Maîtrisez la sécurité de vos échanges de fichiers sensibles

Gouvernance et classification des données

• Classer les données selon leur niveau de sensibilité pour dicter les mesures de sécurité appropriées.

• Appliquer la règle du moindre privilège en limitant les droits d'accès, de modification et de suppression au strict nécessaire.

• Proscrire l'utilisation d'outils de stockage cloud personnels (Shadow IT) via des politiques de filtrage réseau ou de blocage d'URL.

Protocoles de transfert sécurisés

• Garantir le chiffrement de bout en bout des données, aussi bien au repos (stockage) qu'en transit.

• Activer systématiquement l'authentification multifacteurs (MFA) sur l'ensemble des outils de partage.

• Protéger les liens de partage par des mots de passe robustes et une date d'expiration fixe pour limiter l'exposition.

Conformité et surveillance continue

• Vérifier la conformité RGPD du fournisseur, en privilégiant un stockage des données au sein de l'Union européenne.

• Établir une politique de rétention claire pour supprimer automatiquement les accès et les fichiers après la fin d'un projet.

• Conserver et auditer périodiquement les logs d'accès et de transfert pour détecter toute activité anormale ou tentative d'exfiltration.