

Confidential.io for Intellectual Property Protection

Protect your most valuable ideas before they're exposed, misused, or stolen

USE CASE

Intellectual property is one of your most valuable assets, and one of the hardest to control. It's often buried in unstructured documents, shared across teams, vendors, and legal counsel, or embedded into collaboration and AI workflows.

Confidential automatically discovers and classifies sensitive IP, applies selective encryption, and enforces access controls down to the word, formula, or field. Files stay protected wherever they travel, with full visibility and the ability to revoke access at any time. And because Confidential is built on a data-blind architecture, your sensitive information remains private - even from us.

THE CHALLENGE

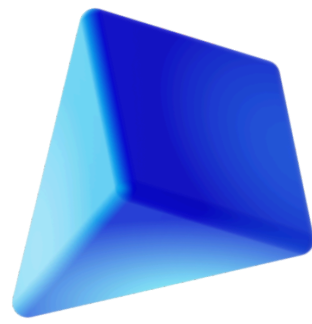
IP spans multiple teams, documents, and workflows—and rarely stays in one place:

- Design specs, research docs, and internal memos
- Technical files tied to patents, models, or training data
- Contracts, slides, or licensing docs sent to partners
- Proposals and inventions under review by legal, investors, or leadership

Without persistent protection, IP can be exfiltrated by insiders, retained by vendors, or accidentally leaked long before it's commercialized or patented.

Why it Matters

- **Competitive Risk:** Leaked IP can erode market advantage or compromise patentability
- **Insider Threat:** Teams, contractors, or ex-employees may retain or misuse IP after access ends
- **Third-Party Exposure:** IP shared with vendors, advisors, or collaborators often leaves your control
- **No Revocation Path:** Once a file is downloaded or copied, you can't take it back



How Confidential Secures Your Intellectual Property

Confidential ensures IP remains encrypted, access-controlled, and auditable, no matter where it goes.

Identify and Protect IP Automatically

Scan and classify unstructured content to discover sensitive IP, then apply targeted encryption, down to the word or formula.

Role-Based Access to Sensitive Content

Control who sees what—down to the clause, formula, or paragraph—based on role, team, or partner permissions.

AI-Safe Collaboration and Sharing

Prevent sensitive IP from leaking into GenAI tools or AI workflows with Confidential's built-in protections.

Full Visibility and Revocation

Monitor every interaction and revoke access instantly—even if a file has been downloaded, copied, or shared.

BUSINESS IMPACT



Preserve competitive advantage by protecting proprietary designs and strategies



Safeguard patent rights by preventing premature or accidental disclosure



Enable secure collaboration across teams and third parties



Strengthen legal defensibility in IP ownership and disputes

Case in Point:



In 2023, Apple banned employees from using ChatGPT and other generative AI tools internally, citing concerns about confidential data and source code being exposed through prompts. This move followed reports that staff at multiple companies had inadvertently entered sensitive information, including internal strategies and proprietary code, into public AI tools.

The lesson? Even helpful AI tools can become a leakage vector for your most sensitive IP. Confidential ensures proprietary data is protected before it's ever exposed to LLMs, APIs, or prompt history.