Description technique de la solution

Les problèmes résolus par OP365 et comment il procède

Dans pratiquement tous les systèmes de gestion et de collaboration de l'information jamais déployés dans la mémoire récente, « qui a accès à quoi » **les fichiers et les informations ont tendance à se dégrader** hors de contrôle au fil du temps. **La plupart des entreprises** utilisant des technologies de collaboration telles qu'Office 365, **ont très peu de visibilité ou de contrôle** de qui a accès à quels fichiers, dossiers, bibliothèques, sites et équipes. Cela entraîne des défis **importants en matière de sécurité et de conformité des données.**

OP 365 UNE APPROCHE RADICALEMENT DIFFÉRENTE DES AUTRES OUTILS CENTRÉS SUR L'ADMINISTRATION INFORMATIQUE QUI VISENT ÉGALEMENT LE MÊME PROBLÈME.

OP365 se concentre principalement sur les utilisateurs professionnels, pas seulement 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** et des rapports sur les personnes qui ont accès à quoi. Il permet aux propriétaires de données de l'entreprise de prendre le contrôle de l'accès à leurs propres informations, et rend extraordinairement rapide et simple pour eux de le faire. OP365 offre une solution véritablement efficace à ce problème difficile, qui n'a pas été résolu par l'industrie depuis de nombreuses années.

Solution Overview

OP365 est une solution logicielle en tant que service, hébergée par Torsion Information Security dans le cloud Microsoft Azure. Un locataire unique, isolé par cryptographie, est créé pour chaque client et connecté en toute sécurité au locataire Office 365 du client et à d'autres systèmes d'information également utilisés dans l'organisation (tels que les partages de fichiers locaux et SharePoint).

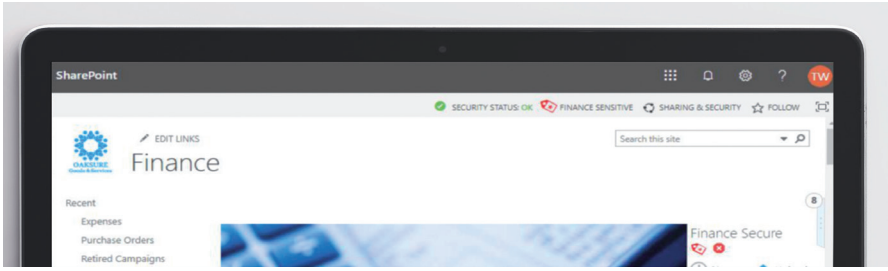
Le client conserve le contrôle complet et exclusif de ses données stockées dans Office 365, ainsi que le contrôle du locataire OP365 via la console d'administration OP365.

OP365 utilise les API du locataire Office 365 pour créer un index des données du client, les autorisations d'accès et l'utilisation, et **analyse constamment** l'index **pour découvrir les problèmes de sécurité, les anomalies d'accès, contrôler intelligemment l'accès aux données et fournir une visibilité d'accès complète et des rapports**. OP365 ne peut pas voir à l'intérieur des fichiers ou des données des clients, ne voyant que des métadonnées telles que le nom de fichier, créée par, modifiée par, etc., et aussi toutes les balises qui peuvent avoir été appliquées aux fichiers par n'importe quelle solution de prévention ou d'étiquetage de classification des pertes de données telles que Microsoft Information Protection (MIP).

Interface utilisateur

Afin d'interagir avec les utilisateurs professionnels, **l'interface utilisateur de OP365 est injectée dans l'expérience utilisateur des systèmes d'information existants**, tels que SharePoint Online et Teams.

Les boutons « partager » de l'expérience utilisateur native sont remplacés par le bouton « Partage et sécurité » de OP365, qui invoque l'interface utilisateur principale de OP365 à l'intérieur du système hôte.

