FIREEYE™

FICHE PRODUIT

FireEye Email Security Server Edition

Une protection intelligente, adaptative et évolutive contre les menaces transmises par e-mail

Figure 1. Exemples d'appliances Email Security intégrées : EX 3500, EX 5500 et EX 8500

POINTS FORTS

- Sécurité intégrale de la messagerie électronique contre le spear-phishing et autres menaces avancées, zero-day et multi-phases
- Analyses basées sur des images des systèmes d'exploitation Microsoft Windows et Apple macOS X
- Recherche de menaces dissimulées dans les pièces jointes (y compris les fichiers cryptés et protégés par mot de passe) et URL contenues dans les e-mails
- Collecte d'informations de Threat Intelligence en temps réel à partir du cloud FireEye DTI
- Analyses contextuelles pour la priorisation et l'endiguement des menaces
- Déploiement sur site avec service MVX intégré ou distribué

Présentation

Principal point d'entrée des données dans l'entreprise, la messagerie électronique représente aussi son vecteur d'attaque n°1. De plus en plus d'attaques avancées passent par l'e-mail, multipliant par là même les problèmes de sécurité.
La majorité de ces attaques prennent la forme de pièces jointes infectées, de liens malveillants et autres tentatives de phishing d'identifiants. En ce sens, la grande flexibilité de l'e-mail en termes de personnalisation et de ciblage en fait le canal d'attaque privilégié des cybercriminels.

FireEye a conçu FireEye Email Security pour contrer ces menaces et réduire les risques de violations de sécurité coûteuses. Déployée sur site, FireEye Email Security Server Edition identifie, isole et neutralise immédiatement les attaques (URL et pièces jointes malveillantes, usurpation d'identité, etc.) avant qu'elles n'atteignent l'environnement d'une entreprise. La solution s'appuie sur une plateforme Big Data évolutive pour faire le tri entre URL malveillantes et inoffensives, grâce notamment à des plug-ins de détection et des données de Threat Intelligence pour apporter tout le contexte nécessaire. Le moteur sans signature Multi-Vector Virtual Execution™ (MVX) analyse les pièces jointes et URL de contenus téléchargeables 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 les pirates, Email Security parvient à prioriser les alertes et à bloquer les menaces en temps réel.

Enfin, la solution s'intègre à FireEye Network Security et Endpoint 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 disponibles 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
- Pièces jointes protégées par des mots de passe envoyés via une image
- URL contenues dans les e-mails, documents MS Office, fichiers PDF, archives (ZIP, ALZip, JAR) et autres (Uuencoded, HTML)
- Fichiers téléchargés à partir d'URL, voire de liens FTP
- URL masquées, imitées, raccourcies ou redirigées dynamiquement
- URL de phishing d'identifiants et de typosquattage
- Vulnérabilités inconnues dans les images, navigateurs et applications des systèmes d'exploitation Microsoft Windows et Apple macOS X
- 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 généralement 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, le moteur MVX et MalwareGuard sont des composants clés de FireEye Email Security. Ces technologies s'appuient sur des fonctions d'analytique et de machine learning 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 référencées 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.

De son côté, MalwareGuard se sert de fichiers binaires pour attribuer une « note de méfiance » à un fichier donné. Cet utilitaire s'appuie sur le machine learning pour analyser tous les fichiers PE (Portable Executable) qui transitent sur le réseau. Une décision est prise en fonction de la note attribuée aux fichiers, puis un nom est octroyé à chaque signal de détection déclenché par MalwareGuard.

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. Il permet d'identifier les exploits et malwares encore inconnus pour stopper les infections et les compromissions.

Neutralisation des attaques par contournement

Email Security intègre une fonction d'analyse en mode Live contrôlé pour protéger les entreprises des attaques tentant de contourner les demandes d'objets distants. Le moteur MVX détecte les malwares effectuant des demandes de téléchargement multiples, puis renvoie les objets distants sollicités par le fichier binaire échantillon. Le mode Live contrôlé réduit les faux négatifs dans l'analyse des téléchargements multi-étapes, attaques avancées par spear-phishing et intrusions de ransomwares.

