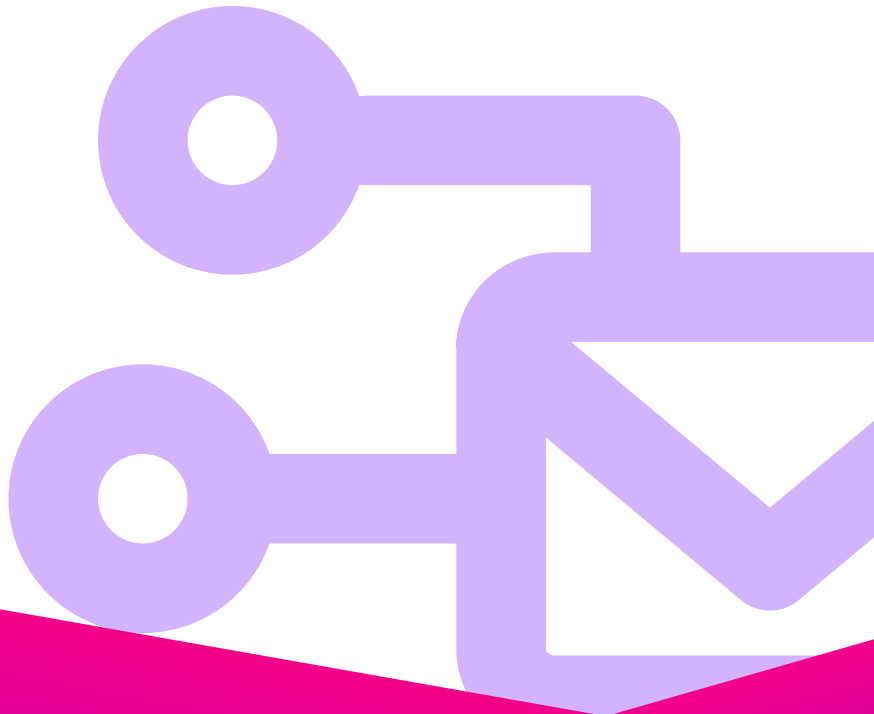
vade

Créez un service de sécurité managé évolutif avec Vade for M365



SOMMAIRE

Introduction 2

I. Sécurité de l'email : un besoin essentiel pour vos clients, une opportunité exceptionnelle pour vous 4

II. Protéger les emails de vos clients n'était pas simple... jusqu'à maintenant 5

III. Présentation de Vade for M365: le moteur d'une offre solide de services de sécurité managés 6

Fonctions intégrées pensées pour les MSP 7

MSP Response 7
Threat Coach 8
Auto-Remediate 8
La puissance de l'intelligence artificielle 9

IV. Conclusion 9

À propos de Vade 10

INTRODUCTION

2020 est maintenant derrière nous, mais les bouleversements apportés par la pandémie restent bel et bien d'actualité. La profondeur et l'envergure de ces transformations, intervenues en l'espace de quelques mois seulement, ont mis en difficulté de nombreuses PME. Désarmées, celles-ci ont aujourd'hui besoin de nouvelles compétences et stratégies pour faire face au « monde d'après ».

D'un côté, la demande en nouveaux produits et services digitaux ne cesse d'augmenter, une opportunité colossale pour les entreprises capables d'évoluer et de répondre à ce besoin. De l'autre, les menaces pesant sur la cybersécurité se font plus fortes, et les stratégies d'attaque du moment sont potentiellement plus dévastatrices que jamais.

Les MSP prêts à aider leurs clients à naviguer dans ces méandres connaîtront certainement un boom d'activité dans les mois et années à venir. Les mieux préparés à répondre aux exigences de ce nouveau monde des affaires, plus dynamique, rafleront la mise.

