IDC Technology Spotlight

Sponsorisé par : **Vade Secure**

Auteur :

Konstantin Rychkov

Avril 2019

Le nouveau paradigme de la messagerie impose de nouvelles approches en matière de sécurité

Les entreprises misent sur la co-innovation pour supporter leurs initiatives de transformation. La messagerie reste toutefois leur principal moyen de communication et le premier vecteur d'attaques. Les solutions de sécurité de la messagerie sont désormais aussi sophistiquées que celles destinées aux terminaux et aux réseaux. Les professionnels de la sécurité doivent cependant renforcer les solutions technologiques et les processus destinés à sécuriser leur messagerie pour qu'elles soient adaptées au nouveau paradigme de la messagerie électronique.

Renforcer la sécurité de l'information à l'aide de technologies novatrices

La transformation numérique n'est plus une option pour les entreprises : il s'agit désormais d'un impératif. Une enquête mondiale menée par IDC auprès de 1 200 cadres dirigeants a montré que seules 3 % des entreprises n'ont aucune stratégie ou initiative en matière de transformation numérique, tandis que 63 % ont créé un lien étroit entre leur stratégie numérique et leur stratégie d'entreprise. Ce processus leur impose de repenser totalement leur métier et de s'appuyer sur des technologies telles que l'intelligence artificielle, le Big Data, l'Internet des objets, l'edge computing, le mobile et le Cloud afin de transformer l'expérience clients, mais aussi leurs processus et leurs infrastructures internes.

Cette économie de l'information a une implication très importante pour les professionnels de la sécurité : la disparition du périmètre. L'infrastructure de l'entreprise empêche en effet l'utilisation de stratégies basées sur la sécurité périmétrique, car la frontière entre l'entreprise et le monde extérieur à tendance à s'estomper, voire à disparaître. La place croissante des collaborateurs en mobilité et le recours massif aux infrastructures dans le Cloud confèrent aux données et à l'identité une importance capitale dans la stratégie de sécurité des entreprises. Pourtant, la transformation numérique se traduit pour nombre d'entre elles par la migration des données et des systèmes d'identification vers des infrastructures externes. Les entreprises en pleine transformation font ainsi face à de nouvelles menaces et à de nouveaux vecteurs d'attaques qui nécessitent d'adopter une approche inédite et multi-niveaux de la protection.

La collaboration s'impose, une nouvelle frontière apparaît

La transformation numérique des entreprises est naturellement vue comme un changement important dans la manière d'utiliser la technologie, associée à une véritable révolution culturelle. Le principal changement repose sur l'abolition des silos d'informations, qui permet de travailler de manière plus collaborative. Désormais, la collaboration est la clé de l'innovation, elle impacte tout autant les communications internes, l'écosystème des partenaires, les fournisseurs et autres tiers de l'entreprise.

Bien que les messageries instantanées soient toujours utilisées pour des communications ponctuelles et que les outils de productivité intègrent des fonctions collaboratives plus sophistiquées, l'email reste le principal moyen de communication des entreprises. Avec la montée en puissance des plateformes de collaboration, les emails évoluent, que ce soit sur le plan de l'architecture ou de l'intégration. La palette de solutions pour l'entreprise ne cesse de s'élargir. Certains experts affirment que la transformation numérique va enterrer l'email. Pourtant, IDC prévoit un taux de croissance annuel moyen (TCAM) de +7,5 % jusqu'en 2022 : les « rumeurs » de sa disparition semblent ainsi exagérées. L'email reste le moyen de communication numérique le plus efficace et le plus prisé par les entreprises : plus de la moitié de la planète l'utilise (3,7 milliards de personnes).

Cette popularité fait de lui le premier vecteur des attaques lancées par les cybercriminels : c'est par un email que commencent ainsi plus de 80 % des attaques. Le dernier rapport Verizon Data Breach Investigations (base de données) suggère que 45,5 % des failles commencent par un email, soit presque deux fois plus que l'année dernière.

