novarina
novamat
novasanit

Résumé
Logiciel d'archivage des documents de l'entreprise

Yanis DAHMAN
informatique@novarina.fr

LIVRABLES

Déploiement d'un gestionnaire de mots de passe

Table des matières

I. Contexte

La sécurité informatique est un enjeu majeur pour les entreprises.

Une mauvaise gestion des mots de passe (mots de passe trop simples, réutilisés ou notés sur des supports non sécurisés) peut entraîner des risques importants : accès non autorisés, perte de données ou incidents de sécurité.

Dans ce contexte, l'entreprise souhaite mettre en place un outil de gestionnaire de mots de passe permettant aux collaborateurs de stocker et d'utiliser leurs mots de passe de manière sécurisée.

Je participe donc activement à ce projet, depuis la compréhension du besoin jusqu'au déploiement de la solution et à l'accompagnement des utilisateurs.

II. Note de cadrage

A. Comprendre ce qu'est un gestionnaire de mots de passe :

Un gestionnaire de mots de passe est un outil de sécurité qui permet aux collaborateurs de générer et stocker des mots de passe de manière sécurisés

Voici quelques fonctionnalités de celui-ci :

Le Coffre-fort unique : Une application qui garde tous tes codes au même endroit. Tu n'as plus qu'à retenir **un seul** mot de passe pour entrer dedans.

Le Remplissage automatique : Quand tu arrives sur un site, l'outil remplit tout seul ton identifiant et ton mot de passe. Plus besoin de les taper au clavier.

La Création de codes "incassables" : Quand tu crées un nouveau compte, l'outil te propose un mot de passe robustes pour que personne ne puisse le deviner.

L'alerte "Mots de passe faibles" : L'outil te prévient si tu utilises un mot de passe trop simple (comme 123456) ou si tu utilises le même partout.

Dans notre cas, nous avons besoins de certaines fonctionnalités particulières :

Importation simplifiée : La solution doit être capable d'importer automatiquement ou très facilement les mots de passe actuellement stockés dans des navigateurs Chrome, Edge)

Facilité d'utilisation : L'interface doit-être intuitive, en français, s'intégrer discrètement aux navigateurs sans perturber les habitudes de travails.

Intégration Active Directory : Afin de faciliter l'adhésion des utilisateurs et la gestion par le service informatique, la solution étudiée devra idéalement s'interfacer avec notre annuaire Active Directory afin de permettre aux nouveaux utilisateurs d'y avoir accès et aux anciens de ne plus avoir accès

B. Identifier les problèmes actuels et les risques associés

L'audit des pratiques aux seins des différents bureaux a permis de mettre en évidence plusieurs problèmes critiques.

Absence d'outil centralisés : L'entreprise ne dispose actuellement d'aucune solution de gestion commune pour les mots de passe et identifiants.

- **Accès non autorisés :** La perte d'un support physique (post-it, carnet) ou le vol de donnée sur le navigateur compromet immédiatement les comptes associés

Stockage non sécurisé dans les navigateurs : La majorité des collaborateurs utilisent la fonction de mémorisation des navigateurs (Chrome, Edge), ce qui expose les accès en cas d'infection par un logiciel malveillant.

- **Vol de données :** Des virus spécialisés (Infostealers) peuvent aspirer ces bases de données en quelques secondes.

Réutilisation des mots de passe : L'emploie d'un mot de passe pour tout l'accès est dangereux, chaque accès doit avoir son mot de passe associé.

- **Effet domino :** Si un service tiers est piraté, l'attaquant peut utiliser ce code pour se connecter à d'autres services tiers.

Faible complexité des mots de passe : De nombreux mots de passe utilisés sont trop simples et ne respectent pas les standards de sécurité actuels.

- **Attaque par force brute :** Un mot de passe simple peut être cassé en quelques minutes par des outils automatisés

C. Comprendre les objectifs du projet et les acteurs impliqués

1. Objectif principal

- Mettre en place et déployer une solution de gestionnaire de mots de passe destinée aux collaborateurs de l'entreprise.

- Réduire les risques d'accès non autorisé et de perte de donnée liés à une mauvaise gestion des mots de passe (navigateur, support non sécurisés).

