Kiteworks Enhances Private Data Network With Trusted Data Format for Mission-Critical Data Security

Secure data exchange platform combining OpenTDF standards-based DRM & persistent encryption with FedRAMP High Ready status & comprehensive compliance controls

SAN MATEO, CA, UNITED STATES, November 20, 2025 /EINPresswire.com/ -- Kiteworks, which empowers organizations to effectively manage risk in every send, share, receive, and use of private data, today announced the integration of Trusted Data Format (TDF) capabilities into the Kiteworks Private Data Network—delivering standards-based digital rights management that embeds granular access controls directly within sensitive data files. The enhancement addresses a critical security gap for military operations, intelligence agencies, government entities, and critical infrastructure organizations that must maintain precise control over classified and sensitive information as it crosses organizational boundaries, dissimilar systems, and remote locations.

> This represents a fundamental shift of perimeter security from organization-level to file-level."
>
> *Yaron Galant, Chief Product Officer at Kiteworks*

Traditional file sharing methods fail when sensitive data leaves the sender's environment since protection doesn't travel with the data. Military operations transmitting intelligence from deployed sensors, government agencies sharing classified data across departments, and critical infrastructure operators transferring IoT data from remote field sites all lose control of their data the moment it leaves the site. Generic file sharing solutions and legacy enterprise platforms cannot enforce security policies that persist across organizational boundaries, creating exposure risks that threaten national security operations, regulatory compliance, and mission-critical infrastructure.

"Organizations operating in high-security environments face a fundamental challenge: How do you maintain control over sensitive data after it leaves your systems?" said Yaron Galant, Chief Product Officer at Kiteworks. "Consider an intelligence analyst sharing operational data with personnel across multiple theaters. Traditional security models break down because the protection doesn't travel with the data. Kiteworks' implementation of OpenTDF solves this by embedding attribute-based access control policies directly within the data file itself. Security

clearance levels, organizational affiliations, geographic restrictions, time-based access windows—all enforced regardless of where the data moves or which systems process it. This represents a fundamental shift of perimeter security from organization-level to file-level."

Standards-Based DRM With Persistent Encryption

Built on the OpenTDF (Open Trusted Data Format) standard, Kiteworks TDF provides standards-based digital rights management with persistent encryption and attribute-based access control (ABAC) that remains embedded within data files throughout their life cycle. Senders define precisely who can access their data based on custom attributes including security clearance level, organizational affiliation, location, operational role, and time windows. Intelligence data marked as Top Secret can be restricted to personnel holding appropriate clearances within specific geographic regions during designated operational periods.

The platform-independent nature of OpenTDF ensures interoperability across diverse technology environments without requiring recipients to use identical systems. Because access controls are embedded in the data file rather than relying on perimeter security, protection persists whether data crosses organizational boundaries, moves between agencies with different infrastructure, or travels to remote locations with minimal connectivity.

Key Access Service Validates Identity Before Granting Access

Kiteworks implementation includes the OpenTDF Key Access Service (KAS) and Policy Enforcement Point (PEP), which validate recipient identity and access privileges before granting data access. Organizations gain complete visibility into data usage through comprehensive audit logs tracking every access attempt—supporting compliance requirements including CMMC, FedRAMP, FISMA, and HIPAA.

Users access TDF-protected data and the policies governing it through the familiar Kiteworks interface alongside standard files, eliminating workflow disruption while maintaining robust security controls. The solution integrates with existing Kiteworks capabilities, including FedRAMP High Ready status.

Mission-Critical Security Across Five Key Sectors

Kiteworks TDF addresses specific security requirements across critical sectors:

- Military operations maintain precise control over intelligence and operational data transmitted from deployed systems, sensors, and personnel across all theaters to authorized command elements—ensuring only cleared personnel with appropriate need-to-know access mission-critical information.

- Government agencies securely share sensitive government data across departments and partner organizations while maintaining strict access controls and supporting compliance with federal security requirements.

- Critical infrastructure operators securely transfer IoT data from sensors and equipment in remote locations such as oil fields, dam sites, and telecommunications facilities to designated analysts and decision-makers at processing centers.

- Healthcare organizations transfer medical records and research datasets between hospitals, clinics, researchers, insurance companies, and other entities while enforcing HIPAA compliance and preventing data breaches.

- Financial services firms securely share financial transaction data, records, and audit logs between institutions, regulators, and partners with granular control over access and comprehensive audit capabilities.

Transforming Data Protection From Perimeter to Persistent
"The organization-level security perimeter has dissolved in modern operations," concluded Galant. "Military units operate across theaters with different network infrastructures. Government agencies collaborate across organizational boundaries. Critical infrastructure spans remote locations with varying connectivity. The old model of protecting data at the organization's perimeter simply doesn't work when fragmented data must cross these boundaries to support mission objectives. Kiteworks TDF fundamentally changes the equation by making security an inherent property of the data itself. Access policies travel with every file. Encryption persists across every system boundary. Compliance validation occurs at every access attempt. Organizations finally have the certainty that their most sensitive data remains protected and controlled regardless of where it travels—transforming data security from a network boundary problem into a data-centric solution."

Learn more about Kiteworks Trusted Data Format by reading the solution brief.

About Kiteworks
Kiteworks' mission is to empower organizations to effectively manage risk in every send, share, receive, and use of private data. The Kiteworks platform provides customers with a Private Data Network that delivers data governance, compliance, and protection. The platform unifies, tracks, controls, and secures sensitive data moving within, into, and out of their organization, significantly improving risk management and ensuring regulatory compliance on all private data exchanges. Headquartered in Silicon Valley, Kiteworks protects over 100 million end-users and over 1,500 global enterprises and government agencies.

David Schutzman
Kiteworks
203-550-8551
email us here
Visit us on social media:
LinkedIn
Facebook

YouTube
X
