STORMSHIELD

STORMSHIELD COLLABORATIVE

ENCRYPTION PLATFORM

ZERO TRUST
DATA CENTRIC SECURITY

CHIFFREMENT
SOUVERAIN

MODE
SaaS/ON-PREM



DATA SECURITY

UNE PROTECTION DE BOUT-EN-BOUT DES DONNÉES SENSIBLES





Data-Centric Security

Notre approche Data-Centric Security apporte une granularité plus fine des contrôles d'accès à l'information pour garantir un niveau de protection plus efficace.

Solution sans concession

Le Zero Trust n'accorde aucune confiance implicite, le déchiffrement se fait uniquement côté client autorisé avec une gouvernance fine des politiques d'accès..

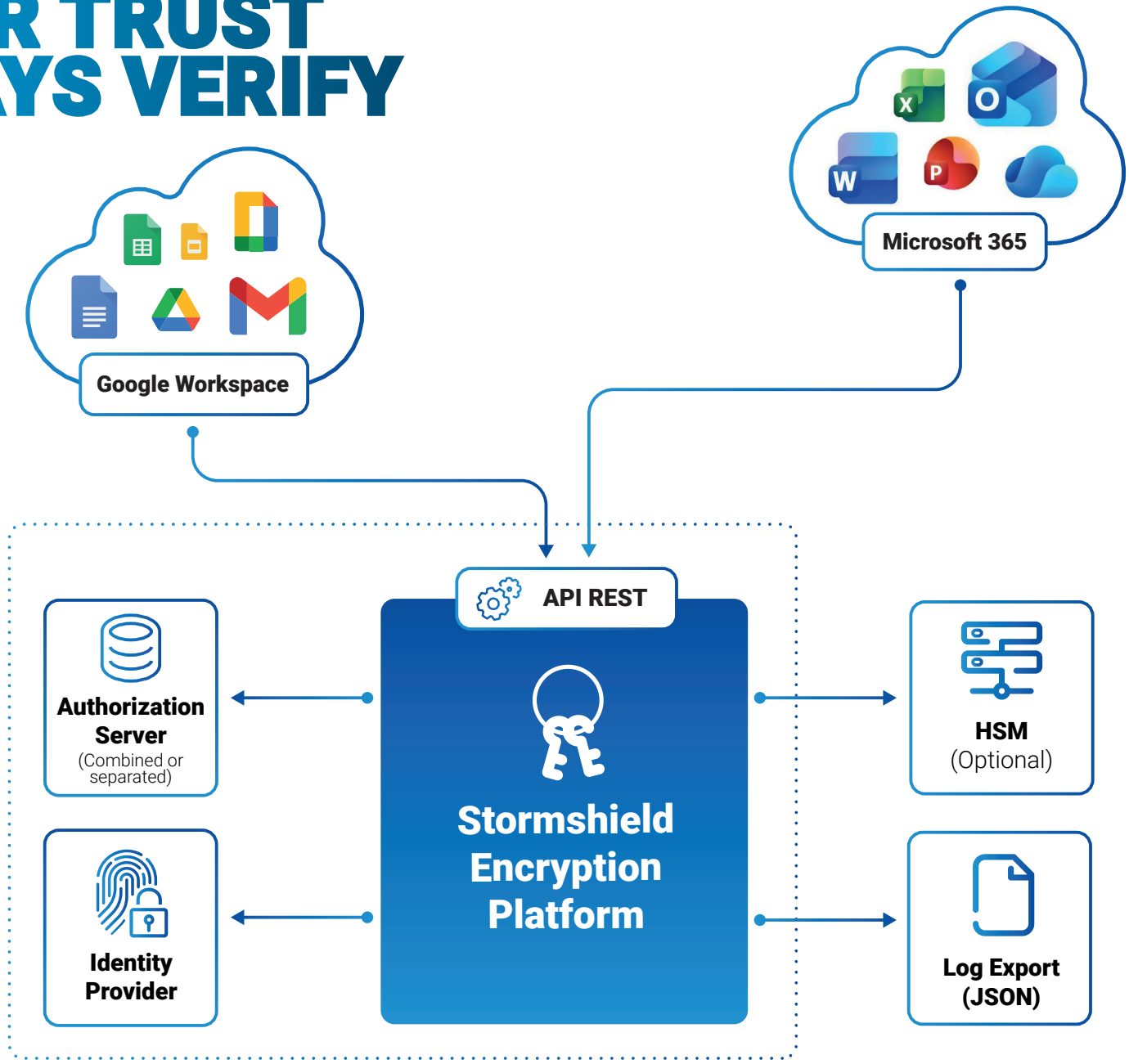
Collaboration sécurisée

Complétement intégrée aux plateformes collaboratives Microsoft 365 et Google Workspace, elle garantit une protection de bout en bout de la donnée en conservant les habitudes des utilisateurs finaux.

POUR UN **CHIFFREMENT SaaS SOUVERAIN**

Stormshield Collaborative Encryption Platform est une solution de chiffrement SaaS souveraine qui renforce la confidentialité des données sensibles et simplifie la mise en conformité aux réglementations comme NIS2, DORA ou RGPD.

NEVER TRUST ALWAYS VERIFY



Maîtrise des données et conformité

Vous conservez le contrôle des données sensibles de votre entreprise et répondez, en la matière, aux exigences de conformité **des réglementations comme DORA ou le RGPD**.

Supervision des accès aux données

Vous **maîtrisez complètement la gestion des clefs** et connaissez les utilisateurs ayant accès aux informations sensibles de son entreprise.

Simplicité de mise en œuvre

Vous utilisez une solution **SaaS clé en main sans agent, sans surcoût** de maintenance et de montée en compétence.

Sérénité

Vos collaborateurs utilisent une solution de cybersécurité qui est **complétement intégrée à leurs outils** et qui ne change pas leurs habitudes de travail.

Gestion des clefs

Seamless Key Management

La solution fournit automatiquement les clés de chiffrement de contenu et effectue les renouvellements nécessaires. La solution permet de révoquer des clés compromises.

Bring/Hold Your Own Key (Option)

