FIREEYE™

FICHE PRODUIT

FireEye Email Security Cloud Edition

Système cloud d'identification, d'analyse et de protection contre les attaques par e-mail

EN BREF

- Protection intégrale des e-mails entrant et sortants
- Solution complète d'un seul et même fournisseur capable de consolider toute la chaîne de protection de la messagerie électronique
- Règles YARA personnalisées pour une détection plus efficace des menaces
- Fonction d'auto-remédiation d'Office 365 pour supprimer les e-mails dont le comportement devient suspect après leur réception
- Intégration à n'importe quel service de messagerie externe
- Connaissance approfondie des attaques et de leurs auteurs issue de travaux d'observation et d'investigation de terrain
- Respect des exigences de sécurité du FedRAMP

« Dans les environnements collaboratifs, l'e-mail occupe une place centrale. FireEye Email Security nous offre une solution unique pour neutraliser les risques de compromission de ce canal sous attaque constante. »

Nils Göldner
Dirigeant associé et conseiller cloud
Blackboat GmbH

Présentation

Principal point d'entrée des données dans l'entreprise, la messagerie électronique représente aussi son vecteur d'attaque n°1. Entre spams, malwares et menaces avancées, de plus en plus d'attaques passent en effet par l'e-mail. La majorité d'entre elles prennent la forme de pièces jointes infectées, de liens malveillants, de fraudes aux virements électroniques et autres tentatives de phishing d'identifiants. Parce qu'il permet de personnaliser les messages, l'e-mail est devenu le canal d'attaque privilégié des cybercriminels.

FireEye Email Security propose une solution de sécurité destinée à contrer les menaces avancées pour non seulement réduire les risques de violations de sécurité, mais aussi baisser les coûts et booster la productivité des salariés. Déployée dans le cloud, FireEye Email Security est une passerelle de messagerie sécurisée très riche en fonctionnalités. Sa mission : identifier, isoler et neutraliser immédiatement les attaques (URL et pièces jointes malveillantes, usurpation d'identité, etc.) avant qu'elles n'atteignent l'environnement d'une entreprise. La fonction d'auto-remédiation d'Office 365 (O365) permet d'extraire de la boîte de messagerie les e-mails qui deviennent suspects après avoir été reçus. En parallèle, la solution analyse le trafic d'e-mails sortants à la recherche de spams, virus ou autres menaces avancées.

La solution s'appuie sur une plateforme Big Data évolutive pour détecter les URL malveillantes. Elle établit pour cela un contexte à partir de données de Threat Intelligence et de plug-ins de détection. FireEye Email Security vérifie l'authenticité des expéditeurs (nom et adresse e-mail) et examine le contenu pour y dénicher et bloquer toute tentative d'imposture et d'usurpation de type « arnaque au président » et autres attaques sans malware. Le moteur sans signature Multi-Vector Virtual Execution™ (MVX) analyse les pièces jointes et URL des e-mails au moyen d'une matrice croisée d'applications, de navigateurs web et de systèmes d'exploitation. Hormis une élimination quasi-totale des faux positifs, Email Security identifie les menaces avec un minimum d'éléments parasites.

Pour profiler les attaquants, FireEye collecte d'énormes volumes d'informations de Threat Intelligence à partir de millions de capteurs et d'innombrables investigations sur des cas de violations réelles. Grâce à ces preuves concrètes et aux informations contextuelles sur les attaques et leurs auteurs, Email Security parvient à prioriser les alertes et à bloquer les menaces en temps réel.

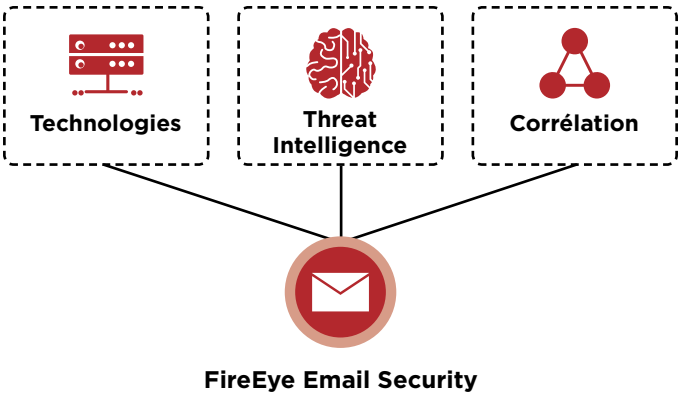

Figure 1. Une passerelle e-mail sécurisée

Enfin, la solution s'intègre à FireEye Network Security pour améliorer la visibilité et la coordination de la protection en temps réel contre les attaques mixtes et multi-vecteurs.

