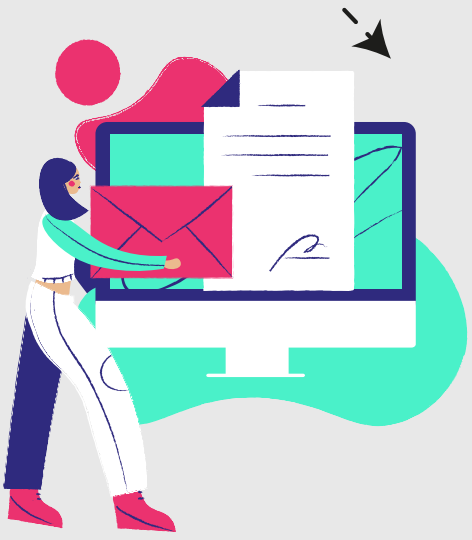
METTRE EN PLACE UNE STRATÉGIE ZERO TRUST

1 Cartographier les accès et les risques

- Identifier qui accède à quelles données
- Détecter les points d'entrée vulnérables
- Supprimer les accès inutiles

2 Installer une authentification forte

- Activer la MFA sur toutes les connexions sensibles
- Opter pour des solutions fluides (SSO, biométrie)
- Appliquer des politiques de mots de passe strictes



3 Segmenter les accès et cloisonner les données

- Créer des zones sécurisées (micro-segmentation)
- Limiter la navigation latérale en cas d'intrusion
- Restreindre l'accès aux fichiers sensibles

4 Surveiller en permanence les activités

- Déployer un SIEM pour analyser les logs
- Configurer des alertes automatiques
- Mettre en place des audits de sécurité réguliers

5 Sensibiliser les collaborateurs

La cybersécurité ne repose pas uniquement sur la technologie, mais aussi sur les bonnes pratiques des utilisateurs. Des formations régulières permettent de réduire considérablement les risques de phishing et d'attaques internes.

epsight

www.epsight.fr