CyberGrant
SECURITY MADE EASY

WHITE PAPER

Secure File Sharing in the Enterprise: Control and Encryption

From Real-World Risks to Effective Governance with FileGrant by CyberGrant

Index

Executive Summary

In today's digital landscape, secure data sharing is a fundamental driver of competitiveness.

Industry research shows that organizations that implement effective file sharing processes significantly reduce operational delays, errors and costs, while maintaining full traceability of activities.

Smooth collaboration with customers, partners and suppliers, combined with the protection of documents even outside the corporate perimeter, becomes a measurable competitive advantage in terms of efficiency and time to market.

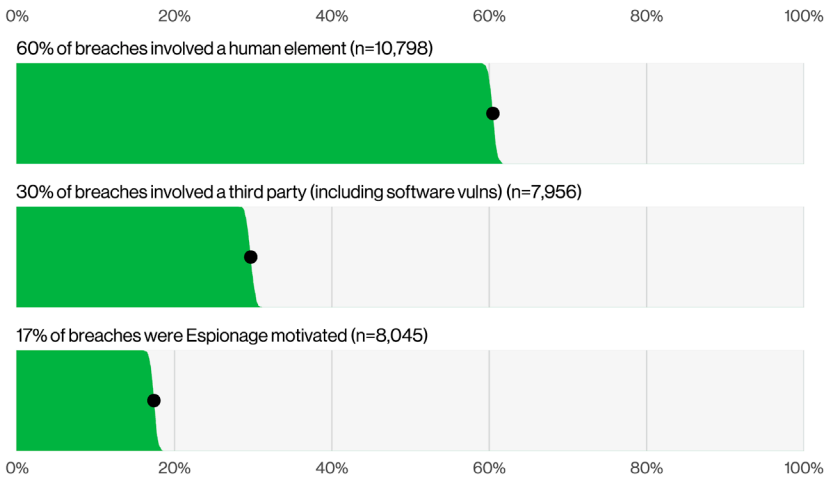
The Threat Landscape: Alarming Data

In 2025 Verizon analyzed 22,052 incidents and 12,195 confirmed breaches across 139 countries.

The human component remains decisive (around 60 percent) and cases involving third parties have doubled, while breaches motivated by espionage account for 17 percent. These trends confirm that human error, excessive permissions and supply chain dependencies are key exposure vectors.

60%

Human components
in data breaches



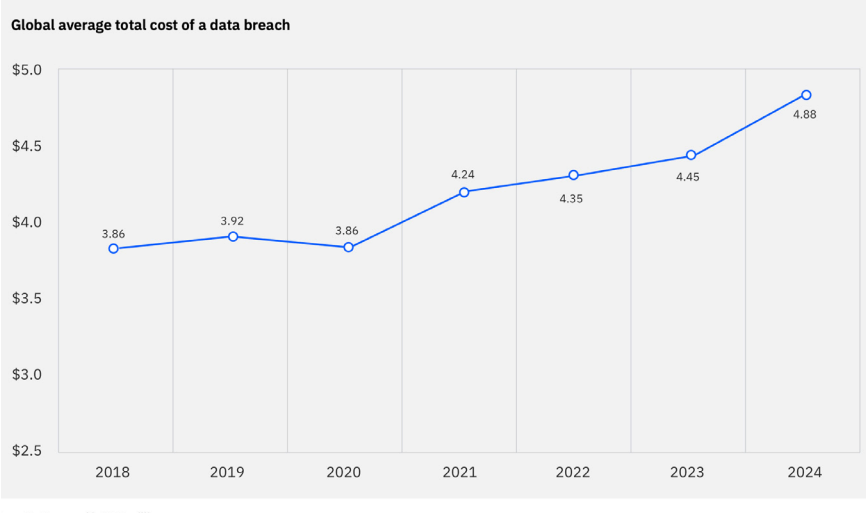
Source: https://www.verizon.com/business/resources/reports/2025-dbir-executive-summary.pdf

The Cost of Breaches: A Major Economic Impact

IBM's Cost of a Data Breach 2024 report quantifies the global average financial impact of a breach at **4.88 million USD**, while for **financial services** the figure reaches **6.08 million USD**. Incidents involving internal actors and compromised credentials are among the most expensive and complex to manage, because they combine longer detection times with broader exfiltration surfaces.

