Kiteworks

Kiteworks Partner Customer Success Stories

Deliver Strategic Value to Clients With the Kiteworks Platform

Transform and Secure Risky Business Processes Across the Supply Chain

Drive strategic value for your clients by enabling digital transformation, while reducing infrastructure costs and ensuring security and compliance. An integrated sensitive content communications platform for secure third-party communications, the Kiteworks platform eliminates ugly tradeoffs, such as productivity vs. security, and reduces risk for both you and your clients.

Kiteworks secures third-party communications for more than 3,800 global organizations, including leading financial institutions, government agencies, law firms, healthcare providers, and high-tech manufacturers. Our clients rely heavily on our partner community for services, support, and operations. The examples that follow demonstrate how you can grow your business with Kiteworks.

Quickly Assemble Secure Solutions to Risky Business Problems

Stringing together point solutions creates lucrative targets for cybercriminals. The Kiteworks platform consolidates security across email, file sharing, mobile, SFTP, MFT, and access to enterprise content repositories to provide complete visibility, compliance, and control over complex business processes.

Email | **File Sharing** | **Managed File Transfer** | **Web Forms** | **APIs**

Don't waste time bolting security solutions onto insecure applications or coding low-margin, unstable integrations that create security vulnerabilities. Quickly deploy complete, secure solutions to complex, risky business problems with the Kiteworks platform.

Find Business Opportunities at Every Stage of the Services Life Cycle

Build Predictable Revenue While Reducing Project Time, Costs, and Risk

ADVISE
One Platform—Many Solutions

Leverage the Kiteworks platform to transform, automate, secure, and ensure compliance over any complex business process involving sensitive data shared with third parties. Utilize it across all common communication channels from email to file sharing to SFTP to MFT, and to provide complete visibility for detection, response, forensics, and audits.

DEPLOY
Easy Configuration

The Kiteworks platform has been deployed in the most complex enterprise environments and comes with extensive built-in security and compliance configurations. It also has out-of-the-box integrations for Microsoft 365, OneDrive, Box, file shares, SFTP, and best-in-class security products.

OPERATE
Low Maintenance

The Kiteworks platform runs as a hardened virtual appliance and has an automated DevSecOps pipeline for fast, secure upgrades. Admin and user experiences are simple and easy to learn. You can turn operations over to your customer or run it as a managed service with minimal overhead and maximum economies of scale.

EXPAND
Seamless Add-ons

It's easy to help clients expand to new use cases, new platform modules, new servers, and new users with the flexible, modular Kiteworks architecture and licensing model. Typical client expansion exceeds 300% of the original purchase. For large global organizations, the sky is the limit.

U.S. Federal Government Agency Digitizes Employee Disputes Workflow

Case File Management System Meets Compliance Requirements While Delivered on Time and Under Budget

This U.S. government agency needed to modernize its process for employees to submit disputes, such as harassment claims. It was required to move from paper to the cloud, but the handling of such sensitive data by multiple stakeholders for each case required tight access controls and compliance. Based on history, the agency also expected frequent audits.

The service provider that won the business faced multiple challenges, including securing the employee portal, locking down data communications, restricting file access, and automating the case management workflow. To make money, the company had to avoid unknown technology risks, debugging custom code, and getting bogged down in the Federal cloud authorization bureaucracy. Also, project success hinged on a simple UX to facilitate quick user acceptance from claim submitters, caseworkers, system administrators, and other stakeholders.

The service provider used the Kiteworks platform as the foundation to meet all these needs. Case file communications and managed case folders were easily protected by built-in security and governance settings. For the claimant submitter portal, the team used Microsoft Forms and uploaded submissions through the Kiteworks REST API. The Kiteworks API was also used to automate case workflow and record the final case disposition in the agency's case management system. Off-the-shelf FedRAMP Moderate Authorized hosting by Kiteworks eased cloud compliance and secure monitoring requirements, while comprehensive standard Kiteworks logging and reporting made audit preparation straightforward.

