Ciphety Docs

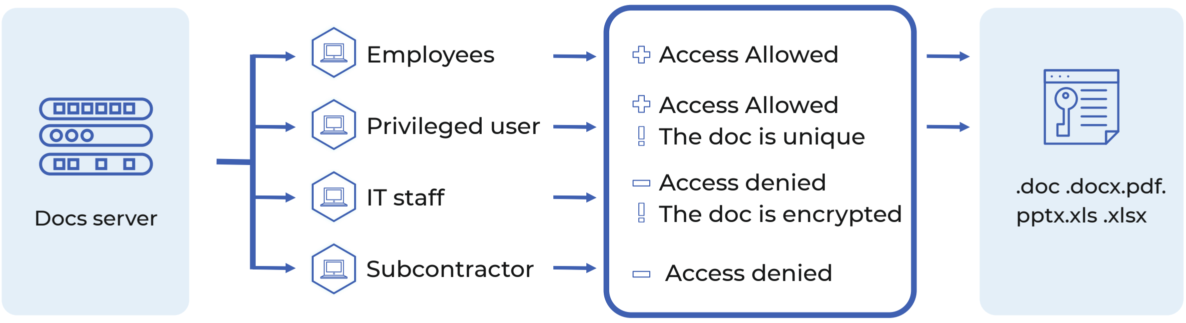
Solution overview

Leaks of confidential data regularly have a significant impact on the overall business performance of the victim organisations. As a result, the key goal of IT Security departments is not only the prompt mitigation an incident but also the investigative work aimed at identifying the entire approach of the perpetrator in order to prevent such incidents from occurring in the future. At the same time, if a confidential document appears in the public domain, the task is not only to remove it but also to identify the source of the leak. While data centric tools provide some assistance when dealing with these requirements, they also create further complications linked to diminished end user experience and a need for additional resources to manage their rule based restrictions.

Ciphety Docs was designed with these considerations in mind, allowing the client organisations to carry out large scale data classification, control end user access to privileged data, identify sources of leaks using timeline analysis and visible or hidden marks, all while improving the efficiency of the DLP systems by giving end users greater level of authority when dealing with sensitive documents.

Key Challenges related to Data Security

- Existing Data Leaks.
- Challenges mitigating the risk of losing confidential information contained in company documents.
- Ensuring that authenticity of internal documents can be easily verified, thereby reducing exposure to phishing/social engineering attacks.



Docs server

Employees → Access Allowed

Privileged user → Access Allowed; The doc is unique

IT staff → Access denied; The doc is encrypted

Subcontractor → Access denied

.doc .docx.pdf. pptx.xls .xlsx

How can we assist you?

IT/Security Directors

- **Improved IT Security posture: Minimising the risks of sensitive information being compromised.**
- **Access Rights Management: Controlling access to confidential documents.**
- **Preventing Data Leaks: Protecting data from internal and external information leaks.**
- **Compliance: Adherence to regional compliance requirements.**
- **Monitoring and Response: Observing and reacting to unauthorised employee activity and responding to high-risk incidents.**

IT Security Officers

- **Balanced Data Protection: Safeguarding data confidentiality, integrity, and availability.**
- **Accelerated Leak Detection: Quickly identifying source of leaks, perpetrators, and responding to incidents.**

Corporate Security Service

- **Reducing Investigation Costs and Time: Gaining in-depth insights about the handling of sensitive data by the employees which facilitates prompt and targeted response to data leaks.**
- **Preventing Unauthorised Disclosure: Avoiding leaks of official and commercial secrets by putting a greater emphasis on personal accountability.**

Employees

- **Increased Responsibility: Enhancing accountability when dealing with confidential information while preserving operational independence when dealing with day to day tasks.**
- **Understanding Security Policies: Actively comprehending the company's information security policies and having clear guidelines on handling sensitive data thus making the process easier and stress free.**

Key outcomes when using Ciphety Docs

Document search: Ability to determine the location of each document across the company infrastructure and who accessed it.

Document Content Analysis: Labelling and categorisation of the sensitive documents across customer infrastructure based on keywords and content review.

Document History Timeline: Recreation and review of the entire history of a document, from draft to final version, including all options for document copy creation.

Document tagging: Application of visible and hidden marks to documents.

Draft and Copy Management: Search for variety of identical document drafts and copies.

Reduction in overall number of accessible copies of sensitive documents: number of document copies and identify outdated versions, easing document flow in the company and reducing potential exposure to data leaks.

User Access Control: Ability to restrict user access to electronic documents according to organisational regulations and security policies.

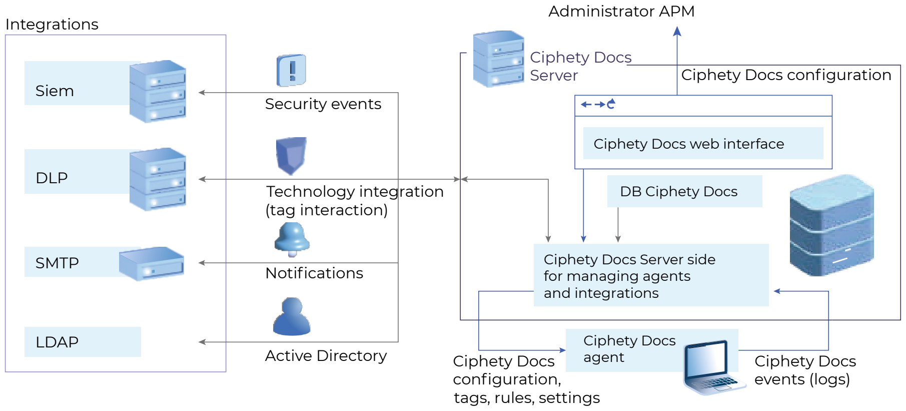
User Tracking: Tracking of all user activity when working with electronic documents.

Policy Violation Detection: Quick identification of attempts and examples of policy violations in confidential . electronic document management.

Leaked Document Analysis: Improvement in efficiency of handling data leaks by quickly identifying their source through user markers identifiable by the Ciphety Docs system.

Ciphety Docs Architecture

The system has a scalable architecture, enabling seamless adjustments for managing large data volumes and the flexibility to integrate or remove additional modules.


Integrations
Siem
DLP
SMTP
LDAP
Security events
Technology integration
(tag interaction)
Notifications
Active Directory
Administrator APM
Ciphety Docs Server
Ciphety Docs configuration
Ciphety Docs web interface
DB Ciphety Docs
Ciphety Docs Server side for managing agents and integrations
Ciphety Docs agent
Ciphety Docs configuration, tags, rules, settings
Ciphety Docs events (logs)

Ciphety Docs supports the following software versions

MS Office 2013, 2016, 2019 (Word, Excel, PowerPoint, Visio, Outlook)

LibreOffice 6.4 and newer

Supports inbedding Ciphety Docs functionality into the GUI of the above software.

PDF 1.4 and newer

- OS integrated functionality for marking documents.
- Two Encryption Algorithms: AES/AES+RSA support.
- Improves DLP System Efficiency: improving ROI of the currently implemented DLP systems by reducing false positives and improving operational efficiency.
- Individual document focused security approach: treating documents as the minimal security entity.

Contacts:

info@ciphety.com

CIPHETY