- Sensibiliser les utilisateurs aux enjeux de la sécurité informatique et les accompagner dans la prise en main d'un nouvel outil.

2. Objectifs pédagogiques

- Comprendre les enjeux de bases de la sécurité des systèmes d'information
- Suivre une méthodologie en gestion de projet
- Participer au choix et a l'analyse d'une solution informatique
- Rédiger des documents clairs (guides, procédures, synthèses)

3. Acteurs impliqués

Le Responsable du Système d'Information (RSI) : En tant que tuteur de stage, il assure l'encadrement, définit les orientations techniques et valide chaque étape et livrable du projet.

Le Chef de Projet (Stagiaire) : Responsable de la mise en œuvre opérationnelle, incluant l'étude comparative, la mise en place du test pilote, la rédaction des guides et le support aux utilisateurs.

Les techniciens du Système d'information (TSI) : Fournit le support nécessaire au bon déroulement des opérations de déploiement

Les Collaborateurs (Utilisateurs finaux) : Ce sont les bénéficiaires de la solution qui devront adopter l'outil au quotidien pour sécuriser leurs accès professionnels.

III. Organisation et planification

A. Différentes étapes du projet :

1. Découverte et cadrage du projet

- Découvrir le service informatique et son fonctionnement
- Comprendre ce qu'est un gestionnaire de mots de passe
- Identifier les problèmes actuels et les risques associés
- Comprendre les objectifs du projet et les acteurs impliqués

2. Organisation et planification

- Découper le projet en étapes simples
- Construire un planning prévisionnel
- Identifier les principaux risques (techniques et humains)

3. Etude des solutions existantes

- Étudier plusieurs solutions de gestionnaires de mots de passe
- Comparer les solutions selon des critères simples :
  - Facilité d'utilisation
  - Sécurité
  - Coût
  - Compatibilité
- Présenter une recommandation argumentée

4. Déploiement pilote

- Installer et configurer la solution choisie avec l'aide du tuteur
- Mettre en place un groupe test d'utilisateurs
- Tester la solution et recueillir les retours

5. Déploiement et accompagnement

- Participer au déploiement de la solution auprès des collaborateurs
- Créer des supports simples d'accompagnement
- Aider les utilisateurs lors de la prise en main

6. Documentation et bilan du stage

- Finaliser la documentation du projet
- Rédiger un bilan de stage
- Présenter les résultats du projet et les enseignements tirés

B. Planning Prévisionnel du projet

Déploiement d'un gestionnaire de mots de passe

Yanis DAHMAN | Janvier-Mars 2026

	Semaine 1	Semaine 2	Semaine 3	Semaine 4	Semaine 5	Semaine 6
Découverte et cadrage du projet						
Organisation et planification						
Etude des solutions existantes						
Déploiement du pilote						
Déploiement et accompagnement						
Documentation et bilan du stage						

C. Principaux risques (techniques et humain)

1. Risques Techniques

Risques Techniques	Gravité
Erreur lors du déploiement du logiciel sur les postes utilisateurs	**Critique**
Erreur de synchronisation entre le Gestionnaire de mot de passe et l'Active Directory (si le choix porte sur un GMP avec AD)	**Fort**
Echec ou corruption des données lors de l'importation des mots de passe entre le Navigateur → GMP (Gestionnaire de mot de passe)	**Fort**
Echec de déploiement de la GPO pour désactiver le Gestionnaire de mot de passe du navigateur	**Critique**

2. Risque Humains

Risques Humains	Gravité
Oubli définitif du Mot de Passe Maître (Si le choix porte sur un GMP sans intégration AD)	**Critique**
Divulgation du mot de passe maître via de l'hameçonnage ou autre	**Critique**
Non-respect du GMP via l'utilisation d'un autre recours	**Modérée**
Mot de passe maître pas assez robuste (Si le choix porte sur un GMP sans intégration AD)	**Fort**

IV. Périmètre du projet

A. Périmètre

Organiser en plusieurs étapes :

D'abord faire les tests sur le service informatique → Novarina → Novamat → Novasanit

B. Communication

Pour le support de communication, envoyer un **teams/mails** avec un formulaire afin de vérifier qui à installer + importer les mots de passe