Une récente enquête conduite par Datto témoigne de l'écart toujours plus important entre les MSP les plus performants et leurs homologues moins développés : seuls 20 % des MSP connaissent une croissance annuelle de plus de 20 % sur les 3 dernières années.[1] La caractéristique de ces leaders ? Générer plus de revenus issus des services managés que la moyenne. Ils sont ainsi capables de maintenir des revenus élevés et réguliers, tout en proposant ce qu'attendent le plus leurs clients : des offres à forte valeur ajoutée qui les aident à préserver leur productivité et leur rentabilité.

Les services managés, notamment la sécurité de l'email et la gestion des terminaux, génèrent actuellement 53 % des revenus des MSP, tandis que les interventions ponctuelles n'en représentent que 10 %. Par ailleurs, chaque augmentation de 10 % des revenus des MSP imputables aux services managés entraîne une hausse de leur croissance annuelle comprise entre 0,25 et 0,75 point.

> ***Chaque augmentation de 10 % des revenus des MSP imputables aux services managés entraîne une hausse de leur croissance annuelle comprise entre 0,25 et 0,75 point.***

Cette tendance a toutes les chances de se poursuivre au cours des années à venir. D'après une enquête conduite en 2020 par CompTIA, 67 % des entreprises affirment être à la recherche d'un partenaire supplémentaire pour renforcer la protection de leurs collaborateurs en télétravail. 75 % des professionnels de sécurité informatique et des services managés expliquent avoir constaté une multiplication des opportunités commerciales depuis début 2020.[2]

Conclusion ? Les MSP souhaitant atteindre leurs objectifs de croissance doivent se mettre en quête de sources de revenus récurrents, et notamment s'intéresser aux services managés. En plus de combiner simplicité de gestion et forte valeur ajoutée pour les clients, ces services suscitent en effet actuellement un véritable engouement.

[1] Datto. *Datto's 2020 State of the MSP Report.* https://www.datto.com/resource-downloads/Datto2020_State-of-the-MSP-Report.pdf

[2] CompTIA. *The Sudden Shift to Remote Work is Driving Business for Tech Firms During COVID-19.* https://connect.comptia.org/blog/tech-business-covid-19

I. Sécurité de l'email : un besoin essentiel pour vos clients, une opportunité exceptionnelle pour vous

Depuis des années, l'email constitue le principal point d'entrée des malwares et des scams basés sur l'ingénierie sociale. Depuis 2020, le nombre de menaces véhiculées par les emails a pourtant encore augmenté. Le phishing a ainsi joué un rôle dans 36 % des violations analysées dans le rapport de recherches 2021 de Verizon sur la fuite de données : il s'agit de la menace la plus exploitée de l'année. Ce chiffre représente une hausse non négligeable par rapport à l'année précédente, car le phishing ne représentait que 25 % des cas en 2019. D'après le rapport 2020 du FBI en matière de cybercrime, le nombre d'attaques de phishing a doublé en valeur absolue par rapport à l'année précédente.

Une majorité de ces attaques par email ciblait l'écosystème Microsoft 365. La demande pour les services Cloud de ce type a littéralement explosé pendant la pandémie, car les entreprises avaient besoin de solutions leur permettant de basculer rapidement vers le télétravail. Alors qu'il s'agissait déjà de la suite logicielle la plus utilisée fin 2019 avec 200 millions d'utilisateurs actifs, Microsoft 365 a atteint pas moins de 258 millions d'utilisateurs à la fin du deuxième trimestre 2020.

Cette croissance du nombre d'utilisateurs de Microsoft 365 et le nombre de cyberattaques véhiculées par les emails ont une conséquence directe : les comptes Microsoft risquent d'être particulièrement visés par les hackers. Après tout, la dominance de la firme de Redmond en faisait déjà une cible de choix pour les attaquants : le géant de la tech a dominé le podium des marques les plus usurpées pendant 4 des 6 trimestres passés. Une étude a également montré que 71 % des utilisateurs de Microsoft 365 ont été victimes d'une usurpation de compte au cours de l'année passée.