Protection contre les attaques par e-mail

Il existe une telle quantité de données personnelles facilement accessibles en ligne que les virtuoses de l'ingénierie sociale n'ont aucun mal à piéger leurs cibles (clic sur un lien malveillant, ouverture d'une pièce jointe infectée, etc.).

Email Security assure la détection et la prévention en temps réel des attaques de spear-phishing, des usurpations d'identité et du phishing d'identifiants qui contournent les systèmes de défense traditionnels. Les e-mails sont analysés et mis en quarantaine (bloqués) dès qu'une menace inconnue ou avancée est détectée. Le champ d'analyse d'Email Security :

- Tous types de pièces jointes, y compris les fichiers EXE, DLL, PDF, SWF, DOC/DOCX, XLS/XLSX, PPT/PPTX, JPG, PNG, MP3, MP4, ainsi que les archives ZIP/RAR/TNEF
- Pièces jointes cryptées et protégées par mot de passe
- URL contenues dans les e-mails, les PDF et les documents Microsoft Office
- URL de phishing d'identifiants et de typosquattage
- Vulnérabilités inconnues dans les navigateurs, applications et systèmes d'exploitation
- Code malveillant contenu dans les e-mails de spear-phishing

Bien que les attaques par ransomware commencent par un e-mail, le cryptage des données passe par le rappel à un serveur de commande et de contrôle (CnC). FireEye Email Security identifie et neutralise ces campagnes de malwares multi-étapes et difficiles à détecter.

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 menaces futures.

Advanced URL Defense et le moteur MVX 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.

Partie intégrante d'Advanced URL Defense, le moteur de classification d'images PhishVision s'appuie sur le deep learning pour compiler des captures d'écran de marques reconnues et régulièrement ciblées, puis les comparer aux pages web et écrans de connexion référencés par les URL contenues dans un e-mail. PhishVision fonctionne en tandem avec Kraken, un plug-in de détection des attaques de phishing qui exploite les analyses de domaines et de contenus de pages pour renforcer les fonctions de machine learning. Enfin, SkyFeed entre en jeu. SkyFeed est un système entièrement automatisé de centralisation des informations sur les malwares qui analyse les blogs, les forums, les comptes de réseaux sociaux et les flux de Threat Intelligence à la recherche de faux négatifs. Avec Advanced URL Defense, les entreprises protégées par Email Security bénéficient d'une sécurité hors-pair contre les usurpations d'identité et les attaques par spear-phishing.

Un e-mail peut apparaître comme inoffensif dans un premier temps afin de passer les systèmes de sécurité. Ce n'est qu'une fois arrivé dans la boîte de réception de l'utilisateur qu'il révèle sa vraie nature. Email Security Cloud Edition effectue des analyses rétroactives et émet des alertes en cas d'e-mail suspect après livraison. Par ailleurs, l'API O365 permet de créer une politique d'auto-remédiation pour extraire automatiquement ce type d'e-mail de la boîte de messagerie.

Quant au moteur MVX, il analyse le trafic dans un environnement virtuel sécurisé, à la recherche des attaques zero-day, multi-flux et autres menaces par contournement. Capable d'identifier des exploits et malwares inconnus, il stoppe les phases d'infection et de compromission d'une chaîne d'attaque.

Protection antivirus/antispam avancée

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 sans malware font exclusivement appel à des techniques d'ingénierie sociale. Elles ne comportent donc 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.

L'âge du domaine utilisé par l'expéditeur constitue par exemple un bon indicateur d'une possible attaque par e-mail. Concrètement, lorsqu'ils fomentent une attaque par usurpation d'identité, les cybercriminels envoient généralement les e-mails à partir d'un domaine semblable à celui de la personne ou de l'entreprise pour laquelle ils se font passer, et ce dans les heures qui suivent la création de ce domaine.

C'est pourquoi Email Security se sert d'outils de NED (Newly Existing Domains) et NOD (Newly Observed Domains) développés en interne pour déterminer avec précision l'âge et le niveau de maturité d'un domaine. Les domaines identifiés comme étant nouvellement créés sont considérés comme suspects et font l'objet d'un examen approfondi pour détecter d'autres indices éventuels (typosquattage, spoofing du nom d'utilisateur ou d'affichage de l'expéditeur, etc.).

Plutôt que d'acheter et d'enregistrer un nom de domaine, certains cybercriminels prennent un raccourci en ne modifiant que le nom d'utilisateur ou d'affichage de l'expéditeur, en espérant que cela suffise pour duper le destinataire. Là encore, Email Security intègre une fonction d'identification des noms qui permet de déterminer l'authenticité d'un nom d'utilisateur ou d'affichage.

