FIREEYE™

FICHE PRODUIT

FireEye Network Security

Protection efficace contre les compromissions de cybersécurité pour les moyennes et grandes entreprises

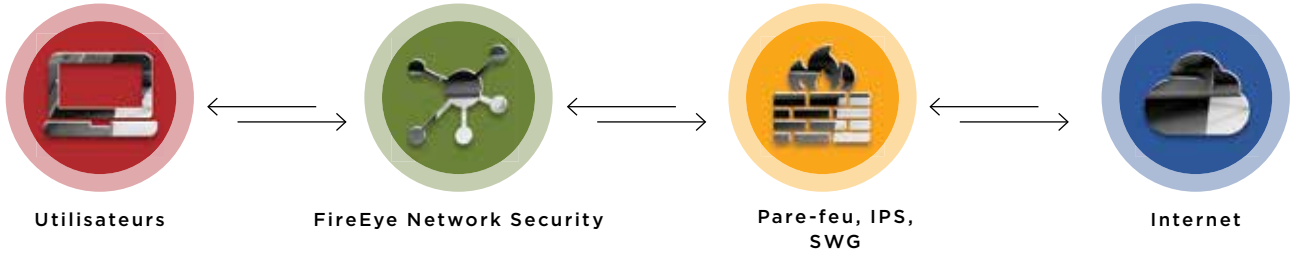
Présentation

FireEye Network Security est une solution de protection efficace contre les cybermenaces. Elle est conçue pour réduire le risque et les coûts de compromissions grâce à une détection précise et un blocage instantané des attaques avancées, ciblées et par contournement qui se dissimulent dans le trafic Internet. La solution permet de résoudre les incidents de sécurité détectés en quelques minutes grâce à l'intégration de preuves concrètes, d'une Cyber Threat Intelligence (CTI) exploitable et des workflows de réponse à incident. Avec FireEye Network Security, les entreprises sont protégées contre les menaces actuelles, qu'elles exploitent les systèmes d'exploitation Microsoft Windows et Apple OS X ou les vulnérabilités des applications, qu'elles soient dirigées contre le siège ou les filiales d'une société, ou qu'elles se camouflent dans la masse de trafic Internet entrant à inspecter en temps réel.

La solution repose sur deux technologies fondamentales : le moteur MVX (Multi-Vector Virtual Execution™) et les moteurs IDA (Intelligence-Driven Analysis). MVX est un moteur d'analyse dynamique sans signatures qui inspecte le trafic réseau suspect pour identifier les attaques conçues pour contourner les systèmes de défense traditionnels basés sur les signatures et les politiques de sécurité. IDA réunit plusieurs moteurs contextuels dynamiques basés sur des règles. Leur mission consiste à détecter et bloquer les activités malveillantes en temps réel ou rétroactivement, en exploitant la CTI la plus récente sur les attaquants, leurs victimes et les machines touchées. Quant à son système de prévention des intrusions (IPS), il utilise une méthode classique de correspondance des signatures pour identifier les attaques courantes.

FireEye Network Security se décline en un large choix d'options de format, de modes de déploiement et de performances. L'appliance est généralement placée de façon à pouvoir inspecter le trafic Internet derrière les équipements de sécurité réseau traditionnels comme les pare-feu nouvelle génération, les systèmes IPS et les passerelles web sécurisées (SWG). FireEye Network Security complète ces solutions par des fonctions capables de détecter rapidement des attaques connues et inconnues avec une très grande précision et un faible taux de faux positifs, tout en offrant la possibilité d'intervenir efficacement à chaque alerte.

Figure 1. Configuration type — Solutions Network Security.



