



ACCELERATE DEALS WITHOUT COMPROMISING DATA

Fine-grained access and built-in policies keeps your data room secure, even after sharing and downloading.

Challenges with Data Rooms

Traditional data rooms often grant broad access: once someone is approved, they can see every file within a folder. After the deal or project ends, access is rarely revoked, leaving sensitive information unnecessarily exposed. When files are downloaded, protection stops, and there's little to no visibility into what happens next. Without insight into who viewed or shared the data, organizations are left with lingering risk that threatens deals, trust, and the bottom-line.

The SafeSuite Advantage

Keyavi SafeSuite redefines how data rooms are secured by embedding access policies directly into each file. Instead of broad folder access, admins can grant granular, file-level permissions, like read-only rights, geolocation restrictions, and auto-expiration. Even after download, access stays controlled and every attempt is logged. This keeps sensitive deal data protected, visible, and controllable, so teams can move faster while reducing risk.



Fine-Grained Access Control

Allow view/edit for specific users at both the file and folder level. No more all-or-nothing access.



Data-Centric Protection

Files carry policies governing who can access it, when, where, and how. This protection remains even after download or sharing.



Auto-Expire & Revoke

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



Full forensic visibility

Monitor every access attempt, successful or blocked, with details like time, location, and device.



Ease of Use

Deploy in minutes with no complex integrations or infrastructure. Works with existing workflows for seamless end user experience.

Why securing your data room matters

- ✓ Reduce exposure risk. Granular access and auto-expiry means fewer over-privileged users.
- ✓ Stay secure. Keep sensitive files safe even after downloading and external sharing.
- ✓ Improve deal confidence. External parties can access what they need, but you retain control.
- ✓ Meet compliance and audit needs. Maintain detailed logs, revocation trails, and adaptive policies.
- ✓ Support collaboration with external investors, advisors, and vendors without giving global access.

	Standard Data Rooms	SafeSuite Protection
Access Granularity	Folder level only, broad "all or nothing" access	File-level, policy-specific
Post-Download Protection	None/limited	Full persistent protection
Auto-Expiry	Manual clean-up	Built-in auto-expiry & instant revoke
External Sharing	High friction	Low friction
Forensic Visibility	Basic logs	Detailed logs

See it in action. Request a live walkthrough of how SafeSuite can transform your secure data room strategy. Contact us at info@keyavi.com today.