Analyse des e-mails sortants

Email Security détecte les menaces avancées et encore inconnues, y compris les pièces jointes malveillantes et les URL de phishing dissimulées dans les e-mails sortants. Le trafic e-mail sortant est, lui aussi, analysé pour détecter d'éventuels malwares et spams susceptibles d'entraîner le "blacklisting" des domaines de l'entreprise.

Intégration pour un traitement plus efficace des alertes

Email Security analyse chaque pièce jointe et chaque URL afin d'identifier avec précision les nouvelles attaques avancées. Grâce à des mises à jour en temps réel de tout l'écosystème de sécurité FireEye et à l'attribution d'attaques à des groupes connus, vous disposez du contexte nécessaire pour prioriser les alertes critiques, intervenir de manière ciblée et bloquer les attaques avancées par e-mail. Email Security parvient à identifier les menaces connues, inconnues et hors malwares avec un minimum d'éléments parasites et de faux positifs. Résultat : vous concentrez vos ressources sur les véritables attaques, avec à la clé une réduction de vos coûts d'exploitation.

Adaptation rapide à l'évolution des menaces

Pour aider votre entreprise à adapter en permanence ses systèmes de défense proactive contre les menaces par e-mail, Email Security s'appuie sur sa propre Cyber Threat Intelligence (CTI) plutôt que sur des sources externes plus lentes à se mettre à jour. Une Threat Intelligence interne spécifique aux e-mails (ou un service de Smart DNS), des fonctions de collecte des données, des experts en sécurité et des analystes des menaces fournissent toute l'assise nécessaire à des technologies anti-spam avancées et à la détection d'attaques par usurpation d'identité. Cette CTI combine des données sur les cybercriminels, les machines et les victimes. Objectifs :

- Fournir une vue plus large et plus actuelle sur le champ des menaces
- Identifier des fonctionnalités spécifiques des malwares et pièces jointes malveillants détectés
- Fournir des analyses contextuelles pour la priorisation et l'accélération des réponses
- Déterminer l'identité et les objectifs probables du cybercriminel, et traquer son activité dans votre entreprise
- Identifier rétroactivement les attaques de spear-phishing et empêcher l'accès aux sites de phishing en réécrivant les URL malveillantes

Les entreprises ont accès au portail Email Security pour consulter des alertes en temps réel, créer des règles personnalisées (Smart Custom Rules) et générer des rapports. Les Smart Custom Rules permettent à votre entreprise de définir des règles et des politiques basées sur un choix granulaire de propriétés et conditions.

Intégration du workflow d'intervention

Email Security s'intègre à plusieurs autres solutions FireEye pour automatiser au maximum les workflows de réponse aux alertes :

FireEye Central Management recoupe les alertes générées par Email Security et Network Security pour améliorer la visibilité sur les attaques et configurer les règles de blocage destinées à empêcher leur propagation.

Spécialement conçue pour simplifier, intégrer et automatiser les opérations de sécurité, la plateforme FireEye Helix agit en parfaite interopérabilité avec Email Security.

Facilité de déploiement et protection de toute l'entreprise

Basée dans le cloud, Email Security Cloud Edition ne nécessite aucune installation matérielle ou logicielle. Elle offre ainsi une solution idéale aux entreprises qui migrent leur infrastructure de messagerie dans le cloud. Cette migration élimine la complexité liée à l'achat, l'installation et la gestion d'une infrastructure physique.

Email Security Cloud Edition s'intègre en toute transparence à vos systèmes de messagerie cloud comme Microsoft Office 365 avec Exchange Online Protection et G Suite.

Pour se prémunir contre les e-mails infectés et frauduleux, il suffit aux entreprises de diriger leurs messages vers Email Security, qui effectue d'abord une recherche de spams, malwares et tactiques d'usurpation d'identité connus. La solution utilise ensuite la technologie de défense anti-URL et la « chambre de détonation » (sandbox) du moteur sans signature MVX pour analyser toutes les pièces jointes / URL et bloquer les attaques avancées en temps réel.

Fonctionnalités supplémentaires

Personnalisation à l'aide de règles YARA

Avec Email Security, les analystes peuvent utiliser des règles YARA personnalisées et ainsi gérer/améliorer la détection, stopper les dernières menaces et identifier les campagnes en cours.

Mode protection active ou surveillance seule

Email Security peut analyser les messages et isoler les menaces pour une protection active. Pour acheminer les messages vers la solution FireEye, les entreprises n'ont qu'à mettre à jour leurs enregistrements MX. Dans le cas de déploiements en surveillance seule, il leur suffit de configurer une règle de copie invisible transparente (Cci) afin d'envoyer les e-mails à FireEye pour leur analyse MVX.

