HORNETSECURITY | ited

MICROSOFT 365

LE GUIDE ESSENTIEL

Avant-propos de Jonathan Johnson de ited

Chers lecteurs et passionnés de technologie,

Nous sommes ravis de vous présenter ce guide numérique, une œuvre collaborative née de l'union entre Les solutions ited inc. et notre estimé partenaire, Hornetsecurity. Cette collaboration est le résultat d'une vision partagée : celle de fournir des solutions de cybersécurité innovantes et exhaustives. L'apport de Hornetsecurity, spécialiste en solutions antispam avancées et en gestion de permissions SharePoint, a enrichi notre offre chez Les solutions ited inc., consolidant ainsi notre statut de prestataire de services de sécurité gérés (Managed Security Service Provider, MSSP) de référence.

Ce guide numérique est une ressource précieuse pour naviguer dans l'univers d'O365 et M365. Depuis les fondamentaux jusqu'aux aspects techniques plus complexes, il vous délivre les clés pour une gestion optimale de la suite 365. Plus encore, nous avons concentré nos efforts pour vous fournir des stratégies vitales en termes de sécurité, de sauvegarde et de conformité, indispensables pour la protection de votre entreprise.

Au cœur de notre mission chez Les solutions ited inc., se trouve la conviction que la sécurité informatique est primordiale. Dans un monde où la connectivité est omniprésente, assurer la sécurité des données et des infrastructures est notre priorité. Nous vous encourageons à visiter notre site https://it-ed.com pour explorer l'étendue de nos services et comprendre comment nous pouvons vous aider à sécuriser votre espace numérique.

Notre partenariat avec Hornetsecurity va au-delà d'une simple collaboration ; c'est un engagement commun pour l'excellence en matière de sécurité informatique. En partageant nos connaissances à travers ce guide, nous aspirons à renforcer vos compétences et la résilience de votre entreprise face aux enjeux numériques actuels et futurs.

Nous vous souhaitons une lecture instructive et enrichissante.

Cordialement,

Jonathan Johnson
Responsable Sécurité, Les solutions ited inc.

INTRODUCTION

BIENVENUE À CE LIVRE ÉLECTRONIQUE GRATUIT DE HORNETSECURITY SUR MICROSOFT 365. DANS CE LIVRE, NOUS VOUS MONTRERONS COMMENT UTILISER CES SERVICES INFONUAGIQUES POUR AMÉLIORER VOS OPÉRATIONS ET TIRER LE MEILLEUR PARTI DE MICROSOFT 365. CETTE ÉDITION EST LA TROISIÈME VERSION DE CE LIVRE ÉLECTRONIQUE ET EST À JOUR EN DATE DE JUILLET 2023.

MICROSOFT 365
LE GUIDE
ESSENTIEL

QUI DEVRAIT LE LIRE?

Ce livre s'adresse aux administrateurs et au personnel des technologies de l'information (TI) qui gèrent un environnement Microsoft 365. Il traite des pratiques exemplaires et des configurations optimales des applications et des fonctions les plus importantes, mais donne aussi un aperçu de la suite, particulièrement utile pour ceux qui se préparent à migrer vers Microsoft 365 ou qui ont déjà migré, et ont besoin de se familiariser avec cette solution. En revanche, si vous êtes un développeur qui cherche à créer des applications et des services sur la plateforme Microsoft 365, ce livre ne vous est pas destiné. Si vous êtes un décideur opérationnel, plutôt qu'un responsable de la mise en œuvre technique, ce livre vous donnera une bonne idée de ce à quoi vous pouvez vous attendre lorsque votre organisation aura migré vers le nuage informatique et vous explique comment adopter divers services dans Microsoft 365 pour améliorer l'efficacité de votre entreprise. Si vous êtes un partenaire Microsoft gérant les déploiements d'autres entreprises et que vous utilisez Microsoft 365 Lighthouse comme solution pour gérer plusieurs locataires dans une seule console, le contenu de ce livre électronique vous convient tout à fait.

STRUCTURE DU PRÉSENT LIVRE ÉLECTRONIQUE

Ce livre comprend trois parties. La partie 1 (chapitres 1 à 6) est une introduction à Microsoft 365. Si vous connaissez déjà les notions de base, vous pouvez passer à la partie 2 (chapitre 7-13) pour en savoir plus sur l'administration et la gestion quotidiennes, les pratiques exemplaires et l'entretien. La dernière partie (chapitre 14-16) se concentre sur trois sujets essentiels de M365 que tous les environnements Microsoft 365 doivent aborder, à savoir la sécurité, la sauvegarde et la conformité.

Nous aborderons les différences de façon plus détaillée plus loin, mais il est bon de préciser qu'O**ffice 365** (désormais appelé O365) est à la fois un service de collaboration par courriel et un ensemble d'autres services fournis sous forme de logiciel-service (Software as a Service ou SaaS en anglais), tandis que **Microsoft 365** (M365) est composé d'Office 365 plus Azure Active Directory Premium, Endpoint Manager (Intune) – solution de gestion infonuagique des appareils et de la sécurité, plus Windows 11 Enterprise. Les deux sont des services d'abonnement utilisateurs qui ne nécessitent pas (ou très peu) de déploiement d'infrastructure dans le site. En ce qui concerne les plans pour petites entreprises (jusqu'à 300 utilisateurs), seule l'application Microsoft 365 est disponible. Bien que les deux soient disponibles dans les plans Enterprise (Entreprise), il est rare d'avoir seulement des plans Office 365 avec les énormes avantages des services ajoutés dans Microsoft 365. Par conséquent, nous ferons principalement référence à Microsoft 365 à partir de maintenant.

Cette édition est la troisième version de ce livre électronique et est à jour en date de juillet 2023.

TABLE DES MATIÈRES

PARTIE 1

NOTIONS DE BASE SUR OFFICE ET MICROSOFT 365

MICROSOFT 365
LE GUIDE
ESSENTIEL

Cette section présente M365, la gestion de base, la migration vers M365, les options de soutien, les applications client que vous pourriez prendre en charge et gérer et Windows 10/11. Si vous avez déjà des connaissances de M365 et que vous cherchez des renseignements plus détaillés sur l'administration de M365, passez directement à la **partie 2**.

DÉBARRASSEZ-VOUS DE VOTRE BAGAGE!

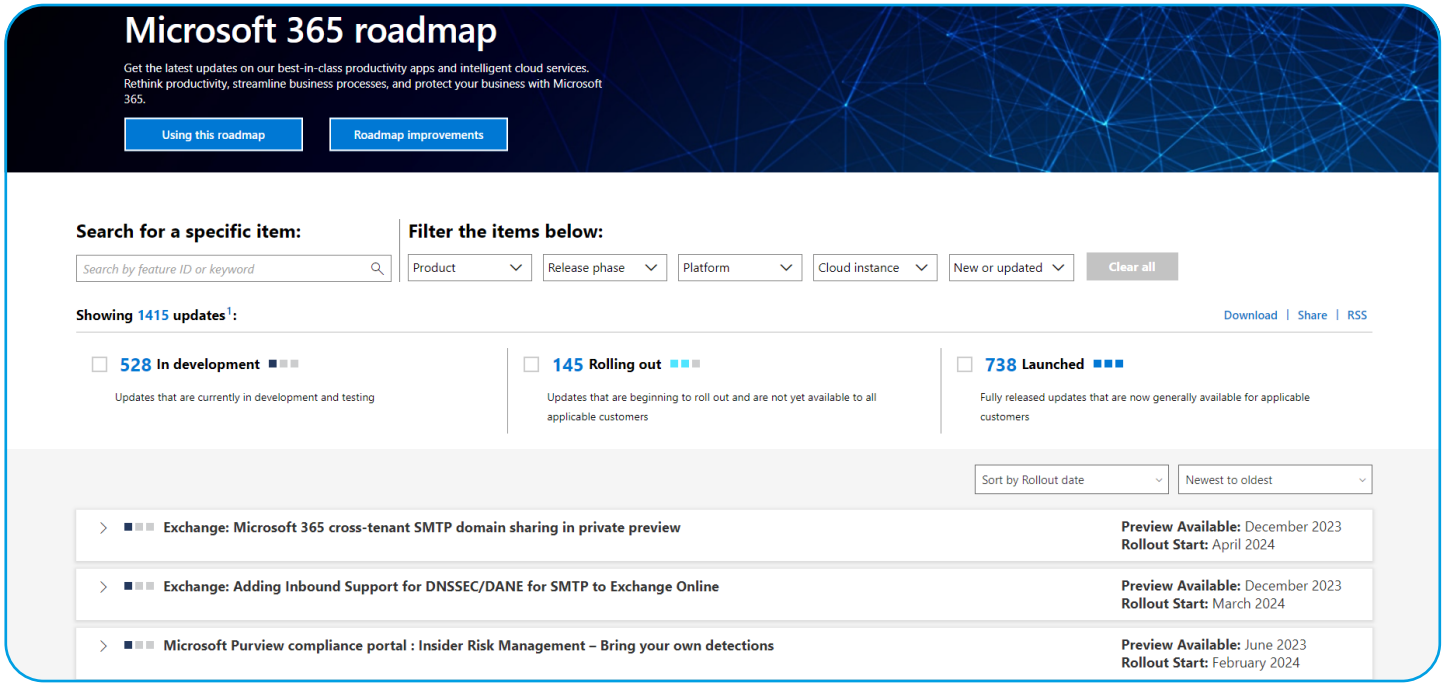
L'une des choses les plus importantes que vous devez faire si vous avez de l'expérience avec Exchange Server ou SharePoint Server sur site est de laisser tomber l'idée selon laquelle M365 n'est qu'une version SharePoint ou Exchange hébergée. Il y a quelques années, c'était vrai et O365 était simplement Microsoft hébergeant des serveurs Exchange, SharePoint et Lync dans leurs centres de données, mais ce n'est plus le cas. M365 est désormais une plateforme homogène dont Exchange Online et SharePoint Online constituent les éléments de base, mais qui comporte de nombreux autres services que vous ne verrez pas (ou comprendrez mal) si vous pensez encore aux serveurs de messagerie hébergés. Un exemple en est Microsoft Teams, un service de collaboration qui utilise Exchange Online pour stocker les données conservées et les clavardages, SharePoint pour stocker les documents, Planner pour la gestion de projets légers et Azure AD pour les identités. Tous ces aspects complexes sont gérés par Microsoft, et vous administrez simplement Teams comme un service distinct. Cela signifie également qu'il n'y aura jamais de « serveur Teams » sur site. Les composantes de base requises sont tout simplement trop complexes pour que la plupart des entreprises puissent les déployer.

L'autre chose qu'il faut abandonner si vous avez de l'expérience de la configuration sur site, c'est la planification de mises à niveau de logiciels tous les deux ou trois ans. La mise à niveau du serveur Exchange, par exemple, peut être un projet de grande envergure (selon la taille de votre environnement), qui prend des mois à planifier et à exécuter. M365 évolue dans un univers différent, avec des mises à jour plus petites chaque jour ou chaque semaine, et votre travail consistera désormais à évaluer ces modifications, leur incidence sur les utilisateurs et la gestion du changement dans l'organisation

COMMENT SUIVRE LE RYTHME

Je travaille avec Exchange Server depuis la version 5.5 (1997) et j'ai appris à suivre le rythme d'une nouvelle version tous les deux ou trois ans. J'ai acheté des livres pour apprendre toutes les nouvelles fonctions et tous les changements en prévision de la prochaine version. Cette méthode de développement de logiciels est terminée.

Presque tous les projets de logiciels (et certainement ceux de M365) visent maintenant des changements graduels fréquents. Cette approche présente plusieurs avantages : premièrement, chaque mise à jour est mineure et aucun plan de projet important n'est requis pour la « mise à niveau »; deuxièmement, les développeurs peuvent modifier le cours et ajouter continuellement de nouvelles fonctions par rapport à la rétroaction des utilisateurs beaucoup plus rapidement.



Feuille de route de Microsoft 365

Toutefois, en tant qu'administrateur de M365, cela représente un défi de taille. Au lieu d'être en mesure de planifier et d'en apprendre davantage sur un vaste ensemble de nouvelles fonctions à venir dans la prochaine grande version, de nouvelles fonctions sont publiées quotidiennement, et vous devez les comprendre et aider votre organisation à en tirer parti. Il y a plusieurs façons de gérer cela – selon votre mode d'apprentissage. Certaines personnes apprennent en lisant, d'autres en écoutant, d'autres en regardant des vidéos et certaines personnes n'apprennent qu'en accomplissant elles-mêmes des tâches (et la plupart d'entre nous apprennent mieux en combinant ces différentes méthodes).

Voici quelques ressources à ajouter à votre ceinture d'outils pour suivre les changements dans M365 :

La feuille de route officielle de **Microsoft 365** (microsoft.com) vous permet de filtrer de nombreux composants différents de M365.

Restez au fait des mises à jour d'Office 365 (techcommunity.microsoft.com) est un excellent article de blogue contenant des liens vers diverses ressources pour gérer les nombreuses mises à jour, pour différents types de publics cibles.

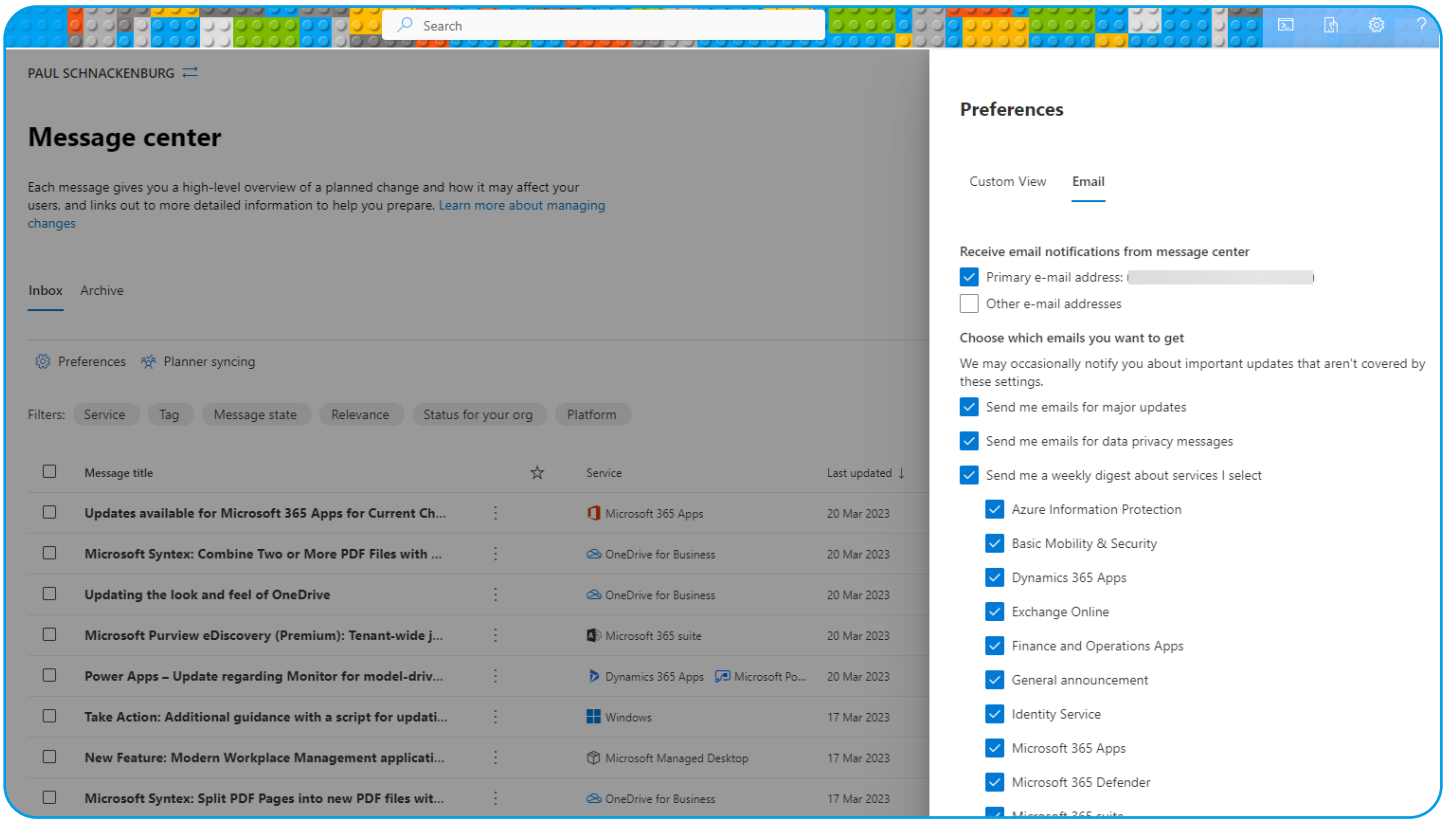
La section Nouveautés **dans Microsoft Intune** décrit en détail les mises à jour hebdomadaires dans Microsoft Intune.

Les nouveautés **dans Azure Active Directory** couvrent les mises à jour mensuelles de Entra ID (auparavant Azure AD) (voir le chapitre 7).

Azure AD Connect : l'historique des versions couvre les mises à jour d'AAD Connect (voir chapitre 7).

Microsoft Mechanics est une chaîne YouTube qui présente des entrevues et des démonstrations sur les fonctions à venir, ainsi que des listes de lecture d'Office et d'Azure.

Enfin, le **Message center (Centre de messages)** du portail (chapitre 2) présente les nombreux changements et de nouvelles fonctions – cliquez sur le lien « Preferences » (Préférences) pour personnaliser les services pour lesquels vous voulez obtenir des mises à jour et recevoir le courriel du bulletin hebdomadaire – une pratique exemplaire consiste à cibler une liste de distribution par courriel afin que le personnel qui n'a pas accès au Message Center puisse recevoir des mises à jour hebdomadaires par courriel.



Contrôle des notifications du Message Center

SOYEZ VOTRE PROPRE COBAYE

En tant qu'administrateur, il est important que vous testiez vous-même les nouvelles fonctions au fur et à mesure qu'elles sont produites ou, idéalement, lorsqu'elles sont à l'étape de prévisualisation. Il existe deux pistes pour les mises à jour publiées dans O365, **Standard et Targeted (Ciblé)**. La première est le rythme normal de déploiement, tandis que la deuxième permet d'obtenir de nouvelles fonctions dès qu'elles sont prêtes.

Dans le passé, il était recommandé d'avoir un petit locataire-test distinct à cette fin lorsque l'ensemble du locataire était en mode **Targeted**, ce qui peut être utile si vous disposez du budget nécessaire. Aujourd'hui, il est plus courant de désigner les membres de l'équipe des TI et les gros utilisateurs de votre entreprise aux fins de **diffusion ciblée pour certains utilisateurs**. Il existe également **une option** pour s'assurer que vos applications Office locales pour l'installation d'entreprise reçoivent les mises à jour avant le reste de vos utilisateurs.

ADOPTION

Si votre défi consiste à aider d'autres personnes de votre entreprise à prendre le train M365 en marche, Microsoft a une **grande communauté** et beaucoup de **ressources** pour vous aider, et si vous avez besoin d'aide sur l'adoption de M365 et les charges de travail connexes, joignez-vous au **Programme des champions** gratuit.

Une autre excellente ressource est **Fasttrack** qui fournit des conseils sur la migration pour les différents locataires M365 (et Dynamics 365 et Azure). Si vous utilisez M365 et que vous avez plus de 150 postes utilisateurs, vous pouvez discuter avec un expert en migration en ligne. De même, si vous avez plus de 500 postes, vous pouvez demander à **un ingénieur de vous assister dans la migration** (à distance) et dans les projets d'adoption ultérieurs.

CHAPITRE 1:

BIENVENUE À MICROSOFT (ET OFFICE) 365

DANS CE CHAPITRE, NOUS EXAMINERONS LES DIFFÉRENTES VERSIONS DE M365, COMMENT CHOISIR LA OU LES BONNES VERSIONS ET LA VALEUR AJOUTÉE QU'ELLES APPORTENT À VOTRE ENTREPRISE. COMME NOUS L'AVONS DÉJÀ MENTIONNÉ, SI VOUS AVEZ DÉJÀ CONFIGURÉ VOTRE ENVIRONNEMENT M365 OU QUE VOUS CHERCHEZ DES RENSEIGNEMENTS PLUS AVANCÉS, PASSEZ DIRECTEMENT À LA PARTIE 2.

UNE FOIS DÉPLOYÉE CORRECTEMENT, MICROSOFT 365 CONTRIBUE NON SEULEMENT AU SUCCÈS DE VOTRE ENTREPRISE, MAIS PERMET ÉGALEMENT À VOTRE PERSONNEL DE TRAVAILLER EN ÉQUIPE ET DE COLLABORER DE MANIÈRE SÉCURISÉE, TANT À L'INTERNE QU'AVEC DES PERSONNES EXTERNES. LA SOLUTION PERMET ÉGALEMENT À VOS EMPLOYÉS DE TRAVAILLER EN TOUTE SÉCURITÉ DE LA MAISON OU DE N'IMPORTE OÙ. EN PLUS DE CHOISIR LA BONNE VERSION DE M365, LA CLÉ D'UNE ADOPTION RÉUSSIE EST LA PLANIFICATION, LA FORMATION DES UTILISATEURS FINAUX, MAIS AUSSI L'ASSURANCE QUE VOTRE PERSONNEL DES TI COMPREND SON NOUVEAU RÔLE.

1.1: OFFICE 365

Microsoft se concentre moins sur Office 365 depuis plusieurs années maintenant et cette tendance se poursuivra. Elle n'est plus une option pour les entreprises de moins de 300 employés et pour les grandes entreprises, il est recommandé de se tourner vers les plans Microsoft 365 (voir ci-dessous).

Certains services mentionnés dans ce chapitre sont examinés plus en détail dans les chapitres suivants. Nous utiliserons le terme UGS qui signifie Unité de gestion des stocks. Ce terme décrit les différents niveaux de licence.

Votre première décision est de choisir entre les plans « SKU Business » (UGS Affaires) et « SKU Enterprise » (UGS Entreprise). La première version est limitée à 300 utilisateurs. Si la taille de votre entreprise est plus grande (ou si vous prévoyez de la développer), optez pour la version Enterprise (Entreprise).

À titre de précision **Microsoft 365 Apps for enterprise** – Applications Microsoft 365 pour les grandes entreprises (**qui s'appelait Office ProPlus** auparavant) est le nouveau nom des applications de bureau comme Word, Excel, etc. qui sont disponibles pour Windows et Mac – certaines UGS l'incluent, d'autres non.

Par ailleurs, tous les plans comprennent Office Online (rebaptisé simplement « Office » – ce qui ne prête pas du tout à confusion), donc Word, PowerPoint, etc. fonctionnant dans un navigateur.

Veuillez noter que ces versions en ligne d'Office sont limitées en ce qui concerne la fonctionnalité par rapport à leurs applications de bureau analogues, mais qu'elles sont utiles pour effectuer des modifications rapides.

En ce qui concerne la version Enterprise (qui est simplement un nom; il n'est pas nécessaire que ce soit pour une grande entreprise; par exemple, vous pourriez avoir cinq avocats qui traitent des données très sensibles dans une PME utilisant l'offre Enterprise E5), il y a l'offre **Apps for enterprise (Applications pour l'entreprise)** qui ne vous fournit que des applications pour l'entreprise et le stockage de fichiers OneDrive, mais aucun autre service infonuagique. **E1** vous fournit Office (en ligne) et Exchange, OneDrive, SharePoint, Teams, Yammer et Stream. **E3** vous fournit Microsoft 365 Apps pour l'entreprise en plus des services infonuagiques de E1, et **E5** inclut également PowerBI comme service infonuagique, ainsi que plusieurs fonctions de sécurité (voir le chapitre 15).

Jetez un coup d'œil à **la comparaison officielle** qui montre clairement les différences entre ces plans.

Les différentes options offertes pour **Microsoft 365 et Office 365** couvrent tous les plans, y compris les versions personnalisées pour l'éducation, le gouvernement et les versions spécifiques à chaque pays pour la Chine et l'Allemagne.

Le point le plus important est que les différentes UGS dans chaque famille ne sont pas incompatibles. Dans une petite entreprise de fabrication, il se peut que les travailleurs de l'usine utilisent la version Business Essentials, le personnel de bureau la version Business et les cadres Business Premium. Dans une entreprise plus importante, les utilisateurs pourraient être répartis entre les licences E1, E3 et E5.

Dans la **description des services des plateformes Microsoft 365 et Office 365**, nous vous expliquons ce que la plateforme offre en détail.

1.2: MICROSOFT 365

En plus des plans Office 365 ci-dessus, M365 inclut également Windows 10 Enterprise, Endpoint Manager (Intune) et Azure Active Directory Premium.

Pour les entreprises (jusqu'à 300 utilisateurs), il existe trois options, **M365 Business Basic**, qui inclut Office (en ligne seulement), le courriel, le partage de fichiers, Teams et des fonctions de sécurité. **M365 Business Standard** inclut également la version pour ordinateur de bureau « Microsoft 365 Apps for Business », tandis que **M365 Business Premium** offre en plus la gestion des appareils iOS, Android et Windows 10/11 et l'application des stratégies d'Intune ainsi que de nombreuses fonctions de sécurité avancées. Voir plus.

En ce qui concerne le plan **Enterprise**, il y a **F3** (pour les travailleurs de « première ligne », anciennement appelé F1) qui vous donne Office (en ligne), Windows 10 Enterprise, Active Directory Premium P1, Azure Information Protection P1 et Intune en plus du plan E1 d'O365. **E3** inclut Active Directory Premium P1, Advanced Threat Analytics (ATA), Azure Information Protection P1, Windows 10 Enterprise et Intune en plus d'O365 E3. Enfin, E5 inclut Active Directory Premium P2, Microsoft 365 Defender, Microsoft Defender for Endpoint, Microsoft Defender for Office 365, Microsoft Defender for Identity et Azure Information Protection P2, Windows 10 Enterprise,

une multitude de fonctions de sécurité et Intune en plus d'O365 E5.

Certes, c'est tentant de penser que « Je suis une petite entreprise, alors je peux économiser quelques dollars avec les UGS Business », mais vous devez être conscient de certaines limites. Le stockage de OneDrive Entreprise est limité à 1 To par utilisateur avec le plan Entreprise, tandis qu'à l'échelle de l'organisation, vous pouvez augmenter cette limite en appelant le service de soutien. Microsoft a apporté des changements importants au plan Business Premium et inclut désormais toutes les fonctions du **Plan 1 Azure AD Premium.** Ainsi, en plus des fonctions de sécurité déjà incluses (accès conditionnel, réinitialisation du mot de passe libre-service et authentification multifactorielle), il inclut également la découverte d'applications infonuagiques, le proxy d'application d'Azure AD, les groupes dynamiques et la fonction d'authentification sans mot de passe. Les plans Enterprise (Entreprise) comportent de nombreuses fonctions de sécurité utiles, en particulier M365 E5 (voir le chapitre 15).

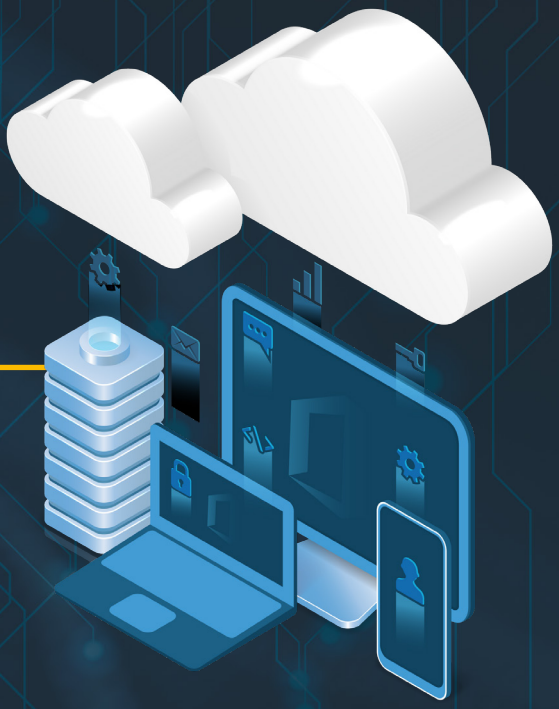
Sachez que vous pouvez déplacer des licences entre différentes UGS (mise à niveau et rétrogradation) et que vous pouvez mettre à niveau des UGS Business vers des UGS Enterprise. Cette discussion a porté sur les UGS complètes et les fonctionnalités qu'elles contiennent, mais il est également possible d'acheter des fonctionnalités individuelles, par exemple Azure Active Directory Premium P1 en tant que fonctionnalité autonome. Selon les besoins de (certains) utilisateurs de votre entreprise, vous pouvez personnaliser un progiciel en y ajoutant les fonctions dont vous avez besoin.

Le **tableau périodique de Microsoft 365** est un excellent moyen de comprendre les différentes parties de M365, comment elles se combinent et une description rapide de chaque service.

La principale leçon à retenir de ce chapitre est de ne pas supposer que, si vous êtes une petite entreprise, vous devriez automatiquement opter pour le forfait UGS Business. Recherchez exactement les fonctions qui répondront aux besoins de votre entreprise et n'hésitez pas à combiner différentes UGS pour divers rôles de travailleurs.

CHAPITRE 2:

GESTION D'O365 ET DE M365



UNE FOIS QUE VOTRE LOCATAIRE EST CONFIGURÉ DANS M365, VOUS DEVREZ LE GÉRER. DANS CE CHAPITRE, NOUS PASSERONS EN REVUE LES DIFFÉRENTES INTERFACES QUE VOUS POUVEZ UTILISER.

SI VOUS N'AVEZ PAS DE LOCATAIRE O365/M365, INSCRIVEZ-VOUS POUR UN LOCATAIRE D'ESSAI – CLIQUEZ SIMPLEMENT SUR « TRY FOR FREE » (ESSAYEZ GRATUITEMENT) SOUS E3 OU E5 CES LOCATAIRES D'ESSAI SONT VALABLES POUR UNE DURÉE DE TRENTE (30) JOURS, MAIS VOUS POUVEZ DEMANDER UNE PROLONGATION DE CES 30 JOURS EN COMMUNIQUANT AVEC LE SERVICE DE SOUTIEN.

2.1: PORTAILS WEB

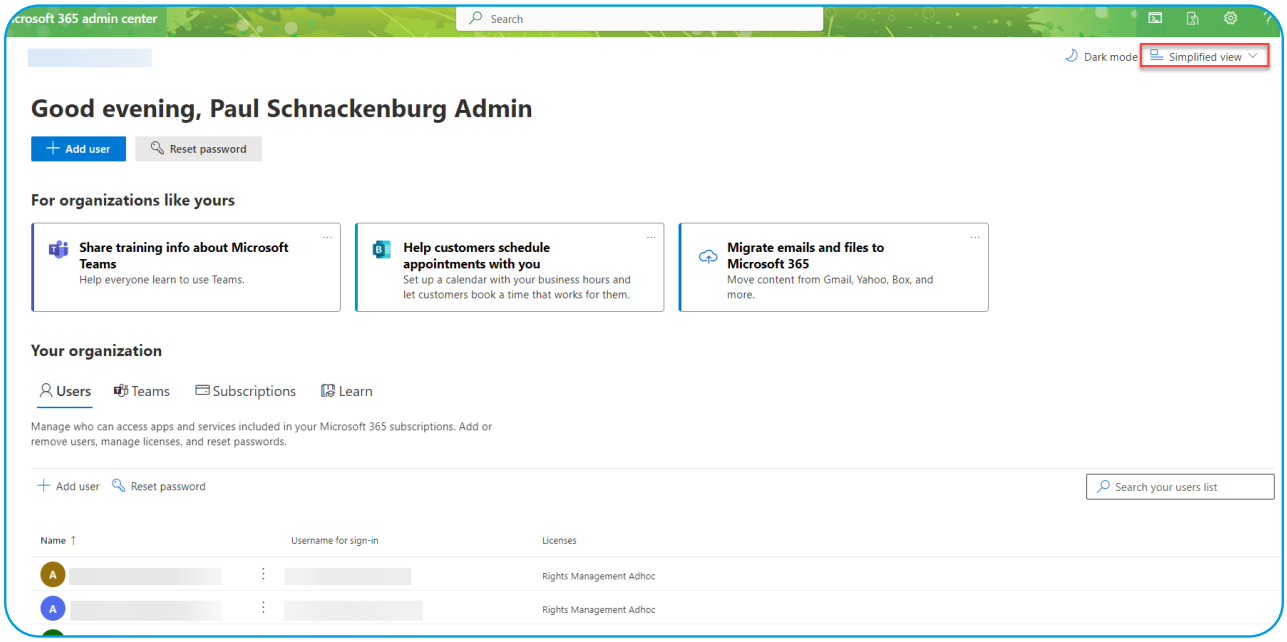
Le portail principal est **admin.microsoft.com**. Vous pouvez également y accéder à partir de **https://www.office.com/?omkt=fr-CA**,en cliquant sur la vignette Admin. Vous trouverez à gauche des liens pour gérer les utilisateurs, les groupes, la facturation et les paramètres et bien plus. Sous Admin Centers (Centres d'administration) plus loin, se trouvent des liens vers les portails individuels d'Exchange, de Teams, de SharePoint, de OneDrive et bien plus. Selon votre UGS, des liens légèrement différents s'afficheront.

Parmi les points saillants du travail quotidien dans votre entreprise, il importe de mentionner la possibilité de sélectionner plusieurs utilisateurs (« Users – Active users »/Utilisateurs – Utilisateurs actifs) et de modifier leur licence, par exemple. Vous pouvez gérer les utilisateurs externes invités qui ont reçu des documents de OneDrive ou de SharePoint, par exemple, sous « Users – Guest users » (Utilisateurs – Utilisateurs invités). Vous pouvez également restaurer un utilisateur récemment supprimé (30 jours ou moins).

Vous pouvez gérer des groupes et des boîtes aux lettres partagées, comme « ventes@nomdentreprise .com », qui est accessible par plusieurs personnes, ainsi que des ressources, telles que des salles et des équipements (réservation de salles de conférence ou de voitures d'entreprise). La facturation est l'endroit où vous pouvez acheter des licences supplémentaires, gérer vos abonnements et vos modes de paiement, et la section Soutien est l'endroit où vous formulez des demandes de service. Sous « Settings » (Paramètres), il y a une zone où vous pouvez configurer différents services et modules complémentaires, tandis que « Setup » (Configuration) vous permet de gérer vos domaines de messagerie. Les rapports comportent à la fois des rapports sur l'utilisation et des rapports sur la sécurité, tandis que ceux sur l'état (Health) comportent deux domaines importants. Les rapports sur l'état du service vous indiquent s'il y a des problèmes dans le nuage avec vos ressources et le Message center contient une liste des mises à jour et des changements à venir.