FedRAMP

Step 1

Employee files dispute form

Step 2

Case administrator received notification and begins managing case

Step 3

Arbitrators, managers, and affected parties review and submit documents

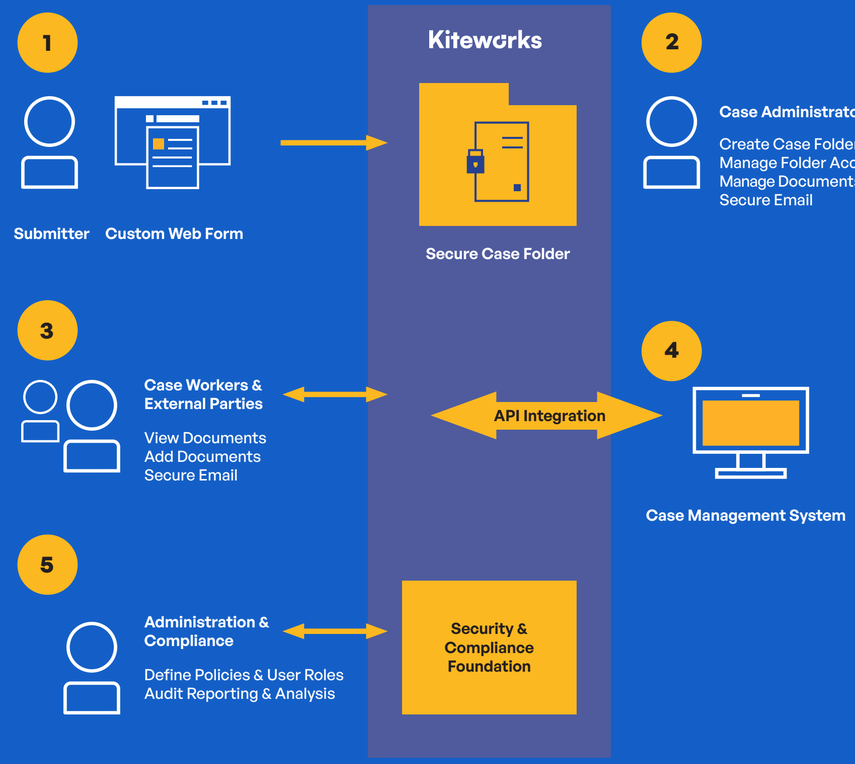
Step 4

Case management system received final records via API

Step 5

IT administers users and policies; compliance manager handles audits

This dispute resolution office ensures employee harassment and whistleblower cases stay organized and completely private as it manages cases from the initial submission, through communications with the affected parties to decision-making and final archive.



Major UK Accounting Firm Secures Payroll Processing for Clients

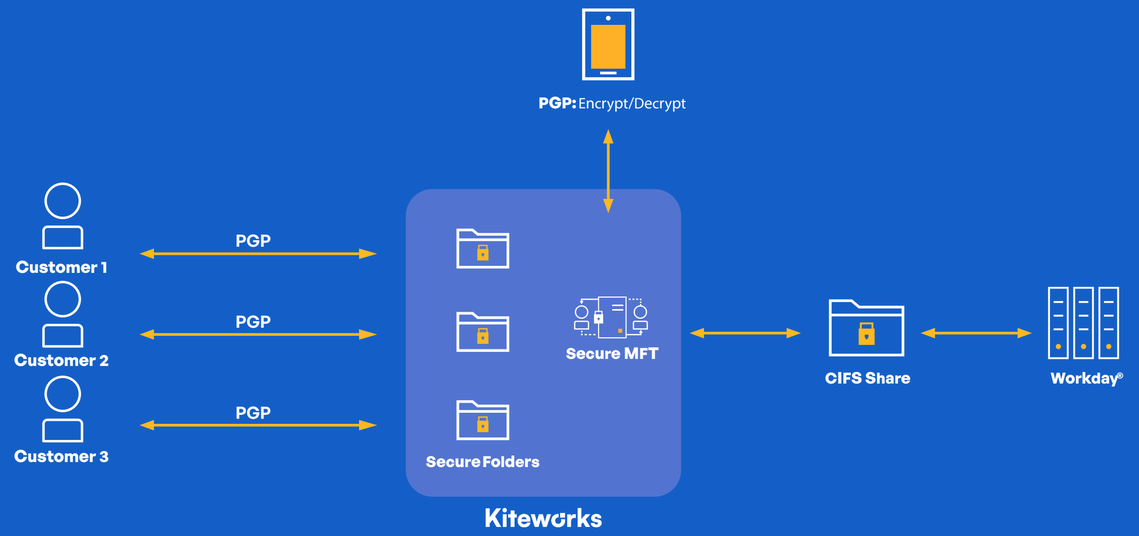
Upgrades Back-end Systems for Compliance and Reliability Without Impacting Customer-facing Processes

