vade
FOR M365

Microsoft 365 :

Protégez votre entreprise face aux nouvelles menaces

TABLE DES MATIÈRES

INTRODUCTION

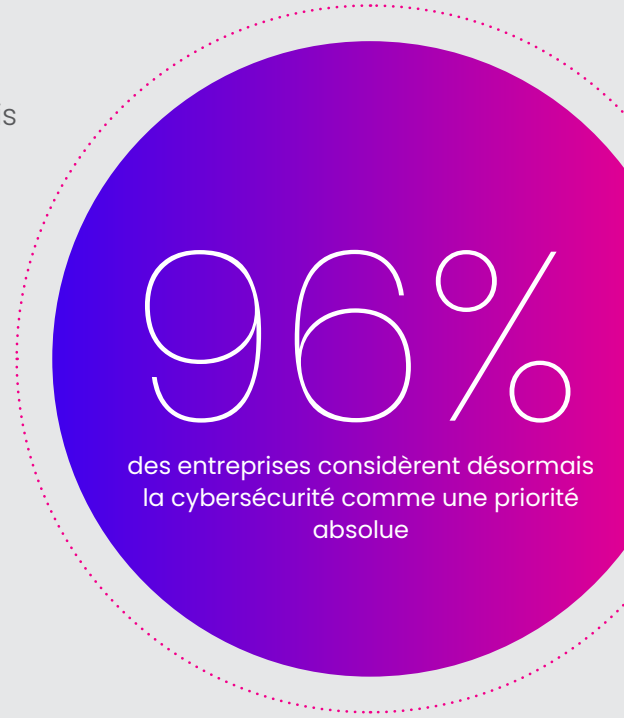
La montée en puissance rapide du télétravail, du cloud et de la communication numérique a transformé les modes de travail des entreprises et les modes de pensée des cybercriminels.

Face à ce bouleversement, un acteur a clairement tiré son épingle du jeu : Microsoft. Principale suite bureautique au monde, la solution Microsoft 365 répond aux besoins de plus de 345 millions d'utilisateurs et joue désormais un rôle essentiel au sein de nombreuses organisations. Parmi elles, on peut bien entendu citer les entreprises, mais aussi les fournisseurs de services managés (MSP), qui utilisent l'application en interne et proposent à leurs clients différents services liés.

Pour autant, l'application n'est pas appréciée que du monde professionnel. **En effet, les hackers en ont fait une cible privilégiée**, ce qui pose un problème de taille aux entreprises, et en particulier à celles qui ne disposent pas des ressources nécessaires pour investir dans des solutions ou équipes de cybersécurité suffisamment robustes. Particulièrement vulnérables, les entreprises et MSP doivent ainsi affronter des menaces sérieuses avec pour seule défense les outils de sécurité basiques intégrés de Microsoft.

La popularité de Microsoft 365 ne se dément pas, mais l'approche adoptée par les entreprises en matière de cybersécurité commence à changer. La quasi-totalité des **entreprises (96 %)** considère désormais la cybersécurité comme une priorité absolue. 88 % prévoient de renforcer leurs investissements dans ce domaine l'année prochaine, et 50 % jugent qu'il s'agit du service managé le plus important.

Face à des cybermenaces toujours plus sophistiquées et nombreuses, les entreprises et MSP sont en quête de solutions pensées spécifiquement pour leurs besoins et l'environnement Microsoft 365.



1. Microsoft. "Earnings Release Q3 2022." https://www.microsoft.com/en-us/investor/earnings/fy-2022-q3/press-release-webcast
2. Vade. "The Time for MSPs is Now: The SMB Cybersecurity Landscape Report 2022." https://info.vadesecure.com/en/the-2022-smb-cybersecurity-landscape-report-survey-results

L'EMAIL : PRINCIPAL VECTEUR DES ATTAQUES CONTRE MICROSOFT 365

Si Microsoft 365 constitue une cible de choix pour les cybercriminels, l'email est leur vecteur privilégié contre les entreprises qui utilisent cette plateforme. En effet, il leur ouvre un accès direct au maillon le plus faible de la surface d'attaque de toute organisation : ses utilisateurs. Un simple email leur permet d'accéder aux réseaux internes des entreprises, puis d'organiser des attaques par ingénierie sociale plus ambitieuses et malveillantes.

Après une analyse approfondie, nous avons détecté trois facteurs qui font de l'email le vecteur le plus intéressant pour les cyberattaques.

