring new clinics. However, each acquisition put the business at serious risk of a HIPAA violation from a breach of protected health information (PHI). The company needed to maintain compliance while integrating newly acquired clinics—a complex endeavor involving the transfer of massive amounts of sensitive data. All the medical records on each clinic’s legacy system had to be transferred to the new corporate system. Everyday email, file sharing, and SFTP provided inadequate security and a poor audit trail, creating a serious business risk.

The Kiteworks platform ensured security and compliance, but it also saved money by improving user productivity, automating routine business processes, and eliminating legacy file sharing applications.

The customer uses Kiteworks file sharing for bulk data transfers from acquired clinics and for ad hoc data transfers with the clinic’s extended supply chain of healthcare providers. This enables a high-quality process to receive and track all incoming medical records, eliminating errors and allowing smooth business integration. The Kiteworks platform centralizes governance and control to ensure HIPAA compliance. Detailed audit logs allow the customer to prove compliance to industry regulators. To minimize the possibility of an expensive breach, the customer deployed the Kiteworks FedRAMP Authorized hosted option—the gold standard of cloud security. The customer also added DLP scanning to strengthen HIPAA compliance, and integrated Kiteworks syslogs to its security information and event management (SIEM) in its security operations center.

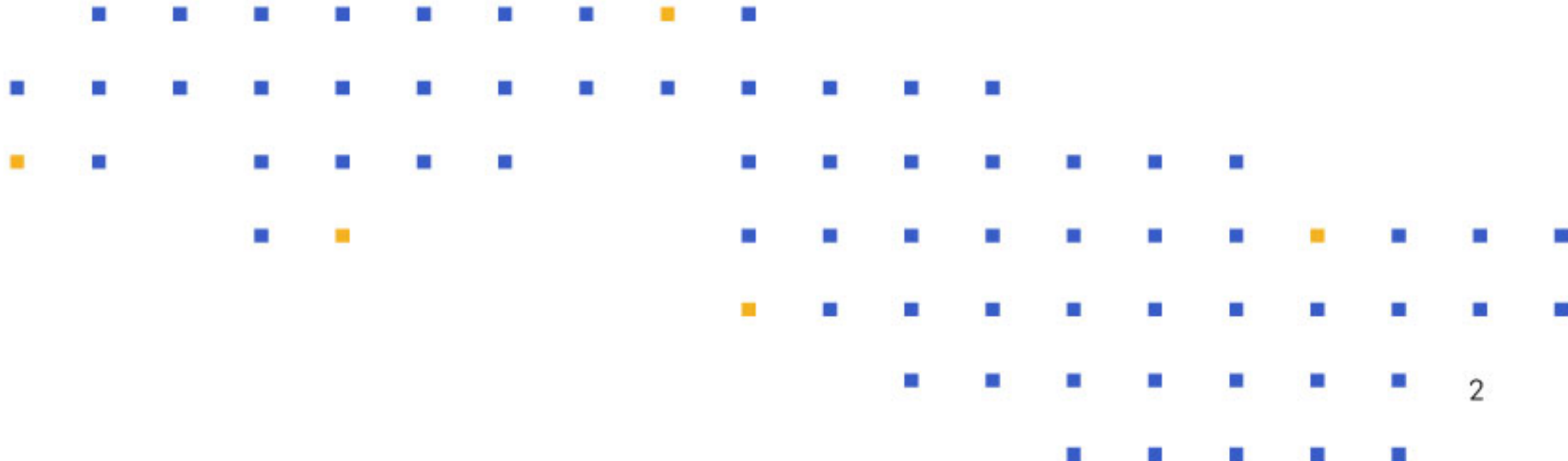


Canadian Law Enforcement Enables Work From Home

Officers Securely Share Evidence and Documents With Courts, Attorneys, and Citizenry

When COVID-19 forced Canadian law enforcement employees of this large provincial police department to work from home, couriers were suddenly required to transfer evidence and sensitive information via flash drives to courts and attorneys, undermining costs, productivity, and chains of custody. Police officers were not the only ones affected; other departments such as finance were impacted as well.

