DATA SHEET

Sécurité de l'email collaborative pour Microsoft 365

vade FOR M365

La popularité de Microsoft 365 auprès des PME génère de nombreuses opportunités commerciales pour les MSP. Toutefois, sa popularité chez les cybercriminels pose quant à elle de nombreux problèmes… Entre les attaques 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 MSP ont donc besoin d'une solution capable de repérer ce que Microsoft laisse passer.

Vade for M365 est une solution low-touch intégrée pour Microsoft 365. Alimentée par l'IA, elle est améliorée par l'humain et pensée pour les MSP. 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.

RENFORCEZ LES DÉFENSES DE MICROSOFT 365

Les fonctions de Vade for M365 s'appuient sur le moteur collaboratif de Vade et diverses technologies liées à l'IA, comme le machine learning, la computer Vision et le natural language processing, pour bloquer les menaces sophistiquées et automatiser les investigations 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, les noms factices, le trafic de messagerie anormal et les textes suspects.

*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.

Solution pensée pour les MSP

- Réponse aux incidents multitenant
- Remédiation automatique et en un clic
- Formation de sensibilisation des utilisateurs post-incident automatisée
- Outils d'analyse des menaces
- Déploiement en 10 minutes
- Offres de licence flexibles

Détection des menaces basée sur l'IA

- Anti-Phishing
- Anti-Spear Phishing (BEC)
- Protection contre les malwares et les ransomwares
- Protection contre le spam

M-SOAR

- Auto-remédiation
- Réponse aux incidents multitenant
- 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, améliorée par les utilisateurs et pensée pour les MSP

Sécurité managée

Centralise vos tenants Vade for M365 dans un tableau de bord unifié. Remédiez aux menaces par email chez tous les tenants, triez les emails signalés par les utilisateurs et remédiez-y, et gérez la cybersécurité de vos clients depuis un espace centralisé.

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 remédier aux 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 pièces jointes, et permet l'exportation des journaux vers n'importe quel SIEM/EDR/XDR.

Boucle de rétroaction intégrée

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.

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.

Contact

Service commercial

sales@vadesecure.com

Vade est une entreprise internationale de cybersécurité spécialisée dans le développement de technologies de détection et de réponse aux menaces grâce à l'intelligence artificielle. Les produits et solutions de Vade protègent les consommateurs, les entreprises et les administrations contre les attaques véhiculées par email, telles que les malwares/ransomwares, le spear phishing, les attaques Business Email Compromise et le phishing.

Créée en 2009, Vade protège 1,4 milliard de messageries professionnelles et personnelles et propose aux marchés des FAI, PME et MSP des solutions et produits reconnus qui permettent de renforcer la cybersécurité et d'optimiser l'efficacité informatique.

En savoir plus: **vadesecure.com**

Suivez-nous :

@vadesecure