ORIZON

FOR CLOUD STORAGES

CONFIDENTIALITE DES DOCUMENTS DANS LE CLOUD

ORIZON garantit la confidentialité des fichiers déposés dans le Cloud. Le chiffrement apporte cette protection à la source, depuis le terminal de l'utilisateur. Il permet le droit d'en connaître : les données sont préservées des accès indésirés du fournisseur Cloud, de collaborateurs ou de personnes externes.

Souveraineté de l'entreprise sur ses données

Les services de synchronisation de fichiers dans le **Cloud** ou dans un système interne de type ***EFSS***, pour du stockage, du partage, et de la sauvegarde, exposent les données au vol, à la divulgation et à l'espionnage lors de leur transport et pendant leur stockage. L'entreprise ne maîtrise plus vraiment qui peut avoir accès à ces données et ne connaît pas la porosité ni le niveau d'exposition au risque (ingérence, hacking et brèches de sécurité, personnel du fournisseur Cloud). Le droit d'en connaître assuré par le chiffrement apporte une réponse forte et mathématique qui garantit que les informations ne sont compréhensibles que par les personnes habilitées, tout en conservant la souplesse et l'élasticité du Cloud.

Données synchronisées protégées

ORIZON protège automatiquement les documents stockés par les utilisateurs dans le Cloud. En effet, les fichiers sont chiffrés, dès leur création et en temps réel, sur l'emplacement source. Ils le restent ensuite lors de leur synchronisation, puis leur stockage, chez l'hébergeur (y compris pendant le transport). Ils ne seront déchiffrés que par le ou les utilisateurs habilités (ayant les clés adéquates) sur le terminal de leur choix. Ainsi, seuls ces derniers *comprennent* le contenu de ces documents.

Partages de documents confidentiels

ORIZON chiffre automatiquement tous les documents synchronisés. Si un partage est effectué, l'application des droits cryptographiques en conséquence est réalisée automatiquement, spécifiquement et uniquement pour les ayants droit. Le droit d'en connaître est ainsi également assuré sur les partages Cloud, et **ORIZON** garantit le cloisonnement de ces informations entre utilisateurs, services, prestataires mais surtout avec le fournisseur Cloud. De plus, même les partenaires externes peuvent travailler sur des documents chiffrés qui leur sont partagés grâce à une version gratuite et multiplateforme d'**ORIZON**.

Pas d'impacts sur l'expérience utilisateur

D'une conception volontairement transparente, **ORIZON** demeure très discret et n'impose aucun changement aux utilisateurs dans leurs habitudes de travail. La collaboration et l'ubiquité d'accès aux données (au bureau, à la maison, sur un téléphone, une tablette) sont conservées. Tout type de fichiers peut être chiffré sans interaction avec l'utilisateur.

Gouvernance de la sécurité

ORIZON applique la politique de chiffrement définie par l'Entreprise : partages ou non, ensemble des dossiers synchronisés ou seulement un dossier « coffre-fort ». Différents types de clés d'accès sont possibles (cartes à puce, certificats, mots de passe ...) et des accès de recouvrement (récupération) peuvent être imposés.

Solution légère et non structurante

ORIZON n'impose aucun changement. Présent uniquement sur les postes de travail ou les mobiles, il se déploie comme tous les composants du socle bureautique, se télécharge simplement depuis les magasins d'application de l'Entreprise ou depuis les magasins officiels des terminaux mobiles.

CONNECTEURS

OneDrive

Dropbox

CHIFFREMENT

- Chiffrement par zones des dossiers synchronisés
- Chiffrement à la volée, transparent pour l'utilisateur
- Chiffrement des données partagées en interne ou en externe

AUTHENTIFICATION

- Authentification par certificat (PKI) et/ou mot de passe
- Compatible avec les cartes et tokens des principaux fabricants (postes de travail)
- Compatible Microsoft CSP/CNG

ADMINISTRATION - IT

- Agent logiciel par poste de travail, pas de composant serveur
- Déploiement via les infrastructures IT courantes (SCCM, AD, etc.), disponible sur les stores d'application
- Pas de changement, pas d'impact dans la gestion des ressources IT

ADMINISTRATION - SÉCURITÉ

- Politiques de Sécurité définies par les responsables de la sécurité
- Plan de chiffrement administré
- Supervision de l'application des politiques de sécurité
- Mécanisme de recouvrement des données configurable
- Secours utilisateurs (perte de clé ou de mot de passe)

CARACTÉRISTIQUES TECHNIQUES

- Compatible avec la plupart des solutions d'EFSS du marché (OneDrive™, Google Drive, Box, Dropbox™...)
- **Windows** 7 à 10+
- Chiffrement **AES 256**
- Accès par **certificats/clés RSA** (jusqu'à 4096 bits) et/ou mots de passe (de force configurable)
- Compatible avec les principaux **badges à crypto-processeurs** PKCS#11 (format carte ou USB)

PRIMX
MAKE ENCRYPTION HAPPEN

business@primx.eu – **Tél.: 01 77 72 64 80**
Siège social: 18 Rue du Général Mouton-Duvernet, 69003 Lyon / Direction commerciale: 21 Rue Camille Desmoulins, 92130 Issy-les-Moulineaux
www.primx.eu