4,88 million USD

Global average financial impact of a breach



Source: Cost of a Data Breach Report 2024

Secure Sharing as a Tool for Compliance and Governance

Secure file sharing is not only a competitiveness issue. It is also a **non negotiable regulatory requirement**. Under GDPR, NIS2 and DORA, being able to prove a clear data chain of custody, minimization criteria and adequate encryption makes audits and regulatory adherence significantly easier. Proper access management, combined with monitoring and control mechanisms, reduces exposure to fines and litigation.

File Sharing: Risk Vector or Governance Opportunity

In this context, **file sharing is at the same time a risk vector and an opportunity** to strengthen governance. Sensitive data travels across cloud services, email, chat platforms and unmanaged tools, often without adequate encryption, monitoring and controls.

At the same time, file sharing can become an opportunity to strengthen governance when it is managed through **tools that make it natural for users to comply with corporate policies**.

Experience shows that intuitive tools reduce so called shadow IT, the tendency of users to rely on unauthorized channels in order to bypass complex processes.

Strategic Recommendations

To effectively address the challenges of secure data sharing, this guide proposes solution selection criteria, compares operational best practices and outlines an implementation roadmap tailored to the needs of large organizations.

The goal is to give business decision makers the tools they need to turn file sharing from a potential vulnerability into a competitive advantage, balancing security, compliance and productivity in a single strategic framework.

What Enterprise File Sharing Looks Like Today

Enterprise file sharing covers very different scenarios. There are tools integrated into productivity suites, privacy centric solutions and platforms for structured exchanges. Understanding the main families helps you choose the right balance between usability and data control.

Solution Families

There are four main families.

1. EFSS solutions, that is **Enterprise File Sync and Share** tools in suites like Microsoft 365, focus on collaboration and versioning.
2. Solutions with **client side encryption and zero knowledge** models prioritize key control by the organization.
3. MFT solutions, that is **Managed File Transfer** platforms, govern structured and recurring exchanges with strict traceability.
4. Ad hoc transfers via **public services or email** offer speed but very little control after download.

How Organizations Actually Use File Sharing

Organizations share content with internal teams and third parties across the supply chain. Value comes from fluidity. Risk comes from loss of control. Balancing these two aspects is the real objective.

Internal and External Collaboration

Internal collaboration involves departments, project teams and committees working on documents, presentations, technical drawings, medical reports and contracts. External collaboration includes customers, partners, law firms, suppliers and auditors. It can be synchronous, such as co authoring during meetings, or asynchronous, such as controlled exchanges and subsequent reviews. Environments can be managed by the company, or unmanaged when people work on personal devices or partner devices.

Employee Behaviors

Shadow IT: : the use of tools, applications and services that are not approved by corporate IT to share or store files, without centralized controls, audit trails, consistent policy enforcement and continuous protection.

Garbage collection: the uncontrolled build up of copies, attachments, versions and links outside governance in personal clouds, chats and email inboxes. It prevents people from identifying the latest version, hinders revocation and deprovisioning and puts compliance and the chain of custody at risk.

People look for the easiest way to get work done. When the official tool is complex, shadow IT emerges, meaning the use of non approved channels.

A second phenomenon is garbage collection, understood as the chaotic accumulation of copies, versions, attachments and links outside governance. These leftovers increase the attack surface, complicate discovery during audits and disrupt collaboration when links expire without traceability.

Security Risks and New Attack Surfaces

The file sharing attack surface grows with federated identities, cloud applications and artificial intelligence. Many incidents start from configuration errors and stolen credentials. Ransomware and extortion with data exfiltration remain rising trends, along with vulnerability exploitation and dependence on third parties.

The human factor is confirmed as the predominant root cause. In the latest Verizon DBIR 2024 report the human component is involved in more than two thirds of breaches. This figure highlights the value of controls that reduce opportunities for error and make safe choices easier for users.

