DATA SHEET

Sécurité de l'email collaborative pour Google Workspace

HORNETSECURITY vade

L'évolutivité, les économies et la standardisation offertes par Google Workspace (GWS) l'ont rendu extrêmement populaire auprès des entreprises. 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 GWS. Les entreprises ont besoin d'une solution qui offre une protection multicouche et qui capture les menaces qui échappent à Google.

Vade for Google Workspace est une solution low-touch intégrée pour GWS, alimentée par l'IA et améliorée par l'humain. Doté d'un puissant moteur d'IA qui apprend en permanence grâce à l'alliance de l'intelligence humaine et de l'intelligence machine, Vade pour Google Workspace bloque les menaces les plus avancées d'aujourd'hui et de demain.

AVANTAGES

- Protège votre entreprise contre les cyberattaques par email les plus sophistiquées et les plus ciblées
- Analyse instantanément les emails avant leur envoi
- Fournit des couches de protection supplémentaires pour détecter plus de menaces que Google seul
- Filtrage et classification du « courrier gris » améliorés et plus précis
- Supprime automatiquement les menaces nouvellement identifiées après livraison
- Invisible pour les utilisateurs finaux
- Interface simplifiée et conviviale
- Ne demande aucune formation des utilisateurs

FONCTIONS

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 tentants 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 Google Workspace 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.

Anti-spear phishing et attaques Business Email Compromise (BEC)

Les emails de spear phishing usurpent l'identité de personnes plutôt que celles 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 virements, à partager des identifiants de connexion, à acheter des cartes cadeaux, à changer des numéros de compte bancaire et bien plus.

Vade for Google Workspace 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.

DATA SHEET

Sécurité de l'email collaborative pour Google Workspace

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 Google Workspace 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 Google Workspace ne se contente pas d'une simple analyse des malwares, mais utilise également la détection comportementale des malwares pour les bloquer en temps réel.

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 GWS à travers des emails de phishing et envoyer des emails malveillants en interne à toute l'organisation.

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

*Complément payant

DES CARACTÉRISTIQUES ROBUSTES POUR UNE SÉCURITÉ MULTICOUCHE

- Auto-remédiation : scanne continuellement les emails 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.
- Threat Intel & Investigation : intègre Vade à votre logiciel de surveillance et réponse aux menaces, et fournit des outils de pointe pour l'analyse et la réponse.*
- Vade Remote Browser Isolation (RBI) : Offre une protection complète contre les attaques de type "zero-day" qui proviennent des emails et se produisent via le navigateur.*
- 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.

À propos de Hornetsecurity

[Vade est fière d'être la nouvelle recrue du groupe Hornetsecurity.]

Hornetsecurity est l'un des principaux fournisseurs mondiaux de solutions de sécurité, de conformité, de sauvegarde et de sensibilisation à la sécurité nouvelle génération basées sur le Cloud, qui aident les entreprises et de toutes tailles dans le monde entier.

Son produit phare, 365 Total Protection, est la solution de sécurité Cloud pour Microsoft 365 la plus complète du marché. Animé par l'innovation et l'excellence en matière de cybersécurité, Hornetsecurity construit un avenir numérique plus sécurisé et des cultures de sécurité durables grâce à son portefeuille primé. Hornetsecurity est présent dans plus de 120 pays grâce à son réseau international de distribution de plus de 12 000 partenaires et MSP. Ses services prémium sont utilisés par plus de 75 000 clients. Pour plus d'informations, visitez le site

www.hornetsecurity.com.

Suivez-nous :

@vadesecure