> ***71 % des utilisateurs de Microsoft 365 ont été victimes d'une usurpation de compte au cours de l'année passée.***

[3] Verizon. *2021 Data Breach Investigations Report.* https://enterprise.verizon.com/resources/reports/2021/2021-data-breach-investigations-report.pdf?_ga=2.42100261.1805425503.1621456782-104164624.1620685073

[4] Federal Bureau of Investigation. *Internet Crime Complaint Center. Internet Crime Report 2020.* https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf

[5] Microsoft. *"Earnings Release FY21 Q2: Microsoft Cloud Strength Drives Second Quarter Results".* https://www.microsoft.com/en-us/Investor/earnings/FY-2021-Q2/press-release-webcast

[6] Vade. *"A Year Like No Other: Phishers' Favorite Brands of 2020".* https://www.vadesecure.com/en/blog/phishers-favorite-brands-2020

II. Protéger les emails de vos clients n'était pas simple... jusqu'à maintenant

Il paraît évident que les clients des MSP ont toujours besoin de davantage de protections plus efficaces des comptes de messagerie de leurs utilisateurs, et par là même, de l'ensemble de leur environnement informatique. En effet, les emails servant de passerelle aux attaques, personne ne doit donc prendre le risque de voir une attaque contre un compte Microsoft 365 réussir.

Certaines entreprises sont tentées de se reposer uniquement sur les solutions de sécurité intégrées de Microsoft, mais des tests indépendants ont montré que ces solutions n'étaient pas satisfaisantes. Microsoft Exchange Online Protection (EOP) et son service complémentaire, Defender (précédemment nommé Advanced Threat Protection (ATP)) se sont ainsi classés dernier et avant-dernier en matière de taux de détection et de taux de faux positifs par rapport aux solutions de sécurité de l'email d'autres fournisseurs lors de tests réalisés par des experts dans les menaces sophistiquées.

Toutefois, la mise en place d'une nouvelle offre de services de sécurité managés n'est pas toujours évidente. L'ajout de solutions de cybersécurité autonomes à votre arsenal peut alourdir la charge de travail et les tâches administratives de vos employés. Vous risquez ainsi d'être contraint de recruter ou de faire certifier certains membres de vos équipes selon les spécifications des fournisseurs. Ce processus peut s'avérer à la fois lourd et coûteux, surtout au vu de l'importance du déficit de compétences actuel en matière de cybersécurité.

En vérité, même si les services de cybersécurité (et notamment la sécurité de l'email) s'annoncent comme l'une des sources de revenus des MSP qui connaîtront la plus forte croissance cette année, votre marge sera nulle si vos coûts administratifs sont trop importants. Une solution facile à administrer pour de nombreux clients depuis un tableau de bord unique, et qui n'exige pas de compétences techniques pointues ou de certifications spécifiques répondrait donc à un vrai besoin.

> ***Même si les services de cybersécurité s'annoncent comme l'une des sources de revenus des MSP qui connaîtront la plus forte croissance cette année, votre marge sera nulle si vos coûts administratifs sont trop importants.***

[7] SE Labs. *Email Security Services Protection. Jan-Mar 2020.* https://selabs.uk/reports/email-security-services-protection/

[8] Altaro Software. *"70% of MSPs saw increased revenue as companies work from home"*. https://www.altaro.com/msp-dojo/msp-survey-microsoft-365/