V. Etude des gestionnaires de mots de passe

A. Tableau comparatif des solutions

	BitWarden	***Keeper Security***
Licence	Open source : Code transparent	Propriétaire : Code fermé, confiance total accordée à l'éditeur
Facilité d'utilisation	Pour l'utilisateur : Simple, sobre et efficace. Pour les administrateurs : Guide complet sur Help Center | Bitwarden	Pour l'utilisateur : Parfois jugé complexe ou moins intuitive, mais beaucoup plus riches en fonctionnalités Pour les administrateurs : Guide complet sur Keeper Docs Portal | Keeper Documentation
Sécurité	Chiffrement AES-256 bit "Zero-Knowledge".	Chiffrement AES-256 bit "Zero-Knowledge".
Fonctionnalité Entreprise	Solides (Politiques, Logs, API, SSO/SCIM en Entreprise), **Auto-Hébergement**	Très riches (Politiques granulaires, Rapports avancés, Rotation de secrets, Connexions distantes sécurisées, Alertes)
Synchronisation Utilisateurs	**(SCIM) :** Synchro directe avec Entra ID	**(SCIM) :** Synchro directe avec Entra ID
Conformité RGPD	Conforme RGPD, Hébergement en Allemagne (Francfort)	Conforme RGPD, Hébergement en Allemagne et en Irlande
Support Client	Priorité aux entreprises, Dispo 24/7	Service réactif, Dispo 24/7
Coût	6$ / Utilisateurs / Mois avec (Essai entreprise 7 jours)	5$ / Utilisateurs / Mois avec un minimum de 5 utilisateurs à l'achat

B. Recommandation argumentée

Suite au tableau comparatif entre BitWarden et Keeper Security, mon choix s'est porté sur BitWarden.

En effet, les deux solutions présentent pourtant des fonctionnalités techniques similaires. Elles répondent toutes deux aux exigences essentielles du projet.

Cependant BitWarden se démarque nettement sur la flexibilité avec 2 avantages en comparaison avec Keeper Security :

- A l'achat, BitWarden ne nécessite aucun montant minimum d'utilisateurs. Il dispose par ailleurs d'un essai gratuit qui va me permettre de faire des tests techniques.
- Contrairement à Keeper Security qui nécessite un minimum de 5 utilisateurs à l'achat.
- De plus, BitWarden est Open Source, son code est public ça nous garantit une transparence totale sur la sécurité.

VI. Plan d'action phase de test

A. Mise en place de l'environnement

1. Préparation

- S'inscrire sur le site web avec un compte administrateur
  Ce compte sera l'administrateur du GMP
- Choisir l'offre entreprise
- Remplir les infos nécessaires

2. Accès à la console

- Ouvrir l'application
- Se rendre dans la console Admin

3. Liaison et Activation

On va ensuite lier BitWarden à l'Entra ID, puis activer l'authentification SSO. Pour la méthode, voir documentation ci-dessous.

Mise en œuvre de l'ID SAML de Microsoft Entra | Bitwarden

Bien choisir « Trusted Devices » Pour permettre aux utilisateurs de se connecter via le SSO sans avoir à créer ni retenir de mot de passe maître.

Configurer le SSO avec des appareils de confiance | Bitwarden

4. Paramétrages des politiques de sécurité

Pour la méthode, voir la documentation ci-dessous

Politiques de sécurité de l'Entreprise | Bitwarden

Activer les paramètres suivants :

- Activer la saisie automatique
- Organisation Unique
- Exiger l'authentification par connexion unique (SSO)
- Générateur de mot de passe
- Administration de récupération de comptes
- Inscription Automatique

5. Synchronisation des utilisateurs (SCIM)

Automatiser la création des comptes (Provisioning) et la désactivation instantanée en cas de départ d'un collaborateur.

Pour la méthode, voir documentation ci-dessous

Microsoft Entra ID SCIM Integration | Bitwarden

Attention : Lors de la phase de test se rendre Dans Entra ID > Application Bitwarden > Utilisateurs et groupes : **Ne sélectionner QUE votre compte admin et les testeurs**

Pourquoi ? L'activation du SCIM envoie automatiquement un email d'invitation. Si le groupe "Tous les utilisateurs" est sélectionné maintenant, toute l'entreprise recevra un email non sollicité (spam), ce qui générera des incidents au support.

