CyberGrant
SECURITY MADE EASY

WHITE PAPER

Filesharing in azienda, controllo e cifratura

Dalla realtà dei rischi alla governance efficace con FileGrant di CyberGrant

Sommario

Executive summary

Nel contesto digitale odierno, la condivisione sicura dei dati rappresenta una leva di competitività fondamentale.

Secondo le analisi di settore, le organizzazioni che implementano processi efficaci di file sharing riducono significativamente ritardi operativi, errori e costi, mantenendo al contempo piena tracciabilità delle operazioni.

La collaborazione fluida con clienti, partner e fornitori, unita alla protezione dei documenti anche al di fuori del perimetro aziendale, costituisce un vantaggio competitivo misurabile in termini di efficienza e risposta al mercato.

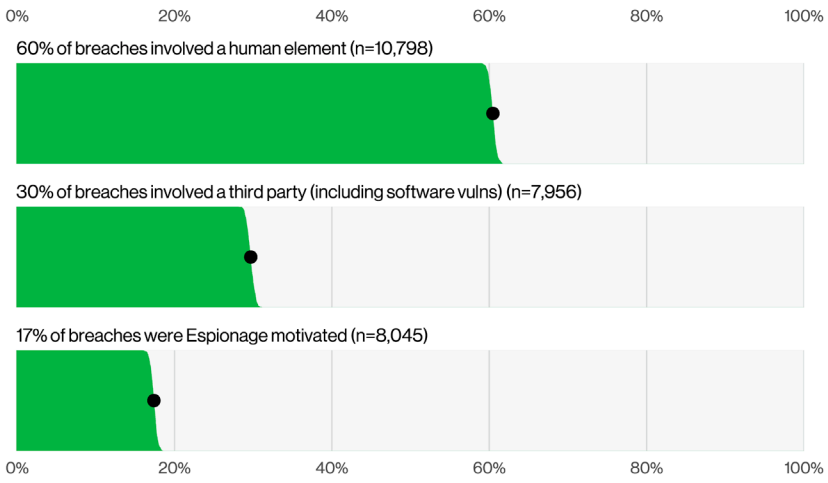
Il panorama delle minacce: dati allarmanti

Nel 2025 Verizon analizza 22.052 incidenti e 12.195 violazioni confermate in 139 paesi. **La componente umana resta decisiva** (circa il 60 percento) e i casi che coinvolgono terze parti raddoppiano, mentre i breach motivati da spionaggio toccano il 17 percento.

Questi trend confermano che errori, permessi eccessivi e dipendenze dalla supply chain sono vettori chiave di esposizione.

60%

Componenete umana
nelle violazioni dei dati



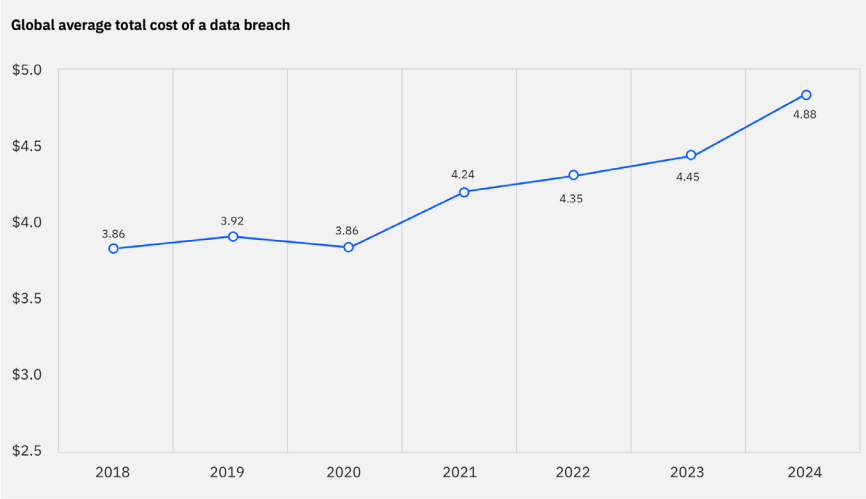
Fonte: https://www.verizon.com/business/resources/reports/2025-dbir-executive-summary.pdf

