Vaultwarden

Gestionnaire de mots de passe auto-hébergé

Un coffre-fort numérique **sécurisé**, open source, entièrement sous votre contrôle — sans dépendance à un cloud externe.

🔐 Auto-hébergé

Vos données restent sur votre infrastructure

⚙️ Open Source

Alternative légère et fiable à Bitwarden

☁️ Zéro cloud externe

Maîtrise totale, sans tiers de confiance

Contexte & Problématique

Les risques actuels

- Mots de passe stockés dans des fichiers non sécurisés ou des Post-it
- Risques élevés de fuite, vol ou perte d'accès
- Gestion multi-appareils complexe et incohérente

Nos objectifs

- Centraliser tous les accès dans un coffre-fort unique
- Sécuriser les identifiants critiques de l'organisation
- Offrir un accès simple, rapide et fiable depuis tous les supports

La Solution Choisie : Vaultwarden

Vaultwarden est une implémentation légère et open source du protocole Bitwarden, conçue pour fonctionner sur des infrastructures modestes tout en restant pleinement compatible avec l'écosystème Bitwarden.

Léger & Efficace

Idéal sur une VM ou un Raspberry Pi. Consommation mémoire minimale comparée au serveur Bitwarden officiel.

100 % Open Source

Code auditable, communauté active, aucune licence propriétaire — transparence totale.

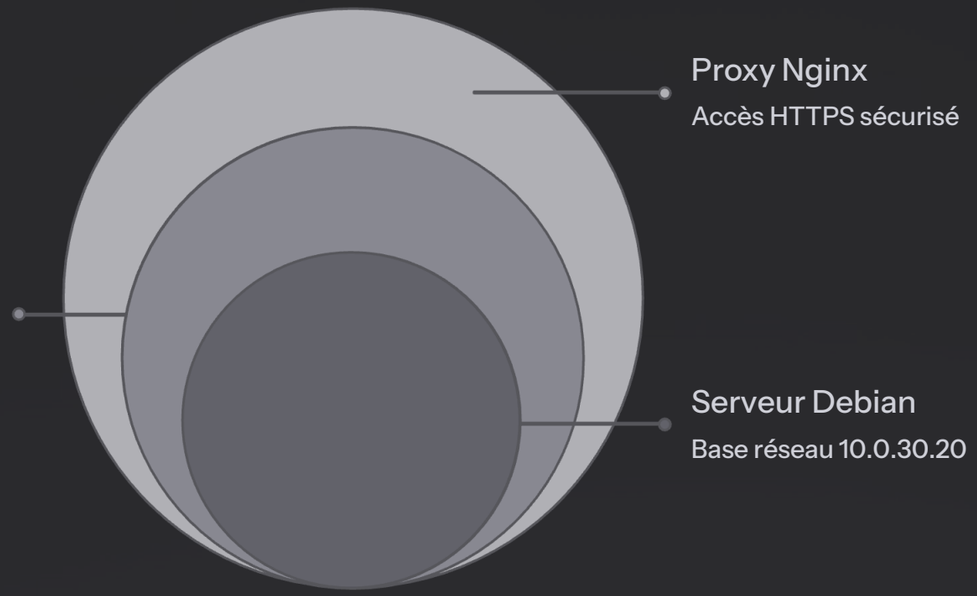
Compatibilité totale

Fonctionne avec toutes les applications Bitwarden : mobile iOS/Android, extensions navigateur, client desktop.

Gratuit

Aucun coût de licence. Déploiement illimité sur votre propre infrastructure.