Using the Kiteworks platform, provincial police officers securely send documents and evidence, including audio files and terabyte-sized dashcam footage, to legal counsel and crown prosecutors during court proceedings. The Kiteworks platform provides a complete audit trail that proves which individuals viewed files and when files were downloaded. The finance department uses the Kiteworks platform to send and receive invoices, contracts, and other sensitive financial documents. And citizens can also report potential crimes by uploading videos and other evidence files over the internet. In order to meet strict Canadian data sovereignty regulations, the customer chose on-premise deployment.



European Bank Achieves GDPR Compliance While Reducing Costs

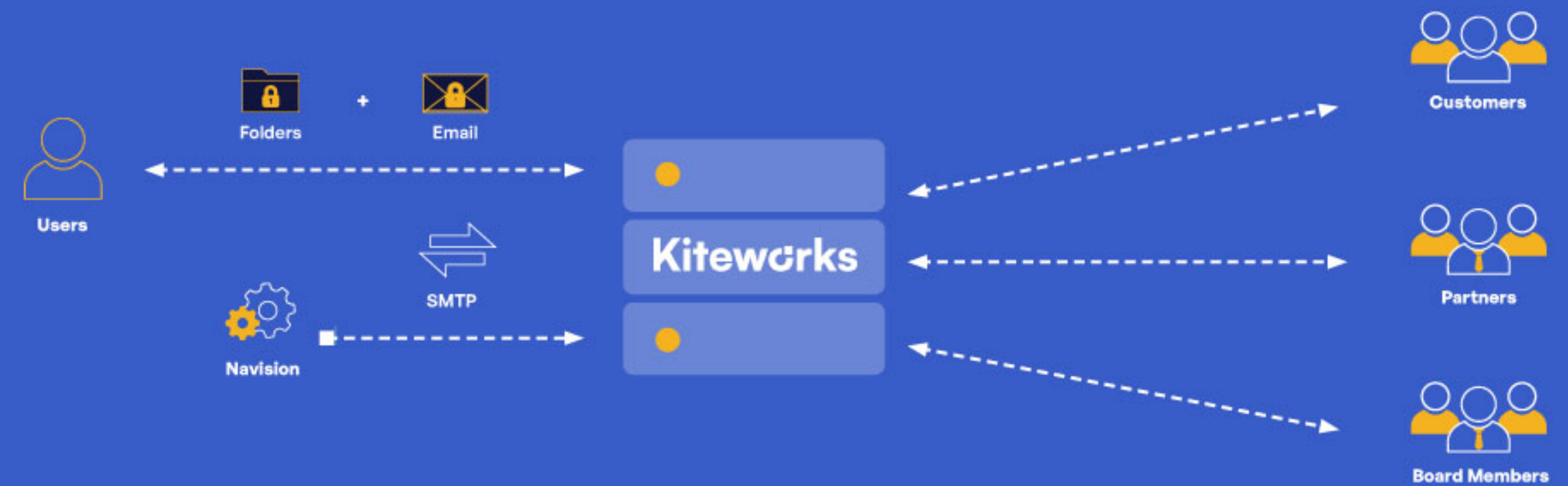
Sends and Receives Sensitive Data Via Email and File Sharing With Automation of Routine Business Processes

This European commercial bank needed GDPR-compliant email and file sharing applications to exchange financial, business, and private individual data with business customers, partners, and board members. The bank's employees and clients constantly complained about the poor usability of its secure file sharing software. This reduced productivity and morale, so the firm decided to look for alternative solutions.

The Kiteworks platform improved user productivity, but it also saved money by eliminating legacy file sharing applications and automating routine business processes. The Kiteworks platform allows users to exchange confidential contracts, negotiation documents, and legal files with clients directly from Microsoft Outlook or from the user-friendly web and mobile applications. They can also collaborate more intensely with Kiteworks secure shared folders.

In addition, Kiteworks SMTP relay automation provides the secure, compliant distribution of statements, invoices, and other sensitive documents sourced from the bank's Microsoft ERP system. The ERP system emails documents to the Kiteworks server using the SMTP protocol. The server then secures the attachments and sends a reformatted email to customers with a secure download link instead of attachments to ensure compliance regulations are met through security and governance controls, and a complete audit log.

A major European commercial bank achieves GDPR compliance while reducing costs by automating the secure distribution of financial documents to business customers.



Step 1

Users share files securely using email and shared folders.

Step 2

Microsoft Dynamics Navision® securely emails documents via SMTP automation.

Step 3

The Kiteworks platform automatically converts Navision email attachments to secure download links.