Chaque centre d'administration vous permet de gérer un service individuel, comme Azure Active Directory ou Teams. La page **Msportals.io** contient des liens mis à jour pour la plupart des différents portails auxquels vous pouvez accéder directement sans passer par le portail principal.

Veuillez noter que si vous êtes une petite entreprise, il est possible d'avoir le centre d'administration dans « Simplified view » (Vue simplifiée) au lieu de l'affichage du tableau de bord, ce qui masque la majeure partie des aspects complexes et permet d'accéder facilement aux tâches de base de l'utilisateur, du groupe, de Teams et de la gestion des appareils. Cliquez simplement sur « Simplified view » dans le coin supérieur droit de la page d'accueil du centre d'administration.



Vue simplifiée du Centre d'administration M365

2.2: POWERSHELL

Pour les petits locataires, vous n'aurez probablement jamais à vous aventurer au-delà du portail Web, mais si vous avez un grand nombre d'utilisateurs, vous voudrez automatiser les tâches courantes dans PowerShell à l'aide du nouveau module **Azure AD**.

Pour installer le module, dans une fenêtre PowerShell surélevée, exécuter simplement la commande suivante :

```
Install-Module -Name AzureAD
```

Pour vous connecter (et vous authentifier éventuellement à l'aide de la fonction d'authentification multifactorielle), exécuter la commande suivante :

```
Connect-AzureAD
```

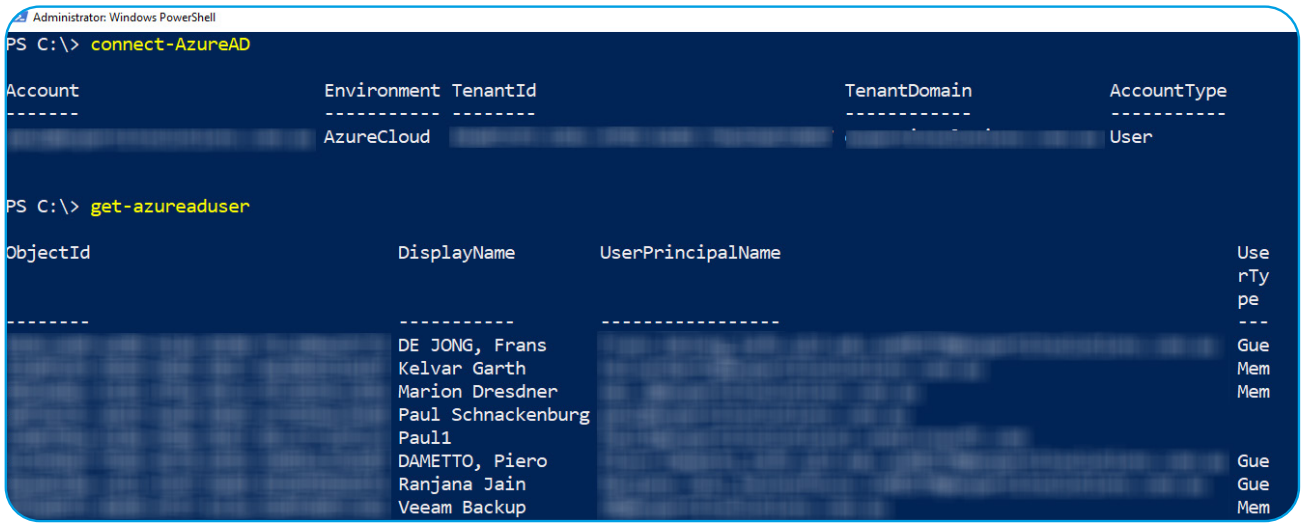
Pour vous assurer que tout fonctionne, exécuter la commande suivante :

```
Get-AzureADUser
```

Cette commande vous donnera une liste des utilisateurs de votre locataire. Reportez-vous aux **instructions complètes**, y compris si vous voulez vous connecter à des locataires gouvernementaux ou chinois/allemands.

Une fois connecté, vous pourrez effectuer de nombreuses tâches, voire les automatiser, et **gérer les comptes utilisateur et les licences, créer des sites SharePoint et gérer des utilisateurs et des groupes, configurer des paramètres Exchange, gérer des migrations de courriels** (chapitre 3) et configurer les informations sur Teams. Veuillez noter que plusieurs de ces tâches nécessitent l'installation de modules supplémentaires.

Microsoft a **finalement établi** une façon officielle et programmée d'exécuter une seule session PowerShell connectée à tous les différents services, que vous utilisiez l'authentification multifactorielle (chapitre 7) ou non.



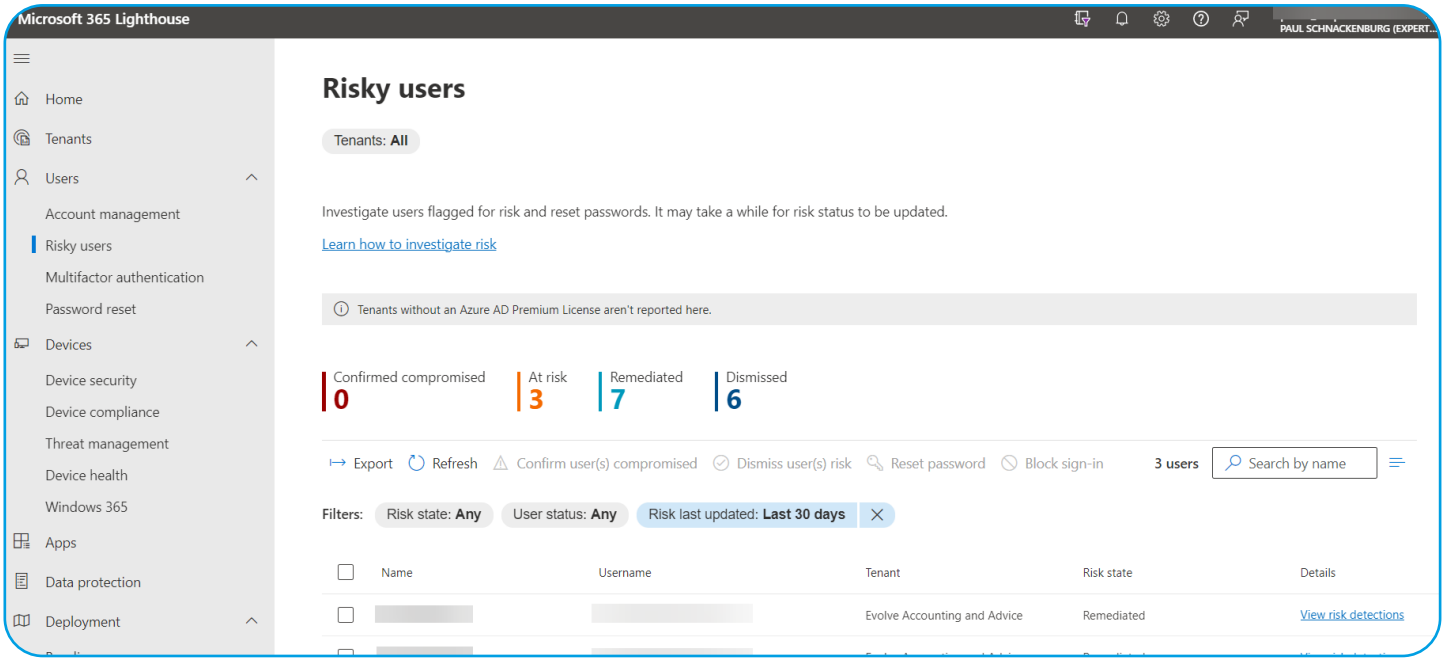
Connexion à PowerShell

Pour SharePoint (en ligne et sur site en 2013, 2016, 2019), il y a une solution de rechange ou un complément libre appelé **PnP PowerShell** au module SharePoint officiel par l'équipe Patterns and Practices (PnP) – Modèles et pratiques. Les cmdlets SharePoint Online officiels sont axés sur la création et la gestion de sites et d'utilisateurs, tandis que les cmdlets PnP sont utiles pour travailler avec des artefacts à l'intérieur de sites qui ont déjà été créés.

Si vous devez gérer les paramètres des locataires M365 ou les extensions SharePoint Framework (SPFX), jetez un coup d'œil sur **l'interface de ligne de commande pour Microsoft 365,** également par l'équipe PnP, **qui fonctionne sous Windows, macOS, Linux.** Par ailleurs, si vous n'avez pas envie de faire vous-même l'installation de l'interface de ligne de commande dans votre boîte, vous pouvez **l'exécuter directement dans Azure Cloud Shell.**

2.3: MICROSOFT 365 LIGHTHOUSE

Si vous êtes un fournisseur de services gérés (FSG) avec plusieurs locataires M365 à gérer, vous devriez utiliser Microsoft 365 Lighthouse, à ne pas confondre avec Azure Lighthouse. Les deux sont des technologies qui permettent aux fournisseurs de services de gérer plusieurs clients locataires, mais là où la version d'Azure est une façon de permettre aux utilisateurs du fournisseur de services d'accéder aux ressources d'Azure, M365 Lighthouse est un portail qui vous permet d'intégrer plusieurs locataires et d'appliquer les stratégies et la gestion (y compris les réinitialisations de mot de passe pour tout utilisateur, dans tout locataire) dans une console unique.



Microsoft 365 Lighthouse

CHAPITRE 3:

MIGRATION VERS O365

SI VOUS ÊTES UNE NOUVELLE ENTREPRISE, CE CHAPITRE NE S'APPLIQUE PAS À VOUS. VOUS N'AVEZ QU'À CRÉER DES COMPTES D'UTILISATEUR DANS LE NUAGE, AJOUTER VOS APPAREILS WINDOWS 10/11 À ENTRA ID ET GÉRER VOS APPAREILS IOS ET ANDROID AVEC ENDPOINT MANAGER ET LE TOUR EST JOUÉ.

3.1: MIGRATION

Cependant, la plupart des entreprises ont investi dans des technologies existantes sur site et doivent **migrer vers M365**. Ce chapitre couvre vos différentes options :

- Migration à basculement
- Migration par étapes
- Migration hybride express
- Migration hybride minimale
- Migration hybride
- Migration PST
- Migration IMAP
- Outils tiers

Si vous n'avez pas Exchange sur site, c'est-à-dire si vous utilisez **Lotus Notes** / Domino, un autre système de courriel, **Google Workspace** ou une autre solution de courriel infonuagique, vous devez envisager une migration IMAP ou des services de migration tiers.

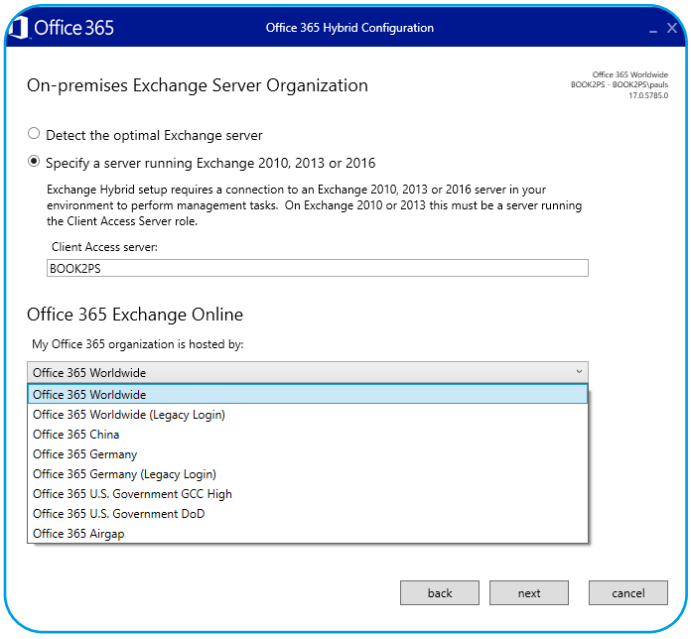
La plupart des autres méthodes de migration reposent sur la synchronisation d'annuaires où vos comptes AD sur site sont synchronisés avec Azure AD, que nous aborderons au chapitre 7.

Si vous êtes toujours sur Exchange 2007, 2010 ou 2013 (tous ne sont plus pris en charge), une configuration **par étapes** vous permet **de migrer des boîtes aux lettres en lots,** une fois que vous avez configuré la synchronisation d'annuaires. Sachez que vous devrez reconfigurer manuellement le profil Outlook de chaque utilisateur pour qu'il puisse pointer vers Office 365 lorsque sa boîte aux lettres aura été migrée.

Pour les environnements plus petits, l'approche de **basculement** est la solution la plus facile. Microsoft parle de **cette méthode** pour moins de 2 000 boîtes aux lettres (Exchange 2003+), mais dans le monde réel, elle convient probablement pour 100 à 150 boîtes aux lettres environ, selon la bande passante d'Internet. L'idée est de déplacer la boîte aux lettres de tout le monde du site vers le nuage au cours d'une fin de semaine ou suivant un autre créneau mieux approprié.

Si vous utilisez Exchange 2010 ou des versions ultérieures et que vous prévoyez déplacer toutes les boîtes aux lettres dans le nuage en l'espace de quelques semaines, envisagez l'option **hybride Express**. Si vous avez une plus grande entreprise et que vous envisagez une période de migration de quelques mois, optez pour l'option **hybride minimale**. Si vous avez un environnement plus vaste (Exchange 2010 ou des versions ultérieures) et que vous vous attendez à être dans un état hybride pendant une période prolongée et que vous avez besoin de la capacité de déplacer les boîtes aux lettres du nuage vers le site (offboarding), envisagez le modèle **hybride complet.** Pour voir la répartition complète des différentes versions des hybrides, voir **ici.** Les divers types d'hybrides **offrent une coexistence riche** avec une liste d'adresses globale unifiée, le partage de renseignements de calendriers libres ou occupés et des déplacements de boîte aux lettres qui sont simples pour les utilisateurs finaux. Lorsque leur boîte aux lettres a été déplacée, ils doivent simplement redémarrer Outlook.

Si vous devez garder un serveur Exchange (ou plusieurs) sur site, soyez conscient de la nécessité de **le tenir à jour de façon à éviter les dysfonctionnements**, et si possible, **cherchez à le retirer**. Utilisez plutôt les cmdlets PowerShell pour gérer les attributs Exchange dans AD.



Assistant de configuration hybride

La **documentation de Microsoft** vous dirigera vers le **conseiller en migration de courrier**, qui peut vous conduire à l'assistant de configuration hybride (ACH), selon vos choix dans le conseiller. L'ACH vous indiquera les étapes individuelles que vous devez suivre, selon le processus choisi, y compris les versions hybrides ainsi que l'approche « Par étapes » et de « Basculement ».

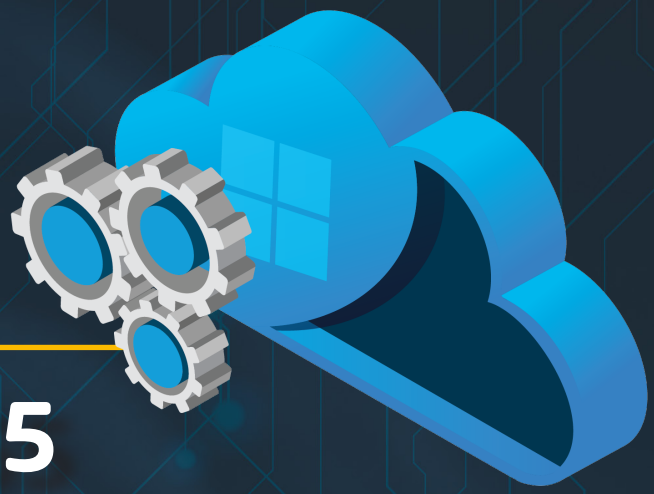
Les **migrations IMAP** vous permettent de passer des systèmes non Exchange qui prennent en charge IMAP avec une limite de 500 000 objets par boîte aux lettres et une taille de courriel maximale de 35 Mo.

Si vous avez des fichiers PST contenant des courriels dans votre site, vous **pouvez les migrer vers Office 365.** D'ailleurs, il y a même un outil de collecte PST pour les retrouver sur votre réseau et les récupérer. Si vous en avez beaucoup, vous pouvez même **les envoyer sur des disques vers Microsoft.**

Une fois la migration terminée, vous devrez tenir compte de votre **enregistrement DNS de Mail Exchanger (MX)**, qui pointera vers votre serveur de courrier sur site et qui doit maintenant être remplacé par Exchange Online. Vous devez également revoir vos **enregistrements DNS Autodiscover,** ce qui permet à Outlook et aux autres clients de courriel de trouver automatiquement le bon serveur Exchange. Si vous cherchez une expérience simple de migration de boîte aux lettres, Hornetsecurity offre l'outil de migration de boîte aux lettres (Mailbox Migration Tool ou MMT) comme module de **365 Total Protection Enterprise** / **Enterprise Backup**.

CHAPITRE 4:

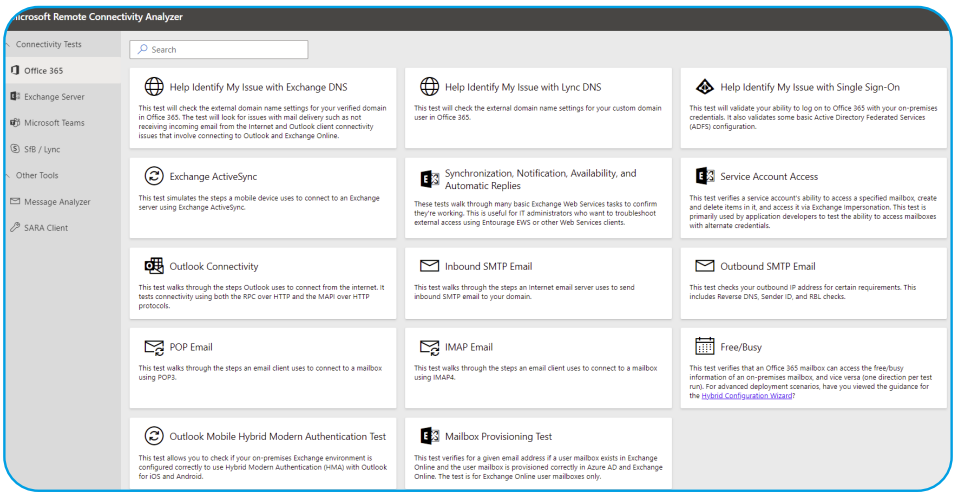
SOUTIEN DE M365



UN GRAND DÉFI POUR NOUS DANS LE DOMAINE DES TI, DU MOINS AU DÉBUT, EST LA PERTE DE CONTRÔLE QUE LE NUAGE ENTRAÎNE. SI VOUS AVEZ UN PROBLÈME DE LIVRAISON DE COURRIELS SUR SITE, VOUS POUVEZ VÉRIFIER CHAQUE MAILLON DE LA CHAÎNE POUR DÉTERMINER OÙ SE SITUE LE PROBLÈME. UNE FOIS QUE VOUS AVEZ MIGRÉ VERS M365, C'EST MAINTENANT UNE RESPONSABILITÉ PARTAGÉE ENTRE VOUS ET MICROSOFT. DANS CE CHAPITRE, NOUS EXAMINERONS DEUX OUTILS D'AUTO-ASSISTANCE QUE J'UTILISE EN CAS DE PROBLÈME, PUIS NOUS EXAMINERONS COMMENT OUVRIR ET TRAITER UN TICKET DE SOUTIEN AVEC MICROSOFT.

4.1: TESTER LA CONNECTIVITÉ

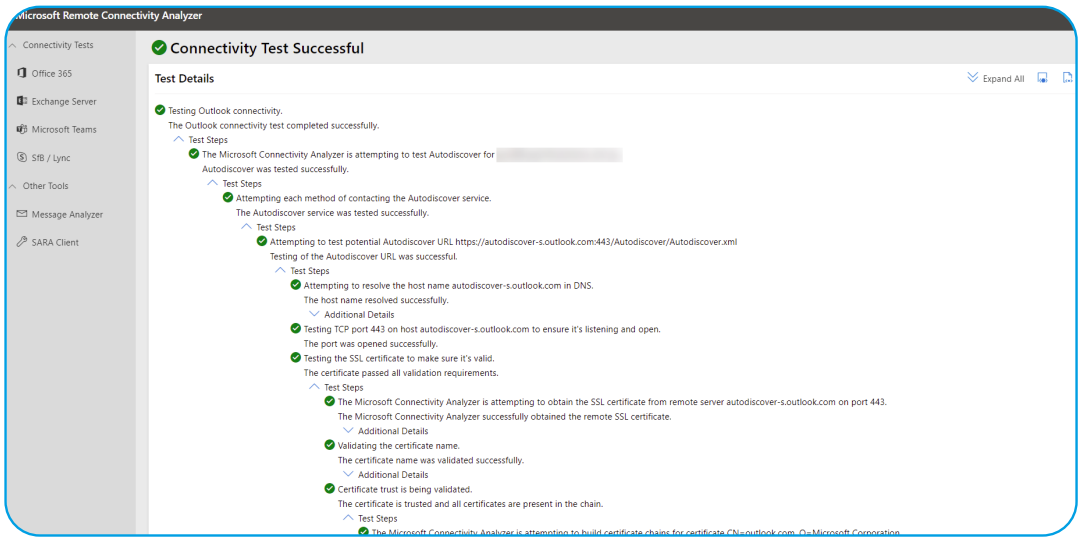
La connectivité aux courriels et à Teams est un facteur récurrent à l'origine des problèmes. Microsoft offre un outil utile, l'Analyseur de connectivité à distance Microsoft, en anglais Microsoft Remote Connectivity Analyzer (MRCA ou RCA) à l'adresse **https://testconnectivity.microsoft.com/.**



Analyseur de connectivité à distance

Ici, vous pouvez tester plusieurs fonctionnalités, notamment les suivantes : entrées DNS, connectivité ActiveSync à Exchange, Outlook, fonctionnalité Outlook Autodiscover, ainsi que les courriels SMTP entrants et sortants et bien plus. Choisissez le test que vous devez effectuer et saisissez les renseignements requis. Selon le type de test, vous devrez peut-être saisir un nom d'utilisateur et un mot de passe valides – je vous suggère de réinitialiser le mot de passe de ce compte une fois le dépannage terminé. La vérification Captcha dure 30 minutes, donc si vous faites plusieurs tests en changeant des valeurs, vous n'avez pas à vérifier que vous êtes un humain à chaque fois.

Les résultats du test sont complets et devraient vous aider à cerner le problème assez rapidement.

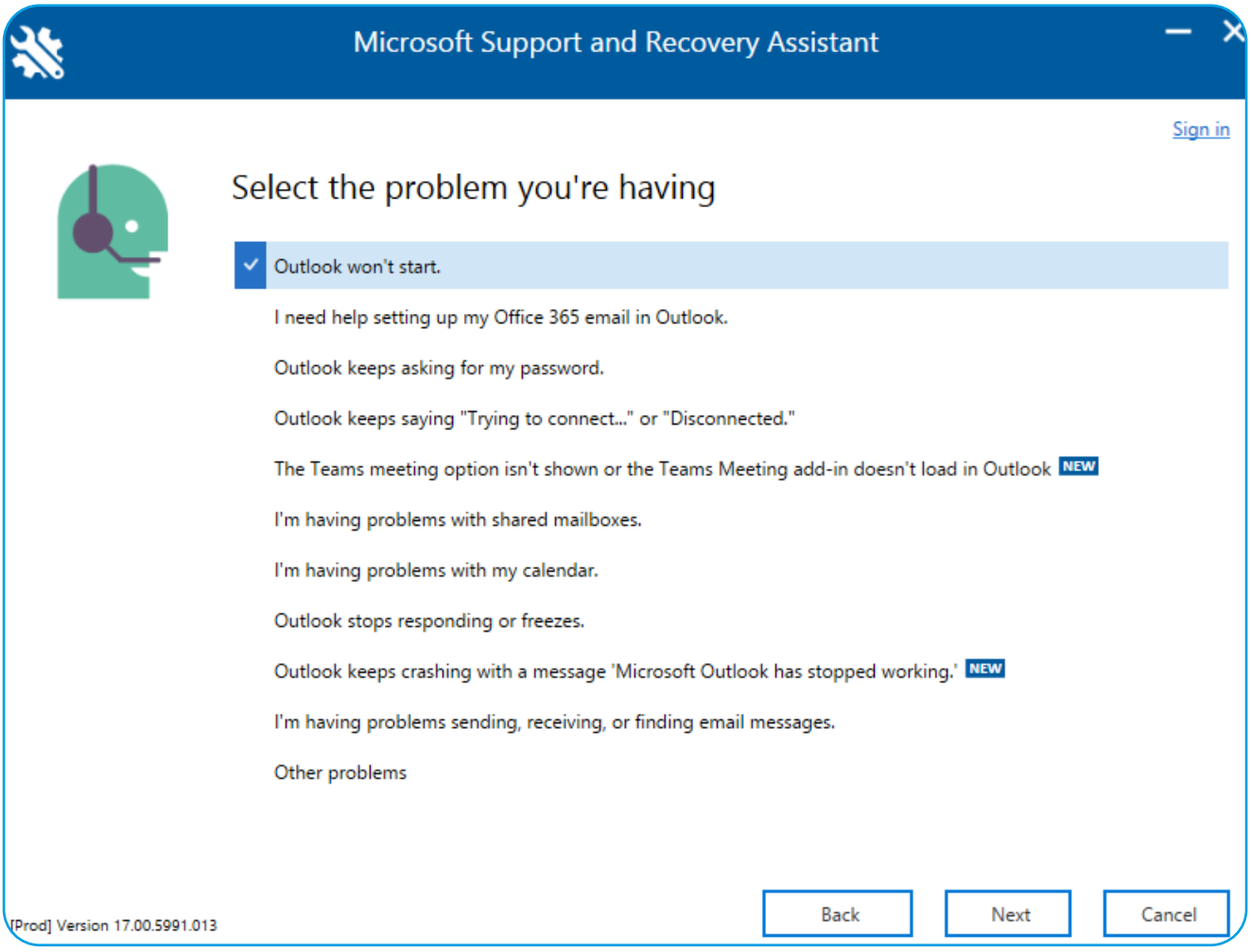


Rapport du test de connectivité

4.2: OUTILS CÔTÉ CLIENT

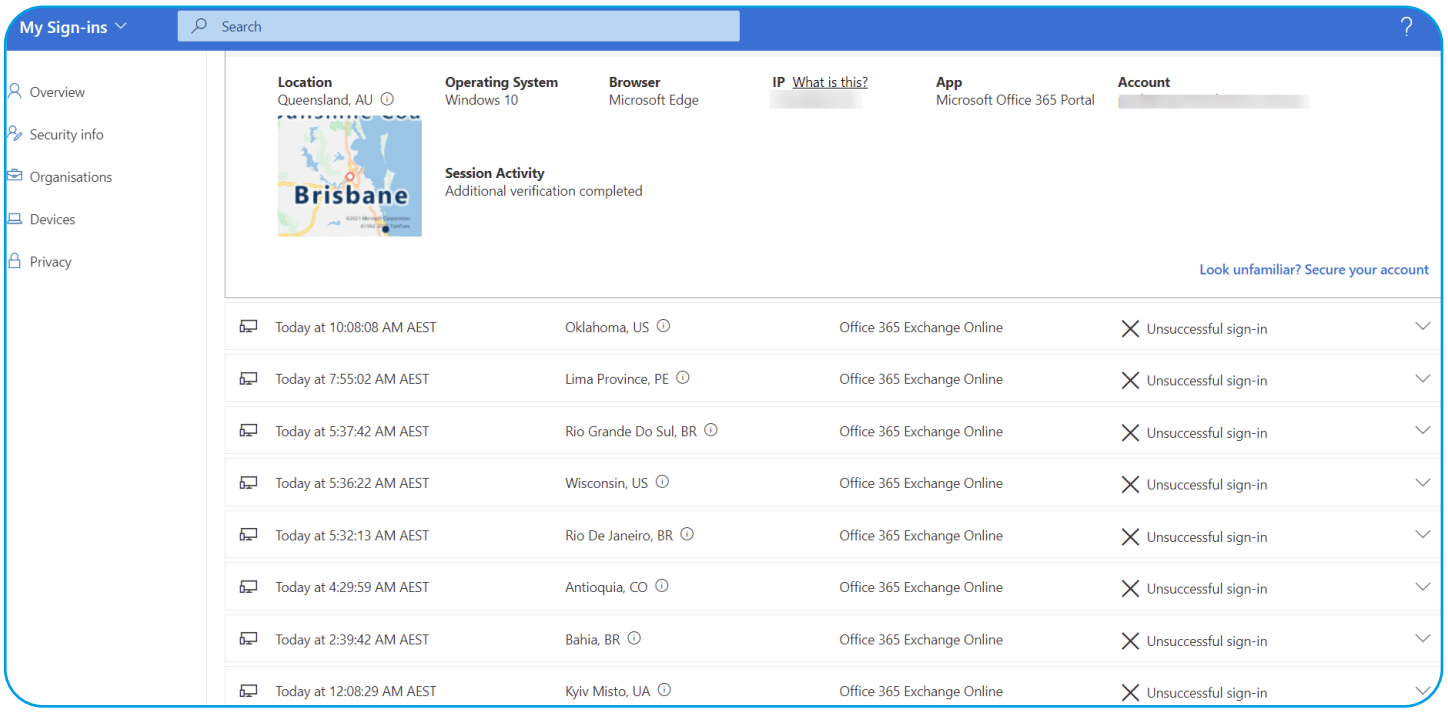
Si le problème n'est pas lié à la connectivité et que vous soupçonnez plutôt un problème sur un appareil client en particulier, vous devez utiliser l'outil **Assistant Support et récupération de Microsoft Office 365 (SARA)**, qui vous aidera à identifier les problèmes liés à Outlook, Dynamics 365 et OneDrive Entreprise, ainsi qu'aux applications pour les problèmes d'entreprise. Il s'agit d'un simple téléchargement que vous exécutez sur l'appareil touché; il vous invite à répondre à quelques questions afin de localiser le problème.

D'après mon expérience, lorsque vous avez des problèmes de profil ou de connexion intermittente (qui ne sont pas attribuables à une mauvaise configuration du côté service – voir le RCA), l'Assistant Support et récupération est un outil assez efficace pour vous aider à trouver la cause.



Assistant Support et récupération

Les sites My Sign-ins (Mes connexions), My Groups (Mes groupes), My Access (Mes accès) et My Applications (Mes applications), donnent aux utilisateurs un bon moyen de gérer leur accès aux services M365. L'option « Mes connexions » est également un excellent outil de formation, car il dresse la liste des connexions réussies et des connexions échouées de la part de pirates. Voici une liste de ce à quoi ressemble mon compte au cours d'une journée typique (l'authentification multifactorielle est activée pour ce compte) :



Mes connexions avec les tentatives d'ouverture de session par des pirates

4.3: DEMANDES DE SERVICE

Une fois que vous avez épuisé les options de libre-service, cliquez sur le bouton « Need help? » (Besoin d'aide?) dans le coin inférieur droit du portail. Commencez par saisir une description de votre problème pour obtenir des résultats en rapport avec des problèmes courants et leur solution. Une fois que vous avez appuyé sur la touche Entrée, l'option Contact support (Contacter le service de soutien) s'allume au bas de l'écran. Saisissez vos coordonnées et votre mode de communication de préférence (téléphone ou courriel). Vous pouvez également joindre des captures d'écran ou des fichiers journaux (jusqu'à cinq, chacun de moins de 25 Mo), choisir un fuseau horaire et une langue pour la communication.

D'après mon expérience, le soutien pour M365 est bon et permet généralement de trouver le problème beaucoup plus rapidement par rapport aux forums et en essayant différentes solutions.

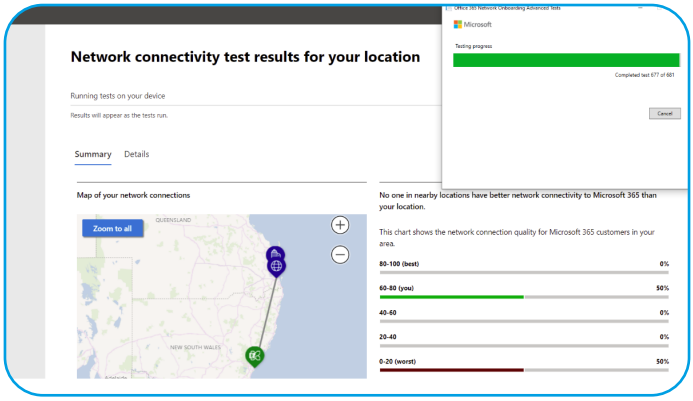
Dans les coulisses, dans les rares cas où l'ingénieur de soutien a besoin d'accéder à un serveur qui héberge vos données, il utilise un « système de boîtier de sécurité » où il demande l'accès et où un superviseur approuve la demande pour une période limitée. Si vous utilisez O365/M365 E5, il se peut que vous ayez activé le service **Customer Lockbox** (boîtier de sécurité du client), ce qui vous associera à ce processus et vous incitera à approuver la demande également.

Si, en revanche, le problème se situe de votre côté, les techniciens d'assistance utilisent la fonction Quick Assist (Assistance rapide) dans Windows pour se connecter à votre serveur ou à votre ordinateur personnel client en mode visualisation seule et résoudre le problème avec vous.

4.4: SERVICE HEALTH (ÉTAT DU SYSTÈME)

La section Health du centre d'administration fournit des renseignements sur l'état général des différents services dans M365 et, en cas de pannes ou d'incidents touchant votre locataire, à condition que vous puissiez accéder au portail. Si la panne touche le portail ou la section Health, essayez à l'aide de la page **https://status.office365.com/**. Assurez-vous également de suivre @Office365Health et @MSFT365Status sur Twitter.