Autorisations et certifications de conformité

ISO 27001

Email Security Cloud Edition est conforme à la norme ISO27001 de sécurité de l'information qui garantit une gestion sécurisée des data centers.

FedRAMP

Email Security Cloud Edition (avec protection antivirus/antispam) satisfait aux exigences de sécurité du FedRAMP pour les services cloud exploités par les administrations et établissements d'enseignement public américains.

SOC 2 Type II

Email Security Cloud Edition a obtenu la certification SOC 2 (Service Organization Controls) Type 2 de l'AICPA (American Institute of Certified Public Accountants) pour la sécurité et la confidentialité.

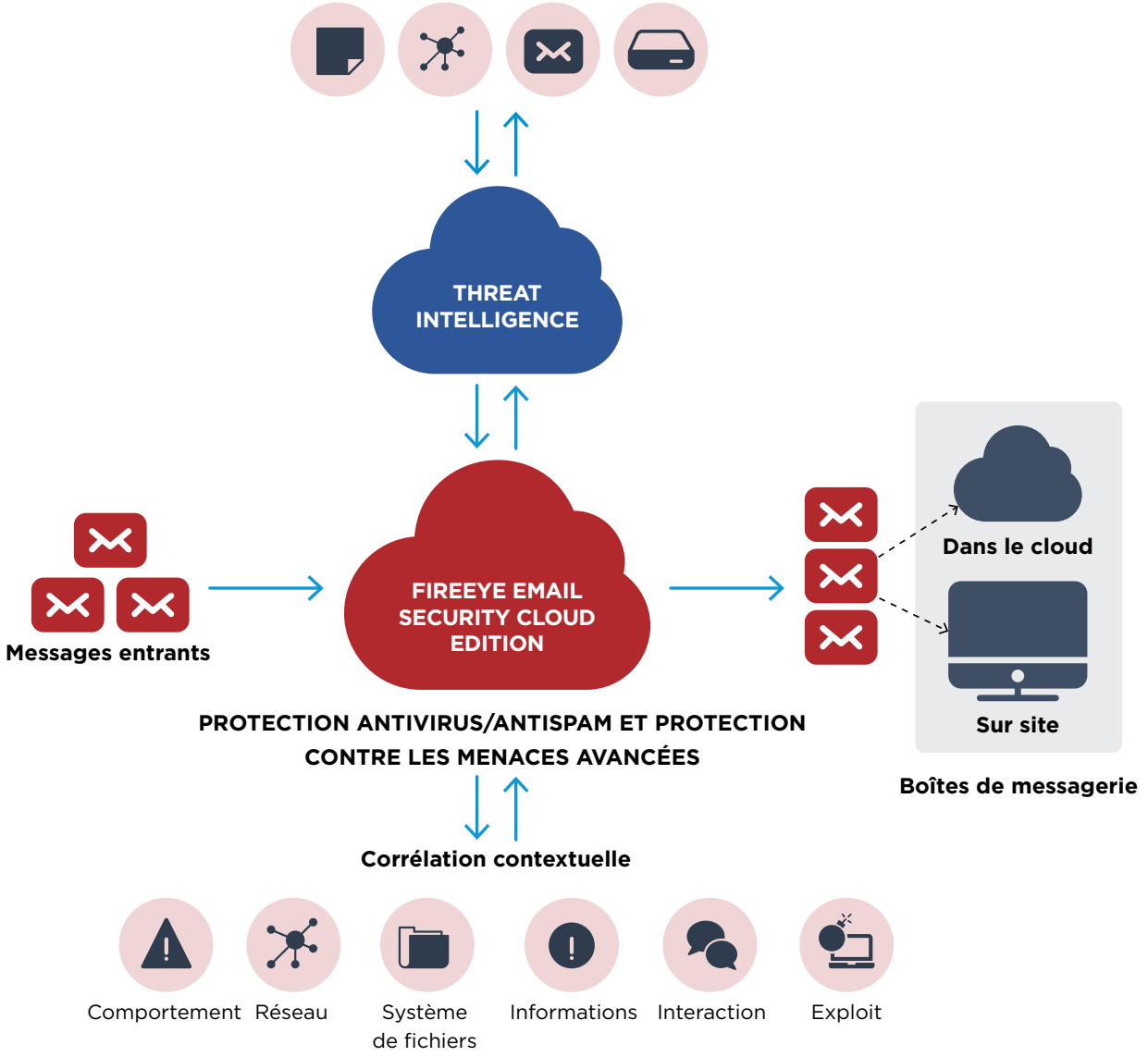

Figure 2. FireEye Email Security – Cloud Edition

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

À propos de FireEye, Inc.

FireEye est spécialisé dans la cybersécurité axée sur la Cyber Threat Intelligence (CTI). 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.