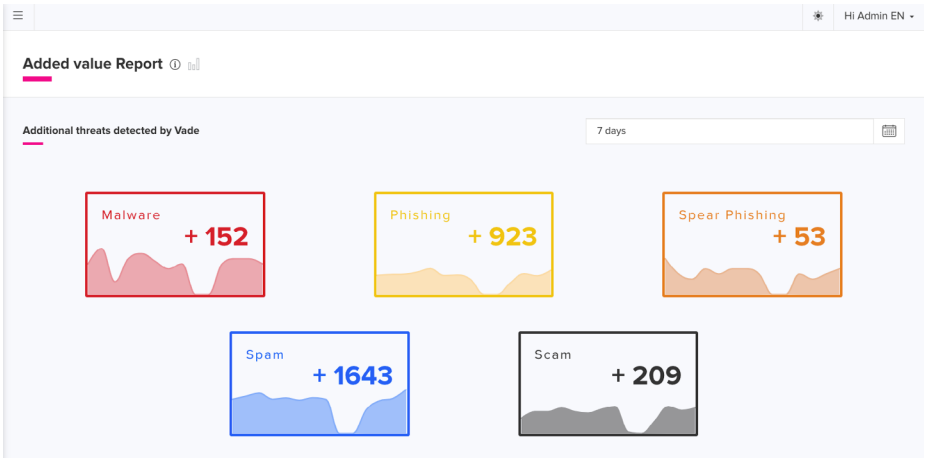
III. Présentation de Vade for M365: le moteur d'une offre solide de services de sécurité managés

Vade for M365 est une solution pensée pour les MSP, conçue pour les aider à proposer un service de sécurité managé solide pouvant être facilement intégré à une offre, vendu et géré. Son architecture repose sur une intégration aux API de Microsoft 365 pour permettre un déploiement rapide et une expérience Outlook native côté utilisateurs finaux. L'intégration aux API offre aussi de nombreuses fonctions et avantages aux MSP :

- Aucune modification des enregistrements MX ;
- Invisibilité de la solution lors d'une interrogation des enregistrements MX ;
- Remédiation post-réception ;
- Simplicité de configuration (paramètres à activer/désactiver) ;
- Boucle de rétroaction automatisée ;
- Assimilation des paramètres Microsoft Exchange

Vade for M365 assure une protection contre les menaces par email dynamiques du moment en tirant profit du machine learning et de la Computer vision pour détecter les tentatives de phishing et spear phishing (business email compromise). Le moteur de filtrage de Vade combine heuristique et IA pour repérer les malwares et ransomwares en temps réel, sans quarantaine ni latence pour les utilisateurs finaux. Dans une évaluation comparative menée en 2021 sur 330 000 emails reçus par un tenant en production sur lequel Microsoft EOP et Defender étaient activés, Vade a bloqué neuf fois plus de menaces sophistiquées que Microsoft Defender. Les « menaces sophistiquées » sont les menaces qui ne sont pas détectées par Microsoft EOP.

> ***Dans une évaluation comparative menée en 2021 sur 330 000 emails reçus par un tenant en production sur lequel Microsoft EOP et Defender étaient activés, Vade a bloqué neuf fois plus de menaces sophistiquées que Microsoft Defender***



Menaces manquées par Microsoft et bloquées par Vade for M365

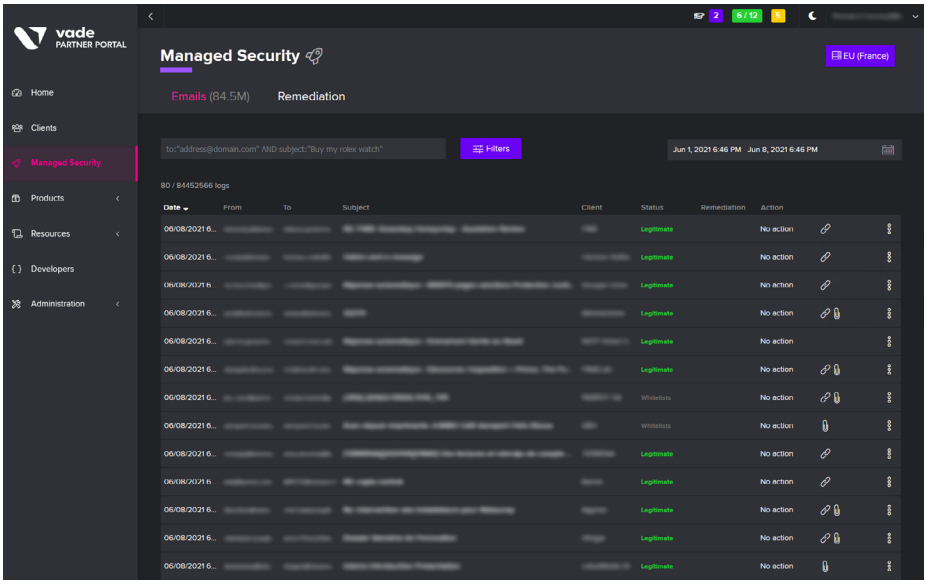
En plus de la protection contre les menaces, Vade for M365 propose des fonctions intégrées sans frais supplémentaires. Ces fonctions automatisées ont pour but d'aider les MSP à aller au-delà de la vente de licences pour bâtir une offre de services managés évolutive sans avoir à recruter des experts en sécurité ni être soumis à des frais de licences et de modules complémentaires en plus.