This large UK accounting firm runs salary processes and payments on behalf of its customers. It must adhere to strict compliance regulations for handling and protecting sensitive employee data, including salaries, national insurance numbers, and banking information. Mistakes can result in large penalties for missed payments and large fines for noncompliance.

Challenged by a long list of business requirements, integration to legacy systems, and limited resources, the firm could not afford to build a custom system, let alone a system that could also meet security, compliance, and audit requirements. Business automation required handling large numbers of files for multiple clients securely and privately. Files had to be collected and distributed to multiple legacy systems, including Workday, CIFS shares, and SharePoint. Also, the system had to use PGP encryption at the customer and at the firm. These legacy requirements were non-negotiable.

The services provider for this project had to meet these demanding requirements, ensure reliable delivery on the accounting firm's SLAs with its customers, and ultimately make a profit. With Kiteworks, the partner was able to focus on business value over technology deployment and custom development, because the Kiteworks platform supplied most of the business automation, integration, security, and compliance capabilities out of the box. A proof-of-value deployment was configured for the customer in five days before starting the project, and dramatically shortened the time to delivery. The Kiteworks managed file transfer module eliminated the need for custom code and provided automation capabilities well beyond the client's initial requirements. Security and compliance requirements were easily met with standard Kiteworks data governance controls, consolidated system logging, and detailed audit reporting.

UK Services Partner Automates Workday®, CIFS, and PGP Integration Utilizing Kiteworks Secure MFT



Step 1
Customers upload PGP-encrypted raw payroll data to Kiteworks secure folders.

Step 2
Kiteworks MFT automatically decrypts the data via a PGP service and moves it to CIFS shares.

Step 3
Workday processes the files and returns the results to the CIFS shares.

Step 4
Kiteworks MFT encrypts the processed payroll files and moves them to secure shared folders.

Step 5
Customers download the encrypted, completed payroll files.

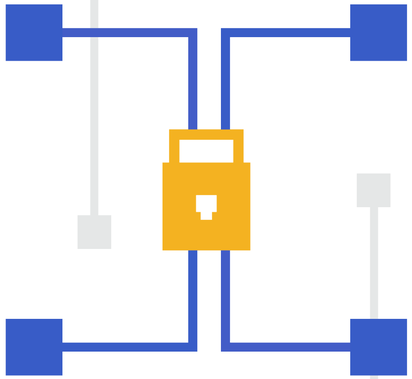
Large Insurance Provider Enables Customer Self-service for Claims Processing

Automates Front Office Business Process and Enables Secure Back Office Communications

The CISO of this specialty vehicle insurer was concerned about security and compliance for claims submissions. Agencies were rejecting their emails, because the file attachments were not secured. Some were so concerned they forced the insurer to use their own various file sharing applications, causing more confusion.