1

Microsoft Exchange Online Protection (EOP) n'est pas à la hauteur

Microsoft 365 intègre une fonction de sécurité de l'email appelée Exchange Online Protection (EOP). Pensée pour filtrer le spam et autres emails envoyés en masse, elle est désormais en mesure d'identifier les emails de phishing et contenant des malwares.

En revanche, elle est bien moins efficace pour repérer les menaces zero-day et autres menaces plus évoluées, par exemple celles dont la signature est inconnue ou qui ont recours à des techniques d'évitement de haut niveau. EOP a également recours au sandboxing, un processus qui ralentit la remise des emails et ne détecte pas les malwares utilisant une machine virtuelle. Par ailleurs, la solution ne recherche pas les menaces cachées dans les emails déjà remis.

Une récente étude a mis en lumière les limites des filtres de sécurité de l'email intégrés comme EOP. Elle révèle que **8 entreprises sur 10 basent leur sécurité sur des outils basiques comme EOP et que presque 70 % ont été victimes d'une violation de données grave malgré cette sécurité au cours de l'année passée.**[3]

3. Vade. "The Time for MSPs is Now: The SMB Cybersecurity Landscape Report 2022." https://info.vadesecure.com/en/the-2022-smb-cybersecurity-landscape-report-survey-results

2 **Les solutions de sécurité de l'email classiques tierces ne sont pas en mesure de répondre aux besoins du monde moderne**

Pour compenser les vulnérabilités d'EOP, de nombreuses organisations se tournent vers des solutions de sécurité de l'email tierces. Parmi les plus utilisées, on trouve notamment les gateways de messagerie sécurisées.

Ces gateways tirent parti de filtres d'analyse de la réputation et de la signature, et proposent donc une protection tout à fait efficace contre les menaces déjà vues, par exemple les emails malveillants provenant d'adresses IP en liste noire ou les malwares dont la signature est connue. Pour autant, elles n'offrent pas une protection suffisante contre les menaces qui n'ont pas encore été analysées, et notamment les plus de 450 000 variantes de malwares et applications potentiellement indésirables découvertes chaque jour en 2022.[4]

Par ailleurs, ces gateways sont placées à l'extérieur de Microsoft 365. Elles ne protègent donc pas l'environnement contre les menaces et attaques venues de l'intérieur. Elles rendent inefficaces les fonctions de sécurité de Microsoft EOP et imposent de modifier les enregistrements MX, un changement que les hackers peuvent repérer.

3 **Les outils de cybersécurité de pointe sont complexes et mobilisent des ressources importantes**

Microsoft Defender for Office 365, un produit de sécurité d'entreprise complémentaire pour les entreprises utilisant Microsoft 365, offre une protection appropriée contre les cybermenaces sophistiquées.

Toutefois, il s'agit d'une solution complexe et chronophage, qui nécessite une équipe dédiée à la cybersécurité. Ce n'est donc pas d'une option envisageable pour de nombreux MSP et entreprises, qui ont besoin d'une sécurité solide sans recruter de personnel dédié ou détourner des ressources de leurs activités. Les MSP recherchent également une solution qui leur permet d'élaborer et d'étendre une offre de services de sécurité managés. Microsoft Defender for Office 365 n'est pas pensé pour un déploiement massif.

Solution tierce de sécurité de l'email, un passage obligé

Les entreprises et MSP ont besoin d'une solution tierce de sécurité de l'email qui s'intègre à Microsoft 365, renforce la protection des outils existants et libère du temps et des ressources pour leur permettre de se concentrer sur leurs autres priorités métier. Cette solution doit également offrir une expérience utilisateur appropriée en faisant des utilisateurs finaux non plus le point d'entrée des hackers, mais une dernière ligne de défense redoutable.

4. AV Test Institute. "Malware." https://www.av-test.org/en/statistics/malware/

LES MENACES ÉVOLUENT

Aujourd'hui, la cybersécurité n'est plus un sujet de second plan. Les entreprises et MSP font face à une nouvelle génération de cybermenaces. Plus sophistiquées que jamais et omniprésentes, elles posent un risque de sécurité à chaque service et chaque niveau hiérarchique, et mettent en danger le bon fonctionnement de leurs opérations. En constante évolution, ces menaces peuvent néanmoins être classées selon diverses catégories.