Step 4

Customers, partners, and board members send and receive sensitive documents securely over the internet.

Step 5

The Kiteworks platform produces a detailed audit trail.



International Governments Develop Joint Research and Policy

Member Nations Demand World-class Data Protection and Compliance

This nonprofit international organization performs research and develops policy standards for the 40 member countries that fund it. The data shared by member countries is highly confidential and often politically sensitive, so tight security is required. In addition, member countries are subject to the numerous and diverse compliance regulations enacted by their respective governments. Members objected to the everyday email and file shares used to send and receive sensitive data and interim research, because there was too much potential for information to leak or be stolen.

“The Kiteworks platform creates a consolidated syslog across all communication channels that integrates with the customer’s SIEM for threat detection, response, and forensics.”

The customer required the highest level of security and control over its data, so it selected an on-premise deployment of the Kiteworks platform for secure email and file sharing with the flexibility to add SFTP in the future. To ensure confidentiality for its member countries, the customer implemented multi-factor authentication with GDPR policy controls for all communications and performed extensive penetration testing during the evaluation. The Kiteworks platform creates a consolidated syslog across all communication channels that integrates with the customer’s SIEM for threat detection, response, and forensics.

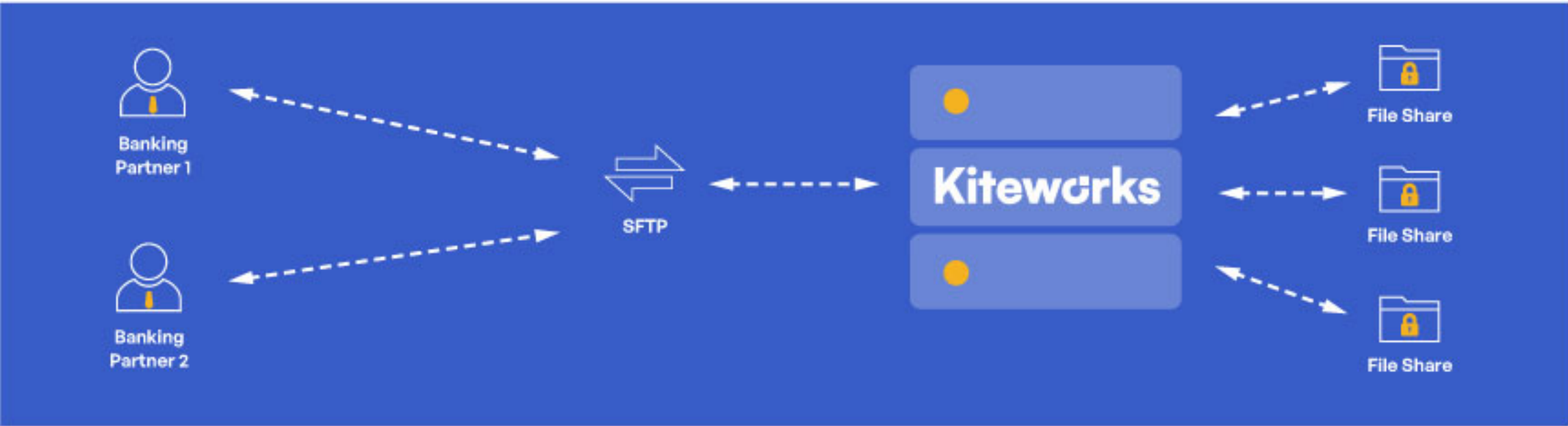
Card Services Firm Meets PCI Compliance While Increasing Profits

Automates Sensitive Data Transfers Between Banking Partners and Customer Service Operations

This credit card services company handles massive amounts of cardholder data, requiring a careful balance between security and efficiency. Subject to the payment card industry's data security standards (PCI DSS), it must demonstrate the higher level of compliance of designated entities (DESV), including implementing a PCI DSS compliance program, documenting and validating PCI DSS scope, incorporating PCI DSS into business-as-usual activities, controlling access to cardholder data, and responding to suspicious events—all while turning a profit. Bulk back-office transfers of cardholder data with banking partners posed a particularly difficult challenge, because this huge pipeline of sensitive data needed to be fed efficiently to the company's customer service and reconciliation teams.