In addition, virtually every back-office department was complaining about out-of-date systems for sharing sensitive data with third parties. HR needed secure email for recruiting. Accounting needed to share detailed financials with auditors every quarter. Legal needed secure collaboration with outside counsel, because it was constantly sharing private customer data. Mergers and Acquisitions needed virtual data rooms to manage projects securely.

The services partner recommended the Kiteworks platform to address all of these issues. Front office claims processing was enabled using Kiteworks secure web forms. Back office employees took advantage of the Microsoft Outlook® plugin and SharePoint connector to send secure email from native desktop applications. The partner enabled collaboration and virtual data rooms using secure web folders, and accomplished bulk data transfers of medical records with third-party healthcare providers using SFTP. Because the deployment was firmwide and involved significant front-office automation, services revenue surpassed product revenue by 3X for this project.



Government Agency Brings Nationwide Epidemiology Report Collection Into Compliance

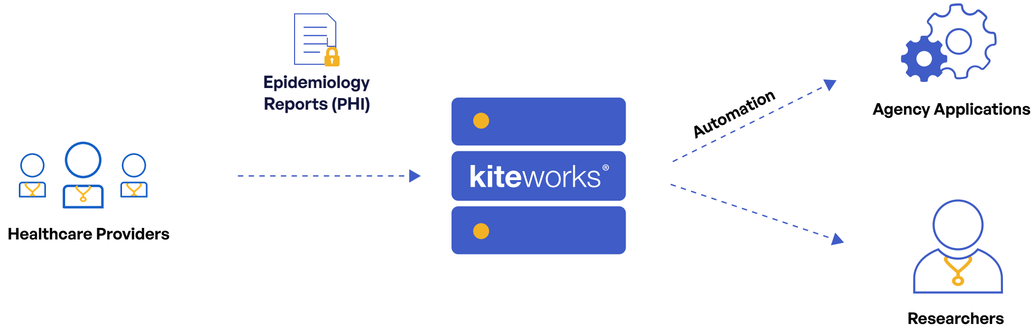
Replaces Custom Legacy Portal With Secure, Scalable, HIPAA-compliant Data Distribution System

This critical government agency collects infectious disease reports from thousands of medical personnel at public and private healthcare organizations across the country. These reports provide raw data to more than one hundred epidemiological applications, including research databases, statistical tracking systems, and disease analytics. Recent tightening of privacy regulations had rendered the home-grown collection system out of compliance. Each submission contains detailed protected health information (PHI) and personally identifiable information (PII) on patients that should only be seen by the patient's doctor or approved healthcare professionals.

The services partner that owned this project had to deliver a solution that not only met functional requirements, but also enforced strict compliance at a granular level, while scaling to thousands of users and millions of submissions. Permissions had to be enforced based on a centralized LDAP system.

Connection from downstream applications by SFTP and APIs was also particularly important.

Under tight time and budget constraints, the partner used the Kiteworks platform to meet compliance requirements out-of-the-box. The partner deployed multiple Kiteworks instances, each enabled by different data access levels specified in the central LDAP system. Each instance utilized a high-availability cluster configuration to ensure availability. Most users work with the system through secure shared folders, or through intermediate applications, while most legacy applications transfer data using Kiteworks SFTP interfaces. Because the data transfer, security, compliance, scale, and high-availability capabilities were provided by the Kiteworks platform, the partner was able to focus on building custom REST API integrations for the remaining downstream applications—ensuring that this critical system suffered minimal downtime.