La section Health présente également un nouvel outil intéressant appelé **Network connectivity (Connectivité réseau)** qui utilise le client OD4B, ainsi que le service de localisation Windows et des tests de collecte manuelle de données facultatifs pour identifier la **qualité de la connectivité de chaque client à Office 365**. Elle a même son **propre portail.**

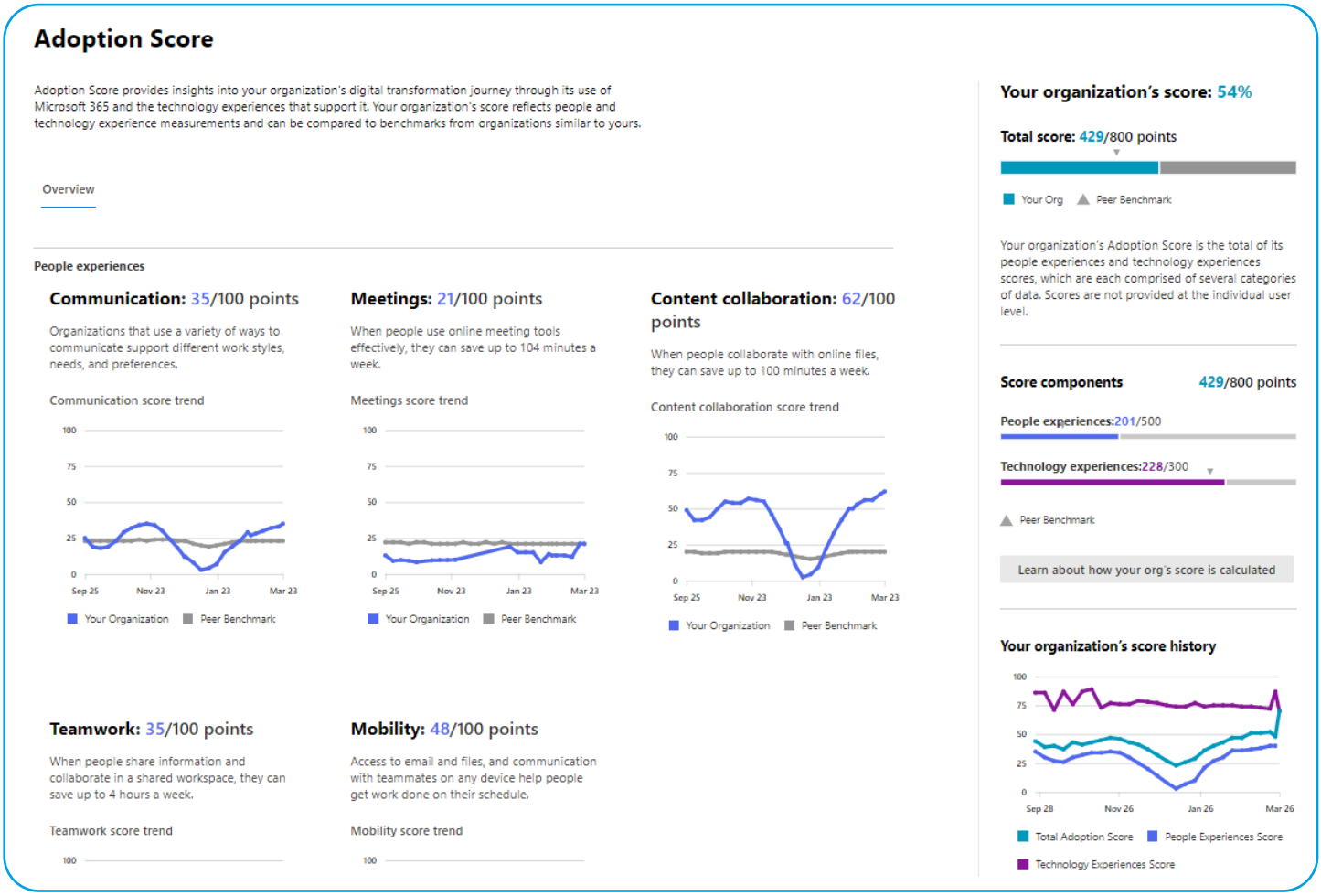


Test de connectivité réseau manuel vers Office 365

4.5: CONNECTIVITÉ RÉSEAU

De nombreuses entreprises offrent une expérience en deçà des normes à leurs utilisateurs en les obligeant à utiliser des connexions RPV (réseau privé virtuel) pour accéder au bureau, puis à Office 365

(dans l'ensemble, une expérience plus lente, mais qui élimine la nécessité d'effectuer des appels vocaux et vidéo de Teams), ou même en mettant une passerelle en place pour l'ensemble du trafic sortant pour des raisons de « sécurité ». Ce dernier scénario repose sur l'hypothèse erronée selon laquelle tous les services Web et les sites Internet sont « mauvais » et que tout le trafic doit être inspecté, au lieu de faire la distinction entre les services opérationnels fournis par Microsoft et d'autres sites de confiance et les sites douteux et de gérer le trafic en conséquence. Voici un **excellent article** décrivant les techniques d'optimisation requises et facultatives pour M365. Microsoft a également établi des partenariats avec de nombreux fournisseurs de services Internet (FSI), partenaires d'Internet Exchange (PIX) et fournisseurs de services de software-defined cloud interconnect ou SDCI (plateforme d'interconnexion en nuage définie par logiciel) pour une connectivité optimale à M365, Dynamics 365 et Azure au moyen d'**Azure Peering Service.**



Note d'adoption de Microsoft 365

Si votre entreprise utilise un Software Defined WAN ou SD-WAN (réseau étendu défini par logiciel), il existe une fonction appelée **routage réseau éclairé** qui vous aidera à optimiser votre connectivité en permettant le partage de données entre Microsoft et le fournisseur de service de réseau étendu défini par logiciel pour réacheminer automatiquement le trafic, le cas échéant. À l'heure actuelle, seul le service IOS XE SD-WAN de Cisco est pris en charge, mais on s'attend à ce que d'autres soient ajoutés à mesure que la prévisualisation progresse.

La nouvelle **note de productivité** est conçue pour vous aider à comprendre où en est votre entreprise dans son parcours de transformation numérique et permet de faire le suivi des mesures dans deux catégories : l'expérience des employés et l'expérience technologique.

4.6: DESIRED STATE CONFIGURATION (CONFIGURATION DE L'ÉTAT SOUHAITÉ) DE MICROSOFT 365

PowerShell dispose depuis longtemps d'une fonction appelée Desired State Configuration (DSC) qui définit comment un système (machine virtuelle, application, etc.) doit fonctionner, applique les stratégies et le gestionnaire de configuration local s'assure que le système dispose des bons paramètres, en vérifiant périodiquement les dérives. C'est ce qu'on appelle Infrastructure as Code (Infrastructure en tant que code) et qui est **maintenant disponible pour M365** de sorte que vous pourriez avoir un locataire test où vous évalueriez de nouvelles configurations et de nouveaux paramètres que vous pourriez ensuite exporter et appliquer à votre locataire de production. Il peut également être utilisé pour exporter toutes vos configurations en tant que « sauvegarde », produire périodiquement des rapports sur les changements de configuration et comparer les paramètres de votre locataire avec les pratiques exemplaires.

CHAPITRE 5:

CLIENTS

IL Y A DE NOMBREUX LOGICIELS QUE VOUS POUVEZ UTILISER POUR VOUS CONNECTER À M365 – NOUS LES EXAMINERONS DANS CE CHAPITRE, AINSI QUE LA FAÇON DONT VOUS LES GÉREZ DU POINT DE VUE DE LA GOUVERNANCE.

5.1: CHOIX DE BUREAU

Microsoft recommande la dernière version de Chrome, Edge, Firefox, Safari ou Internet Explorer 11 pour accéder à M365.

Si vous avez installé le client Microsoft Office, toutes les versions prises en charge devraient fonctionner avec M365, mais il est préférable d'utiliser les applications pour les versions d'entreprise pour Windows et Mac qui sont incluses avec Business Premium et E3+. Vous pouvez **contrôler quels utilisateurs obtiennent le Current Channel (canal actuel) recommandé** et qui obtient le Monthly Enterprise channel (Canal Entreprise mensuel) ou le Semi-Annual Enterprise Channel (Canal Entreprise semestriel). Si vous souhaitez vivre à la pointe de la technologie, vous pouvez vous inscrire au **programme Office Insider** pour tester de nouvelles fonctions bêta.

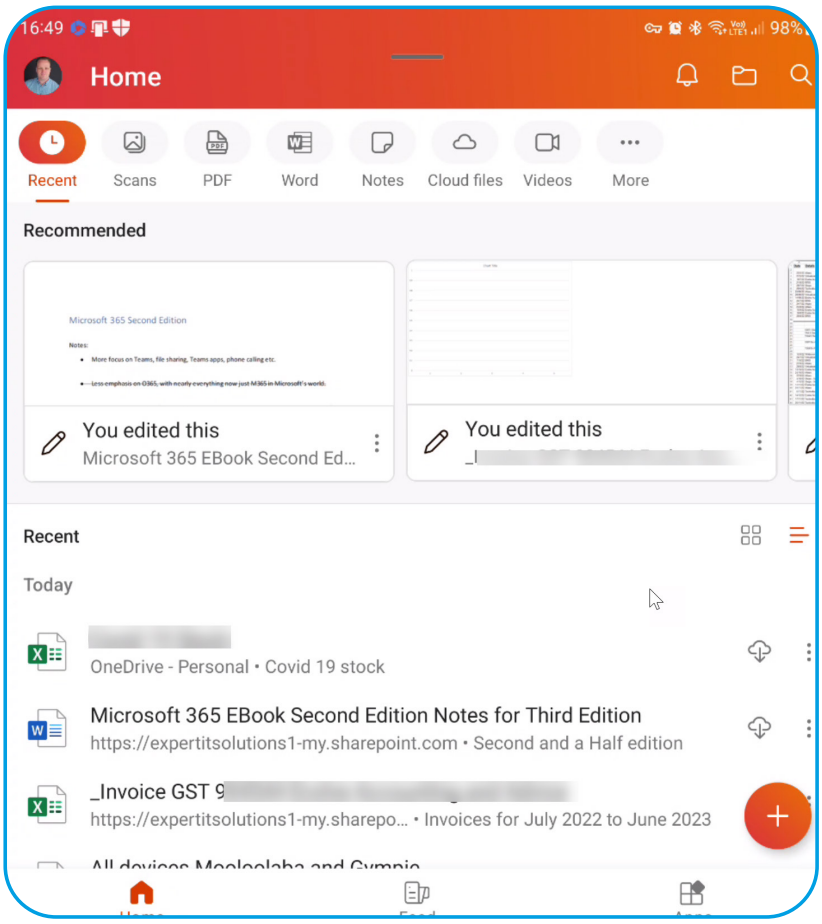
Le service Outlook Web App (OWA) ou Outlook pour le Web mérite d'être mentionné, car il s'agit d'une version extrêmement efficace et non pas d'une version « modifiée » d'Outlook qui s'exécute dans un navigateur. En fait, Microsoft teste souvent de nouvelles fonctions et approches dans le client Web parce qu'il permet de déployer les changements beaucoup plus rapidement. Vous pouvez utiliser les stratégies OWA pour **contrôler les fonctions** disponibles pour vos utilisateurs finaux.

Vous pouvez contrôler les protocoles que les utilisateurs peuvent utiliser pour se connecter à Exchange avec **Client Access Rules (Règles d'accès client)**.

5.2: CHOIX D'APPAREILS MOBILES

Pendant de nombreuses années, la façon privilégiée de se connecter à Exchange en ligne pour le courrier électronique était d'utiliser ActiveSync, un protocole que le client de courrier dans iOS et Android prend en charge (certaines fonctions n'étaient pas prises en charge par les différents fournisseurs). Microsoft recommande maintenant d'utiliser l'application client Outlook gratuite, qui permet à Microsoft d'introduire de nouvelles fonctions beaucoup plus rapidement, sans avoir à attendre qu'Apple ou Google procède à la mise à niveau. Cette application est de plus en plus utilisée par plus de 100 millions de personnes, notamment pour se connecter à Gmail et à d'autres services de courriel.

Il y avait autrefois des applications Word, Excel, etc. distinctes pour les appareils mobiles, mais elles sont toutes regroupées dans l'application Microsoft 365 (Office) qui vous permet d'ouvrir les différents types de documents Office et de les modifier sur les appareils mobiles. L'installation est gratuite, mais la fonctionnalité dépend du compte avec lequel vous ouvrez une session.



Application M365 (Office) sur appareil mobile

5.3: ONEDRIVE ENTREPRISE

Le client de synchronisation est automatiquement installé sur le système d'exploitation Windows ou Mac lorsque les applications pour entreprise sont installées, et vous pouvez contrôler son comportement à l'aide de **ce modèle de stratégie de groupe**. Veuillez former vos utilisateurs à l'utilisation de OneDrive Entreprise. Il ne faut pas sous-estimer la capacité de mettre vos fichiers à disposition sur n'importe quel appareil que vous utilisez, en particulier la capacité d'accéder à n'importe quel appareil (si vous n'avez pas vos propres appareils à portée de la main), ouvrez une session sur **www.office.com** dans n'importe quels navigateur et modifier ces mêmes fichiers.

5.4: TEAMS

L'application Teams (chapitre 11) est le client de collaboration tout-en-un de Microsoft qui offre du soutien pour les clavardages par messagerie instantanée, les clavardages de groupe, les appels vocaux, les appels vidéo et, si vous avez la licence, les appels du réseau téléphonique public commuté (RTPC) à destination et en provenance des téléphones normaux. Teams remplacera Skype Entreprise et, à compter du début de 2019, le client sera automatiquement installé lorsque vous installerez des applications pour entreprise. Si vous devez les déployer au moyen de votre outil de déploiement logiciel préféré, utilisez ce **Microsoft Windows Installer (MSI).**

Au moment de la rédaction de la nouvelle application client de Teams, la prévisualisation publique devrait régler les deux principaux problèmes que les gens ont avec le client actuel : la performance (le client est une application électronique et utilise beaucoup d'unité centrale et de mémoire) et l'échange entre différents locataires.

5.5: APPS ADMIN CENTER (CENTRE D'ADMINISTRATION DES APPLICATIONS)

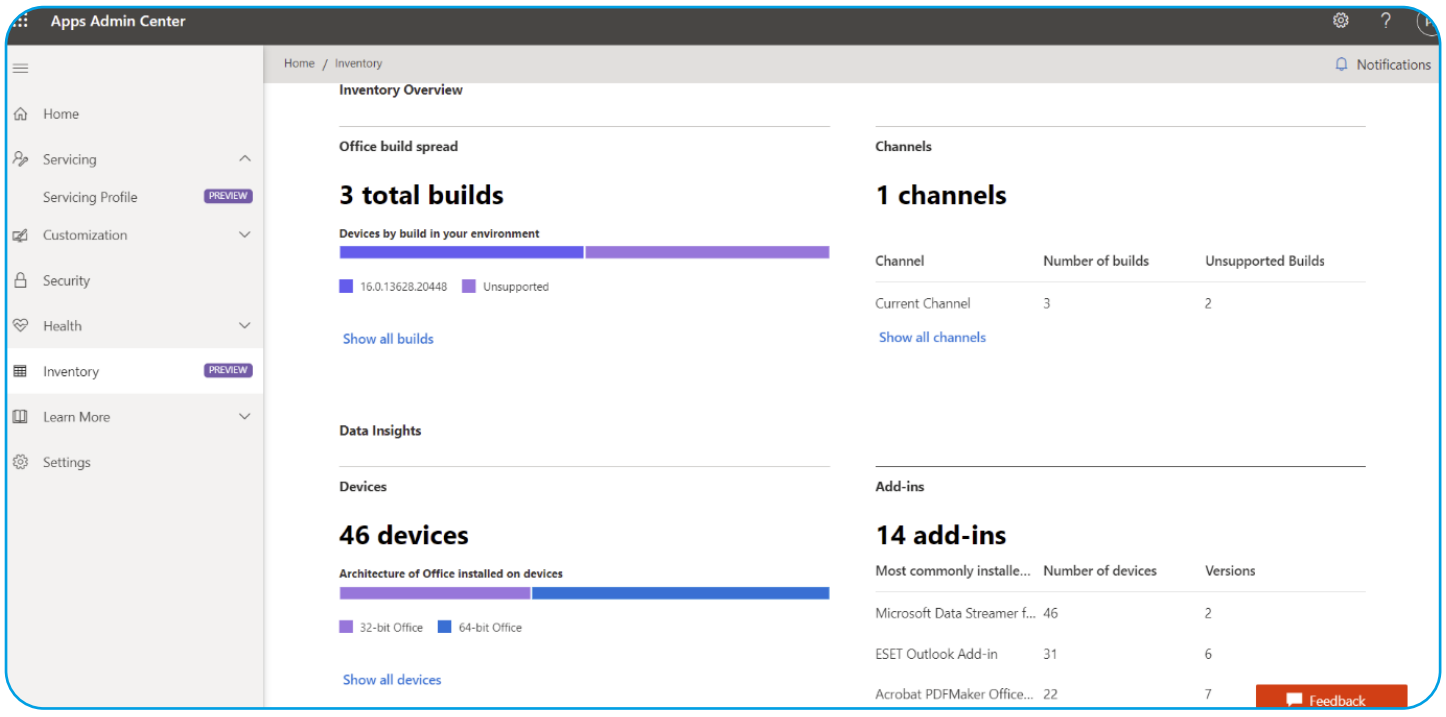
Le centre d'administration des applications Microsoft 365 est une fonction de gestion infonuagique des applications d'entreprise très intéressante (Office sur bureau Windows). Au lieu de gérer les paramètres de personnalisation à l'aide de l'outil Office Deployment Tool ou ODT (outil Déploiement d'Office), vous utilisez le portail infonuagique pour créer les fichiers XML requis. Le centre d'administration des applications vous permet toutefois de faire beaucoup plus. Il présente la liste des installations d'Office dans l'ensemble de votre locataire, vous permet de faire le suivi des versions et des numéros de versions installées, celles qui ne sont plus prises en charge et de créer des profils de service pour déployer des versions plus récentes d'Office. Il utilise également le Security Policy Advisor (Outil de définition de stratégies de sécurité) pour analyser l'utilisation actuelle des applications et vous permet de créer et de déployer des configurations de stratégies dans toutes les applications pour installations d'entreprise (sans vous fier aux objets de stratégie de groupe ou à la gestion des appareils mobiles) et de suivre les modules complémentaires qui sont utilisés sur tous vos appareils.

Si vous avez un grand nombre d'utilisateurs, vous devez désactiver l'option permettant aux utilisateurs de télécharger des applications pour entreprise à partir de **www.office.com** (portail M365 – Settings [Paramètres] – Services & add-ins [Services et modules complémentaires] – Office software download settings [Paramètres de téléchargement du logiciel Office]) et les déployer à l'aide de votre méthode préférée. Si votre entreprise utilise le System Center Configuration Manager, il peut être utilisé pour **déployer et mettre à jour des applications pour l'entreprise.**

Étant donné qu'aucune licence supplémentaire n'est requise pour le centre d'administration des applications, vous devriez vérifier si cela peut vous faciliter la vie en tant qu'administrateur d'Office 365.

Si vous devez fournir un environnement d'impression moderne à vos utilisateurs sans avoir à vous soucier des serveurs d'impression ou à installer des pilotes individuels pour les imprimantes sur chaque appareil, envisagez l'option **Universal Print (Impression universelle).**

L'utilisation de la fonction **Search (Rechercher)** est une autre façon de savoir comment les différentes composantes de M365 sont intégrées. Elle vous permet de faire des recherches à divers endroits dans M365 et d'obtenir du contenu pertinent pour vous, et de vous montrer uniquement le contenu auquel vous avez accès, depuis votre locataire.



Apps Admin Center

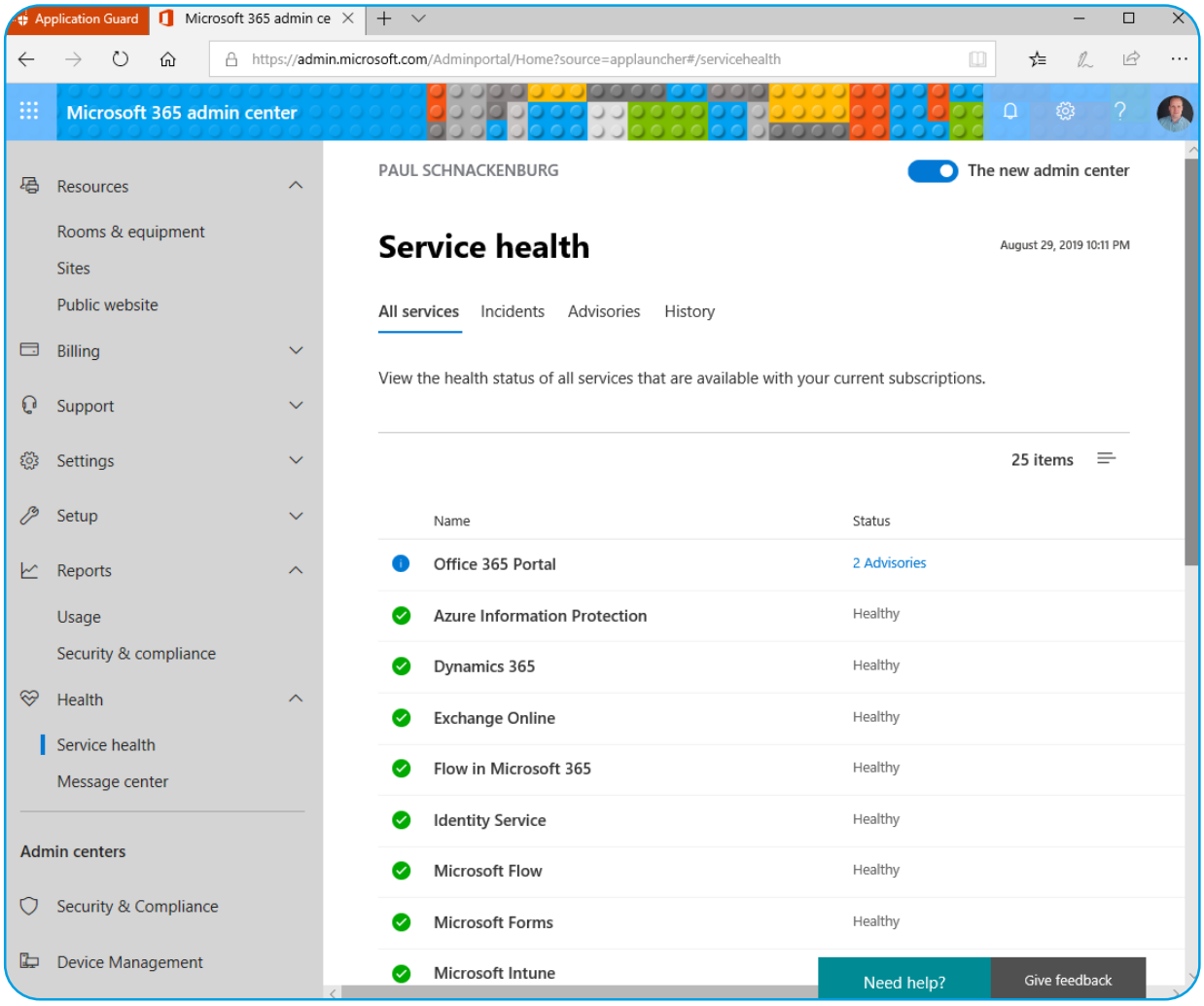
CHAPITRE 6:

WINDOWS 11 ENTERPRISE

LE DERNIER PILIER DE M365 EST WINDOWS 11 ENTERPRISE, CINQ APPAREILS POUR CHAQUE UTILISATEUR SOUS LICENCE QUI METTRA AUTOMATIQUEMENT À NIVEAU WINDOWS 11 PRO VERS ENTERPRISE DÈS QU'UN UTILISATEUR OUVRE UNE SESSION. DANS CE CHAPITRE, NOUS ABORDERONS LES FONCTIONS DE SÉCURITÉ SUPPLÉMENTAIRES QUE CELA APPORTE À VOTRE ENTREPRISE.

6.1: WINDOWS 11 ENTERPRISE

La version Enterprise inclut **Defender Application Guard** et **Defender Application Control** en plus des fonctions de sécurité de Windows 11 Pro. **Application Guard** protège vos utilisateurs lorsqu'ils naviguent sur des sites potentiellement malveillants en utilisant Edge de manière isolée sur le plan matériel. Cette technologie a également **été étendue à Word, Excel et PowerPoint. Application Control,** quant à lui, repose sur des versions antérieures d'AppLocker et empêche les applications non fiables de fonctionner, y compris les modules d'extension (plug-ins) et les modules complémentaires (add-ins).



Navigation dans une fenêtre Application Guard

Always On VPN ne nécessite pas Windows 11 Enterprise et succède à **Direct Access**, si vous avez toujours besoin d'utiliser un réseau privé virtuel (RPV) client dans votre entreprise.

Bien que ce ne soit pas exclusif à Windows 11 Enterprise, consultez **Windows Hello Entreprise** pour améliorer l'expérience d'ouverture de session de votre utilisateur ainsi que votre sécurité (un cas rare où tout le monde gagne en sécurité) en abandonnant les mots de passe.

Si vous déployez un grand nombre d'appareils Windows 11 et que vous voulez réduire le fardeau lié à l'élimination de chaque nouvel appareil et à l'installation de votre image personnalisée, **envisagez d'utiliser Windows Autopilot**, c'est un moyen puissant de « déployer » Windows 11 en transformant simplement l'image déjà installée telle qu'elle est livrée par votre fabricant d'équipement d'origine.

PARTIE 2

GESTION, MAINTIEN ET SOUTIEN DE MICROSOFT 365

Nous examinerons ici des fonctions et des configurations plus avancées de M365, comme Entra, pour sécuriser les identités de vos utilisateurs et de votre charge de travail, gérer Exchange et SharePoint Online, Teams et la façon de configurer de manière centralisée tous vos appareils au moyen d'Intune.

CHAPITRE 7:

ENTRA ID

DERRIÈRE M365 SE TROUVE UN RÉPERTOIRE QUI CONTIENT DES COMPTES D'UTILISATEUR, DES GROUPES ET D'AUTRES OBJETS DE SÉCURITÉ. PENDANT DE NOMBREUSES ANNÉES, CELA A ÉTÉ CONNU SOUS LE NOM D'AZURE ACTIVE DIRECTORY, MÊME S'IL AVAIT TRÈS PEU EN COMMUN AVEC ACTIVE DIRECTORY SUR SITE. AZURE AD A ÉTÉ RENOMMÉE ENTRA ID EN JUILLET 2023. DANS CE CHAPITRE, NOUS EXAMINERONS ENTRA ID ET LA FAÇON DONT VOUS INTERAGISSEZ AVEC LUI POUR M365.

7.1: ENTRA, PRIVA ET PURVIEW

Avant de passer à Entra ID, jetons un coup d'œil au nouveau portail sur lequel vous y accéderez, **entra.microsoft.com**. Tous les services liés à l'identité sont hébergés ici, tandis que toutes les fonctions liées à la gouvernance des renseignements se trouvent sur **compliance.microsoft.com**, appelé le portail Purview (chapitre 14), et il comporte une section contenant toutes les fonctions liées à la protection des renseignements personnels appelés Priva.

Outre Entra ID, le portail Entra héberge également **Entra Permissions Management** (Gestion des autorisations d'Entra) qui permet de faire l'inventaire et de dimensionner correctement les autorisations administratives dans Azure, AWS et GCP (IaaS [Infrastructure en tant que service] et PaaS [Plateforme en tant que service]) – sans lien avec les autorisations de Microsoft 365. Il y a aussi Verified ID (ID vérifiées) qui aidera à l'avenir avec les nouveaux employés et la gestion des identités externes, ainsi que l'accès à Global Secure. Toutefois, elles ne sont pas abordées dans ce livre.

7.2: DÉCOUVRIR ENTRA ID ET HYBRID IDENTITY (IDENTITÉ HYBRIDE)

AD utilise Kerberos et la stratégie de groupe, a une structure hiérarchique et utilise également le Lightweight Directory Access Protocol ou LDAP (Protocole d'accès aux annuaires léger). Il importe toutefois de mentionner qu'aucun de ces éléments n'est compatible avec le nuage. Entra ID fonctionne au moyen de HTTPS, est accessible à partir d'une interface API REST et prend en charge des protocoles d'authentification modernes comme le Security Assertion Markup Language – Langage de balisage des assertions de sécurité (SAML), WS-Federation et OpenID Connect pour l'authentification et OAuth pour l'autorisation. Il prend également en charge la fédération afin que vous puissiez la connecter à d'autres systèmes d'authentification.

Trois types d'authentification sont pris en charge dans Entra ID : **Synchronisation d'annuaires sur le nuage et authentification unique (SSO) avec AD FS (systèmes de fichiers Active Directory)**. Le premier convient lorsque vous n'avez pas d'AD sur site (ou que vous voulez le retirer) et que vous créez des comptes dans le nuage seulement. C'est certainement le plus simple à configurer. Pour les deux autres, vous devez lier votre AD sur site à votre locataire Entra ID au moyen de l'outil gratuit **AAD Connect.**

7.3: AAD CONNECT – VOTRE CORDON OMBILICAL

AAD Connect (qui sera probablement renommé Entra ID Connect) a eu plusieurs prédécesseurs au fil des ans qui portent des noms différents. Si vous trouvez une installation utilisant DirSync ou AAD Sync, assurez-vous de passer à AAD Connect, car ces outils ne sont plus pris en charge. AAD Connect **prend en charge la connexion de plusieurs répertoires sur site à AAD**. Il y avait également la version 1 d'AAD Connect, qui est obsolète. Vous devriez utiliser la version 2, qui se met à jour automatiquement.

Vous pouvez installer l'outil directement sur un contrôleur de domaine ou sur un serveur membre. Il n'y a pas vraiment d'option haute disponibilité réellement active/active, mais vous pouvez configurer une deuxième installation de **AAD Connect** sur un serveur distinct en **mode Staging (mise à disposition)** et effectuer un basculement manuel si le serveur principal est hors ligne temporairement.

AAD Connect synchronisera les comptes d'utilisateur et de groupe dans les unités organisationnelles que vous avez sélectionnées (ou dans tout le répertoire – non recommandé) avec Entra ID. Vous attribuez ensuite des licences à ces comptes d'utilisateur, qui peuvent commencer à utiliser les services infonuagiques. Veuillez noter que cela signifie également que c'est toujours sur le site qu'il faut créer de nouveaux comptes et mettre à jour, désactiver ou supprimer des comptes existants.

Il y a **peu de choix** dans la façon dont vous traitez les mots de passe dans AD. La plus simple est d'utiliser **Password Hash Synchronization** (Synchronisation de hachage de mot de passe) qui prend les hachages de mots de passe sur site, les hache à nouveau avec un algorithme moderne et stocke le hachage du hachage dans le nuage. Cela donne à vos utilisateurs un moyen d'authentification unique (même s'il s'agit techniquement de la même ouverture de session, puisque les deux comptes utilisateur se trouvent dans deux répertoires différents). Un autre avantage de cette méthode est que Microsoft peut vous avertir lorsqu'il trouve des identifiants sur le Web ou le Web invisible avec des comptes de votre locataire où les mots de passe correspondent.

Si vous êtes catégorique sur le fait que les mots de passe de votre utilisateur ne peuvent pas être stockés dans le nuage **(pas même un hachage de hachage)**, la fonction **Pass-through authentication ou PTA (Authentification de passage)** est une autre option. Vous **configurez des agents** sur plusieurs (au minimum 3, au maximum 40) serveurs Windows Server 2012 R2 ou versions ultérieures (aucun port entrant requis) et lorsqu'un utilisateur ouvre une session sur le site **www.office.com** par exemple, Entra ID vérifiera que le bon mot de passe est fourni en communiquant avec votre AD sur site via des agents PTA.

Les fonctions de synchronisation PTA et de synchronisation de hachage de mot de passe vous permettent d'activer en option **Seamless Single Sign On** (Seamless SSO – Authentification unique directe) lorsque l'utilisateur se connecte à AD. Lorsqu'il accède à **www.office.com**, il est automatiquement connecté.

Un compagnon est **AAD Connect Cloud Sync**, qui est configuré à partir du nuage et ne dépend que d'agents légers sur site, ce qui signifie également que vous disposez d'une haute disponibilité intégrée, à condition de déployer plusieurs agents. La synchronisation infonuagique a lentement gagné en fonction **parité** avec AAD Connect, et les principales fonctions manquantes aujourd'hui sont la prise en charge des objets des appareils, la capacité de synchronisation à partir de répertoires LDAP non AD, la prise en charge de PTA, certaines options de filtrage et de grands groupes comptant plus de 250 000 membres. Pour beaucoup, cependant, le bloqueur fera en sorte qu'il n'y aura pas de prise en charge de l'écriture hybride Exchange. Je m'attends à ce que la synchronisation infonuagique remplace éventuellement AAD Connect.

La façon traditionnelle de ne pas stocker les hachages de mot de passe dans le nuage est d'utiliser **AD Federation Services (ADFS)**. Ceci est **beaucoup plus complexe et nécessite la configuration de plusieurs serveurs** sur site (ou sous forme de machines virtuelles dans Azure), mais offre plus de flexibilité. Si votre organisation a déjà déployé AD FS à d'autres fins, l'établissement d'une fédération avec O365 n'est pas un projet énorme, mais ma recommandation (et celle de Microsoft) est de conserver les services PTA ou Password Hash Sync. Compte tenu de la brèche dans la chaîne d'approvisionnement de Solarwinds et de l'intrusion subséquente dans diverses organisations utilisant ADFS, ainsi que de la recommandation de Microsoft au cours des dernières années de migrer d'ADFS à Azure AD, si vous avez déployé ADFS, il est **temps de passer** à Azure AD.

