DATA SHEET

Sécurité de l'email collaborative pour Microsoft 365

vade FOR M365

L'évolutivité, les économies et la standardisation offertes par Microsoft 365 ont considérablement boosté la popularité de Microsoft auprès des entreprises de toutes tailles. Toutefois, sa popularité chez les cybercriminels pose quant à elle de nombreux problèmes… Entre les emails de phishing dynamiques et les malwares de plus en plus difficiles à repérer, les emails sont devenus la première porte d'entrée vers la suite Microsoft 365. Les entreprises ont donc besoin d'une solution capable de repérer ce que Microsoft laisse passer.

Vade for M365 est une solution de sécurité de l'email low-touch et intégrée pour Microsoft 365, alimentée par l'IA et améliorée par l'humain. Son moteur d'IA collaboratif apprend en continu en associant interactions humaines et vérifications technologiques, ce qui lui permet de bloquer les menaces sophistiquées que la solution de Microsoft ne détecte pas.

AVANTAGES

- Intercepte 10 fois plus de menaces avancées que Microsoft
- Bloque les menaces sophistiquées en temps réel
- Supprime automatiquement les menaces après réception
- Se déploie et se gère facilement
- Offre une expérience native dans Outlook sans quarantaine externe
- Propose des options de licence flexibles et adaptées à votre entreprise

RENFORCEZ LES DÉFENSES DE MICROSOFT 365

Vade for M365 utilise le moteur collaboratif de Vade pour déployer des modèles d'IA comportementaux qui bloquent les menaces les plus sophistiquées, et automatisent les analyses et les réponses.

Anti-Phishing

Vade for M365 utilise des modèles de machine learning et de computer Vision entraînés à reconnaître les comportements malveillants, y compris les URL obfusquées, les URL à retardement, l'usurpation de l'adresse email, les redirections, les images hébergées à distance et les images et logos de marque altérés.

Protection contre le spear phishing et le BEC*

Le natural language processing et les algorithmes de détection des usurpations analysent les éléments d'un email susceptibles de révéler des anomalies et des schémas suspects, notamment les adresses email et domaines usurpés, le contenu textuel suspect, les noms affichés factices et les anomalies dans le trafic de messagerie.

*En cas de suspicion de spear phishing, Vade affiche une bannière d'avertissement personnalisable.

Protection contre les malwares et les ransomwares

Les technologies de détection des malwares et ransomwares de Vade ne se limitent pas à l'étude de la signature : elles procèdent à une analyse comportementale, mais aussi à une analyse heuristique des emails, pages Web et pièces jointes. Elles sont aussi capables d'analyser les pièces jointes et les fichiers hébergés sur OneDrive, SharePoint, Google et WeTransfer.

Détection des menaces

- Machine Learning
- Deep Learning
- Computer Vision
- Natural Language Processing

M-SOAR

- Auto-remédiation
- Formation automatisée des utilisateurs
- Tri et remédiation des emails signalés
- Intégration aux systèmes SIEM/EDR/XDR
- Intégration native de Splunk
- Bannières d'alerte de spear phishing personnalisables

FONCTIONS POST-RÉCEPTION ET CAPACITÉS DE RÉPONSE AUX INCIDENTS

Basée sur l'IA et améliorée par l'humain

Auto-Remediate

Analyse continuellement les emails après leur remise et supprime automatiquement les messages des boîtes de réception dès la détection d'une nouvelle menace. Les administrateurs peuvent également neutraliser des messages manuellement en un clic.

Vade Threat Coach™

Propose une formation automatisée et contextualisée avec de vrais emails et pages de phishing pour corriger le comportement d'un utilisateur qui ouvre un email ou clique sur un lien malveillant.

Threat Intel & Investigation

Analyse les emails signalés par les utilisateurs et y remédie, décortique les fichiers, télécharge les emails et leurs pièces jointes, et permet l'exportation des journaux vers n'importe quel SIEM/EDR/XDR.*

Boucle de rétroaction intégrée

Transforme les retours des utilisateurs et des administrateurs en informations stratégiques sur les menaces permettant de renforcer en permanence l'efficacité du filtre et de la fonction Auto-Remediate.

Intégration native de Splunk

Permet aux administrateurs d'intégrer les journaux d'email Vade for M365 à Splunk sans avoir à développer un logiciel spécifique.

*Module complémentaire

Contact

Service commercial

sales@vadesecure.com