FIREEYE

PRÉSENTATION DE SOLUTION

Protection contre les menaces avancées avec Email Security

Présentation

De par son côté personnel et extrêmement malléable, l'e-mail augmente considérablement les chances de réussite d'une attaque. C'est pourquoi il demeure à ce jour le principal point d'entrée des cyberattaques. Certes, les logiciels antivirus et les filtres antispam traditionnels parviennent à intercepter une multitude de menaces de phishing et leur lot de pièces jointes, liens et contenus malveillants. Toutefois, ils se révèlent impuissants face aux attaques ciblées et avancées par spear-phishing ou usurpation d'identité.

Quant aux passerelles de messagerie sécurisées (SEG), la plupart se montrent en général très efficaces face aux spams et aux malwares connus les plus classiques. Cependant, elles n'intègrent pas la CTI, l'expertise et les technologies nécessaires pour bloquer les campagnes d'e-mails malveillantes et les menaces plus élaborées dès leur apparition. En effet, ces passerelles s'appuient sur des filtres antispam et des logiciels antivirus basiques, dont la mission principale consiste à réagir aux menaces de masse. Au final, plusieurs minutes (voire plus face à la diversification des techniques) peuvent s'écouler avant la détection, laissant aux spammers et aux cybercriminels suffisamment de temps pour exploiter la faille. Par ailleurs, inutile de compter sur les pare-feu. Ces derniers sont incapables d'examiner le trafic e-mail qui, souvent, se camoufle via le protocole TLS (Transport Layer Security) pour véhiculer les attaques par ransomware ou spear-phishing.

Spams, ransomwares, e-mails de spear-phishing, campagnes d'impostures… face à la multiplicité des menaces, les solutions de sécurité doivent pouvoir s'adapter rapidement et agir sur plusieurs fronts :

- Détection des menaces avancées dès leur première apparition et sans recours aux signatures
- Identification des menaces critiques avec un minimum de faux positifs
- Blocage immédiat des menaces (p. ex. les ransomwares) pour préserver l'intégrité de l'environnement
- Exploitation des informations préventives sur les attaquants et des données recueillies à partir d'une Cyber Threat Intelligence (CTI) de terrain pour accélérer les interventions

Pourquoi votre solution de sécurité existante ne suffit pas

Souvent initiée par un e-mail de phishing, une violation de données expose les informations, les collaborateurs et les processus d'une entreprise. Elle perturbe ses activités, ternit sa réputation et suscite la défiance de ses clients. Quant à l'impact financier, il s'élève en moyenne à 3,62 millions de dollars par violation[2]. Aujourd'hui, il est très probable que le volume d'e-mails volés au fil des années dépasse celui de toutes les autres formes de vol de données combinées.[3]

Les e-mails sont des cibles faciles pour les hackers. Pour savoir si votre solution actuelle est à la hauteur, posez-vous les bonnes questions :

1. Outre ses fonctions de détection des malwares connus et sa protection antivirus et antispam, votre SEG est-elle capable de bloquer les menaces avancées telles que les pièces jointes infectées et URL malveillantes, les sites de phishing et les techniques d'impostures ?
2. En cas d'alertes, parvient-elle à bloquer les menaces, à les classer par ordre de priorité et à proposer une marche à suivre ?
3. Fournit-elle des informations contextualisées et actualisées qui permettent de s'adapter rapidement à l'évolution des menaces ?
4. S'intègre-t-elle à vos autres outils de sécurité pour gérer les différents vecteurs de menace et vous protéger des attaques combinées ?
5. Peut-elle évoluer au rythme de croissance de votre entreprise ?

91 % des cyberattaques commencent par un e-mail de spear-phishing.[1]

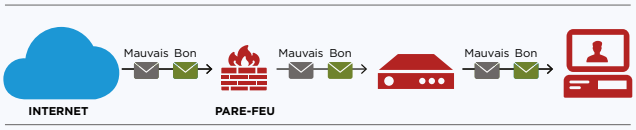
[1] PhishMe (2016). « Enterprise Phishing Susceptibility and Resiliency Report »
[2] Ponemon Institute LLC (juin 2017). « 2017 Cost of Data Breach Study: Global Overview »
[3] Mandiant, une entreprise FireEye (2017). « M-Trends 2017. A View From The Front Lines. »

1 **Alors que les menaces par e-mail ne cessent d'évoluer, bon nombre d'entreprises se tournent vers les services de messagerie dans le cloud.**
Dans un contexte plus large, on assiste à une migration massive de leurs informations, opérations et ressources vers le cloud. Si l'on ajoute à cela la prolifération des appareils connectés, pas étonnant que les cybercriminels fassent du cloud leur nouveau champ de bataille. D'où le besoin croissant d'une sécurité adaptée.