Fonctionnalités	Avantages
Détection	
Détection précise des cyberattaques ciblées, avancées et par contournement	Limitation du risque de compromissions onéreuses
Architecture de sécurité modulaire et extensible	Pérennité de l'investissement
Niveau de protection cohérent pour les environnements exécutant différents systèmes d'exploitation et tous les points d'accès Internet	Création d'une défense efficace dans toute l'organisation pour tous les types de terminaux
Options de déploiement intégré, distribué, physique, virtuel, sur site et dans le cloud	Alignement flexible sur les préférences et ressources de l'entreprise
Corrélation multi-vecteur avec les solutions de sécurité du contenu et de la messagerie	Visibilité sur une surface d'attaque plus étendue
Prévention	
Blocage instantané des attaques à des débits allant de 10 Mbit/s à 8 Gbit/s	Protection en temps réel contre les attaques par contournement
Réponse	
Faible taux de fausses alertes, catégorisation des riskwares et validation automatique des alertes IPS	Diminution des coûts d'exploitation liés au tri des alertes non justifiées
Passage rapide aux phases d'investigation et de validation des alertes, d'isolement des terminaux et de réponse à incident	**Automatisation et simplification des workflows de sécurité**
Preuves d'exécution et CTI exploitable avec informations contextuelles	**Priorisation et résolution accélérées des incidents de sécurité détectés**
Protection extensible, d'un seul site à plusieurs milliers	**Solution évolutive qui accompagne la croissance de l'entreprise**

Avantages techniques

Détection précise des menaces

FireEye Network Security fait appel à plusieurs techniques d'analyse pour détecter les attaques avec une grande précision et très peu de faux positifs :

- Le moteur **Multi-Vector Virtual Execution™ (MVX)** détecte les attaques zero-day, multiflux et par contournement grâce à une analyse dynamique et sans signatures dans un environnement virtuel sécurisé. Il stoppe les phases d'infection et de compromission d'une chaîne d'attaque en identifiant des exploits et malwares encore inconnus.
- Pour détecter et bloquer les attaques masquées, ciblées ou personnalisées, les moteurs **Intelligence-Driven Analysis (IDA)** ont recours à une analyse contextuelle basée sur des règles. Celle-ci se fonde sur des informations en temps réel tirées de sources telles que les millions de verdicts rendus par MVX, les données collectées par Mandiant, une société FireEye, lors de milliers d'heures de réponse à incident, et les travaux des équipes de recherche sur les menaces iSIGHT. Les moteurs IDA bloquent les phases d'infection, de compromission et d'intrusion d'une chaîne d'attaque en identifiant les exploits malveillants, les malwares et les rappels aux serveurs de commande et contrôle (CnC). Par ailleurs, ils extraient et transmettent le trafic réseau suspect au moteur MVX, qui à son tour l'analyse et rend un verdict définitif.
- Enfin, il est possible d'ajouter des indicateurs de menaces personnalisés aux moteurs IDA grâce au **Structured Threat Intelligence eXpression (STIX)**, un format normalisé destiné à l'acquisition de Threat Intelligence de sources externes.

Protection résiliente et instantanée

FireEye Network Security propose plusieurs modes de configuration flexibles :

- Surveillance hors bande via une connexion TAP/SPAN, surveillance instantanée ou blocage actif instantané. Un déploiement en mode blocage actif bloque automatiquement les exploits et malwares entrants, ainsi que les rappels multiprotocoles sortants. En mode surveillance instantanée, la solution génère des alertes et laisse aux entreprises le choix des actions à engager. En mode prévention hors bande, FireEye Network Security envoie des réinitialisations TCP pour le blocage hors bande des connexions TCP, UDP ou HTTP.
- Certains modèles proposent une option haute disponibilité active pour assurer la résilience en cas de pannes du réseau ou de l'équipement.

Couverture d'une large surface d'attaque

FireEye Network Security offre un niveau de protection cohérent aux environnements réseau hétérogènes d'aujourd'hui :

- Prise en charge de la plupart des systèmes d'exploitation Microsoft Windows et Apple Mac OS X
- Analyse de plus de 140 types de fichiers différents, dont les fichiers PE (Portable Executable), le contenu web, les archives, les images, les fichiers multimédias et les applications Java, Microsoft et Adobe
- Exécution du trafic réseau suspect dans de multiples combinaisons de systèmes d'exploitations, service packs, types et versions d'applications
- Protection contre les attaques et malwares difficiles à détecter via des systèmes de signatures traditionnels : uploads de web shells, exécution de web shells, ransomwares, cryptomineurs, etc.