Il costo delle violazioni: un impatto economico rilevante

Il rapporto **Cost of a Data Breach 2024 di IBM** quantifica l'impatto finanziario medio globale di una violazione in **4,88 milioni di USD,** mentre nei servizi finanziari la cifra raggiunge i **6,08 milioni USD**. Gli incidenti che coinvolgono attori interni e credenziali compromesse rientrano tra i più costosi e complessi da gestire, poiché combinano tempi di scoperta più lunghi con superfici di esfiltrazione più ampie

4,88 milioni di USD

Costo medio globale di una violazione



Fonte: Cost of a Data Breach Report 2024

La condivisione sicura come strumento di compliance e governance

La condivisione sicura non è solo una questione di competitività, ma rappresenta un requisito normativo imprescindibile. Secondo gli standard GDPR, NIS2 e DORA, dimostrare una chiara catena di custodia dei dati, criteri di minimizzazione e cifratura adeguata facilita audit e aderenza ai regolamenti. La corretta gestione degli accessi, unita a meccanismi di monitoraggio e controllo, riduce significativamente l'esposizione a sanzioni e contenziosi.

File sharing: vettore di rischio o opportunità di controllo?

In questo scenario, la condivisione dei file rappresenta contemporaneamente un vettore di rischio e un'opportunità di rafforzamento della governance. I dati sensibili attraversano cloud, e-mail, chat e strumenti non governati, spesso senza cifratura, monitoraggio e controlli adeguati.

Allo stesso tempo, la condivisione dei file può diventare un'opportunità di rafforzamento della governance, se gestita attraverso strumenti che rendono naturale rispettare le policy.

L'esperienza dimostra infatti che strumenti intuitivi riducono il cosiddetto "shadow IT" la tendenza degli utenti a utilizzare canali non autorizzati per aggirare processi complessi.

Raccomandazioni strategiche

Per affrontare efficacemente le sfide della condivisione sicura dei dati, questa guida propone criteri di scelta delle soluzioni, confronta best practice operative e delinea una roadmap implementativa calibrata sulle esigenze di grandi organizzazioni.

L'obiettivo è fornire ai decisori aziendali gli strumenti per trasformare il file sharing da potenziale vulnerabilità in vantaggio competitivo, bilanciando sicurezza, compliance e produttività in un unico framework strategico.

Che cos’è oggi il filesharing in azienda

La condivisione dei file in azienda copre casi molto diversi. Esistono strumenti integrati nelle suite di produttività, soluzioni orientate alla privacy e piattaforme per scambi strutturati. Comprendere le famiglie aiuta a scegliere il giusto equilibrio tra usabilità e controllo sul dato.

Famiglie di soluzioni

Le principali famiglie sono quattro.

1. Le soluzioni EFSS cioè **Enterprise File Sync and Share** nelle suite come Microsoft 365 si focalizzano su collaborazione e versioning.
2. Le soluzioni con **cifratura lato client e modello zero knowledge** privilegiano il controllo chiavi da parte dell’azienda.
3. Le soluzioni MFT cioè **Managed File Transfer** governano scambi strutturati e ripetibili con tracciabilità rigorosa.
4. Gli invii ad hoc tramite **servizi pubblici o e-mail** offrono velocità ma poco controllo dopo il download.

Come le aziende lo usano davvero

Le organizzazioni condividono contenuti con team interni e con terze parti lungo la supply chain. Il valore nasce dalla fluidità, il rischio nasce dalla perdita di controllo. Bilanciare questi due aspetti è il vero obiettivo.

Collaborazione interna ed esterna

La collaborazione interna coinvolge reparti, progetti e comitati che lavorano su documenti, presentazioni, disegni tecnici, referti e contratti. La collaborazione esterna include clienti, partner, studi legali, fornitori e auditor. La forma può essere sincrona, come co authoring in riunione, oppure asincrona, come scambi approvati e revisioni successive. Gli ambienti possono essere gestiti dall'azienda oppure non gestiti quando si lavora su dispositivi personali o di partner.