Architecture de Déploiement



Points d'accès utilisateurs

Navigateur web

Interface complète via HTTPS

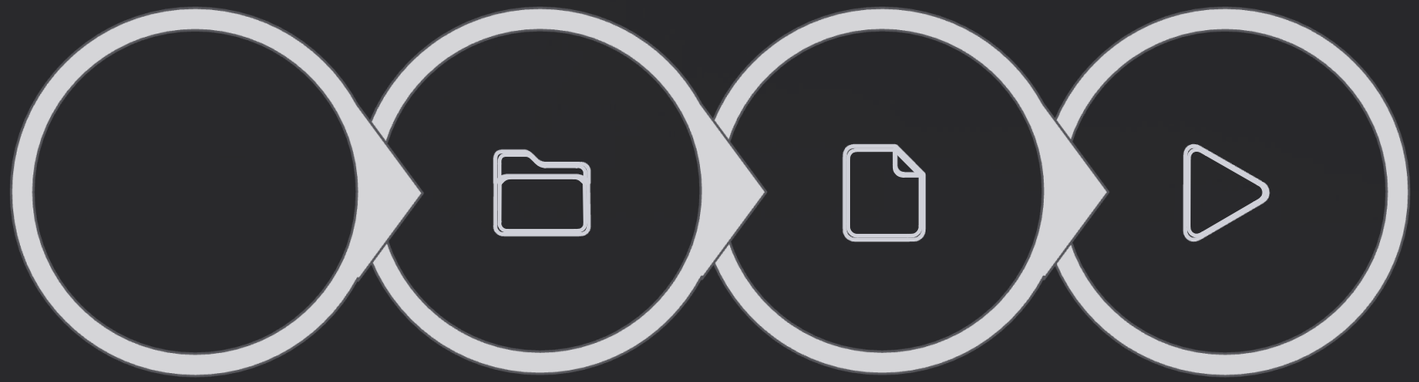
Application mobile

iOS & Android natif

Extension navigateur

Chrome, Firefox, Edge...

Installation via Docker



Installer Docker

Créer /opt/vaultwarden

Rédiger docker-compose.yml

Lancer le conteneur

Le conteneur démarre automatiquement au boot du serveur grâce à la politique de redémarrage `restart: always` définie dans le compose.

Structure du projet

```
/opt/vaultwarden/
├── docker-compose.yml
└── data/
    ├── db.sqlite3
    ├── attachments/
    └── config.json
```

Le dossier `data/` contient l'intégralité des données chiffrées. Il doit impérativement être sauvegardé régulièrement.

Configuration Nginx & HTTPS

Reverse Proxy

Nginx redirige les requêtes entrantes vers le conteneur Vaultwarden en local sur le port dédié.

