



Service Definition Document

G-Cloud 15

Version 1.0
December 2025
sales.gcloud@kiteworks.com



Table Of Contents

Contents

1.

Introduction

4

Kiteworks Company Overview.....

4

Social Value

4

Overview of the G-Cloud Service.....

5

Enable Your Private Data Network (PDN) With the Kiteworks Platform

5

Addressing the Modern Threat Landscape

5

Associated Services.....

6

Kiteworks, what’s included

6

2. Data Protection

10

Information Assurance.....

10

Security and Compliance

10

Data Back-up and Restoration

10

Business Continuity Statement / Plan

10

Scope:.....

10

Privacy by Design.....

11

Enterprise Security

11

Auditing and Reporting

11

Antivirus

11

Restricted Administrator Access to Data

11

SSO (SAML/Kerberos).....

11

LDAP/AD Integration.....

12

Data Loss Prevention (DLP)

12

File Integrity Monitoring

12

Fail2ban Intrusion Prevention.....

12

Web Application Firewall (WAF)

12

Secure Delete

12

Encryption

12

Encrypted Data While at Rest and in Transit

12

256-bit AES.....

12

Ownership of Encryption keys

13

Compliance

13

Product Compliance.....

13

3. Using the Service.....

14

Ordering & Invoicing

14

Ordering

14

Service Activation.....

14

Invoicing.....

14

Availability of Trial Service

14

On-Boarding, Off-Boarding, Service Migration, Scope Etc

15

On-Boarding Process.....

15

Off-Boarding Process

15

Training

15

Implementation Plan

15

Service Management

15

Service Constraints

16

Kiteworks G-Cloud 15

Performance and Availability	16
Service Levels.....	16
Outage and Maintenance Management.....	16
Financial Recompense Model for not Meeting Service Levels.....	17
Support Hours	17
4. Provision of the Service.....	18
Customer Responsibilities	18
Technical Requirements and Client-Side Responsibilities.....	18
Customer Responsibilities – Customer-Hosted Deployments.....	18
Customer Responsibilities – Kiteworks-Hosted Deployments.....	18
Identity, Integrations, and Third-Party Services.....	18
Technical Requirements and Client-Side Requirements.....	19
Outcomes/Deliverables	19
Deliverables.....	19
Development Lifecycle of the Solution.....	20
Secure Development Approach	20
Agile Methodology.....	20
Release Cadence	20
Quality Assurance	20
Aftersales Account Management.....	20
Termination Process.....	21
Termination by the Customer	21
5. Our Experience.....	22
Case Studies.....	22
Jaja Finance	22
Clients	23
Contact Details	23

1. Introduction

Kiteworks Company Overview

Kiteworks enables organizations to effectively manage risk in every send, share, receive, and save of sensitive data. To this end, we created a platform that delivers data governance, compliance, and protection to customers. The platform unifies, tracks, controls, and secures sensitive data moving within, into, and out of their organization, significantly improving risk management while ensuring regulatory compliance on all sensitive data communications. Founded in 1999 and headquartered in San Mateo, California, Kiteworks has over 600 employees worldwide and serves over 3,800 customers and 100 million users.

Kiteworks' mission is to empower organizations to effectively manage risk in every send, share, receive, and save of sensitive data. With 70% of organizations needing to demonstrate compliance with at least six security frameworks, and 61% experiencing breaches involving third-party interactions, Kiteworks addresses these critical challenges through its unified Private Data Network approach. Organizations using Kiteworks reduce compliance reporting time by 68% by eliminating redundant efforts across siloed systems, while detecting cross-channel threats that siloed solutions miss.

Social Value

Social Value Declaration

At Kiteworks, we recognise that social value is best delivered through proportionate, practical actions that align with the scale and nature of the contract. We are committed to contributing positively to fair working practices, skills development, equality of opportunity, and community and environmental outcomes, in line with the PPN 002 Social Value Model, while remaining flexible and responsive to contractual and operational needs.

Kickstart economic growth

Where relevant to the contract, Kiteworks will support fair working conditions by ensuring new workers are informed of their employment rights. We will also seek to apply inclusive workforce policies in line with existing statutory and organisational frameworks.

To support in-work progression and skills development, Kiteworks will explore opportunities to offer placements, or training initiatives aligned to contract needs and skills shortages. These may include supported internships, or T Level industry placements, with a focus on creating quality opportunities and clear routes to progression where appropriate. We will also aim to support access to employment for individuals facing barriers to work, including disabled people and those from under-represented groups, through proportionate outreach, fair recruitment practices, and targeted training where relevant.

Break down barriers to opportunity

Kiteworks is committed to promoting equality of opportunity through transparent and fair pay and reward practices, inclusive recruitment approaches, and ongoing efforts to reduce barriers for disabled people and those with health conditions. Where appropriate, we will engage with employees and representative organisations to inform improvements. Our supply chain approach will be structured to encourage fairness, ethical behaviour, and accessibility, supporting participation from a diverse range of organisations, including SMEs, start-ups, VCSEs, and supported businesses, where this aligns with contract delivery requirements.

Community, wellbeing, and environmental considerations

Where appropriate, Kiteworks will engage with local communities and stakeholders, such as education providers, charities, and industry bodies, to support skills pipelines, awareness-raising, and community integration linked to the contract. We will remain open to adapting our engagement approaches based on feedback and emerging opportunities. In addition, we will seek to contribute to workforce wellbeing through access to appropriate HR and occupational health support, and to environmental objectives through proportionate actions that support resource efficiency, reduced environmental impact, and collaboration with suppliers and stakeholders.

Conclusion

Kiteworks is committed to delivering meaningful and proportionate social value through this contract. Our approach is flexible, scalable, and focused on practical outcomes, ensuring that social value commitments support both successful contract delivery and positive, lasting impact for people, communities, and the wider economy.

Overview of the G-Cloud Service
Enable Your Private Data Network (PDN) With the Kiteworks Platform

5.

The Kiteworks Private Data Network provides organizations security, governance, and compliance over the sensitive data they share with trusted parties by email, file sharing, managed file transfer, and other channels. Security features like end-to-end email encryption, multi-factor authentication, and a hardened virtual appliance ensure the sensitive data in emails and files stays protected from unauthorized access. Comprehensive tracking—who sends what to whom and when—and audit logs demonstrate compliance with data privacy regulations and standards. With Kiteworks, organizations know that the sensitive data they share is fully protected and in compliance.

The Private Data Network architecture eliminates the chaos of fragmented data ecosystems by consolidating email protection, secure file sharing, managed file transfer, SFTP, and web forms under unified governance. This unified approach provides centralized visibility and consistent controls across all communication channels, enabling organizations to scale secure collaboration without increasing administrative burden through automated, self-service capabilities.

