

# DIFENSO Add-Ins and Connectors

Protection and security measures should be **focused on data**.

All data should be available until its owner decides to make it unavailable.

Difenso has developed a full ecosystem to ensure data security and traceability.

With Difenso your data is protected all along its lifecycle!

## KEY FEATURES

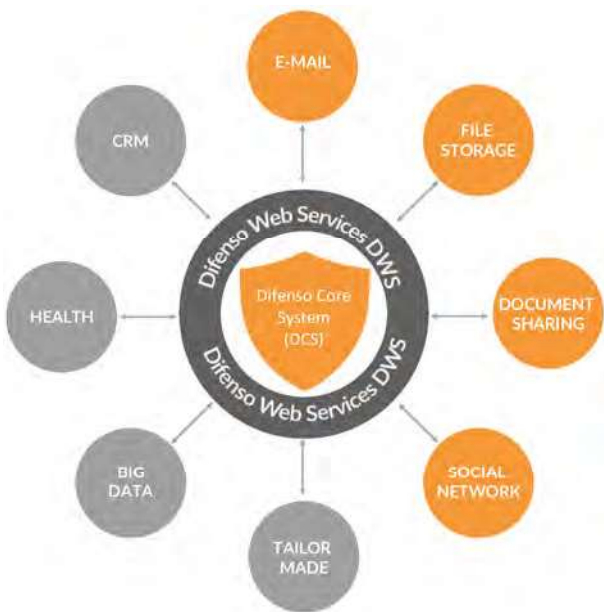
- 1) Strong data protection
- 2) Ensure **strong integrity**
- 3) **Strong authorization** control
- 4) Key **activation/deactivation**
- 5) **Traceability** of all access to key encryption
- 6) Dynamic access right management
- 7) **Easy** to integrate
- 8) Encrypted data **never stored by Difenso**
- 9) Each data, file or document **are encrypted by a new key**

Better data dissemination control (...)

Reduced risk of data loss (...)

New opportunities brought by encryption key management

Difenso secure major applications (...) and is able to develop specific Add-Ins or connectors On Demand



Each data is encrypted with a new and unique key with its own authorization list

## COMPETITIVE ADVANTAGES

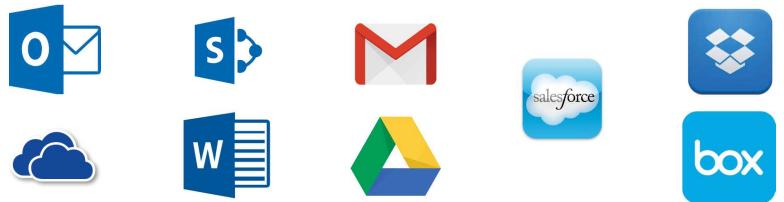
With our Add-Ins and Connectors, we guarantee:

- \* **Better data dissemination control:**  
Traceability of all access to encryption keys, authorization management (add/remove authorized user to access encryption keys)
- \* **Reduce risk of data loss:**  
The user is the only one able to access the same time encrypted data and encryption key, and encryption keys are never stored by **Difenso**
- \* **New opportunities brought by management of encryption keys:**  
Start date, expiration date, unlimited activation/deactivation

## DIFENSO PRODUCT PORTFOLIO

Data exchange is mainly by mail, file sharing and storage, business applications, Customer Relationship Management (CRM), or internal development, etc...

Difenso secures major applications such as Outlook, Gmail, OneDrive, etc... and is able to develop specific Add-Ins or Connectors On Demand.



## HOW DO OUR ADD-INS AND CONNECTORS WORK?

To encrypt and decrypt your data, Add-Ins and Connectors use the **Difenso Web Service (DWS)** and avail of the same robust and certified cryptographic background.

They identify and secure the data to be protected from the beginning (i.e. creation), they transmit a request with metadata to the DWS which generate and send a cryptographic key (protected by a transaction key) to encrypt data. Process is the reverse for decryption. They provide a dedicated interface respecting the user experience and ensure specific protection to each SaaS application. Neither the data in clear nor the encrypted data are seen or stored by Difenso.

**Each data is encrypted with a new and unique key with its own authorization list.**

Each Add-In and Connector ensures traceability of all data access.