

# Détection des menaces et réponse aux incidents pour Microsoft 365

**POURQUOI** – L'évolutivité, l'économie de coûts et la standardisation offertes par Microsoft 365 ont considérablement boosté la popularité de Microsoft auprès des PME. Toutefois, sa popularité chez les cyber-criminels pose de nombreux problèmes... Entre les attaques de phishing dynamiques et les attaques par ransomware avancées, les menaces véhiculées par email sont devenues la première porte d'entrée vers la suite Microsoft 365. Les PME ont donc besoin d'une solution capable de repérer ce que Microsoft laisse passer.

**LA SOLUTION** – Vade for M365 propose une protection avancée contre les cyberattaques dynamiques orchestrées par email qui ciblent Microsoft 365, notamment le phishing, les malwares/ransomwares et le spear phishing (Business Email Compromise). Vade for M365 procure une expérience utilisateur Microsoft Outlook native ainsi qu'une couche de sécurité qui vient renforcer la sécurité intégrée de Microsoft, avec la capacité d'intercepter 10 fois plus de menaces avancées que Microsoft.

## Fonctionnalités



### Protection contre le phishing

Les emails de phishing usurpent l'identité des marques auxquelles vos utilisateurs se fient le plus. Au moyen de techniques d'ingénierie sociale élaborées, les usurpateurs induisent leurs victimes en erreur avec des objets d'email alarmants ou alléchants pour les pousser à cliquer sur des liens dangereux, qui les mèneront sur des sites frauduleux, ou à télécharger un malware ou un ransomware.

Vade for M365 scanne tous les éléments de l'email, y compris les adresses, liens, images et pièces jointes, bloquant les attaques de phishing avancées qui contournent les autres solutions. Vade peut également scanner les pages web en lien dans les emails afin de déterminer leur nature frauduleuse ou inoffensive.



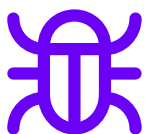
### Protection contre le spear phishing

Les emails de spear phishing usurpent l'identité de personnes plutôt que de marques. Avec pour objectif d'inciter les utilisateurs à entreprendre une action, les auteurs de spear phishing se montrent amicaux ou pressants pour pousser les utilisateurs à programmer des vêtements, à partager des identifiants de connexion, à acheter des cartes cadeaux, à changer des numéros de compte bancaire et bien plus.

Vade for M365 examine la totalité de l'email à la recherche d'indices de spear phishing qui ne peuvent être détectés par simple scan de l'URL ou des pièces jointes, notamment des noms affichés factices et du contenu textuel suspect. En cas de suspicion de spear phishing, Vade affiche une bannière d'avertissement dans l'email afin d'avertir l'utilisateur de la nature potentiellement frauduleuse de l'email.

### Avantages

- ✓ Protège votre entreprise des cyberattaques véhiculées par email
- ✓ Intercepte 10 fois plus de menaces avancées que Microsoft
- ✓ Bloque les menaces sophistiquées qui contournent les solutions traditionnelles
- ✓ Propose une formation de sensibilisation au phishing automatisée
- ✓ Solution transparente invisible pour les utilisateurs finaux
- ✓ Ne retarde pas la réception des emails
- ✓ Ne nécessite aucune formation des utilisateurs



### Protection contre les **malwares** et les **ransomwares**

Le malware est un virus conçu pour endommager les ordinateurs, le matériel et les réseaux. Les malwares sophistiqués peuvent modifier leur comportement et même se cacher des filtres email jusqu'à leur exécution, avec pour objectif final de voler des données, d'infecter d'autres systèmes ou, dans le cas des ransomwares, de désactiver les systèmes et réseaux.

Vade for M365 analyse les caractéristiques malveillantes de l'email, des pages web, des fichiers partagés et des pièces jointes afin de détecter les malwares et ransomwares dissimulés. Vade for M365 ne se contente pas d'une simple analyse des malwares, mais utilise également la détection comportementale des malwares pour les bloquer en temps réel, sans pour autant retarder la réception des emails pour les utilisateurs finaux.





### Protection contre les **menaces** venues de l'intérieur

Transférer un email de phishing ou partager une pièce jointe infectée par un malware : parfois, une simple erreur d'un employé peut donner lieu à un incident de cybersécurité. Si les menaces internes résultent bien souvent d'une erreur humaine, les cybercriminels peuvent également prendre le contrôle des comptes Microsoft 365 à travers des emails de phishing et envoyer des emails malveillants en interne à toute l'organisation.


Vade for M365 scanne le trafic des emails internes pour empêcher toute attaque venue de l'intérieur par des comptes Microsoft 365 compromis, en bloquant les emails de phishing et spear phishing ainsi que les malwares et ransomwares avant qu'ils ne puissent infecter l'intégralité de votre entreprise.

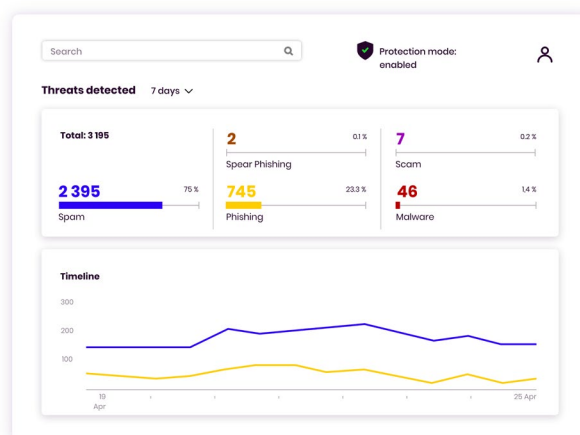
## Fonctionnalités post-réception

 **Auto-remédiation** – Scanne continuellement les emails et supprime automatiquement les messages des boîtes de réception dès la détection d'une nouvelle menace.

 **Threat Coach** – Propose automatiquement à l'utilisateur une formation de sensibilisation au phishing lorsque ce dernier interagit avec des emails de phishing.

 **Journaux et rapports** – Offrent une visibilité immédiate sur les menaces détectées et neutralisées grâce aux tableaux de bord et rapports.

 **Boucle de rétroaction** – Permet aux utilisateurs de signaler les menaces directement au centre de sécurité de Vade avec le bouton Signaler le phishing de Microsoft Outlook.



### À propos de Vade

- 1 milliard de boîtes mails protégées
- 100 milliards d'emails analysés / jour
- 1400+ partenaires dans le monde
- Renouvellement annuel de 95%
- 17 brevets internationaux actifs

### En savoir plus

[www.vadesecure.com](http://www.vadesecure.com)



@vadesecure

### Contact

Service commercial

[sales@vadesecure.com](mailto:sales@vadesecure.com)