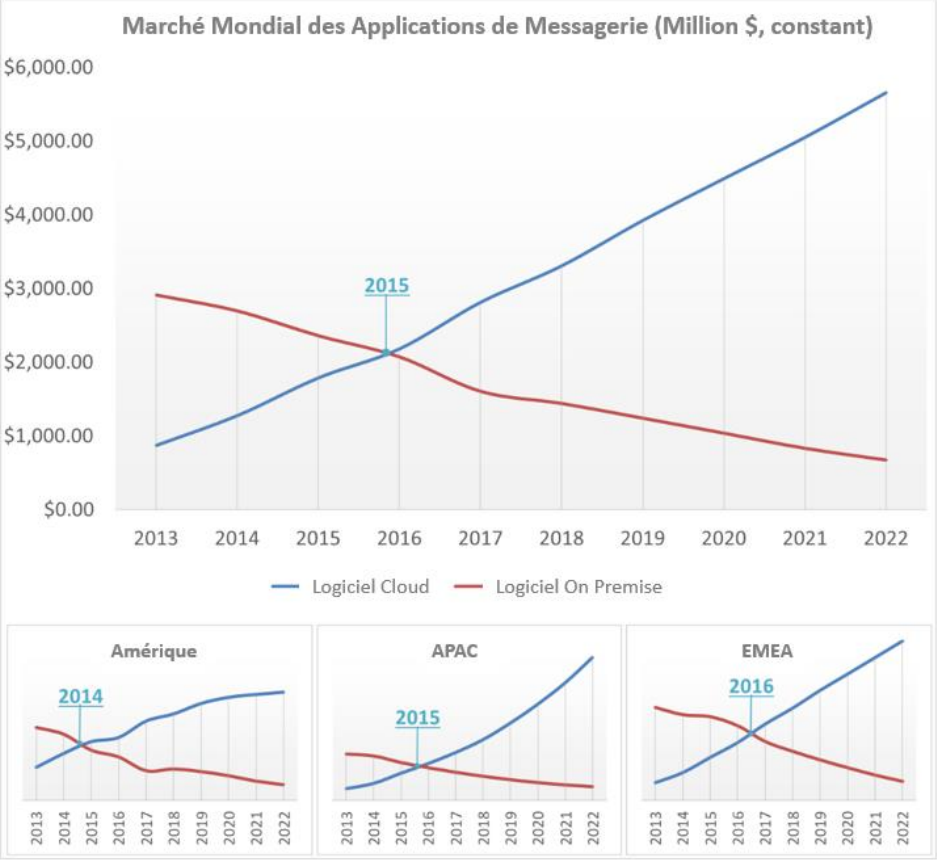
À mesure que les emails gagnent en importance en incluant toujours plus de fonctions collaboratives et en intégrant une palette toujours plus large d'applications de productivité, la possibilité de propagation des menaces au sein d'un centre de données et de leur diffusion sur l'infrastructure d'entreprise augmente de manière exponentielle. La valeur cumulée des actifs exposés suit la même tendance et attise les convoitises.

Nouvelles architectures

Le Cloud constitue l'une des pierres angulaires de la transformation numérique. Son intérêt en matière de flexibilité, d'évolutivité et de coût a entraîné une accélération de son adoption au cours des dernières années. Les applications dans le Cloud, accessibles à tout moment et depuis n'importe quel appareil, éliminent la nécessité d'effectuer une maintenance et des mises à niveau des infrastructures régulières, et réduisent les temps d'arrêt et autres interruptions.

Les applications de messagerie étant omniprésentes dans les entreprises, la migration vers des plateformes d'email dans le Cloud était inévitable. L'enquête d'IDC montre qu'en 2018, 68,4 % des emails étaient déjà dans le Cloud et qu'en 2022 ce chiffre atteindra 89,4 % (voir Figure 1). Le point de bascule est survenu entre 2014 et 2016, l'Amérique ayant été la première région à sauter le pas.

Figure 1 : Le Cloud constitue l'option de déploiement privilégiée pour les applications de messagerie depuis 2015-2016



Source: IDC Worldwide Software tracker, 2018

La possibilité d'intégration à d'autres solutions par l'intermédiaire d'API pour assurer l'agilité et l'efficacité des opérations métiers explique également pourquoi les entreprises préfèrent les infrastructures de messagerie Cloud à celles sur site.

Cette même raison explique la prédominance d'Office 365 et des applications de messagerie de Microsoft en général sur le marché de la messagerie Cloud d'entreprise.