The firm's security manager decided to start by implementing PCI DSS compliant email and file sharing for commercial and retail customers. To increase efficiency, the company implemented Kiteworks secure managed file transfer (MFT) to integrate back-office SFTP exchanges with partner banks by automatically distributing data to the file shares used by customer services operations. Preferring to deploy in a Kiteworks-hosted cloud, the company implemented a hybrid architecture, using Kiteworks Enterprise Connect servers to integrate securely to internal systems. The Kiteworks platform was the only consolidated SFTP-MFT solution that also offered the long-term file retention, detailed audit logs, alerts, and forensics required of PCI DSS designated entities.

A credit card services company achieves PCI DSS compliance for designated entities by automating bulk back-office transfers of cardholder data with banking partners using the Kiteworks platform.



Step 1
Partner users and systems upload financial files to SFTP.

Step 2
Kiteworks MFT automatically moves files from SFTP to correct on-premise file shares.

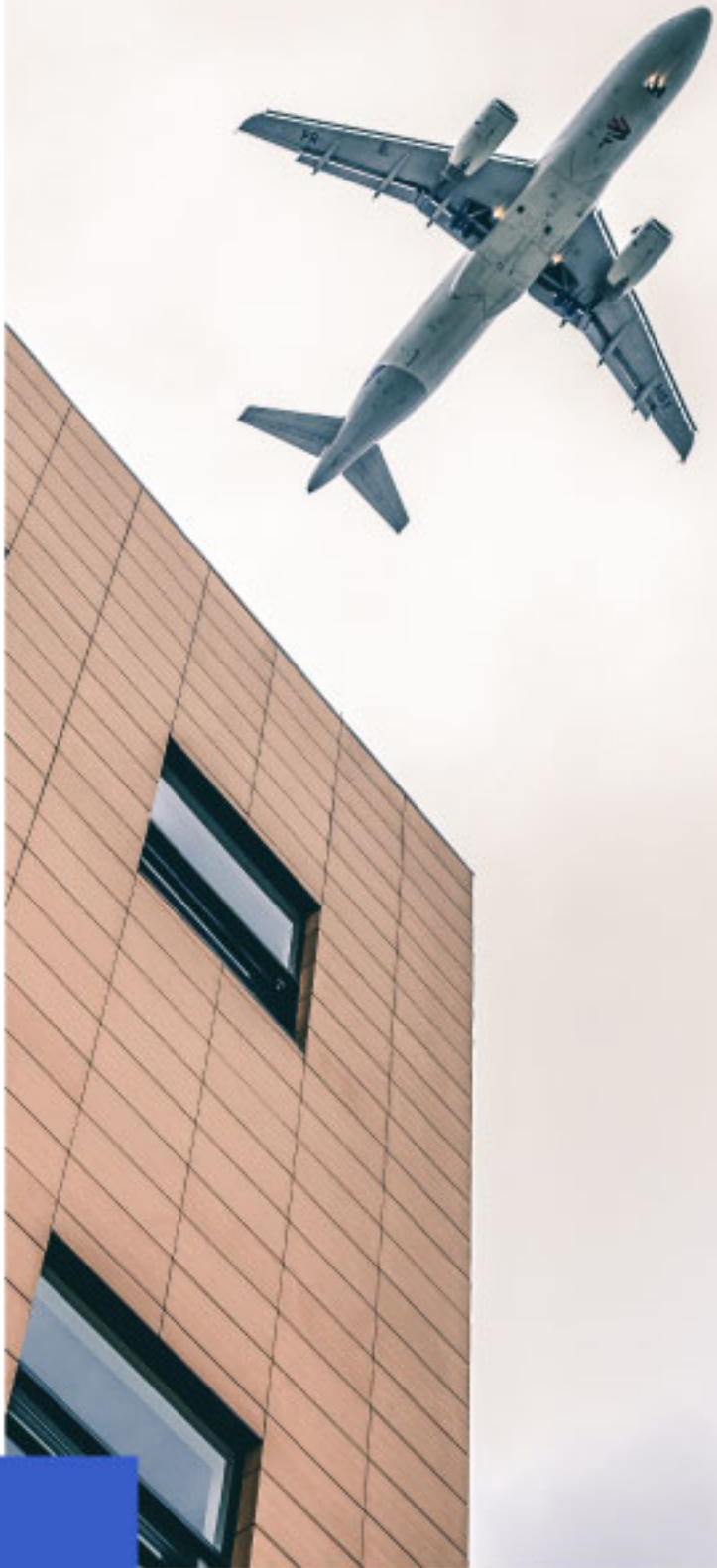
U.S. Flight Simulator Manufacturer Delivers Secure Software Updates

