Confidencial

Data Protection for AI Operations

21%

of organizations have established policies governing employees' use.

As AI adoption accelerates, many organizations face the dual challenge of securing sensitive data while leveraging the immense potential of generative AI. With 95% of data unstructured, businesses are either leveraging it for growth through LLMs or missing out on it's potential.

The rapid integration of LLMs has outpaced the development of necessary governance frameworks, leading to increased risks of data exposure. Sensitive information can inadvertently be leaked through AI models, underscoring the need for a solution that not only secures and controls sensitive data but also allows businesses to fully harness the benefits of LLMs while protecting intellectual property and personal data.

72%

organizations that have adopted AI in at least 1 function [1]

Unlock the Value of LLMs While Safeguarding Sensitive, Unstructured Data

By automatically analyzing and identifying sensitive information within data repositories, Confidencial applies Selective Encryption, protecting specific content without compromising the usability of the data. This approach allows organizations to safely leverage LLMs for efficiencies and insights, knowing that proprietary or personal information is securely shielded during AI operations. With auditable logs and alignment with NIST standards, Confidencial makes it straightforward to govern, audit, and adapt security measures, ensuring compliance and long-term data protection.

Scan and Analyze

Identify and locate sensitive data across AWS and other storage environments.

Secure and Utilize

Maximize utility and secure sensitive information with precise, selective encryption.

Track and Audit

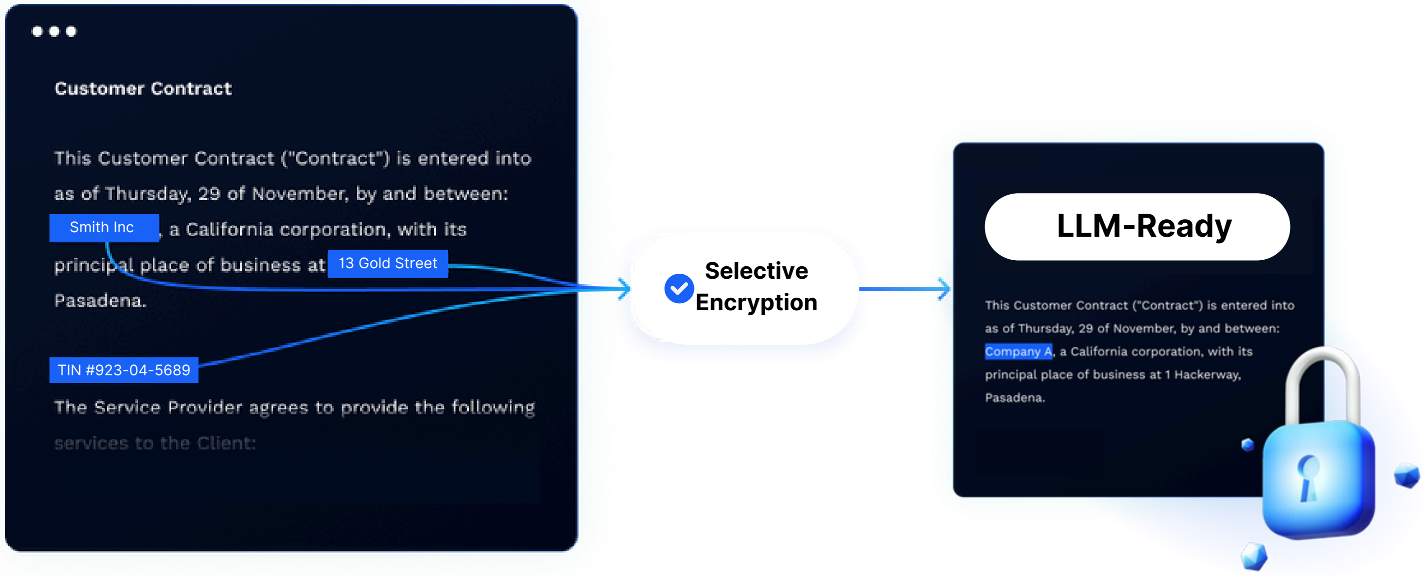
Ensure AI governance and compliance with detailed tracking and audits.

A solution partnering with and trusted by leading global organizations.

DARPA AFWERX pwc MC MASSCHALLENGE SRI Microsoft Partner powered by aws

sales@confidencial.io

Confidencial enables organizations to selectively shield sensitive or proprietary content within documents before being used in LLM training and operations for maximum utility.



Customer Contract

This Customer Contract ("Contract") is entered into as of Thursday, 29 of November, by and between: Smith Inc, a California corporation, with its principal place of business at 13 Gold Street Pasadena.

TIN #923-04-5689

The Service Provider agrees to provide the following services to the Client:

This Customer Contract ("Contract") is entered into as of Thursday, 29 of November, by and between: Company A, a California corporation, with its principal place of business at 1 Hackerway, Pasadena.

The Confidencial Advantage

File-Format Preserving Selective Encryption

Control what data is shared and safeguard sensitive information like SSNs, credit card details, and more, even outside your perimeter.

Built-In Protection to Follow Your Data

Protection is embedded directly into the document, regardless of how it is shared or stored.

Data-blind architecture

Your data never leaves your infrastructure. We do not store your files or data, nor can we access it.

Traceability and Audit Logs

Detailed activity logs provide an audit trail into the entire document lifecycle: where they're forwarded and how they're accessed, including geographical location.

Seamless Integrations with Apps and Storage Sites

Platform agnostic: Integrates with standard applications, cloud storage, vaults, and Key management system providers.

Path to Post-Quantum-Encryption Upgrades

Ready to protect unstructured data now for the long-term.

Confidencial's underlying patented technology was developed by Stanford Research Institute (SRI) for DARPA. To date, Confidencial has been used across 170+ organizations in 34 countries and was awarded the Cyber Solution of the Year for 2023 by PwC Luxembourg.

sales@confidencial.io