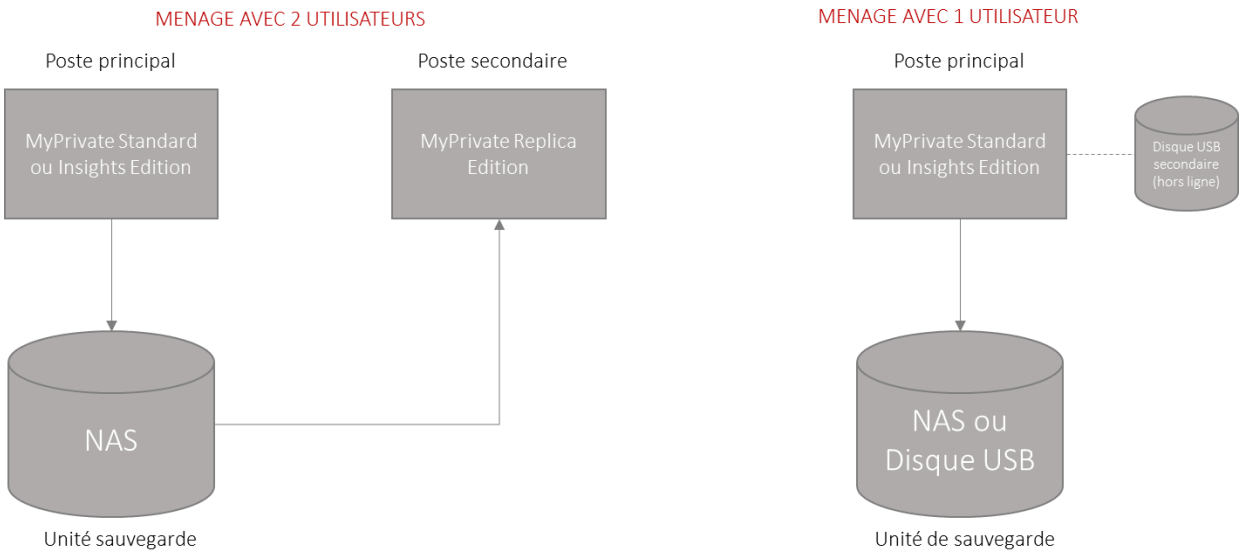
Recommandations concernant la protection des données de MyPrivate

Les utilisateurs de MyPrivate accumulent un historique précieux au cours des années, et il est vital de protéger ces informations contre perte, vol ou corruption.

Bien qu'il n'existe pas de solution 100% sûre, en appliquant les bonnes pratiques il devient fort improbable qu'une perte ou fuite de données se produise.

La plupart des ménages utilisent MyPrivate avec un ou deux utilisateurs ; la configuration minimale du matériel est recommandée ci-dessous pour une protection efficace :



Recommandations pour la configuration

- Windows 10 Professionnel avec téléchargement et installation automatique des mises à jour.
- Utilisation de l'antivirus Windows Defender ainsi que le pare-feu Windows Firewall
- Utilisation d'un VPN lors d'une connexion à un réseau extérieur tel qu'un café, un hôtel ou un aéroport.
- Cryptage des données de vos lecteurs ; pour l'ordinateur principal, l'ordinateur secondaire et les périphériques USB, la fonctionnalité native Windows BitLocker peut être utilisée alors que pour le lecteur NAS, le fournisseur doit fournir ce support de cryptage. En cas de vol de l'ordinateur, disque dur NAS ou USB, les données ne seront pas lisibles par des tiers.
- Pour des ménages avec un seul utilisateur
    - En plus de la sauvegarde sur disque NAS ou USB, un disque USB additionnel est requis pour une sauvegarde mensuelle à l'aide de la fonction native de sauvegarde MyPrivate. Hors de la sauvegarde, cette unité doit-être tenue hors-ligne.

En cas d'infection par rançongiciel de l'ordinateur principal et / ou NAS, ce stockage hors-ligne restera ainsi intact.

- Pour des ménages avec deux utilisateurs
    - Pas de partage de fichiers entre l'ordinateur principal et l'ordinateur secondaire ; cela garantit une protection en cas d'infection d'un des deux ordinateurs et / ou NAS.
    - Sur l'ordinateur principal, activation de l'historique des fichiers Windows ; ceci avec une fréquence de mise à jour quotidienne, ainsi qu'activation de la sauvegarde native MyPrivate avec fréquence hebdomadaire.
    - Plusieurs options de récupération restent disponibles en cas de corruption de disque, de la base de données, de l'ordinateur ou du NAS.
- L'ordinateur principal et secondaire, ainsi que le NAS et/ou disque USB ne doivent jamais être laissés physiquement au même endroit pour se protéger contre le vol ou dégâts d'eau ou incendie.
- Configuration du navigateur Web avec des liens prédéfinis vers des sites communs tels que les institutions financières ; ceci réduit le risque de devenir une victime de phishing.
- Activation d'un économiseur d'écran avec mot de passe avec un court délai d'attente, protégeant contre un accès non autorisé dans des lieux publics.
- Lecture attentive des directives de sécurité concernant la gestion des codes dans le module « Famille » de MyPrivate.
- Aucune utilisation de fonctions de stockage « Cloud » telles que OneDrive et DropBox pour stocker les données MyPrivate.
- Des clés USB ne doivent pas être branchées sur l'ordinateur à moins d'être d'une origine sûre : il existe des cas de clés USB infectées par des virus et / ou de rançongiciel.