Phishing

Menace la plus courante, le phishing est un scam par email consistant pour son auteur à se faire passer pour une marque afin de pousser ses victimes à divulguer leurs identifiants ou à exécuter un malware. La plupart du temps, les hackers ont recours à des liens menant à des sites frauduleux ou à des pièces jointes contenant des malwares.

Habituellement, le phishing vise large, mais des campagnes plus évoluées commencent à apparaître. Dans certains cas, les hackers adaptent leurs campagnes à un nombre limité de victimes qu'ils ont étudiées dans le détail.

D'après une étude conduite par IBM et le Ponemon Institue, **le phishing a coûté environ 4,91 millions de dollars aux entreprises du monde entier en 2021 et représente la deuxième cause des violations de données.**[5] Cette cybermenace reste la préférée des hackers. Au premier semestre 2022, Vade a ainsi détecté plus de **315 millions d'emails de phishing dans le monde, soit deux fois plus que d'emails contenant des malwares.**[6]

Les hackers ont fréquemment recours à des techniques d'évitement pour tromper les solutions de sécurité de l'email classiques, notamment :

USURPATION DE L'ADRESSE EMAIL

L'idée consiste à reproduire un nom d'affichage (à l'identique) ou un nom de domaine légitime (nom voisin).

MANIPULATION D'IMAGES OU DE LOGOS

Les hackers modifient les signatures des logos ou images des marques pour contourner les filtres de messagerie traditionnels.

OBFUSCATION DES URL

Les hackers empêchent les filtres de détecter les menaces en camouflant leurs URL par ajout de redirections, raccourcissement, intégration dans des QR codes ou des pièces jointes, ou encore introduction d'URL légitimes.

5. IBM. "The Cost of a Data Breach Report 2022." https://www.ibm.com/downloads/cas/3R8N1DZJ
6. Vade. "Rapport sur le phishing et les malwares - T3 2022" https://www.vadesecure.com/fr/blog/rapport-sur-le-phishing-et-les-malwares-t3-2022

Spear phishing (Business Email Compromise)

Le spear phishing prend la forme d'un email malveillant dont l'auteur prétend être quelqu'un qu'il n'est pas afin de pousser sa victime à effectuer une action bien précise, généralement de nature financière. Bien souvent, le hacker se fait passer pour une connaissance de la victime, comme un collègue, un supérieur, un client ou un fournisseur.

Les techniques de spear-phishing couramment utilisées sont la fraude au président, les demandes de carte cadeau et la fraude à la fiscalité des employés. Le spear phishing est également souvent utilisé dans les attaques en plusieurs étapes. Il constitue alors le moyen initial d'accéder à un réseau interne.

Les attaques BEC ont coûté aux entreprises en moyenne 4,89 millions de dollars en 2021, ce qui en fait le deuxième type de cyberattaque le plus coûteux dans le monde.[7] Les attaques BEC ont représenté 6 % des violations de données sur cette période.

Les hackers ont recours à des techniques de spear phishing courantes pour tromper leurs victimes, notamment :

USURPATION DE L'ADRESSE EMAIL

En ursurpant le nom affiché d'un supérieur, d'un collègue, d'un fournisseur ou d'une connaissance, les hackers gagnent immédiatement la confiance de leurs victimes et les poussent à agir.

PRETEXTING

Les hackers envoient des questions ou emails amicaux pour endormir la méfiance des victimes et créer un faux sentiment de sécurité.

SENTIMENT D'URGENCE

Les malandrins suscitent un sentiment d'urgence poussant les victimes à agir de manière impulsive et à suivre des instructions sans réfléchir à leur légitimité.

SIGNATURES D'APPAREILS MOBILES

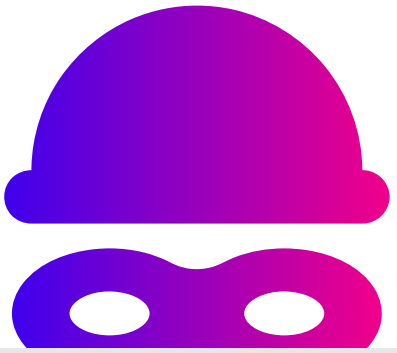
Les hackers ajoutent une signature de type « Envoyé depuis mon smartphone » pour faire oublier l'apparence suspecte d'une demande.

