Lors d'un audit de routine sur l'environnement de travail, j'ai découvert un fichier partagé contenant une liste de comptes utilisateurs accompagnés de leurs mots de passe... en clair.

Cette pratique, extrêmement risquée, exposait directement l'ensemble du système à des intrusions potentielles, que ce soit par négligence interne ou par une attaque ciblée. Face à cette situation critique, j'ai dû agir rapidement pour sécuriser les accès.

J'ai commencé par analyser les usages pour comprendre pourquoi ce fichier existait et comment il était utilisé. Puis, j'ai mis en place une solution centralisée et sécurisée via un gestionnaire de mots de passe, permettant aux utilisateurs de stocker et de partager leurs identifiants de manière chiffrée, avec un contrôle d'accès rigoureux.

Une fois la nouvelle méthode en place, j'ai également organisé une série de formations de sensibilisation destinées à tous les utilisateurs concernés, afin de leur expliquer les dangers du stockage de mots de passe en clair, les bonnes pratiques en matière de cybersécurité, et les réflexes à adopter pour protéger leurs accès. Cette démarche a permis non seulement de corriger une faille critique, mais aussi de faire évoluer les comportements pour renforcer durablement la sécurité de l'organisation.

Benchmarking des gestionnaires de mot de passes :

Fonctionnalité	1Password	LastPass	Bitwarden	Dashlane	Keeper
Chiffrement de bout en bout	✅ AES-256	✅ AES-256	✅ AES-256	✅ AES-256	✅ AES-256
Hébergement On-Premise	❌ (Cloud only)	❌	✅	❌	✅
Authentification à 2 facteurs (2FA)	✅	✅	✅	✅	✅
Intégration SSO (SAML, etc.)	✅	✅	✅	✅	✅
Partage sécurisé de coffres	✅	✅	✅	✅	✅
Interface intuitive et ergonomique	✅ Très fluide	Moyen	Assez simple	✅ Moderne	Moyen
Stockage d'éléments variés	✅ (notes, docs, etc)	✅	✅	✅	✅
Audit de sécurité (coffres, mots de passe faibles)	✅	✅	✅	✅	✅
Open source	❌	❌	✅	❌	❌
Prix entreprise (env. 10-50 users)	💰💰	💰↓	💰 (moins cher)	💰💰	💰💰

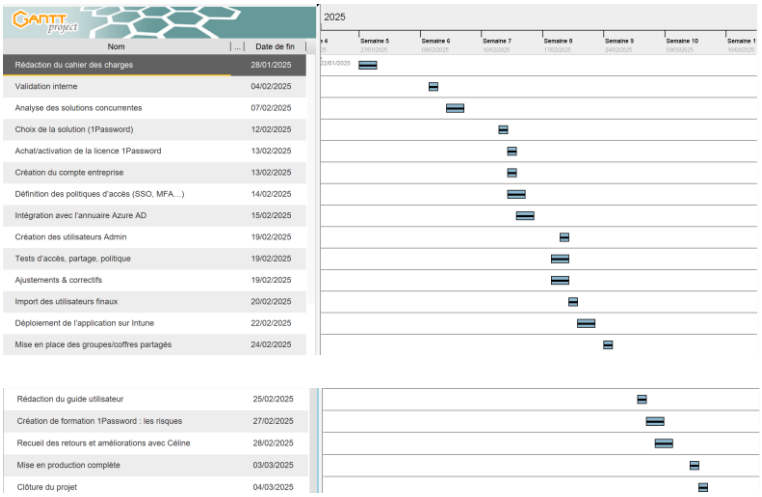
Nous avons choisi 1Password car Il 'intègre facilement avec les principaux fournisseurs cloud comme Azure. Et divers outils SaaS que nous utilisons au quotidien. Cela simplifie la gestion centralisée des accès. Il utilise aussi une architecture Zéro Trust, chiffrement au bout à bout, et des clés privées exclusivement détenues côté client, réduisant considérablement les risques liés à une architecture cloud-only dans notre cas.

L’interface de 1Password est intuitive et facilite l’adoption rapide par les équipes. Grace à ses capacités d’automatisation, de partage sécurisées et simplifié, cela simplifie grandement l’efficacité opérationnelle.