Vérifier ensuite que les personnes synchronisées pour la phase de test apparaissent bien dans Bitwarden

6. Vérification de mon côté

- Lancer l'application de bureau Bitwarden.
- Ensuite, se connecter avec un des comptes sélectionnés pour la phase de test.
- Se connecter avec le SSO
  - **Validation 1 :** L'application ne doit **PAS** demander de créer un mot de passe maître.
  - **Validation 2 :** L'application doit afficher *"Approbation de l'appareil en attente"* (ou se connecter si l'auto-approbation est active).
- Si le message apparaît *:* Le paramètre "Trusted Devices" est fonctionnel.

Action finale : Valider l'appareil dans la console Admin. L'accès au coffre est alors ouvert.

7. Déploiement de l'application Bitwarden

- Création d'une seule GPO de Bitwarden qui va déployer **l'application bureau** et **l'extension**.
- Création d'une GPO pour la désactivation des mots de passes qu'on activeras seulement sur les personnes ayant déjà fait l'importation

Vérifier sur les postes concernés que les 2 GPO fonctionnent bien

8. Attributions des droits

Maintenant que le service informatique a accès au GMP, il faut leur donner les **permissions** adéquate.

Donc on accordera le niveau de privilège maximale à tous les membres du services informatiques. Ca va donc permettre à chaque administrateur d'avoir un **contrôle absolu** sur l'organisation Bitwarden.

Pour la méthode, voire documentation ci-dessous

- Types d'Utilisateurs et Contrôle d'Accès | Bitwarden

Tous les membres du service informatique possèdent désormais les **pleins pouvoirs** sur l'instance Bitwarden.

B. Importation des mots de passe

Pour des raisons de sécurité, les navigateurs bloquent **l'importation automatique** : nous utiliserons donc la méthode manuelle décrite dans le guide d'importation

Ce **Guide Utilisateur** (joint en annexe) détaille la procédure pas à pas avec des captures d'écran

C. Désactivation du GMP Edge

Création d'une GPO pour la désactivation des mots de passes qu'on activeras seulement sur les personnes ayant déjà fait l'importation

- Créer une GPO qui cible l'ensemble des collaborateurs,
- Dans la configuration il faut désactiver le paramètre « **Activer l'enregistrement des mots de passe dans le gestionnaire de mots de passe** » voir le lien suivant : GPO Microsoft Edge : désactiver le gestionnaire de mots de passe
- Déployer la GPO en fonction du périmètre

D. Mise en situation

1. Mise en situation

- Côté Service informatique

- Côté Utilisateurs

1. Se rendre sur l'ENTRA ID/Application d'entreprise/Bitwarden/Utilisateurs et Groupe et ajouter les utilisateurs concernés
2. Etendre le périmètre des GPO (extension et lien Bitwarden login en favoris) à ces utilisateurs
3. Les informer du nouveau gestionnaire de mots de passe et leur fournis les vidéos pour la mise en place
4. Ils suivent la vidéo de connexion et envoie une demande d'acceptation dans Bitwarden
5. Je me rends dans Bitwarden/Console Admin/Membres et j'approuve leurs comptes (étape obligatoire lors de la première connexion.)
6. Ils ont donc accès au coffre-fort pour l'instant vide
7. Ils suivent la vidéo d'importation des mots de passe
8. Ils réalisent l'importation de leurs mots de passe à l'aide du guide d'importation fournis
9. Ils ont donc accès au GMP avec leurs mots de passe et l'ancien désactiver

Attribution de privilèges :

- Service informatique : Propriétaire
- Collaborateurs : Utilisateur

Guide utilisateur :

- Vidéo qui montre la connexion à Bitwarden
- Vidéo d'importation des mots de passe
- Vidéo avec la présentation de ses fonctionnalités

Guide Administrateur :

- Documentation technique

Mettre en place la GPO pour mettre le lien BitWarden en favoris https://vault.bitwarden.eu/#/login la déployer selon le périmètre

Suivi du document

Date	Version	Résumé	Auteur
28/01/2026	0.1	Création du document	Yanis DAHMAN

Validation du document

Validée le	Nom et prénom	Fonction	Signature