Alertes validées et priorisées

En plus de détecter des attaques réelles, la technologie MVX de FireEye permet de déterminer la fiabilité des alertes détectées par des méthodes classiques de correspondance de signatures, mais aussi d'identifier et prioriser les alertes critiques :

- Le système de prévention des intrusions (IPS), allié à la validation du moteur MVX, réduit le temps nécessaire au tri des détections basées sur les signatures, souvent sources de fausses alertes.

- La catégorisation des riskwares permet de distinguer les véritables tentatives de compromission des activités certes indésirables mais moins nocives (par exemple les adwares et spywares) afin de prioriser les réponses.

Threat Intelligence exploitable

Les alertes générées par FireEye Network Security incluent une CTI contextuelle et des preuves concrètes qui vous permettent de prioriser les réponses et d'endiguer rapidement une menace :

- **Dynamic Threat Intelligence (DTI) –** Données en temps réel partagées partout dans le monde pour bloquer de façon rapide et proactive les attaques ciblées et récemment détectées.
- **Advanced Threat Intelligence (ATI) –** Informations contextuelles et recommandations pour accélérer la réponse et neutraliser la menace.

Intégration du workflow de réponse

Plusieurs produits s'intègrent à FireEye Network Security pour automatiser au maximum les workflows de réponse aux alertes :

- FireEye Central Management recoupe les alertes générées par FireEye Network Security et FireEye Email Security pour fournir une vue plus complète d'une attaque et configurer les règles de blocage destinées à empêcher sa propagation.
- FireEye Network Forensics s'intègre à FireEye Network Security pour associer des captures de paquets détaillées à une alerte et permettre de mener des investigations plus poussées.
- FireEye Endpoint Security identifie, valide et endigue les compromissions détectées par FireEye Network Security pour simplifier l'isolement et la remédiation des terminaux concernés.

Options de déploiement flexibles

FireEye Network Security propose plusieurs options de déploiement adaptées aux différents besoins et budgets des entreprises :

- **Solution Network Security intégrée –** Appliance matérielle et autonome tout-en-un, avec service MVX intégré pour sécuriser le point d'accès Internet d'un seul site. FireEye Network Security est une plate-forme sans client facile à gérer et déployable en moins de 60 minutes. Elle ne nécessite ni règles, ni politiques, ni paramétrages.
- **Solution Network Security distribuée –** Appliances extensibles avec partage central du service MVX pour sécuriser les points d'accès Internet d'une entreprise et/ou de ses filiales.
  - **Solution Network Smart Node –** Appliances physiques ou virtuelles qui analysent le trafic Internet 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.
  - **FireEye Cloud MVX –** Abonnement à MVX, un service hébergé par FireEye qui garantit la confidentialité des informations grâce à une analyse du trafic sur l'appliance Network Smart Node. Seuls les objets suspects sont transmis via une connexion cryptée au service MVX, qui ensuite écarte les objets reconnus comme inoffensifs.
  - **Protection sur site ou dans le cloud –** En plus des appliances autonomes et virtuelles, FireEye offre sa solution Network Security dans les environnements de cloud public avec mise à disposition d'images AMI (Amazon Machine Images).

Figure 2. Exemples d'appliances Network Security intégrées : NX 2550, NX 3500, NX 5500 et NX 10550.