With on-premises, private cloud, hybrid, and FedRAMP deployment options, the Kiteworks platform provides the security and governance C-suite leaders need to protect their organizations, mitigate risk, and adhere to rigorous compliance regulations such as NIST CSF (National Institute of Standards & Technology Cybersecurity Framework), CMMC (Cybersecurity Maturity Model Certification), HIPAA (Health Insurance Portability and Accountability Act), SOX (Sarbanes-Oxley Act), GDPR (General Data Protection Regulation), GLBA (Gramm-Leach-Bliley Act), and FISMA (Federal Information Security Management Act), among others.

Kiteworks implements a zero-trust architecture with assume-breach principles, integrated managed detection and response (MDR) capabilities, and comprehensive encryption. This approach ensures that all data exchanges are authenticated, encrypted, and monitored—regardless of the communication channel or endpoint. The platform's



sophisticated access controls combine granular permissions with multi-factor authentication (MFA), while strategic micro-segmentation creates secure, isolated network environments that prevent lateral movement of threats.

Ensure regulatory compliance and effectively manage risk with four critical capabilities:

- **Unify.** Reduce complexity and lower costs by consolidating secure data communication technologies and standardizing multiple data audit logs into one centralized system.
- **Track.** Achieve comprehensive situational awareness of data, user, and system activity to boost security operations center (SOC) effectiveness, report on third-party access, and easily meet regulatory compliance reporting requirements.
- **Control.** Adhere to compliance and internal policy requirements by implementing data access and functional rules matched to risk profiles and user roles.
- **Secure.** Eliminate unintended exposure of sensitive information to malicious actors through data communications encryption, a hardened virtual appliance, secure software development life cycle, active worldwide bounty-hunter program, and zero trust principles.

Addressing the Modern Threat Landscape

With zero-day attacks increasingly targeting data exchange systems (44% of attacks in 2025), and third-party breaches doubling to 30% according to the Verizon 2025 Data Breach Investigations Report, organizations need comprehensive protection for their most vulnerable attack surface. Kiteworks Private Data Network addresses these evolving threats through:

- **Zero-Trust Architecture:** Continuous authentication and least-privilege access across all data exchanges
- **Supply Chain Security:** Comprehensive third-party risk management and governance, addressing the nearly 60% of organizations that lack comprehensive governance for third-party data exchanges
- **Unified Visibility:** Single-pane visibility that detects cross-channel threats that siloed solutions miss
- **Assume-Breach Posture:** Integrated MDR capabilities ensure organizations are prepared for rapid incident response

www.kiteworks.co

Associated Services
Kiteworks, what’s included

Kiteworks Secure File Sharing Features	
Flexible Deployment	Kiteworks can be deployed in the following ways: - As either a pre-hardened on-premise appliance supporting Vmware, Hyper-V or Nutanix Hypervisors. - Cloud hosted by the customer, utilizing AWS or Azure hosting providers - Cloud hosted by Kiteworks, in the IaaS or PaaS model using AWS or Azure hosting providers - Air-gapped and fully offline, utilizing the customers on-prem hypervisors (Vmware, Hyper-V or Nutanix) - Hybrid deployment
Secure Email (including large file support via plugin)	Users send and receive encrypted email in web, mobile, and plugin interfaces. Provides Request File and shared mailbox capabilities. Includes basic DRM that provides view-only access with a full audit trail, access controls, and expiration, without losing control over the asset.
Secure Email Gateway (Optional)	The Kiteworks EPG (Email Protection Gateway) provides a robust, in-line gateway in order to apply granular policy based control to some or all inbound & outbound email. - Transparent for the users sending / receiving email - Supports TLS, S/MIME, PGP & web portal based security - Automated policy engine, reducing the risk of user error - Granular visibility of data exchange
Secure Shared Folders	Secure web folders, collaboration, automatic versioning, simplified virtual data rooms (VDR), and full text search.
Microsoft Office Concurrent Editing Integration	Kiteworks secure web folders provide seamless Microsoft Office concurrent editing integration, in web, mobile, and plugin interfaces, fully integrated with Kiteworks folder versioning.
NEW - View-only SafeVIEW DRM	Highly sensitive files are converted into a set of static image files to prevent their data from being copied or returned in search results. View-only privileges are controlled by email senders and folder managers.
Large File Sizes	Transfer files up to 16 TB in size.

Mobile Apps	Native apps for Android and iOS supporting secure email, secure file sharing, secure photos, remote access to Enterprise Connect (if licensed), jailbreak detection, Touch ID, Face ID, Fingerprints, and secure container for offline access, with remote wipe.
Secure & Advanced Data Forms Via Web and Email	Utilizing the Advanced Forms capability, users granted the “Form Builder” role can create custom data forms enabling secure, compliant collection of data & text fields. This form data is automatically sent directly to a Kiteworks folder, which is subject to the corresponding secure policies on the Kiteworks platform supporting attribute based access controls, role specific access & integration with business workflows.
Branding, Appearance, and Custom Text	Apply logos and color schemes to login screens on the web and mobile apps, customize templates for all types of emails and legal disclaimers, and customize end-user documentation.
Standard Plugins	• Microsoft Outlook® (desktop and online) • Microsoft Office® Word, PowerPoint, Excel (desktop, mobile, and online) • Microsoft Teams® (desktop, mobile, and online) • Google Workspace® (Drive, Docs, Sheets, Slides)
API & Automation Capabilities (Optional)	RESTful API enables integration with existing workflows, ITSM platforms, and custom business applications. Automate user provisioning, folder management, and reporting to reduce administrative overhead and ensure consistent policy enforcement.
Secure MFT Suite	Automates compliant end-to-end file transfer workflows with both client and server-based options. Comprehensive support for SFTP, FTPS, HTTPS, and AS2 protocols, plus dedicated connectors for cloud storage (AWS S3, Azure Blob, Google Cloud) and enterprise repositories. Scalable, high-availability architecture with scheduled transfers, automated retry logic, and complete audit trails ensures reliable, secure automated operations for high-volume business-critical transfers.
NEW - Support for MCP based AI integration	Interact directly with the Kiteworks platform via AI agents using the Model Context Protocol (MCP). This extends support for interpretive API based actions, for example moving data, creating folders, re-creating forms and more.

7.