Generative AI increases visibility when permissions are not properly configured. When you connect bots or agents to repositories and sharing platforms, the model can access and resurface everything it is authorized to see. Overly broad or inconsistent permissions can lead to disclosure of content that was never meant for those users.

The OWASP community has cataloged the main specific risks, such as prompt injection that manipulates model instructions, insecure output handling when results are reused without validation, and software supply chain vulnerabilities in plugins and connectors. For file sharing this means carefully verifying integrations between bots, agents and document repositories, enforcing the principle of least privilege on permissions and validating model output before it triggers sharing or actions that could bypass the intended governance.

One of the less visible vectors is **screen capture during calls and automatic meeting recordings**. Without adequate defenses, a confidential document can leave your control without leaving a trace. Anti screenshot protection on the viewer side reduces this silent leakage.

Compliance and Chain of Custody

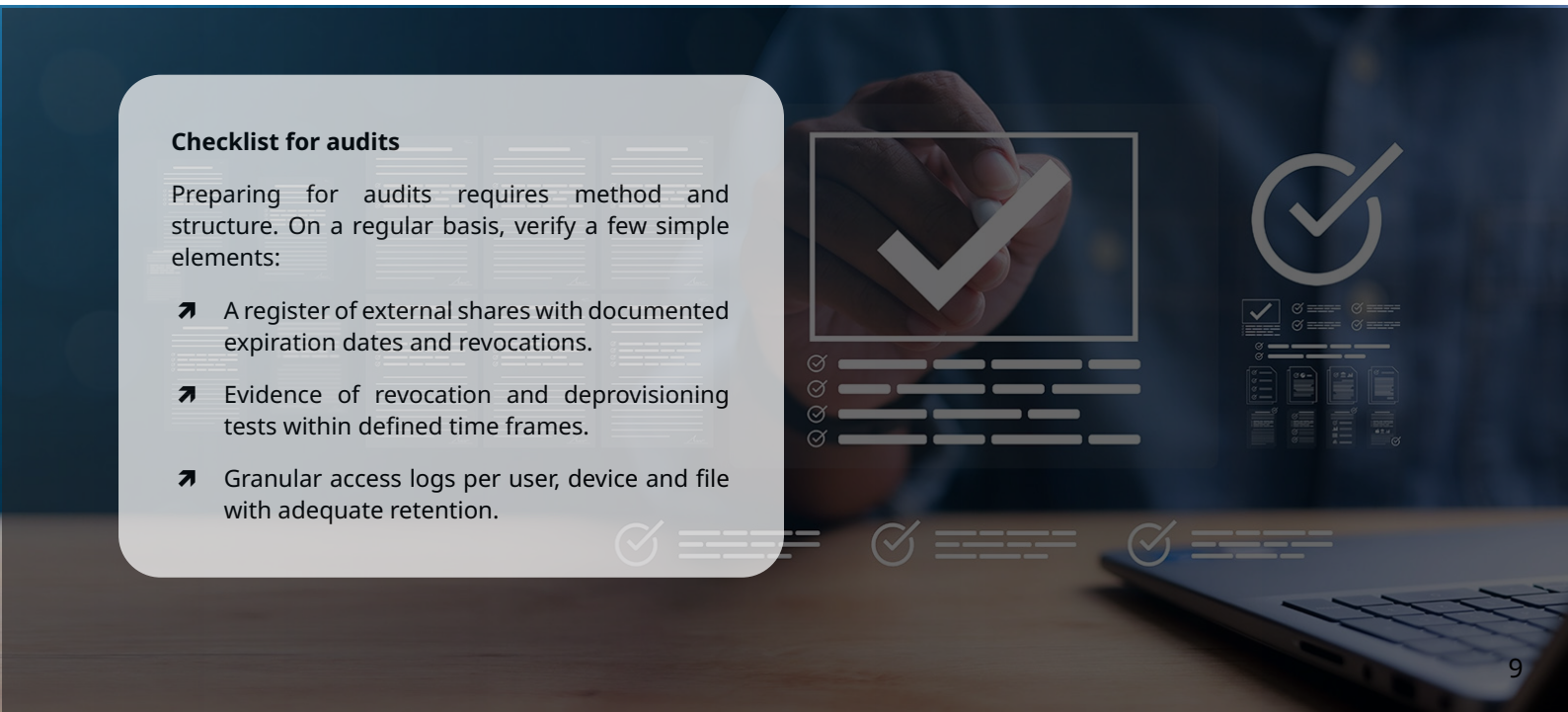
Compliance lives on evidence.