7. IBM. "The Cost of a Data Breach Report 2022." https://www.ibm.com/downloads/cas/3R8N1DZJ

Malware/Ransomware

Un malware est un logiciel malveillant conçu pour infecter des systèmes informatiques et en dérober des informations. Il existe de nombreux types de malwares, dont les plus courants sont les ransomwares, les spywares, les chevaux de Troie, les keyloggers et les adwares. Les malwares sont souvent remis lors de campagnes de phishing, lorsqu'un compte est compromis, lors de l'exploitation d'une vulnérabilité serveur ou lors d'attaques par force brute contre le RDP (Remote Desk Protocol).

Les malwares sont les cyberattaques les plus coûteuses. Les coûts liés aux ransomwares devraient ainsi dépasser 30 milliards de dollars dans le monde.[8] Au 1er semestre 2022, Vade a détecté plus de 125 millions d'emails contenant des malwares.[9]



Pour contourner les solutions de sécurité de l'email classiques, les hackers font couramment appel aux outils suivants :

MALWARES POLYMORPHES

Ces malwares font évoluer leur code d'une victime à l'autre pour ne pas être détectés.

MALWARES MÉTAMORPHES

Ces malwares réécrivent leur code à chaque infection. Les antivirus n'ont ainsi presque aucune chance de les repérer, les mettre en quarantaine et les éliminer.

GÉNÉRATION DE BRUIT

Ajout de code ou de texte sans signification dans les fichiers ou les macros pour modifier l'empreinte d'une menace connue.

OBFUSCATION DU CODE

Techniques d'évitement destinées à rendre plus difficile la détection de code par les filtres de messagerie.

MALWARES CONSCIENTS DE LEUR ENVIRONNEMENT

Ces malwares entrent en dormance lors de leur analyse dans une machine virtuelle ou une sandbox, et ne s'exécutent que lorsqu'ils atteignent leur environnement cible.

8. InfoSecurity Magazine. "Global Ransomware Damages Exceed $30bn by 2023." https://www.infosecurity-magazine.com/news/ransomware-exceed-30bn-dollars-2023/
9. Vade. "Rapport sur le phishing et les malwares - T3 2022" https://www.vadesecure.com/fr/blog/rapport-sur-le-phishing-et-les-malwares-t3-2022

IMPACT DES MENACES VÉHICULÉES PAR LES EMAILS SUR LES ENTREPRISES

En mai 2022, les **autorités de cybersécurité** du Royaume-Uni, d'Australie, du Canada, de Nouvelle-Zélande et des États-Unis ont publié **un communiqué commun alertant de la multiplication des cyberattaques ciblant les MSP et les entreprises.**[10] Cet avertissement fait suite à une hausse massive des attaques contre ces deux cibles, qui témoigne de l'intérêt des hackers pour les entreprises dont la cybersécurité est limitée.

Une attaque réussie contre une entreprise ou un MSP peut avoir des conséquences durables. Bien souvent, les dégâts réels dépassent de loin ceux mentionnés dans la presse. Leur nature est variable, mais ils appartiennent généralement aux catégories suivantes.

DOMMAGES FINANCIERS

Les victimes peuvent être confrontées à des temps d'arrêt, à une perte de leur propriété intellectuelle, à la perte de clients ou à une demande de rançon.

RÉPUTATION DÉGRADÉE

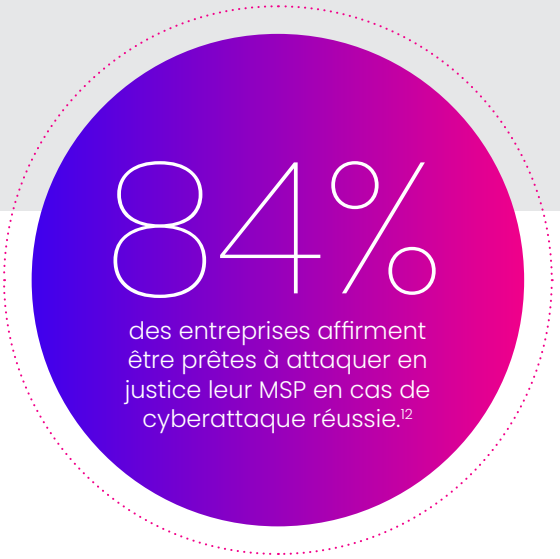
Les victimes peuvent être blâmées de la fuite de données sensibles, ou celan peut entraîner la compromission de clients ou partenaires.

