# Top 7 Reasons to Select Kiteworks Over ShareFile

## Strongest Content Risk Management and Compliance

Whether you store your sensitive data in the cloud or on your own premises, Kiteworks combines the best productivity with the strongest protection from the risks of breaches and noncompliance, even when collaborating with third parties.

### 1. No Vendor Access to Metadata or Content, Ever

Kiteworks hosted and on-premises systems have layers of protection designed so Kiteworks employees—and external attackers—cannot access any of your content or metadata. With ShareFile, the vendor has access to your metadata that describes your files, policies, and users—even if you use on-premises StorageZones—and they can access your content when it's hosted in their cloud.

### 2. Built-in Hardening That Keeps Insiders and Attackers Out

Kiteworks provides unmatched virtual appliance hardening with a built-in network firewall, WAF, and intrusion detection. An ongoing bounty program and regular pen testing, along with one-click appliance updates, minimize vulnerabilities. With ShareFile on-premises StorageZone Controllers, however, no hardening is provided to protect the system from internal or external attackers, so admins have access to the files, operating system, and application code. Their updates must be done manually for each component, increasing maintenance costs and the risk of missing security patches.

### 3. Comprehensive Audit Log Feed to SecOps and Compliance Teams

Kiteworks unifies all component logs into a single, continuous stream to your SIEM for threat detection and mitigation, in addition to domain-specific and custom reporting. The thorough audit log helps ensure you pass compliance audits with the minimum effort. In contrast, ShareFile provides only a scattering of separate topical reports that admins must schedule, run, and export; it has no live feed to Splunk, Datadog, ArcSight, or other SIEMs.

### 4. CMMC- and Agency-ready U.S. Federal Compliance

Kiteworks encryption has passed the rigorous NIST FIPS 140-2 validation certificate process, and the cloud-hosted product and processes undergo yearly FedRAMP audits and continuous monitoring by a certified third-party assessor (3PAO). ShareFile lacks FedRAMP authorization and NIST validation for FIPS 140-2.

### 5. Possessionless Editing to Manage Collaboration Risk

Kiteworks SafeEDIT next-generation digital rights management (DRM) enables editing of shared files of any type by internal and external parties in a browser virtual UI, while the file itself stays protected in the Kiteworks server cluster. No agents or plugins are needed. With ShareFile, you must give third parties possession of your sensitive content to edit it, whether via the Microsoft 365 cloud or via download.

## 6. Absolute Privacy With Single-tenant Cloud Hosting

Reduce the risk of unintended or unauthorized content access with an independent Kiteworks private cloud for each customer, with no intermingling of data, metadata, or shared application resources. ShareFile's multi-tenant cloud, on the other hand, intermingles your data and metadata with that of other customers, leading to the risk of a security breach between tenants in the case of software bugs and configuration errors.

## 7. Secure Large File Sharing for Compliant Productivity

Reliably and securely encrypt, send, share, receive, scan, view, and save data-intensive, imaging, CAD, and other types of files up to 16 terabytes in size. When networks fail, transfers restart where they left off. ShareFile's 100 GB size cap, on the other hand, incents users to revert to other insecure forms of communication when their business process utilizes larger files.