En réalité, la transition vers la messagerie en mode Cloud est principalement portée par l'adoption des solutions de Microsoft et de Google. Toutefois, cette normalisation des plateformes suscite inévitablement l'intérêt des hackers et accroît les risques pesant sur les déploiements « approximatifs ». Fournisseur d'infrastructures de messagerie Cloud de premier plan, Microsoft (mais aussi son concurrent Google) attire les acteurs malintentionnés du monde entier. Pour limiter les risques de sécurité posés par ces plateformes, il convient d'adopter des mesures et solutions de sécurité à la fois natives et pensées pour le Cloud.

Le Cloud n'est pas qu'un moteur d'efficacité opérationnelle : c'est également aujourd'hui le lieu de stockage de données sensibles. Plus de 40 % des entreprises suivent ainsi un modèle SaaS, PaaS ou IaaS pour le stockage sécurisé de leurs données (emails compris). Toutefois, l'utilisation du Cloud ne décharge pas pour autant l'équipe interne de la gestion de la sécurité. En effet, d'après le modèle de responsabilité partagée, le prestataire de services est comptable (selon le niveau de service) des failles de sécurité au niveau des applications, des plateformes ou des infrastructures, tandis que les données et la gestion des accès restent de la responsabilité du client.

Microsoft propose une solution performante contre la perte de données. Les données sont ainsi très bien protégées en cas d'accès aux serveurs de messagerie de back-end ou d'accès physique au centre de données visant à s'emparer des informations directement depuis un rack de serveurs. Par ailleurs, les capacités d'ATP (Advanced Threat Protection, Protection avancée des menaces), la solution native d'Office 365, se sont considérablement améliorées. Les entreprises ayant opté pour des licences E3 ou E5 peuvent véritablement constater la différence. Pour autant, la modification des règles et mécanismes de remise des emails au sein d'une entreprise et la protection contre l'usurpation d'identité des cadres dirigeants imposent de bien connaître les membres de l'entreprise et leurs façons de communiquer. Ce ne sont pas des prestations que proposent Google, Microsoft ou Amazon. Nous quittons en effet le domaine de l'infrastructure pour entrer dans celui de la sécurité de l'information.

Le sentiment de sécurité qu'inspirent les solutions intégrées des prestataires de services éloigne toujours plus les informations sensibles et transactions des contrôles traditionnels dans lesquels les entreprises ont déjà investi. Il devient ainsi nécessaire d'ajouter un niveau de défense et/ou de vérification côté client. Au final, la migration vers le Cloud offre l'occasion de réévaluer l'architecture de sécurité de l'email et d'optimiser ainsi la continuité de l'activité.

Le fait que les entreprises gèrent les problèmes de sécurité de l'email depuis plus de 20 ans laisse croire, à tort, que la protection de la messagerie ne pose plus aucune difficulté. Rien n'est plus faux !

La place de la sécurité des messageries en mode Cloud

Jusqu'à récemment, la messagerie faisait partie des composants les plus surveillés par les logiciels de sécurité, en particulier dans la mesure où les fonctionnalités de ces derniers sont toujours plus nombreuses à être intégrées dans les principales plateformes de messagerie. Le fait que les entreprises gèrent les problèmes de sécurité de l'email depuis plus de 20 ans laisse croire, à tort, que la protection de la messagerie ne pose plus aucune difficulté.

Effectivement, ces bons vieux spams et les classiques malwares en pièce jointe ne sont plus un problème. Les passerelles de messagerie sécurisées (SEG) classiques et autres solutions similaires, qui se concentrent sur la sécurisation du périmètre, obtiennent des résultats remarquables contre ces menaces. Les défenses basées sur la réputation et la signature bloquent efficacement les menaces connues et sont particulièrement adaptées aux contenus envoyés en volume aux serveurs Exchange internes.

Toutefois, l'adoption du Cloud et la multiplication des attaques ciblées par email ont mis en lumière les faiblesses de ces anciennes architectures SEG :

- Les passerelles de messagerie sécurisées imposent de modifier l'enregistrement Mail Exchange (MX) et ne peuvent ainsi pas s'intégrer efficacement aux solutions de sécurité natives de la plateforme de messagerie. En effet, le trafic étant redirigé, celles-ci n'ont plus accès à l'expéditeur d'origine ni aux informations d'en-tête.