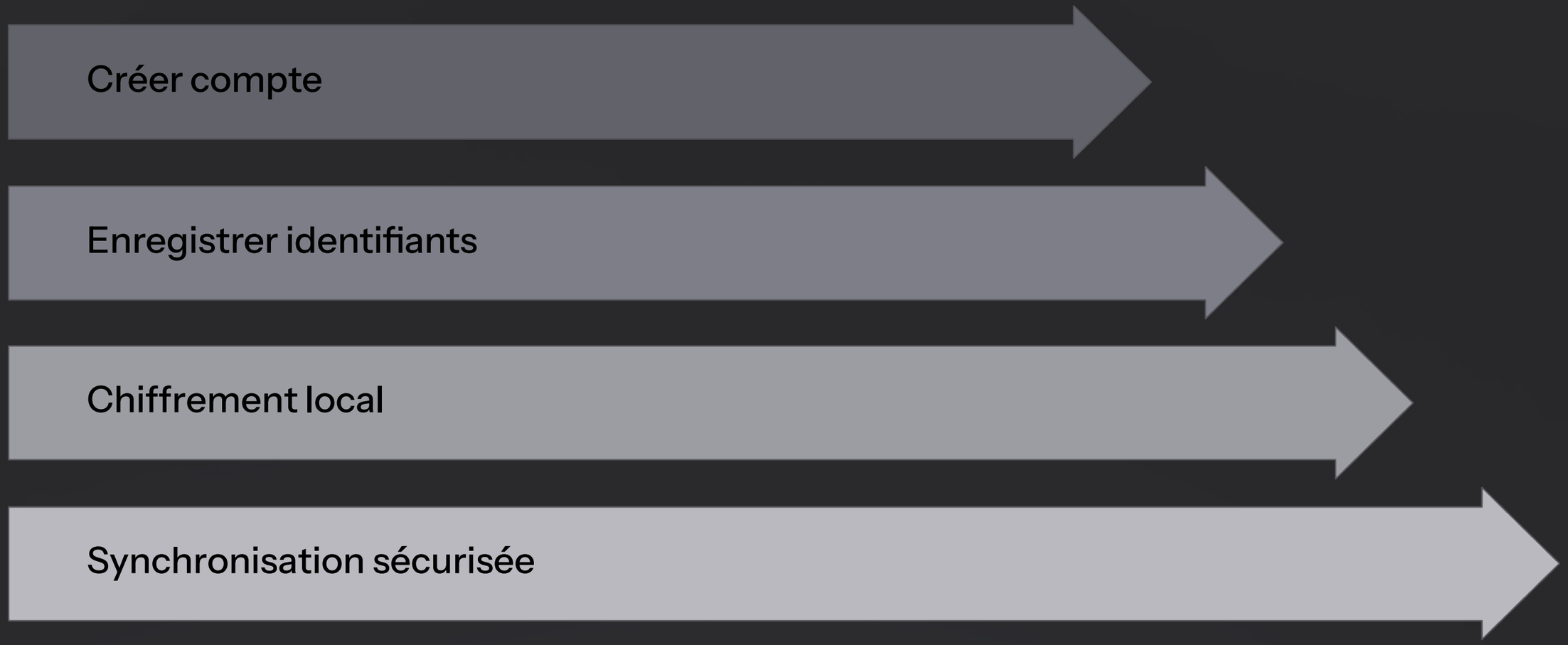
Redirection HTTP → HTTPS

Toute connexion non chiffrée est automatiquement redirigée vers HTTPS — aucun accès en clair possible.

Certificat SSL

Certificat Let's Encrypt gratuit, renouvelé automatiquement via Certbot. Chiffrement TLS en transit.

Comment ça fonctionne ?



Le chiffrement s'effectue **côté client**, avant tout envoi vers le serveur. Même l'administrateur système ne peut pas lire les mots de passe stockés en clair.

Sécurité : Maîtrise Totale

🔐 Chiffrement de bout en bout

AES-256 côté client. Les données transitent et sont stockées de manière chiffrée — le serveur ne voit jamais les données en clair.

🔑 Mot de passe maître unique

Seul l'utilisateur détient la clé de déchiffrement. En cas d'oubli, aucune récupération n'est possible — c'est une garantie de confidentialité.

🌐 Aucune dépendance cloud

Les données ne quittent jamais votre infrastructure. Pas de tiers, pas de RGPD tiers à gérer, pas de risque d'exposition externe.

Avant / Après Vaultwarden

ÉTAT ACTUEL

Mots de passe dispersés

Fichiers et notes éparpillés.

Risques élevés de sécurité

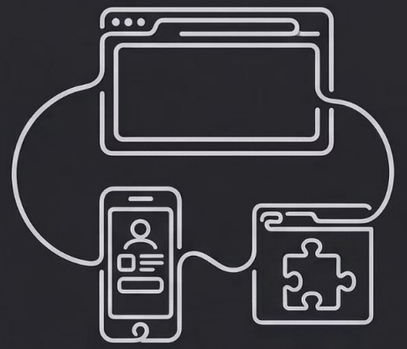
Aucun chiffrement.

Absence de centralisation

Perte d'accès facile.

Coffre-fort chiffré, point d'accès unique

Sécurité maximale, gestion centralisée.



Accès multi-appareils : navigateur, mobile, extension

Synchronisation transparente, gestion simplifiée.

Cas d'Usage

Comptes professionnels

Centralisation de tous les accès applicatifs métier : ERP, CRM, outils SaaS internes.

Gestion des accès IT

Mots de passe d'infrastructure (serveurs, switches, routeurs, VPN) stockés et accessibles de manière sécurisée.

Partage sécurisé

Partage d'identifiants entre collaborateurs autorisés via des organisations Vaultwarden, sans exposer le mot de passe.

Identifiants critiques

Stockage des clés API, certificats, accès bases de données et secrets sensibles de l'organisation.

Bonnes Pratiques

1

Sauvegarde régulière

Sauvegardez le dossier `/opt/vaultwarden/data` quotidiennement. C'est l'unique source de vérité de vos coffres.

2

HTTPS obligatoire

N'exposez jamais Vaultwarden en HTTP. Un certificat SSL valide est indispensable pour chaque accès.

1

Double authentification (2FA)

Activez le TOTP (Google Authenticator, Aegis...) sur tous les comptes utilisateurs pour une protection renforcée.

2

Accès restreint

Limitez l'exposition du service au réseau interne (LAN) ou via VPN. Évitez une exposition directe sur Internet.

Conclusion & Perspectives

✅ Sécurité renforcée

Chiffrement de bout en bout, 2FA, accès contrôlé — une posture de sécurité professionnelle.

🏠 Indépendance totale

Aucune donnée ne quitte votre infrastructure. Conformité RGPD facilitée, zéro dépendance fournisseur.

🚀 Évolutivité

Intégration LDAP/SSO envisageable pour une gestion centralisée des utilisateurs à l'échelle de l'entreprise.

Prochaine étape : Intégration avec l'annuaire Active Directory via LDAP et déploiement à l'échelle de l'organisation pour une gestion unifiée des identités.