STORMSHIELD

DATA SECURITY

STORMSHIELD
POUR GOOGLE WORKSPACE

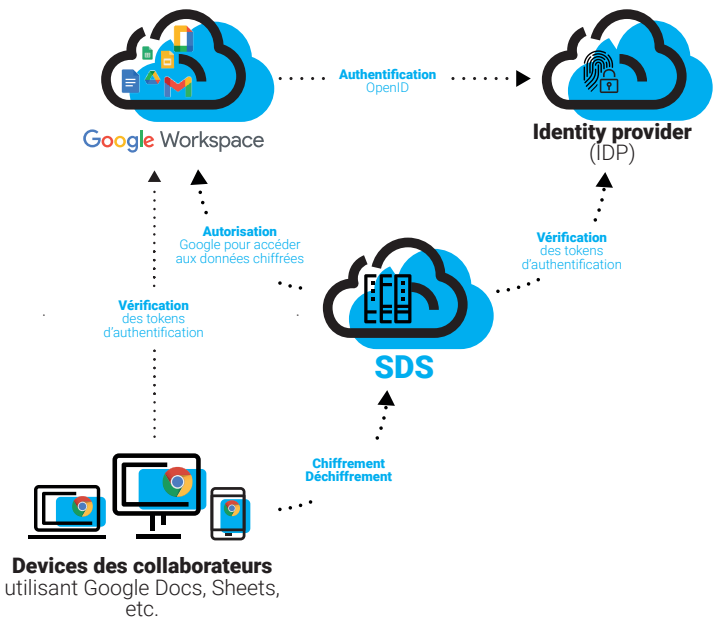
Gardez le contrôle de la confidentialité de vos données sensibles dans une infrastructure cloud non maîtrisée

Agentless
FACILITE LES ÉCHANGES SÉCURISÉS

Transparence
CHIFFREMENT AUTOMATISÉ

Conformité
CONTRAINTES LÉGALES

Simplicité
CHIFFREMENT MODE SAAS



Chiffrement

Dans le contexte des communications et des échanges permanents dans le Cloud, l'information est exposée aux risques induits par ces usages. Stormshield Data Security pour Google Workspace propose le chiffrement sécurisé des informations stockées dans les espaces Google.

Simplicité d'usage

- Protection des données en mode SaaS
- Conservation de l'expérience utilisateur
- Aucun agent à déployer

Intégration à Google Workspace

- Utilisation de l'option Google Client Side Encryption
- Même authentification que votre espace Google
- Utilisation possible d'un IAM ou IDP

Conformité aux contraintes légales

- Protection de bout en bout des données sensibles
- Amélioration de la protection des données personnelles
- Clés de protection sous le contrôle unique de l'entreprise

Page d'accueil MySDS.io

Page de statut

FONCTIONNALITÉS

SDS pour Google Workspace

- Support du mécanisme Client Side Encryption
- Vérification des utilisateurs via OpenID
- Support des applications Google Drive, Gmail, Meet, Calendar, Docs, Sheets et Slides
- Collaboration Google de n'importe quel device

Fonctionnement sans agent avec un simple navigateur Chrome

- Conservation de l'expérience utilisateur Google
- Solution adaptée à un parc de systèmes hétérogènes

Intégration gestionnaire de clé

- Support des générateurs de clés logiciels
- Support des générateurs de clés matériels
- Protocole KMIP

Traçabilité des actions de chiffrement et déchiffrement des utilisateurs dans le portail SDS

- Suivi de l'usage de la solution dans l'organisation
- Facilitation de l'audit de sécurité en cas de suspicion de fuite de données

Séparation des droits

- Hébergeur, administrateurs, et utilisateurs

Conformité réglementaire

- ITAR, CJIS, TISAX, IRS 1075 et EAR

Administration centralisée

- Support du standard OPA (Open Policy Agent) pour définir des règles de sécurité

COMPATIBILITÉ

Serveur Client-side encryption

- Protection des données en mode SaaS
- Possibilité de déploiement OnPrem (système d'exploitation : Red Hat 8 et 9 - environnement d'exécution : Node.js 16 et 20)

Poste de travail

- Aucun agent installé
- Compatibilité Chrome sur Desktop
- ChromeOS, iOS et Android

Traçabilité

- Logs générés en local sur la machine
- Possibilité d'envoi par syslog