Complies With ITAR When Distributing Software Updates to International Clients

The International Traffic in Arms Regulations (ITAR) control the manufacture, sale, and distribution of defense and space-related products and services of U.S. companies. Besides military hardware, it also restricts the plans, diagrams, software, and other technical data used to build ITAR-controlled items. This U.S. flight simulation vendor needed ITAR compliance for software update exports to its customers outside the U.S.

To minimize the possibility of an expensive breach, the customer deployed the Kiteworks FedRAMP Authorized hosted option—the gold standard of cloud security.

The customer uses the Kiteworks platform to send very large software update files with a complete audit trail of uploads and downloads. Fulfillment employees use forms that inject additional parameters into the audit trail of the files they send, strengthening compliance and simplifying audit preparation. The company's customers enjoy a simple user experience, receiving an email link that enables them to authenticate and download the software updates. To ensure U.S. federal government approval, the customer chose a Kiteworks FedRAMP Authorized hosted deployment of the Kiteworks platform.



This major health insurer combines the Kiteworks secure managed file transfer and secure email to automate the HIPAA-compliant distribution of statements containing personal health information.



Step 1

The Kiteworks secure MFT client pulls health insurance reports from an insurance application and converts the .CSV format to a user-friendly PDF format.

Step 2

The Kiteworks platform securely emails the reports and maintains a complete audit trail.

Step 3

Patients and health care providers receive a simple email with a download link.

Major Health Insurer Distributes HIPAA Compliant Statements

Automation Streamlines Risky Handling of Sensitive Patient Health Information

This large insurer was already using the Kiteworks platform for secure ad hoc communications over email and file sharing, and was looking for the same level of visibility, security, and compliance over its back-office operations. In particular, the company needed to distribute large numbers of statements and reports on insurance payments to patients and healthcare providers—a complex process full of sensitive PHI subject to HIPAA regulations. The code-intensive, custom integration it had been using was out of compliance and difficult to maintain.



The Kiteworks platform maintains a detailed audit trail that includes the attributes of every file transfer to demonstrate compliance.

The company used the Kiteworks platform to automate the whole process with simple configuration settings—no coding required! The Kiteworks secure managed file transfer client (MFT client) automatically picks up CSV files produced by the company's insurance application and converts them to user-friendly PDFs for distribution. Then, the Kiteworks platform sends them out by secure email to patients and healthcare providers. Because Kiteworks consolidates security across communication channels, the customer was able to extend existing compliance policies and access controls for automatic enforcement. Plus, the consolidated Kiteworks syslog automatically provided a complete audit trail of secure MFT and email logs to demonstrate HIPAA compliance.



Pharmaceutical Firm Secures Manufacturing Quality Control

Automates Hand-offs Across Purdue Model Network Segments to Meet Good Practice Guidelines

The security team of this innovative pharmaceutical company mandated that manufacturing communications used to monitor, measure, and analyze production processes must be secure, audited, and in compliance with strict Good Practice guidelines (GxP). Because the firm's networks follow the five-layer Purdue segmentation model, isolating critical production equipment in the lowest level from everyday business activity in the highest level, the process of getting data from the manufacturing line up to production analysts and ultimately up to the executive management created a unique security challenge. Batch quality measurement log files must hop up each level, crossing multiple firewalls and gateways, constrained to the SFTP, whereas software updates must hop down each level to the zone containing the product to be updated.

To automate the process, the company deployed the Kiteworks secure managed file transfer client (MFT client) within each network zone of the Purdue model in each manufacturing plant. According to schedule, each MFT client hands off files to the next MFT client one level over to pass data securely between zones. The Kiteworks platform maintains a detailed audit trail that includes the attributes of every file transfer to demonstrate compliance.



The Kiteworks platform implements the five-layer Purdue Model that securely isolates manufacturing production from everyday business activities.

Enable GxP Compliant Manufacturing

- Protect process quality and data
- Segment network levels on Purdue Model
- Full audit trail required

Strictly Control File Transfers

- Move files level to level only
- Only MFT and SFTP allowed
- All files for software maintenance, workstations, industrial measurements, etc.

