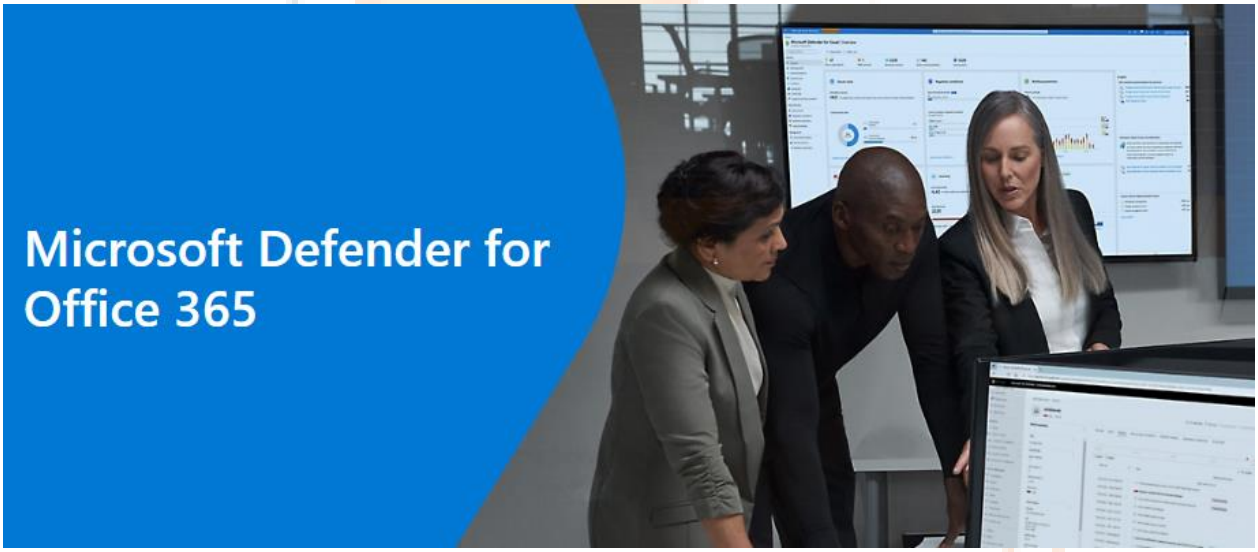
TECHNEWS

Octobre 2023 -Bulletin n°10

Nous avons le plaisir de partager avec vous notre 10ème Bulletin TECHNEWS de l'année 2023.
Ce bulletin, réalisé par notre équipe technique, contient les nouveautés de Microsoft, des astuces et des conseils qui vous seront bénéfiques.

Nous restons à votre entière disposition pour toute suggestion concernant le contenu de ce document

MICROSOFT DEFENDER FOR OFFICE 365



SOMMAIRE

Microsoft Defender pour Office 365

Dans l'ère numérique actuelle, où la connectivité et la collaboration en ligne sont cruciales pour les entreprises, la sécurité informatique revêt une importance capitale. Microsoft Defender pour Office 365 se positionne comme une forteresse essentielle dans la protection contre les menaces cybernétiques, fournissant une défense solide au cœur de l'écosystème Office 365. Cette solution avancée de sécurité, développée par Microsoft, est élaborée pour anticiper, repérer et contrer une diversité de menaces, procurant ainsi une tranquillité d'esprit aux organisations qui dépendent des services Office 365.

Microsoft Defender pour Office 365 représente un service de filtrage des courriels basé dans le cloud, conçu pour assister les organisations dans leur défense contre différentes formes de menaces en ligne, incluant les tentatives de phishing, les logiciels malveillants et d'autres activités néfastes. Son intégration fluide avec Office 365 offre une approche complète de la sécurité qui transcende les méthodes traditionnelles de protection des passerelles de messagerie. Cette plateforme est dotée d'une méthode proactive utilisant l'intelligence artificielle et des données en temps réel pour repérer et contrecarrer les menaces. Que ce soit face à des logiciels malveillants, des tentatives de phishing astucieuses, ou des liens frauduleux, Microsoft Defender pour Office 365 se positionne comme un rempart numérique exhaustif, offrant une protection complète aux organisations cherchant à sécuriser leurs communications et leurs données sensibles.