Les attaquants tentent aussi de contourner les technologies de détection des URL suspectes. C'est pourquoi les fonctions de blocage des tentatives de contournement sont constamment améliorées dans le cadre de l'offre Advanced URL Defense. Par ailleurs, il est possible de paramétrer des Guest Images de façon à imiter un terminal "utilisé" lorsqu'un objet potentiellement malveillant est exécuté. De nombreuses tentatives de contournement sont ainsi déjouées grâce à des Guest Images capables de reproduire le domaine d'un terminal, un utilisateur de domaine, des données Outlook et un historique de navigation.

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. La catégorisation des riskwares permet de distinguer les véritables tentatives de violation de sécurité des activités certes indésirables, mais moins nocives (par exemple les adwares et spywares), afin de prioriser les interventions.

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 les informations de Cyber Threat Intelligence (CTI) fournies en temps réel par le cloud FireEye Dynamic Threat Intelligence™ (DTI). 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 de l'intervention
- Déterminer l'identité et les objectifs probables du cybercriminel, et traquer son activité dans votre entreprise
- Réécrire toutes les URL contenues dans un e-mail pour protéger les utilisateurs des liens malveillants
- Identifier rétroactivement les attaques de spear-phishing et empêcher l'accès aux sites de phishing en blacklistant les URL malveillantes

Intégration du workflow d'intervention

Email Security est compatible avec FireEye Helix et FireEye Central Management.

- Composant de la plateforme de sécurité opérationnelle FireEye Helix, Email Security offre une visibilité sur l'ensemble de votre infrastructure. FireEye Helix agit dans le prolongement de solutions tierces pour enrichir les alertes d'informations de CTI, d'automatisation et de corrélations avec les données des terminaux, sans oublier des conseils pour orienter vos investigations. La solution possède ainsi tous les éléments nécessaires pour détecter les menaces cachées et fiabiliser les décisions des équipes de sécurité.
- 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.
- Central Management gère le balisage des utilisateurs par rôle pour identifier les personnes ciblées.
- Central Management s'appuie sur des critères de rôle pour répondre aux alertes.

Fonctionnalités supplémentaires

Personnalisation à l'aide de règles YARA

FireEye Email Security permet aux analystes de définir et tester des règles d'analyse des pièces jointes à la recherche d'éventuelles menaces ciblant leur entreprise.

Protection contre l'usurpation de l'identité de cadres dirigeants

Email Security Server Edition permet de bloquer les tentatives de compromission des e-mails professionnels pour empêcher des escrocs de se faire passer pour des acteurs clés de l'entreprise. Pour cela, la solution compare les noms d'affichage des e-mails entrants à une liste d'expéditeurs approuvés.

Files d'attente de messages et gestion des alertes et des mises en quarantaine

Email Security Server Edition vous permet de contrôler de façon ciblée les e-mails analysés. En mode protection active, la solution FireEye vous aide à suivre et gérer les messages à mesure qu'ils progressent dans la file d'attente MTA. Vous pouvez également spécifier des attributs de recherche pour vous assurer que les e-mails concernés ont bien été reçus, analysés et relayés vers l'étape suivante. De même, un tableau de bord intuitif vous permet d'observer les tendances. Enfin, les listes de blocage et d'autorisation vous confèrent un contrôle sur mesure du traitement des e-mails. Les attributs d'alerte communs peuvent être recherchés et sélectionnés. Vous avez également la possibilité d'effectuer des opérations de groupe sur les alertes et messages mis en quarantaine.

Mode protection active ou surveillance seule

Email Security peut analyser les messages et isoler les menaces pour une protection active. Dans le cas de déploiements en surveillance seule, il suffit de configurer une règle de copie invisible transparente (Cci) afin d'envoyer les e-mails à Email Security pour analyse.

Options de déploiement flexibles

Email Security Server Edition propose plusieurs options de déploiement adaptées aux différents besoins et budgets des entreprises :

- **Solution Email Security intégrée —** Appliance matérielle et autonome tout-en-un, avec service MVX intégré pour sécuriser le point d'entrée e-mail d'un seul site. FireEye Email Security est une solution facile à gérer et déployable en moins de 60 minutes. Elle ne nécessite ni règles, ni politiques, ni paramétrages.
- **Solution Email Security distribuée –** Appliances extensibles avec partage central du service MVX pour sécuriser les points d'accès au système de messagerie électronique d'une entreprise et/ou de ses filiales.
- **Solution Email Smart Node –** Capteurs virtuels qui analysent les e-mails pour détecter et bloquer le trafic malveillant, puis transmettre les activités suspectes via une connexion cryptée au service MVX pour qu'il les analyse et rende un verdict définitif.
- **MVX Smart Grid –** Service MVX élastique, installé sur site, qui offre une évolutivité transparente, une tolérance aux pannes N+1 intégrée, ainsi qu'un équilibrage de charge automatique.