FireEye Email Security Cloud Edition est une passerelle de messagerie sécurisée qui bloque les URL de phishing, les malwares entrants et sortants et les tentatives d'impostures. Équipée d'un module antivirus et antispam, la solution protège votre entreprise contre les campagnes de spam et les usurpations d'identité. Aussi efficace contre les offensives de masse que contre les attaques ciblées et avancées, FireEye Email Security Cloud Edition assure une sécurité complète dans une seule et même solution, permettant ainsi aux entreprises d'exploiter la puissance du cloud pour consolider la sécurité de tout leur environnement de messagerie.

2 **Les dispositifs de défense obsolètes n'offrent qu'une protection illusoire.** Les passerelles e-mail qui s'appuient sur une CTI standard et des informations provenant de tiers (signatures, réputations) ne sont pas faites pour détecter les menaces nouvelles et inconnues. De même, un pare-feu est incapable de contrer les campagnes de ransomware et de spear-phishing perpétrées par e-mail.

Figure 1. Quand les cyberattaques ciblées échappent aux solutions de sécurité traditionnelles.



Leur architecture ne leur permet pas de confiner un e-mail pour l'analyser. Par conséquent, les e-mails contenant des pièces jointes ou des URL malveillantes ainsi que les tentatives d'impostures atterrissent dans les boîtes de messagerie des utilisateurs.

FireEye Email Security aide les entreprises de toutes tailles à réduire les risques de violations de sécurité coûteuses. Capable de détecter et de bloquer les campagnes de spam, FireEye Email Security assure aussi une protection optimale contre les attaques ciblées et avancées qui échappent à d'autres solutions. Pour preuve, lors d'une évaluation POV effectuée récemment pour un grand spécialiste des produits de consommation, FireEye a détecté des milliers de tentatives de phishing et d'impostures qui avaient échappé à la passerelle en place.

3 **Une CTI alimentée par des signatures ne peut suivre le rythme d'évolution des attaques par e-mail.**
Ces flux de données ne sont ni en mesure d'anticiper les attaques, ni de guider une réponse rapide. Au final, tout ce que la multiplication des logiciels et technologies de sécurité spécialisés apporte, c'est une explosion du volume d'alertes. Avec FireEye Email Security, plus besoin d'attendre les informations d'intervenants externes (signatures, réputations). Ses capacités de détection interne lui permettent d'évoluer beaucoup plus vite pour bloquer immédiatement les nouvelles campagnes de spam. Ses algorithmes comparent l'expéditeur du message et son domaine aux noms connus du domaine cible pour déjouer les formes d'usurpation sans malware ni URL malveillante (p. ex., arnaque au président), aujourd'hui en plein essor.

FireEye Email Security se base sur des données issues d'investigations de terrain et d'observations des attaquants pour détecter les éléments à bloquer. Munies de ces informations, les équipes de sécurité disposent du contexte nécessaire pour mieux prioriser les alertes. Les e-mails malveillants sont mis en quarantaine, tandis que des informations précises sur l'attaque et son auteur facilitent la neutralisation des menaces avancées.

Enfin, les traces laissées par les cybercriminels sont partagées à l'échelle mondiale, permettant un blocage immédiat des attaques jusqu'alors inconnues et une accélération des interventions. Les menaces sont détectées avec un minimum d'éléments parasites et de faux positifs. Résultat : les équipes de sécurité peuvent recentrer leurs efforts sur les attaques réelles, avec à la clé une réduction des coûts d'exploitation et du risque organisationnel.

4 **De nombreuses attaques combinent des tactiques visant le réseau (Internet) et la messagerie électronique à différentes étapes dans le but de contourner les dispositifs de protection du réseau ou des e-mails qui ne couvrent qu'une partie de l'attaque.** Une cyberattaque peut se composer d'un malware sophistiqué qui exploite une vulnérabilité zero-day, d'un e-mail de spear-phishing, d'une URL malveillante, voire d'un réseau complexe de serveurs de commande permettant de contrôler les équipements compromis pour effectuer des cyberbraquages.