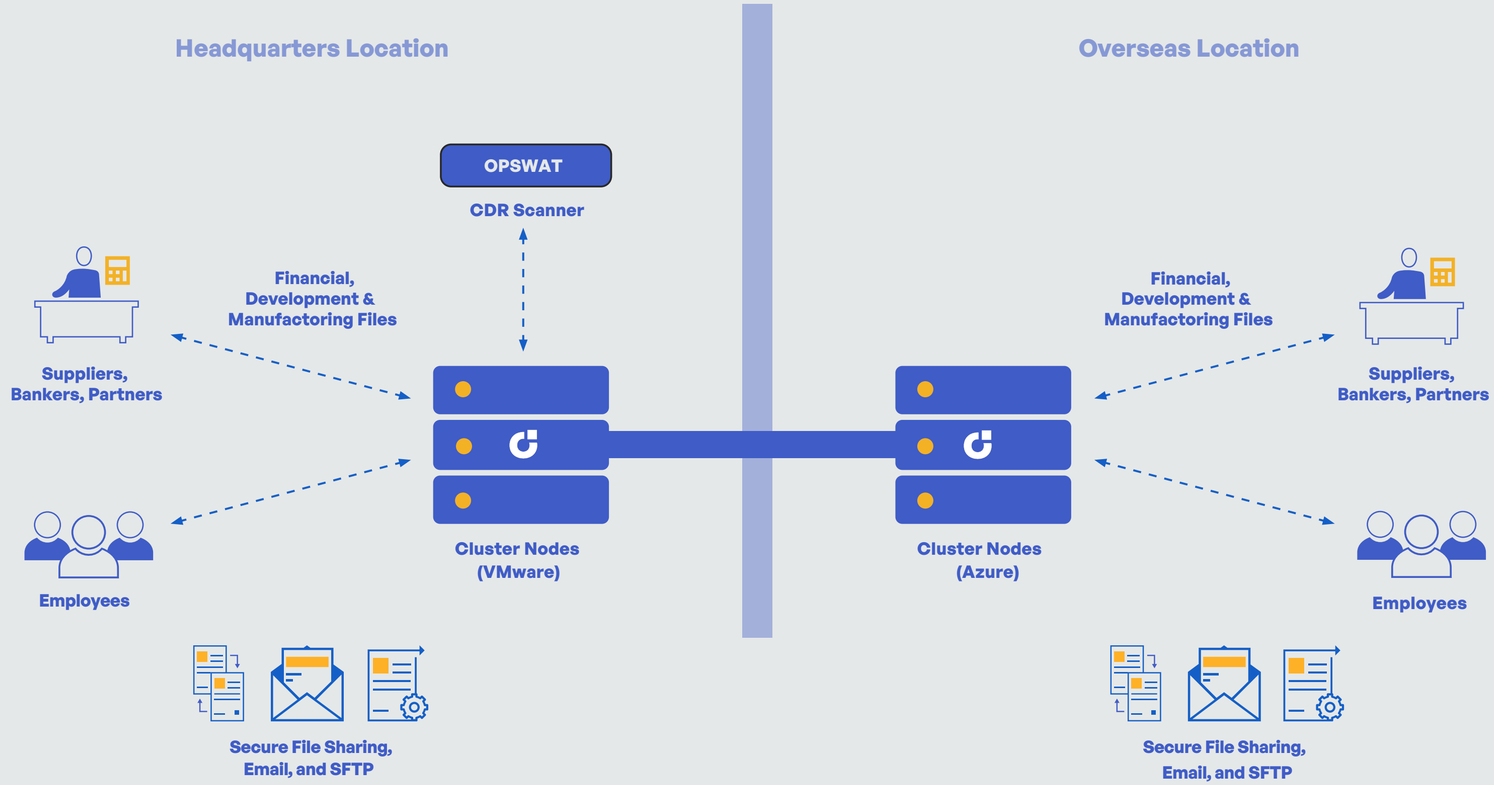
Global Pharmaceutical Company Consolidates Secure Communications Across Countries

Confidential Clinical Trial, Manufacturing, and Financial Documents Shared Securely Around the World

This major pharmaceutical provider wanted to dramatically simplify the communication of sensitive information with regulators, suppliers, and international subsidiaries. Every day the firm needed to automate the exchange of clinical trial and safety reports between local regulators and more than one hundred internal groups. Manufacturing facilities had to share trade secrets with subcontractors all over the world. Subcontractors had to supply production reports twice per day. And subsidiaries needed to roll up financial reporting with headquarters.