- Par ailleurs, les enregistrements MX des passerelles de sécurité peuvent être contournés et le spam arrive alors directement sur le serveur SMTP (si son adresse IP est connue).
- Lorsque leur paramétrage est trop strict, les passerelles génèrent une quantité phénoménale de faux positifs. Elles interrompent ainsi les opérations et pèsent lourdement sur les ressources limitées dédiées à la sécurité de l'information.
- Les passerelles sont intrinsèquement incapables d'analyser le trafic de messagerie qui transite d'une entreprise à l'autre. En réponse à la montée en puissance des solutions SEG, les hackers ont élaboré des stratégies dites « Business email compromise » (BEC) visant une propagation entre les serveurs d'un même centre de données, la mise en place de plusieurs étapes et d'une procédure d'escalade.
- Les passerelles de messagerie imposent la mise en place et/ou la reconfiguration d'une mise en quarantaine externe pour le spam, ce qui génère une complexité de gestion supplémentaire et nécessite des compétences spécifiques en interne.
- Pour la majorité des professionnels, la faiblesse des fonctions de remédiation des solutions SEG est directement responsable des difficultés de gestion et du manque d'efficacité opérationnelle des politiques de sécurité d'entreprise.

L'architecture des solutions actuelles va s'intégrer aux processus en s'appuyant sur des API natives ouvertes. Cette approche permettra de compléter la sécurité native de la plateforme de messagerie, avec des analyses prédictives et des mécanismes de détection non basés sur la signature.

L'architecture des solutions actuelles va s'intégrer aux processus en s'appuyant sur des API natives ouvertes. Cette approche permettra de compléter la sécurité native de la plateforme de messagerie, avec des analyses prédictives et des mécanismes de détection non basés sur la signature. De plus, étant donné que l'email constitue le principal vecteur d'attaque, la sécurité offerte sera complète : anticipation, gestion des incidents, remédiation et mise à niveau.

Le manque de compétences disponibles en matière de sécurité, ainsi que le temps et les ressources investis par les professionnels pour lutter contre les menaces liées à la messagerie, génèrent un intérêt nouveau pour des produits de sécurité de la messagerie véritablement efficaces. Dans le même temps, la multiplication des nouveaux types d'attaques par email et le passage généralisé aux architectures Cloud génèrent un vif intérêt pour les environnements cloud natifs et cognitifs.

Voici les principaux composants de sécurité nécessaires à une solution moderne de protection des emails :

- **Automatisation :** le manque de spécialistes de sécurité et la nature chronophage de la lutte contre l'impact des menaces provenant de l'email génèrent une forte demande pour des fonctions automatisées de reporting et de remédiation. Les plateformes et produits de messagerie doivent donc chercher de plus en plus à remplacer l'humain dans la gestion de ces menaces. Par ailleurs, la sécurité de l'email doit s'intégrer dans l'automatisation et l'orchestration du reste de la sécurité de l'entreprise pour fluidifier l'ensemble des processus. Pour cela, il est nécessaire de proposer des solutions clés en main et préconfigurées disposant de ces fonctionnalités.
- **Plateforme SaaS :** la mise en place d'une plateforme Saas est rapidement devenue incontournable pour les acteurs du marché de la sécurité de l'email. Les fonctions natives Cloud et l'intégration transparente sont deux éléments clés permettant à la sécurité de faciliter la transformation numérique. Par ailleurs, la prise en charge des environnements hybrides restera un point important pour simplifier la tâche des entreprises en pleine transition vers les solutions Cloud de messagerie.
- **Microservices / architecture modulaire :** l'adoption de nouvelles technologies et infrastructures a modifié les applications de messagerie classiques, qui sont devenues modulaires. Les utilisateurs les plus avancés demandent désormais des solutions de sécurité compatibles avec les API et capables de s'intégrer en toute transparence à l'environnement global de sécurité de l'entreprise.