NEW - Attribute-based Risk Policy Administration and Enforcement (Up to 2 Policies)	See the description in the Attribute-based Risk Policy entry in Option: Advanced Governance. Note that an Advanced Governance license allows an unlimited number of policies, but an Enterprise license enables only 2 policies.
Comprehensive, Immutable Audit Logs	The Kiteworks platform provides the unified audit logging needed to identify threats, take remedial action, and perform forensics. While other platforms may store logs in separate files for each subsystem, Kiteworks syslog entries and audit reports across all communication channels and system services are unified, comprehensive, standardized, and cleaned. Logs can be exported to one or more syslogs for import into your SIEM, such as IBM QRadar® or FireEye Helix®. A Splunk® App using its native Splunk Forwarder is also provided.
Trusted Audit Logs	The system converts logs to various human-readable forms for many uses: • Administrative reporting of all activities, filterable and searchable • Report generation and export for use in compliance audits • End-user-visible tracking of all views, downloads, uploads, and edits
Tracking of Sent Emails for End-users	When end-users view their sent mail in the Kiteworks web interface, Outlook Plugin, or mobile app, they can click a Track button to see a table showing which recipients have opened the email, viewed the attachments, or downloaded them. A detailed report gives them an exportable audit trail including timestamps. The sender can enable others in their organization to track message activity on key emails, thus streamlining certain business processes.
NEW - Risky Settings Detection	The admin console guides administrators through tightening existing security settings to reduce potential exposure of the system. If risky settings are detected, the system displays an alert upon each admin login until the settings are confirmed or changed. It also sends periodic email alerts.
Tracking of Shared Folders and Files for End-users	When end-users view a shared folder where they have Owner, Manager, or Collaborator privileges, they can click a Track button next to each file and folder to see a table showing which recipients have accessed or modified it, and click any entry to see its exact history of downloads, views, etc., with timestamps. A detailed report provides an exportable, timestamped log of every user who viewed, downloaded, uploaded, changed, or renamed any file in the folder, as well as changes to user invitations and permissions of the folder itself.

Security Analytics	Use the CISO Dashboard and Splunk® App visualizations to show suspicious traffic patterns, such as anomalies in download locations, traffic levels, user activities, and individual file activities, across all communication channels utilized, such as email, file shares, SFTP, MFT, and Microsoft Teams. Drill down to the details of each transfer to track down who touched which files, where they are, and what users did with them. AI-powered alerts notify you of suspicious activities so you can investigate them before they become breaches.
Unified Security and Governance	• Central, common role-based policies, access controls, and administration that apply across the communication channels • Configurable administrator roles • Hardened virtual appliance with enterprise-grade encryption, embedded zero-maintenance network firewall and web application firewall (WAF) with automated rules update, multiple forms of intrusion detection, file integrity monitoring (FIM), zero-trust communication principles between services, and other layers of defenses • Customer-managed keys • Enterprise integrations: LDAP/AD, SSO/2FA/MFA, Splunk, SIEM, authenticators (Google, Microsoft, and Authy), SMS, HSM, and AWS KMS • ~90% coverage of CMMC 2.0 level 2 requirements for defense contractors
Data Sovereignty and Geofencing	• Enforce geofencing by setting block-lists and allow-lists for IP address ranges • Configure a distributed system to store a user's data only in their home country • Use built-in reporting to see where data is stored and prove it to auditors
File Storage Options	• Kiteworks supports local storage of user data, in the following ways: • For On-Prem hosted systems, storage is directly attached via the hypervisor • For cloud hosted systems, Kiteworks supports EBS based storage (AWS) or Blob based storage (Azure). • Kiteworks also supports NFS storage.

Embedded Anti-virus (AV) Scanner	
Anti-virus Scanning and Quarantine Option	A built-in WithSecure® Anti-virus (AV) service option scans files for malware on download and upload. Files of any size can be scanned, including those passing to or from Enterprise Connect sources or through the Email Protection Gateway (EPG). The administrator can configure Kiteworks settings to quarantine infected files or simply log and alert. When using AV with the EPG feature, it is not used in EPG Database nodes.

2. Data Protection

Information Assurance

Security and Compliance

Kiteworks offers a hardened appliance with all unnecessary services disabled, built with only the necessary software for Kiteworks to run. All communications to the server are over an SSL/TLS encrypted transport layer. All requests are funneled through a secure channel communication limiting the attack-surface to a tier that does not store sensitive information.

A multi-tier architecture provides flexibility in deployment options that are explained in the next section SSH access is shut off by default and file storage is completely encrypted. Files are directly available only to the system they are mounted on, and services running on other systems access files through a secure internal API not available to the outside world.

Kiteworks integrates with an on-system antivirus scanner (F-Secure Atlant) and with third-party DLP systems that support the ICAP protocol Periodic penetration tests and security audits are performed These include the web server, Enterprise Connect, mobile, and desktop Clients Kiteworks is built using OWASP secure coding practices and is FIPS-140-2 certified All software updates (OS, services, and application) are provided by Kiteworks hardened update servers over SSL/TLS Packaging is digitally signed and validated upon update.

Organizations implementing Kiteworks' unified security and compliance framework experience significant operational benefits beyond risk mitigation. The CISO Dashboard provides complete visibility into all system activities, enabling rapid response to potential security incidents. With comprehensive audit logs and centralized compliance capabilities, organizations reduce compliance reporting time by 68%, addressing the challenge that 62% of organizations face when expending 1,500+ hours annually on compliance reporting. This unified approach delivers 35% higher customer trust scores and 42% faster partner onboarding times, transforming compliance challenges into strategic advantages.

Data Back-up and Restoration

Kiteworks employs a comprehensive data protection strategy to safeguard customer data:

- **Backup Frequency:** Automated daily incremental backups with weekly full backups ensure minimal data loss in the event of an incident. Backup schedules can be customized based on customer requirements and documented in the Order Form.
- **Backup Retention:** Backups are retained for a minimum of 30 days, with configurable retention periods available to meet specific compliance requirements.
- **Data Restoration:** Kiteworks maintains a 24 hour RTO (Recovery Time Objective) with a 72 hour RPO (Recovery Point Objective).
- **Testing and Validation:** Backup processes are reviewed, updated, and tested quarterly to ensure data integrity and successful restoration capabilities. Test results are documented and available upon request.
- **Customer Control:** Administrators can initiate on-demand backups and restore specific files or folders through the admin console. Backup configurations and schedules can be discussed and agreed prior to order placement.

Business Continuity Statement / Plan

Commented [BR1]: Needs review by compliance

Scope:

This business continuity plan covers all of the Kiteworks Private Data Network (PDN) including secure email, file sharing, managed file transfer, and administrative functions.

Key Business Areas:

- **Service Delivery and Operations** – hosting, monitoring, and management of services
- **Information Security and Incident Response** – security monitoring, incident handling, and escalation
- **Customer Support** – service desk, customer communications, and issue resolution
- **Engineering and Platform Management** – infrastructure, application support, and recovery activities
- **Management and Governance** – decision-making, communications, and supplier coordination

Critical Functions:

- Platform availability and uptime
- Data availability and Integrity
- Security monitoring and incident response
- Customer support, customer communication and technical assistance

Please treat this information as private and confidential.