GDPR (General Data Protection Regulation) requires adequate technical and organizational measures, including encryption, impact assessments and records of processing activities.

NIS2 (Network and Information Security Directive) strengthens security obligations and introduces specific responsibilities for essential and important entities.

DORA (Digital Operational Resilience Act) imposes on the financial sector requirements for digital operational resilience, management of third party ICT providers and incident reporting.

The chain of custody is the complete and tamper proof trail of who created, opened, modified or shared a file, when and from which device, with which authorizations, including versions, revocations, expirations and access logs. To build it, you start from principles: minimization and versioning reduce unnecessary copies; tracking and audit trails document every step; key management adopts BYOK (Bring Your Own Key) and CSE (Client Side Encryption) up to a zero knowledge model in which the provider has no access to the keys. Clear roles across IT, security, the DPO and vendors define who decides, who executes and who verifies.



Checklist for audits

Preparing for audits requires method and structure. On a regular basis, verify a few simple elements:

- A register of external shares with documented expiration dates and revocations.
- Evidence of revocation and deprovisioning tests within defined time frames.
- Granular access logs per user, device and file with adequate retention.

File Sharing and Recurring Issues in Organizations

The following scenarios occur frequently and create exposure. Addressing them with clear procedures and technical controls immediately reduces risk and improves user experience.

- **Public links that escape control** When a link that is accessible to anyone continues to circulate, the owner loses visibility. The technical solution is authentication via email and one time code, plus automatic expirations and revocations. The organizational solution is a publishing policy with approvals and periodic reports.

- **Unencrypted attachments and local copies** Attachments in clear text and files exported to desktops expand the attack surface. The technical solution is enforcing always encrypted downloads with a protected viewer. The organizational solution is a single, standard procedure for external sending.

- **Divergent versions and garbage collection** Copying and renaming creates remnants that are hard to track. The technical solution is centralized versioning and corporate tags with inheritance. The organizational solution is clear ownership and scheduled cleanup.

- **Invisible leaks via screenshots and recordings** Screen capture during meetings is a silent exfiltration channel. The technical solution is blocking capture at the viewer level and using dynamic watermarks. The organizational solution is a meeting policy with clear restrictions and explicit notices to participants.

- **Exposure through AI tools** Unmanaged bots can read excessive content. The technical solution is enforcing permissions and tags for the corporate AI and enabling anti scraping protections. The organizational solution is a registry of authorized tools.

Criteria for Choosing a Solution

> *"The primary criterion is persistent control over the file even after download"*

When you choose a file sharing platform, **you need to balance security and adoption**. If users do not adopt it because it is cumbersome, they will fall back to email, public links and non authorized tools.

1. **The primary criterion is persistent control over the file even after download.** This means that even if a document leaves the corporate environment, you can still limit its use, set expirations, revoke access and prevent copying or printing. In practice, ask yourself: if a supplier saves a local copy tomorrow, can I still block it or not.
2. Right after that, **end to end encryption along the entire path is crucial**. In transit, when the file is moving. At rest, when it is stored. On the client side, before it leaves the device, with keys managed by the organization. That way, even if someone intercepts or exports the file, the data remains unreadable.
3. **Access governance** defines who sees what and under which constraints. Roles, labels or tags enforce consistent rules. Expirations and revocations close access at the right time. Watermarks and blocks on printing, copying and downloading reduce abuse and help during audits.
4. **Operational defenses** are the controls that act during use. A protected viewer allows you to let people read documents without handing over a usable copy. AI protections reduce scraping risks and prevent unauthorized reuse of content by connected bots and agents.
5. **Usability and integrations determine adoption speed**. Tight integration with Microsoft 365, the IdP (Identity Provider), SIEM (Security Information and Event Management) and CASB (Cloud Access Security Broker) removes friction and reduces shadow IT. Users can work where they are used to working, but with rules and full tracking in place.

