Kiteworks

SOLUTION BRIEF

Zero-Trust Data Exchange

Secure Sensitive Information Beyond the Perimeter With Kiteworks

Every data access point creates potential risk. Traditional security approaches—those that implicitly trust users inside the network perimeter—leave organizations vulnerable to multiple data access risks, including external threats and internal misuse. Organizations need a more robust approach to protect sensitive information as it moves between employees, partners, and systems.

Kiteworks Zero-Trust Data Exchange revolutionizes data protection by implementing zero-trust principles at the data layer itself. This solution enables organizations to maintain control over sensitive information throughout its life cycle while facilitating secure collaboration. By combining double encryption, possessionless editing, and granular controls that persist with the data, Kiteworks creates a comprehensive security framework that moves with your information.

The Challenge of Traditional Data Exchange

Trust-based Data Access

Conventional trust-based data access focuses on protecting networks and applications, but not the most valuable business assets: your data. Similarly, one-time authentication implicitly grants broad access privileges by default, and because trust is assumed, it provides limited visibility into data movement and usage.

Data Protection Gaps

With protection focused on the perimeter, data inside it may be at risk due to inconsistent or weak encryption, static, coarse-grained access controls, and insecure data handling. Logging may be siloed, delayed, and incomplete, resulting in reactive threat detection and response. And once data is shared outside the perimeter, control and audit logging are lost.

Business Risk

These problems compound the risks of data oversharing and unauthorized access. Organizations are unable to maintain compliance and protect intellectual property, or prove who accessed what data, when. Even seemingly legitimate file sharing can result in data leaks.

The Kiteworks Zero-Trust Data Exchange Advantage

Kiteworks transforms this security paradigm through zero-trust data exchange capabilities:

Zero-Trust Data Access

Kiteworks verifies every access request rather than assuming implicit trust. By implementing data-centric security that operates independently of network location, organizations protect their information no matter where it resides. Granular, attribute-based access controls enable precise permissions management, while providing complete visibility into all data interactions.

Comprehensive Data Protection

Kiteworks protects data through double encryption at both file and disk levels, while enforcing secure data handling practices. It maintains complete audit logs of all data access, and proactively detects and responds to threats. Dynamic, context-aware access controls adapt to changing conditions, and organizations can retain persistent control over their data even after sharing it and collaborating with others.

Business Assurance

The platform enforces least-privilege data access by default while providing proof of who accessed specific files and when. Organizations can implement granular data governance policies and enforce need-to-know access requirements. Built-in compliance controls work alongside prevention mechanisms to stop unauthorized data movement, giving organizations comprehensive control over their sensitive information.

By implementing these comprehensive security measures, organizations can confidently share and collaborate on sensitive data while maintaining control and compliance. The Kiteworks Zero-Trust Data Exchange solution provides the tools needed to protect information assets in an increasingly complex threat landscape while enabling efficient business operations.

Kiteworks Zero-Trust Data Exchange Features

Always-verify Access Controls

- Role-based access
- Least-privilege defaults
- Data-based risk policies (ABAC)
- Continuous authentication and authorization
- SafeVIEW secure viewer
- SafeEDIT possessionless editing
- Granular folder/file permissions

Data-centric Protection

- Customer-owned keys
- Double encryption (file & disk)
- Data watermarking
- Secure data previews
- Automated DLP scanning
- Access expiration controls

Compliance and Governance

- GDPR/HIPAA reporting
- Data movement dashboard
- Custom risk policies
- Automated compliance monitoring
- Complete audit logs
- SIEM integration

Zero-Trust Architecture

- Tiered service isolation
- No admin OS access
- Open-source library sandboxing
- Embedded WAF
- Embedded network firewall
- Customer key management
- Secure build process

Continuous Monitoring and Validation

- Real-time activity tracking
- Comprehensive audit logging
- Intrusion detection system (IDS)
- Immediate threat alerts
- Geographic access monitoring

Kiteworks