Kiteworks MFT Client

- Install one client per network zone (level)
- Workflows meet GxP requirements
- Transfers on schedule or trigger

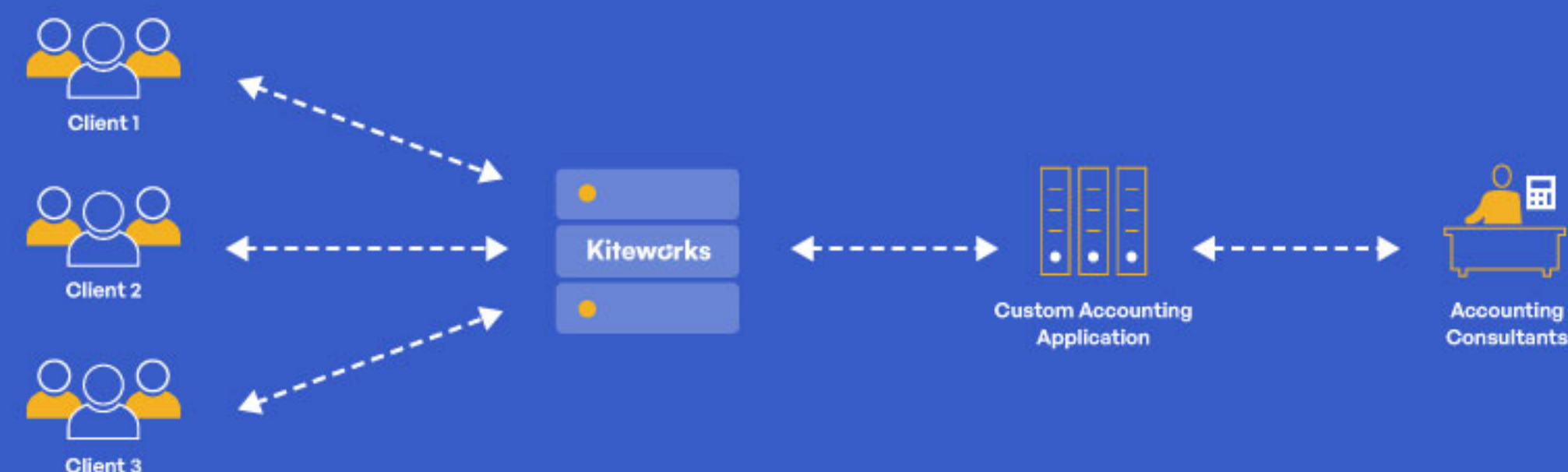
Accounting Firm Ensures Privacy Across Multiple Clients

GDPR Compliant Automation Isolates the Communication of Sensitive Financial Data

This leading professional services firm serves clients all over the world, but it must keep each client's data confidential, including PII that is subject to GDPR. Accounting consultants must routinely relay data between individual clients and consolidated internal systems. With consultants working on multiple accounts, the risk of an accidental data breach between accounts was ever present. The firm needed an efficient way to ensure client confidentiality, while maintaining consultant productivity.

On the client-facing side, the Kiteworks platform provided easy-to-use shared folders, cleanly isolated for each individual client. On the consultant-facing side, the firm used Kiteworks APIs to integrate to its internal applications. The integration automatically exchanged the right files with the right clients with complete confidentiality, and in compliance with GDPR.

A major global accounting firm keeps client data confidential by ensuring consultants don't disclose information to the wrong account as they relay data between individual clients and centralized internal systems.



Step 1

Client accountants collaborate on financial information in shared folders.

Step 2

A custom application uses Kiteworks APIs to manage folders, permissions, and file transfers.

Step 3

Accounting firm consultants collaborate with clients through the custom accounting application.



“The prosecutor’s office saw unique value in document download notifications and immutable audit logs, because the claim: “I didn’t get the documents!” is a common tactic to delay legal proceedings.

Big City Public Prosecutor Must Comply With Digital Discovery Law

Remote Legal Workers Need to Communicate Securely With the Courts, Clients, and Attorneys

The public prosecutor’s office of one of the world’s largest cities needed to enable its staff to work efficiently under the constraint of strict new digital discovery regulations. This problem was compounded by an increasing rate of cyberattacks, and an urgent work-from-home mandate due to COVID-19. Legal staff needed to exchange documents with courts, clients, and external attorneys. The data included sensitive legal documents, PII, and evidence files, such as body camera footage in terabyte-sized files.