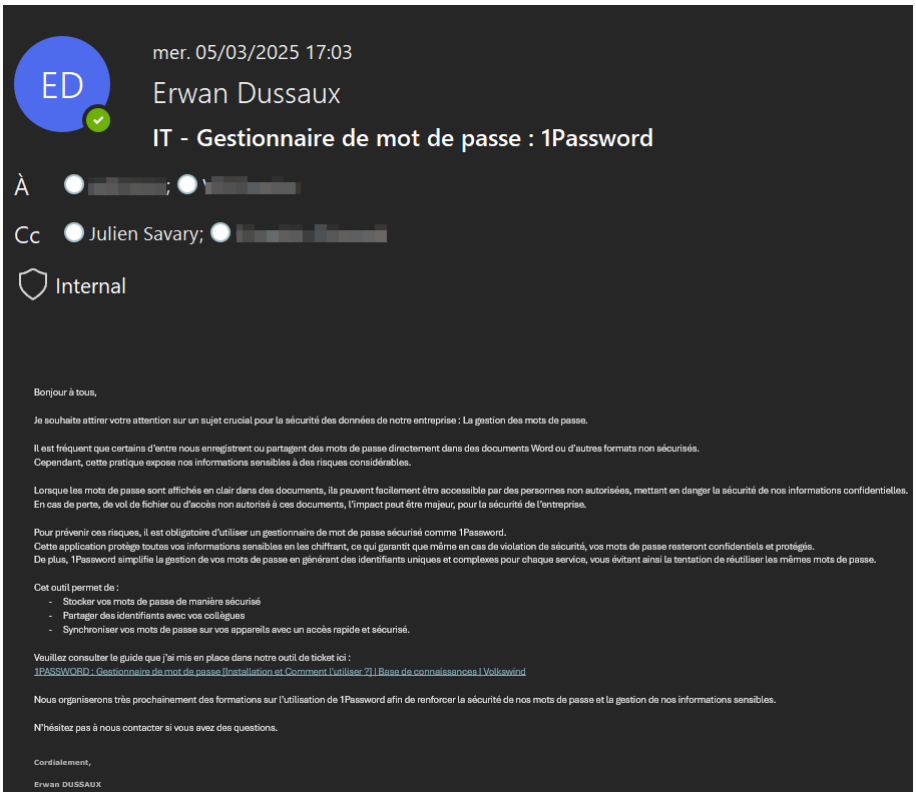
De plus 1Password fournit des fonctionnalités d’audit et des contrôles d’accès adaptés aux exigences réglementaires strictes (ISO 27001, RGPD…) garantissant une conformité simplifiée à long terme.

Quelques exemples :

- **Identification des mots de passe faible**
- **Journal d’activité : Consultation des mots de passes supprimés/modifiées/partagés à n’importe quel moment elle a eu lieu**
- **SSO pour renforcer la détection des anomalies ou d’incidents de sécurités via le SIEM**



Par la suite, j’ai rédigé un mail en informant l’ensemble des utilisateurs qu’il sera désormais obligatoire d’utiliser 1Password pour la gestion et la sécurisation de leurs mots de passe professionnels. Ce message précise que cette décision a été prise dans le but de renforcer la sécurité des données de l’entreprise et de limiter les risques de compromission liés à l’utilisation de mots de passe non sécurisés, faibles ou réutilisés. Le mail explique également que des sessions de formation seront mises en place dans les prochaines semaines, afin d’accompagner les utilisateurs dans la prise en main de 1Password, de leur présenter les fonctionnalités essentielles de l’outil, et de les sensibiliser aux bonnes pratiques de cybersécurité. Cette communication vise à assurer une adoption fluide du gestionnaire de mots de passe et à garantir une compréhension partagée des enjeux liés à la protection des identifiants professionnels.



mer. 05/03/2025 17:03

Erwan Dussaux

IT - Gestionnaire de mot de passe : 1Password

À [redacted]

Cc Julien Savary; [redacted]

Internal

Bonjour à tous,

Je souhaite attirer votre attention sur un sujet crucial pour la sécurité des données de notre entreprise : La gestion des mots de passe.

Il est fréquent que certains d'entre nous enregistrent ou partagent des mots de passe directement dans des documents Word ou d'autres formats non sécurisés.
Cependant, cette pratique expose nos informations sensibles à des risques considérables.

Lorsque les mots de passe sont affichés en clair dans des documents, ils peuvent facilement être accessible par des personnes non autorisées, mettant en danger la sécurité de nos informations confidentielles.
En cas de perte, de vol de fichier ou d'accès non autorisé à ces documents, l'impact peut être majeur, pour la sécurité de l'entreprise.