> ***Ces fonctions automatisées ont pour but d'aider les MSP à aller au-delà de la vente de licences pour bâtir une offre de services managés évolutive***

Fonctions intégrées pensées pour les MSP

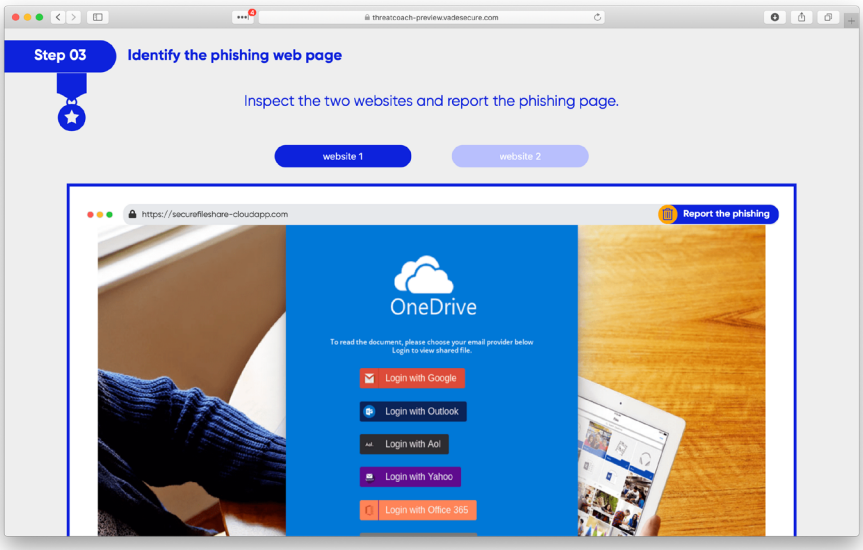
MSP Response

MSP Response unifie la gestion des menaces et la réponse aux incidents sous forme de Dashboard unique dans le Portail Partenaire Vade. Son interface multilocataire réunit ainsi l'ensemble de vos tenants Microsoft 365. Si vous repérez une menace dans l'un des journaux d'emails de vos clients, vous pouvez déterminer en un clin d'œil si cet email a été remis à d'autres clients et en éliminer toutes les instances chez l'ensemble de votre clientèle, en un clic.