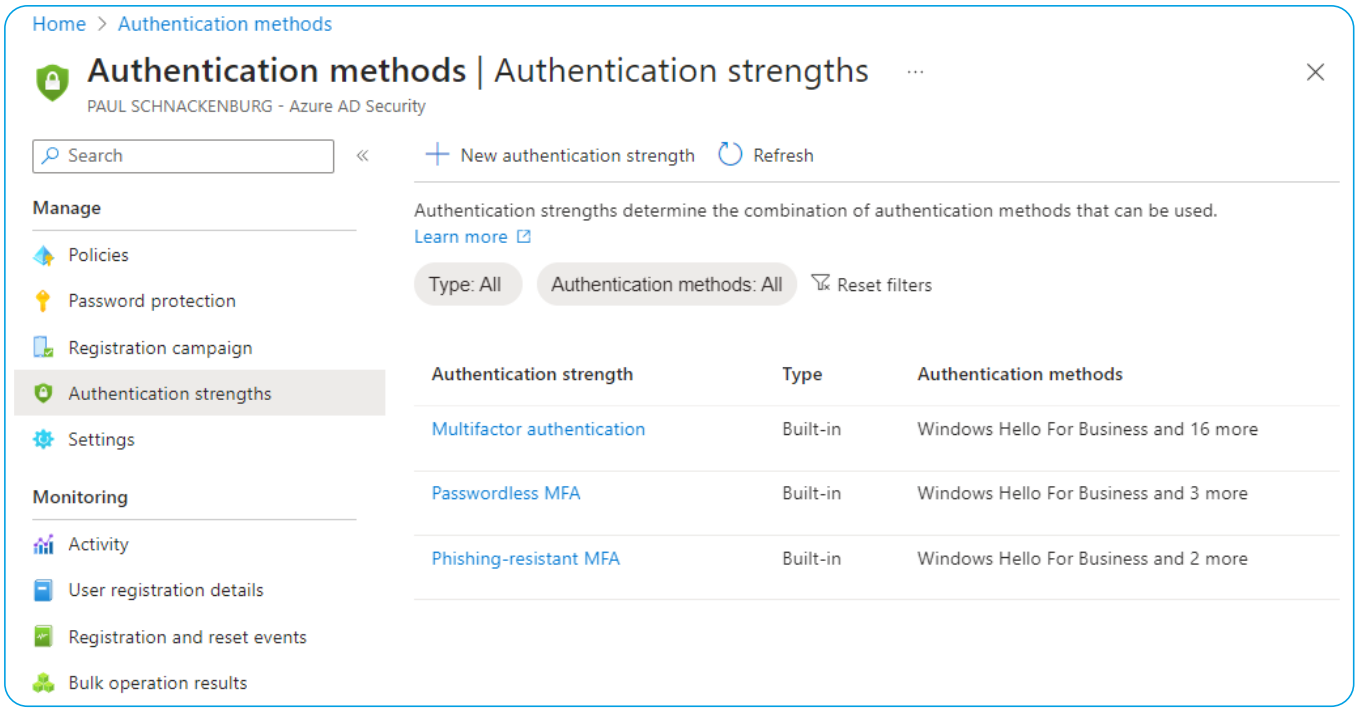
7.4: AUTHENTIFICATION MULTIFACTORIELLE AZURE

L'une des meilleures choses qu'Entra ID vous offre est la configuration facile de l'authentification multifactorielle pour les utilisateurs (MFA). Les mots de passe sont l'un des maillons les plus faibles du paysage informatique d'aujourd'hui, et la majorité des atteintes que nous constatons sont attribuables à la compromission des données d'identification de quelqu'un. Une solution à ce problème consiste à utiliser l'authentification multifactorielle MFA (parfois appelée 2FA ou authentification à deux facteurs), où l'authentification nécessite non seulement un nom d'utilisateur et un mot de passe, mais aussi un appareil ou un geste biométrique. Cela réduit considérablement (de **99 % selon Microsoft**) le nombre d'attaques ciblant les identifiants réussis.

MAF peut appeler votre téléphone, envoyer un message texte avec un code ou envoyer une notification/exiger un code à partir de l'application gratuite **Microsoft Authenticator**. À moins d'une exigence absolue, n'utilisez pas les fonctions d'appel téléphonique ou de message texte, ils sont moins sécurisés que les options de l'application.

Comme base de référence, tous vos comptes privilégiés (Global, Exchange, SharePoint et administrateurs de la conformité, etc.) DOIVENT utiliser l'authentification multifactorielle. **Ce service est gratuit à tous les niveaux d'Office 365** et est **facile à configurer.** L'expérience utilisateur est relativement fluide si vous installez l'application sur votre téléphone intelligent. Si vous êtes un décideur des TI, vous pouvez vous attendre à recevoir de la résistance de la part de vos administrateurs sur ce point, mais pour maintenir une posture de sécurité acceptable, cette étape n'est pas négociable – tous les administrateurs DOIVENT utiliser l'authentification multifactorielle. Soit dit en passant, j'utilise l'authentification multifactorielle Azure pour mon propre locataire d'entreprise et pour tous les locataires de mon client que j'administre depuis de nombreuses années, sans problème.

Vous devez toutefois prévoir les moments **où l'authentification multifactorielle Azure n'est pas disponible**, ce qui comprend la création d'un (de préférence deux) comptes infonuagiques Global Admin qui sont exemptés de l'authentification multifactorielle et de toute stratégie d'AC. Ces comptes devraient avoir des mots de passe très longs et complexes qui ne sont accessibles qu'aux administrateurs de haut niveau et la surveillance devrait être activée afin de déclencher des alertes en cas d'utilisation non autorisée.



Ponts forts de l'authentification multifactorielle

Ces comptes de secours et d'accès d'urgence ne doivent être utilisés que pour récupérer l'accès des utilisateurs. Par exemple, si l'authentification multifactorielle Entra ID ne fonctionne, vous pourriez désactiver les exigences relatives à l'authentification multifactorielle pendant la durée du dysfonctionnement afin de permettre aux utilisateurs d'ouvrir une session et d'être productifs.

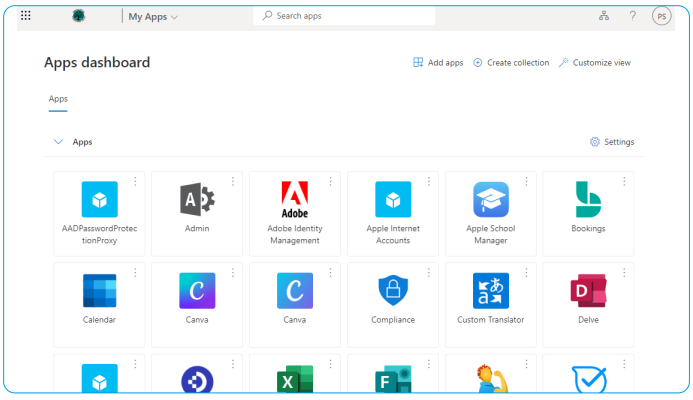
L'activation de l'authentification multifactorielle pour vos utilisateurs finaux nécessite une certaine planification et une formation pour les utilisateurs finaux. Le niveau de connaissance de la technologie de vos utilisateurs et le fait qu'ils travaillent normalement dans les bureaux de l'entreprise ont une incidence sur le mode de déploiement du service d'authentification multifactorielle. Les administrateurs obtiennent toujours l'authentification multifactorielle gratuitement, si vous utilisez des UGS Business, la MFA est intégrée, mais les deux ne disposent pas des fonctionnalités avancées offertes par Entra ID Premium P1 (M365 E3) ou Entra ID Premium P2 (M365 E5). Ces options comprennent le contournement ponctuel, les adresses IP de confiance/**les emplacements nommés**; ce qui vous permet de définir les plages d'adresses IP des bureaux de l'entreprise où les utilisateurs ne seront pas invités à utiliser l'authentification multifactorielle. Veuillez noter que tous les niveaux d'authentification multifactorielle vous permettent (si vous activez cette fonction) de vous souvenir de l'authentification multifactorielle sur un appareil fiable pendant un certain nombre de jours (de 7 à 60 jours). Si un utilisateur a ouvert une session sur un appareil et qu'il a réussi l'authentification multifactorielle, il ne sera pas invité à utiliser cet appareil pendant la période visée, et si l'appareil est perdu ou volé, l'utilisateur ou vous pouvez facilement déclarer l'appareil « comme un appareil qui n'est plus fiable ». À compter de mai 2023, Microsoft activera le numéro correspondant pour toutes les approbations de Microsoft Authenticator. Au lieu d'appuyer simplement sur Approve (Approuver) ou Reject (Rejeter), vous devez entrer un code à deux chiffres affiché sur l'écran de votre ordinateur. L'application vous indiquera également l'emplacement géographique d'où provient la demande d'authentification multifactorielle. Les deux fonctions sont conçues pour lutter contre les attaques de fatigue de l'authentification multifactorielle, où l'attaquant tente à plusieurs reprises d'ouvrir une session, ce qui génère tellement de demandes sur votre téléphone qu'au bout du compte, certains utilisateurs finissent par appuyer sur Approve (Approuver) pour arrêter ces demandes.

Microsoft active désormais la fonction **Security Defaults (Paramètres de sécurité par défaut)** pour tous les nouveaux locataires, et vous **pouvez l'activer manuellement** pour vos locataires existants. Cela permet d'appliquer l'authentification multifactorielle à tous les utilisateurs et administrateurs, en utilisant uniquement l'application Microsoft

Authenticator, bloquera l'authentification traditionnelle (voir le chapitre 15) et contrôlera l'accès au portail Azure AD. Bien que ces mesures de sécurité soient un bon point de départ pour une petite entreprise ayant des exigences limitées, je conseille la prudence aux organisations plus complexes, car il n'y a aucune façon d'exclure les comptes de secours ou les comptes de service de l'authentification multifactorielle ou des façons de traiter les utilisateurs qui n'ont pas ou ne peuvent pas accéder à l'application d'authentification sur un téléphone.

7.5: PUBLICATION DES APPLICATIONS

L'une des fonctions les plus puissantes d'Entra ID est la capacité de **publier des applications** (tierces parties et **sur site**) pour vos utilisateurs finaux. Elles s'affichent juste à côté des applications Office normales sur **myapplications.microsoft.com** ou **www.office.com** pour que les utilisateurs puissent les lancer en un seul clic.



Portail MyApps (Mes applications)

Prenez un compte Twitter d'entreprise, par exemple, où plusieurs utilisateurs ont le nom d'utilisateur et le mot de passe pour envoyer des tweetsau nom de l'entreprise. Non seulement vous devrez réinitialiser le mot de passe dès que quelqu'un quitte l'entreprise (vous ne voulez pas qu'il envoie un tweet au nom de votre organisation après qu'il eut été congédié), mais vous avez peu de contrôle sur les autres personnes avec qui ce mot de passe a été partagé. Si vous faites des publications sur Twitter au moyen d'Entra ID et que vous créez un groupe AD auquel les utilisateurs devraient avoir accès, vous n'avez qu'à ajouter un compte d'utilisateur à ce groupe, qui aura automatiquement la fonction d'accès par authentification unique sur Twitter dans le portail My Apps sans jamais connaître le mot de passe et, une fois qu'ils quittent l'entreprise et que leur compte est désactivé, ils ne peuvent plus y accéder. Pour certaines applications parmi les 2400 et plus prises en charge à partir de la boîte, vous pouvez même configurer une fonction de **configuration automatique** de sorte que lorsque vous ajoutez un utilisateur au groupe AD Salesforce, un compte est automatiquement créé pour lui dans Salesforce – encore une fois, sans même qu'il connaisse le mot de passe.

Une option populaire consiste à utiliser l'application d'ouverture de session unique d'AWS **pour intégrer AAD et AWS.**

7.6: FONCTIONS DE PREMIÈRE QUALITÉ

Entra ID Premium P1 ne fait pas que déverrouiller d'autres fonctions d'authentification multifactorielle, il vous permet également **d'interdire les mots de passe couramment utilisés** dans votre AD sur site (y compris **une liste de mots personnalisée**), de permettre aux utilisateurs de **réinitialiser leurs propres mots de passe** en cas d'oubli, d'intégrer **l'authentification multifactorielle avec accès conditionnel** et de permettre aux utilisateurs de s'inscrire à la fois à l'authentification multifactorielle et à la réinitialisation du mot de passe en libre-service (SSPR) dans **la même expérience**.

Le niveau P2 ajoute l'expérience complète de la protection de l'identité dans Entra, où vous obtenez **des rapports et pouvez bloquer des authentifications** en fonction du niveau de risque du compte de l'utilisateur et de l'ouverture de session, voire générer une invitation à l'authentification multifactorielle **supplémentaire** en fonction du profil de risque de la tentative d'authentification. P2 offre également une fonction **Privileged Identity Management ou PIM – Gestion des identités privilégiées (GPP)** qui vous permet de convertir tous les comptes administratifs en comptes admissibles et où les utilisateurs doivent demander des privilèges plus élevés lorsqu'ils doivent effectuer des tâches administratives (connues sous le nom de « Just in Time administration » [Administration en temps voulu]).

Au lieu d'attribuer des rôles d'administrateur dans Entra ID à des comptes d'utilisateur individuels, vous pouvez **maintenant utiliser des groupes pour accorder l'accès administrateur.** Les groupes doivent avoir un attribut spécifique défini (isAssignableToRole) sur true et une appartenance à un compte utilisateur statique (plutôt que dynamique – attribuer automatiquement des comptes d'utilisateur à un groupe en fonction d'un attribut comme « service » dans le répertoire).

Lorsqu'AD a une structure hiérarchique, s'appuyant sur les unités organisationnelles (UO) pour structurer vos comptes d'utilisateur, de machine et de groupe en fonction du service, de la géographie ou d'une autre approche, Entra ID a une structure plate. L'option **Administrative Units (AUs) – Unités administratives (UA)** permet de modifier cette fonction. Vous pouvez utiliser des UA pour structurer des comptes d'utilisateur et de groupe, puis **déléguer des autorisations administratives** à une ou plusieurs UA. Les administrateurs des UA ont besoin d'une licence Entra ID Premium. Veuillez noter que, contrairement aux UO où un compte ne peut se trouver que dans une seule UO, un compte de groupe ou d'utilisateur peut être membre de plusieurs UA (jusqu'à 30).

Si vous avez un grand environnement et des licences Premium P2, envisagez d'utiliser la **gestion des droits,** un moyen de regrouper l'application, l'appartenance au groupe (y compris Teams) et l'accès au site dans un progiciel d'accès unique. Cette solution est utile pour les utilisateurs internes (« Vous êtes la nouvelle personne du service Marketing – voici votre progiciel qui vous donne tous les accès dont vous avez besoin ») et peut également être utilisée pour accorder l'accès aux utilisateurs externes. Pour les organisations partenaires avec lesquelles vous travaillez fréquemment, vous pouvez même la configurer de façon à ce que leurs utilisateurs puissent présenter une demande de progiciels en libre-service. La gestion des droits peut également permettre aux TI de se libérer du rôle d'attribution des autorisations en déléguant les fonctions d'attribution de progiciels aux utilisateurs fonctionnels.

7.7: STRATÉGIES D'ACCÈS CONDITIONNEL

P1 et P2 déverrouillent une autre fonction puissante dans Entra ID, l'**Accès conditionnel (AC)**. Cela vous permet d'élaborer des stratégies d'accès aux applications (les applications infonuagiques et les applications sur site) en fonction du compte de l'utilisateur et des groupes dont il est membre, de l'application à laquelle il accède, de l'état de son appareil, de son emplacement, du risque de connexion et du type d'application client à laquelle il accède. Ces règles « si ceci, alors faites cela » améliorent grandement la sécurité de vos données en gérant les facteurs de risque qui ont une incidence sur les identités et les accès dans M365.

Les **modèles** (en prévisualisation au moment de la rédaction) qui couvrent la fondation sécurisée, la confiance zéro (Zero Trust), le travail à distance, la protection des administrateurs et les menaces émergentes facilitent davantage l'établissement de bonnes stratégies d'AC.

Pour vous assurer de ne pas créer par erreur une stratégie de verrouillage du compte du PDG cinq minutes avant la présentation au conseil d'administration, l'option de déployer les stratégies d'AC en **mode rapport seulement** vous permet d'évaluer l'incidence des stratégies sans les appliquer réellement.

Il existe une **API pour accéder aux stratégies d'AC.** Cela permet de sauvegarder (en utilisant PowerShell, par exemple) vos stratégies d'AC, de les restaurer, de surveiller les changements et de les traiter comme des codes plutôt que de les gérer manuellement dans le portail. Vous pourriez également mettre à l'essai les stratégies d'un locataire test avant de les exporter et de les importer dans votre locataire de production après la validation.

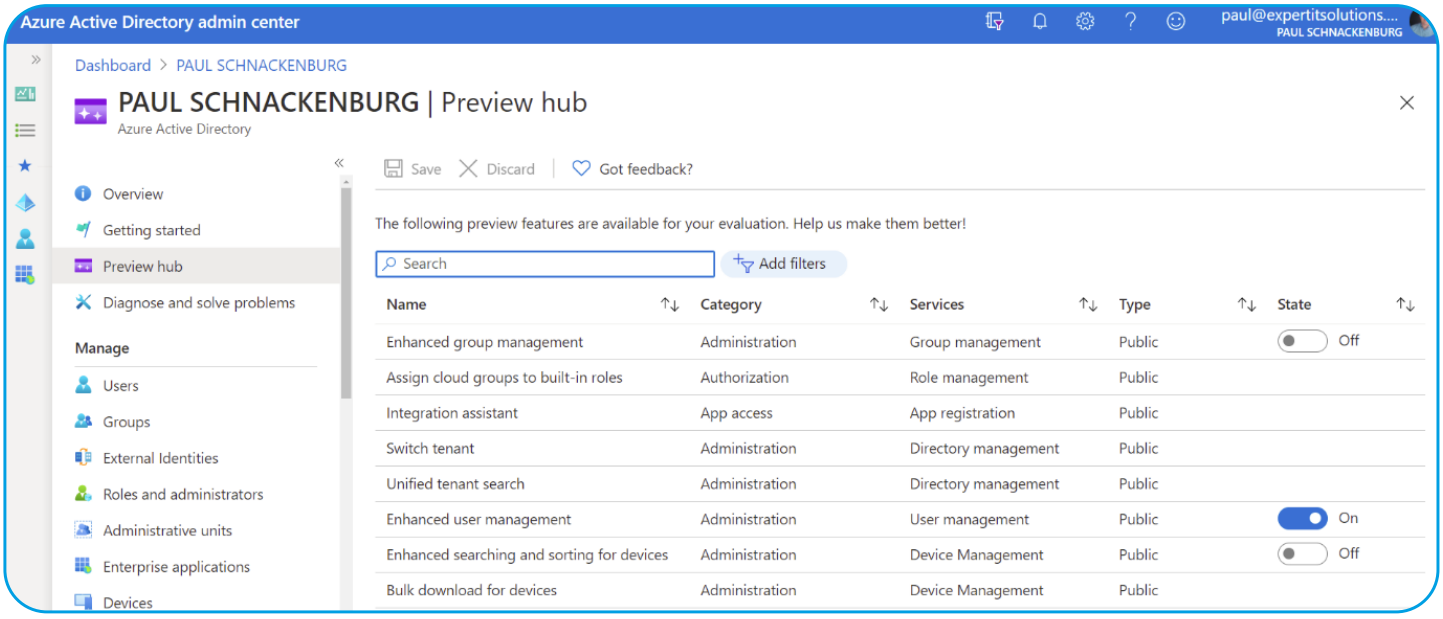
7.8: GESTION DU CYCLE DE VIE DU COMPTE

Une fois que vous avez mis en œuvre AAD Connect, assurez-vous de mettre à jour votre documentation de processus afin de tenir compte du cycle de vie complet des comptes d'utilisateurs, par exemple en vous assurant qu'ils reçoivent les bonnes licences, qu'ils sont ajoutés aux bons groupes et que lorsque vient le temps de désactiver le compte, les **bonnes étapes** sont suivies.

Pour vous assurer que les utilisateurs (et les invités) n'accumulent pas d'accès dont ils n'ont plus besoin, **utilisez la fonction Access Reviews (Examens d'accès)** (Premium P2), qui vous permet maintenant **de passer en revue tous les comptes d'invités dans une seule opération,** plutôt que par équipe/groupe M365.

Pour un plus petit nombre de locataires d'Office 365 ou de M365, vous n'aurez jamais besoin d'accéder au portail AD Azure complet; vous n'aurez qu'à gérer les utilisateurs dans le portail M365 (chapitre 2). C'est toutefois une bonne idée d'explorer le portail « complet » d'Entra sur **https://entra.microsoft.com.**

Si vous souhaitez essayer les fonctions à venir dans Entra ID, utilisez le hub « Preview » (Prévisualisation) pour en savoir plus et activer les fonctions de prévisualisation publique.



Hub Preview d'Azure AD

CHAPITRE 8:

EXCHANGE EN LIGNE

LE COURRIER ÉLECTRONIQUE EST LE SOCLE DE LA COMMUNICATION D'ENTREPRISE, ET CE, MÊME À L'ÈRE DE TEAMS ET DE SLACK ET DE NOMBREUX AUTRES OUTILS DE COMMUNICATION. C'EST LE PLUS PETIT DÉNOMINATEUR COMMUN – L'OUTIL QUE VOUS POUVEZ TOUJOURS UTILISER POUR JOINDRE QUELQU'UN SI VOUS AVEZ SON ADRESSE COURRIEL. LE COURRIER ÉLECTRONIQUE EST UN PRODUIT DE BASE : TOUTES LES ENTREPRISES EN ONT BESOIN, MAIS AUCUNE ENTREPRISE NE SERA PLUS CONCURRENTIELLE EN LE GÉRANT « PLUS EFFICACEMENT » QU'UNE AUTRE.

8.1: C'EST UN MONDE HYBRIDE

L'un des ponts forts de M365 par rapport à Google Workplace, par exemple, est la voie claire de la migration de ce que vous avez aujourd'hui vers le nuage, en raison de la grande présence de Microsoft dans les centres de données d'entreprise partout dans le monde.

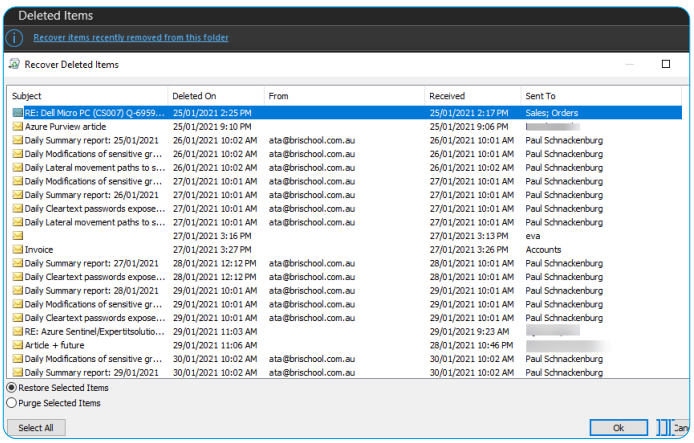
Si vous avez Exchange 2013 et des versions ultérieures sur site, vous pouvez choisir n'importe laquelle des méthodes de migration que nous avons examinées au chapitre 3, dont certaines offrent une coexistence hybride. L'option hybride complète vous permet de continuer à exploiter votre infrastructure sur site aussi longtemps que vous le souhaitez et de déplacer les boîtes aux lettres en lots dans le nuage selon votre propre calendrier. Vous pouvez même déplacer les boîtes aux lettres sur site si le besoin s'en fait sentir. Comme vous vous y attendez, il y a de nombreux détails à gérer dans une **configuration hybride**, y compris les **conditions préalables**, la **connectivité ActiveSync** et les **autorisations de boîte aux lettres** – en particulier lorsqu'un utilisateur sur site a des permissions pour une boîte aux lettres dans le nuage ou vice versa.

Si tout ce que vous cherchez, c'est un moyen simple de faire passer les boîtes aux lettres d'Exchange à Exchange Online – Hornetsecurity offre un excellent **outil de migration des boîtes aux lettres.**

8.2: SAUVEGARDE ET PROTECTION DES DONNÉES NATIVES

Une chose à comprendre au sujet d'Office 365, c'est que Microsoft veillera à ce que vous ne perdiez pas les données de votre boîte aux lettres, grâce à la protection des données natives dans Exchange – en conservant trois copies des données de votre boîte aux lettres sur des serveurs distincts, ainsi qu'une « copie différée » (décalée, pour les cas où les données sont corrompues plutôt que perdues) sur un quatrième serveur.

Toutefois, ils NE conservent PAS de copies de sauvegarde de vos données qui remontent dans le passé, ce qui pourrait poser un problème pour votre entreprise, selon vos besoins réglementaires. Il existe plusieurs services tiers sur le marché qui effectueront des sauvegardes de vos données Exchange et SharePoint Online. Hornetsecurity **365 Total Backup** est une excellente solution de sauvegarde, pour les boîtes aux lettres, Teams, OneDrive pour les entreprises, SharePoint et les fichiers des points de terminaison, voir le **chapitre 16.**



Récupérer les éléments supprimés dans Outlook

Un compte utilisateur et une boîte aux lettres supprimés **peuvent être récupérés** si un délai de plus de trente (30) jours n'est pas encore écoulé.

8.3: AUTODISCOVER

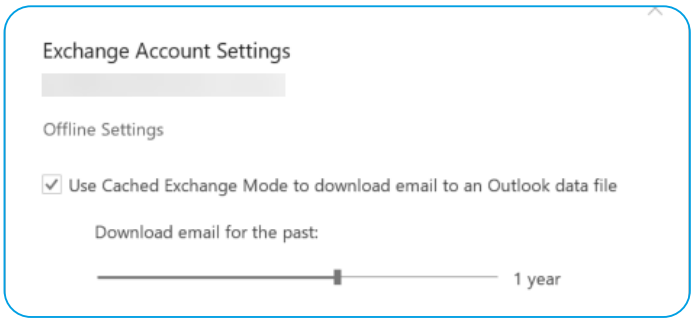
Que votre serveur Exchange soit dans le nuage ou sur votre site, il est important que les applications client puissent le trouver – c'est la tâche des enregistrements d'Autodiscover dans DNS. Plusieurs autres enregistrements DNS sont requis pour M365 – vous les trouverez dans **cet article**.

Si vous avez un déploiement hybride d'Exchange, les enregistrements d'Autodiscover doivent indiquer votre serveur de boîte aux lettres Exchange 2016-2019 sur site.

8.4: GESTION DES BOÎTES AUX LETTRES

De nombreuses tâches sont associées à la gestion de la boîte aux lettres, dont la **gestion des quotas**. Les licences F3 offrent des quotas de 2 Go, les licences E1 sont définies à 50 Go (avec des archives de 50 Go) et E3+ ont des quotas de 100 Go avec des boîtes aux lettres d'archivage pouvant atteindre un maximum de 1,5 To. La différence entre une boîte aux lettres et une boîte aux lettres d'archives, c'est que les archives ne sont disponibles que lorsque vous êtes en ligne. Vous pouvez contrôler la quantité de données de boîte aux lettres stockées hors ligne sur chaque appareil à l'aide d'un curseur dans Outlook.

Si vous migrez de grandes boîtes aux lettres vers Office 365, assurez-vous que leur taille soit inférieure à 100 Go et qu'aucun élément ne dépasse 150 Mo avant de commencer la migration.



Paramètre du cache hors ligne d'Outlook

Dans la console Exchange, vous pouvez configurer les paramètres d'une boîte aux lettres, comme l'ajout d'alias de courriel, voir l'utilisation de quota, contrôler les clients (OWA, messagerie unifiée) et les protocoles (EAS, MAPI, IMAP et POP) que l'utilisateur peut utiliser ainsi que la conservation des messages et la délégation des boîtes aux lettres. Cette dernière option vous permet de configurer d'autres utilisateurs pour utiliser les options **Send As (Envoyer en tant que)** en tant qu'utilisateur, **Send on Behalf (Envoyer de la part)** où le destinataire peut voir que le courriel est envoyé au nom de l'utilisateur et **Full Access (Accès sans restriction).**

8.5: ARCHIVES DES BOÎTES AUX LETTRES

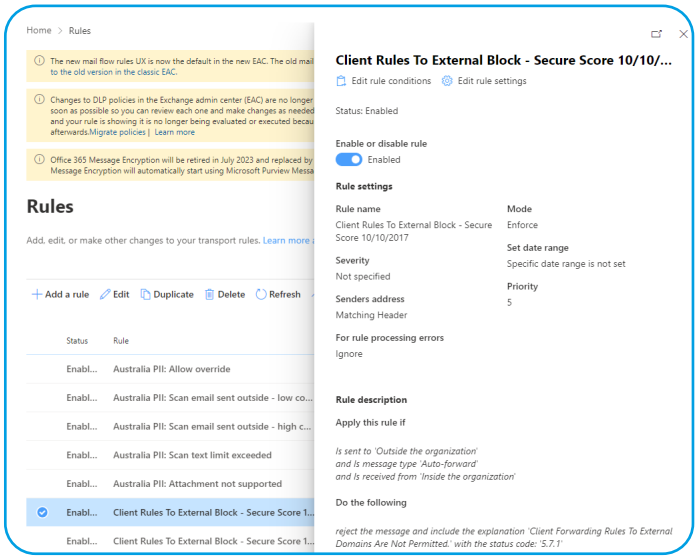
Comme nous l'avons mentionné plus tôt, vous pouvez activer une boîte aux lettres d'archives pour le contenu de la boîte aux lettres qui sert essentiellement de zone de stockage « sans fond » pour le contenu plus ancien, ce qui, nous l'espérons, empêchera les utilisateurs d'adopter les fichiers PST comme solution d'archivage. Le client mobile Outlook (iOS et Android) ne peut pas accéder aux boîtes aux lettres des archives. Vous pouvez activer l'**extension automatique des archives pour les utilisateurs sous licence E3 et E5** en utilisant PowerShell :

```
Set-OrganizationConfig -AutoExpandingArchive
```

Vous pouvez également activer les boîtes aux lettres Archives par utilisateur. Veuillez noter que le dossier Archives créé dans une boîte aux lettres lorsque vous cliquez avec le bouton droit de la souris sur un élément et sélectionnez Archive n'est pas lié à la boîte aux lettres Archives.

8.6: REDIRECTION DU COURRIER

Sachez que les utilisateurs peuvent configurer leurs boîtes aux lettres pour rediriger le courrier à une adresse courriel externe (livraison facultative aux deux boîtes de réception). C'est une pratique que vous devriez surveiller de près, car même s'il peut y avoir des raisons commerciales légitimes de rediriger le courrier, il s'agit également d'un vecteur d'attaque de prédilection des pirates informatiques, qui peuvent lire les courriels en catimini, puis les utiliser à diverses fins malveillantes. Il y a un rapport dans le tableau de bord du Flux de messagerie pour vous montrer les règles de redirection en place. Vous pouvez également empêcher **les utilisateurs de rediriger le courrier** de plusieurs façons.



Règle du Flux de messagerie pour bloquer la redirection des courriels externes

8.7: BOÎTES AUX LETTRES PARTAGÉES

Il y a des moments où vous aimeriez une boîte aux lettres qui n'appartient pas à un utilisateur en particulier, comme ventes@ ou soutien@, où une équipe d'utilisateurs accède au même pseudonyme. Tant que la **boîte aux lettres partagée** n'a pas un quota supérieur à 50 Go ou qu'elle utilise une boîte aux lettres Archives, elle ne consommera pas de licence. Il s'agit également d'une option pour gérer les employés qui ont quitté votre entreprise alors que vous devez toujours surveiller leurs courriels en ce qui concerne les messages entrants, convertir leur boîte aux lettres en une boîte aux lettres partagée et attribuer l'accès au personnel compétent libérera la licence à attribuer à un nouvel utilisateur. Du point de vue de la sécurité, assurez-vous que la connexion directe aux boîtes aux lettres partagées est bloquée – les utilisateurs ne doivent accéder qu'aux boîtes aux lettres partagées en les ajoutant comme boîtes supplémentaires dans Outlook.

8.8: PERSONNES-RESSOURCES ET UTILISATEURS DE COURRIER

Les **contacts** et les **utilisateurs** du courrier s'affichent dans Tous les contacts, la liste d'adresses globale (GAL) et le carnet d'adresses hors ligne (OAB). Un **contact** renvoie vers une adresse courriel dans un système externe, tandis qu'un **utilisateur** renvoie également vers une adresse externe, mais l'utilisateur a des identifiants O365 pour accéder à SharePoint Online ou à OneDrive Entreprise. Ce dernier est un vestige d'Exchange sur site, le partage externe moderne comme Teams, Planner et autres utilise l'outil de collaboration A**zure Business to Business (B2B)** pour l'accès des invités.

8.9: LISTES DE DISTRIBUTION (LD)

Le regroupement des adresses courriel pour faciliter la communication avec les équipes est une chose que les systèmes de courriel font depuis des décennies – vous pouvez créer des listes de distribution (LD) dans le Centre d'administration en ligne d'Exchange. Veuillez noter que l'option par défaut consiste à créer un **groupe M365** et que **Microsoft pousse à remplacer les LD par des groupes.** Les **groupes dynamiques** facilitent le maintien de l'appartenance, en basant l'appartenance sur un attribut Entra ID tel que « service » – s'il est défini sur Marketing par exemple, l'utilisateur est automatiquement inclus dans le bon groupe.

CHAPITRE 9:

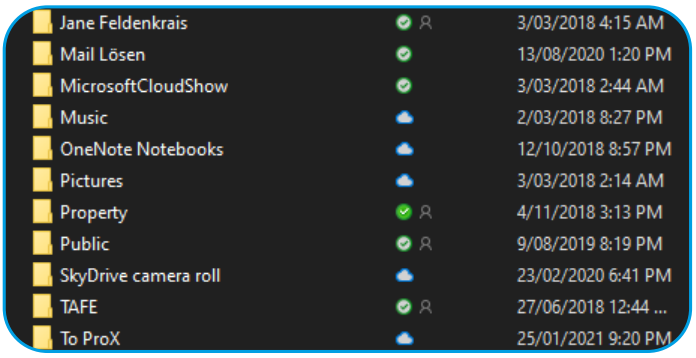
ONEDRIVE ENTREPRISE ET SHAREPOINT

LE PARTAGE DE FICHIERS ET LA FOURNITURE D'UNE PLATEFORME INTRANET FONT PARTIE INTÉGRANTE DE M365. DANS CE CHAPITRE, NOUS EXAMINONS ONEDRIVE ENTREPRISE (OD4B) POUR LE STOCKAGE ET LE PARTAGE DE FICHIERS PERSONNELS, AINSI QUE LA COLLABORATION WEB DANS SHAREPOINT.

9.1: ONEDRIVE ENTREPRISE

OD4B s'appuie sur SharePoint Online pour fournir à chaque utilisateur sous licence son propre stockage de documents; 1 To pour la plupart des UGS. Ce quota **peut être augmenté** à 5 To pour certaines licences.