Dependencies:

- **Cloud Providers (AWS and Azure):** compute, storage, networking, and managed services
- **Identity and Access Management Services:** authentication and role-based access
- **Monitoring and Alerting Tools:** detection of availability or performance issues

Acceptable Downtime:

- Critical functions (Level 1): Maximum 4 hours unplanned downtime
- High priority functions (Level 2): Maximum 8 hours unplanned downtime
- Planned maintenance: Scheduled during agreed maintenance windows with advance notification

Operational Continuity:

Kiteworks maintains redundant infrastructure across multiple availability zones, automated failover capabilities, 24/7 monitoring, and dedicated incident response teams to ensure service continuity. Disaster recovery procedures include data replication, alternative processing sites, and documented recovery procedures. The Business Continuity Plan is reviewed at least annually and following significant changes to the policies/procedures outlined above. A more detailed plan can be provided to the buyer on request.

Privacy by Design

Kiteworks adheres to Privacy by Design principles as mandated by GDPR, embedding data protection from the initial design phase through the entire lifecycle of the service:

- **Proactive Measures:** Data minimization principles ensure only necessary data is collected and processed. Encryption at rest and in transit protects data throughout its lifecycle.
- **Default Settings:** Privacy-protective defaults include automatic encryption, granular access controls, and comprehensive audit logging enabled by default.
- **End-to-End Protection:** Zero-trust architecture ensures data protection across all communication channels without creating additional risks or compromising functionality.
- **Transparency:** Complete audit trails provide visibility into all data access and transfers, enabling organizations to demonstrate GDPR compliance and respond to data subject access requests.
- **User Control:** Data subjects maintain control through granular permissions, time-limited access, secure deletion capabilities, and the ability to revoke access at any time.
- The platform supports the "right to be forgotten" while maintaining necessary audit trails for compliance requirements through cryptographic deletion of encryption keys.
- These configurations are fully customizable and the configuration on the platform is owned & managed by the customer & the customers administrators.

Enterprise Security
Auditing and Reporting

Kiteworks provides reporting to both end users and administrators.

Administrators view all end user and administrator activity through the Admin Console on the Kiteworks server. They can also export activity logs to an external syslog server.

End users view activity through the Kiteworks web application, such as file uploads, downloads, deletions, comments, and tasks for folders that have been shared with them. Each Kiteworks folder has its own activity log which tracks its file uploads, downloads, and deletions as well as the creation or deletion of subfolders.

Antivirus

Kiteworks uses WithSecure Atlant antivirus to perform definition based malware scanning of all data uploaded or transferred through the Kiteworks system. Detected files will be quarantined, triggering notifications to administrators in order to allow remedial action prior to user access.

Restricted Administrator Access to Data

Access to data within the Kiteworks platform is based on explicit access being granted via data owners, and administrators of the platform are unable to access user data without explicit access being granted.

SSO (SAML/Kerberos)

Kiteworks fully supports SSO via SAML or Kerberos based authentication protocols. This allows Kiteworks to extend support for key SSO based identity providers such as Microsoft Entra, Okta and more. Kiteworks also supports the

Kiteworks G-cloud 15
ability for the RBAC profile & location of storage for the user data to be automatically assigned based on the SAML assertion. 12.

LDAP/AD Integration

Kiteworks can be integrated with LDAP/AD so users can sign in with their network password. Additionally, Kiteworks allows administrators to add LDAP groups directly to the platform.

Data Loss Prevention (DLP)

Kiteworks integrates with several market-leading DLP products enabling data-aware sharing restrictions.

File Integrity Monitoring

Kiteworks offers file integrity monitoring with open-source host intrusion detection security (OSSEC)

If any file modification is detected, a warning displays with the exact time and when the file modification was detected The syslog shows the activity, before and after the modification of the file The email daemon sends an email to the administrator. The Activities report displays the alert and the details of the activity.

Fail2ban Intrusion Prevention

Kiteworks offers the Fail2ban intrusion prevention framework to protect servers from brute-force attacks Specific IPv4 and IPv6 addresses can be banned. The functionality offers:

- Banning of specific IP addresses
- Banning of IP address ranges Banning IPv4 or IPv6 addresses
- Changing the number of failed attempts before banning
- Changing the time IP addresses are blocked for, after failed login attempts
- Maintaining a list of banned and allowed IP addresses (and the settings) after Fail2ban is restarted.

By default, Kiteworks blocks an IP address for 10 minutes after five failed SSH or SFTP login attempts Blocked IP addresses are then listed in a Banned IP list.

Web Application Firewall (WAF)

Kiteworks utilizes the ModSecurity Web Application Firewall (WAF) to actively defend against web-based attacks The ModSecurity WAF is installed on every Kiteworks web node.

ModSecurity protection is based on a local database (ruleset) of known signatures of attacks (or rules) Each rule in the ruleset is comprised of two parts: a set of characteristics that define a known attack and an assigned risk score Every web request arriving at a Kiteworks web node is analysed and compared against the local ruleset If it matches, the assigned risk score is accumulated to the request's risk score Once a request has accumulated a "high-enough" risk score, it is blocked by the WAF.

The Kiteworks ModSecurity signatures database is specially curated by internal Kiteworks security researchers and is continuously maintained by them This allows for maximizing protection against attacks, while keeping false positives to an absolute minimum Protection against all major web-based attacks, such as XSS, CSRF, SQL injections, and more, is included as they pertain to Kiteworks The WAF ruleset on Kiteworks instances is updated with each release of the product.

Secure Delete

Kiteworks supports secure delete processes in order to ensure data marked for deletion on the platform is deleted securely & rendered unrecoverable. All files are encrypted on the Kiteworks platform both at the disk & file level. In the event of secure delete, the encryption key used to encrypt the file in question is overwritten with random data, prior to the deletion of the file & encryption key. This renders the data entirely unrecoverable.

Encryption

Kiteworks provides the following encryption features.

Encrypted Data While at Rest and in Transit

Files are encrypted while in motion and at rest using AES 256-bit disk encryption, and files through transit using a secure SSL connection.

256-bit AES

All data is stored either on the Kiteworks server or client In the Kiteworks mobile apps. There are two layers of encryption for data on the system. All client files are encrypted using FIPS 140-3 approved AES 256-bit algorithm for disk encryption. In addition, each file is individually encrypted with a unique key using FIPS 140-3 approved AES-256-CTR algorithm.

As data is moved throughout the Kiteworks system, 128-bit or 256-bit TLS is implemented to protect data in transit. All data transactions are also logged by user/IP address. Significant metadata is captured for each transaction.

Ownership of Encryption keys

All data on the Kiteworks platform is encrypted by default, utilizing keys that are automatically managed by the Kiteworks platform. The encryption keys used by the platform are owned exclusively by the customer. Kiteworks as the vendor has no ability to access customer data stored on the platform regardless of hosting location.