Rapid implementation of the Kiteworks platform immediately allowed prosecutor office attorneys, paralegals, finance staff, and other employees to communicate securely and in compliance, even from home offices. Employees found the Kiteworks platform’s familiar email and shared folder interfaces easy and efficient to use. The prosecutor’s office saw unique value in document download notifications and immutable audit logs, because the claim: “I didn’t get the documents!” is a common tactic to delay legal proceedings. Although not required by regulation, the customer purchased an AWS-hosted FedRAMP Authorized deployment to combat the increase in cyberattacks.



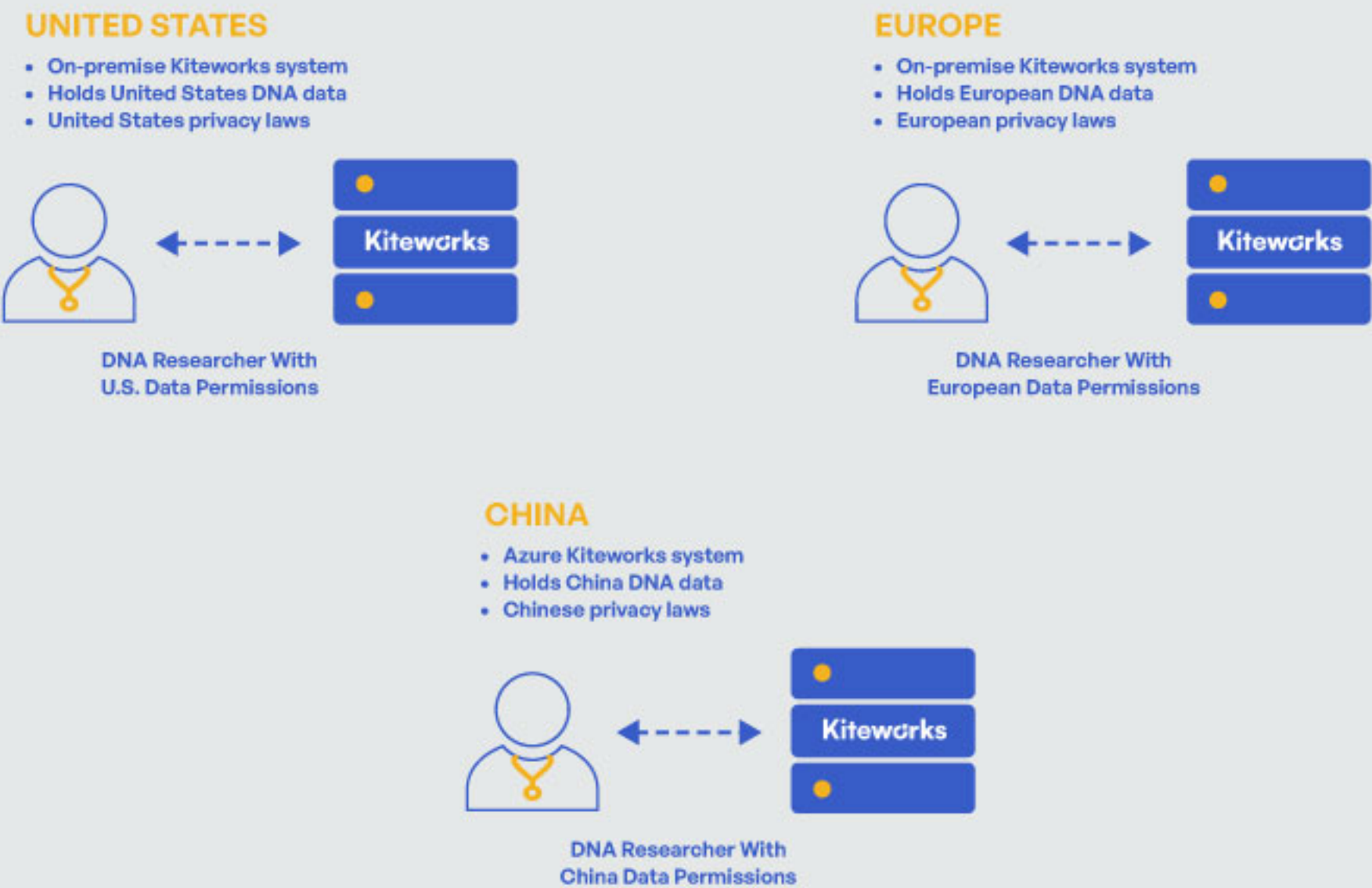
Global Biotech Firm Protects Patient Privacy and IP Internationally