Comme nous l'avons mentionné, une fois que vous stockez des fichiers dans OD4B, vous pouvez y accéder à partir de n'importe quel appareil, par l'entremise des clients pour Android, iOS, Windows, MacOS et d'une interface Web. Il existe des **restrictions** en ce qui concerne les noms, les types et les tailles des fichiers à connaître. Le client de synchronisation OD4B vous permet **de voir tous les fichiers** sur un appareil que vous avez synchronisé. Ils peuvent être à l'état **Online-only (En ligne seulement)** où vous pouvez les voir, mais ils ne sont pas réellement présents sur l'appareil. Lorsque vous ouvrez ce type de fichiers, ils sont téléchargés et mis en cache et donc **disponibles localement.** Un utilisateur peut également choisir un ou plusieurs fichiers à **conserver sur cet appareil.**



Fichiers locaux uniquement sur le nuage et épinglés dans OD4B

Vous pouvez limiter la synchronisation aux **dispositifs connectés au domaine**. Pour aider les utilisateurs à gérer le contenu des dossiers communs, vous pouvez utiliser **Known Folder Move (KFM) – Déplacement de dossiers connus** pour synchroniser le contenu des dossiers Desktop (Bureau), Documents et Pictures (Images) avec OD4B et donc entre les appareils.

9.2: SHAREPOINT

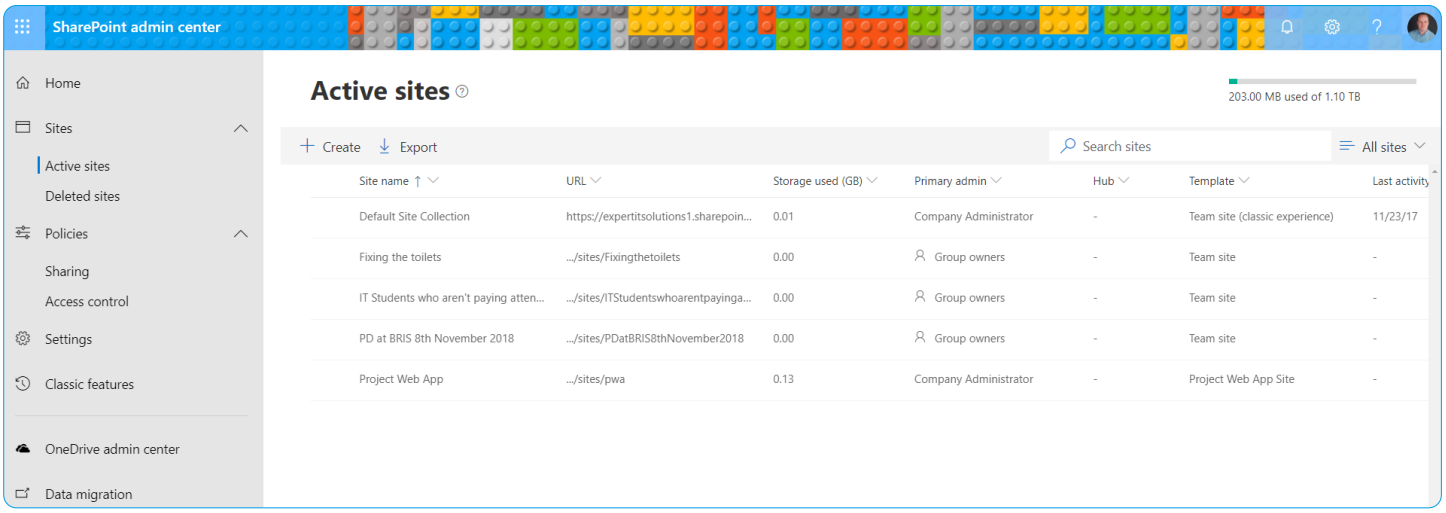
Si vous êtes un administrateur SharePoint sur site, vous connaissez bien la gestion de l'infrastructure sous-jacente de vos serveurs, ainsi que du Web complexe des sites et des flux de travail de documents que les utilisateurs finaux utilisent en plus. Si ce n'est que maintenant que vous découvrez SharePoint dans le nuage pour la première fois, vous vivrez probablement une expérience très différente où vous verrez SharePoint simplement comme le stockage de documents sous-jacent pour d'autres applications (Teams, Groups, Planner) et peut-être comme la plateforme de l'intranet de votre entreprise.

Les composantes de base de SharePoint sont des sites où le contenu est stocké, et vous pouvez contrôler la mise en page, le thème, la navigation et la sécurité avec des versions classiques et modernes. Si vous démarrez ou créez de nouveaux sites, les sites modernes sont **la solution** et il existe plusieurs types de sites disponibles, tels que les **sites de communication**, les **sites d'équipe** et les **sites Hub**. Dans le cadre d'une vision plus vaste pour SharePoint, les sites et les pages modernes sont très utiles, car ils s'adaptent aux résolutions d'écran des téléphones intelligents et des écrans d'ordinateur de différentes tailles.

La fonction de **Recherche** vous permet de trouver des sites, des fichiers (y compris des fichiers OneDrive Entreprise), des personnes et du contenu de nouvelles. S'il y a des images dans le contenu, l'intelligence artificielle (IA) aura extrait des métadonnées et (le cas échéant) du contenu textuel de ces images. Si vous avez configuré un **déploiement hybride**, vos documents sur site apparaîtront également dans les résultats de recherche. Les **applications** sont des modules complémentaires/Web qui élargissent la fonctionnalité des sites et les **collections de sites** sont un moyen de regrouper des sites ayant le même objectif.

Pour configurer différents sites, utilisez les **modèles de site** pour commencer. Si vous créez un site intranet, il y a un excellent **service Lookbook** qui offre de magnifiques sites et des expériences modernes.

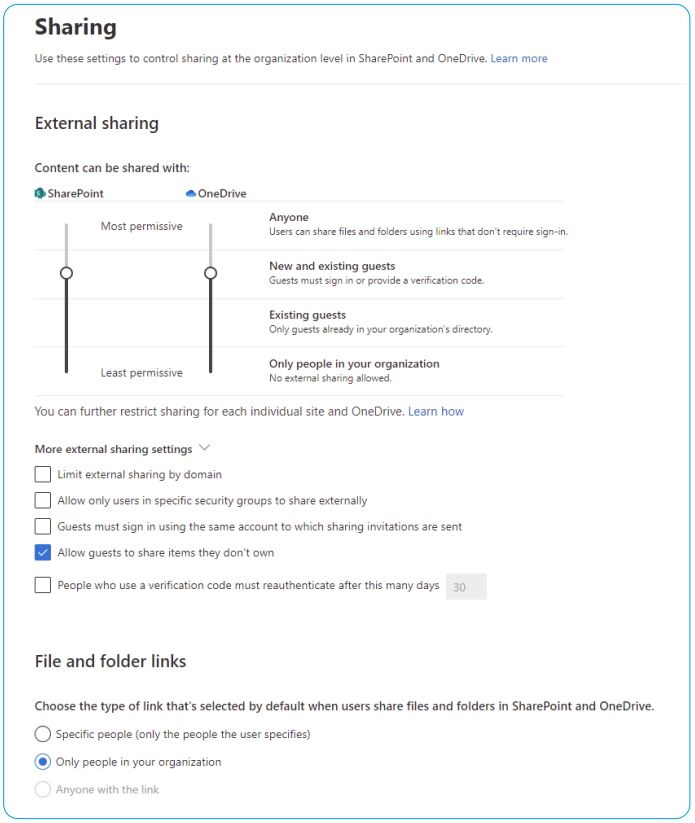
SharePoint Syntex est une technologie qui utilise l'intelligence artificielle et l'apprentissage machine pour automatiser le traitement du contenu et le transformer en connaissances. Il comprend vos documents, traite vos formulaires et s'applique aux grandes organisations ayant des flux de travail et des processus complexes.



Centre d'administration SharePoint Online

Soyez conscient des **limites de SharePoint Online,** notamment du stockage total disponible qui est de 1 To + 10 Go par licence achetée. Search (Recherche) est une section que vous voulez **personnaliser** afin que vos utilisateurs finaux bénéficient d'une bonne expérience. Sharing (Partage) est une autre section que vous voulez contrôler puisque **la façon dont les utilisateurs peuvent partager du contenu** à l'interne et (surtout) à l'externe influence directement l'équilibre entre la collaboration et la sécurité.

La migration du contenu du serveur SharePoint sur site et des partages de fichiers réseau vers M365 est la tâche de **SharePoint Migration Tool**, ainsi que de nombreux services tiers. Si des utilisateurs suppriment accidentellement des fichiers ou si un rançongiciel a crypté des fichiers chiffrés, vous pouvez utiliser l'interface **Restore Files (Restaurer les fichiers)** pour restaurer des fichiers et des dossiers ou des bibliothèques entières datant de jusqu'à trente (30) jours. Il y a aussi la **Corbeille** (93 jours de conservation) pour les restaurations de fichiers individuels et la fonction **Restore Files (Restaurer les fichiers)** pour OneDrive.



Contrôle de partage externe SharePoint et OD4B

CHAPTER 10:

GROUPES MICROSOFT 365

LES GROUPES M365 SONT UNE COMPOSANTE DE BASE DE DIFFÉRENTS SERVICES. DANS CE CHAPITRE, NOUS EXAMINERONS LES DIVERSES UTILISATIONS QUI EN SONT FAITES.

10.1: TYPES DE GROUPES

Une section qui est souvent une source de confusion pour les nouveaux administrateurs d'Office 365 est celle des **différents types de groupes**. Voici un petit récapitulatif pour y voir plus clair :

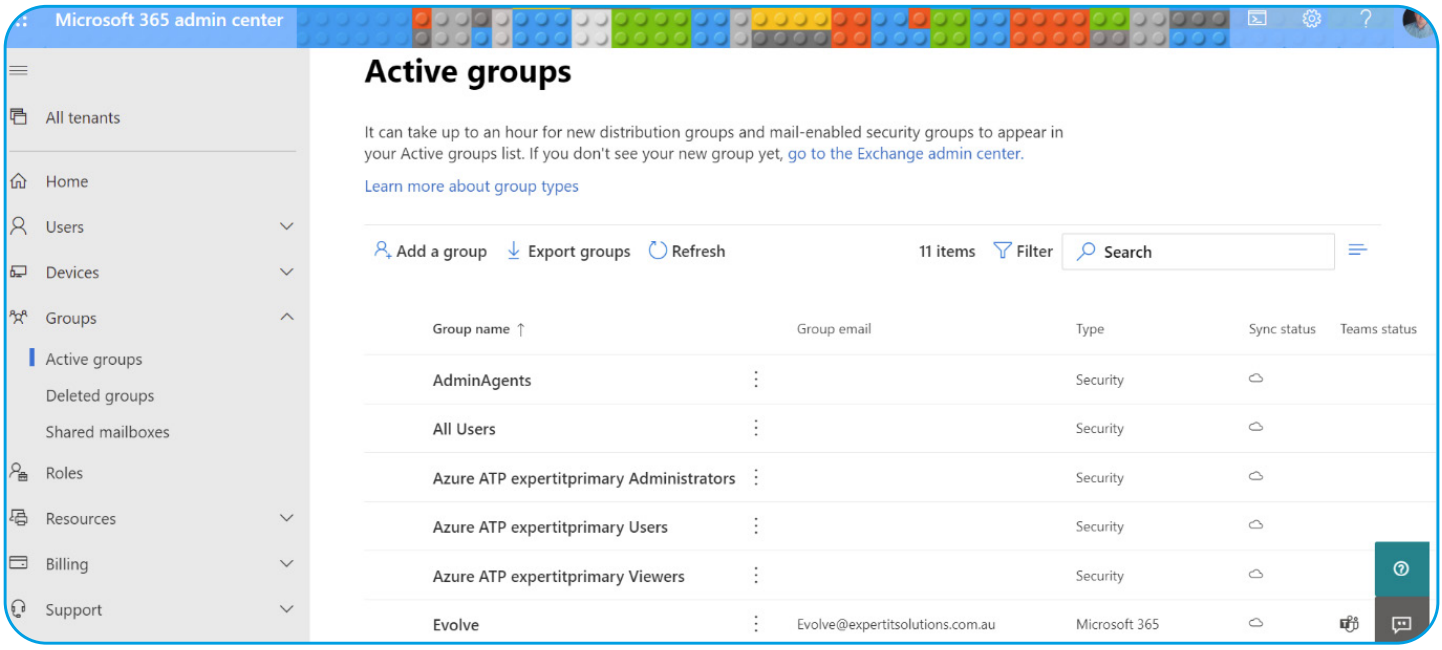
- **Groupes Microsoft 365** (le type couvert dans ce chapitre)
- **Groupes de distribution** (chapitre 8)
- **Les groupes de sécurité** sont utilisés pour accorder l'accès aux ressources
- **Les groupes de sécurité pour le courrier électronique** sont également utilisés pour accorder l'accès et peuvent également être envoyés par courriel, ce qui signifie que tous les membres recevront une copie du courriel.
- **Boîtes aux lettres partagées** (chapitre 8)

Bien que vous puissiez créer des groupes Microsoft 365 directement, vous avez plus de chance d'interagir avec eux en tant que composante de base, offrant une identité unique pour l'ensemble des services de Microsoft 365, comme Teams, Yammer et d'autres. De plus, Outlook peut utiliser les groupes M365. Les sites d'équipe modernes SharePoint sont conçus à partir de ceux-ci, et Stream et PowerBI les utilisent pour contrôler l'accès.

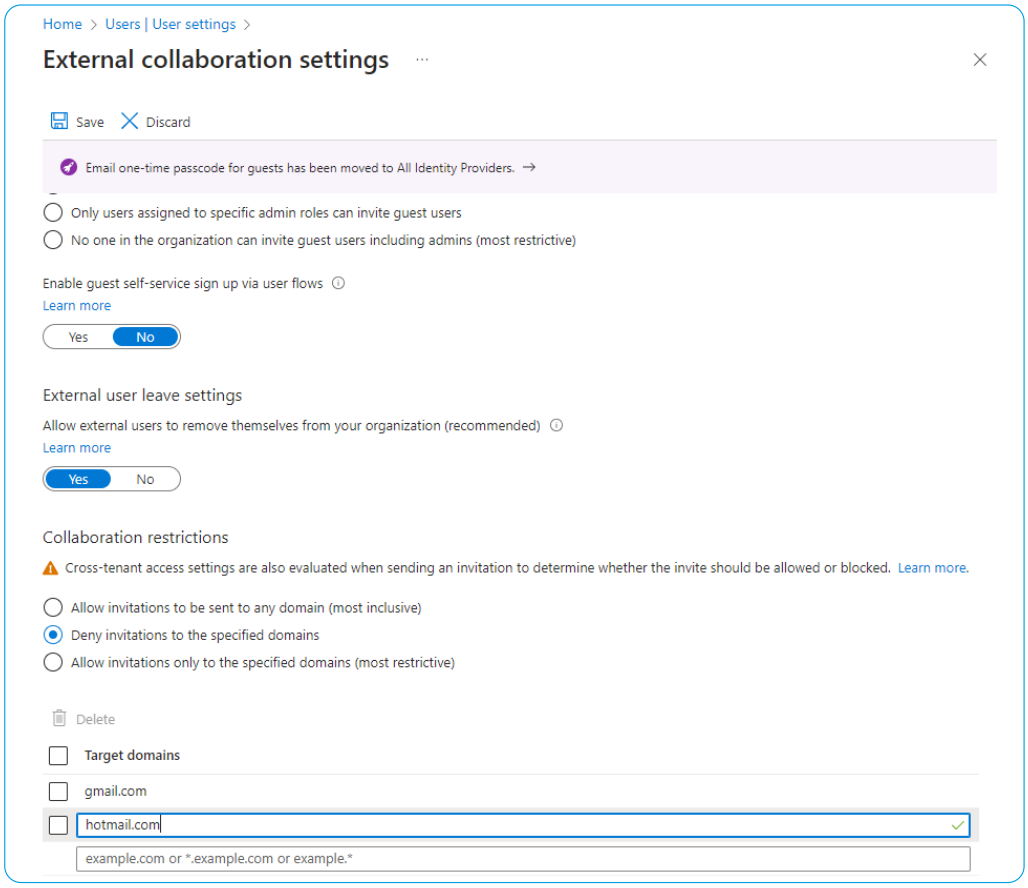
Si la configuration est effectuée de cette façon, vous pouvez inscrire les groupes M365 dans votre AD sur site, où ils se présentent comme des groupes de distribution. Vous ne pouvez pas intégrer des groupes M365 à d'autres groupes, et ils ne peuvent contenir que des comptes d'utilisateur M365 réels, tandis que les groupes de distribution Exchange peuvent contenir des comptes d'utilisateur, des utilisateurs de courrier et des contacts (voir le chapitre 8). À moins que vous ayez modifié les valeurs par défaut, n'importe quel utilisateur de votre locataire peut créer un groupe M365, ce qui **pourrait entraîner des problèmes de gouvernance.** Vous pouvez à la place **désigner des utilisateurs** qui peuvent créer des groupes. De même, vous pouvez utiliser divers **paramètres de stratégie** pour contrôler le comportement du groupe O365 chez votre locataire, telles que les **stratégies d'expiration** pour gérer le cycle de vie des groupes et vous pouvez contrôler l'**appellation des groupes** via une stratégie.

Il est facile de partager du contenu à partir d'un groupe M365 avec des utilisateurs externes, et les groupes M365 sont également un répertoire partagé de contenu historique, car tous les membres peuvent voir les contenus dès la création du groupe. Auparavant, chaque utilisateur sous licence dans votre locataire vous donnait cinq **licences d'invité** B2B, et vous pouviez utiliser des **codes de vérification à usage unique** pour les invités externes qui n'ont pas de compte Google, Microsoft (MSA) ou de compte dans Azure AD.

Ce modèle de licence pour les utilisateurs externes a changé, Microsoft regroupe Azure B2B et B2C (en utilisant Azure comme magasin pour les identités des consommateurs pour votre application développée à l'interne) et le nouveau modèle de licence signifie que chaque locataire peut avoir jusqu'à 50 000 utilisateurs externes sans frais supplémentaires.



Groupes dans le Centre d'administration M365



Paramètres de collaboration externe dans Entra – blocage des domaines spécifiés

Veuillez noter que les invités ont un accès complet au contenu de tous les groupes par défaut. Vous pouvez **contrôler les domaines** d'utilisateurs externes destinés (ou non) à un accès externe.

Aujourd'hui, lorsque vous créez un groupe, il s'agit d'un groupe **privé** dans lequel les propriétaires du groupe doivent approuver une demande d'adhésion. Vous pouvez également rendre un groupe **public** que tout le monde peut rejoindre. Vous pouvez modifier la valeur par défaut du locataire, ce qui permettra de rendre publics les nouveaux groupes, ou vous pouvez modifier les paramètres d'un groupe après l'avoir créé. Chaque groupe peut compter jusqu'à 100 propriétaires et plus de 1000 utilisateurs; un utilisateur individuel ne peut pas créer plus de 250 groupes. Comme pour d'autres produits dans M365, vous avez 30 jours pour **restaurer un groupe** une fois qu'il a été supprimé, tandis que les documents individuels du groupe sont hébergés dans la corbeille SharePoint pendant 93 jours.

Les **groupes dynamiques** sont un excellent moyen de réduire les frais administratifs liés à la gestion manuelle de l'appartenance aux groupes, en fonction des requêtes sur les attributs d'Entra ID, mais sachez qu'ils nécessitent une licence Entra ID Premium P1.

CHAPITRE 11:

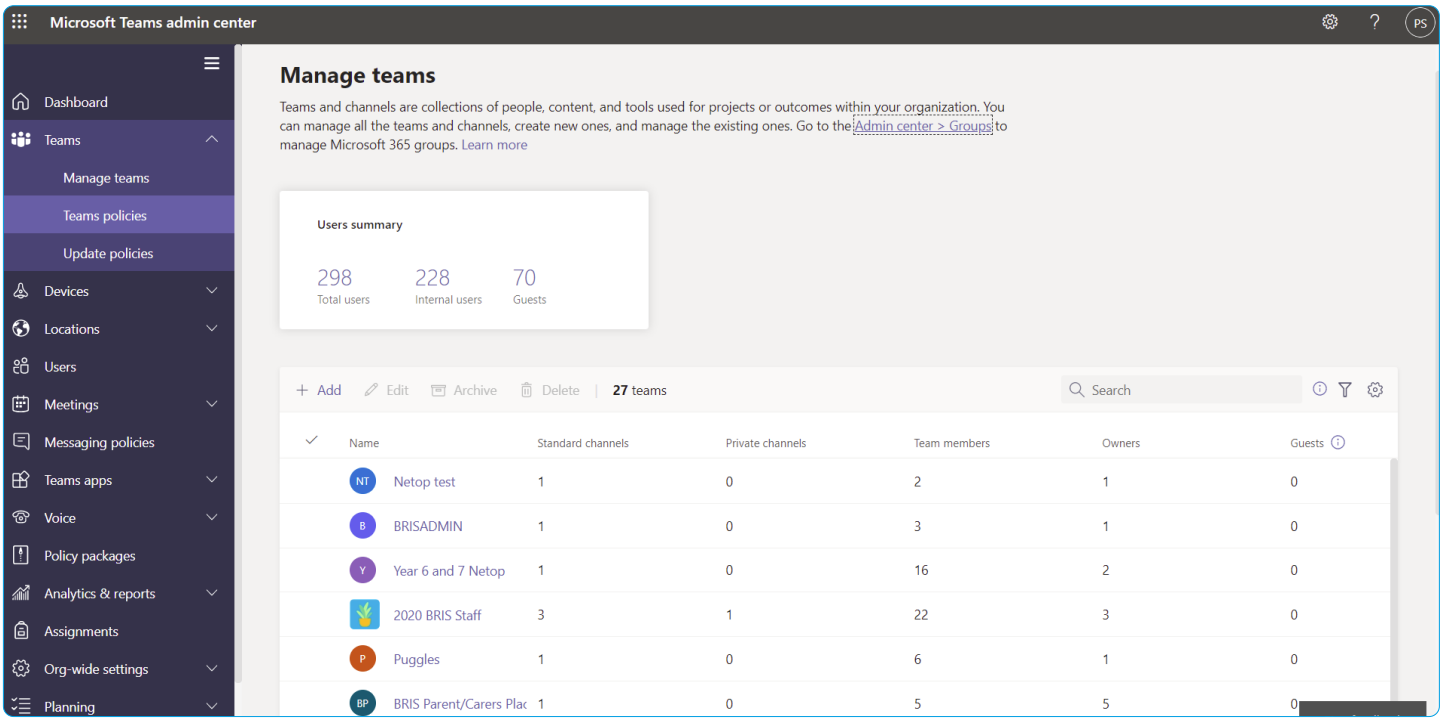
TEAMS

DE NOMBREUSES APPLICATIONS DE MESSAGERIE INSTANTANÉE ET DE CLAVARDAGE ONT TENTÉ DE PRENDRE EN CHARGE LES COMMUNICATIONS D'ENTREPRISE, ET IL NE FAIT AUCUN DOUTE QUE MICROSOFT TEAMS EST LA MEILLEURE À CE JOUR. C'EST EN GRANDE PARTIE ATTRIBUABLE À LA PANDÉMIE DE COVID-19, QUI A FAIT PASSER L'UTILISATION DE TEAMS DE 13 MILLIONS D'UTILISATEURS ACTIFS QUOTIDIENS EN JUILLET 2019 À PLUS DE 300 MILLIONS (!) EN 2023. DANS CE CHAPITRE, NOUS VERRONS CE QUE TEAMS PEUT FAIRE POUR VOS COMMUNICATIONS ET LA COLLABORATION DANS VOTRE ENTREPRISE.

11.1: DÉCOUVRIR TEAMS

De nombreux développements sont en cours dans Teams pour garantir qu'il s'agit du meilleur endroit où des groupes de personnes peuvent travailler ensemble. La preuve la plus récente est la nouvelle **application client Teams** (en prévisualisation publique en mars 2023).

Une équipe **peut avoir jusqu'à 25 000 utilisateurs** mais, d'après mon expérience, elle fonctionne mieux avec des équipes plus petites (jusqu'à quelques centaines). Si vous organisez un événement de type webinaire avec des gens qui regardent seulement, il y a une limite de 20 000 participants. Il existe des applications client pour Windows, MacOS (mises à jour toutes les deux semaines), iOS et Android, ainsi qu'une interface Web (mise à jour chaque semaine). Comme bien d'autres éléments de M365, l'adoption réussie comporte deux volets : l'aspect technique et la formation des utilisateurs.



Teams Admin Center (Centre d'administration de Teams)

Si vous avez des salles de conférence, assurez-vous de prendre en compte la technologie dont vous les équipez. **Les salles Teams** sont un moyen puissant d'utiliser la technologie pour mettre le personnel au bureau en contact avec le personnel qui travaille à domicile. Les salles Teams sont divisées en salles Basic (gratuit, jusqu'à 25 systèmes peuvent avoir ce type de licence) et Pro, qui comprend de nombreuses **fonctions de sécurité, de commodité et de collaboration supplémentaires**. L'ancienne licence Teams Room Premium a été retirée.

Jusqu'à récemment, il n'y avait que les licences Teams (dans le cadre de la licence M365) et une licence gratuite Teams pour les petites équipes (qui est en cours de retrait). En février 2023, une nouvelle catégorie de licences payantes, appelée Teams Premium, est devenue disponible. Comme pour tout ensemble de fonctions M365, vous devez évaluer soigneusement si les fonctions supplémentaires répondent aux besoins opérationnels des utilisateurs à qui vous attribuez une licence (tout le monde n'a pas besoin d'avoir Teams Premium). Les **fonctions Premium** comprennent des réunions protégées avec des filigranes sur les enregistrements (avec l'adresse électronique de la personne qui enregistre), des étiquettes de sensibilité pour les réunions et le chiffrement de bout en bout, ainsi que des modèles et des thèmes de réunions personnalisés. Pour les webinaires, il y a beaucoup d'autres fonctions qui améliorent l'expérience globale, et enfin, les rendez-vous virtuels gèrent ces types de réunions, y compris les avis par message texte.

11.2: TÉLÉPHONE TEAMS

L'un des grands attraits de Teams est que vous pouvez **le connecter** au réseau téléphonique public commuté (RTPC), ce qui permet à vos utilisateurs d'appeler n'importe qui dans le monde à partir de leur client Teams (sur n'importe quelle plateforme) et d'avoir un numéro de téléphone pour que n'importe qui puisse les appeler. Cette combinaison d'appels téléphoniques externes, de conférences vocales et vidéo internes, de réunions ou de webinaires par vidéoconférence, de **partage et de co-création faciles de fichiers,** ainsi que de messagerie instantanée et de clavardage asynchrones, a fait de Teams la plaque tournante de facto de collaboration et de communication dans de nombreuses entreprises.

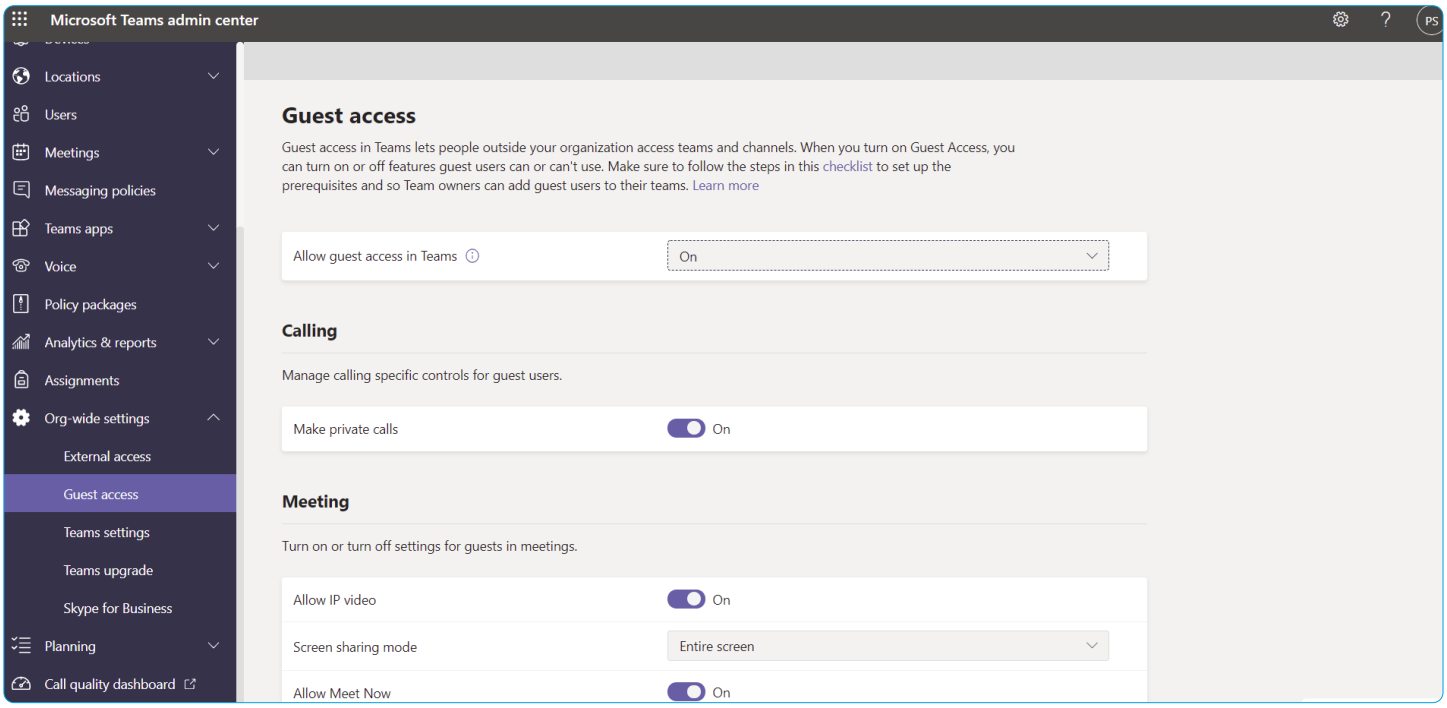
Il y a quelques options sur la façon de vous connecter, et selon votre emplacement géographique dans le monde, elles ne seront pas toutes disponibles. Vous pouvez utiliser des **Plans d'appels**, où Microsoft est en fait votre fournisseur de services de télécommunications ou **Operator Connect** si votre entreprise de télécommunications existante participe au programme et peut assurer la connectivité. Il y a aussi la **Téléphone mobile** où une entreprise de télécommunications existante utilise des numéros de téléphone mobile compatibles SIM avec Teams, et enfin l'**Acheminement direct** où vous connectez l'infrastructure sur site à Teams. Vous pouvez en utiliser plusieurs ensembles dans de plus grands environnements.

11.3: GESTION DE TEAMS

Votre interface principale est le **portail d'administration de Teams** , et il y a un **module PowerShell** disponible. Sous chaque équipe se trouve un groupe M365 (chapitre 10) avec les messages de clavardage stockés dans le stockage de la table Azure, les fichiers partagés dans la bibliothèque SharePoint de l'équipe et les fichiers personnels dans le OD4B de chaque utilisateur, les messages vocaux et les calendriers sont stockés dans les boîtes de courriel Exchange de l'utilisateur et les enregistrements de réunions dans les services de médias Azure. Si vous travaillez dans une entreprise plus importante, assurez-vous de **planifier la gouvernance** de Teams au début de votre déploiement. Visitez les **paramètres d'accès des invités** de votre équipe de locataires pour vous assurer d'avoir un bon équilibre entre la sécurité et la collaboration pour votre entreprise. Une autre fonction pratique est la capacité d'utiliser des **modèles pour la création de Teams**, y compris la création de vos propres modèles personnalisés.

Chaque équipe a un canal général par défaut, et vous pouvez créer d'autres canaux pour organiser les communications. Dans chaque canal, vous pouvez ajouter des onglets pour Planner, OneNote, PowerBI, Stream, Wiki, les sites Web et les applications de tiers. Pour limiter la prolifération de Teams dans votre organisation, vous pouvez **limiter le nombre de personnes pouvant créer des comptes Teams** (par défaut, tous les utilisateurs peuvent le faire), ainsi que d'utiliser des **canaux privés dans une équipe**. Vous pourriez avoir une équipe pour le service des ventes avec un canal privé réservé aux directeurs des ventes pour discuter de renseignements confidentiels, par exemple.

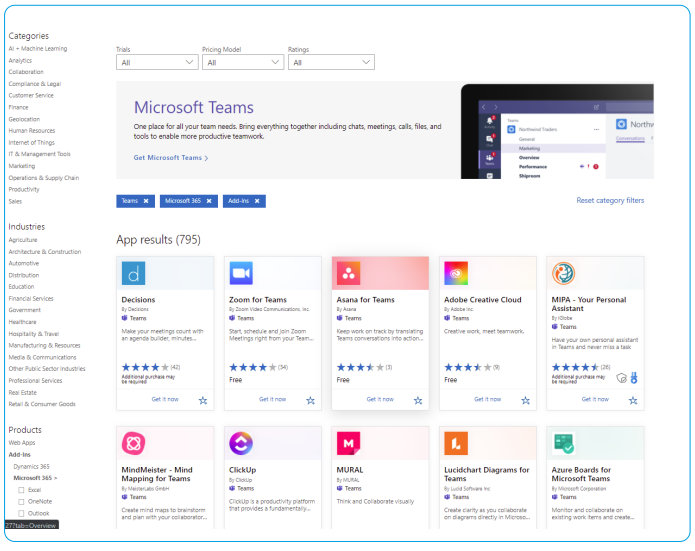
Il est également possible de **partager un canal** avec un utilisateur externe, plutôt que de partager toute une équipe. Le principal avantage pour l'utilisateur invité est qu'il peut ouvrir une session avec son propre compte de locataire et accéder au canal partagé de clavardage et aux documents sans avoir à fermer sa session et à ouvrir une nouvelle session dans Teams à l'aide de son compte d'invité. Vous pouvez seulement créer un nouveau canal en tant que canal partagé; vous ne pouvez pas convertir un canal normal en un canal partagé.



Paramètres d'accès des invités dans Teams

La production de présentations au moyen de Teams est courante, la **fonction PowerPoint en direct** la rend plus interactive en permettant aux participants d'interagir avec la présentation à leur propre rythme et le **mode présentateur** vous donne un meilleur contrôle sur la façon dont votre présentation apparaît chez l'auditoire. Pour pratiquer votre présentation (dans PowerPoint en général), utilisez **Speaker Coach (Encadreur de conférenciers).**

Une excellente fonction est celle des **salles de discussion en petits groupes**. Cela vous permet d'envoyer des utilisateurs vers des « salles » ou demander aux utilisateurs de choisir des salles où ils peuvent collaborer avec un petit groupe d'utilisateurs dans une équipe pendant une réunion, puis de revenir à la réunion principale plus tard.