Les trois cas d'utilisation de Microsoft Defender pour Office sont :

- **Environnement de mails On Prem :** Cette solution se présente comme une ressource polyvalente, avec une utilisation principalement axée sur le filtrage. Son objectif principal est de renforcer la sécurité des solutions de messagerie SMTP sur site, telles que Microsoft Exchange Server. En adoptant cette approche, vous bénéficiez d'une protection dédiée tout en optimisant les performances globales de votre environnement de messagerie.
- **Boites mails sur le Cloud :** Cette solution se révèle être un outil polyvalent, avec un usage principalement dédié à la protection. Vous pouvez activer cette solution de manière spécifique pour sécuriser les boîtes aux lettres hébergées dans Microsoft Exchange Online. En intégrant cette solution à votre infrastructure, vous bénéficiez d'une protection ciblée et adaptée dans un environnement hébergé en ligne.
- **Déploiement Hybride :** Cette solution se distingue par sa polyvalence. Vous avez la possibilité de configurer cette solution de manière spécifique pour garantir la protection des environnements de messagerie tout en exerçant un contrôle sur le routage des courriels. Cela s'étend aussi bien aux boîtes aux lettres dans le cloud qu'à celles sur site, offrant une flexibilité complète pour répondre aux exigences spécifiques de votre infrastructure.

Les fonctionnalités Microsoft Defender pour Office 365

Prevention & Détection

Prévenir les attaques avant même qu'elles ne se déclenchent constitue la méthode la plus efficace pour garantir la sécurité. Microsoft Defender pour Office 365 utilise une intelligence artificielle de pointe pour repérer les contenus malveillants et suspects, en corrélant les modèles d'attaque afin d'identifier spécifiquement les campagnes conçues pour contourner les protections. Une robuste pile de filtrage bloque une vaste gamme d'attaques, qu'elles soient volumineuses ou ciblées, englobant des menaces telles que la compromission de messagerie professionnelle, le phishing d'informations d'identification, le ransomware, et les malwares sophistiqués.

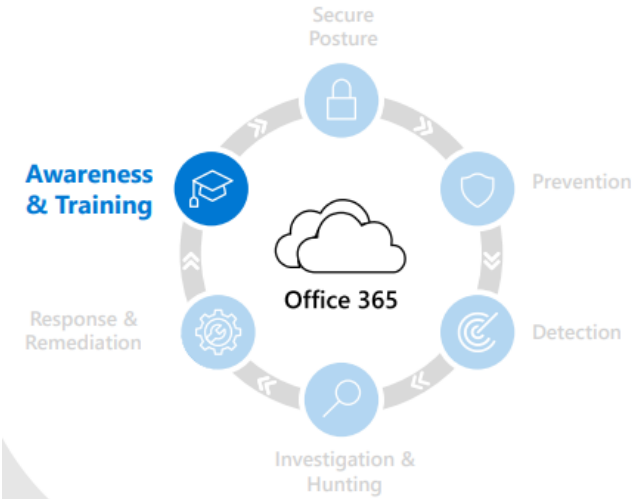
Enquête de Repérage

La proposition d'une vision approfondie du paysage des menaces avec Microsoft Defender pour Office 365. Ce puissant outil offre des expériences conçues pour faciliter l'identification, la priorisation et l'investigation des menaces, dotées de capacités avancées de chasse pour traquer les attaques au sein d'Office 365. Defender pour Office 365 joue également un rôle central dans la solution étendue XDR de Microsoft, connue sous le nom de Microsoft 365 Defender. Grâce à Microsoft 365 Defender, vos équipes de sécurité peuvent détecter les menaces et automatiser la réponse à travers différents domaines tels que la messagerie électronique, les points d'extrémité, l'identité, et les applications cloud.