Operating under a “cloud-first” mandate, the firm was looking to replace multiple legacy solutions with a platform that could protect its data from modern cyber threats and supply the necessary audit trail to demonstrate compliance to numerous local regulatory authorities. Moreover, as core global IT infrastructure, the platform needed to be highly available and highly scalable.

The services provider deployed the Kiteworks platform on Microsoft Azure®. By leveraging Kiteworks built-in security, integration, and deployment capabilities, the services partner was able to reduce project risk and focus its energy on enumerating, rearchitecting, and automating global data flows throughout the firm to run through this new centralized security and compliance infrastructure.



European Bank Achieves GDPR Compliance While Reducing Costs

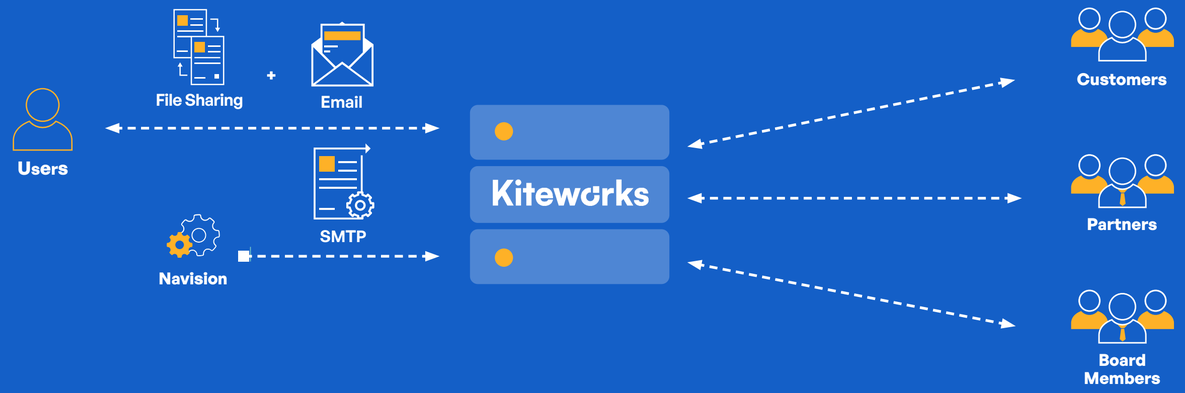
Sends and Receives Sensitive Content via Email and File Sharing With Automation of Routine Business Processes

This European commercial bank needed GDPR-compliant distribution of statements and invoices to clients. In addition, the bank's employees and clients constantly complained about the poor usability of the bank's email and file sharing applications used to exchange sensitive financial, business, and private client data with business customers, partners, and board members.

The services partner deployed the Kiteworks platform to address all three problems with a single solution. Statements and invoices had to be sourced from the bank's Microsoft ERP system, so the partner implemented the Kiteworks SMTP relay automation to provide secure, compliant distribution to customers and partners. 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 unsecured attachments. Compliance regulations are met through governance controls and are demonstrated with a complete audit log.

Once the Kiteworks platform was deployed for automated document distribution, it was an easy task to enable secure email and file sharing for end-users. The Kiteworks platform allows employees to exchange confidential contracts, negotiation documents, and legal files with clients directly from Microsoft Outlook and from modern web and mobile apps. Employees are also able to collaborate more intensely with Kiteworks secure shared folders. By deploying a single platform for multiple use cases, the partner helped its client save money by consolidating and retiring costly legacy file sharing applications.

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.

Your Client's Private Content Network

Kiteworks creates a dedicated Private Content Network (PCN) of internal and external digital communications that ensures zero-trust privacy protection and compliance of an organization's most sensitive information.

