Confidencial.io for Insider Threat

Stopping Insider-Driven Data Leaks Before They Happen

USE CASE

Employees, contractors, and even trusted partners often need access to sensitive information, but that access can be misused. Whether intentional or accidental, insider threats lead to some of the most costly and difficult-to-detect breaches.

Confidencial protects sensitive files from misuse by embedding granular controls directly into the data, enabling internal collaboration without losing control.

THE CHALLENGE

Even with IAM and device policies in place, organizations struggle to stop insiders from:

- Copying files to USBs or personal drives
- Emailing IP or regulated data externally
- Misusing AI tools that retain prompt content
- Retaining access to data after termination

These behaviors are often invisible until it's too late, especially in unstructured environments like email, shared drives, and collaboration platforms.

Why it Matters

- **Undetectable Risk:** Insider actions often look like normal behavior
- **High Cost of Breaches:** Insider breaches cost 3x more than external hacks
- **AI Era Acceleration:** Tools like ChatGPT amplify accidental leakage
- **Audit & Compliance Failures:** Can't prove who accessed what, when, or why

Confidencial

How Confidencial Protects Against Insider Threats

With Confidencial, every file becomes self-defending, automatically encrypted, access-controlled, and traceable to stop insider misuse before it happens.

Granular Encryption

Encrypt only sensitive content down to the word or field, while keeping documents fully usable.

Revocable Access

Instantly revoke or change access to documents, even after they've been shared or downloaded.

Traceability and Oversight

Monitor file access, edits, and sharing in real time to detect and investigate insider risk.

Portable Security

Protection travels with the file across users, systems, and locations, without losing control or context.

BUSINESS IMPACT

- **Prevent data exfiltration** via email, USB drives, AI tools, or personal accounts
- **Reduce insider risk** without slowing down legitimate work
- **Ensure compliance** with built-in encryption, access controls, and audit trails
- **Gain visibility** into who accesses, edits, or shares sensitive content

Case in Point: The Tesla Insider Leak

TESLA

In 2023, a Tesla employee leaked over 100GB of internal data—including customer complaints, financial records, and proprietary manufacturing secrets—to a German newspaper. The employee had legitimate access but no restrictions on what could be shared, copied, or exported.

The lesson? *Insider access isn't the same as data control. Confidencial ensures sensitive content stays protected—even from those on the inside.*

sales@confidencial.io