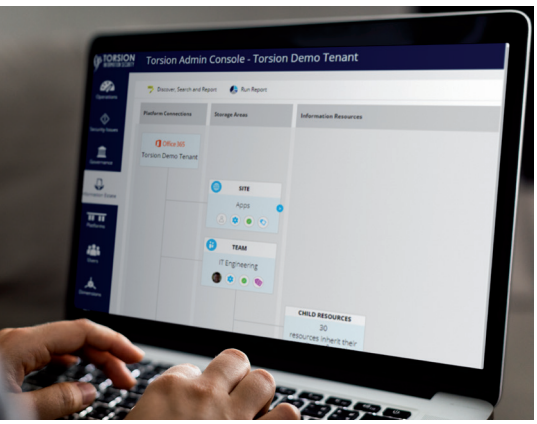


La subtilité de la OP365 augmente l'expérience utilisateur native pour superposer les problèmes de sécurité, les classifications et les notifications selon le cas. Ces éléments guident le comportement des utilisateurs à l'égard de l'utilisation de l'information commerciale d'une manière qui est consciente du contexte et des implications en matière de sécurité et de conformité, sans obstruer ou ralentir l'utilisateur.

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.

Administration Console

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



À l'aide de la console d'administration, les administrateurs informatiques (et éventuellement les équipes de service gérés par des partenaires) peuvent obtenir une surveillance centralisée de tous les problèmes de sécurité, des opérations de gouvernance et de l'application de la loi, de l'accès des utilisateurs et de l'ensemble des données clients.

Bien que OP365 soit en grande partie automatisée et autonome, les tâches opérationnelles des administrateurs surgissent de temps à autre. Il s'agit de tâches qui exigent qu'un administrateur tienne compte d'une situation et effectue une réponse. Ces tâches opérationnelles sont effectuées dans la console d'administration.

Hosted in the Microsoft Azure Cloud

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

Chaque client OP365 a son propre locataire unique. **Chaque locataire dispose de sa propre base de données et de clés de chiffrement de données uniques**, ainsi que de son propre ensemble d'instances de traitement en cours d'exécution – ce qui garantit avec force que chaque locataire est isolé de façon cryptographique et logique de tous les autres.

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 de la charge et de l'utilisation du client.

Office 365 Connection

La connexion entre le locataire OP365 du client et le locataire 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 locataire Office 365.**

Les API sont utilisées pour lire des listes de fichiers, de dossiers, de bibliothèques, de sites et d'équipes – où ces données incluent strictement les métadonnées sur les objets d'information uniquement. Les API sont également utilisées pour lire des listes d'utilisateurs, de groupes et d'autorisations d'accès, et pour manipuler ces autorisations afin de les automatiser.

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 en ingérant les journaux d'activité et l'analyse répétée.

OP365 n'a en aucun cas 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, y compris le nom de fichier, créés par, modifiés par, etc. et aussi toutes les balises qui peuvent avoir été appliquées aux fichiers par n'importe quelle solution de prévention ou d'étiquetage de classification des pertes de données telles que Microsoft Information Protection (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 locataires Office 365. Dans ce cas, un agent proxy local doit être installé sur un serveur à l'intérieur du réseau client.