UNIFY

Reduce complexity and lower costs by consolidating secure content communications technologies and normalizing multiple content audit trails into one centralized system.

TRACK

Achieve comprehensive situational awareness of content, user, and system activity to boost SOC effectiveness and easily meet regulatory compliance reporting requirements.

CONTROL

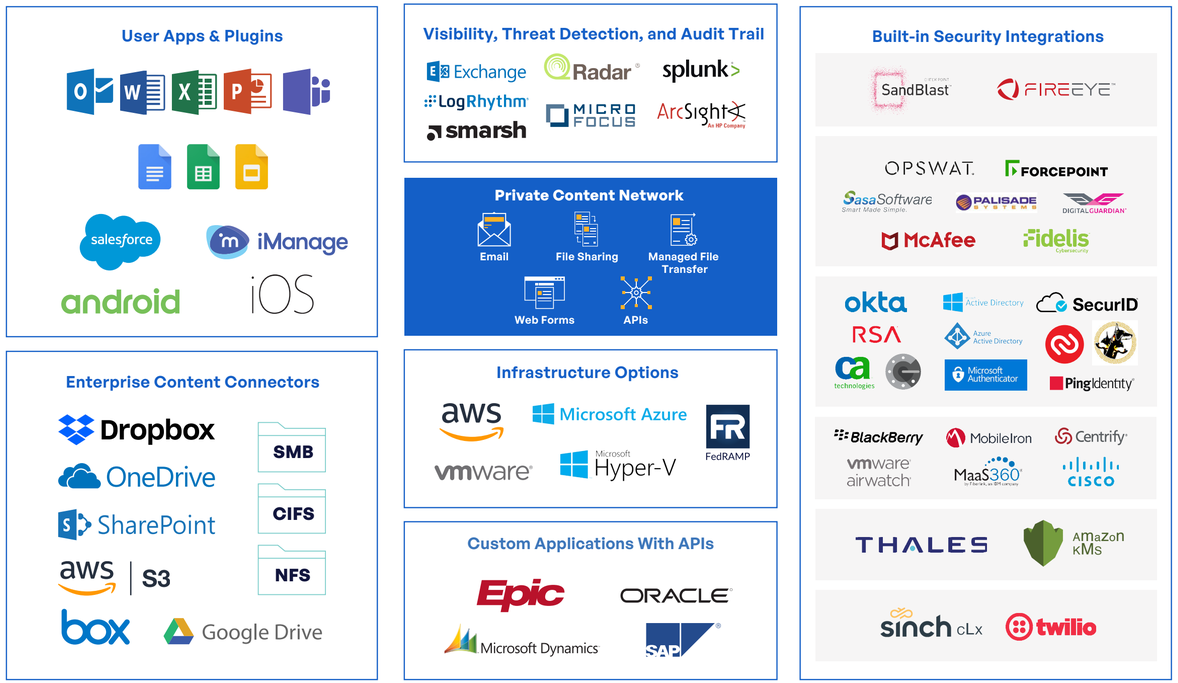
Adhere to compliance and internal policy requirements by implementing content access and functional rules matched to risk profiles and user roles.

SECURE

Eliminate unintended exposure of sensitive information to malicious actors through content communications encryption.

Create Tailored Solutions From a Wide Array of Standard Kiteworks Components

Designed to Adapt to Your Clients' Specific Environment With Minimal Effort



The modular architecture of the Kiteworks platform allows service providers to solve difficult customer problems by assembling unique solutions from standard platform components. Complex business processes can be automated across multiple communication channels and secured with granular policy controls. End-user apps and plugins combined with content connectors simplify the user experience, while integration to SIEM, IAM, ATP, DLP, MFA, and myriad best-in-class solutions ensure the highest level of security and compliance. A wide array of deployment options ensure that each solution fits comfortably into the customer's native environment.

Kiteworks

www.kiteworks.com
April 2022