PÉNALITÉS RÉGLEMENTAIRES

Les victimes peuvent encourir des pénalités élevées en cas de non-conformité aux lois de protection du consommateur. Le RGPD prévoit par exemple des amendes pouvant atteindre 4 % du chiffre d'affaires annuel ou 20 millions d'euros.[11]

CONSÉQUENCES JURIDIQUES

Les victimes peuvent faire face aux poursuites de leurs clients qui leur reprochent de ne pas avoir su assurer leur cybersécurité. Ce risque est très concret : 84 % des entreprises affirment être prêtes à attaquer en justice leur MSP en cas de cyberattaque réussie.[12]



10. Cybersecurity & Infrastructure Security Agency. "Protecting Against Cyber Threats to Managed Service Providers and their Customers." https://www.cisa.gov/uscert/ncas/alerts/aa22-131a
11. GDPR.eu. "What are the GDPR fines?" https://gdpr.eu/fines/
12. ConnectWise. "The State of SMB Cybersecurity in 2022." https://www.connectwise.com/resources/smb-research-2022

VADE FOR M365

Vade for M365 est une solution de détection et de réponse aux menaces pour Microsoft 365, pensée spécifiquement pour les MSP et les entreprises. **Elle s'appuie sur l'IA pour déjouer les menaces les plus sophistiquées véhiculées par les emails et intercepte 10 fois plus de ces menaces qu'EOP**. Autre avantage, elle n'impose pas aux entreprises et MSP de mobiliser des ressources les détournant de leurs priorités. Vade for M365 est basée sur des API, ce qui signifie qu'elle prend place au sein de l'environnement Microsoft 365 et peut ainsi assurer une défense contre les attaques et les cybermenaces internes.

Enfin, elle adopte une approche centrée sur l'humain en permettant aux utilisateurs de devenir des acteurs clés de la sécurité plutôt que de rester des points d'entrée bien pratiques pour les hackers.

Vade for M365 combine diverses technologies, fonctions et capacités.

Moteur de détection basé sur l'IA

Vade for M365 filtre les menaces les plus évoluées à l'aide d'un ensemble de technologies centrales. Grâce à l'IA, elles sont en mesure de procéder à une analyse comportementale et heuristique détectant les anomalies du texte ou des images, ainsi que les incohérences ou les comportements malveillants, que ce soit dans les emails, les liens, les pièces jointes ou les pages Web.

Le moteur de détection des menaces de Vade inclut les technologies suivantes :

MACHINE LEARNING (ML)

Analyse 47 caractéristiques des emails, URL et pièces jointes pour repérer des anomalies ou des comportements malveillants. Les algorithmes de ML sont entraînés à partir de vastes ensembles de données d'emails malveillants et légitimes leur permettant de reconnaître les caractéristiques de toutes les cybermenaces.

COMPUTER VISION

Analyse les images des emails et pages Web pour détecter les anomalies et comportements suspects. La Computer Vision est capable de repérer les techniques d'évitement pourtant efficaces contre les filtres traditionnels, comme la manipulation d'image visant à masquer une signature, les images contenant du texte évitant l'analyse, l'hébergement distant d'images sur des domaines de bonne réputation, etc.

NATURAL LANGUAGE PROCESSING (NLP)

Analyse le texte pour détecter de subtils choix grammaticaux et stylistiques qui pourraient indiquer une menace, par exemple des mots ou expressions clés. Les modèles de NLP fournissent une protection contre les attaques d'ingénierie sociale textuelles.

Auto-Remediate

Auto-Remediate est une fonction automatisée de réponse aux incidents de Vade for M365. Elle est capable de supprimer automatiquement les emails malveillants après qu'ils aient été remis. Cette fonction tire parti du moteur d'IA de Vade, et notamment de ses algorithmes de Machine Learning, de Computer Vision et de Natural Language Processing, pour analyser en continu les boîtes de réception et remédier aux menaces détectées en s'appuyant sur les informations en temps réel issues de 1,4 milliard de boîtes aux lettres dans le monde.

Auto-Remediate comble les lacunes des gateways de messagerie sécurisées en assurant la sécurité de l'email directement au sein des environnements Microsoft 365. Cette fonction stimule également la productivité des ressources IT en éliminant automatiquement les menaces.

MSP Response

La solution MSP Response de Vade permet aux MSP de proposer une offre de services managés complète et autonome. Grâce à elle, les MSP peuvent gérer l'ensemble de leurs tenants Vade for M365 depuis un seul et même tableau de bord, sur lequel ils peuvent fournir des services de réponse aux incidents, comme le suivi et la remédiation des menaces multilocataire en un clic.

