FONCTIONNEMENT

Dans pratiquement tous les systèmes collaboratifs déployés ces dernières années, **la gestion des accès** utilisateurs **aux fichiers et informations a tendance à se dégrader** avec le temps.

La plupart des entreprises utilisant des technologies collaboratives telles qu'Office 365, **ont très peu de visibilité ou de contrôle** sur les accès de chaque utilisateur aux fichiers, dossiers, bibliothèques, sites et équipes. Cela entraîne des défis **importants en matière de sécurité et de conformité des données.**

OP365 PROPOSE UNE APPROCHE RADICALEMENT DIFFÉRENTE DES OUTILS CLASSIQUEMENT DEDIES AU PERSONNEL IT.

OP365 AvePoint® se concentre principalement sur des utilisateurs nommés, pas seulement sur les équipes informatiques. Il **détecte automatiquement les cas d'accès inapproprié, automatise le contrôle de l'accès à l'information et offre une visibilité parfaite aux « Business owners »** ainsi que des rapports sur les droits d'accès et accédants. Il permet aux propriétaires de données de l'entreprise de prendre le contrôle de la gestion des accès à leurs informations. OP365 offre une solution simple et efficace sans passer par la case IT.

LA SOLUTION

OP365 AvePoint® est une solution SaaS, hébergée par AvePoint® dans le cloud Microsoft Azure. Un tenant unique, isolé par cryptographie, est créé pour chaque client et connecté de façon sécurisée à son (ses) tenant Office 365, ainsi qu'à d'autres systèmes d'information qui seraient utilisés dans l'organisation (tels que les partages de fichiers locaux et SharePoint onprem).

Le client conserve le contrôle complet et exclusif de ses données stockées dans Office 365, ainsi que le contrôle du tenant OP365 via sa console d'administration.

OP365 AvePoint® utilise les API du tenant Office 365 pour créer un index des données, les autorisations d'accès et leurs utilisations. OP365 **AvePoint® analyse constamment** l'index **pour identifier les problèmes de sécurité, les anomalies d'accès, contrôler l'accès aux données et fournir une visibilité complète sur les accès (rapports). OP365 AvePoint®** ne peut accéder au contenu des fichiers ou des données des clients, ne voyant que des métadonnées (nom de fichier, créée par, modifiée par, dates etc.,) et les balises appliquées par une solution de classification comme Microsoft Information Protection (MIP).

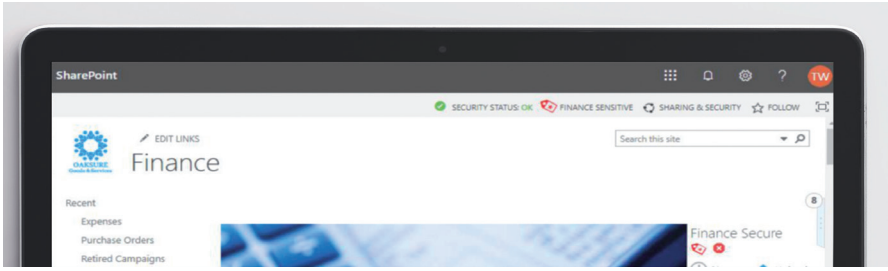
INTERFACE UTILISATEUR

Afin d'interagir avec les utilisateurs, **l'interface utilisateur de OP365 AvePoint® est ajoutée à celle des systèmes d'information existants**, tels que SharePoint Online et Teams.

Le bouton « partager » de l'interface native est remplacé par le bouton « Partage et sécurité » de **OP365**, qui appelle la console **OP365** à l'intérieur du système hôte.

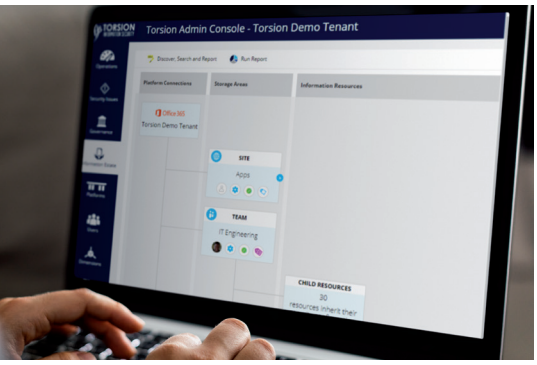
OP365 AvePoint® améliore l'expérience utilisateur native pour lui superposer les incidents de sécurité, les classifications et les notifications selon les cas. Ces éléments guident les actions des utilisateurs à l'égard des décisions à prendre en matière de sécurité et de conformité.

