



SAFEGUARD SENSITIVE LEGAL DATA BEYOND THE NETWORK

Ensure client files, contracts, and case materials remain protected, even after sharing, downloading, or forwarding.

The Current State

Legal teams collaborate across clients, opposing counsel, expert witnesses, and third-party service providers. Sensitive files like case folders, contracts, evidence, client data are shared constantly through email, shared drives, and data rooms.

Traditional security tools often stop at the perimeter. If a document is downloaded or forwarded, control disappears. Access isn't revoked when cases close, and there's no visibility into who saw what, when, or where. This creates unnecessary exposure, client risk, and compliance challenges.

A Smarter Way to Protect Data

Keyavi SafeSuite gives legal teams unprecedented control over sensitive documents by embedding access policies directly into the data itself. With SafeSuite, files are encrypted and bound to customizable rules, such as who can open them, where, when, and how. This allows firms to securely share contracts, discovery materials, and client files with external parties while retaining the ability to revoke access, track usage, and enforce policies. Even if a document is forwarded or downloaded, protection remains intact and adaptive, reducing the risk of data leaks, unauthorized use, or mishandled privileges.



Data-Centric Protection

Govern data with granular policies on who can access it, when, where, and how., even after download or sharing.



Secure Sharing with Clients

No special software required for recipients to open protected files. Works with existing workflows for smooth end user experience.



Automatic Expiration

Set expiration dates aligned with case timelines. Instantly revoke access at any time.



Immutable Audit & Logging

Track every access attempt (successful or blocked) for audit confidence.

Traditional Approaches

- Protects only within your environment
- No control after sharing
- Unclear who accessed what
- Forgotten access after case closes
- Over-permissioned folder access with broad visibility

With SafeSuite

- Embedded protection travels anywhere
- Revoke or update access after sharing
- Full forensic audit logs
- Expiration tied to case timelines and NDAs
- Granular file-level permissions for users with adaptable policies

Use Cases

- Client Document Exchanges
- E-Discovery Production
- M&A Legal Document Review
- Expert Witness File Sharing
- Contract Negotiation & Redlining
- External Counsel Sharing

Case Study

Situation

A mid-sized corporate law firm struggled to control sensitive files once shared outside the firm. Password-protected PDFs and client portals offered no post-sharing control, no visibility into who access files, and no way to stop forwarding or downloading.

Solution

With SafeSuite, the firm gained ability to restrict access by user, geography, and time, revoke access instantly, and log every attempt to open a file, even after download. The solution was deployed within a day and required minimal training.

Results

- Reduction in IT time managing permissions
- Full audit trail for all shared files
- Easier, seamless, safer collaboration for attorneys and clients
- Increased trust in legal matters

Client trust starts with data control. Discover how SafeSuite protects legal files wherever they go. Contact info@keyavi.com to arrange a demo today.