Réponse & Correction

En matière de détection des menaces, la capacité à agir rapidement peut faire la différence entre une réponse efficace et une potentielle vulnérabilité. Avec Microsoft 365 Defender, non seulement vous bénéficiez de la détection précoce des menaces, mais vous pouvez également étendre vos capacités de réponse aux incidents grâce à des processus d'automatisation sophistiqués. Cette intégration de pointe offre la possibilité d'arrêter les attaques en utilisant des outils automatisés, créant ainsi un bouclier de sécurité inter-domaines.
Imaginez pouvoir non seulement identifier rapidement une menace, mais également déclencher automatiquement des contre-mesures, bloquer des attaques potentielles, et coordonner une réponse globale à travers divers domaines tels que la messagerie électronique, les points d'extrémité, l'identité, et les applications cloud. Cela ne se traduit pas seulement par une réactivité accrue, mais également par une efficacité opérationnelle renforcée au sein de votre équipe de sécurité. En automatisant certaines tâches répétitives et en assurant une coordination transparente des réponses, Microsoft 365 Defender optimise votre capacité à faire face aux menaces émergentes dans un environnement cybernétique en constante évolution.

Sensibilisation & Formation



Les membres de votre équipe constituent le périmètre vital de votre sécurité informatique. Au-delà de simplement sensibiliser, la formation à la simulation d'attaque offre une expérience immersive et des sessions de formation approfondies. Ces programmes sont minutieusement élaborés pour habiliter les utilisateurs à détecter les menaces potentielles en les confrontant à des scénarios réalistes de cyberattaques.

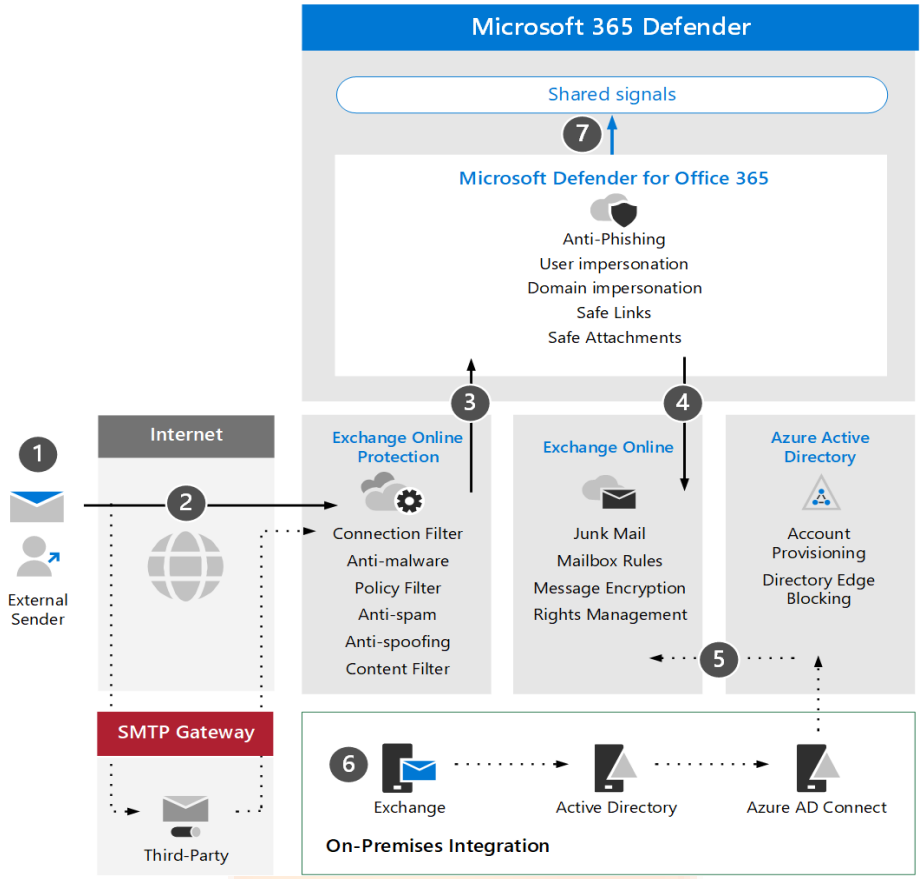
Les fonctionnalités intégrées au sein des applications client de Defender pour Office 365 jouent un rôle pivot dans ce processus de formation, construisant une sensibilisation proactive aux indicateurs clés d'activité suspecte. Cela va au-delà de l'information sur les menaces possibles, fournissant une formation concrète pour que les utilisateurs reconnaissent et réagissent de manière adéquate face à ces situations. Ces simulations offrent une compréhension approfondie des tactiques employées par les cybercriminels, renforçant ainsi la résilience de votre équipe contre les attaques potentielles.