  Lors des pics de trafic, la fonctionnalité de "bursting" fait intervenir FireEye MVX Smart Grid pour renforcer votre capacité à détecter et analyser les menaces transmises par e-mail.
- **FireEye Cloud MVX –** Abonnement à MVX, un service qui garantit la confidentialité des informations grâce à une analyse du trafic sur l'appliance Email Smart Node. Seuls les objets suspects sont transmis via une connexion cryptée au service MVX, qui ensuite écarte les objets reconnus comme inoffensifs.

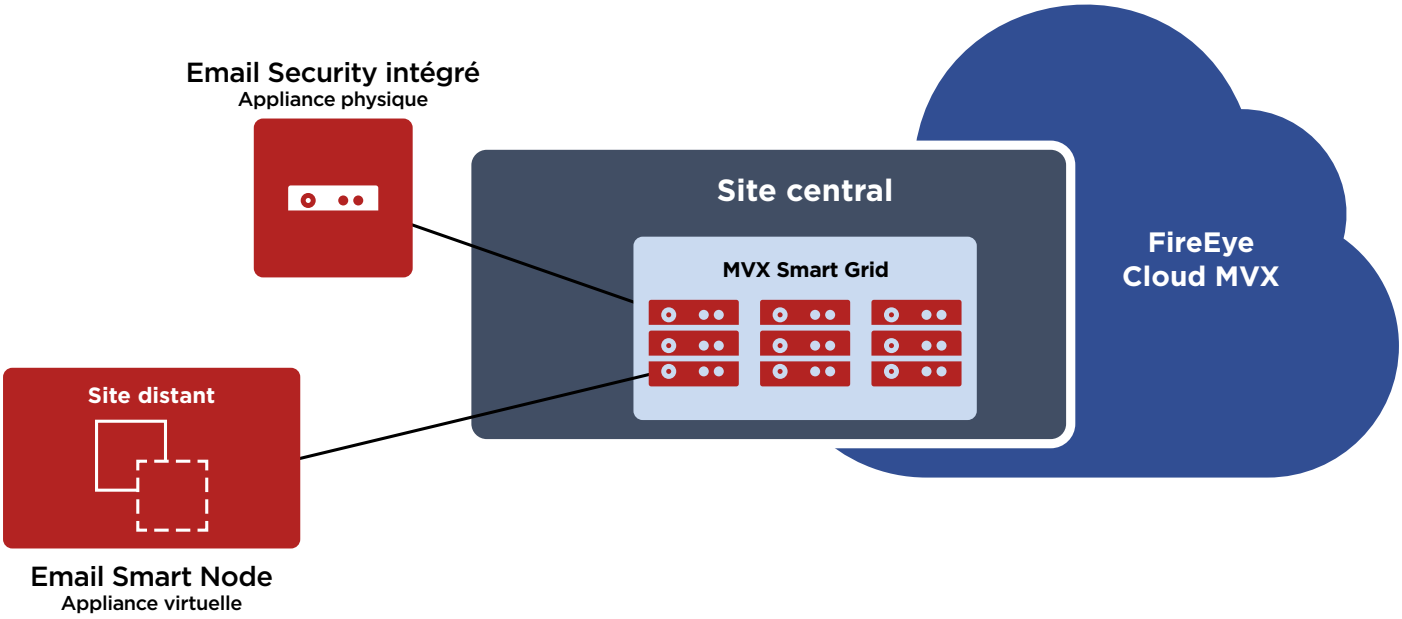

Figure 2. Modèles de déploiement distribués et en mode "bursting" pour Email Security