Bien que les attaques par ransomware commencent par un e-mail, le chiffrement des données passe par le rappel à un serveur de commande et de contrôle (CnC). Ces menaces multi-phases contournent aisément la plupart des environnements sandbox destinés à l'analyse des fichiers dans un milieu isolé. De fait, lorsqu'une solution de sécurité détecte un problème, il est généralement trop tard : les données de la victime sont déjà chiffrées. Les solutions Email Security et Network Security de FireEye interagissent pour détecter et déjouer les attaques combinées. Ensemble, elles examinent le cycle de vie des cyberattaques pour remonter jusqu'à l'e-mail de spear-phishing d'origine et son auteur.

Détection hors-pair des menaces

Pour limiter le risque de violations de sécurité coûteuses, Email Security identifie et isole les attaques avancées, ciblées et furtives qui se camouflent dans le trafic légitime. Une fois détectées, ces attaques sont immédiatement neutralisées, puis analysées et enregistrées pour une identification plus rapide des futures menaces.

Advanced URL Defense et le moteur MVX (Multi-Vector Virtualization Execution™) sont des composants clés de FireEye Email Security. Ces technologies s'appuient sur des fonctions d'analytique et de machine learning de pointe pour identifier les attaques qui échappent aux dispositifs de défense traditionnels basés sur des politiques et des signatures.

Pour la détection d'usurpations d'identité et d'attaques courantes caractérisées par une signature, Email Security Cloud Edition intègre également une protection antivirus et antispam classique.

À l'image des arnaques au président, les impostures et attaques par usurpation d'identité continuent d'avoir un impact financier important sur les entreprises.

Cette situation s'explique en partie par le fait que ces attaques ne comportent aucun des indicateurs de menaces traditionnels (liens malveillants, pièces jointes infectées, etc.). Pour mieux protéger les entreprises, FireEye a développé des algorithmes, systèmes et outils innovants, spécialement pensés pour la détection et la neutralisation de ce type d'attaques.

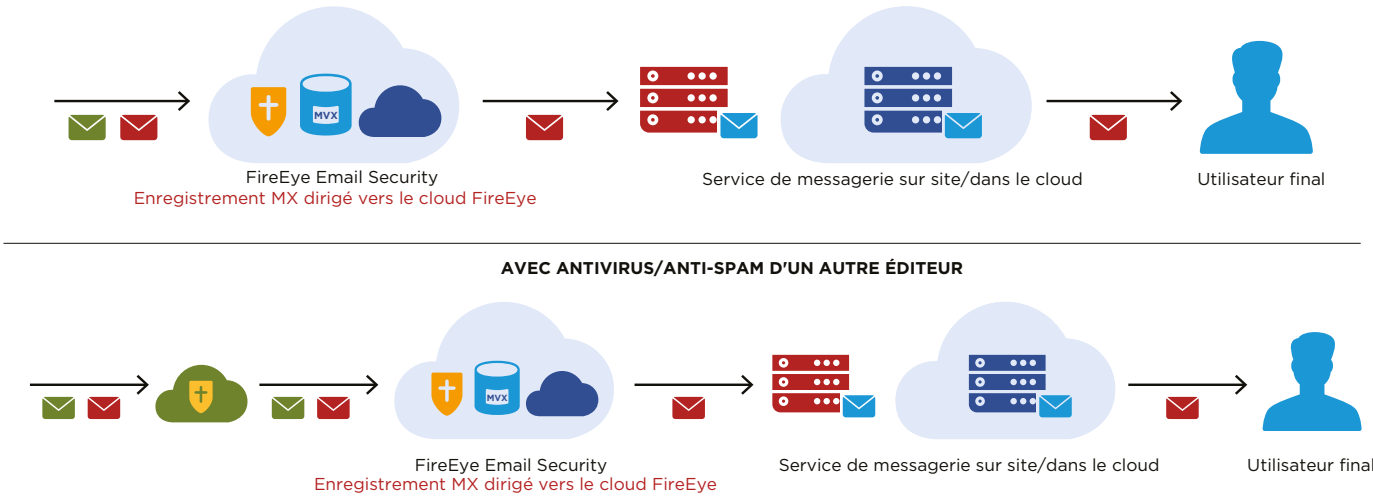
Grâce à la CTI spécifique aux e-mails, aux investigations menées sur de précédentes attaques et aux observations de l'activité des attaquants, FireEye Email Security identifie les menaces avec un minimum d'éléments parasites et quasiment aucun faux positif. Les équipes de sécurité peuvent ainsi se concentrer sur l'analyse et la gestion des attaques avérées, sans gaspiller de précieuses ressources.

Options de déploiement flexibles

FireEye Email Security peut être déployée à chaud pour assurer un contrôle renforcé et une intervention en temps réel contre les attaques en cours. Ce type de déploiement empêche toute transmission des e-mails malveillants, avec ou sans malware, à l'utilisateur final. Il se révèle donc particulièrement efficace contre des attaques de type ransomwares où la prévention reste la meilleure forme de protection.