Compliance

Kiteworks is SOC 2, Cyber Essentials, Cyber Essentials+ and ISO 27001, ISO 27017, ISO 27018 certified. Kiteworks is FedRAMP authorized and satisfies compliance requirements for NIST 800-171 and ITAR, and supports PII, PHI, GDPR, SOC 2 (SSAE-16), FISMA, FIPS 140-2, and EAR compliance among others.

In today's regulatory environment, where penalties can reach up to €20 million or 4% of annual global turnover under GDPR, Kiteworks' comprehensive compliance framework becomes a decisive competitive advantage. The platform's support for FedRAMP Moderate Authorization, combined with its ability to handle complex, multi-jurisdictional compliance requirements, enables organizations to meet evolving regulations like the EU AI Act and CMMC 2.0 Level 2—which Kiteworks supports for nearly 90% of requirements—while maintaining operational efficiency.

Product Compliance

Kiteworks is used by organizations across various industry sectors, including financial services, federal, state, and local government, healthcare, legal, pharmaceutical and life sciences, manufacturing, technology, and others in environments operating under compliance regulations. These include, but are not limited to, Data Protection Act (DPA), Network and information systems Directive (NIS2), Digital Operational Resilience Act (DORA) Cyber Maturity Model Certification (CMMC), the Health Insurance Portability and Accountability Act (HIPAA), General Data Protection Regulation (GDPR), the Federal Information Security Management Act (FISMA), Family Educational Rights and Privacy Act of 1974 (FERPA), the Financial Industry Regulatory Authority (FINRA), the Gramm-Leach-Bliley Act of 1999 (GLBA), the Sarbanes-Oxley Act of 2002 (SOX), International Traffic in Arms Regulations (ITAR), Export Administration Regulations (EAR), National Institute of Standards and Technology (NIST) 800-53, and NIST 800-171, among others. Thousands of cybersecurity (CISOs/CSOs), IT (CIOs), risk management, and compliance leaders rely on the Kiteworks Private Data Network to protect sensitive data communications and to remain compliant with regulations and laws like the above.

Thousands of organizations in highly regulated sectors—including defense contractors, healthcare providers, financial institutions, and legal firms—rely on Kiteworks' Private Data Network to secure their sensitive data and manage complex compliance mandates. The unified governance approach consolidates multiple data audit logs into one centralized system, eliminating the complexity where nearly half of organizations must consolidate over 11 separate logs associated with sensitive data exchanges. This consolidation directly addresses the finding that organizations implementing unified governance frameworks reduce compliance reporting time by 68% while improving security effectiveness through single-pane visibility that detects cross-channel threats that siloed solutions miss.

3. Using the Service

Ordering & Invoicing

Ordering

UK public sector customers can request a formal quote based on the published **G-Cloud 15 pricing** by contacting sales.gcloud@kiteworks.com. All quotes are issued strictly in line with the applicable G-Cloud 15 pricing and scope.

Once a quote has been provided and agreed, the customer places an order by issuing a **Purchase Order (PO)** referencing the approved quote. A valid PO is mandatory before the service can be activated.

The minimum contract term is **12 months**, with **1-year or 3-year** contract options available.

Customers may **increase user quantities during the contract term**. Where required, a **true-up model** can be made available on request. Reductions in quantities are not supported during the active contract term.

To place an order, customers must provide standard invoicing and contractual information, including:

- Approved quote reference
- Selected service tier(s)
- Quantities and products ordered
- Contract term length
- Customer invoicing details

Service Activation

Billing and service entitlement commence on the **contract start date**.

Provisioning and onboarding are aligned to the agreed contract start date and are delivered according to a **mutually agreed schedule** between Kiteworks and the customer.

Invoicing

Invoices are issued once the order has been processed, typically **within 24 hours** of order confirmation.

All invoices are:

- Issued **electronically**
- Denominated in **GBP**
- Payable within **30 days** from the invoice date

Where user quantities are increased during the contract term, additional charges are **pro-rated for the remainder of the contract period** and invoiced accordingly.

There are **no setup, onboarding, or implementation fees** associated with the service.

Availability of Trial Service

Kiteworks offers flexible evaluation options to ensure the platform meets your organization's specific requirements before committing to a full deployment:

Discovery Workshops: We provide discovery workshops to help organizations understand how Kiteworks addresses their specific security, compliance, and collaboration challenges. These workshops include demonstrations of relevant features, integration discussions, and requirements gathering sessions as well as a comprehensive exploration of the in-scope solutions & configurations.

Proof of Value (PoV) Exercises: For complex deployments or specific use case validation, Kiteworks offers structured Proof of Value exercises. These engagements include:

- Defined success criteria agreed upfront with key stakeholders
- Technical implementation support during the evaluation period

- Kiteworks G-cloud 15
- Regular checkpoint meetings to assess progress against success criteria

Documented outcomes demonstrating value delivery
15.

Introductory Support: During trial and PoV periods, customers receive dedicated technical support to ensure successful evaluation. This includes configuration assistance, integration guidance, and access to documentation and training materials.

Transition to Production: Upon successful completion of the evaluation, we provide a seamless transition path to production deployment, with all trial configurations and learnings incorporated into the implementation plan.

On-Boarding, Off-Boarding, Service Migration, Scope Etc.

On-Boarding Process

Kiteworks provides comprehensive on-boarding support to ensure successful adoption and rapid time-to-value:

Kick-Off Meeting: Upon contract execution, we schedule a kick-off meeting with key stakeholders including technical teams, security personnel, and end-user representatives to align on objectives, timeline, and success criteria.

Dedicated Resources: Each customer is assigned a dedicated Customer Success Manager (CSM) and technical implementation specialist who provide hands-on assistance throughout the on-boarding journey. This dedicated support continues through the first 90 days of service, with ongoing account management thereafter.

Implementation Support:

- Deployment planning and architecture review
- Integration with existing systems (LDAP/AD, SSO, DLP, SIEM)
- Configuration assistance & guidance per customer use case & requirements
- Guidance on data migration from legacy systems (where applicable)

Training and Documentation: Comprehensive training is provided for administrators and end-users, including live sessions, recorded webinars, and access to our extensive knowledge base. User adoption materials and change management guidance help ensure smooth rollout across the organization.

Testing and Validation: A structured testing phase ensures all requirements are met before production launch, including user acceptance testing and security validation.

Go-Live Support: Enhanced support is available during the go-live period to address any immediate issues and ensure business continuity.

Off-Boarding Process

Kiteworks facilitates orderly service transitions to minimize disruption:

Termination Notice: Customers must provide 30 days written notice of termination as specified in the contract terms.

Exit Planning: Upon receipt of termination notice, customers will retain full access to all data on the platform up until the point of license expiration. This data can be downloaded, deleted or otherwise retrieved based on the customers requirement as needed.

