STORMSHIELD

STORMSHIELD
GOOGLE WORKSPACE

Keep control over the confidentiality of your sensitive data in an unsupervised cloud infrastructure

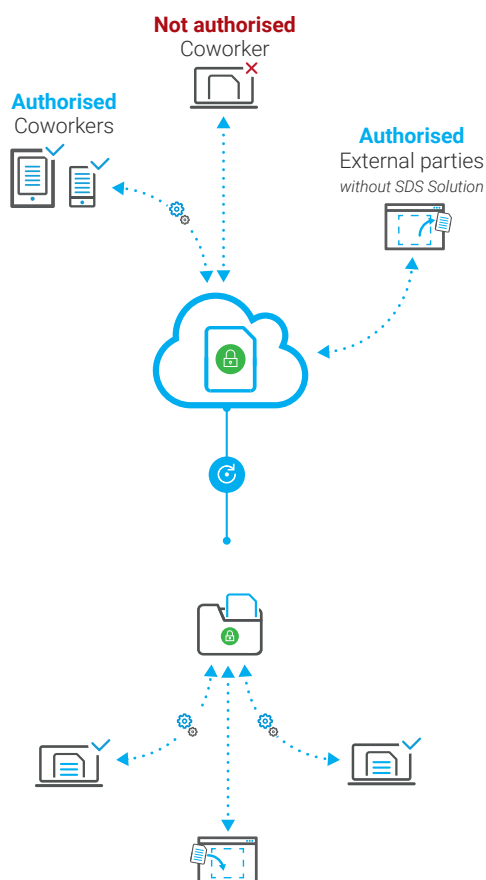## Agentless
SECURE EXCHANGES
MADE EASY

Transparency
AUTOMATED
ENCRYPTION

Compliance
LEGAL CONSTRAINTS

Confidence
A CERTIFIED
SOLUTION

Not authorised
Coworker

Authorised
Coworkers

Authorised
External parties
without SDS Solution

Data encryption

In the context of constant communication and data exchanges in the Cloud, information is exposed to the risks arising from such usage. Stormshield Data Security for Google Workspace allows for the secure encryption of information stored in Google workspaces.

Integration with Google Workspace

- Use of the Google Client Side Encryption option
- Same authentication as for your Google workspace
- Possible use of an IAM or IDP

Compliance with legal requirements

- End-to-end protection for sensitive data
- Improved protection of personal data
- The protection keys are under the exclusive control of the company

Ease of use

- Maintains the user experience
- Fully integrated in Chrome
- No agent to be deployed

**NEXT GENERATION
DATA PROTECTION**

**MEDIUM AND LARGE
COMPANIES**

WWW.STORMSHIELD.COM

Management chart

Security policy

A user's view

FONCTIONNALITÉS

SDS For Google Workspace
- Supports the Client Side Encryption mechanism
- User verification via OpenID
- Secured Google Drive sharing
- Google collaboration from any device
- Automatic encryption in local folders and synchronizers

Agentless operation with a simple Chrome browser
- Maintains the Google user experience
- A solution adaptable to a mixture of system types

Integration of a key manager
- Supports software-based key generators
- Supports hardware-based key generators
- KMIP protocol

Traceability of encryption and decryption actions by users on the SDS portal
- Monitoring of the use of the solution within the organisation
- Facilitates security audits in the event of a suspected data breach

Separation of rights
- Host, administrators and users

Regulatory compliance
- ITAR, CJIS, TISAX, IRS 1075 et EAR

Centralised management

COMPATIBILITY

Client-side server encryption

OnPrem deployment or in the cloud
Operating system: Red Hat 7
Implementation environment: Node.js 14

Workstation

No agent installed
Chrome compatibility on Desktop
ChromeOS

Traceability

Logs generated locally on the machine
Possibility to send via syslog