TeraStation™

BUFFALO™

Le NAS le plus sécurisé du marché

Alors que les risques de cyberattaque (notamment par ransomware) ou d'espionnage industriel sont à la hausse, les réglementations européennes relatives à la protection des données à caractère personnel se font plus strictes, notamment avec l'entrée en application, en mai 2018, du RGPD (Règlement général sur la protection des données). Pour protéger leurs propres informations confidentielles et celles de leurs clients, les entreprises se doivent de mettre en place des solutions de stockage fiables et sécurisées.

La plupart des structures de petite ou moyenne taille stockent, sauvegardent et partagent leurs fichiers par le biais de périphériques de stockage réseau (NAS). Buffalo, fabricant renommé de NAS, met un point d'honneur à assurer la protection des données de ses clients. Ses produits constituent des solutions sûres sous bien des aspects.

Système fermé

Configuration sécurisée

Chiffrement des données

Protection contre le vol
- Protection logicielle : authentification au démarrage
- Protection physique

Mots de passe

Antivirus
(TS3000/3010 et TS5000/5010 ; vendu séparément)

Sauvegarde, réplication, reprise et chiffrement

www.buffalo-technology.fr

TeraStation™

Méthodes de protection

Système fermé

Il s'agit de l'une des caractéristiques essentielles des NAS de Buffalo : les systèmes sont fermés et même les administrateurs ne disposent pas de droits de super-utilisateur. Beaucoup de périphériques concurrents autorisent l'installation d'applications tierces via une boutique dédiée. Cependant, ceci peut être la porte ouverte aux logiciels malveillants, logiciels espions et autres virus. La solution TeraStation ne se connecte qu'aux services réseaux disponibles. Afin de limiter les risques, vous pouvez activer uniquement ceux dont vous avez besoin, ainsi que les ports LAN appropriés.

Configuration sécurisée

La protection commence par une configuration adéquate. Avec les TeraStation, Buffalo a toujours préféré une configuration locale. La configuration ne nécessite aucune connexion à Internet. Contrairement à d'autres fournisseurs, Buffalo n'exige pas la création d'un compte en vue de la gestion à distance du périphérique. Ainsi, ni identifiants ni mots de passe, cibles potentielles des attaquants, ne sont requis.

Chiffrement

Chiffrement des disques : les données inscrites sur les disques durs peuvent être chiffrées à l'aide de l'algorithme AES 256 bits[1]. Cela permet d'empêcher, en cas de vol des disques de l'unité, que les informations soient lues par un PC ou par un autre périphérique TeraStation.

Chiffrement des données transférées : la connexion établie lors de la gestion à distance de votre TeraStation ou de l'utilisation du service WebAccess est protégée par le protocole HTTPS, qui assure le chiffrement des données transférées. Par ailleurs, les unités TeraStation prennent en charge le protocole SFTP, afin de sécuriser les transferts de fichiers entre les hôtes du réseau.

Protection contre le vol

Protection logicielle : authentification au démarrage (gammes TS3010 et TS5000/5010)

Au démarrage, l'unité est automatiquement connectée, par le biais d'un réseau local ou VPN, à un serveur ou un PC Windows doté d'un outil de gestion de l'authentification. Si l'authentification échoue, ou si l'unité est bloquée par l'outil de gestion, la TeraStation ne démarre pas et ne peut pas être réinitialisée. Cette procédure a pour but d'éviter le démarrage non autorisé ou la réinitialisation d'un périphérique volé. L'outil de gestion de l'authentification pour PC Windows permet de gérer plusieurs TeraStation. Les problèmes peuvent ainsi être résolus plus rapidement. Si la fonctionnalité d'authentification au démarrage est activée, les données sont automatiquement cryptées par le biais de l'algorithme AES 256 bits.

Le bouton de réinitialisation peut être désactivé (même sur les anciens modèles ne profitant pas de la fonctionnalité d'authentification au démarrage), afin d'empêcher l'utilisation de l'unité après un vol.

Protection physique

Tous les périphériques TeraStation (versions de bureau et en rack) ont des encoches pour les antivols Kensington. Les versions de bureau disposent même de portes qui ferment à clé empêchant le retrait des disques.

Mots de passe

Un mot de passe est exigé pour pouvoir gérer les unités TeraStation. Vous pouvez également définir d'autres mots de passe afin de restreindre l'accès aux fichiers. Les gammes TS3010 et TS5010 prennent en charge les listes de contrôle d'accès des sous-dossiers et fichiers. Ces listes permettent une gestion des droits très précise, contrairement aux systèmes de contrôle des accès classiques. Par ailleurs, des mots de passe empêchent des NAS secondaires de détecter ou d'utiliser le TeraStation pour des tâches de sauvegarde ou de réplication.

Antivirus*

Une fonction d'analyse prévient la propagation des virus sur votre réseau. Si un PC compromis se connecte et envoie des données infectées à la TeraStation, le virus est automatiquement détecté et mis en quarantaine afin d'empêcher qu'il ne se répande sur d'autres appareils.

*TS3000/3010 et TS5000/5010 ; licence à acheter pour l'activer

Sauvegarde, réplication, reprise et chiffrement

Les sauvegardes ne constituent pas à proprement parler une fonction de sécurité, mais elles vous protègent des pertes de données en cas de faille ou d'attaque sur votre système. Elles sont indispensables, dans un contexte professionnel comme privé. Les périphériques TeraStation offrent quantité d'options de protection : fonctions de sauvegarde (via USB ou le réseau), réplication, réplication chiffrée[2], sauvegarde ou réplication via Rsync et le protocole SSH[3] (pour le chiffrement des transferts), reprise et sauvegarde dans le cloud.

[1] Les périphériques TS3010/TS5010 utilisent le chiffrement AES 256 bits ; tous les autres modèles ont recours au chiffrement AES 128 bits.
[2] Sauf pour le modèle TS5000
[3] Pris en charge uniquement par le modèle TS3010/5010