Training

Kiteworks provides comprehensive training to administrators of the platform via guided live-sessions with the Customer Success Team, bespoke recorded video guidance and via the knowledgebase & available help materials.

Kiteworks Customer Success will engage with the customer in the early instance in order to identify the preferred method of training for administrators and will work together to deliver a plan, ensuring the most effective & preferred training is delivered relevant to the customers unique use case & requirements.

End user training is also provided via the use of recorded videos & customizable help guides.

Implementation Plan

A detailed implementation plan can be provided to the buyer on request. The plan will include project timeline, resource allocation, integration requirements, testing phases, and go-live activities tailored to the customer's specific deployment model and use cases.

Service Management

Kiteworks is designed to be as easy to manage & administer as possible. Kiteworks is deployed as either a cloud hosted virtual appliance (hosted by Kiteworks or hosted by customer) or an on-premise virtual appliance. In all cases, the customer has full ownership of the data on the platform and of the administration of the platform itself. The customer is solely responsible for planning maintenance windows, applying updates via the one-click update process & managing configuration changes of the platform.

In the case of **Kiteworks Hosted** deployments, Kiteworks will manage the infrastructure itself. Administration, downtime,

Please treat this information as private and confidential.

Commented [BR2]: Scott to validate

Commented [ES3R2]: Done by Philipp

Service Constraints

Performance and Availability

Platform Availability: Kiteworks targets 99.9% uptime for cloud-hosted services, measured monthly excluding scheduled maintenance windows. Performance is monitored continuously with proactive alerting to maintain optimal service delivery.

Concurrent User Capacity: The platform is designed to support the licensed user count specified in the Order Form. Performance testing ensures the system maintains responsiveness under expected load conditions.

File Transfer Limits: Individual file transfers support up to 16 TB per file. Bulk transfer operations are optimized for high-volume scenarios with throttling mechanisms to ensure fair resource allocation across all customers.

Service Levels

Kiteworks shall provide support to Licensee in accordance with the following tiered approach:

Severity Level	Definition	Business Procedures
Level 1 Critical	An error on a properly configured environment that is reproducible and resulting in material functionality being unavailable or material loss of data	Response from time of receipt of Licensee’s error report to contact of Licensee with status report shall be four (4) hours. Kiteworks shall assign personnel to review and create work arounds for critical errors on a priority basis. Resolution: Kiteworks shall use reasonable efforts to resolve the critical error and/or provide a work around within forty-eight (48) hours from initial report of problem. Kiteworks shall provide status reviews to Licensee every eight (8) hours until such error is resolved
Level 2 High	An error on a properly configured environment, that is reproducible and resulting in severely restricted functionality.	Response from time of receipt of Licensee’s error report to contact of Licensee with status report shall be eight (8) hours. Kiteworks shall assign personnel to review and create work arounds for high level errors on a priority basis, subject to personnel deployed in resolving critical errors. Resolution: Kiteworks shall use reasonable efforts to resolve the critical error and provide a work around within seventy-two (72) hours from initial report of problem. Kiteworks shall provide status reviews to Licensee every eight (8) hours until such error is resolved.
Level 3 Medium	An error on a properly configured environment, that is reproducible and resulting in impact on non-material functionality or having a minor impact on material functionality.	Appropriate resources will be assigned during regular business hours to investigate problem and resolution. Resolution: Delivery of resolution will be prioritized for a scheduled release.
Level 4 Low	A non-reproducible error, an error which results in no material degradation of material functionality, or an inquiry type or clarification problem.	Appropriate resources will be assigned during regular business hours to investigate problem and resolution. Resolution: Delivery of resolution may be prioritized for a scheduled release.

Outage and Maintenance Management

Kiteworks provides a 99.9% uptime guarantee for Kiteworks hosted platforms, passed on from our hosting providers (AWS/Azure). Planning of outages for system maintenance / configuration changes is always owned by the customer as the customer retains complete control of the updates & maintenance of the platform regardless of the deployment model.

Financial Recompense Model for not Meeting Service Levels

Service Credits

If Kiteworks fails to meet the Up-Time Commitment, Customer shall have the right, as Customer’s sole remedy for such failure, to receive Service Credits pro rata to the amount of time Hosted Services are unavailable, subject to the exclusions above, after Service Credits are claimed in writing by Customer and the corresponding unavailability is confirmed by Kiteworks with the hosting provider. By way of example, if such unavailability is for twenty- four (24) hours, Customer shall be entitled to Service Credits equal to 1/365th of fees applicable to an annual License Term. Service Credits will be applied to any amounts due from Customer or if no amounts are due, Kiteworks shall pay Customer an amount equal to the dollar amount of Service Credits within thirty (30) days following the month during which Service Credits are earned. Service Credits shall not be awarded unless claimed within fifteen (15) days following the end of the month during which the corresponding unavailability occurred.

Support Hours

Kiteworks shall provide technical support by telephone seven (7) days per week, twenty-four (24) hours per day. Coverage is available by

- support@kiteworks.com
- [North America: +1-888-654-3778](#)
- [International: +1-650-485-4350](#)
- [Australia: +61 \(0\)2 7908 3819](#)
- [Germany: +49 \(0\)711 9533-9989](#)
- [Israel: +972 \(0\)2 374-0148](#)
- [New Zealand: +64 \(0\)4 831-0761](#)
- [Singapore: +65 3159 3269](#)
- [UK: +44 \(0\)20 3608-6370](#)

4. Provision of the Service

18.

Customer Responsibilities

Commented [BR4]: @Scott - any contractual obligations on the customer?

Technical Requirements and Client-Side Responsibilities

In all deployment models, the customer retains ownership and control of their data and configuration within the Kiteworks platform.

Kiteworks can be deployed either as a customer-hosted (on-premises or private cloud) solution or as a Kiteworks-hosted service. A Kiteworks-hosted deployment requires significantly fewer customer-side technical prerequisites, as infrastructure provisioning, platform operations, and core service management are handled by Kiteworks.

Where the service is deployed in a customer-hosted environment, the customer is responsible for providing, maintaining, and operating the required infrastructure and supporting services.

Customer Responsibilities – Customer-Hosted Deployments

For customer-hosted deployments, the customer is responsible for:

- Provisioning and operating the underlying virtual infrastructure (e.g. VMware or equivalent), including compute, storage, and networking resources
- Providing private IP addressing, DNS records, and network connectivity in line with documented requirements
- Implementing and maintaining required firewall rules and network access controls
- Supplying and maintaining SSL certificates for the application URL
- Providing an identity provider for authentication (SAML 2.0 and/or LDAP) and associated service accounts
- Providing and operating an SMTP relay for system email notifications
- Performing user and data administration within the platform, including ongoing user lifecycle management
- Managing end-user environments and local security controls
- Integrating and operating third-party technologies supplied by the customer (e.g. antivirus, DLP, SIEM, SMS gateways)
- Configuring and maintaining antivirus integration (mandatory); DLP and SIEM integrations are optional
- Developing, configuring, and maintaining any custom APIs, automations, or workflow integrations
- First-line troubleshooting by designated platform administrators

Kiteworks is not responsible for service issues arising from customer-managed infrastructure or third-party systems.