Avec FireEye Email Security Cloud Edition, vous n'avez rien à installer – l'idéal pour les entreprises qui migrent leur infrastructure de messagerie électronique vers le cloud. Cette solution s'intègre en toute transparence aux systèmes de messagerie dans le cloud comme Microsoft Office 365 et G Suite. Son module de protection antispam et antivirus instantanée garantit la neutralisation des campagnes de spam et des techniques d'impostures (Fig. 2).

Figure 2. Déploiement à chaud de FireEye Email Security Cloud Edition



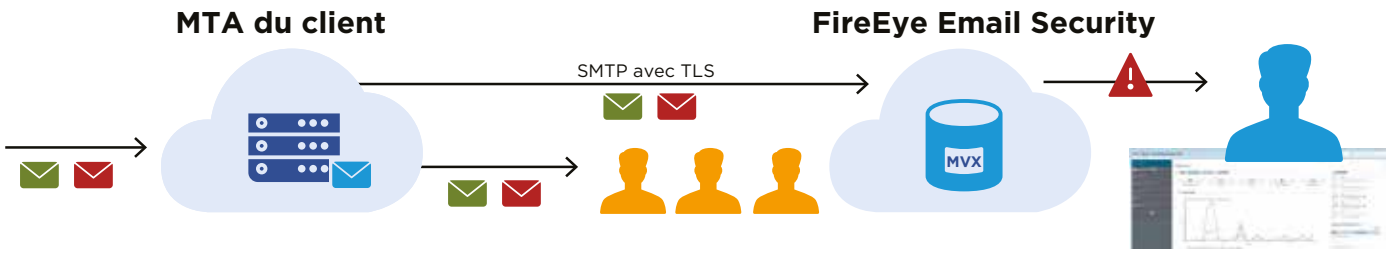
Pour les entreprises qui préfèrent commencer par une approche plus conventionnelle, FireEye Email Security peut également être déployée en mode hors bande ou en mode surveillance uniquement (Fig. 3). Dans ce cas, la solution surveille l'ensemble du trafic à la recherche d'activités malveillantes et génère des rapports, sans aucun mécanisme de prévention automatisée.

Enfin, il y a FireEye Email Security Server Edition, une gamme d'appliances sur site. FireEye et ses partenaires vous aideront à choisir et déployer l'option la plus adaptée à vos besoins.

Prochaines étapes

Face à des cybercriminels toujours plus habiles et des menaces toujours plus mouvantes, les entreprises doivent bien cerner les dangers qui les entourent. Identification des ressources exposées au risque, détection et neutralisation rapides des menaces, résolution instantanée des incidents : tels sont aujourd'hui les mots d'ordre d'une entreprise bien protégée. Pour ne pas perdre de vue leur mission et réduire le risque, les entreprises doivent s'équiper d'une solution de sécurité axée sur la détection et le blocage des menaces par e-mail, dès leur première apparition. Dans ce contexte, les technologies de protection et la CTI acquise sur les lignes de front sont d'une importance cruciale pour déjouer les cyberattaques les plus dangereuses.

Figure 3. **FireEye Email Security Cloud Edition en mode BCC.**



Pour en savoir plus, rendez-vous sur **www.fireeye.fr**

FireEye, France | Nextdoor Cœur Défense
110 Esplanade du Général de Gaulle
92931 Paris La Défense Cedex 92974
+33 1 70 61 27 26
france@FireEye.com
www.FireEye.fr FireEye, Inc.
601 McCarthy Blvd. Milpitas, CA 95035
+1 408 321 6300
info@FireEye.com

© 2019 FireEye, Inc. Tous droits réservés. FireEye est une marque déposée de FireEye, Inc. Tous les autres noms de marques, de produits ou de services sont ou peuvent être des marques commerciales ou des marques de service de leurs propriétaires respectifs.
E.EXT.SB.FR-FR-000118-01

À propos de FireEye, Inc.

FireEye est spécialisé dans la cybersécurité axée sur la Threat Intelligence. Prolongement naturel et évolutif des opérations de sécurité des clients, la plateforme unique de FireEye combine des technologies de sécurité innovantes, des services de CTI d'envergure internationale et les services réputés de Mandiant® Consulting. FireEye simplifie ainsi la cybersécurité et son administration, devenant un allié précieux des entreprises confrontées au casse-tête que représentent la prévention et la neutralisation des cyberattaques.