New Division Must Transfer DNA Files in Compliance With China Privacy Laws

This global biotech company develops gene splicing technology that requires careful handling of patient DNA data. Its current operations are subject to GDPR, but a new division in China must also adhere to local regulations. Foreign companies must collaborate with a domestic Chinese research organization to use genetic material from Chinese citizens and to take DNA data outside of China. Plus, all collaborations and transfers must be approved by the Chinese science ministry. The company must comply with Chinese privacy law, while protecting its trade secrets.

The Kiteworks platform enabled the secure transfer of terabyte-sized files containing sophisticated IP, using SFTP between research facilities and corporate systems in the U.S., EMEA, and China. These transfers had to be both confidential and in compliance. Each location has its own local deployment of the Kiteworks platform, making it easy to prove that Chinese DNA data has not been transferred outside the country. However, the Chinese deployment must again be done with a local trading partner. While U.S. and EMEA systems are deployed in the company’s own data centers, the two China systems are deployed on Azure, where Microsoft has relationships with local Chinese hosting companies.

The Kiteworks platform protects a global biotech firm by enabling the secure transfer of terabyte-sized files containing sophisticated IP using SFTP between research facilities and corporate systems in the U.S., EMEA, and China.



German Equipment Leasing Company Complies With GDPR

Third-party Communications Containing Financial and Personal Data Must Be Protected

The CISO of a German equipment leasing company determined that files shared through email and a leading cloud file sharing SaaS did not meet GDPR compliance requirements, and therefore the system had to be replaced. In the normal course of business, employees routinely exchanged financial documents, contracts, and personally identifiable information (PII) with customers and partners. These communications required both confidentiality for business interests and privacy for GDPR compliance. Employees also needed to store and retrieve final documents efficiently and securely on the company's Microsoft SharePoint archive.

The customer used the Kiteworks platform to implement uniform security and governance policies that ensured confidentiality and privacy across both email and file sharing.

The customer used the Kiteworks platform to implement uniform security and governance policies that ensured confidentiality and privacy across both email and file sharing. The Kiteworks SharePoint connector provided easy access to documents, including native SharePoint search, so users could find archived documents quickly and efficiently. Automatic notifications of file downloads also increased productivity by eliminating uncertainty in the leasing process. The customer selected on-premise deployment of the Kiteworks platform to maintain complete control over its data.



International Toy Company Protects Products From Piracy

Secure File Sharing and Email Protects Company IP Across U.S., Europe, and China

This international toy company invests millions of dollars developing a commercially successful toy or game, bringing it to market, and building the brand. Unfortunately, counterfeit toys and games are also a big business that eats into profits, violates trademarks, and exposes the firm to liability. As a result, the company must vigorously protect its IP throughout its global supply chain of manufacturers, marketing partners, and advertising agencies.

The Kiteworks platform allows the company to share IP, including terabyte-sized files, with its trusted digital supply chain suppliers and partners—and no one else. The company deployed Kiteworks secure file sharing and email across its own global data centers in the U.S. and Europe, as well as hosted Azure networks in China. To monitor communications, it integrated the detailed, consolidated Kiteworks syslog with its SIEM to enable centralized security alerts, analysis, and forensics. Kiteworks keeps the firm's IP out of the hands of pirates all around the world.





Kiteworks

www.kiteworks.com

March 2025

Copyright © 2025 Kiteworks. Kiteworks' mission is to empower organizations to effectively manage risk in every send, share, receive, and save of sensitive data. The Kiteworks platform provides customers with a Private Data Network that unifies, tracks, controls, and secures sensitive data moving within, into, and out of their organization, significantly improving risk management and ensuring regulatory compliance on all sensitive data exchanges. Headquartered in Silicon Valley, Kiteworks protects over 100 million end users for over 35,000 global enterprises and government agencies.