Tableau 1. Spécifications techniques

	EX 3500	EX 5500	EX 8500
Performance*	Jusqu'à 700 pièces jointes uniques par heure	Jusqu'à 1 800 pièces jointes uniques par heure	Jusqu'à 2 650 pièces jointes uniques par heure
Ports de l'interface réseau	2 x 1 GigE BaseT	2 x 1 GigE BaseT	4 ports SFP+ (fibre 10 GigE, cuivre 10 GigE, cuivre 1 GigE), 2 x 1 GigE BaseT
Interfaces de gestion	2 x 1 GigE BaseT	2 x 1 GigE BaseT	2 x 1 GigE BaseT
Surveillance IPMI	Inclus	Inclus	Inclus
Port VGA (panneau arrière)	Inclus	Inclus	Inclus
Ports USB (panneau arrière)	4 ports USB de type A (arrière)	2 ports USB de type A (avant), 2 ports USB de type A (arrière)	2 ports USB de type A (avant), 2 ports USB de type A (arrière)
Port série (panneau arrière)	115 200 bit/s, pas de parité, 8 bits, 1 bit d'arrêt	115 200 bit/s, pas de parité, 8 bits, 1 bit d'arrêt	115 200 bit/s, pas de parité, 8 bits, 1 bit d'arrêt
Capacité de stockage	4 disques durs 2 To, RAID 10, 3,5 pouces, remplaçables	4 disques durs 2 To, RAID 10, 3,5 pouces, remplaçables	4 disques durs 2 To, RAID 10, 3,5 pouces, remplaçables
Châssis	Montage en baie 1U, s'intègre en baie 19 pouces	Montage en baie 2U, s'intègre en baie 19 pouces	Montage en baie 2U, s'intègre en baie 19 pouces
Dimensions du châssis (L x P x H)	43,7 x 65 x 4,32 cm	43,8 x 62 x 8,84 cm	43,8 x 62 x 8,84 cm
Alimentation en courant alternatif	Redondante (1+1) 750 W à 100 - 240 Vca, 9 - 4,5 A, embase secteur IEC 60320-C14 50 - 60 Hz, remplaçable	Redondante (1+1) 750 W à 100 - 240 Vca, 9 - 4,5 A, embase secteur IEC 60320-C14 50 - 60 Hz, remplaçable	Redondante (1+1) 750 W à 100 - 240 Vca, 9 - 4,5 A, embase secteur IEC 60320-C14 50 - 60 Hz, remplaçable
Alimentation en courant continu	Non disponible	Non disponible	Non disponible
Enveloppe thermique maximale	245 W (836 BTU/h)	456 W (1 556 BTU/h)	530 W (1 808 BTU/h)
Temps moyen de bon fonctionnement	54 200 heures	57 401 heures	53 742 heures
Poids de l'appliance seule/avec emballage	13,6 kg / 18,6 kg	20 kg / 29,6 kg	20,2 kg / 29,8 kg
Certifications de conformité	IEC 60950 EN 60950-1 UL 60950 CSA/CAN-C22.2	IEC 60950 EN 60950-1 UL 60950 CSA/CAN-C22.2	IEC 60950 EN 60950-1 UL 60950 CSA/CAN-C22.2
Compatibilité électromagnétique (CEM)	FCC Partie 15 ICES-003 Classe A AS/NZS CISPR 22 CISPR 32 EN 55032 EN 55024 IEC/EN 61000-3-2 IEC/EN 61000-3-3 IEC/EN 61000-4-2 V-2/2015 & V-3/2015	FCC Partie 15 ICES-003 Classe A AS/NZS CISPR 22 CISPR 32 EN 55032 EN 55024 IEC/EN 61000-3-2 IEC/EN 61000-3-3 IEC/EN 61000-4-2 V-2/2015 & V-3/2015	FCC Partie 15 ICES-003 Classe A AS/NZS CISPR 22 CISPR 32 EN 55032 EN 55024 IEC/EN 61000-3-2 IEC/EN 61000-3-3 IEC/EN 61000-4-2 V-2/2015 & V-3/2015
Certifications de sécurité	FIPS 140-2, CC NDPP v1.1	FIPS 140-2, CC NDPP v1.1	FIPS 140-2, CC NDPP v1.1
Conformité aux normes environnementales	Directive RoHS 2011/65/UE, REACH, Directive DEEE 2012/19/UE	Directive RoHS 2011/65/UE, REACH, Directive DEEE 2012/19/UE	Directive RoHS 2011/65/UE, REACH, Directive DEEE 2012/19/UE
Température de fonctionnement	0 ~ 35 °C	0 ~ 35 °C	0 ~ 35 °C
Plage d'humidité relative tolérée	10 ~ 95 % à 40 °C, sans condensation	10 ~ 95 % à 40 °C, sans condensation	10 ~ 95 % à 40 °C, sans condensation
Altitude maximale de fonctionnement	3 000 m	3 000 m	3 000 m

* Les performances peuvent varier en fonction de la configuration système et du profil du trafic e-mail traité. Les appliances devront être choisies en fonction de leurs capacités de traitement de pièces jointes uniques par heure.