Comportamenti dei dipendenti

Shadow IT: uso di strumenti, applicazioni e servizi non approvati dall'IT aziendale per condividere o archiviare file, senza controlli centralizzati, audit trail, applicazione coerente delle policy e continuità della protezione.

Garbage collection: accumulo incontrollato di copie, allegati, versioni e link fuori governance in cloud personali, chat e caselle email, che impedisce di identificare l'ultima versione, ostacola revoche e deprovisioning e mette a rischio conformità e catena di custodia.

Le persone cercano la strada più comoda per finire il lavoro. Quando lo strumento ufficiale è complesso nasce lo shadow IT, cioè l'uso di canali non approvati.

Un secondo fenomeno è la garbage collection, intesa come accumulo disordinato di copie, versioni, allegati e link fuori governance. Questi residui aumentano la superficie di attacco, complicano il recupero durante un audit e interrompono le collaborazioni quando i link scadono senza traccia.

Rischi di sicurezza e nuove superfici di attacco

La superficie di attacco del filesharing cresce con identità federate, applicazioni cloud e intelligenza artificiale. Molti incidenti partono da errori di configurazione e credenziali rubate. Ransomware ed estorsione con esfiltrazione restano tendenze in crescita insieme allo sfruttamento di vulnerabilità e alla dipendenza da terze parti.

Il fattore umano è confermato come concausa prevalente. Nell'ultimo report Verizon DBIR 2024 **la componente umana è coinvolta in oltre i due terzi dei breach**. Questo dato evidenzia il valore di controlli che riducano occasioni di errore e semplifichino scelte sicure per gli utenti.

L'AI generativa amplia la visibilità se i permessi non sono corretti: quando colleghi bot o agent a repository e piattaforme di condivisione, il modello accede e ripropone tutto ciò che è autorizzato a vedere, quindi permessi troppo ampi o incoerenti possono portare a divulgare contenuti non destinati a quegli utenti.

La comunità OWASP ha catalogato i principali rischi specifici come la prompt injection che manipola le istruzioni del modello, la gestione insicura dell'output quando i risultati vengono riusati senza validazione e le vulnerabilità della filiera del software in plugin e connettori. Per il filesharing questo significa verificare con cura le integrazioni tra bot, agent e repository documentali, applicare il principio del minimo privilegio sui permessi e validare l'output del modello prima che generi condivisioni o azioni che possano oltrepassare la governance prevista.

Uno dei vettori meno evidenti sono le **catture dello schermo durante call e registrazioni automatiche**. Senza difese adeguate un documento riservato può uscire dal controllo senza lasciare traccia. La protezione anti screenshot lato viewer riduce questa fuga silenziosa.