Posture sécurisée

La simplicité, en tant que principe fondamental de votre stratégie de sécurité, apporte une valeur inestimable à la protection de votre environnement numérique. En choisissant délibérément une solution épurée, pourvue de conseils de configuration d'une clarté exceptionnelle et d'outils intuitifs, vous entreprenez une démarche proactive pour renforcer la robustesse de votre posture de sécurité. Ces conseils détaillés et ces outils conviviaux ne servent pas seulement à simplifier les processus, mais ils se révèlent également être des alliés puissants dans l'identification précise des éventuelles lacunes de couverture au sein de votre système.

En investissant dans une approche où la simplicité est privilégiée, vous créez un environnement sécurisé qui demeure à la fois efficace et exempt de complexités inutiles. L'objectif ultime est de vous armer contre les menaces potentielles tout en optimisant la gestion de la sécurité. En favorisant cette simplicité stratégique, vous établissez une base solide pour une défense proactive, vous permettant de naviguer avec confiance dans un paysage numérique en constante évolution.

Microsoft Defender pour Office 365 Workflow



1. Le serveur hôte de l'expéditeur se connecte au serveur de messagerie de votre organisation via Exchange Online (EXO) ou une passerelle SMTP qui relaie le trafic vers EXO.
2. Exchange Online Protection vérifie la connexion entrante, vérifie les en-têtes et le contenu des messages, et applique les stratégies et balises appropriées.
3. EXO utilise Microsoft Defender pour Office 365, fournissant des données sur le message entrant et recevant des recommandations pour une protection et une atténuation avancées des menaces.
4. Si le message n'est pas détecté comme malveillant, bloqué ou mis en quarantaine, il est remis à un destinataire EXO. À ce stade, les préférences de l'utilisateur concernant les filtres de boîte aux lettres, les règles et les courriers indésirables sont traitées.
5. EXO s'intégrer à Azure AD Connect et l'utiliser pour accéder aux domaines AD sur site, pour provisionner et synchroniser les objets et paramètres liés à la messagerie.
6. Dans un environnement sur site, Microsoft recommande de déployer Exchange Server pour gérer et administrer les attributs de messagerie d'Active Directory.
7. À la fin du processus, Microsoft Defender pour Office 365 partage les signaux de menace liés aux courriels avec la suite Microsoft 365 Defender pour permettre un

traitement plus large des événements et des incidents dans le cadre de la détection et réponse étendues (XDR) de Microsoft.

Microsoft Defender pour Office 365: Plans & Tarifs

Ce programme met l'accent sur la prévention, l'investigation et la réponse aux menaces au sein de l'environnement Office 365. Defender pour Office 365 offre une variété de niveaux de forfaits, souvent intégrés dans le type d'abonnement Microsoft que vous possédez.
Cependant, il est également possible de migrer indépendamment vers un autre plan Defender pour Office 365. Cette option s'avère particulièrement avantageuse pour les entreprises aux besoins spécialisés.
Il existe deux plans disponibles pour Defender pour Office 365 : le Plan 1 et le Plan 2.

Plan 1: Defender pour Office ($2.00 user/month)

Le Plan 1 pour Defender pour Office représente une avancée significative par rapport à l'EOP standard (ou Exchange Online Protection). Alors qu'EOP se concentre principalement sur la détection et la prévention de base des menaces, le Plan 1 va au-delà en amplifiant les capacités de prévention et de détection.

Les principales fonctionnalités intégrées dans le Plan 1 comprennent :

- Pièces jointes sécurisées : Defender peut désormais analyser rapidement les pièces jointes dans les communications entre les utilisateurs de votre organisation.
- Liens sécurisés : Defender peut utiliser la base de données de Microsoft pour tester les liens dans un environnement contrôlé et détecter toute activité suspecte.
- Pièces jointes sécurisées pour SharePoint, OneDrive, et Microsoft Teams : Le plan 1 protège les pièces jointes SharePoint, OneDrive et Microsoft Teams, contrairement à EOP, qui présente plus de limitations.
- Anti-hameçonnage dans la protection Defender pour Office : Il existe une couche supplémentaire de protection contre l'hameçonnage. Defender signale ou met en quarantaine les communications qui vous demandent de manière suspecte de fournir des informations.
- Détection en temps réel : La capacité de voir les menaces en temps réel permet l'intégration SIEM (Security Information and Events Management).

