



Engagements de moyens sur les architectures WAYNIUM

Ce document présente les **moyens garantis** par WAYNIUM pour tendre vers une **disponibilité et une sécurité maximale de ses services**.

Disponibilité des services

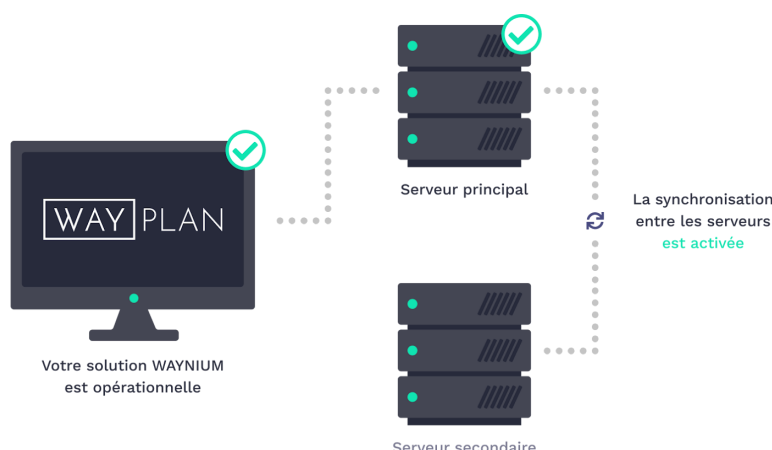
Architecture déployée du parc de serveurs

Les solutions WAY-Plan sont distribuées sur des dizaines de serveurs, entièrement infogérés par WAYNIUM. Le parc de serveurs est réparti chez deux fournisseurs et dans des data centers multiples.

WAYNIUM dispose d'outils permettant le déploiement rapide des solutions WAY-Plan, facilitant leur installation, leur migration et leur mise à jour. L'ensemble des solutions sont monitorées 24h/24 et 7j/7, afin de garantir une haute disponibilité des services.

A noter : il est possible au client des services WAY-Plan de souscrire l'option "serveur dédié", pour garantir 100% de la performance de l'hébergement qui lui sera attribué.

Synchronisation sur serveur distant



Les solutions WAY-Plan sont toutes synchronisées en temps réel sur un second serveur distant, volontairement hébergé dans un data center différent, et chez un fournisseur différent.

En cas de panne serveur, ou data center, il est possible d'accéder à l'ensemble de ses données sur sa solution de secours en modifiant l'url d'accès à sa solution de la façon suivante : remplacer la terminaison de l'url en ".com" par ".net".

Une fois le serveur principal rétabli, les données sont synchronisées à nouveau, de façon à ne perdre aucune trace de l'activité réalisée sur le serveur de secours.

Sécurité des données

Tests d'intrusion et cybersurveillance

WAYNIUM dispose de ressources indépendantes, expertes en cybersécurité, lui permettant de déployer des plans successifs d'amélioration de la sécurité de ses solutions.

Date du dernier test d'intrusion réalisé : du 4 au 9 Septembre 2023

Aucune faille critique ou majeure n'a été relevée lors du test.

Sauvegarde cryptée des bases de données.

Ce procédé a deux objectifs :

- rendre inefficace toute tentative de hameçonnage des données clients
- permettre de réinstaller tout ou partie des données clients, sur la solution du client ou sur une solution tierce

Deux serveurs viennent à fréquence « horaire » récupérer l'intégralité des bases de données sur les serveurs de nos clients. Ces deux serveurs n'ont aucun lien entre eux et agissent en toute indépendance, ils sont positionnés chez des fournisseurs différents, dans des data centers différents.

Chaque serveur de sauvegarde **crypte les données** via le protocole "PGP" (Pretty Good Privacy).

Lien Wikipédia : https://fr.wikipedia.org/wiki/Pretty_Good_Privacy

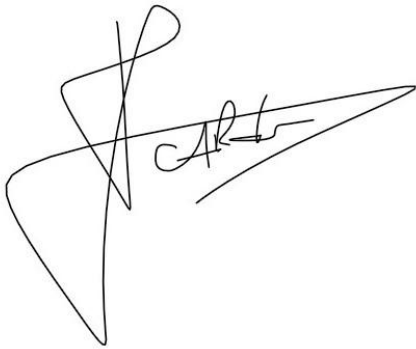
L'accès à ces serveurs n'est autorisé que pour les trois ressources de confiance suivantes :

- le CTO de WAYNIUM (20 ans d'ancienneté dans l'entreprise)
- le responsable technique "architecture" (plus de 15 ans d'ancienneté dans l'entreprise)
- le consultant expert technique externe en charge de la surveillance et de la maintenance des serveurs (accès avec des droits limités, sans possibilité de décryptage des données de sauvegarde)

Seules les ressources de confiance peuvent accéder aux serveurs de sauvegarde (via les clés SSH stockées sur leur poste de travail en local).

Le processus de cryptage inversé (via un logiciel spécialisé) n'est possible que par une clé "privée" stockée sur les postes des deux ressources autorisées. En cas d'incident quel qu'il soit, cette procédure leur permet de télécharger en local les fichiers cryptés, de les lire, et de les réinstaller sur une nouvelle solution.

Ce document vaut pour engagement de moyens de la société WAYNIUM

A handwritten signature in black ink, appearing to read 'CARLIER', with a large, stylized flourish to the left.

Bruno CARLIER, président.