FileGrant and DLP Extended to the Cloud with AIGrant

Data Loss Prevention must follow the file everywhere. FileGrant integrates AIGrant, **CyberGrant's private AI that creates specialized agents to automatically classify documents**, apply tags and assign roles based on corporate rules. This makes it possible to extend DLP to cloud repositories and documents shared outside the organization, with policies that automatically enforce encrypted download, anti capture, copy limits and expirations.

For high value data, the organization can adopt client side encryption with autonomous key management. In this way, **content remains inaccessible outside authorized devices and identities**, even in environments with multiple vendors and tools.

Come funziona FileGrant

FileGrant ENTERPRISE

FileGrant by CyberGrant combines ease of use and advanced controls to make sharing secure without slowing down the work.

Encryption that follows the file Downloads always take place in protected format with Lock&Go technology based on secure PDF. Files protected in this way remain usable only by authorized users and revocations remain effective even after sending.

Long term protection and key management FileGrant supports post quantum encryption with CRYSTALS Kyber key exchange, selected by NIST, and a zero knowledge option in which the organization retains full control of the keys.

Access control with roles and absolute priority tags Roles define what each profile can do. Tags enforce restrictions that override any permission. For example, the no download tag prevents saving in clear text even for editors. Rules can be inherited from folders and activate limits such as view only, anti capture and watermarks.

Proprietary viewer with AI protections The viewer opens documents in read only mode and blocks screenshots and screen sharing during calls. AI protections prevent content from being captured by unwanted artificial intelligence tools.

Simple but fully tracked sharing Links are protected through email and one time codes, expirations and immediate revocations. Alternatively, external sending via protected PDF remains synchronized with the permissions of the original file. QuickShare enables urgent transfers without losing audit trails and control.

Intuitive interface that reduces shadow IT Bulk uploads, drag and drop, automatic tagging and versioning encourage users to rely on the official tool instead of resorting to non approved channels.

End to garbage collection Every transfer is monitored and recoverable. Tags, versioning and always encrypted downloads prevent unmanaged copies and scattered attachments.

Real World Use Cases Solved with FileGrant

Healthcare: protecting reports and sensitive data at every stage of sharing

Context

A multi specialty medical center shares reports and diagnostic attachments with patients, external specialists and insurance companies.

Problem

Inoltri via e-mail e download in chiaro aumentano il rischio di violazioni e accessi impropri durante consulti remoti.

Solution with FileGrant

- AI Classification detects healthcare data and automatically applies a dedicated tag that enforces opening in a protected viewer, blocks clear text download and activates anti capture. Access is granted via email and one time code, with expirations, revocations and full audit. AI features are enabled only for authorized roles.

Result

Reduced risk of data breaches, complete traceability of consultations and support for GDPR compliance and healthcare requirements.

Manufacturing: protecting drawings, IP and know how across the supply chain

Context

A manufacturer shares CAD drawings and bills of materials with suppliers and partners.

Problem

Loss of control after download and unauthorized distribution of critical information.

Solution with FileGrant

- Automatic classification marks files as trade secrets. RBAC and tags enforce download only as protected PDF for internal and external editors and view only for suppliers, with enforced anti capture. Tags are inherited from folders and override every other permission. Logs and timestamps guarantee a complete chain of custody.

Result

Smooth collaboration with third parties without giving up control, with full traceability and IP protection across the entire document lifecycle.

Conclusion.

Fast Sharing, Substantive Security, Demonstrable

FileGrant brings the simplicity of file sharing into a framework of substantive security.

In a context where every file can act as a risk vector, and where collaboration, compliance and visibility are strategic criteria, it is no longer enough to simply “share”. You need to share in a secure, governed and collaborative way.

With FileGrant, file sharing becomes a strategic asset: advanced protection, controlled collaboration, verifiable governance.

If you want to give IT, security and compliance teams a platform that delivers visibility, control and real collaboration, it is time to discover FileGrant.

www.cybergrant.net