L'interface utilisateur de OP365 fonctionne également pour OneDrive et les bibliothèques synchronisées hors connexion à l'aide du client de synchronisation OneDrive. Cette expérience est accessible par les utilisateurs sous forme de clic droit dans l'Explorateur de fichiers Windows. Pour cette interface utilisateur, un petit module logiciel doit être déployé sur le pc de l'utilisateur, soit en tant qu'installateur EXE direct, soit en tant que MSI qui peut être déployé avec une stratégie de groupe. Si ce module n'est pas déployé, l'interface utilisateur de OP365 est toujours visible pour SharePoint et Teams.



CONSOLE D'ADMINISTRATION

OP365 fournit des fonctionnalités complètes aux administrateurs IT pour la création et la gestion de connexions à partir du tenant OP365 au tenant Office 365, ainsi qu'à d'autres systèmes d'information.



À l'aide de la console d'administration, les administrateurs IT peuvent effectuer une surveillance centralisée de tous les problèmes de sécurité, des opérations de gouvernance, des accès utilisateurs et de l'ensemble des données clients.

Bien que OP365 soit en grande partie automatisée et autonome, certaines tâches opérationnelles surgissent de temps à autre. Il s'agit de tâches qui exigent qu'un administrateur tienne compte d'une situation particulière et puisse la traiter directement dans la console d'administration.

HÉBERGÉ DANS LE CLOUD MICROSOFT AZURE

OP365 est hébergé par AvePoint® dans le cloud Microsoft Azure. Le système est géré et exploité par des ingénieurs de AvePoint, qui utilisent des systèmes et des processus sophistiqués de surveillance et d'atténuation.

Chaque client **OP365** a son propre tenant, unique. **Ce tenant dispose de sa propre base de données, de clés de chiffrement de données uniques**, ainsi que de son propre ensemble d'instances de traitement et d'exécution. Ce qui garantit l'isolation de chaque tenant de façon cryptographique et logique.

OP365 s'exécute sur un éventail de serveurs d'applications et de bases de données basés sur le cloud, qui incluent la redondance dynamique et la réactivité au traitement.

CONNECTION À OFFICE 365

La connexion entre le tenant OP365 du client et le tenant Office 365 est créée dans le cadre du processus de configuration de la console d'administration OP365. La connexion prend la forme d'une application Azure Active Directory, qui fournit un certificat d'authentification sécurisé à l'application **OP365. OP365 utilise la connexion sécurisée pour accéder aux API du tenant Office 365**.

Les API sont utilisées pour lire les fichiers, les dossiers, les bibliothèques, les sites d'équipes – strictement limités aux métadonnées, et uniquement sur les objets d'information. Les API sont également utilisées pour lire les informations des utilisateurs, des groupes et des autorisations d'accès, ainsi que pour manipuler ces autorisations.

Les données des API sont utilisées pour créer un index complet de chaque objet d'information, de chaque utilisateur, de chaque instance d'un utilisateur ayant accès à un objet d'information et de chaque instance d'une personne accédant réellement à un objet d'information. L'index est compilé en effectuant une analyse initiale complète du système, et maintenu en temps réel de façon incrémentale en ingérant les journaux.

OP365 n'a pas accès au contenu des données des clients. Lorsqu'il y a un fichier dans un dossier, il y a une ligne correspondante dans la base de données d'index OP365, mais les seules données de l'index sont les métadonnées, (nom de fichier, créés par, modifiés par, etc.) et les balises de classification (ex MIP).

ON-PREMISES CONNECTION

Dans son abonnement Premium, OP365 prend également en charge la connexion aux systèmes SharePoint et File Shares locaux, en plus des tenants Office 365. Dans ce cas, un agent proxy local doit être installé sur un serveur à l'intérieur du réseau client.