Teams Third-Party Add-Ins

Les enregistrements des réunions Teams (y compris les **transcriptions**) étaient auparavant stockés dans Stream, et **ils sont maintenant enregistrés dans OD4B/SharePoint** où ils peuvent être facilement partagés (y compris avec les participants externes). Un bon conseil est de connaître l'expiration par défaut des enregistrements de réunions : 120 jours. Vous pouvez modifier cela (pour les enregistrements dans votre locataire) dans Teams admin center - Meetings - Meeting policies - Recording & transcription (Centre d'administration de Teams – Réunions – Stratégies de réunion – Enregistrement et transcription). En parlant de transcriptions, si vous avez Teams Premium, vous pouvez activer les **sous-titres traduits**, de sorte qu'une réunion présentée en anglais puisse être visualisée par un visualiseur allemand avec des sous-titres dans sa langue, et qu'un autre visualiseur puisse avoir des sous-titres en chinois, par exemple.

11.4: UTILISATION DE TEAMS

Si vous avez l'habitude de communiquer par courriel, voici quelques lignes directrices pour être efficace avec Teams. Utilisez le symbole @ pour attirer l'attention d'un membre spécifique de l'équipe, d'un canal ou de l'équipe entière. Ne soyez pas avare en compliments lorsque quelqu'un fait quelque chose de bien pour l'équipe. Pour accuser réception d'un message, aimez-le tout simplement au lieu de rajouter du bruit avec une réponse textuelle. Lorsque vous êtes sur le point de publier quelque chose, vérifiez s'il y a déjà un fil conducteur connexe et ajoutez plutôt votre message. Utilisez le style de texte (ou un GIF, un autocollant ou un mème) lorsque vous voulez faire passer votre message et des réactions (tristesse, colère ou joie) pour contribuer à la conversation, le cas échéant.

Vous pouvez rendre l'arrière-plan flou lorsque vous participez à une réunion vidéo ou **remplacer l'image d'arrière-plan** et si vous avez des travailleurs de première ligne qui doivent communiquer avec les autres, utilisez la fonction push-to-talk (Presser pour parler) du **Walkie-Talkie (Émetteur-récepteur).** Vous pouvez également utiliser **un avatar** pour remplacer votre flux vidéo, ce qui est pratique pour les réunions du lundi matin lorsque vous êtes mal coiffé, en présentant plutôt une version « caricaturale » de vous-même.

Teams **traduira automatiquement les messages** dans d'autres langues dans la langue définie en fonction de vos paramètres personnels. Par ailleurs, il existe la **fonctionnalité hors ligne**. Donc, si vous n'êtes pas connecté, Teams enregistrera vos messages non envoyés et les enverra à votre retour en ligne.

Lorsque vous participez à une réunion, vous pouvez utiliser le **mode Ensemble** qui montre la vidéo de chaque participant comme s'il était assis dans une salle de conférence, en enlevant l'ambiance « Brady Bunch » de la grille traditionnelle des flux vidéo.

11.5: VIVA

Si vous aviez besoin d'une preuve supplémentaire de la place centrale qu'occupe Teams dans la vision et la feuille de route de Microsoft en matière de collaboration et de travail modernes, ne cherchez pas plus loin que la plateforme d'expérience de l'employé **Viva** (EXP). Viva a huit piliers, tous apparus dans Teams : **Viva Connections** prend en charge votre site d'accueil SharePoint Online, vos applications sectorielles (LOB) et d'autres sources de nouvelles internes et vous permet de cibler les nouvelles de l'entreprise et les connexions avec les bonnes personnes.

Viva Insights est la prochaine version de My Analytics pour aider le personnel à gérer le temps et à éviter l'épuisement professionnel, l'intégration avec Headspace pour les méditations guidées et une fonction de navette virtuelle pour terminer la journée de travail. Les gestionnaires ont une vue dépersonnalisée qui leur permet de voir le comportement d'une équipe sur le plan du stress, de la santé mentale et de la productivité. Les cadres ont accès à une vue Responsables qui leur permet de voir l'état général de leur personnel. Le troisième pilier est **Viva Learning**, qui présente **des cours de formation et du contenu de micro-apprentissage** tout en s'intégrant à d'**autres systèmes de gestion de l'apprentissage** (Cornerstone OnDemand, Saba, SAP SuccessFactors et Workday) pour faire de l'apprentissage une partie intégrante du travail quotidien de chacun. Les gestionnaires peuvent planifier des formations et les membres du personnel peuvent partager des cours particulièrement intéressants entre eux qui sont tous disponibles directement dans Teams. **Viva Topics** s'appuie sur Cortex/Syntex et utilise l'IA pour organiser le contenu à l'échelle de l'entreprise (projets internes, produits, acronymes) et l'expertise du personnel, en le présentant sous forme de fiches thématiques ou de pages dans Teams, Microsoft Search, SharePoint et Office. Voyez cela comme une sorte de Wikipédia pour votre entreprise.

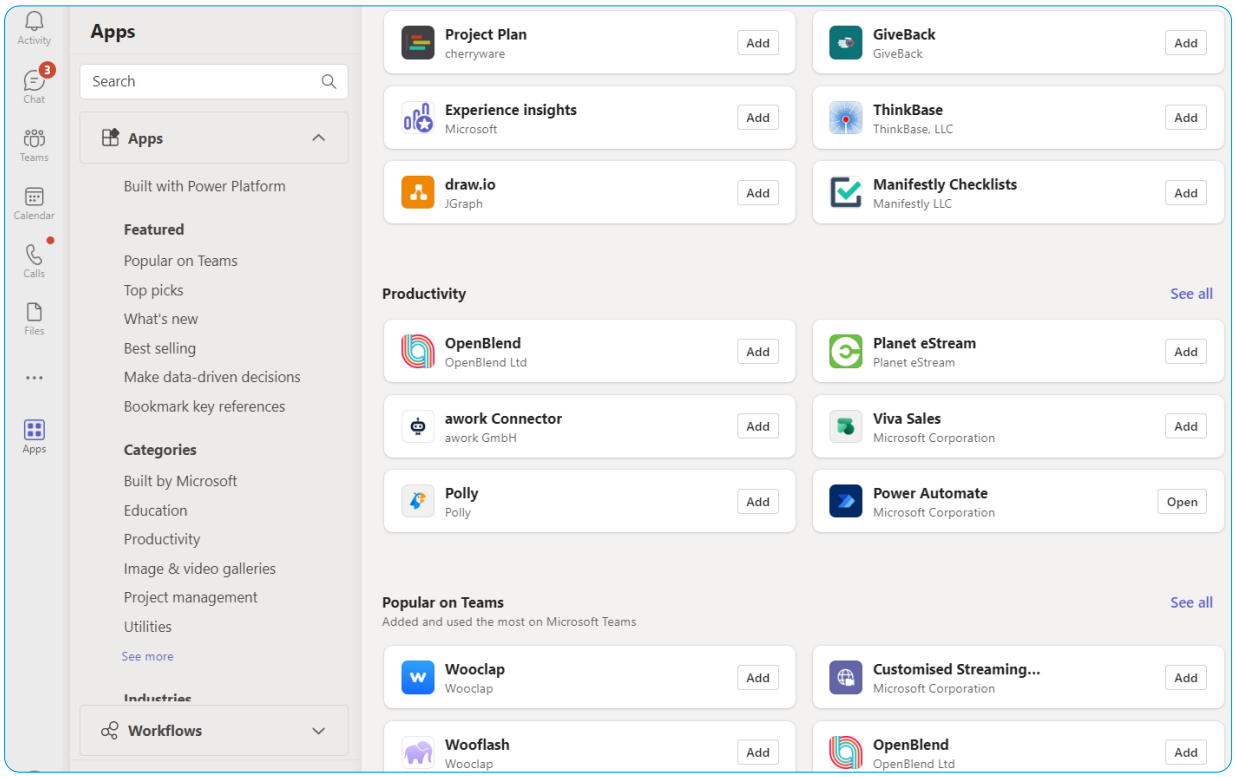
Viva Goals utilise la puissance du cadre des objectifs et des résultats clés (ORC) pour aider le personnel à suivre ses progrès par rapport aux objectifs. **Viva Engage**, quant à lui, relie les personnes au sein d'une organisation (il s'agit en fait du nouveau nom de ce qui s'appelait auparavant Yammer). Le nouvel outil **Viva Sales** s'intègre à n'importe quel système de gestion des relations avec la clientèle (y compris, bien sûr, Microsoft Dynamics 365) pour une meilleure compréhension et une plus grande mobilisation des clients. Enfin, **Viva Pulse** (en prévisualisation publique au moment de la rédaction) aide les dirigeants et les gestionnaires à recevoir les commentaires internes d'une organisation et à y donner suite.

Comme vous pouvez probablement le constater d'après ces brèves descriptions, la plupart des modules Viva sont susceptibles de trouver leur place dans de grandes entreprises, car c'est là que les défis de la « gestion des personnes » à grande échelle se font le plus sentir.

11.6: EXTENSION DE TEAMS

Une autre capacité puissante est l'**ajout d'applications** à Teams via Teams Store. Microsoft teste et valide ces applications. Il existe des centaines d'applications différentes pour l'intégration avec d'autres plateformes, l'amélioration de la productivité, l'amélioration des réunions, la gestion des relations avec la clientèle (GRC) et bien plus encore. Une application très populaire est le **Tableau blanc de Microsoft**, gratuite sur toutes les plateformes, que vous pouvez utiliser à la fois à l'intérieur de Teams et de façon autonome pour réfléchir et planifier ensemble.

En tant qu'administrateur, vous disposez d'un contrôle granulaire, vous pouvez **autoriser ou bloquer des applications**, **contrôler les permissions** qui leur sont accordées, gérer la façon dont les **applications sont mises à la disposition des utilisateurs**, et **établir des rapports sur l'utilisation des applications.** Vous pouvez également développer des **applications personnalisées** en interne.



Boutique Teams avec applications tierces

Vous pouvez également **étendre Teams avec des robots** qui peuvent interagir naturellement avec vos utilisateurs au moyen de clavardage ou d'un assistant virtuel de notification capable de transmettre des renseignements pertinents à vos utilisateurs.
Avec l'avènement de Slack (le principal concurrent de Teams) et Teams, de nombreuses personnes ont (encore) proclamé la fin de l'ère des courriels. Comme d'habitude, nous avons tendance à voir la nouvelle technologie comme une remplaçante directe de l'ancienne, alors que la réalité est plus complexe. Je trouve que Teams est plus efficace pour le travail de groupe, le partage des fichiers et la communication surpassent le courrier électronique, mais la communication en dehors des projets de clients dans lesquels je suis impliqué repose toujours sur le courrier électronique. Vous pouvez utiliser le courriel pour envoyer des messages à un canal d'une équipe.

CHAPITRE 12:

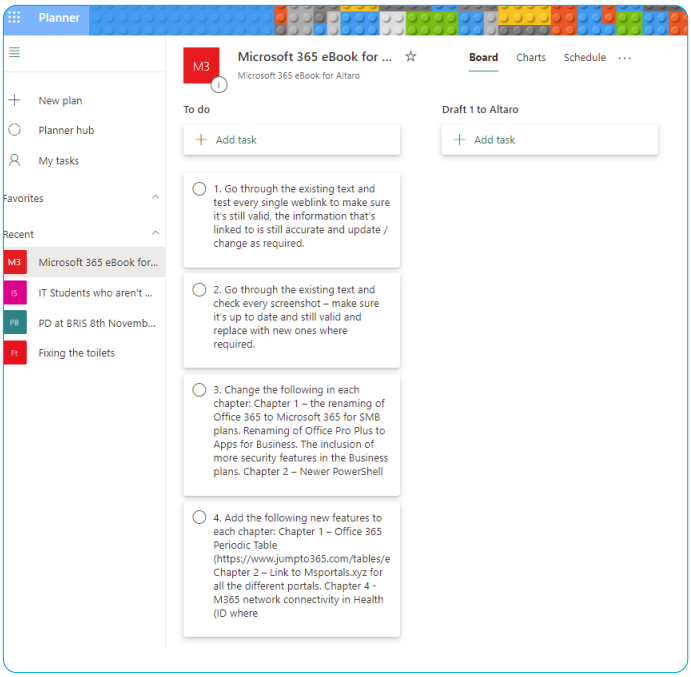
AUTRES APPLICATIONS OFFICE 365

IL Y A BEAUCOUP D'AUTRES APPLICATIONS ET SERVICES DANS LE PORTEFEUILLE D'OFFICE 365. DANS LE PRÉSENT CHAPITRE, NOUS EXAMINERONS CERTAINS D'ENTRE EUX AVEC UNE BRÈVE INTRODUCTION.

12.1: PLANNER

Microsoft propose Project pour la gestion de projets à grande échelle depuis de nombreuses années, mais pour les petites et moyennes entreprises, c'est excessif (la courbe d'apprentissage est abrupte) et c'est là que Planner se démarque de la concurrence. Si vous avez déjà utilisé Trello, vous devriez être à l'aise avec le flux de travail de Planner.

Il y a une interface Web, ainsi que des clients iOS et Android, mais pas de client PC. Si vous ajoutez un onglet Planner à une équipe, vous pouvez créer un nouveau plan ou joindre un plan existant. Vous organisez les tâches en catégories, attribuez des tâches à différentes personnes et faites le suivi de l'avancement de ces tâches. Les tâches peuvent également être visualisées dans un calendrier et vous pouvez exporter un plan dans Excel.



Un plan dans Planner

D'autres offres de gestion des tâches de Microsoft comprennent To-Do (les clients mobiles, Web et PC sont disponibles) qui s'intègre aux tâches d'Outlook.

12.2: STREAM

C'est la meilleure façon de partager **des vidéos** au sein de votre entreprise, et c'est semblable à YouTube. Il y a des clients pour iOS et Android et une interface Web, mais il n'y a actuellement aucune licence en place pour le partage de vidéos avec des personnes à l'extérieur de votre locataire.

Lorsque vous téléchargez une vidéo, elle est traitée et si les participants parlent l'anglais, le chinois, le français, l'allemand, l'italien, le japonais, le portugais ou l'espagnol, elle **génère automatiquement des sous-titres** qui peuvent être consultés dans Stream, ce qui facilite la recherche de la bonne vidéo ou du bon passage dans la vidéo. Elle tentera également de reconnaître les personnes dans la vidéo et, si l'identification est réussie, elle dressera la liste de ces personnes avec les renseignements de la vidéo. Auparavant, Teams utilisait Stream pour stocker les enregistrements de réunions, mais ils sont maintenant stockés dans OD4B ou SharePoint.

12.3: KAIZALA

Il s'agit d'une application comme Teams, conçue pour les travailleurs de première ligne et de passage qui ont une mauvaise connectivité. Considérez-la comme une version gérée de WhatsApp.

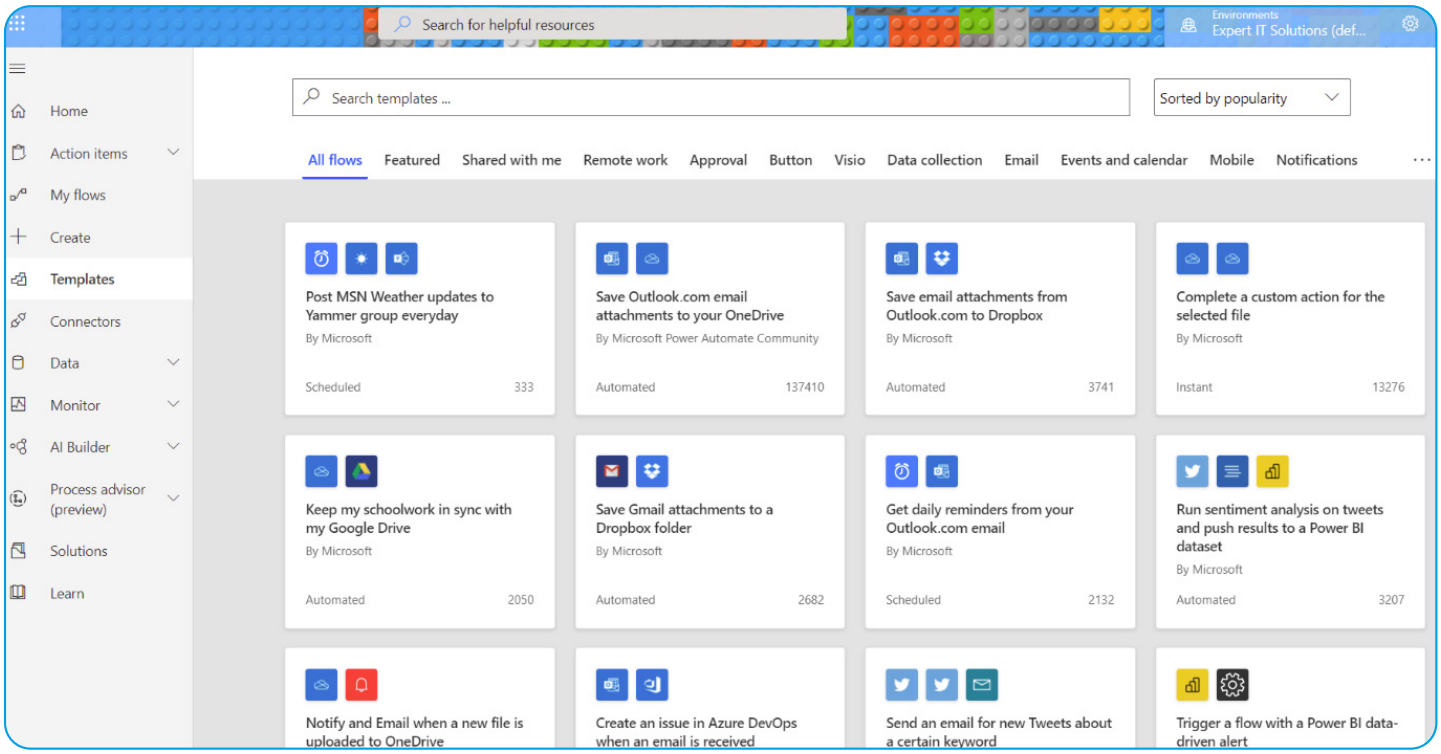
12.4: POWERBI

La visualisation des données est importante pour toute entreprise moderne qui veut se focaliser sur les données et **PowerBI** est la solution de Microsoft pour répondre à ces besoins. Il y a un client de bureau où vous créez vos tableaux de bord de même qu'une interface Web. L'octroi de licences est **un peu difficile**, selon ce que vous avez conçu et les personnes avec qui vous voulez les partager.

C'est très amusant à utiliser et les résultats peuvent être extrêmement utiles pour de nombreux aspects de votre entreprise.

12.5: POWER AUTOMATE

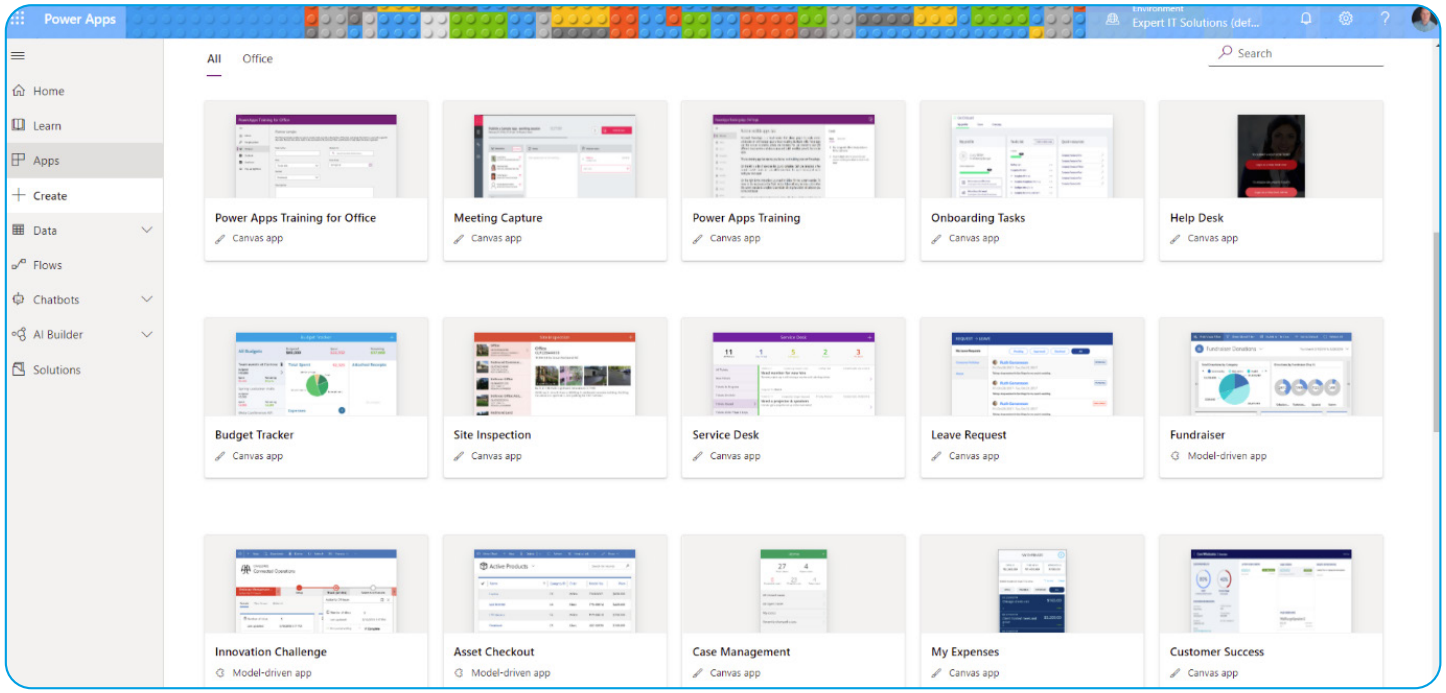
Cet outil Web d'une simplicité apparente est conçu pour automatiser les tâches sans avoir à écrire de code (auparavant appelé Flow). Il suffit de déplacer les actions, de les relier à des systèmes externes et de les programmer pour qu'elles soient exécutées régulièrement ou déclenchées par un événement. Il existe de nombreux modèles pour vous aider à démarrer, ainsi que des connecteurs pour vous relier à Microsoft et à des systèmes tiers. Si vous avez utilisé If This Then That ou Zapier, **Power Automate** est facile à utiliser.



Power Automate Templates

12.6: POWERAPPS

Vous avez déjà souhaité doter votre personnel d'une application mobile personnalisée pour recueillir des données sur le terrain ou y accéder, mais vous vous êtes rendu compte que les coûts de développement étaient trop élevés? **PowerApps** est la solution, fournissant un environnement de développement low code/no code pour construire des applications qui se connectent à SharePoint, Excel, O365, Dynamics 365 ou SQL server sur site ou dans le nuage; ou la plateforme **Dataverse**. Les applications ainsi produites fonctionnent sur iOS, Android, dans un navigateur Web ou dans Teams et SharePoint Online. Si vous devez gérer des données dans vos applications, il y a **Dataverse** pour Teams et la version complète de Dataverse.



Modèles PowerApps

12.7: MICROSOFT LISTS

Oui, l'ancien concept de liste SharePoint a reçu un nouveau souffle, y compris une application distincte et est également disponible dans Teams. Utilisez-le pour faire le suivi des listes de « choses » et gérer les renseignements.

12.8: MICROSOFT LOOP

La technologie la plus déroutante que Microsoft a publiée au cours des dernières années (actuellement en prévisualisation publique) est Loop. Le concept est assez simple. Vous avez des composantes de Loop que vous pouvez intégrer à divers endroits, comme des documents, des clavardages dans Teams ou un courriel, et celles-ci sont tenues synchronisées entre ces différents endroits. Les pages Loop vous permettent de réunir des composants, des liens, des tâches et d'autres données. Enfin, les espaces de travail Loop sont des espaces partagés qui rassemblent les pages et les composantes. Je trouve que Loop est la plus utile aux premières étapes d'un projet ou d'une idée – lancez des idées, collaborez avec les autres sur un concept et tenez les personnes avec qui vous travaillez informées.

Le problème aujourd'hui, c'est qu'en raison du stockage sous-jacent des composantes de Loop dans la version OneDrive Entreprise personnelle de l'utilisateur, le partage à l'extérieur d'une organisation ne fonctionne pas vraiment, et même dans un locataire, cela peut être difficile. Si Microsoft parvient à relever ces défis, Loop a un avenir radieux devant lui.

CHAPITRE 13:

MICROSOFT INTUNE

M365 E3 ET E5 VOUS FOURNISSENT MICROSOFT INTUNE, LE SERVICE INFONUAGIQUE MOBILE DEVICE MANAGEMENT (MDM) DE MICROSOFT. DANS CE CHAPITRE, NOUS VERRONS COMMENT IL PEUT VOUS AIDER À GÉRER LES APPAREILS ET LES ORDINATEURS PERSONNELS, LES APPLICATIONS MOBILES, À PROTÉGER LES DONNÉES DE L'ENTREPRISE ET À APPLIQUER LES STRATÉGIES DE SÉCURITÉ.

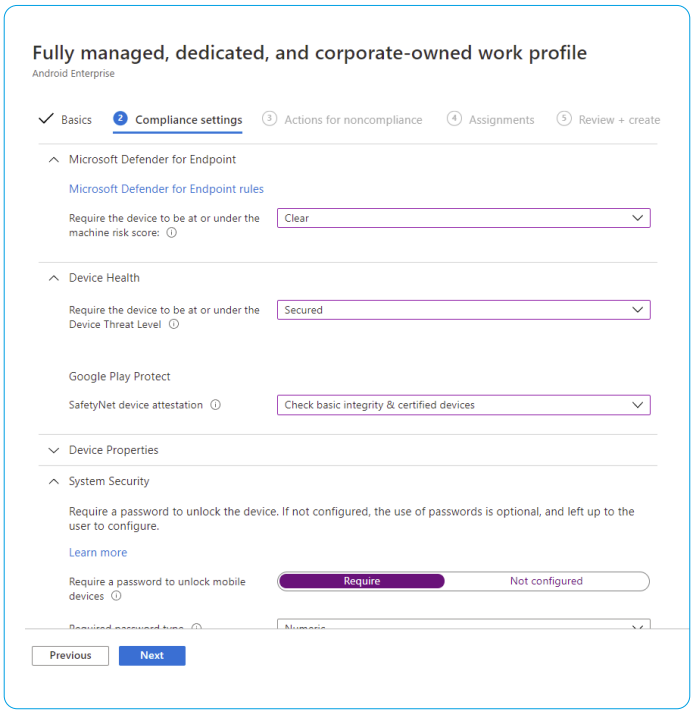
Il existait auparavant un produit sur site appelé System Center Configuration Manager (SCCM), maintenant appelé **Microsoft Configuration Manager**, que vous pouvez intégrer étroitement à Intune.

Auparavant, les administrateurs Intune devaient être titulaires d'une licence pour Intune, mais **ce n'est plus le cas**. L'**analyse des points de terminaison** est une partie intéressante d'Intune. L'utilisation de signaux provenant de vos appareils pour repérer les ordinateurs personnels problématiques ou lents fait partie de la **note d'adoption** globale.

Si vous avez des dispositifs Windows 10/11 qui servent à des fonctions spécifiques (sur un atelier de production, dans un poste de soins infirmiers d'un hôpital par exemple), vous pouvez utiliser la configuration en nuage pour **les gérer facilement en utilisant Intune**, avec des paramètres de configuration de base sous forme de scripts.

13.1: GESTION DES APPAREILS MOBILES (GAM)

Il y a plusieurs façons d'utiliser Intune. Si vous avez des appareils (téléphones intelligents, tablettes, ordinateurs portatifs) qui appartiennent à l'entreprise, vous pouvez **les inscrire dans Intune**. Cela vous donne un grand contrôle sur l'appareil, y compris la capacité de gérer les paramètres, les applications et la possibilité d'effacer l'appareil en cas de perte ou de vol. Vous pouvez également utiliser Intune pour gérer les mises à jour du système d'exploitation pour les appareils Windows, envoyer des applications vers des appareils, configurer des profils Wi-Fi et déployer des certificats, ainsi que bloquer les appareils iOS débridés et des appareils Android enracinés.



Stratégie de conformité Android dans Endpoint Manager

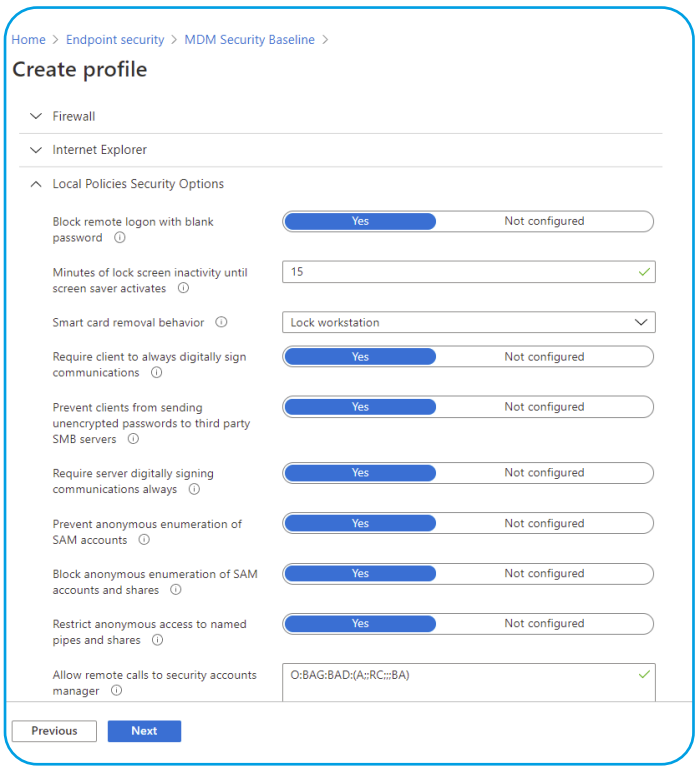
Si l'appareil est un appareil personnel, appartenant à l'employé, il se peut qu'il ne soit pas à l'aise de l'enregistrer afin que vous puissiez utiliser le service Gestion des applications mobiles (GAM) pour ces appareils.

13.2: GESTION DES APPLICATIONS MOBILES

Cette approche moins intrusive vous permet de créer des **stratégies de protection des applications (APP)** pour des applications spécifiques, le courriel étant l'exemple classique. Les utilisateurs veulent accéder aux courriels d'entreprise sur leur téléphone intelligent personnel afin que vous puissiez y ajouter des stratégies qui leur permettent d'utiliser uniquement Outlook (application mobile gratuite pour Android et iOS), et non les applications de courrier intégrées. Vous pouvez également protéger davantage les données d'entreprise afin qu'un utilisateur ne puisse pas les copier vers une application non destinée aux entreprises (application de courriel personnel, etc.). Si l'appareil est perdu ou volé, vous pouvez effacer les données d'entreprise sans toucher les photos personnelles et autres.

Le choix entre la Gestion des appareils mobiles et la Gestion des applications mobiles dépend de nombreux facteurs comme votre base d'utilisateurs, vos contrats de travail, vos besoins opérationnels et de sécurité, etc. Assurez-vous de passer du temps à la **phase de planification** pour bien faire les choses.

Une autre partie de la gestion des applications mobiles pourrait consister à les relier aux ressources sur site en toute sécurité. Microsoft offre maintenant son propre RPV pour iOS et Android appelé **Tunnel** – et il est intégré à Microsoft Defender for Endpoint.



Bases de référence de la sécurité de la Gestion des appareils mobiles

13.3: MICROSOFT CONFIGURATION MANAGER

Si vous avez déployé MCM sur site pour gérer vos serveurs et vos ordinateurs personnels clients traditionnels, vous pouvez intégrer Intune dans votre flux de gestion **par cogestion** pour tirer parti du meilleur des deux mondes et préparer votre environnement à une migration graduelle vers la gestion en nuage. Ne confondez pas cela avec la **Gestion des appareils mobiles hybride**, qui est l'approche plus ancienne et obsolète pour marier SCCM et Intune.

13.4: SUITE INTUNE

À la manière de Microsoft, il y a **des modules d'extension pour Intune** que vous pourriez envisager pour votre entreprise, s'ils résolvent un problème opérationnel particulier pour vous. Il y a des modules d'extension autonomes, un plan Intune Plan 2 et la suite Intune complète, qui comprend ce qui suit : **Advanced endpoint analytics (Analyse avancée des points de terminaison)** pour suivre et optimiser les expériences des utilisateurs finaux, **Endpoint Privilege Management (Gestion des privilèges des points de terminaison),** qui permet aux utilisateurs finaux d'effectuer certaines tâches administratives sur leur appareil Windows sans être administrateur local et **Microsoft Tunnel pour la Gestion des applications mobiles**, ce qui étend la fonction RPV par application pour les applications Android et iOS à la Gestion des applications mobiles. Il y a aussi **Remote Help (Assistance à distance)**, qui est un moyen sécurisé de permettre au service d'assistance d'accéder à l'écran du personnel pour l'aider et la **gestion des appareils spécialisés**, comme le casque d'écoute Réalité augmentée (RA) et réalité virtuelle (RV) et les gros appareils à écran intelligent.

PARTIE 3

SÉCURITÉ, SAUVEGARDE ET CONFORMITÉ

MICROSOFT 365
LE GUIDE
ESSENTIEL

CHAPITRE 14:

LA SÉCURITÉ DANS O365

LORSQUE L'INFORMATIQUE EN NUAGE A FAIT SON APPARITION, LA SÉCURITÉ DES DONNÉES TRANSFÉRÉES DANS « LE CENTRE DE DONNÉES DE QUELQU'UN D'AUTRE » SUSCITAIT DE NOMBREUSES INQUIÉTUDES. JE PENSE QU'IL EST CLAIR POUR LA PLUPART DES RESPONSABLES DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION (RSSI) AUJOURD'HUI QUE LES GRANDS FOURNISSEURS FONT UN BIEN MEILLEUR TRAVAIL EN MATIÈRE DE SÉCURITÉ DES TI QUE LA PLUPART DES ENTREPRISES (OU QU'ELLES ONT LE BUDGET POUR LE FAIRE). LEUR MOTIVATION EST ÉGALEMENT FORTE, CAR SI UNE FAILLE IMPORTANTE SE PRODUISAIT, ELLE POURRAIT AFFECTER PLUSIEURS MILLIERS D'ENTREPRISES, ET ELLES DÉPENSENT DONC BEAUCOUP D'ARGENT POUR S'ASSURER QUE LEURS SERVICES SUR LE NUAGE SONT AUSSI SÛRS QUE POSSIBLE.