Plan 2: Defender pour Office ($5.00 user/month)

Le Plan 2 de Defender pour Office 365 englobe l'intégralité des fonctionnalités du Plan 1 et d'EOP. Il étend ces plans antérieurs en mettant l'accent sur l'éducation à la sécurité, les

enquêtes sur les menaces, la réponse aux menaces, et l'automatisation des protocoles de sécurité.

Les fonctionnalités supplémentaires clés du Plan 2 comprennent :

- Traqueurs de menaces : Le suivi des menaces vous permet de voir le cheminement d'une menace au sein de votre organisation. Il peut fournir des informations précieuses sur d'éventuelles failles de sécurité dans votre système.
- Explorateur de menaces : L'explorateur de menaces fournit une analyse plus approfondie des menaces en temps réel contre les personnes de votre organisation.
- Détection et réponse automatisées : La détection automatisée des menaces permet à votre personnel informatique de consacrer plus de temps à la gestion des menaces qui nécessitent un jugement humain.
- Formation à la simulation d'attaque : Pour souligner l'importance d'un programme de sécurité holistique, Defender pour Office Plan 2 comprend une formation. La formation à la simulation d'attaques aide le personnel à jouer un rôle proactif dans la gestion de sa sécurité.

Endpoint vs Identity vs Cloud Apps

La figure qui suit englobe l'ensemble de l'entendu de Microsoft Defender pour Office 365 qui dispose des services suivants.

Defender pour Office

Defender pour Office se concentre sur les menaces résultant de votre utilisation d'Office 365. Cette solution convient mieux aux entreprises qui s'appuient sur Office 365.

Defender pour Identity

Defender pour Identity (anciennement Defender pour Azure) exploite le comportement des utilisateurs et l'analyse d'Active Directory pour détecter les éventuelles menaces de sécurité basées sur l'identité.

Defender pour Endpoint

Defender pour Endpoint est spécialisé dans les menaces liées aux points de terminaison. Il utilise l'IA (Intelligence Artificielle) pour évaluer les menaces pesant sur votre système.

Defender pour Cloud Apps

Defender pour Cloud Apps (anciennement connu sous le nom de Cloud App Security) se concentre sur l'analyse de la sécurité des applications cloud déployées dans votre organisation.

How to : Activer Defender pour Office 365

Microsoft Defender pour Office 365 s'active automatiquement lorsque les clients éligibles disposant des autorisations requises visitent le portail de services.

Autrement, pour activer Microsoft Office 365 Defender, il faut procéder comme suit :

1. Vérifiez l'éligibilité à la licence et confirmez les autorisations requises. Si vous disposez d'une licence pour un produit de sécurité Microsoft 365, vous avez la garantie d'utiliser Defender pour Office 365 sans aucun coût de licence supplémentaire.

2. Vérifiez votre rôle. Vous devez être connecté à Defender pour Office 365 avec l'un des rôles suivants :
   - Administrateur de sécurité
   - Administrateur général
   - Opérateur de sécurité
   - Lecteur de sécurité
   - Lecteur général
   - Administrateur de conformité
   - Administrateur de conformité des données
   - Administrateur d'application
   - Administrateur d'application Cloud