Compliance e catena di custodia

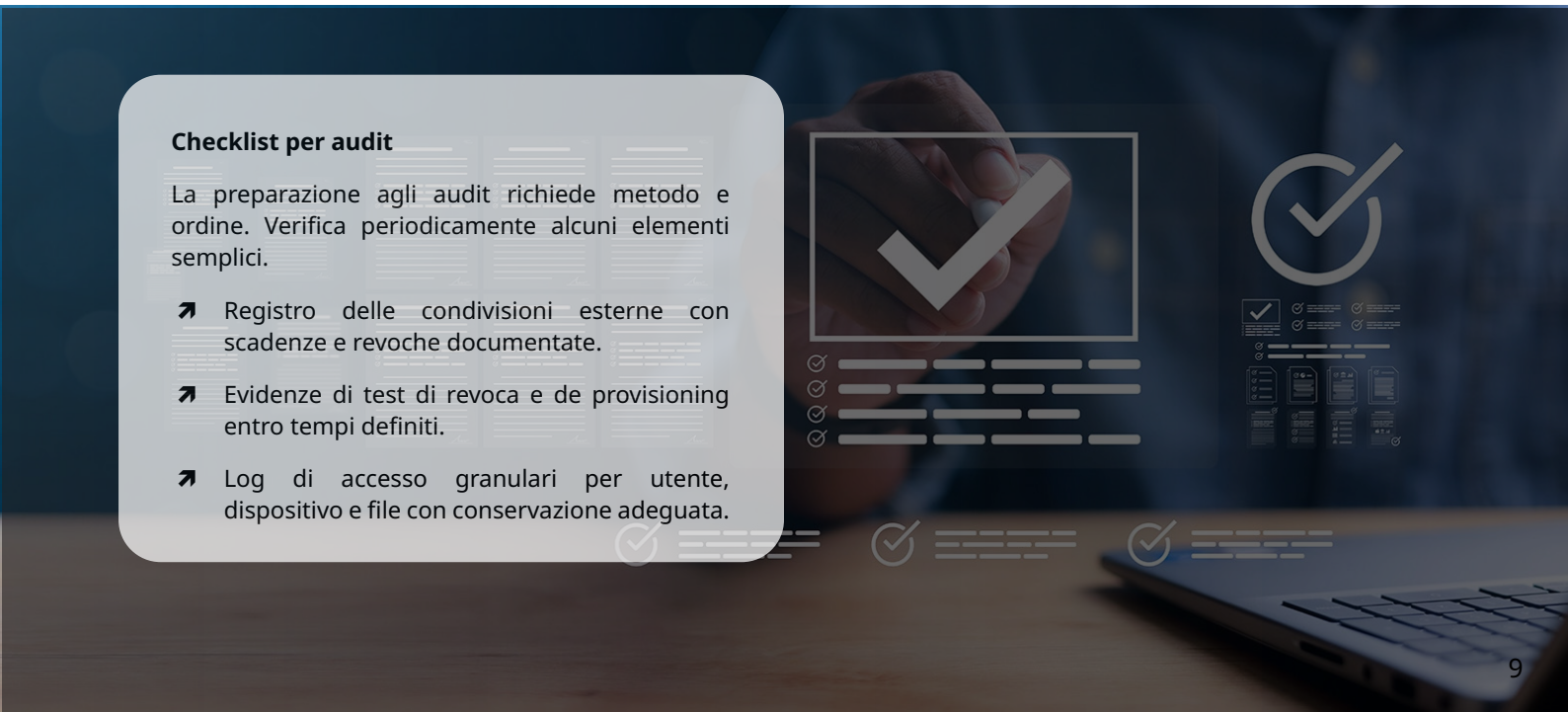
La conformità vive di evidenze.

GDPR (General Data Protection Regulation) richiede misure tecniche e organizzative adeguate, tra cui cifratura, valutazioni d'impatto e registri delle attività di trattamento.

NIS2 (Network and Information Security Directive) rafforza gli obblighi di sicurezza e introduce responsabilità specifiche per soggetti essenziali e importanti.

DORA (Digital Operational Resilience Act) impone al settore finanziario requisiti su resilienza operativa digitale, gestione dei fornitori terzi ICT e reporting di incidenti.

La catena di custodia è la traccia completa e inalterabile di chi ha creato, aperto, modificato o condiviso un file, quando e da quale dispositivo, con quali autorizzazioni, inclusi versioni, revoche, scadenze e log di accesso. Per costruirla si parte dai principi: minimizzazione e versioning riducono copie superflue, tracciamento e audit trail documentano ogni passaggio, la gestione delle chiavi adotta BYOK cioè Bring Your Own Key e CSE cioè Client Side Encryption fino al modello zero knowledge in cui il provider non ha accesso alle chiavi. Ruoli chiari tra IT, sicurezza, DPO e fornitori definiscono chi decide, chi esegue e chi verifica.



Checklist per audit

La preparazione agli audit richiede metodo e ordine. Verifica periodicamente alcuni elementi semplici.

- Registro delle condivisioni esterne con scadenze e revoche documentate.
- Evidenze di test di revoca e de provisioning entro tempi definiti.
- Log di accesso granulari per utente, dispositivo e file con conservazione adeguata.

Filesharing e problemi ricorrenti in azienda

I seguenti scenari si verificano con frequenza e generano esposizione. Affrontarli con procedure chiare e controlli tecnici riduce subito il rischio e migliora l'esperienza.

- **Link pubblici che sfuggono al controllo**: Quando un link accessibile a chiunque continua a circolare, il proprietario perde visibilità. La soluzione tecnica è l'autenticazione con e-mail e codice monouso, scadenze e revoche automatiche. La soluzione organizzativa è una policy di pubblicazione con approvazioni e report periodici.