Cela ne veut pas dire que vous pouvez tout laisser à Microsoft, il y a ce qu'on appelle le **modèle de responsabilité partagée** et tous les fournisseurs de services infonuagiques en ont une version. Vous êtes toujours responsables de certains aspects, tels que les points de terminaison que vos utilisateurs utilisent pour accéder aux services infonuagiques, les infrastructures sur site qui fonctionnent en mode hybride avec Office 365, ainsi que le provisionnement et le dé-provisionnement des utilisateurs. Il y a également de nombreux dispositifs de contrôle de sécurité dans O365 que vous devez personnaliser pour répondre aux besoins de votre entreprise, où vous et Microsoft partagez la responsabilité de la sécurité. Dans ce chapitre, nous examinerons ces dispositifs de contrôle pour voir où et comment vous les configurez.

Le fondement de « la façon dont vous pensez à la sécurité » devrait être la Confiance zéro (Zero Trust), au lieu de faire confiance à une connexion en fonction de son origine (« si elle se trouve sur le réseau local interne, il est sûre, si elle vient de l'extérieur, elle est dangereuse »). Chaque accès est vérifié en fonction de vos règles d'accès conditionnel, ce qui vous donne une meilleure posture de sécurité. Et fondez votre sécurité sur l'identité, c'est-à-dire le nouveau pare-feu, et **tenez-vous au courant des nouvelles fonctionnalités dans le domaine de la sécurité.**

Lorsque vous réfléchissez à la façon de défendre vos systèmes, n'oubliez pas de tenir compte des pirates **qui passent des actes sur site au nuage**, comme nous l'avons vu dans la **faille de Solarwinds**. Si vous possédez une licence M365 E5, vous pouvez suivre la formation sur la simulation d'attaque pour tester vos utilisateurs avec de faux courriels de phishing et leur fournir automatiquement une formation en plusieurs étapes en fonction des risques de tomber dans les pièges de ces pirates. Si vous souhaitez plus de contrôle et d'optimisation, essayez la solution **Security Awareness Service** de Hornetsecurity, qui offre une analyse comparative entièrement automatisée, une simulation de spear-phishing et une formation en ligne pour sensibiliser et protéger les employés contre les cybermenaces.

N'oubliez pas qu'Entra ID Premium P1 et P2, que vous pouvez acheter sous forme de module d'extension d'O365 (inclus dans M365), sont décrits dans le chapitre 7.

Il y a un argument solide à faire valoir selon lequel le fait de miser sur Microsoft pour fournir la plateforme (Office 365) et de payer des frais supplémentaires pour des fonctions de sécurité avancées de la même entreprise constitue un conflit d'intérêts. Après tout, Microsoft pourrait inclure plus de fonctions de sécurité dans la plateforme de base (Office 365 E3 et Microsoft 365 E3, par exemple), plutôt que de facturer des coûts supplémentaires. C'est pourquoi de nombreuses entreprises choisissent un service tiers pour des services de sécurité avancés en plus de la plateforme de base, comme la solution 365 Total Protection de Hornetsecurity.

14.1: 365 TOTAL PROTECTION

365 Total Protection est une solution de sécurité infonuagique qui couvre tous les aspects de la gestion de la sécurité et de la protection des données de Microsoft 365 d'une organisation, tels que la sécurité des courriels, la sauvegarde et la récupération, la conformité, la gestion des permissions et la sensibilisation à la sécurité. La solution est spécifiquement développée pour Microsoft 365 et ne nécessite ni matériel, ni logiciel, ni maintenance, tout en fournissant des couches de sécurité et de protection des données supplémentaires nécessaires contre les pourriels, les maliciels et les menaces avancées.

La solution 365 Total Protection de Hornetsecurity est offerte en quatre plans différents :

1. **365 Total Protection Business** vous offre des solutions de pointe en matière de sécurité des courriels, de protection contre les pourriels et les logiciels malveillants, de signatures et de courriels chiffrés.
2. **365 Total Protection Enterprise** ajoute la fonction d'archivage des courriels, la conservation pendant une période de dix (10) ans, eDiscovery (preuve électronique), Advanced Threat Protection (ATP) et le bac à sable des courriels suspects, la numérisation d'adresses URL et l'analyseur de codes QR.

3. **365 Total Protection Enterprise Backup** ajoute la sauvegarde automatisée des boîtes de courriel, de Teams, de OneDrive et de SharePoint, ainsi que la récupération facile, la sauvegarde et la récupération des points de terminaison Windows.
4. **365 Total Protection Compliance & Awareness** ajoute les produits Permission Manager, Security Awareness Service et AI Recipient Validation à l'offre.

Cette large gamme de fonctions de sécurité et de conformité Microsoft 365 est disponible en **un seul progiciel et sous une seule licence.**

14.2: 365 PERMISSION MANAGER

L'un des trois piliers de Zero Trust, l'utilisation de l'accès au moindre privilège, est remarquablement difficile à atteindre à grande échelle. Cela est particulièrement évident dans SharePoint et OneDrive, où vous avez non seulement un ensemble complexe d'options d'autorisation qui se chevauchent, mais aussi le partage de fichiers et de sites avec des utilisateurs externes, que ce soit par l'intermédiaire de SharePoint, de OneDrive ou, maintenant, de Teams.

Pour répertorier toutes ces autorisations qui ont été accordées et produire des rapports connexes, il faut parcourir plusieurs écrans ou exécuter des scripts PowerShell. Il n'y a pas non plus de moyen facile d'obtenir des autorisations de « taille appropriée » lorsqu'elles sont trop vastes, ni de moyen rapide de révoquer des autorisations rapidement dans tous les sites lorsqu'on découvre qu'un compte d'utilisateur a été compromis, par exemple.

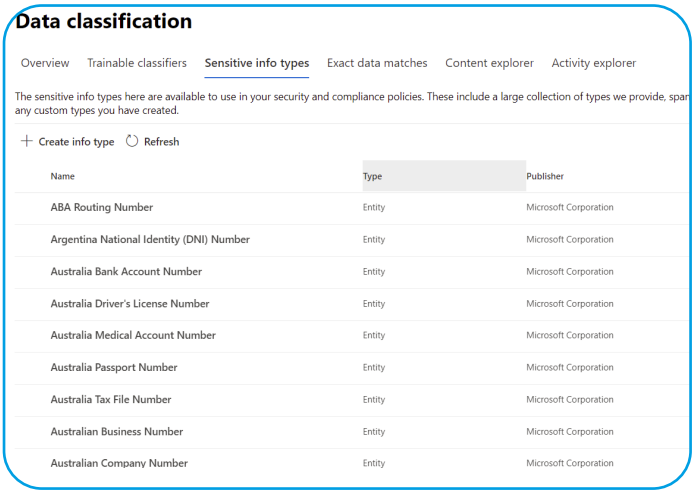
Un produit unique de Hornetsecurity, **365 Permission Manager** permet d'atténuer tous ces problèmes, et plus encore. Un tableau de bord centralisé vous montre tous vos sites et dans quelle mesure ils sont conformes à vos stratégies de partage. Pour ajuster les permissions, utilisez tout simplement le bouton Fix (Réparer) ou, si les besoins de l'entreprise justifient une exception à la stratégie, Approuver un cas particulier. Les stratégies intégrées ou personnalisées qui contrôlent le partage externe, le partage interne et les paramètres connexes peuvent être appliquées à des sites SharePoint individuels ou à des emplacements OneDrive, ce qui améliore considérablement la gouvernance et la gestion des risques.
Vous pouvez également voir les permissions dans SharePoint, OneDrive et Teams pour un utilisateur sélectionné, ce qui est très utile lorsque vous soupçonnez une compromission de compte, ou peut-être dans le cas d'une enquête de risque interne.

Une autre fonction très utile est Quick Actions (Actions rapides), qui vous permet d'effectuer des actions en lots pour gérer les autorisations et maintenir une infrastructure SharePoint, Teams et OneDrive conforme.

14.3: PROTECTION DES RENSEIGNEMENTS DE MICROSOFT PURVIEW

Toutes les fonctions de gouvernance, de prévention des pertes de données et de protection de l'information dans M365 relèvent de Purview, le portail se trouvant à l'adresse **compliance.microsoft.com**.

L'utilisation d'**étiquettes pour classer les données,** que ce soit manuellement ou automatiquement en parcourant des documents ou des courriels, vous permet de commencer à gérer les renseignements de votre entreprise. Une fois qu'un document a été étiqueté, vous pouvez utiliser MIP ou OME pour le protéger (voir ci-dessous), ou contrôler l'accès aux points de terminaison Windows au moyen d'une stratégie et gérer l'accès dans Office pour Mac, Windows, iOS et Android.



Types de renseignements de nature délicate (TRD)

14.4 : MICROSOFT INFORMATION PROTECTION

L'une des fonctions les plus puissantes et les moins déployées est la capacité de protéger les documents, peu importe leur emplacement. Les accès aux fichiers et aux documents SharePoint traditionnels sont étroitement contrôlés au niveau du serveur, mais dès qu'un document est envoyé par courriel à quelqu'un ou stocké sur une clé USB, ce contrôle est perdu.

Avec Microsoft Information Protection (MIP), vous pouvez configurer des étiquettes et des règles de chiffrement des documents et qui permettent à leurs utilisateurs d'y accéder, de sorte que, peu importe la façon dont ils sont partagés, seules les bonnes personnes y ont accès. Si vous commencez à utiliser MIP, vous utiliserez le client intégré dans les applications Office sous Windows, Mac, iOS et Android. Il est important de configurer des **comptes super-utilisateurs** afin de pouvoir accéder aux documents lorsqu'un utilisateur quitte l'entreprise. La liste des types de renseignements de nature délicate s'allonge de plus en plus et il est maintenant possible de personnaliser les niveaux de confiance des règles, de copier les règles intégrées, de les personnaliser et de créer des dictionnaires de mots-clés plus grands (pour chaque mention d'une étiquette d'identification du personnel ou d'un numéro de dossier de patient).

Il est possible de **rédiger conjointement des documents protégés en temps réel** (avec prise en charge de la sauvegarde automatique!) et, dans les déploiements plus importants, vous pouvez utiliser des variables dans les règles MIP pour faciliter le marquage du contenu par application. Vous pouvez apposer des étiquettes (et éventuellement chiffrer des documents) sur des documents, des sites SharePoint en ligne et SharePoint et des partages de fichiers sur site. Vous pouvez également numériser des images à l'aide de la fonction de **reconnaissance optique de caractères (ROC)** pour capturer des renseignements de nature délicate dans des captures d'écran et autres.

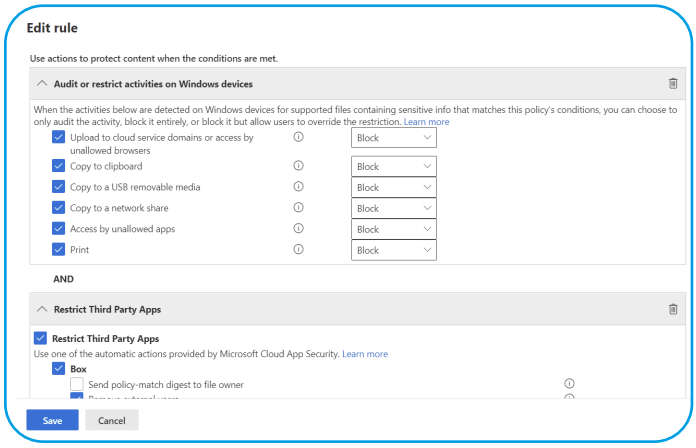
Les étiquettes de confidentialité sont maintenant également disponibles pour **les sites SharePoint**, **les groupes M365 et Teams**. Cela ne s'applique pas au contenu stocké dans ces emplacements, mais plutôt à la gestion de la confidentialité du contenant, de l'accès des utilisateurs externes et peut également s'intégrer aux stratégies d'accès conditionnel pour bloquer l'accès à partir d'appareils non gérés, par exemple. Vous pouvez toutefois configurer une **étiquette de confidentialité par défaut pour un site SharePoint.**

14.5: OFFICE 365 MESSAGE ENCRYPTION

De la même façon que MIP vous permet de partager des documents protégés avec n'importe qui, vous pouvez utiliser **O365 Message Encryption** pour envoyer des courriels à un destinataire et savoir que seule cette personne peut y accéder. Comme MIP, vous pouvez également établir des règles pour que les courriels contenant des renseignements précis (numéros de carte de crédit, numéros de sécurité sociale) soient automatiquement chiffrés.

14.6: DATA LOSS PREVENTION (PRÉVENTION DE LA PERTE DE DONNÉES)

L'objectif de **Data Loss Prevention (DLP)** est d'aider les utilisateurs à faire ce qu'il faut en les alertant lorsqu'ils sont sur le point de partager des données de nature délicate par courriel, SharePoint Online, OD4B ou Teams. Il peut également être intégré à MIP, car Microsoft poursuit les efforts d'unification de l'étiquetage et de la protection dans M365. La protection DLP a été étendue à Windows 10 et 11 avec **Endpoint DLP**, permettant ainsi de bloquer le téléchargement de documents avec du contenu de nature délicate vers le stockage en nuage, de copier des renseignements de nature délicate vers le presse-papiers, un support de stockage USB, les portails de partages réseau ou d'impression. Il y a également une extension pour Google Chrome qui étend la protection DLP aux tâches du navigateur. La protection DLP a également **été étendue sur le site** en utilisant MIP Scanner (Numériseur MIP) pour trouver des documents de nature délicate. La gestion des alertes pour les violations de DLP est également grandement améliorée.

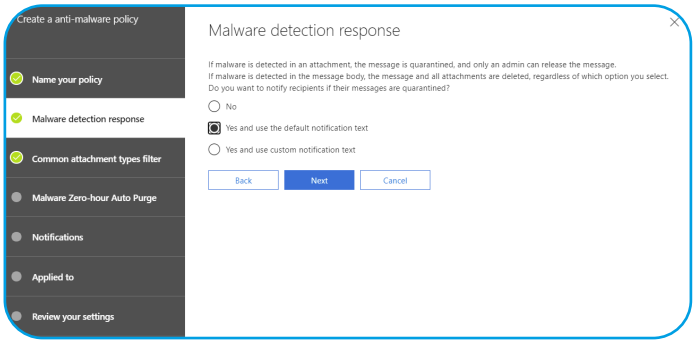


Paramètres DLP des points de terminaison

14.7: EXCHANGE ONLINE PROTECTION

Exchange Online Protection (EOP) est la solution d'hygiène de courrier pour Office 365 et peut également protéger vos boîtes aux lettres Exchange sur site si vous utilisez un mode de déploiement hybride (chapitre 8). Il y a quelques paramètres que vous pouvez contrôler pour EOP ainsi qu'une configuration supplémentaire que vous devriez envisager pour une protection complète contre les pourriels, comme **Sender Policy Framework** (SPF), **Domain-based Message Authentication, Reporting, and Conformance (DMARC)** et **Domain Keys Identified Mail** (DKIM).

Si vous constatez que l'EOP ne détecte pas suffisamment de courriels malveillants, considérez les services de tiers. Hornetsecurity offre un outil gratuit appelé **Threat Monitor** (qui n'exige aucun changement à vos enregistrements MX) qui identifiera les courriels publicitaires (pourriels), menaces et courriels de menaces avancées et vous permet également de les supprimer des boîtes aux lettres des utilisateurs. La surveillance des menaces fournit à votre locataire de précieuses données statistiques par courriel sur ce qui manque dans l'EOP, ce qui facilite la mise à niveau des services d'hygiène des courriels.



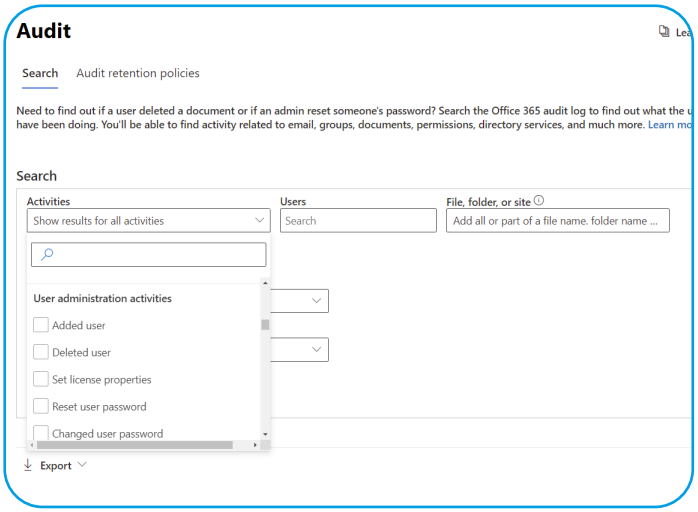
14.8: DEFENDER FOR OFFICE 365

Les **protections** Defender pour O365 (disponibles dans O365 E5 ou sous forme de modules d'extension autonomes) s'ajoutent à EOP et vous offrent l'outil **Safe Attachments** qui permet d'ouvrir les fichiers joints des courriels entrants qui pourraient être malveillants dans une machine virtuelle et de les analyser avant qu'ils soient livrés aux utilisateurs finaux. **Safe Links** vérifie que les liens dans les courriels et les fichiers Office ne sont pas malveillants au moment où les utilisateurs cliquent sur ces liens. **Anti-phishing (logiciel anti-hameçonnage)** détecte les tentatives d'usurpation d'identité d'utilisateurs. Ces mesures de protection s'appliquent également à SharePoint, OD4B et Teams.

Si vous trouvez Defender pour Office 365 trop cher (il est inclus dans M365 E5, E5 Security ou dans un module d'extension distinct), jetez un coup d'œil sur le produit **Hornetsecurity 365 Total Protection** en versions Business et Enterprise. La version Business vous donne un contrôle granulaire des catégories et du contenu des courriels afin que vous puissiez bloquer les courriels indésirables. Vous pouvez configurer les signatures de courriel avec les avis de responsabilité de l'entreprise et utiliser la norme PGP ou S/MIME pour le chiffrement des courriels, avec fonction de gestion de certificat intégrée. La version Enterprise offre également les fonctions suivantes : archivage et tenue de journal des courriels avec une période de conservation de jusqu'à dix (10) ans; eDiscovery (preuve électronique) et analyse des pièces jointes en bac à sable; réécriture et numérisation des adresses URL (dans les courriels et les pièces jointes) et couverture d'urgence au moyen d'un environnement de basculement des courriels en cas de dysfonctionnement de Microsoft 365.

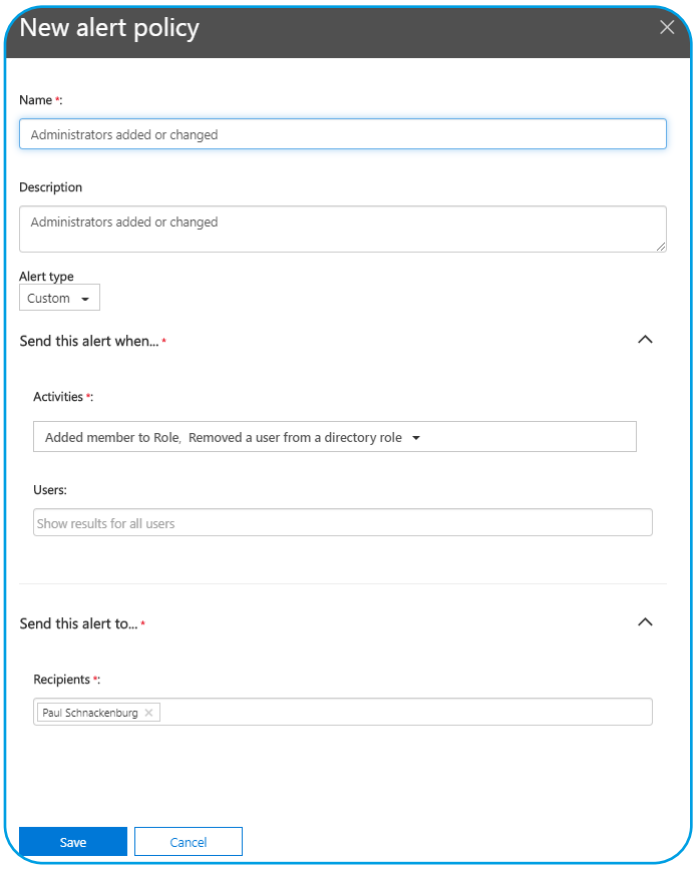
14.9: AUDIT

L'une des fonctionnalités intéressantes de la plateforme unifiée d'Office 365 est la possibilité de **vérifier les actions des utilisateurs et des administrateurs** sur l'ensemble de la plateforme.



Recherche dans le journal d'audit

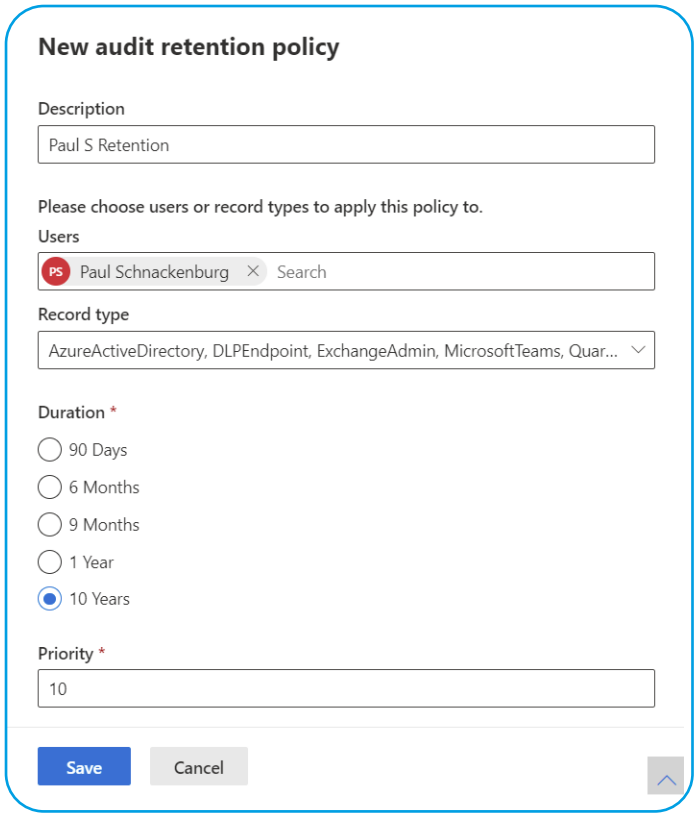
Vous devez au minimum **configurer les alertes** sur les actions d'Entra ID, accéder au portail Compliance – Search – Audit log search (Conformité – Rechercher – Recherche dans le journal d'audit) et voir toutes les différentes activités que vous pouvez vérifier et signaler, ainsi que **définir des stratégies d'alerte** connexes.



Creating an Alert policy

Par défaut, les journaux d'audit d'Office 365 sont conservés pendant 180 jours (les journaux Entra ID pendant 30 jours), ce qui peut ne pas être suffisant pour votre entreprise ou les règlements que vous devez respecter.

Vous avez deux options : utiliser un service tiers pour exporter continuellement les journaux et les archiver pendant la période requise, ou attribuer des licences M365 E5 (ou Conformité / Découverte et audit M365 E5) aux utilisateurs dont vous souhaitez conserver les journaux plus longtemps. Cela permet de conserver les journaux pendant des durées d'un (1) ou dix (10) ans.



Stratégie de conservation des audits

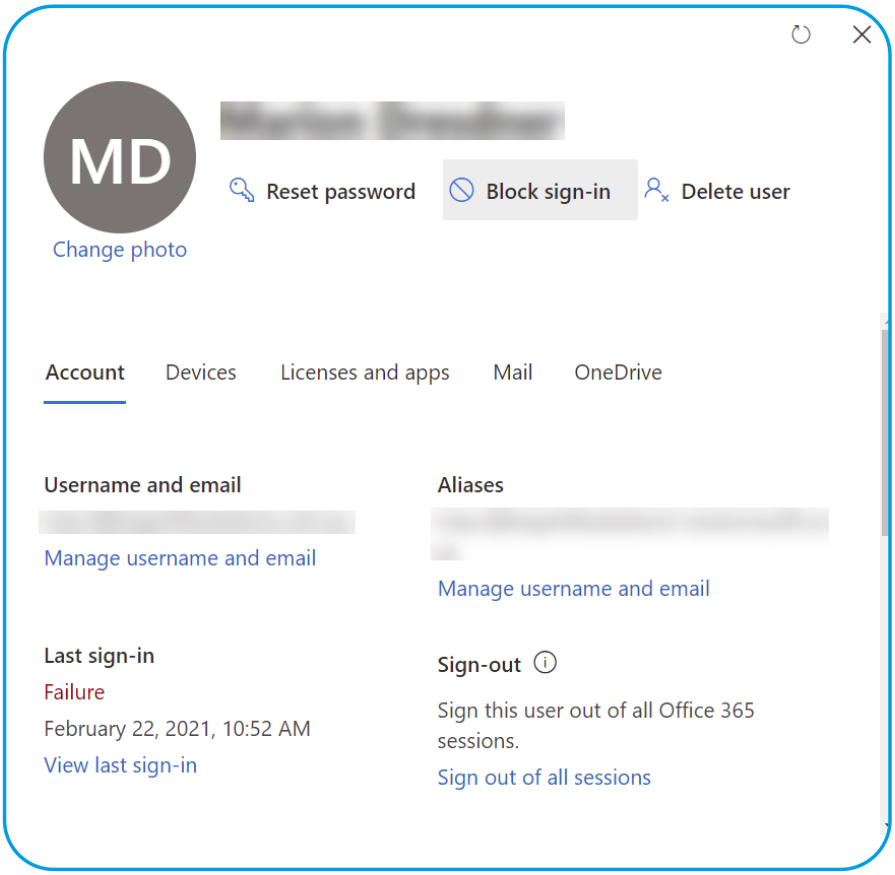
14.10: VOULEZ-VOUS DIRE ADIEU AUX MOTS DE PASSE?

En définitive, la meilleure façon de gérer les mots de passe est de ne pas les stocker dans votre répertoire et de ne pas les faire utiliser par vos utilisateurs – c'est ce qu'on appelle la méthode de connexion sans mot de passe. Il y a **de nombreuses étapes à franchir pour atteindre cet objectif final**. Aujourd'hui, vous pouvez utiliser l'application Authenticator pour ouvrir une session dans un compte Azure AD (pas comme deuxième facteur, mais comme facteur unique), Windows Hello Entreprise ou une clé USB/NFC de type FIDO 2.

Entre-temps, activez la **protection par mot de passe** pour interdire les mots de passe couramment utilisés (2 000 dans une liste tenue à jour par Microsoft et jusqu'à 1 000 mots personnalisés courants dans votre organisation/ville/équipes sportives). Cette méthode fonctionne sans problème pour les comptes en nuage seulement et peut facilement **être étendue aux AD sur site.** Lorsque vous demandez à vos utilisateurs de s'inscrire à l'authentification multifactorielle, ils s'inscrivent également au service de réinitialisation du mot de passe en libre-service **en même temps**.

14.11: BLOQUER L'ACCÈS DES UTILISATEURS

Si vous soupçonnez ou confirmez qu'un compte d'utilisateur a été compromis, la première étape devrait être de désactiver la fonction d'ouverture de session du compte dans le centre d'administration.
Vous devez toutefois savoir que l'utilisateur (ou le pirate) n'est pas immédiatement déconnecté des services auxquels il accède, et qu'il peut s'écouler jusqu'à une heure avant que le compte ne soit effectivement bloqué, en raison de la durée de vie des jetons d'actualisation. La solution à ce problème est l'**évaluation de l'accès continu** qui, aujourd'hui, s'applique uniquement à la connectivité en ligne Exchange, Teams et SharePoint et bloquera l'accès en temps quasi réel (temps de latence allant parfois jusqu'à 15 minutes en raison de la propagation des événements).



Bloquer l'ouverture de session pour un compte d'utilisateur

CHAPITRE 15:

SÉCURITÉ DANS MICROSOFT 365

DE NOMBREUX OUTILS DE SÉCURITÉ SONT INTÉGRÉS À LA PLATEFORME OFFICE 365, MAIS LORSQUE VOUS PASSEZ À M365 E3 OU E5, VOUS DÉVERROUILLEZ UN TOUT NOUVEL ENSEMBLE DE FONCTIONS AVANCÉES POUR SÉCURISER LES DONNÉES DE VOTRE ENTREPRISE. DANS CE CHAPITRE, NOUS EXAMINERONS CES OUTILS, À L'EXCEPTION DE ENDPOINT MANAGER, QUE NOUS ABORDERONS DANS LE CHAPITRE SUIVANT, ET DE WINDOWS 11, QUE NOUS AVONS ABORDÉ DANS LE CHAPITRE 6.

15.1: MICROSOFT 365 DEFENDER

Presque tous les produits de sécurité axés sur M365 de Microsoft ont la marque Defender, et la console centrale avec laquelle travailler est security.microsoft.com. Vous trouverez ici un service complet Extended Detection and Response (XDR) qui recueille des données à partir des courriels, de l'identité, des points de terminaison, des services infonuagiques et des alertes que vous envoyez aux intrus dans l'ensemble de votre domaine numérique M365.

Voici un aperçu des différents services de Defender :

- **Microsoft Defender pour Office 365** – Offre une protection pour les courriels, les sites SharePoint, OD4B et Teams
- **Microsoft Defender for Identity** – Permet de surveiller votre Active Directory (AD) sur site, de l'intégrer à votre outil Security Information and Events Management (SIEM) et de vous avertir des brèches de compte, des mouvements latéraux et des attaques ciblant les AD
- **Microsoft Defender for Endpoint** – Gestion centralisée des logiciels malveillants sur tous les points de terminaison de votre environnement (Windows, Linux, macOS, Android et iOS)
- **Microsoft Defender for Cloud Apps** – Un courtier en sécurité des applications infonuagiques (CASB), qui ajoute des fonctions correspondant au mot le plus à la mode, **Gestion de la posture de sécurité des applications SaaS.**

Microsoft offre également Microsoft Sentinel – un SIEM sur le nuage; Microsoft Defender pour le nuage (pour les charges de travail Azure, AWS et GCP IaaS et PaaS) et Entra pour la gestion et la protection des identités.

15.2: MICROSOFT DEFENDER FOR ENDPOINT

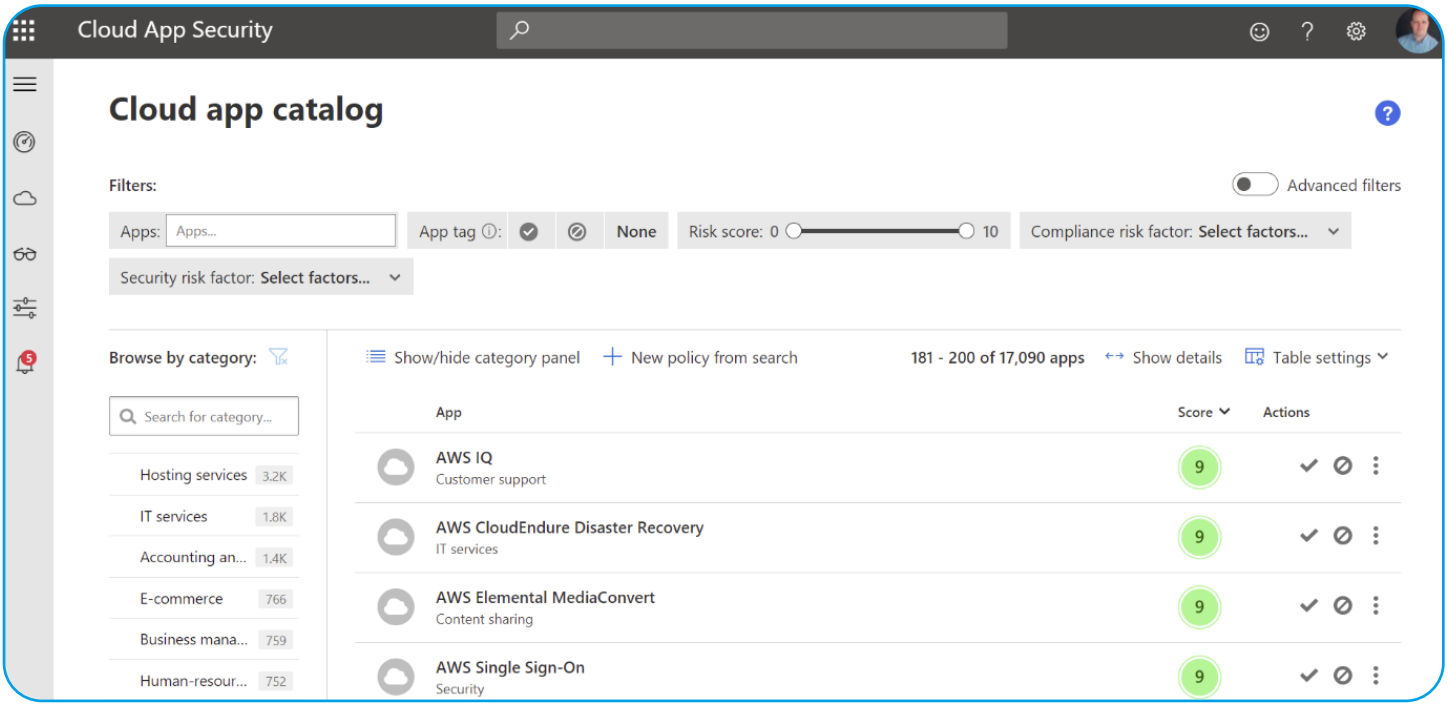
Microsoft Defender for Endpoint (MDE) est une solution de sécurité Endpoint Detection and Response ou EDR (Détection et réponse des points de terminaison) complète qui utilise l'analyse comportementale de l'apprentissage machine pour Windows, MacOS, les serveurs Linux, iOS et les appareils Android. Il établit la liste des applications installées (Windows et MacOS) et, grâce à **Gestion des menaces et des vulnérabilités (TVM)**, classe par ordre de priorité les applications qui présentent les risques les plus graves pour votre organisation en fonction de l'étendue du déploiement de chaque application et de la gravité de la vulnérabilité divulguée. MDE fournit également des **règles de réduction de la surface d'attaque** et une **protection de nouvelle génération**, ainsi que de nombreuses autres fonctions de sécurité. MDE est disponible avec M365 E5 / E5 Security ou sous forme de licence autonome.

