Kiteworks

SOLUTION BRIEF

Your Data, Your Sovereign Control

Protect Private Data From Cloud Provider Access Risks With a Private Data Network (PDN)

Organizations exchanging sensitive data face increasing risks of access by cloud providers and foreign governments. In European markets particularly, where data sovereignty is paramount under GDPR and the NIS 2 Directive, conventional cloud services expose organizations to significant legal and compliance vulnerabilities through the U.S. CLOUD Act and similar extraterritorial legislation.

Kiteworks' Private Data Network (PDN) helps you control these risks by establishing complete data sovereignty, ensuring your sensitive data remains exclusively under your control regardless of where it's stored or processed. This approach safeguards against both cloud provider overreach and government surveillance, delivering true data ownership in an era of compromised privacy.

Architected for Security and Sovereignty

Single-Tenant Cloud: Security Without Compromise

Kiteworks eliminates many risks with a dedicated single-tenant architecture that provides:

- Complete isolation from other customers' data and traffic
- Exclusive infrastructure not shared with other organizations
- Dedicated security resources that focus solely on your environment
- Customizable security controls aligned to specific organizational needs

Hosted in Your/Your Partner's Data Center: Maximum Data Residency Control

For organizations with strict data residency requirements or those concerned about the U.S. CLOUD Act's jurisdictional reach, Kiteworks makes it easy for its customers to deploy its hardened virtual appliances themselves in their own data centers or cloud resources, or for their preferred managed service provider (MSP) to host it for them. This enables customers to:

- Keep all data within specific geographic regions
- Provide immunity from foreign data access requirements
- Deliver complete control over physical security measures

Data Sovereignty Solutions for Global Operations

European organizations must navigate complex data sovereignty requirements that vary by country. Kiteworks addresses these challenges through:

- Configurable geofencing that restricts access via IP address controls
- Regional data storage controls that ensure compliance with local regulations
- Granular controls that prevent unauthorized cross-border data transfers
- Comprehensive audit logs that document all data access and movement

Solution Highlights

Single-tenant cloud or on-premises

Air-gapped deployment option

Designed for data sovereignty

Built-in hardening and policy controls

Air-Gapped Deployment for the Highest Security Environments

Organizations with classified data or critical infrastructure face unique challenges implementing air-gapped environments. Kiteworks simplifies this process with:

- Self-contained deployment architecture requiring minimal external dependencies
- Off-line update mechanisms that maintain security without internet connectivity
- Internal certificate authority management
- Robust offline authentication mechanisms

Unified Platform: Secure Across All Data Exchange Channels

Unlike point solutions that address only SFTP or file transfer, Kiteworks provides a unified security framework across all data exchange methods:

- Protected file sharing with granular access controls
- Secure SFTP for automated system-to-system transfers
- Managed file transfer (MFT) with comprehensive security and audit capabilities
- Secure email exchange with encryption and DLP server integration capabilities

This unified approach ensures consistent security policies, simplified administration, and comprehensive audit log and reporting visibility across all data exchange channels.

Compliance Advantages for European Regulatory Requirements

Kiteworks' flexible deployment options deliver specific compliance advantages for European regulations, such as:

GDPR

The platform's data sovereignty features ensure personal data remains within appropriate jurisdictions while providing the necessary controls for data subject rights management and breach notification requirements.

NIS 2 Directive

Kiteworks' hardened virtual appliance architecture implements security-by-design principles required by NIS 2, with comprehensive audit logs that support mandatory incident reporting obligations.

SOC 2 Type II, ISO 27001/27017/27018

Kiteworks holds SOC 2 Type II certification, demonstrating its platform's effective controls for securing sensitive data across security, availability, confidentiality, integrity, and privacy. It is also ISO 27001, 27017, and 27018 certified, validating robust controls for information security, cloud security, and personal data privacy across its platform

Security by Design Across All Deployment Models

Regardless of the deployment model, a PDN implements security through:

- Encryption keys controlled by the customer, with no vendor access to data possible
- Hardened virtual appliance architecture that integrates multiple security layers
- Zero-trust principles applied to all services and data exchanges
- Comprehensive audit logs for all data access and transfer activities
- Role-based and attribute-based access controls aligned to NIST CSF, ISO 7001, and other frameworks

Organizations in healthcare, finance, legal, and government sectors rely on Kiteworks' deployment flexibility to secure their most sensitive data exchanges while maintaining regulatory compliance. The platform's adaptable architecture ensures security without compromise, regardless of deployment requirements or constraints.