Customer Responsibilities – Kiteworks-Hosted Deployments

For Kiteworks-hosted deployments, Kiteworks is responsible for provisioning and operating the underlying infrastructure and core platform services.

Customer responsibilities are limited to:

- Providing identity provider details for SAML or LDAP integration
- Defining user roles, access policies, and organisational configuration
- Managing users and data within the platform
- Configuring business-specific settings, integrations, and workflows as required
- Supplying branding assets where custom visual branding is required

Certain advanced operational services and training may require a Premium Support package.

Identity, Integrations, and Third-Party Services

Kiteworks configures authentication integrations within the platform based on information provided by the customer. The customer remains responsible for the availability, configuration, and operation of their identity provider and any integrated third-party services.

Kiteworks does not assume responsibility for service degradation or failures caused by external systems, customer-managed infrastructure, or third-party technologies.

Technical Requirements and Client-Side Requirements

In all deployment models, the customer retains complete ownership & control of the data and configuration on the Kiteworks platform. In order to ensure effective deployment, the following requirements exist on the customer side:

- Provision of appropriate authentication service (Eg, Entra) & integration with the platform
- Provision of appropriate mail relay & integration with the platform
- User / data administration on the platform itself
- End user troubleshooting (Kiteworks support is provided to platform administrators)
- Configuration of custom API applications & automation workflows if/as required
- Management & integration of all third party technologies provided by the customer (Eg, SIEM, DLP, ATP, SMS gateway)

Outcomes/Deliverables

Deliverables

Upon successful implementation and ongoing service delivery, customers receive:

Platform Access:

- Fully deployed Kiteworks Private Data Network environment (in the case of Kiteworks hosted systems), with configuration supported by the Kiteworks Customer Success Team
- Full deployment assistance for the Kiteworks Private Data Network, supported by the Kiteworks Customer Success Team (in the case of on-premise / air-gapped deployments)
- Administrative console with complete governance and policy management capabilities
- End-user access via web interface, mobile applications, and desktop plugins
- API access for integration with existing enterprise systems (API license required)

Documentation and Knowledge Transfer:

- Comprehensive administrator guides and configuration documentation
- End-user training materials and quick-start guides
- Live / Webinar based administrator training
- Integration documentation for connected systems (LDAP/AD, SSO, SIEM, DLP)
- Further bespoke training and configuration assistance as required based on customer use case

Compliance and Security Artifacts:

- Relevant compliance certificates and attestations (SOC 2, ISO 27001, FedRAMP, etc.)
- Security audit reports and penetration test summaries (available upon request)
- Data processing agreements and GDPR-compliant documentation
- Detailed audit logs and compliance reporting capabilities

Support and Ongoing Service:

- 24/7 technical support with defined SLAs
- Regular platform updates and security patches
- Quarterly business reviews and account management
- Access to customer success resources and best practices
- "Hands-off" system updates performed by the Kiteworks support team (Premium support only)

Compliance and Governance:

- Simplified compliance demonstration for multiple frameworks (GDPR, HIPAA, CMMC, NIST, etc.)
- Automated policy enforcement across all communication channels
- Immutable audit logs providing evidence for regulatory audits and investigations
- Support for up to 90% of CMMC 2.0 Level 2 requirements for defense contractors

Cost Savings:

- Reduction in security and compliance tooling costs through platform consolidation
- Decreased breach risk and associated remediation costs
- Lower administrative burden through automation and unified management
- Elimination of redundant systems and associated licensing costs

Long-Term Strategic Outcomes

Digital Transformation Enablement: Kiteworks provides the secure foundation for organizations to confidently pursue digital transformation initiatives, enabling secure data sharing with partners, customers, and third parties without introducing unacceptable risk.

Regulatory Readiness: Organizations gain the ability to rapidly adapt to evolving regulatory requirements, with flexible policy frameworks and comprehensive audit capabilities that support compliance with current and future data protection regulations.

Trust and Reputation: Demonstrable commitment to data security and privacy through industry-leading certifications and transparent governance strengthens organizational reputation with customers, partners, and regulatory bodies.

Scalability and Future-Proofing: The platform scales seamlessly with organizational growth and evolving security requirements, protecting the technology investment and eliminating the need for costly replacements or major architectural changes.

All specific outcomes, success criteria, and measurable KPIs can be defined and agreed during the implementation planning phase and documented in the Order Form based on organizational priorities and requirements.

Development Lifecycle of the Solution

Kiteworks follows an Agile software development methodology with a secure software development lifecycle (SDLC) that prioritizes security, compliance, and quality throughout the development process.

Secure Development Approach

Kiteworks adheres to industry standards including the OWASP Software Assurance Maturity Model, implementing:

- Formal change management processes with separation of duties to ensure proper oversight
- Security-first design principles embedding data protection from initial concept through deployment
- Comprehensive quality assurance testing including functional, integration, and user acceptance testing
- Vulnerability scanning and security validation before all production releases
- Code reviews and static/dynamic application security testing to identify and remediate vulnerabilities

Agile Methodology

The Agile approach enables Kiteworks to rapidly adapt to:

- Evolving regulatory requirements and compliance frameworks
- Emerging security threats and vulnerability disclosures
- Customer feedback and feature requests
- Changes in the threat landscape and security best practices

Development is organized in iterative sprints, allowing for continuous improvement and flexible response to changing requirements while maintaining rigorous security standards.

Release Cadence

Major Releases: Four per year, delivering significant new features, enhancements, and capabilities

Minor Releases: Four per year, containing bug fixes, incremental improvements, and routine security patches

Security Patches: Additional patches deployed as needed when urgent security issues arise, typically within 48-72 hours of vulnerability identification

Emergency Patches: Critical security issues are addressed immediately with expedited testing and deployment

Cloud-Hosted Services: Updates are available via the “one-click” update process. The customer retains control and ownership of applying the updates to the system. Managed updating is available with the premium support model.

On-Premise Deployments: Digitally signed software packages are distributed through secure update servers with comprehensive release notes and upgrade documentation. Offline updates are available for air-gapped / offline deployments.

Quality Assurance

All releases undergo:

- Automated and manual testing across multiple environments
- Security validation and penetration testing
- Compliance verification against relevant frameworks (FedRAMP, FIPS 140-3, ISO 27001)
- Performance and scalability testing

This secure, agile development lifecycle ensures Kiteworks delivers reliable, secure, and compliant software that meets the evolving needs of customers in highly regulated environments.