Avec Vade for M365, les services de sécurité managés deviennent efficaces et peuvent être déployés à grande échelle. Les MSP sont alors en mesure de libérer de précieuses ressources informatiques tout en répondant aux exigences de leurs clients.

Vade Threat Coach™

Vade Threat Coach vient corriger le maillon faible de la surface d'attaque des entreprises et des MSP : les utilisateurs. Cette solution aborde la cybersécurité du point de vue de l'humain en proposant une formation de sensibilisation des utilisateurs à la volée.

À la différence des simulations génériques ou des formations en salle de classe, Vade Threat Coach fournit des informations personnalisées et pratiques au moment où les utilisateurs en ont le plus besoin : lorsqu'ils font face à une menace. La formation est ainsi personnalisée en fonction du contenu de la menace et du contexte des emails quotidien de l'utilisateur afin de lui proposer une expérience pertinente, qui améliorera réellement son comportement.

Threat Intel and Investigation

Conçue pour les utilisateurs avancés et les MSSP, l'option Threat Intel and Investigation (TII) de Vade permet aux centres des opérations de sécurité (SOC) d'acquérir les informations dont elles ont besoin pour mener des enquêtes, vérifier la présence de menaces sur plusieurs réseaux et élaborer des capacités de réponse aux incidents sans pour autant multiplier les outils de cybersécurité habituellement nécessaires pour suivre et analyser les données.

Avec cette solution, les SOC peuvent exporter les journaux d'email vers leur solution SIEM, XDR ou EDR, analyser des pièces jointes et fichiers à l'aide des outils Vade pour les fichiers PDF et Microsoft Office, et télécharger des emails et pièces jointes pour les étudier. TII donne également accès à de nombreuses API de Vade.

Module pour Splunk

Le module Vade for M365 pour Splunk permet aux partenaires et clients de Vade d'intégrer les journaux d'emails de Vade for M365 à Splunk sans avoir à coder de solution dédiée. L'exportation des journaux d'emails de Vade for M365 vers Splunk permet de combiner les informations sur les menaces de Vade aux fonctions SIEM et SOAR de Splunk. Cette association offre aux services informatiques une meilleure visibilité sur les menaces et des informations exploitables leur permettant de lancer des réponses rapides.

BOUCLE DE RÉTROACTION

La cyberprotection prédictive de Vade for M365 repose sur une boucle de rétroaction. **En effet, Vade for M365 s'appuie sur des informations sur les menaces issues de plus de 1,4 milliard de boîtes aux lettres dans le monde.** Toutes ces informations permettent d'affûter la précision de son moteur d'IA et de rester au fait des dernières cybermenaces. Les faux négatifs et positifs sont ainsi limités, et Vade for M365 peut intercepter 10 fois plus de menaces avancées que la solution EOP de Microsoft. Fidèle à son approche centrée sur l'humain, Vade simplifie aussi le signalement des menaces par les utilisateurs, dont les rapports sont utilisés en continu pour améliorer la solution. Les utilisateurs peuvent ainsi signaler des emails suspects directement depuis Outlook, en un seul clic.

3. Vade. "The Time for MSPs is Now: The SMB Cybersecurity Landscape Report 2022." https://info.vadesecure.com/en/the-2022-smb-cybersecurity-landscape-report-survey-results

Solution basée sur des API, unifiée et autonome

Vade for M365 élimine le principal obstacle que rencontrent les entreprises et les MSP dans la mise en place d'une cyberdéfense : le manque de temps, de ressources et d'expertise. De plus, cette solution est basée sur des API et s'intègre nativement à Microsoft 365. Elle est donc installée dans le tenant Microsoft, reste invisible pour les hackers et ne nécessite pas de modification des enregistrements MX. Facile à utiliser et installer, elle complète EOP et Microsoft Defender for Office 365, offre une protection contre les attaques internes et ne nécessite aucune quarantaine externe.

À PROPOS DE VADE

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 organisations contre les attaques véhiculées par email, y compris les malwares/ransomwares, le spear phishing, les attaques Business Email Compromise et le phishing. Fondée en 2009, Vade protège 1,4 milliard de messageries professionnelles et personnelles et propose aux marchés des FAI, entreprises et MSP des solutions et produits acclamés qui permettent de renforcer la cybersécurité et d'accroître l'efficacité informatique.

Suivez-nous sur
Twitter et **LinkedIn**

Abonnez-vous à notre blog:
www.vadesecure.com/fr/blog