- **Conformité :** les solutions de sécurité de l'email doivent tout faire pour respecter le maximum de normes imposées aux diffétents secteurs d'activité. Ce point est particulièrement important pour les secteurs fortement réglementés, comme la finance, l'administration centrale et les collectivités locales, ou encore le secteur de la santé. La non-conformité des solutions de sécurité peut tout simplement les empêcher d'accéder à ces marchés rémunérateurs.

- **Analyse et protection spécialisées des menaces (STAP) :** la STAP constitue un niveau supplémentaire de sécurité de l'email qui permet de détecter les menaces sans signature capables de passer entre les mailles de nombreuses méthodes de détection traditionnelles. Elle est généralement nécessaire pour assurer une protection contre le spear phishing, les ransomwares et le whaling par le biais de l'analyse comportementale, la vision par ordinateur, la détection d'anomalies, l'exploration de l'URL et de la page au moment du clic, ainsi que d'autres stratégies. La prolifération de ces menaces et les dégâts importants qu'elles peuvent causer imposent désormais de recourir à ce composant dans toutes solutions de sécurité de l'email pensées pour l'entreprise.

- **Sensibilisation et formation :** la montée en puissance de l'automatisation est directement liée à la recherche d'une plus grande efficacité. Pour autant, cette recherche d'efficacité impose également de renforcer la sensibilisation et la formation des collaborateurs à la sécurité. En effet, ce sont bien souvent les faiblesses humaines que visent les menaces. De plus, l'apprentissage en continu et la correction des comportements doivent compléter les sessions ponctuelles de formation des collaborateurs.

Pourquoi confier la sécurité de l'email à Vade Secure ?

Vade Secure est un spécialiste de la sécurité de l'email et propose un produit spécifiquement conçu pour Office 365. L'entreprise a recours à des méthodes de défense proactives et à l'apprentissage automatique pour renforcer les mécanismes de protection intégrés de la plateforme. Par ailleurs, elle améliore l'expérience des utilisateurs en prenant en charge la gestion des emails non prioritaires.

Ses solutions sont conçues pour assurer une protection dans le Cloud non intrusive contre le spear phishing, les attaques sophistiquées et dynamiques par email en plusieurs étapes, le phishing, ainsi que les malwares et ransomwares polymorphes zero-day. Vade Secure propose des mécanismes de signalement et de remédiation permettant une intégration aux outils et workflows SOC et/ou SIEM. Ainsi, il devient possible d'exploiter les processus de détection pour mettre à jour les politiques de réponses aux incidents et les règles.

Vade Secure adopte une approche globale pour bloquer les menaces avant, pendant et après l'attaque : anticiper, décimer, remédier (voir Figure 2). Cette approche est basée sur la collaboration et la complémentarité entre l'humain et la technologie.

Figure 2 : Approche de la sécurité de l'email de Vade Secure

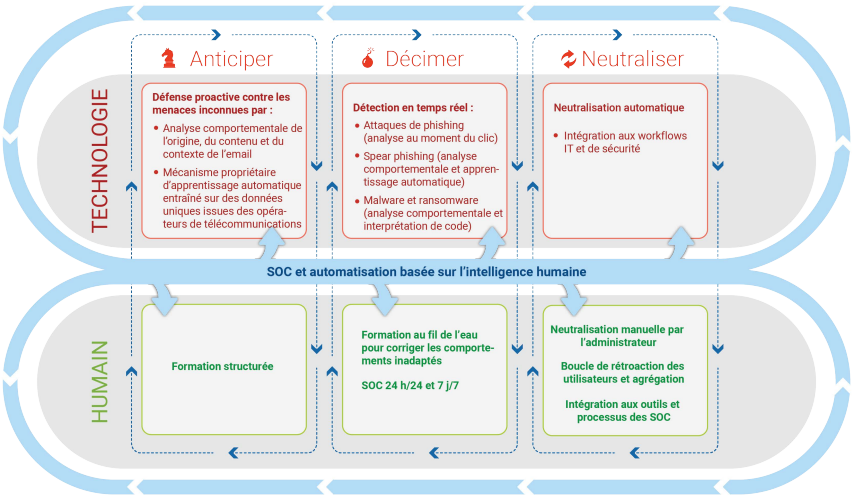


Image fournie par Vade Secure

La solution Vade Secure pour Office 365 peut être déployée en appelant des API. Les autres solutions de la gamme permettent le déploiement d'une passerelle en ligne proposant une configuration clés en main, similaire à celle d'un service.