Pour prévenir ces risques, il est obligatoire d'utiliser un gestionnaire de mot de passe sécurisé comme 1Password.
Cette application protège toutes vos informations sensibles en les chiffrant, ce qui garantit que même en cas de violation de sécurité, vos mots de passe resteront confidentiels et protégés.
De plus, 1Password simplifie la gestion de vos mots de passe en générant des identifiants uniques et complexes pour chaque service, vous évitant ainsi la tentation de réutiliser les mêmes mots de passe.

Cet outil permet de :

- Stocker vos mots de passe de manière sécurisé
- Partager des identifiants avec vos collègues
- Synchroniser vos mots de passe sur vos appareils avec un accès rapide et sécurisé.

Veuillez consulter le guide que j'ai mis en place dans notre outil de ticket ici :
1PASSWORD : Gestionnaire de mot de passe [Installation et Comment l'utiliser ?] | Base de connaissances | Volkswind

Nous organiserons très prochainement des formations sur l'utilisation de 1Password afin de renforcer la sécurité de nos mots de passe et la gestion de nos informations sensibles.

N'hésitez pas à nous contacter si vous avez des questions.

Cordialement,

Erwan DUSSAUX

Afin de procéder au déploiement de 1Password sur l'ensemble des ordinateurs du domaine, j'ai mis en place une stratégie automatisée en utilisant Microsoft Intune couplé à un script PowerShell. Ce script a été conçu pour télécharger directement la dernière version de l'exécutable d'installation depuis le site officiel de 1Password, garantissant ainsi que chaque poste reçoit une version à jour, sécurisée et vérifiée du logiciel. Une fois l'exécutable récupéré, le script exécute l'installation en mode silencieux, sans intervention de l'utilisateur, assurant un déploiement fluide et homogène sur toutes les machines concernées. Cette méthode permet non seulement un gain de temps significatif dans la gestion du parc informatique, mais elle garantit également une cohérence dans la configuration de l'outil de gestion des mots de passe au sein de l'organisation. Grâce à cette approche centralisée, tous les collaborateurs disposent désormais de 1Password installé localement, prêt à être utilisé dans le cadre des formations à venir et conformément aux nouvelles exigences en matière de sécurité informatique. Le script se nomme : install-1password.ps1

```
# Installer 1Password via Intune

# Ce script télécharge et installe la dernière version de 1Password sur Windows


$InstallerUrl = "https://downloads.1password.com/win/1PasswordSetup.exe"

$InstallerPath = "$env:TEMP\1PasswordSetup.exe"


Write-Output "Téléchargement de l'installateur depuis $InstallerUrl..."
```

Invoke-WebRequest -Uri $InstallerUrl -OutFile $InstallerPath

Write-Output "Installation de 1Password en cours..."

Start-Process -FilePath $InstallerPath -ArgumentList "/S" -Wait

Write-Output "Suppression de l'installateur..."

Remove-Item -Path $InstallerPath -Force

Write-Output "1Password a été installé avec succès."

Dans le but de permettre aux utilisateurs d'installer manuellement l'application 1Password, j'ai pris l'initiative de rendre le logiciel accessible via le Portail d'entreprise (Company Portal), en le conditionnant au préalable dans un format compatible avec Microsoft Intune. Pour cela, j'ai téléchargé l'exécutable officiel de 1Password, puis je l'ai converti au format .intunewin à l'aide de l'outil Microsoft Win32 Content Prep Tool, indispensable pour packager des applications Win32 destinées à Intune. Ce package a ensuite été importé dans la console Intune, avec tous les paramètres nécessaires pour garantir une installation silencieuse et sans erreur. En configurant l'application comme disponible pour les appareils inscrits, j'ai permis aux utilisateurs finaux de l'installer à leur convenance directement depuis le Portail d'entreprise, sans devoir passer par une procédure technique complexe ou solliciter le support informatique. Cette approche facilite grandement le déploiement autonome du logiciel tout en gardant un contrôle centralisé, et s'intègre pleinement dans notre stratégie de sécurisation des accès à travers l'adoption généralisée de 1Password dans l'environnement professionnel.

Voici la commande pour créer un fichier en Intunewin via Powershell en mode adminsitrateur :

.\IntuneWinAppUtil -c C:\temp\ -s C:\temp\ install-1password.ps1 -o C:\temp\

Dans l'interface d'administration Intune :

Il y a des informations qui seront cachés dans la capture d'écran ci-dessous car il y a des identifiants pour l'abonnement de 1password.

Voici le résultat :