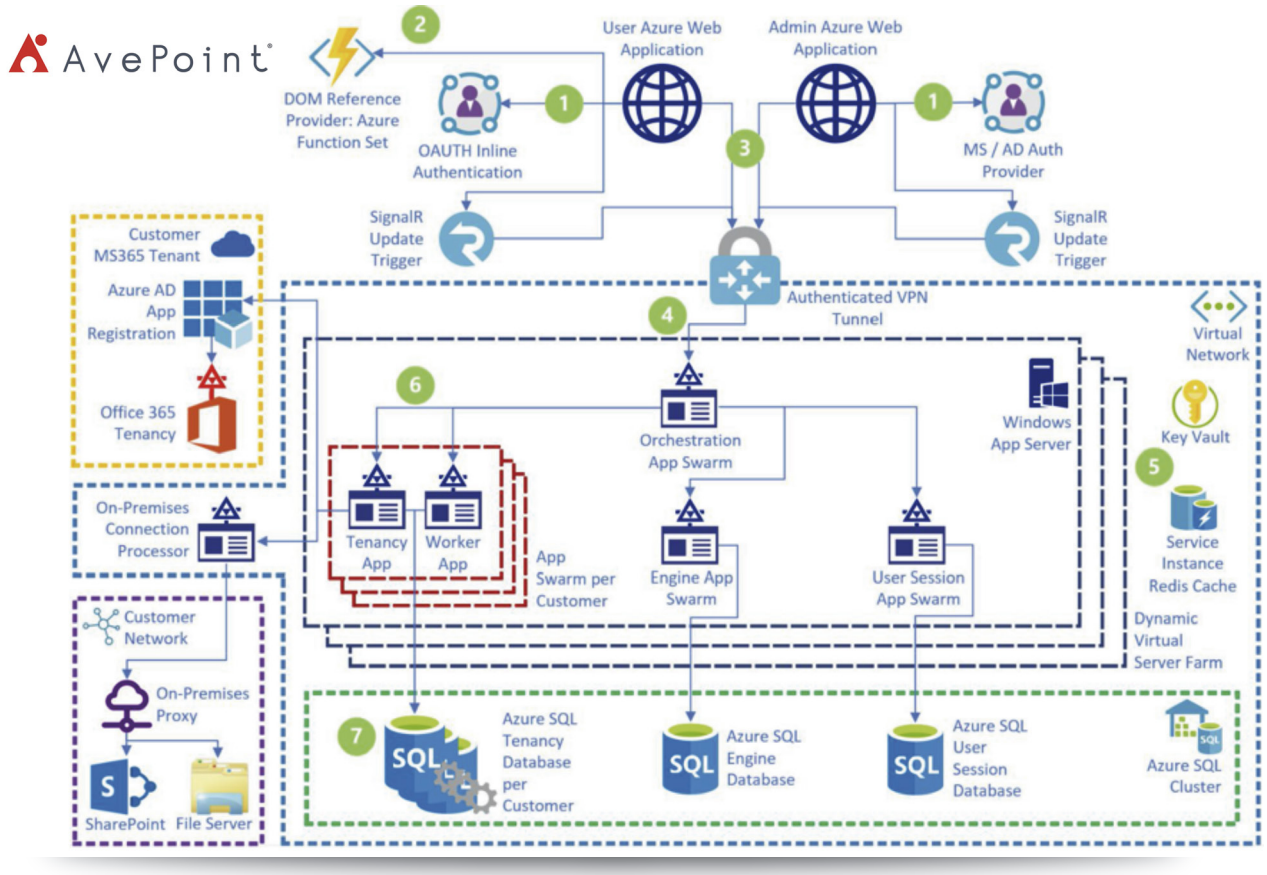
L'agent prend la forme d'une machine virtuelle préconfigurée sous Linux, encapsulée à l'intérieur d'une image Docker. L'agent n'effectue aucun traitement. Son seul rôle est celui d'un proxy pour les appels API entre le cloud **OP365** et les serveurs SharePoint ou File Shares locaux.

Dans ce cas, le nom d'utilisateur et le mot de passe d'un compte de service doivent être fournis lors de la configuration du tenant **OP365**. Il est recommandé de créer un compte de service unique ayant le minimum de privilèges nécessaires pour faire fonctionner OP365. Les autorisations et les étapes spécifiques requises sont clairement documentées lors du processus de configuration.

USER IDENTITY

- **La connexion** au tenant Office 365 utilise une application Azure Active Directory, qui **n'implique pas la création de comptes de service**.
- **Les utilisateurs** des applications Office 365 **sont authentifiés** silencieusement à l'aide de leurs **identités Office 365 existantes**.
- **Les administrateurs s'authentifient** sur la console d'administration à l'aide de leurs **comptes Office 365 existants**.
- **OP365 n'a pas accès aux mots de passe et ne gère aucun mot de passe**.

ARCHITECTURE DE RÉFÉRENCE



EXPÉRIENCE UTILISATEUR TYPE

L'utilisateur accède à son expérience utilisateur Office 365 existante (SharePoint Online, Teams, etc.) OP365 améliore l'expérience utilisateur Office 365 avec des informations et des fonctionnalités supplémentaires.

L'utilisateur peut cliquer sur les boutons pour appeler l'expérience utilisateur OP365, qui est intégrée à l'intérieur de l'expérience utilisateur Office 365.

DATA FLOW

1. Le code JavaScript du moteur AvePoint® est injecté dans la page, authentifiant de façon silencieuse l'utilisateur.
2. Le code JavaScript du moteur AvePoint® invoque les fonctions d'augmentation Azure permettant d'afficher l'interface OP365.
3. Les fonctions d'augmentation sont transmises à l'application Web en passant par un tunnel VPN sécurisé.
4. Les requêtes sont dispatchées au Tenant applicatif correspondant.
5. Les demandes des clés d'authentification sont récupérées du «Key Vault». Le contexte est référencé dans une instance «Redis Cache».
6. Les requêtes sont transmises au tenant application pour être traitées.
7. Les informations sont stockées en base SQL.