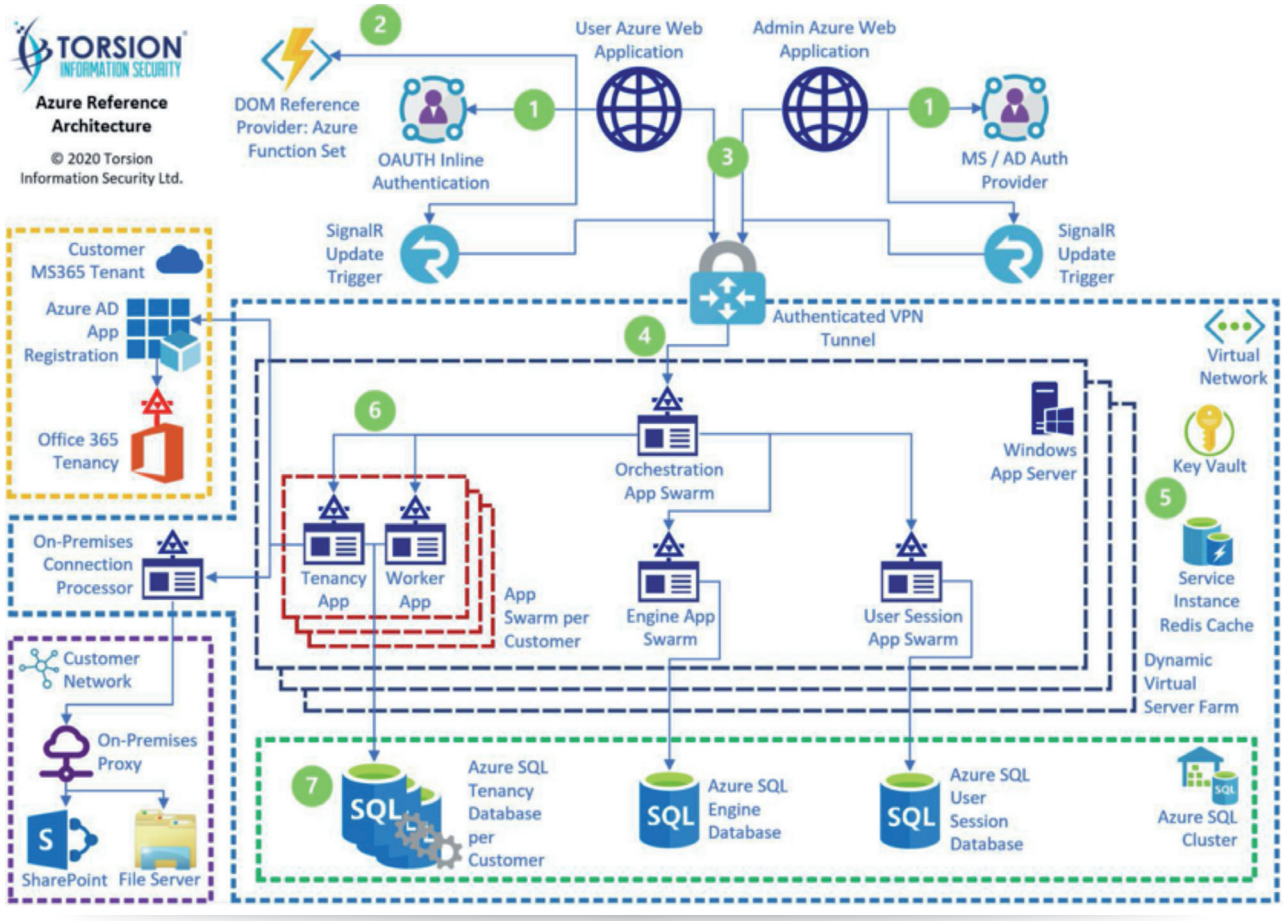
L'agent prend la forme d'une machine virtuelle préconfigurée exécutant Linux, encapsulée à l'intérieur d'une image Docker. L'agent n'effectue aucun traitement du tout. Son seul but est de proxyr les appels API entre le cloud OP365 et les serveurs SharePoint et File Shares locaux.

Dans ce cas, le nom d'utilisateur et le mot de passe d'un compte de service doivent être fournis à la configuration du locataire De OP365. Il est recommandé de créer un compte de service unique uniquement à cette fin, et ne compte tenu que de l'ensemble minimum de privilèges nécessaires pour que OP365 fonctionne. Les autorisations et les étapes spécifiques requises sont clairement documentées pour prendre en charge le processus de configuration.

User Identity

- **La connexion** au locataire Office 365 utilise une application Azure Active Directory, qui **n'implique pas la création de comptes de service**.
- **Les utilisateurs professionnels** des applications Office 365 **sont authentifiés** silencieusement à l'aide de leurs **identités Office 365 existantes**.
- **Les administrateurs informatiques s'authentifient** sur la console d'administration à l'aide de leurs **comptes Office 365 existants** de Microsoft.
- **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 augmente l'expérience utilisateur Office 365 avec des informations et des fonctionnalités en ligne 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. OP365 JavaScript injecté dans la page, authentifie silencieusement l'utilisateur
2. OP365 JavasScript appelle Azure Function Set pour les commandes d'augmentation de page
3. Les commandes d'augmentation de page sont transmises à l'application Web, qui la passe à travers le VPN pour le tunnel à la batterie de serveurs d'applications.
4. La demande est portée à la demande d'orchestration, à envoyer à la demande de location pertinente.
5. Les clés d'authentification de demande sont récupérées à partir du coffre-fort de la clé. Le contexte est référencé dans instance Redis Cache.
6. La demande est transmise à la demande de location pour traitement.
7. Le traitement des demandes fait référence à la base de données Location SQL