Caractéristiques clés de Vade Secure pour Office 365

Vade Secure exploite les données de 600 millions de boîtes aux lettres protégées par sa technologie et hébergées par des FAI et fournisseurs de télécommunication du monde entier. Vade Secure entraîne ses algorithmes d'apprentissage automatique pour qu'ils détectent le phishing, le spear phishing, les malwares et le gray mail. Des accords de partage avec les FAI visant une amélioration du service permettent à Vade Secure d'utiliser l'email plutôt que les métadonnées pour recueillir des informations sur les menaces. Ces informations sont habituellement très difficiles à obtenir auprès des entreprises clientes en raison de la réglementation sur la confidentialité des données. Vade Secure a donc choisi de collaborer avec des FAI pour y accéder et les exploiter dans ses solutions à destination des entreprises.

Grâce à ces volumes massifs de données (en moyenne, plus de 10 milliards d'emails et des millions de retours utilisateurs chaque jour), Vade Secure peut entraîner des modèles précis et réduire le nombre de caractéristiques pour une précision optimale. Les modèles identifient les menaces inconnues par une analyse comportementale qui tient compte de l'origine de l'email, de son contenu et de son contexte. De plus, ils appliquent des algorithmes heuristiques pour détecter les menaces au lieu de s'appuyer sur des signatures prédéfinies. À l'aide de techniques propriétaires d'extension des données permettant d'augmenter la taille de l'échantillon, les algorithmes d'apprentissage automatique de Vade Secure sont également entraînés à intercepter les tentatives isolées, voire uniques de spear phishing. Les capacités de la solution de sécurité de Vade Secure pour Office 365 sont résumées dans la Figure 3.

Figure 3 : Protection à 360° pour Office 365 contre toutes les menaces

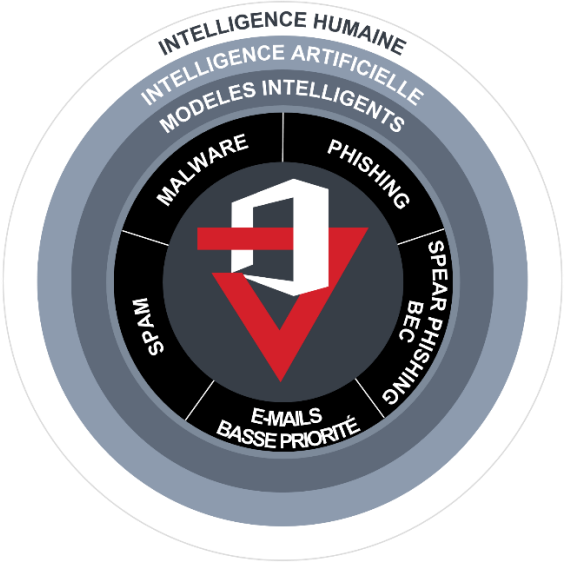


Image fournie par Vade Secure

Plus précisément, la solution de Vade intègre les technologies suivantes :

Contre le "phishing"

- **Anonymisation des jetons :** les jetons contenus dans les URL sont remplacés de manière aléatoire pour pouvoir explorer en toute sécurité le contenu de la page au nom de l'utilisateur sans déclencher d'action/de suivi. Cette fonction est essentielle pour l'analyse au moment du clic, qui bloque les attaques basées sur des liens dynamiques et des pages dormantes.

Grâce à son intégration native avec l'API de Microsoft, Vade Secure pour Office 365 utilise et renforce EOP. Elle propose ainsi une fonctionnalité non native complémentaire.

- **Rendu mobile :** les pages sont explorées avec plus de 30 combinaisons d'appareil/de navigateur (par ex. Safari sur iPhone, Chrome sur Android) pour bloquer les attaques conçues pour ne s'afficher que sur des appareils mobiles.
- **Exploration des pages régionales :** les pages sont explorées depuis quatre régions (Amérique du Nord, Amérique du Sud, Europe et Asie) pour lutter contre les pages de phishing ne s'affichant que lorsque l'internaute est localisé dans la région ciblée.

