

ZONECENTRAL

FOR FILES AND FOLDERS

CONFIDENTIALITÉ ET CLOISONNEMENT

ZONECENTRAL utilise le chiffrement pour apporter un service de confidentialité applicable sur l'ensemble des fichiers d'une organisation. Il permet de gérer le droit d'en connaître et protège les données sensibles contre les accès externes et internes en cloisonnant les informations entre utilisateurs et services ainsi que vis-à-vis des opérateurs IT.

Ségrégation des données sur les postes, les partages et les environnements virtualisés

Protéger les données sensibles contre la perte et la divulgation, mais aussi contre le vol et l'espionnage est un impératif pour les entreprises et entités gouvernementales. Pour garantir la confidentialité de ses données sensibles, une organisation doit pouvoir gérer le droit d'en connaître en s'assurant que les informations à protéger ne sont disponibles que pour les personnes habilitées. Le chiffrement est une technologie parfaitement adaptée pour répondre à ces attentes.

Confidentialité de l'environnement étendu de l'utilisateur

ZONECENTRAL peut chiffrer les fichiers locaux de l'utilisateur et ceux stockés sur des dossiers personnels en réseau, en appliquant automatiquement un cloisonnement cryptographique en conformité avec la politique de chiffrement définie par l'organisation. Les fichiers sont maintenus chiffrés en permanence, seul l'utilisateur est en mesure de comprendre leurs contenus, et ce sans impacter les services IT.

Cloisonnement des dossiers partagés ou personnels sur les serveurs

ZONECENTRAL peut chiffrer automatiquement les fichiers depuis le poste de l'utilisateur lorsqu'ils sont déposés sur les espaces disponibles en réseau (filers, NAS, etc.), en respectant les droits cryptographiques définis sur ces espaces par les responsables de la sécurité. La gestion du droit d'en connaître est ainsi assurée sur les partages

chiffrés et sur les extensions réseau des profils des utilisateurs: **ZONECENTRAL** apporte le cloisonnement entre utilisateurs, prestataires, groupes de travail ou services.

Gouvernance de la sécurité par l'entreprise

ZONECENTRAL applique automatiquement la politique de sécurité de l'entreprise. L'utilisateur fournit simplement sa clé d'accès lorsqu'il démarre sa session de travail, les espaces qu'il utilise sont maintenus chiffrés de façon transparente selon les règles prédéfinies.

Par ailleurs, pour les zones partagées, un outil de supervision permet aux responsables désignés de gérer les accès cryptographiques des groupes d'utilisateurs. Les équipes en charge de la sécurité disposent de moyens de recouvrement et de dépannage (perte de clés, départ d'un collaborateur, audit, etc.).

Solution légère et non structurante

ZONECENTRAL n'impose aucun changement dans la topographie et l'organisation des espaces de stockage. Il n'impose pas non plus de matériel ou de serveur additionnel (ni d'installations sur les serveurs existants). Uniquement présent sur les postes de travail, il se déploie comme tous les composants de la pile de sécurité du socle bureautique.

Pas d'impact sur l'expérience utilisateur

Par nature transparent, puisqu'il applique en arrière-plan les règles de l'entreprise, **ZONECENTRAL** demeure très discret et n'impose aucun changement aux utilisateurs dans leurs habitudes de travail.



CHIFFREMENT

- Chiffrement par zones des dossiers et des fichiers locaux et en réseau (*filers, NAS, SAN*)
- Chiffrement du profil utilisateur étendu (*Bureau, Documents, Homedir, etc.*)
- Chiffrement sur les supports amovibles (*clé USB, disque externe*)
- Chiffrement des fichiers techniques (*temporaires, swap, etc.*)
- Chiffrement des environnements multisessions (*TSE, Citrix™, etc.*)
- Chiffrement à la volée, transparent pour l'utilisateur
- Effacement sécurisé automatique des fichiers (*wiping*)



AUTHENTIFICATION

- Authentification par certificat (*PKI*) et/ou mot de passe
- Compatible avec les cartes et tokens des principaux fabricants
- Compatible Microsoft CSP/CNG
- Gestion coordonnée des accès avec Active Directory
- Gestion de groupes pour les partages
- Renouvellement des accès automatique



ADMINISTRATION - IT

- Agent logiciel poste de travail, pas de composant serveur
- Déploiement via les infrastructures IT courantes (*SCCM, AD, etc.*)
- 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
- Console de supervision des accès aux zones partagées
- Mécanisme de recouvrement des données configurable
- Secours utilisateurs (*perte de clé ou de mot de passe*)



PACKAGING

La licence de ZONECENTRAL intègre les fonctionnalités de ZED! (*conteneurs chiffrés pour les échanges*) et de ZEDMAIL (*plug-in MS Outlook™ pour le chiffrement des courriels*).



CARACTÉRISTIQUES TECHNIQUES

- + **Windows 7 à 11+**
- + Compatible avec tous types de serveurs de fichiers (*Windows, Linux, propriétaire, etc.*)
- + 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*)
- + Compatible avec la plupart des **PKI** (*IGC*) du marché

CERTIFICATIONS



Certification critères communs EAL3+



Visa de sécurité et qualification ANSSI



Protection des données marquées : diffusion restreinte OTAN et UE