vade
FOR M365

Solution de protection native et proactive de la messagerie, utilisant les API de Microsoft 365

POURQUOI – Bien que les mécanismes de sécurité (notamment EOP) inclus dans Microsoft 365 parviennent à intercepter la plupart des spams et des menaces connues, les entreprises doivent adopter un niveau de protection supplémentaire pour se prémunir des menaces inconnues et dynamiques. C'est pourquoi Gartner recommande aux entreprises utilisant Microsoft 365 de compléter la sécurité de la messagerie avec un niveau de protection supplémentaire.

SOLUTION – Intégré à Microsoft 365 via l'API Microsoft, Vade utilise l'IA pour venir renforcer les couches de sécurité de la solution Microsoft 365, basées principalement sur des technologies d'analyse de réputation et de signature. Vade apporte ainsi une défense prédictive de la messagerie sans que les utilisateurs aient à changer leurs habitudes.

L'intelligence artificielle au service de la détection des attaques inconnues et ciblées

Vade for Microsoft 365 bloque les attaques dès le premier email en s'appuyant sur un moteur de filtrage comportemental qui exploite des règles heuristiques et plusieurs technologies d'IA. Notre solution procède à des analyses comportementales en temps réel de l'intégralité des emails, URL et pièces jointes incluses, et utilise les données et retours des utilisateurs du 1 milliard de boîtes aux lettres qu'elle protège pour affiner en continu son moteur de filtrage et garantir un taux de précision élevé.

Protection contre le phishing multi facettes – La solution réalise une analyse comportementale de l'email et de l'URL, à différents niveaux et en temps réel, en suivant toutes les redirections pour déterminer si la page finale est malveillante. Des modèles d'apprentissage automatique analysent 47 caractéristiques de l'emails et de l'URL pour repérer des comportements malveillants, tandis que des algorithmes de Computer Vision scrutent les modifications apportées aux logos, QR Codes et autres images couramment utilisées dans les attaques de phishing.

Protection contre le spear phishing avec une bannièr – Des algorithmes de traitement du langage naturel interprètent les textes suspects, tandis qu'une fonction de détection des anomalies établit un profil anonyme qui définit les habitudes de communication de chacun de vos employés. Les anomalies détectées, comme les tentatives d'usurpation d'identité ou les demandes d'ordre financier, déclenchent l'affichage d'une bannière d'alerte personnalisable.

Protection contre les malwares par analyse comportementale – Vade réalise une analyse complète de l'origine, du contenu et du contexte des emails et des pièces jointes. Cette analyse ne se limite pas aux pièces jointes et permet ainsi à la solution de détecter les malwares bien avant les antivirus et les technologies de sandboxing, sans latence perceptible par les utilisateurs.

Protection contre les menaces venues de l'intérieur – Grâce à son intégration native à Microsoft 365, la solution analyse le trafic des emails internes pour éviter les attaques issues de comptes compromis.

Fonctionnalités post-réception

Technologie basée sur l'IA, améliorée par les utilisateurs et conçue pour les administrateurs débordés

Auto-Remediate – Améliore la détection des menaces en permettant la remédiation des menaces post-réception. La fonction Auto-Remediate s'appuie sur la capacité de Vade à avoir une vision en temps réel sur les menaces mondiales provenant du 1 milliard de boîtes aux lettres protégées, ce qui permet d'analyser en permanence les emails et de supprimer automatiquement les messages des boîtes de réception des utilisateurs lorsque des nouvelles menaces sont détectées. Les administrateurs peuvent également neutraliser des messages manuellement en un clic.

Vade Threat Coach™ – Propose une formation automatisée et adaptative pour corriger le comportement d'un utilisateur qui ouvre un email de phishing ou clique sur un lien de phishing. Elle offre une sensibilisation au phishing adaptée à la marque usurpée dans l'email de phishing et vient compléter les formations structurées avec des informations complémentaires fournies à la volée afin de renforcer le respect des bonnes pratiques.

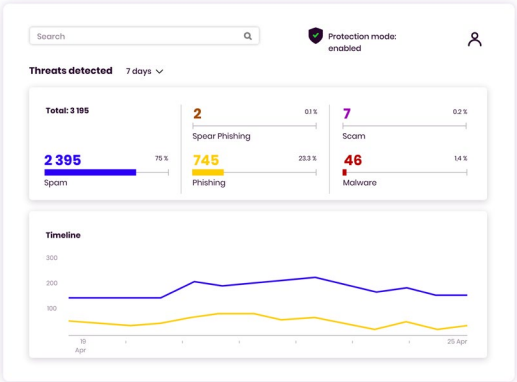
Journaux et rapports – Des tableaux de bords, rapports et journaux en temps réel permettent de bénéficier d'une visibilité immédiate sur les menaces détectées et neutralisées. Les administrateurs peuvent garder un œil sur le trafic d'emails, repérer les menaces liées à des événements actuels et neutraliser les emails mal classés en un clic.

Boucle de rétroaction intégrée – Permet aux utilisateurs de signaler les menaces directement au SOC de Vade par le biais des boutons Courrier indésirable et Phishing de Microsoft Outlook. La boucle de rétroaction (feedback loop) de Vade Secure transforme les retours des utilisateurs en informations stratégiques sur les menaces permettant de renforcer en permanence l'efficacité du filtre et de la fonction Auto-Remediate.

Expérience utilisateur native de Microsoft 365

À la différence des passerelles de messagerie sécurisées, qui imposent une modification des enregistrements MX et perturbent les flux d'emails, Vade for M365 s'intègre directement à la plateforme grâce à son utilisation native des API Microsoft. Cette approche architecturale offre plusieurs avantages aux administrateurs comme aux utilisateurs finaux :

- **Pas de modification des MX** – Activez la solution en quelques clics, sans avoir à modifier votre enregistrement MX.
- **Complémentarité avec EOP** – Complétez EOP à l'aide de technologies permettant d'intercepter les menaces passant au travers des mailles du filet de Microsoft. Le rapport de valeur ajoutée intégré quantifie l'amélioration du taux de détection apporté par Vade.
- **Pas de règles ou de configurations complexes** – Configurez des règles simples, en fonction des menaces, et récupérez de manière transparente vos paramètres Exchange Online pour éviter de recommencer votre paramétrage.
- **Pas de changement de l'interface, pas de quarantaine externe** – Permettez aux utilisateurs de continuer à travailler dans Microsoft Outlook, dans la même interface et sans avoir à gérer une quarantaine externe. Vade filtre les emails dans les dossiers Outlook en fonction des règles définies.



À propos de Vade
- 1 milliard de boîtes mails protégées
- 100 milliards d'emails analysés / jour
- 1,400+ partenaires dans le monde
- Renouvellement annuel de 95%
- 15 brevets internationaux actifs

En savoir plus
www.vadesecure.com

@vadesecure

Contact
Service commercial

sales@vadesecure.com