- **Allegati e copie locali non cifrate**: Gli allegati in chiaro e i file esportati su desktop ampliano la superficie di attacco. La soluzione tecnica è il download sempre cifrato con viewer protetto. La soluzione organizzativa è una procedura unica per gli invii esterni.

- **Versioni divergenti e garbage collection**: Copiare e rinominare genera residui difficili da tracciare. La soluzione tecnica è il versioning centralizzato e l'uso di tag aziendali con ereditarietà. La soluzione organizzativa è la definizione di ownership e la pulizia programmata.

- **Fughe invisibili via screenshot e registrazioni**: Le catture schermo in riunione sono una via di esfiltrazione silenziosa. La soluzione tecnica è il blocco della cattura lato viewer e watermark dinamici. La soluzione organizzativa è la policy riunioni con divieti chiari e notifica ai partecipanti.

- **Esposizione tramite strumenti di AI**: Bot non governati possono leggere contenuti in eccesso. La soluzione tecnica è far rispettare permessi e tag all'AI aziendale e abilitare protezioni anti scraping. La soluzione organizzativa è il registro degli strumenti autorizzati.

Criteri per scegliere una soluzione

> *"Il criterio principale è il controllo persistente sul file anche dopo il download"*

Quando scegli una piattaforma di filesharing devi **bilanciare sicurezza e adozione**. Se gli utenti non la usano perché è scomoda, torneranno a e-mail, link pubblici e strumenti non autorizzati.

1. **Il criterio principale è il controllo persistente sul file anche dopo il download**. Significa che, anche se il documento esce dall'ambiente aziendale, puoi ancora limitarne l'uso, applicare scadenze, revocare accessi e impedire copie o stampe. In pratica chiediti: se domani un fornitore salva una copia locale, posso ancora bloccarla oppure no.
2. Subito dopo conta **la cifratura completa lungo tutto il percorso**. In transito, quando il file viaggia. A riposo, quando è archiviato. Lato client, prima che lasci il dispositivo, con chiavi gestite dall'azienda. Così, anche se qualcuno intercetta o esporta il file, i dati restano illeggibili.
3. **La governance degli accessi** definisce chi vede cosa e con quali limiti. Ruoli, etichette o tag impostano regole coerenti. Scadenze e revoche chiudono l'accesso nel momento giusto. Watermark e blocchi di stampa, copia e download riducono gli abusi e aiutano negli audit.
4. Le difese operative sono i **controlli che agiscono durante l'uso**. Un viewer protetto ti permette di far leggere i documenti senza consegnarne una copia utilizzabile. Le protezioni contro l'AI riducono rischi di scraping e riuso non autorizzato dei contenuti da parte di bot e agent collegati.
5. Usabilità e integrazioni decidono la **velocità di adozione**. Collegarsi bene con Microsoft 365, con l'IdP cioè Identity Provider, con SIEM cioè Security Information and Event Management e con CASB cioè Cloud Access Security Broker evita attriti e riduce lo shadow IT. Gli utenti lavorano dove sono abituati, ma con regole e tracciamento.

FileGrant e la DLP estesa al cloud con AIGrant

La prevenzione delle perdite di dati deve seguire il file ovunque. FileGrant integra AIGrant, **l'AI privata di CyberGrant che crea agent specializzati per classificare automaticamente i documenti,** applicare tag e assegnare ruoli in base a regole aziendali. Questo consente di estendere la DLP cioè Data Loss Prevention a repository cloud e a documenti condivisi fuori dall'azienda, con policy che attivano download cifrato, anti capture, limiti di copia e scadenze in modo automatico.

Per i dati ad alto valore l'azienda può adottare cifratura lato client con gestione autonoma delle chiavi. In questo modo **i contenuti restano inaccessibili fuori dai dispositivi e dalle identità autorizzate**, anche in scenari con più fornitori e strumenti.

Come funziona FileGrant

FileGrant ENTERPRISE

FileGrant di CyberGrant unisce semplicità d'uso e controlli avanzati per rendere sicura la condivisione senza rallentare il lavoro. La piattaforma protegge il file in modo persistente, anche quando esce dai confini aziendali.