Le client gère et fournit les clés de chiffrement qui seront utilisées par la solution (*Bring*). Le client gère une clé principale qui protégera les clés de chiffrement utilisées dans la solution qui ne stockent pas la clé principale (*Hold*).



For Google Workspace

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

Contrôle d'accès
Attribute-Based-Access-Control (ABAC) et Role-Based-Access-Control (RBAC) • Support du standard OPA (Open Policy Agent) pour personnaliser les contrôles d'accès • Intégration avec l'IDP du client (standard OpenID) • Intégration avec un IDP extérieur au client final pour la collaboration externe

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
Sauvegarde et Restauration de configuration • Gestion des Log • Exportation des Logs (Option) • Scalabilité de la solution Onprem (dokerisé)

For Microsoft 365

SDS pour Microsoft 365
Support du mécanisme Double Key Encryption • Vérification des utilisateurs via OpenID • Support des applications Microsoft Word, Excel, Powerpoint • Fonctionnement sans agent avec un simple navigateur (Conservation de l'expérience utilisateur Microsoft)

Contrôle d'accès
Attribute-Based-Access-Control (ABAC) et Role-Based-Access-Control (RBAC) • Support du standard OPA (Open Policy Agent) pour personnaliser les contrôles d'accès • Intégration avec l'IDP du client (standard OpenID) • Intégration avec un IDP extérieur au client final pour la collaboration externe

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
Règlement sur la protection des données (RGPD) • Loi HIPAA (Health Insurance Portability and Accountability Act) • La loi Gramm-Leach-Bliley (GLBA)

Administration centralisée
Sauvegarde et Restauration de configuration • Gestion des Log • Exportation des Logs (Option) • Scalabilité de la solution Onprem (dokerisé)

Encryption Platform *Framework*

Pour répondre aux contraintes techniques et aux besoins spécifiques liés à vos infrastructures, Stormshield vous accompagne avec Encryption Platform Framework (SDK).

LE **CHOIX**
EUROPÉEN
DE LA **CYBERSÉCURITÉ**

www.**stormshield**.com