Sensitive Data Security for the Legal Industry

Confidencial

Protect your most sensitive data across matters, collaborators, and compliance demands

56%

56% of law firms that experienced a data breach in the last year lost sensitive client information.

Law firms manage massive volumes of sensitive data including privileged emails, meeting notes, transcripts, contracts, case files, IP, and compliance records, that are spread across iManage, NetDocuments, SharePoint, local drives, email servers, and legacy tools.

Most firms lack visibility into where this data lives, what it contains, or how it's being shared. Disorganized and untagged content creates blind spots that make it difficult to enforce protection, prove compliance, or prevent breaches. This lack of control introduces serious risks: loss of privilege, regulatory penalties, and client trust erosion.

How Confidencial Can Help

Confidencial brings control to legal data, enabling firms to discover, protect, and govern sensitive content across systems and workflows.

We go beyond file-level protection to secure what's inside: filings, agreements, internal memos, and more, down to the sentence or clause. Our embedded, format-preserving encryption travels with the file, keeping it protected even if it's leaked, mishandled, or shared externally. With Confidencial, firms can lock down sensitive work product without locking up legal workflows.

◆ Identify and classify sensitive legal data (e.g., pleadings, contracts, HR/M&A docs) across cloud and on-prem environments

◆ Demonstrate compliance with GDPR, HIPAA, CCPA, and client audits using file-level tracking and audit logs

◆ Apply persistent encryption and access controls to secure external sharing with clients, co-counsel, and regulators

◆ Control AI exposure by securing privileged data before it reaches tools like Harvey, CoCounsel, or Copilot

box

aws

OneDrive

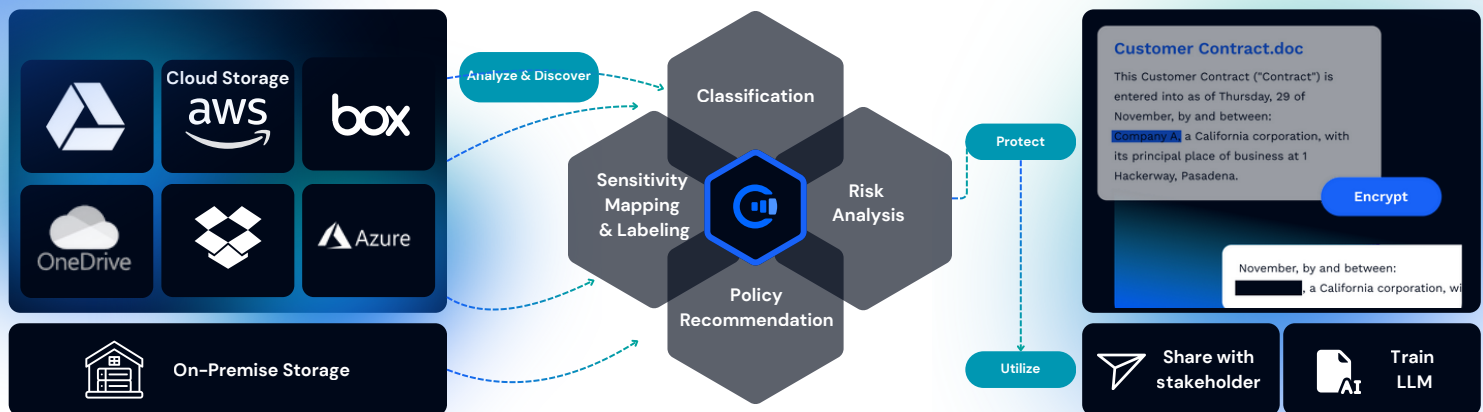DARPA · AFWERX · pwc · MC MASSCHALLENGE · SRI · Microsoft Partner · powered by aws

sales@confidencial.io

Built on IP originally developed for DARPA, Confidencial brings complete data protection to the most complex legal data environments.

01
Confidencial scans on-premises and distributed cloud environments to **identify sensitive information stored** *within* **documents** across your organization.

02
Our solution automatically **classifies, maps, and labels sensitive data**, while our dashboards provide the telemetry needed to help you **understand and manage risks** across your entire data landscape.

03
Selective encryption protects access down to the specific data points and fields inside a document to fortify security while maximizing the **utility** of non-sensitive information for other stakeholders and **LLMs**.

Confidencial's unified solution simplifies discovery, remediation, and secure sharing.

Uncover hidden data risks
Reveal and map data risks with intelligent, granular scanning to identify sensitive unstructured data, quantify financial risks, and assess security posture.

Classify and tag sensitive data
Identify, categorize, and tag sensitive data across cloud and on-prem environments for comprehensive visibility and control.

Secure data at field level
Auto-protect sensitive portions of documents, while keeping the rest fully accessible. Encryption is embedded in metadata, preserving the document's native format.

Control access and secure sharing
Facilitate protected sharing and requesting of sensitive and regulatory data with external parties, secured by true end-to-end encryption and robust access controls.

Get end-to-end data & document traceability
Get robust activity logs with an audit trail for the entire document lifecycle: where they're forwarded and how they're accessed, including geographical location.

Set a faster, firmer path to AI readiness
Secure sensitive portions of data with tokenization or selective encryption—protect critical data and enable future use with AI models, agents, and services.

sales@confidencial.io