Aftersales Account Management

Kiteworks is committed to building long-term partnerships with our customers through comprehensive account management and proactive customer success initiatives:

Dedicated Account Management: Each customer is assigned a dedicated Account Manager who serves as the primary point of contact for relationship management, commercial discussions, and strategic planning. Your Account Manager

Customer Success Support: Beyond your Account Manager, a Customer Success Manager (CSM) provides ongoing technical guidance, platform optimization recommendations, and proactive support to drive adoption and ensure your teams are leveraging Kiteworks capabilities effectively.

Regular Business Reviews: We conduct quarterly business reviews (QBRs) with key stakeholders to:

- Review usage patterns and adoption metrics
- Assess service performance against agreed SLAs
- Discuss challenges and identify solutions
- Share product roadmap updates and upcoming features
- Explore opportunities for expanded use cases or additional capabilities

Proactive Communication: Our account management approach includes:

- Advance notification of platform updates and new features
- Proactive outreach when usage patterns suggest optimization opportunities
 - Regular check-ins to ensure continued satisfaction
 - Escalation support for urgent business needs

Relationship Growth: We work collaboratively to identify opportunities that support your evolving requirements:

- Scaling to accommodate organisational growth
- Expanding into new use cases or departments
- Integrating with additional enterprise systems
- Supporting regulatory or compliance changes

Customer Retention Through Satisfaction: Our success is measured by your success. We prioritise customer satisfaction through:

- Responsive support and rapid issue resolution
- Continuous service improvement based on customer feedback
- Investment in features and capabilities that address customer needs
- Transparent communication and partnership approach

Feedback Integration: Customer feedback directly influences our product development roadmap. Through regular engagement, your Account Manager channels your requirements and suggestions to our product teams, ensuring Kiteworks continues to meet the evolving needs of our customer base.

Contract Management: Your Account Manager assists with contract renewals, service modifications, licensing adjustments, and any commercial or administrative requirements, ensuring a seamless experience throughout your partnership with Kiteworks.

Termination Process

Termination by the Customer

The customer may terminate the contract at any time by providing written notice to Kiteworks. To be effective, the termination notice must include the customer’s relevant account information and be sent by email to legal@kiteworks.com and renew@kiteworks.com.

Where termination is intended to take effect at the end of the current contract term, notice must be provided at least 90 days prior to the end of that term.

Termination by Kiteworks

Kiteworks may terminate the contract without prior notice if:

- The customer fails to pay applicable fees when due
- The customer otherwise breaches the express terms of the agreement
- Kiteworks is prevented from providing part or all of the hosted service due to the actions or failure of a third party outside Kiteworks’ reasonable control

Effect of Termination

Where the contract is terminated because Kiteworks is unable to provide the hosted service due to third-party actions, Kiteworks will refund any prepaid fees on a **pro-rata basis** for the unused portion of the service. In all other termination scenarios, the customer is **not entitled to a refund** of prepaid fees and remains liable for any applicable usage-based charges incurred prior to termination.

Upon termination:

- All licences granted under the contract immediately cease
- Customer access to the service is withdrawn following settlement of any outstanding charges
- The customer may no longer use the Kiteworks service

Any contractual provisions intended to survive termination, including payment obligations and relevant legal terms, will remain in effect after the contract ends.

5. Our Experience

Case Studies

Jaja Finance

Jaja Finance was founded in 2015 by three London-based Norwegian entrepreneurs with a goal of simplifying credit card usage for consumers. In recent years it has acquired the credit card businesses of the Bank of Ireland, the UK Post Office, and the UK Automobile Association to add to its Jaja-branded credit cards. According to Jim Newman, head of Information Security at Jaja Finance, the company initially chose Kiteworks to facilitate secure file sharing, primarily via the use of secure virtual data rooms (VDRs). After the first successful applications, Jaja opened up the Kiteworks platform to new use cases. “Every department uses it now,” Newman reports.

Leveraging Kiteworks for Multiple Use Cases: Today, Kiteworks usage at Jaja is as diverse as the company’s departments, tasks, and workflows, which include:

- Customer access to PII - In compliance with GDPR, Jaja gives customers 30-day access to their records using Kiteworks’ secure VDR.
- Workflow efficiency - Jaja uses Kiteworks’ application programming interfaces (APIs) to route information coming in from the Apache Airflow workflow management platform. Once analyzed by Airflow, the information is routed through Kiteworks to the appropriate team or person at Jaja, removing inefficient manual processes.
- Internal transfer of sensitive information - Newman and his team concluded Microsoft solutions are insufficient for sensitive data transfer. Instead, Kiteworks is the only approved solution for sharing credit card numbers internally. Jaja also transfers all customer call recordings internally using Kiteworks.
- Series funding - Jaja uses Kiteworks as a secure file repository for financing rounds. Kiteworks provides an integrated audit trail with detailed logs, so authorized Jaja employees are notified when a potential investor accesses or downloads prospectuses, financial tables, and other investment documents.
- Board communications - Jaja uses Kiteworks for secure communications between board members, who can easily and securely share confidential information before, during, and after meetings.
- Emailing sensitive information - Users upload customer lists in CSV format into Kiteworks and sends them to trusted third parties using Kiteworks secure email.
- Reassigning work of terminated contractors - Jaja leverages an integration with the JumpCloud directory platform and its LDAP functionality to reallocate Kiteworks folders created by temporary workers once they have left the company.

Realizing Significant Business Benefits: These extensive use cases have resulted in numerous direct benefits for Jaja:

- Ease of use - “We just had an onboarding session with the Kiteworks guys for a couple hours and then we were up and running, so we didn’t need any formal training,” Newman recalls. Ease of use was a key driver of high adoption throughout the company.
- Single sign-on (SSO) integration - Kiteworks is integrated with Jaja’s SSO solution, making it easier and more secure for users to sign in and access the platform.
- Responsive customer service - “The Kiteworks team is good at dealing with any problems and have an exceptional attention to detail,” Newman says. “You really get the sense that they care about their customers and want them to be happy with the product. That level of customer service is rare these days.”
- Transparent pricing - Newman contends that this is one of Kiteworks’ standout features. Jaja previously used a VDR provider to give consumers access to their private information. But Jaja was charged every time a customer accessed their data, which resulted in tens of thousands of pounds in unplanned usage fees. “We always know how many users we have and how much data is being transferred, so cost control is a piece of cake,” he explains.

Enjoying a Unique Partnership: “Nobody offers what Kiteworks does—the combination of virtual data rooms, simple file sharing and data transfer, and the flexible pricing that lets you shift the number of users up or down,” Newman asserts. “We have an excellent relationship and rapport with everyone we’ve dealt with at Kiteworks.”

Clients



Contact Details

For any queries regarding this service or G-Cloud opportunities, buyers may contact the Kiteworks G-Cloud team via: sales.gcloud@kiteworks.com.