Tableau 2. Spécifications de FireEye MVX Smart Grid

	VX 5500	VX 12500
Systèmes d'exploitation pris en charge	Microsoft Windows Apple macOS X	Microsoft Windows Apple macOS X
Performance*	Jusqu'à 480 pièces jointes uniques par heure	Jusqu'à 3 780 pièces jointes uniques par heure
Haute disponibilité**	N+1	N+1
Interfaces de gestion (panneau arrière)	1 port 10/100/1000 Mbit/s BASE-T	1 port 10/100/1000 Mbit/s BASE-T
Ports cluster (panneau arrière)	3 ports 10/100/1000 Mbit/s BASE-T	1 port 10/100/1000 Mbit/s BASE-T, 2 ports de 10 Gbit/s BASE-T
Port IPMI (panneau arrière)	Inclus	Inclus
Écran LCD et clavier (panneau avant)	Non disponible	Inclus
Ports VGA	Inclus	Inclus
Ports USB (panneau arrière)	4 ports USB de type A	2 ports USB de type A
Port série (panneau arrière)	115 200 bit/s, pas de parité, 8 bits, 1 bit d'arrêt	115 200 bit/s, pas de parité, 8 bits, 1 bit d'arrêt
Capacité des disques	2 disques durs SAS de 2 To, RAID 1, 3,5 pouces, remplaçables	4 disques durs SAS3 de 4 To, RAID 1, 3,5 pouces, remplaçables
Châssis	Montage en baie 1U, s'intègre en baie 19 pouces	Montage en baie 2U, s'intègre en baie 19 pouces
Dimensions du châssis (L x P x H)	17. 43,7 x 65 x 4,32 cm	43,7 x 85,1 x 8,9 cm
Alimentation en courant continu	Non disponible	Non disponible
Alimentation en courant alternatif	Redondante (1+1) 750 W à 100 - 240 Vca, 8 - 3,8 A, embase secteur IEC 60320-C14, 50 - 60 Hz, remplaçable	Redondante (1+1) 800 W à 100 - 127 V, 9,8 - 7 A, 1 000 W à 220 - 240 V, 7 - 5 A, embase secteur IEC 60320-C14, 50 - 60 Hz, remplaçable
Consommation électrique maximale	285 W	760 W
Dissipation thermique maximale	972 BTU/h	2 594 BTU/h
Temps moyen de bon fonctionnement	54 200 heures	38 836 heures
Poids de l'appliance seule/avec emballage	15 / 21,8 kg	21 / 40,2 kg
Certification de sécurité	FIPS 140-2 Niveau 1, CC NDPP v1.1	FIPS 140-2 Niveau 1, CC NDPP v1.1
Conformité aux normes de sécurité	IEC 60950 EN 60950-1 UL 60950 CSA/CAN-C22.2	IEC 60950 EN 60950-1 UL 60950 CSA/CAN-C22.2

* Les performances peuvent varier en fonction de la configuration système et du profil du trafic traité.

** Avec les configurations matérielles redondantes appropriées.

Tableau 3. FireEye Email Security Smart Node, spécifications des capteurs virtuels.

	EX 5500V
Systèmes d'exploitation pris en charge	Microsoft Windows, Apple macOS X
Performance*	Jusqu'à 1 250 pièces jointes uniques par heure
Interface de surveillance réseau	2
Ports de gestion réseau	2
Cœurs de processeur	8
Memory	16 Go
Capacité des disques	384 Go
Cartes réseau	VMXNet 3, vNIC
Prise en charge d'hyperviseur	VMware ESXi 6.0 ou ultérieur

* Les performances peuvent varier en fonction de la configuration système et du profil du trafic traité.

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-DS-FR-FR-000044-02

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.