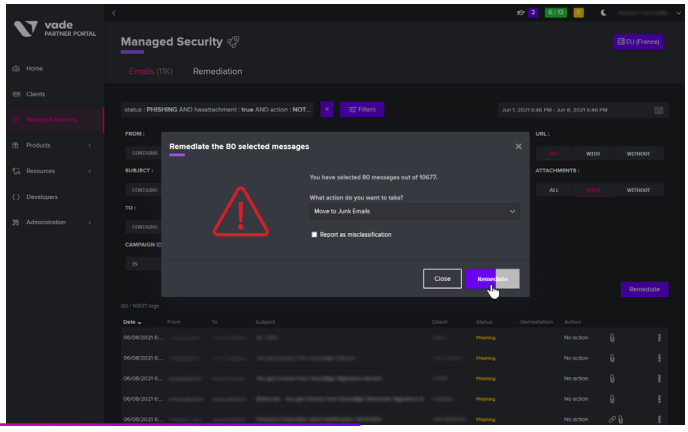
Threat Coach

Threat Coach est un outil de formation automatisée des utilisateurs qui lance une campagne de sensibilisation ciblée en fonction de leur comportement. Il utilise des exemples actuels d'emails de phishing et d'autres menaces pour faire le lien entre attaques simulées et sensibilisation de routine. À la différence des simulations basées sur des modèles, Threat Coach utilise de véritables emails de phishing, interceptés par Vade. Les exemples sont générés automatiquement en fonction des types d'emails reçus habituellement par l'utilisateur et des marques qui les envoient.



Auto-Remediate

Le moteur de filtrage de Vade analyse en moyenne 100 milliards d'emails chaque jour et plus d' 1 milliard de boîtes aux lettres. Capable d'apprendre de manière autonome, l'IA étudie en continu ces boîtes aux lettres et élimine les menaces déjà remises, sans action de l'administrateur. Les administrateurs peuvent également neutraliser des messages manuellement en un clic. Auto-Remediate repose sur le flux continu d'informations liées aux menaces détectées, aux signalements des utilisateurs et à nos équipes des SOC et de recherche, qui affinent en permanence le moteur.



La puissance de l'intelligence artificielle

L'intelligence artificielle est une discipline scientifique visant à créer des ordinateurs capables de reproduire les capacités humaines de résolution des problèmes et de prise de décision. Dans des solutions de sécurité de l'email de pointe comme Vade for M365, l'IA permet de se détacher de la simple détection basée sur la signature pour repérer les menaces plus discrètes et évoluées que les autres outils, comme ceux intégrés aux solutions Microsoft, ne voient pas. Pour y parvenir, l'IA apprend en continu de la base d'utilisateurs de Vade. Avec plus de 1 milliard de boîtes aux lettres protégées qui sont autant de sources d'informations sur les dernières menaces, l'intelligence de Vade for M365 est actualisée en continu et reconnaît les dernières stratégies d'attaque mondiales en date.

Vade for M365 est une solution simple d'utilisation. Conçue pour être déployée en 10 minutes, elle ne demande pas de configuration complexe et offre une expérience Outlook native, simple et intuitive.

IV. Conclusion

En offrant à vos clients une défense proactive basée sur l'IA, vous préservez leur productivité et leur rentabilité. Armé d'une unique solution pensée avant tout pour la simplicité d'utilisation, vous pouvez proposer une offre de services de sécurité managés sans lourdeurs administratives. En parallèle, vous bénéficierez des meilleures ventes, campagnes marketing et assistance technique du marché. Avec Vade, vous avez l'esprit tranquille : la route de votre succès est déjà toute tracée.

À propos de Vade

Vade aide les MSP et les FAI à protéger leurs utilisateurs contre les cybermenaces sophistiquées telles que le phishing, le spear phishing, les malwares et les ransomwares. La solution de protection de l'email proactive de notre entreprise utilise l'intelligence artificielle et les données d'un milliard de messageries afin de bloquer les attaques ciblées et novatrices dès le premier email. Qui plus est, la détection des menaces en temps réel permet aux Security Operations Centers (SOC) d'identifier instantanément les nouvelles menaces et de coordonner les interventions pertinentes. La technologie de Vade peut s'utiliser en tant que solution native basée sur des API pour Microsoft 365, en tant que solution basée sur le Cloud, ou encore comme des API extensibles et peu volumineuses pour les SOC.

Suivez-nous sur

@vadesecure

Abonnez-vous à notre blog
www.vadesecure.com/en/blog