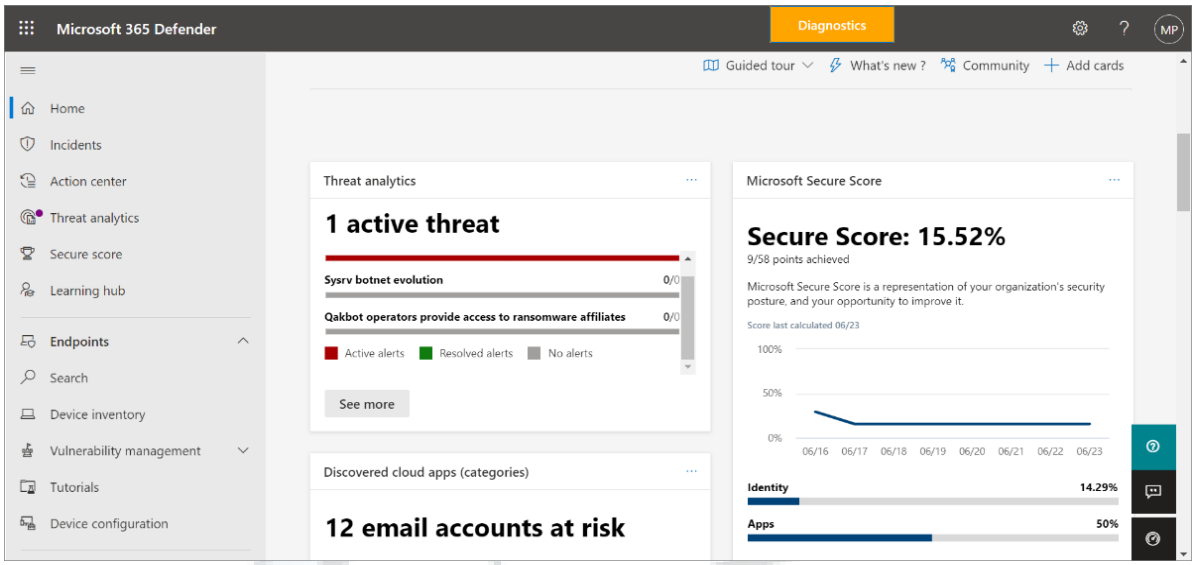
3. Connectez-vous au portail de service Defender pour Office 365 (centre d'administration).

4. Activez Microsoft Defender pour Office 365 pour tout service de messagerie ou Office 365 de votre choix.

5. Vérifiez la liste des éléments dans le volet de gauche du portail de services et cliquez sur « Afficher tout ».

6. Sous le centre d'administration, cliquez sur Sécurité. Cela vous apporte une protection à Microsoft 365 avec d'autres navigateurs.

7. Vous passerez ensuite par certains paramètres que vous configurerez selon vos besoins puis confirmerez si le service est activé.



L'interface de Microsoft Defender for Office 365 offre une expérience utilisateur intuitive et conviviale, facilitant la gestion et la surveillance des aspects cruciaux de la sécurité de votre environnement de messagerie. Avec une conception ergonomique, l'interface permet un accès facile aux fonctionnalités essentielles telles que la configuration des politiques de sécurité, la visualisation des rapports d'analyse, et la gestion des alertes de sécurité. Les tableaux de bord clairs et les menus bien organisés facilitent la navigation, offrant une visibilité complète sur les activités de sécurité en temps réel. Grâce à cette interface intelligente, les utilisateurs peuvent prendre des décisions informées et réagir rapidement aux menaces éventuelles, renforçant ainsi la résilience de leur système de messagerie. Que ce soit pour l'administration des politiques de sécurité, la surveillance des incidents de sécurité ou l'analyse approfondie des rapports, l'interface de Microsoft Defender pour Office 365 garantit une gestion efficace et proactive de la sécurité des courriels.

Bulletin de sécurité

Date de publication	Produit	Impact	Gravité	Article	Details
10 Octobre 2023	Azure Identity SDK for .NET	Remote Code Execution	Important	More Information	CVE-2023-36414
10 Octobre 2023	Microsoft Dynamics 365 (on-premises) version 9.1	Spoofing	Important	5026501	CVE-2023-36416
10 Octobre 2023	Windows 10 Version 1809 for x64-based Systems	Remote Code Execution	Important	5031361	CVE-2023-36436
10 Octobre 2023	Microsoft Exchange Server 2019 Cumulative Update 13	Remote Code Execution	Important	5030877	CVE-2023-36778
10 Octobre 2023	Microsoft SQL Server 2019 for x64-based Systems (GDR)	Remote Code Execution	Important	5029377	CVE-2023-36417

.