Contre le "spear phishing"

- **Profilage de l'entreprise :** pour détecter le spear phishing, Vade Secure pour Office 365 commence par extraire le modèle d'entité de l'entreprise par le biais de l'API de Microsoft afin d'identifier les utilisateurs légitimes.
- La fonction de **détection autonome des anomalies** compare ensuite l'expéditeur du message à ce modèle pour repérer les tentatives d'usurpation d'identité, par exemple l'usurpation de l'alias visible ou l'utilisation de domaines voisins.
- De plus, Vade Secure a recours au **traitement du langage naturel** pour analyser le contenu de l'email et détecter les intentions malveillantes et le sentiment d'urgence. La solution s'appuie ensuite sur la combinaison de l'analyse de l'expéditeur et du contenu pour déterminer la probabilité que le message constitue une tentative de spear phishing. Si cette probabilité dépasse un certain seuil, une bannière d'avertissement entièrement personnalisable s'affiche pour alerter l'utilisateur.

La solution de Vade Secure est intégrée à Office 365 via l'API Microsoft Graph. Ce système permet une intégration transparente et non intrusive au serveur Exchange (pas de remplacement de l'enregistrement MX). Le déploiement de la solution est ainsi extrêmement simple, car elle est entièrement préconfigurée et ne nécessite pas de mise en quarantaine externe. De plus, les éléments visibles par l'utilisateur peuvent ainsi être configurés pour afficher des avertissements nativement, c'est-à-dire directement dans Microsoft Outlook et non pas dans un module complémentaire.

Grâce à son intégration native avec l'API de Microsoft, Vade Secure pour Office 365 utilise et renforce Exchange Online Protection (EOP) en proposant ainsi une fonctionnalité non native complémentaire. Il est également capable d'assurer certaines fonctions payantes de Microsoft (accessibles avec une licence E5) en permettant la détection et la remédiation des attaques BEC internes à l'entreprise qui échappent aux passerelles de protection classiques. Vade Secure analyse à la fois les vecteurs internes et externes pour identifier et neutraliser les attaques internes, et propose ainsi une protection efficace contre les menaces internes.

La capacité de remédiation suit deux approches. La première est la gestion manuelle par l'administrateur : la solution guide l'administrateur pour neutraliser la menace. Ces réponses sont enregistrées par les algorithmes d'apprentissage automatique et améliorent les modèles et le processus au fil du temps. La deuxième approche prend davantage en compte l'humain. Elle est basée sur la surveillance des réponses des utilisateurs, encore une fois pour optimiser l'apprentissage automatique. Il s'agit d'une approche intermédiaire entre la formation au fil de l'eau des collaborateurs et la remédiation active.

Lorsque des avertissements sont enregistrés, les algorithmes d'apprentissage automatique surveillent les réponses des administrateurs et des utilisateurs pour apprendre les comportements généraux, mais aussi les comportements spécifiques de certains utilisateurs. Les modèles sont ainsi personnalisés selon le workflow de l'entreprise. Avec le temps, Vade Secure affine ses réponses et les personnalise. En parallèle, les incidents sont consignés dans le SIEM ou tout autre programme de surveillance et signalement centralisé des incidents de sécurité. Vade Secure pour Office 365 se présente sous la forme d'une solution mutualisée évolutive basée sur Azure. Elle dispose de diverses API permettant son intégration à l'infrastructure globale de sécurité de l'entreprise. Il devient ainsi possible de réaliser des intégrations personnalisées avec des solutions pré-déployées. Enfin, la solution bénéficie du soutien d'un centre d'analyse des menaces disponible 24 h/24 et 7 j/7. Il surveille les emails échangés dans le monde entier en continu et déploie des contre-mesures si nécessaire.

Perspectives pour Vade Secure

Vade Secure vise la niche en constante expansion que représentent les solutions natives de sécurité de la messagerie Cloud destinées à une nouvelle vague d'applications collaboratives reposant sur des architectures distribuées. À mesure que les entreprises poursuivent leur migration vers des outils de productivité modernes basés sur le Cloud, la demande pour des solutions similaires à celle de Vade Secure va continuer à augmenter.

