

# Confidencial.io for Third-Party Risk

*Keeping sensitive data safe after it's been shared*

## USE CASE

When you share data with vendors, partners, or contractors, you often lose visibility and control the moment it leaves your systems. That blind spot is where data gets mishandled, forwarded, or exposed.

Confidencial solves this by enabling secure document exchange and request workflows. Protection, governance, and auditability are embedded directly into each file. Controls stay intact, even after sharing, so you can collaborate without compromising security or compliance.

## THE CHALLENGE

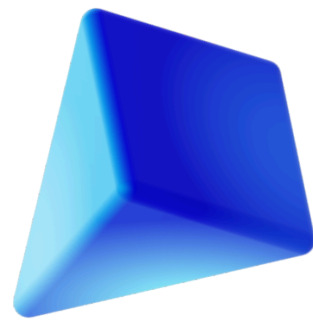
Third-party collaboration is essential, but it introduces risk at every turn:

- Vendors save files in unmanaged storage
- Contractors retain access after contracts end
- Documents are forwarded, copied, or mishandled without oversight
- Upload portals and email offer no security guarantees
- There's no clear way to revoke or trace access once a file is sent

Traditional tools stop protecting data the moment it leaves your environment.

### Why it Matters

- **Widespread Exposure:** 60% of breaches involve third parties (IBM 2024)
- **Regulatory Pressure:** EO 14117, ISO 27001, and others require secure external data handling
- **Loss of Visibility:** You can't audit, control, or recall what you can't see
- **Insecure Ecosystems:** Even trusted suppliers may operate with weaker security or unknown vulnerabilities



# How Confidential Mitigates Third-Party Risk

Confidential embeds protection, control, and traceability directly into every file, so your data stays secure and governed, even after it's shared beyond your four walls.

## Secure File Exchange

Collect and share sensitive documents with third parties using built-in encryption, auditability, and data-blind protection, no special viewer required.

## Granular Access Control

Limit access to only the information needed, apply field-level restrictions, and revoke access instantly when contracts or roles change.





## Persistent Protection

Security travels with the file across systems, inboxes, and cloud platforms, ensuring data stays protected wherever it goes.

## Full Visibility & Auditability

Track external file access, downloads, and interactions with complete audit trails for compliance, forensics, and vendor accountability.

## BUSINESS IMPACT

-  **Prevent data exposure through** third-party systems and email-based sharing
-  **Enforce access restrictions,** even after files are sent
-  **Support audit readiness** with full visibility and control
-  **Track vendor and contractor activity** across file uploads and downloads

Case in Point:

### THE MOVEit

### Vendor Breach



*In 2023, attackers exploited a zero-day vulnerability in the MOVEit file transfer tool. The result: massive data exposure across vendors, government agencies, and private organizations. Most companies had no idea what had been shared or where the data had ended up.*

**The lesson?** Relying on third-party systems for security is not enough. Confidential keeps your data protected, even after it's been shared externally.