15.3: MICROSOFT DEFENDER FOR IDENTITY

Avec M365 E5, vous pouvez passer à **Defender for Identity (MDI)**, qui surveille vos contrôleurs de domaine Active Directory, et vos serveurs Active Directory Federation avec seulement des agents légers, le reste est pris en charge par le service infonuagique. Tout pirate qui prend le contrôle d'un appareil de votre réseau doit toucher l'AD pour se déplacer latéralement et transmettre les privilèges à un échelon supérieur, et MDI l'attrapera lorsqu'il le fera.

15.4: MICROSOFT DEFENDER FOR CLOUD APPS

À une certaine époque, lorsque vos utilisateurs restaient au bureau de l'entreprise, tout ce dont vous aviez besoin pour les protéger était un bon pare-feu, mais dans le monde d'aujourd'hui où vous « travaillez n'importe où, sur n'importe quel appareil », vous avez besoin d'un nouveau type d'outil pour les protéger, un courtier en sécurité d'accès infonuagique. Microsoft Defender for Cloud Apps (MDA) fait partie de M365 E5 et protège vos utilisateurs en temps réel lorsqu'ils accèdent aux services infonuagiques. Le catalogue de plus de 31 000 services infonuagiques différents donne aux TI un moyen de découvrir et de gérer Shadow IT (services infonuagiques que les utilisateurs ont fournis sans que le service de TI le sache) dans l'ensemble de votre base d'utilisateurs.



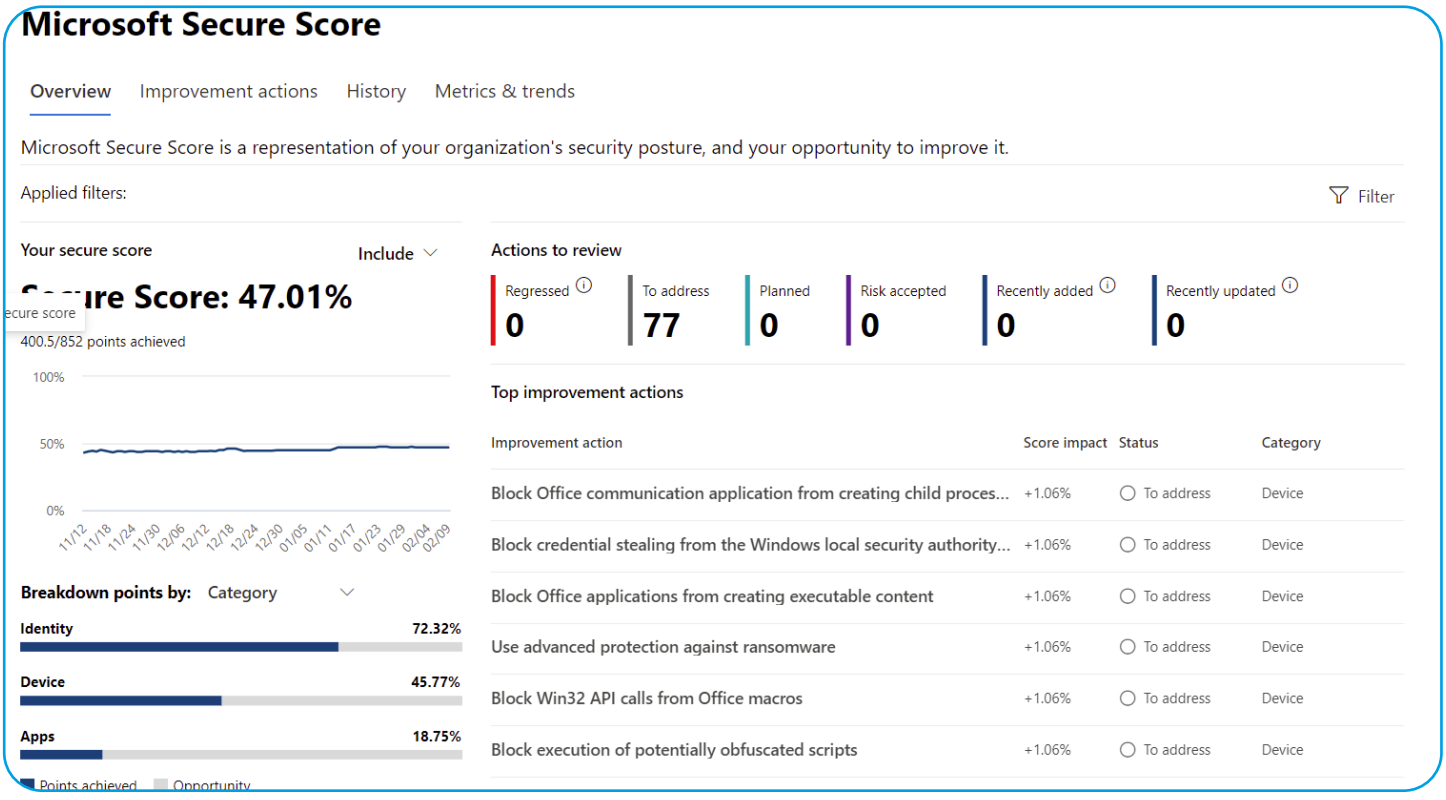
Catalogue SaaS de sécurité des applications infonuagiques

15.5: NOTE DE SÉCURITÉ

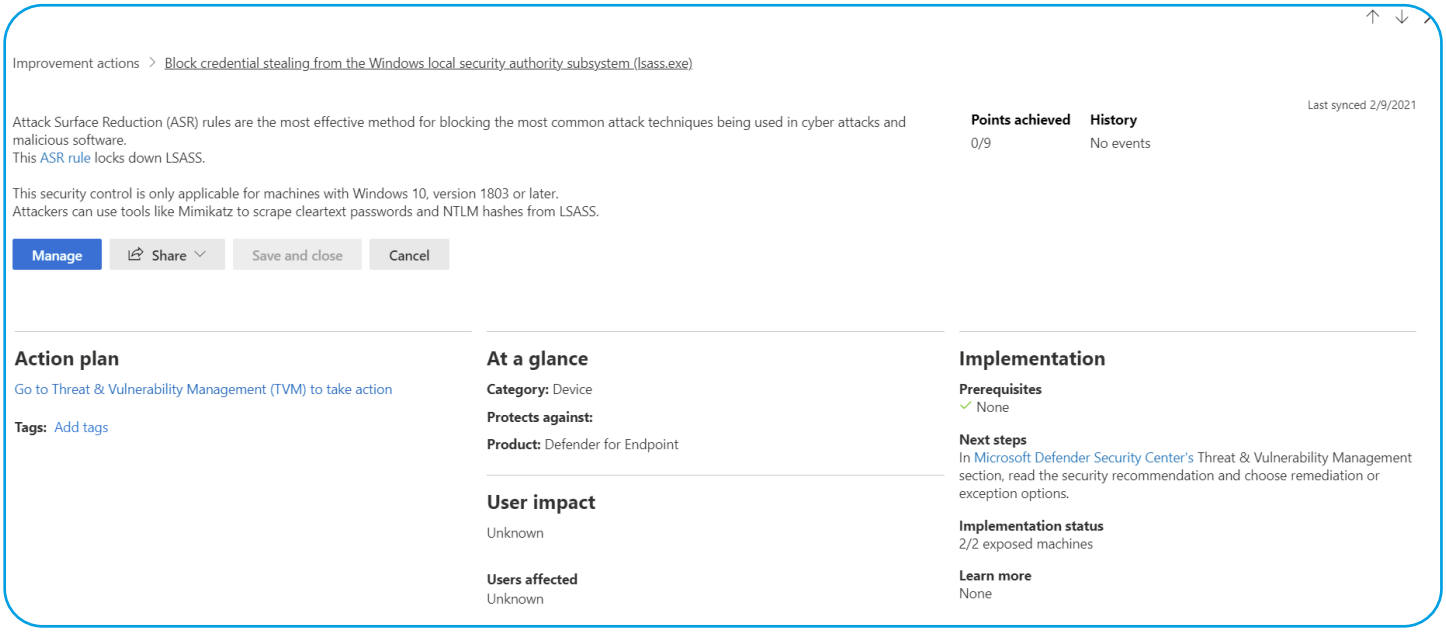
Dans le dernier chapitre et celui-ci, nous avons examiné bon nombre des contrôles de sécurité que vous pouvez utiliser. Mais par où commencer? Comment savoir ce qui est le plus important à surveiller? Et où, dans tous les portails (ou PowerShell), faut-il aller pour configurer chaque réglage?

Les réponses à ces questions se trouvent dans la Note de sécurité, qui fait maintenant partie du **portail de sécurité**. Vous voyez ici une note globale pour votre locataire (pour les contrôles liés à l'identité, aux données, aux appareils, aux applications et à l'infrastructure) et vous pouvez la comparer à la moyenne mondiale pour M365, la moyenne pour votre industrie et pour des entreprises de même taille. Dans le deuxième onglet, vous pouvez voir les mesures que vous devriez prendre pour améliorer votre note, le nombre de points que chaque action vous donnera, l'incidence sur l'utilisateur et l'effort administratif requis.

Le fait de cliquer sur une action fournit des détails sur les risques que le contrôle atténue, la réglementation de conformité à laquelle il correspond, la possibilité de cliquer sur un bouton pour aller directement au bon endroit pour la configurer et l'option de dire au système que vous avez déjà atténué ce risque avec un service tiers.



Aperçu de la note de sécurité



Exemple d'action pour améliorer votre sécurité

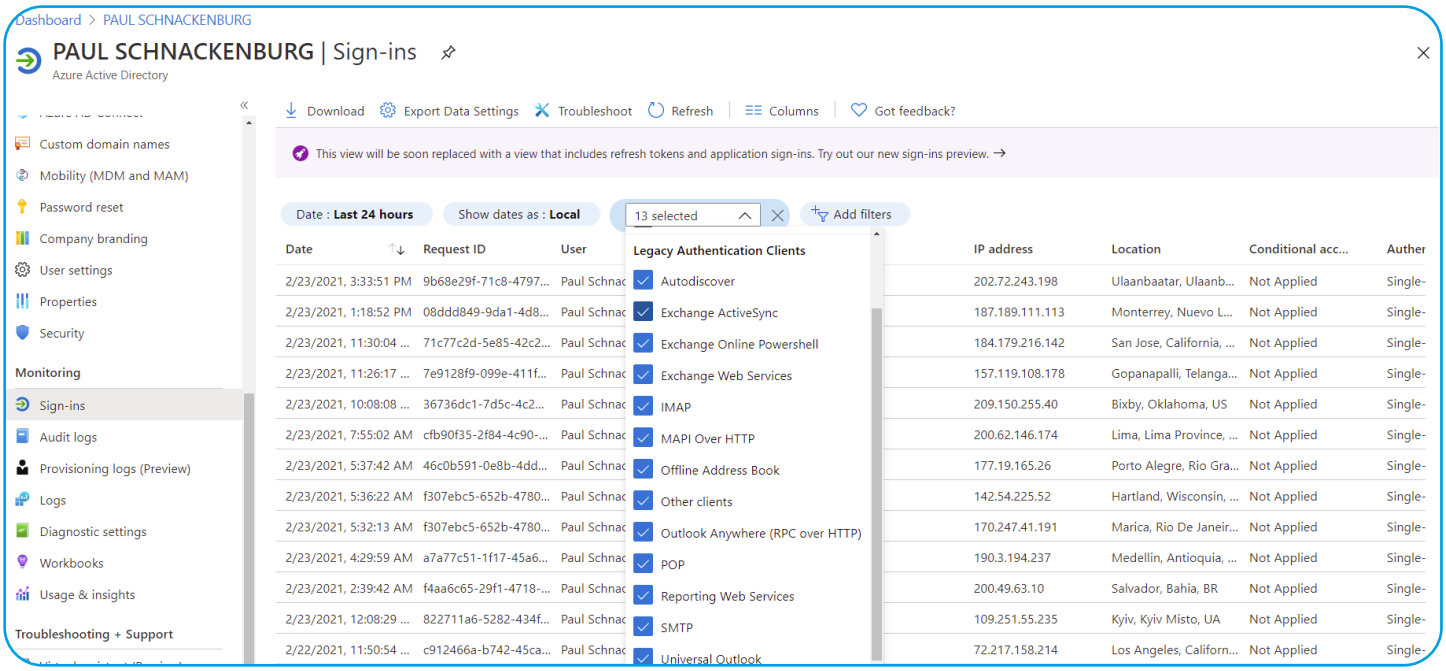
À mesure que vous mettez en œuvre d'autres dispositifs de contrôle, votre note augmente (cela peut prendre de 24 à 48 heures) et vous faites le suivi de vos progrès dans l'onglet History (Historique). La section Note de sécurité est le MEILLEUR endroit pour commencer à améliorer la posture de sécurité de votre locataire.

J'aimerais souligner un autre dispositif de contrôle (à l'exception de l'authentification multifactorielle) qui vous permettra d'améliorer rapidement la sécurité globale – **le blocage de l'ancienne méthode d'authentification.** En effet, même si vous avez activé l'authentification multifactorielle, les attaquants peuvent toujours accéder aux comptes de votre utilisateur avec simplement un nom d'utilisateur et un mot de passe au moyen d'anciens protocoles qui ne prennent pas en charge l'authentification multifactorielle. Pour vérifier s'il y a des connexions légitimes utilisant ces anciens protocoles (qui devront être mis à niveau ou exemptés de votre stratégie de blocage de l'ancienne authentification), accédez au portail AD Azure, cliquez sur « Sign-ins » (Ouvertures de session) sous « Monitoring » (Surveillance), cliquez sur « Add filters » (Ajouter des filtres), sélectionnez l'application client, puis cliquez sur « None selected » (Aucune sélectionnée) et ajouter les 13 options de connexion existantes.

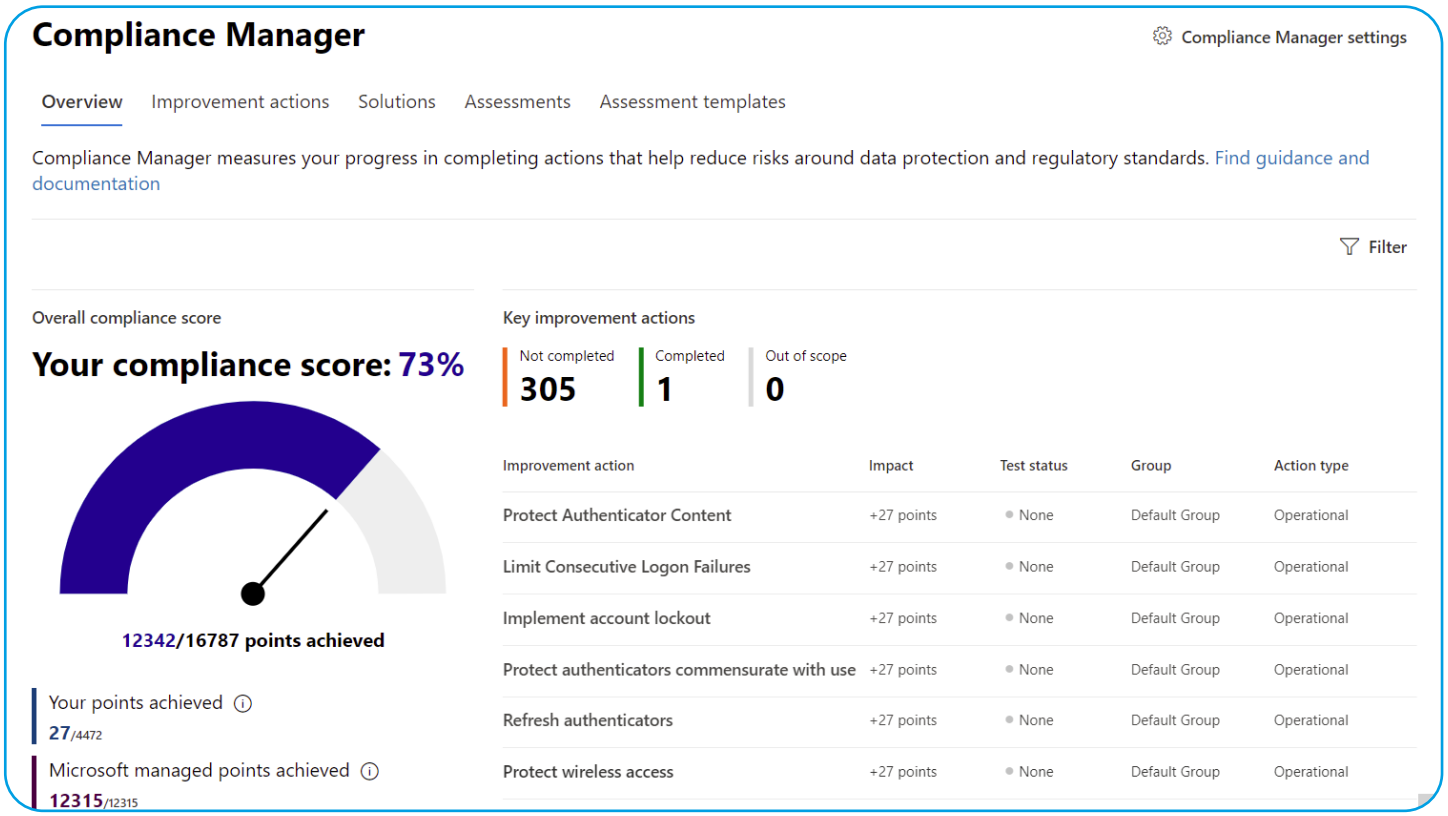
Ici, vous pouvez voir un locataire dont l'authentification multifactorielle est activée, mais dont l'ancienne authentification est toujours activée avec de nombreuses tentatives d'accès échouées.

Une fois que vous êtes certain qu'il n'y a pas de besoins légitimes pour l'ancienne méthode d'authentification, utilisez **les stratégies d'AC pour la bloquer.**

Le concept de Note de sécurité s'est propagé à d'autres parties de M365, dans le **Compliance Manager.** Il y a une note de conformité pour indiquer dans quelle mesure votre entreprise est conforme aux cadres réglementaires que vous devez respecter. Microsoft a récemment ajouté des centaines de règlements supplémentaires de partout dans le monde pour vous aider à faire le suivi de votre conformité, à assigner des tâches aux utilisateurs pour atteindre et maintenir la conformité.



Tentatives de connexion à Entra ID au moyen de l'ancienne méthode d'authentification



Note de conformité dans Compliance Manager

Gérer la conformité pour vos sites SharePoint et OneDrive et leur posture de sécurité ou leurs paramètres de partage à l'aide des outils intégrés est un exercice frustrant, car ils sont répartis sur plusieurs portails. En revanche, Hornetsecurity **365 Permission Manager** offre un seul volet pour voir les paramètres de chaque site de votre locataire, appliquer les stratégies, corriger les cas de violation de la conformité, voir tous les accès d'un utilisateur particulier, produire des rapports et plus encore.

15.6: LA SÉCURITÉ EST LA RESPONSABILITÉ DE TOUS

Les deux derniers chapitres vous ont donné un aperçu de haut niveau des nombreuses fonctions de sécurité disponibles dans M365. La triste vérité est que la plupart des petites et moyennes entreprises ne déploient pas suffisamment les fonctions pour lesquelles elles ont déjà payé et que même les grandes entreprises ont du mal à mettre en place ces protections pour tous leurs utilisateurs.

Cela est dû en partie à la complexité inhérente de nombreuses fonctions de sécurité natives de Microsoft – rappelez-vous le dicton : « La complexité est l'ennemi de la sécurité. » C'est pourquoi de nombreuses organisations se tournent vers des solutions de sécurité tierces comme Hornetsecurity pour les aider à rendre les principales fonctions de sécurité plus accessibles et à réduire la complexité.

D'autre part, la négligence à l'égard de la sécurité est également due à une certaine insouciance, qui découle du fait que dans de nombreuses entreprises, l'état d'esprit de l'époque « sur site » prévaut toujours. En effet, on pensait que (presque) tout était déjà fait avec un pare-feu – et les services de TI s'en occuperont.

Le monde d'aujourd'hui est différent : nous devons comprendre que la responsabilité de la sécurité est entre nos mains à tous et que notre chaîne de cyberdéfense ne peut être aussi solide que son maillon le plus faible.

Envisager une formation de sensibilisation à la sécurité pour les employés puisqu'il est essentiel de réduire le risque de cyberattaques, de prévenir les atteintes à la sécurité des données et d'assurer la conformité aux règlements. Cette formation permet aux employés de reconnaître les menaces à la sécurité et d'y réagir, ce qui favorise une solide culture de cybersécurité et protège les actifs et la réputation de l'entreprise. Au bout du compte, investir dans la formation de sensibilisation mène à des économies et à un environnement numérique plus sûr.

15.7: GARDER MICROSOFT HONNÊTE

Si l'idée de payer pour la plateforme sous-jacente à partir de Microsoft, puis d'acheter de nouveau des fonctions de sécurité supplémentaires en plus, ne vous convient pas, envisagez une solution tierce pour vos besoins de sécurité et de conformité M365. Hornetsecurity offre **plusieurs plans différents** avec la puissante solution Advanced Threat Protection pour vos courriels, la prévention des pertes de données (DLP), un service de sensibilisation à la sécurité (simulation d'hameçonnage et formation de l'utilisateur final), le chiffrement des courriels, l'archivage des courriels et plus encore.

Hornetsecurity offre également un livre électronique gratuit complet axé sur la sécurité d'un locataire Microsoft 365, **La liste de vérification de sécurité de Microsoft 365**. Il couvre tous les paramètres de sécurité et les configurations que vous devez connaître pour chaque licence M365 afin de sécuriser correctement votre environnement et donne plus de détails sur les paramètres réels que ceux décrits ici.

CHAPITRE 16:

SAUVEGARDE DANS MICROSOFT 365

DANS CE CHAPITRE, NOUS EXAMINONS LA NÉCESSITÉ DE PROTÉGER LES DONNÉES DANS MICROSOFT 365 – CE DONT MICROSOFT EST RESPONSABLE – ET CE DONT VOTRE ORGANISATION EST RESPONSABLE.

16.1: RÉSILIENCE DES DONNÉES NATIVES

Comme tout service infonuagique, Microsoft prend très au sérieux la disponibilité des données des clients dans M365. Comme nous l'avons déjà mentionné, **les boîtes aux lettres Exchange ont quatre copies**, trois à jour et une quatrième différée (24 heures de retard). Cette dernière copie est utilisée en cas de corruption systémique des trois autres copies. Ces quatre copies sont distribuées dans au moins deux centres de données. Tout cela est traité automatiquement par le système, et ce n'est pas quelque chose que les utilisateurs finaux remarqueront.

De même, le stockage de SharePoint et de OneDrive Entreprise r**epose sur le stockage de données dans deux régions Azure distinctes** – une écriture ne sera considérée comme terminée que si elle est correctement rédigée pour les deux régions. Et le stockage sous-jacent utilise Append-Only, garantissant que les données antérieures ne peuvent pas être corrompues ou chiffrées par un pirate. Ce système de version permet également de restaurer les versions précédentes des fichiers.

Ça semble bien, n'est-ce pas? Microsoft prend clairement des mesures pour protéger mes données, alors je n'ai pas à m'en inquiéter? Pas si vite – tout ce qui est décrit ci-dessus concerne la résilience des données et la grande disponibilité de vos données. Ce qu'il ne fournit pas, en dehors de certaines options limitées, c'est une sauvegarde de vos données.
Les sauvegardes sont des copies de vos données de production, dans un système distinct, qui sont régulièrement (toutes les heures, tous les jours) copiées des données de production vers l'emplacement de sauvegarde. Elles offrent les fonctions suivantes :

- La capacité de « revenir en arrière » et de rétablir les courriels, les documents, les boîtes aux lettres et les emplacements à un point antérieur dans le temps – soit à un lieu de production, soit à un emplacement d'exportation distinct.

- La possibilité d'accéder à vos données de production en cas de défaillance grave ou de panne de services dans Microsoft 365.

Autrement dit, la résilience des données et la haute disponibilité ne sont pas la même chose que la sauvegarde. Elles sont liées, mais servent à des fins différentes. Selon les besoins de votre entreprise ou les règlements de conformité que vous devez respecter, vous pourriez avoir besoin des deux.

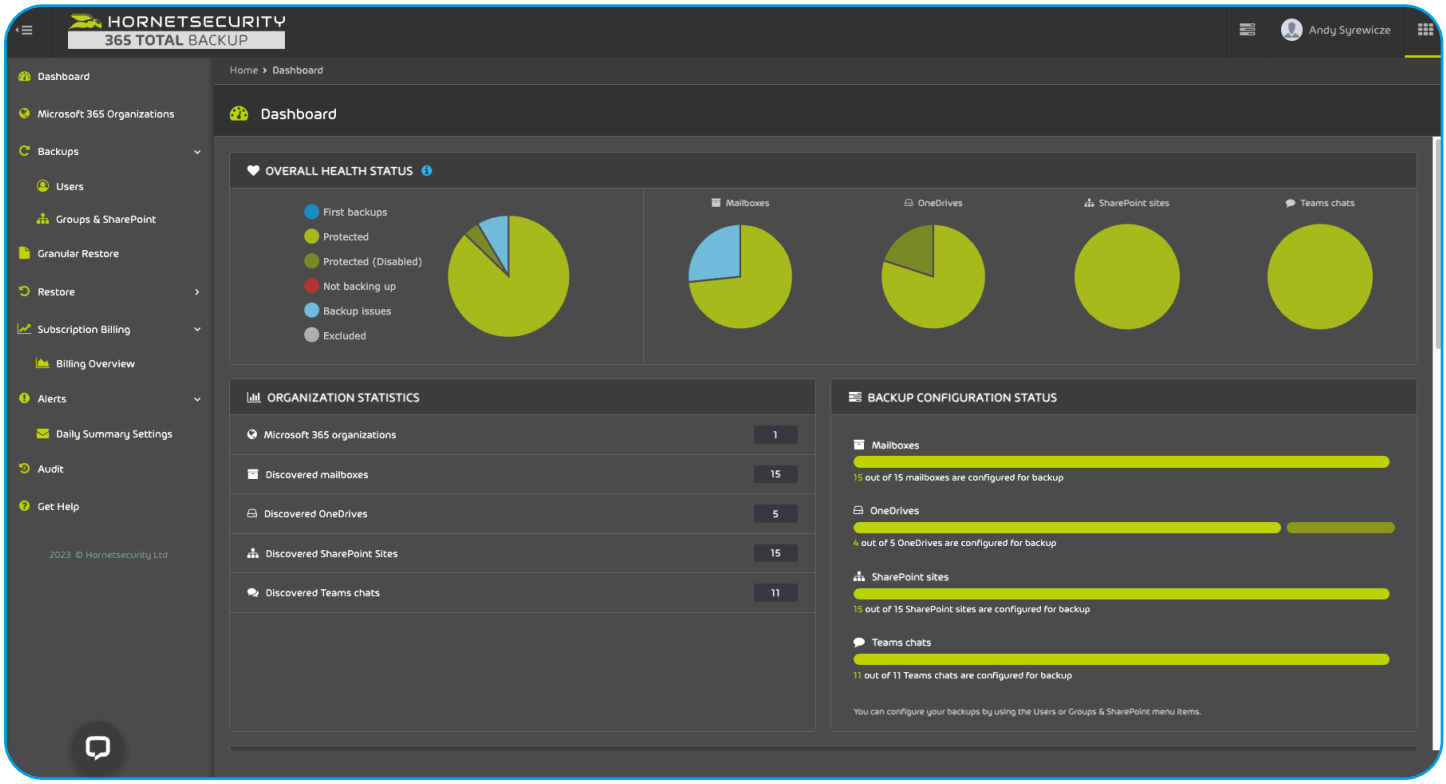
Examinons vos options natives pour restaurer les versions antérieures des données. Une fois les **Exchange items – Éléments Exchange** (emails, contacts, calendar appointments – courriels, contacts, rendez-vous du calendrier) supprimés, vous pouvez les récupérer du dossier Outlook Deleted Items (Éléments supprimés d'Outlook). Ces éléments y sont conservés **pendant une durée indéfinie**, à moins que vous ne changiez la stratégie de votre locataire. S'ils sont supprimés du dossier Éléments supprimés, vous pouvez les récupérer dans un délai de jusqu'à quatorze (14) jours à partir du dossier Recoverable Items (Éléments récupérables) masqué. Vous devrez former vos utilisateurs sur la façon de le faire eux-mêmes, ou vous assurer que votre équipe du service d'assistance est prête à vous aider régulièrement, car l'interface utilisateur n'est pas vraiment intuitive.

Dans SharePoint/OneDrive for Business, les **documents supprimés** sont conservés par défaut pendant 93 jours, d'abord dans une corbeille accessible aux utilisateurs et, s'ils y sont supprimés, dans une corbeille accessible aux administrateurs. Encore une fois, le processus de restauration d'un document supprimé par erreur n'est pas simple et nécessitera donc une certaine formation.

Pour modifier les paramètres par défaut, vous pouvez utiliser les **Retention Policies (stratégies de conservation)** pour conserver les éléments plus longtemps (ils peuvent être restaurés, même si les utilisateurs les suppriment de leur dossier Éléments supprimés). Celles-ci peuvent être appliquées aux données Exchange et SharePoint. Pour Exchange, vous utilisez également **In-Place and Litigation Holds (Scénarios de mise en attente et pour litige en place)** pour certaines boîtes aux lettres afin de gérer la conservation.

16.2: 365 TOTAL BACKUP

Si vous souhaitez réduire les difficultés liées à l'utilisation des fonctions de protection des données intégrées comme solution de récupération, Hornetsecurity offre une solution complète de sauvegarde et de récupération M365 **365 Total Backup** ou comme module du produit **365 Total Protection Compliance & Awareness**. Cette solution protège les boîtes de courriel, le clavardage Teams, le stockage OneDrive pour les entreprises, les sites SharePoint et les points de terminaison Windows. Elle est simple à installer et offre une protection complète à l'ensemble de votre locataire.



N'ARRÊTEZ JAMAIS D'APPRENDRE!

Nous espérons que ce livre et ses liens vers des renseignements techniques plus approfondis vous ont aidé à explorer l'univers du nuage. Une fois que vous aurez migré, l'exploration se poursuit, car la gestion du paysage en constante évolution de M365 est un parcours sans fin.

Comme nous l'avons mentionné dans la partie 1, se tenir au courant des dernières applications et fonctions de M365 est une tâche permanente. Vous devez donc consulter régulièrement les ressources officielles de Microsoft, mais n'oubliez pas de consulter le **blogue Hornetsecurity** pour lire nos articles sur l'administration et la sécurité de M365.

Si vous préférez avoir votre contenu en format audio ou vidéo, consultez la section **The Security Swarm Podcast** – Une tribune de conversation hebdomadaire sur les enjeux les plus critiques auxquels fait face le monde de la cybersécurité aujourd'hui, animée par Andy Syrewicze, évangéliste de la sécurité chez Hornetsecurity. De l'utilisation malveillante des outils d'intelligence artificielle aux arnaques d'ingénierie sociale, chaque épisode porte sur un sujet pertinent disséqué par un expert de l'industrie et étayé par des données réelles provenant directement de notre laboratoire de sécurité (Security Lab).

Bonne chance!

À PROPOS DE HORNETSECURITY GROUP

HORNETSECURITY

Hornetsecurity is a leading global provider of next-generation cloud-based security, compliance, backup, and security awareness solutions that help companies and organizations of all sizes around the world. Its flagship product, 365 Total Protection, is the most comprehensive cloud security solution for Microsoft 365 on the market. Driven by innovation and cybersecurity excellence, Hornetsecurity is building a safer digital future and sustainable security cultures with its award-winning portfolio.

Hornetsecurity operates in more than 30 countries through its international distribution network of 8,000+ channel partners and MSPs. Its premium services are used by more than 50,000 customers.

For more information, visit **www.hornetsecurity.com.**

À PROPOS DE L'AUTEUR

PAUL SCHNACKENBURG
FORMATEUR CERTIFIÉ DE MICROSOFT

Paul Schnackenburg, formateur certifié de Microsoft, a commencé sa carrière dans le secteur des TI lorsque le DOS et les processeurs 286 étaient à la fine pointe. Il dirige Expert IT Solutions, une petite entreprise de conseil en TI sur la Sunshine Coast, en Australie. Il travaille également comme professeur de TI dans une Microsoft IT Academy. Auteur de contributions sur les technologies très respecté, Paul est actif au sein de la collectivité et a rédigé des articles techniques approfondis sur Hyper-V, le System Center, le nuage privé et hybride, Office 365 et les technologies infonuagiques publiques Azure. Il détient les certifications MCSE, MCSA et MCT.

HORNETSECURITY | ited

365 TOTAL PROTECTION

PLAN 4 - COMPLIANCE & AWARENESS

PROTECTION DE NOUVELLE GÉNÉRATION POUR MICROSOFT 365 :
SÉCURITÉ DU COURRIER ÉLECTRONIQUE, SAUVEGARDE, CONFORMITÉ ET SENSIBILISATION À LA SÉCURITÉ

PLAN 1	PLAN 2	PLAN 3	PLAN 4		
BUSINESS	ENTERPRISE	BACKUP	COMPLIANCE & AWARENESS		
SPAM & MALWARE PROTECTION	ADVANCED THREAT PROTECTION	BACKUP & RECOVERY OF MAILBOXES & TEAMS	PERMISSION MANAGEMENT	PHISHING & ATTACK SIMULATION	COMMUNICATION PATTERN ANALYSIS
EMAIL ENCRYPTION	EMAIL ARCHIVING	BACKUP & RECOVERY OF ONEDRIVE & SHAREPOINT	PERMISSION ALERTS	SECURITY AWARENESS	AI RECIPIENT VALIDATION
EMAIL SIGNATURES & DISCLAIMERS	EMAIL CONTINUITY	BACKUP & RECOVERY OF ENDPOINTS	PERMISSION AUDIT	ESI® REPORTING	SENSITIVE DATA CHECK

365 Total Protection couvre tous les aspects de la gestion de la sécurité et de la protection des données de Microsoft 365 d'une organisation : sécurité du courrier électronique, sauvegarde et récupération, conformité, gestion des autorisations et sensibilisation à la sécurité. La solution s'intègre de manière transparente à Microsoft 365, fournissant des couches supplémentaires de sécurité et de protection des données contre le spam, les logiciels malveillants et les menaces avancées.

ESSAI GRATUITE