À l'avenir, Vade Secure doit continuer à innover et appliquer sa vision d'une nouvelle architecture de sécurité qui regroupe détection des menaces avancées et automatisation de la remédiation des menaces. Une des grandes difficultés qui se pose à l'entreprise réside dans les erreurs commises par les utilisateurs finaux, qui restent responsables de failles en dépit des progrès technologiques. Vade Secure doit montrer à ses clients comment ces erreurs peuvent être corrigées par la complémentarité technologie/humain et la formation continue.

Vade Secure doit également tenir compte des dynamiques du marché, car les prestataires de services de messagerie travaillent activement sur les mêmes problématiques que Vade Secure. IDC estime qu'avec sa feuille de route technologique axée sur l'innovation, sa valeur ajoutée (automatisation, intégration, simplicité, configuration clés en main) et son approche complémentaire, Vade Secure est en bonne voie pour gagner la bataille de la notoriété et des investissements auprès des multinationales qui lancent leurs stratégies de transformation numérique, poussées par leurs besoins en matière de collaboration.

Toutefois, sa concentration sur une seule plateforme d'email (Microsoft Office 365) peut à long terme limiter son potentiel sur le marché et nuire à sa position face aux autres fournisseurs et plateformes. Par conséquent, l'adoption de solutions autres que celles de Microsoft fera partie de sa feuille de route technologique et renforcera considérablement sa stratégie globale. L'entreprise doit commencer par suivre de près le rôle croissant de Google dans le monde des plateformes de messagerie Cloud.

Enfin, pour assurer une intégration fluide à l'ensemble de l'architecture de sécurité des entreprises, Vade Secure doit s'assurer que la documentation publiée sur ses API est complète. Cette exhaustivité permettra en effet une mise en œuvre rapide dans les environnements hétérogènes. Pour faciliter les déploiements et les rendre plus compréhensibles, il pourrait être intéressant de se pencher sur la création de connecteurs pour les solutions les plus fréquemment utilisées en entreprises. Ces connecteurs pourraient à la fois recevoir des données des plateformes de protection des messageries et leur en envoyer. Vade Secure devrait partager ses solutions et feuilles de route liées aux processus d'intégration et aux nouvelles technologies pour que ses clients puissent profiter de ces compétences.

Conclusion

La transformation numérique bouleverse de nombreuses facettes des entreprises, notamment les stratégies de sécurité. L'intérêt croissant pour la collaboration, la multiplication des applications de messagerie Cloud et l'intérêt toujours plus grand des hackers pour l'email en tant que vecteur d'attaques doivent pousser les professionnels de la sécurité à revoir leur stratégie de protection de l'email. Les technologies classiques perdent de leur efficacité dans un monde où les périmètres s'effacent. Il devient ainsi critique d'imaginer de nouvelles architectures de défense.

L'utilisation de couches de protection complémentaires permettra aux entreprises de se concentrer sur davantage d'automatisation, et de recourir à des architectures modulaires ainsi qu'à des plateformes Cloud natives de sécurité de la messagerie, basées sur l'apprentissage automatique. Ceci les aidera à bloquer les menaces inconnues, dynamiques et avancées. L'efficacité de la protection de la messagerie doit être maximisée, grâce notamment à la formation continue des équipes et à des remontées permanentes des informations en provenance des machines afin d'affiner et de personnaliser les mécanismes de défense. Ces stratégies permettront d'établir une protection adaptée à l'environnement dans lequel évolue l'entreprise.

IDC UK

5th Floor, Ealing Cross,
85 Uxbridge Road
London
W5 5TH, United Kingdom
44.208.987.7100
Twitter: @IDC
idc-community.com
www.idc.com

A propos d'IDC

IDC est un acteur majeur de la Recherche, du Conseil et de l'Évènementiel sur les marchés des Technologies de l'Information, des Télécommunications et des Technologies Grand Public. IDC aide les professionnels évoluant sur les marchés IT et les investisseurs à prendre des décisions stratégiques basées sur des données factuelles. Plus de 1 100 analystes proposent leur expertise globale, régionale et locale sur les opportunités et les tendances technologies dans plus de 110 pays à travers le monde. Depuis plus de 50 ans, IDC propose des analyses stratégiques pour aider ses clients à atteindre leurs objectifs clés. IDC est une filiale de la société IDG, leader mondial du marché de l'information dédiée aux technologies de l'information.