Cifratura che segue il file: Il download avviene sempre in formato protetto con tecnologia Lock&Go basata su PDF sicuro. I file così protetti restano utilizzabili solo dagli utenti autorizzati e le revoche hanno effetto anche dopo l'invio.

Protezione nel tempo e gestione chiavi: FileGrant supporta cifratura post quantum con scambio chiavi CRYSTALS Kyber selezionato dal NIST e opzione zero knowledge in cui l'azienda detiene il pieno controllo delle chiavi.

Controllo accessi con ruoli e tag a priorità assoluta: I ruoli definiscono cosa può fare ogni profilo. I tag applicano restrizioni che prevalgono su qualsiasi permesso, per esempio il tag no download impedisce il salvataggio in chiaro anche agli editor. Le regole possono ereditarsi dalle cartelle e attivare limiti come sola visualizzazione, anti capture e watermark.

Viewer proprietario con protezioni anti AI: Il viewer apre i documenti in sola lettura e blocca lo screenshot e lo screen sharing durante le call. Le protezioni anti AI impediscono l'acquisizione del contenuto da

strumenti di intelligenza artificiale indesiderati.

Condivisione semplice ma tracciata: I link sono protetti con e-mail e codice monouso, scadenze e revoche immediate. In alternativa, l'invio esterno tramite PDF protetto resta sincronizzato con i permessi del file originale. QuickShare consente invii urgenti senza perdere audit e controllo.

Interfaccia intuitiva che riduce lo shadow IT: Upload massivi, drag and drop, tag automatici e versioning spingono gli utenti a usare lo strumento ufficiale invece di ricorrere a canali non approvati.

Stop alla garbage collection: Ogni invio è monitorato e recuperabile. Tag, versioning e download sempre cifrati evitano copie non governate e allegati dispersi.

Casi d'uso concreti risolti con FileGrant

Sanità: proteggere referti e dati sensibili in ogni fase della condivisione

Contesto

Un poliambulatorio condivide referti e allegati diagnostici con pazienti, specialisti esterni e assicurazioni.

Problema

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

Soluzione con FileGrant

- AI Classification riconosce i dati sanitari e applica automaticamente il tag dedicato che impone apertura in viewer protetto, divieto di download in chiaro e anti-capture. Accesso tramite e-mail e codice monouso, scadenze, revoche e audit completo. Le funzioni AI sono abilitate solo per ruoli autorizzati.

Risultato

Riduzione del rischio di data breach, tracciabilità completa delle consultazioni e supporto alla conformità con GDPR e requisiti sanitari.

Manifatturiero: proteggere disegni, IP e know-how lungo la supply chain

Contesto

Un’azienda condivide disegni CAD e distinte base con fornitori e partner.

Problema

Perdita di controllo dopo il download e diffusione non autorizzata di informazioni critiche.

Soluzione con FileGrant

- La classificazione automatica marca i file come segreto industriale. RBAC e tag impongono download solo in PDF protetto agli editor interni ed esterni e sola visualizzazione ai fornitori, con anti-capture forzato. I tag si ereditano dalle cartelle e prevalgono su ogni permesso. Log e timestamp garantiscono una catena di custodia completa.

Risultato

Collaborazione fluida con terze parti senza cedere controllo, con tracciabilità completa e protezione dell’IP lungo tutto il ciclo di vita del documento.

Conclusione.

Condivisione veloce, sicurezza sostanziale, governance dimostrabile

FileGrant porta la semplicità del filesharing dentro una cornice di sicurezza sostanziale.

In un contesto in cui ogni file può rappresentare un vettore di rischio, e in cui collaborazione, compliance e visibilità sono criteri strategici, non è più sufficiente “condividere”: è necessario condividere in modo sicuro, governato e collaborativo.

Con FileGrant, la condivisione dei file diventa un asset strategico: protezione avanzata, collaborazione controllata, governance verificabile.

Se desideri offrire a IT, sicurezza e compliance una piattaforma che garantisca visibilità, controllo e collaborazione reale, è il momento di scoprire FileGrant.

www.cybergrant.net