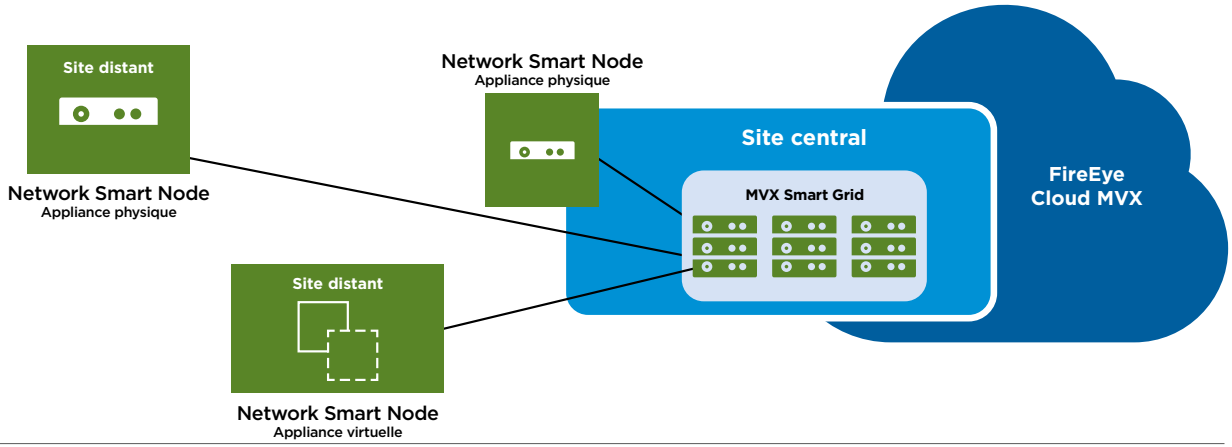


Figure 3. Modèles de déploiement distribués pour Network Security.

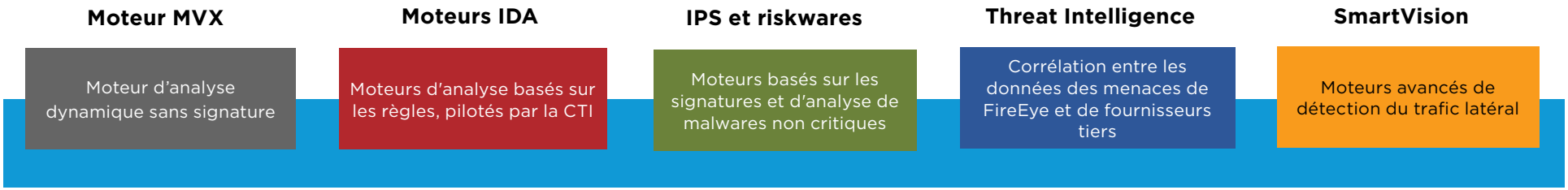


Figure 4. Composants modulaires de FireEye Network Security

Performances et évolutivité élevées

FireEye Network Security offre une protection des points d'accès Internet à différents débits, selon les besoins des entreprises (siège et/ou filiales).

Grâce à l'architecture évolutive de MVX Smart Grid et FireEye Cloud MVX, le service MVX peut prendre en charge entre un et plusieurs milliers d'appliances Network Smart Node, avec possibilités d'extension selon les besoins.

Format	Performance
Solution Network Security intégrée	50 Mbit/s à 5 Gbit/s
Appliance physique Network Smart Node	**50 Mbit/s à 10 Gbit/s**
Network Smart Node (appliance virtuelle et cloud public)	50 Mbit/s à 1 Gbit/s

Avantages métier

Conçu pour satisfaire les besoins des entreprises mono- ou multi-sites, FireEye Network Security offre de multiples avantages :

Limitation du risque de compromissions

FireEye Network Security est une solution de cyberdéfense ultraperformante :

- Elle bloque les attaques ciblées, avancées et par contournement visant à infiltrer une entreprise pour faire main basse sur ses ressources critiques ou perturber ses activités.
- Elle bloque les attaques et les intrusions plus rapidement grâce à des preuves concrètes, une CTI exploitable, un blocage instantané et des workflows de réponse automatisés.
- Elle élimine les points vulnérables du dispositif de sécurité d'une entreprise grâce à une protection cohérente de nombreux systèmes d'exploitation, types d'applications, filiales et sites principaux.

Amortissement rapide

Selon une étude récente de Forrester Consulting[1], les clients FireEye Network Security peuvent escompter un retour sur investissement de 152 % sur trois ans et un amortissement de l'investissement initial en seulement 9,7 mois. Les avantages de la solution FireEye Network Security :

- Elle permet à l'équipe de sécurité de se concentrer sur les véritables attaques et favorise ainsi une diminution des coûts d'exploitation.
- Elle optimise les dépenses d'investissement grâce à un service MVX partagé et de nombreuses options de performances permettant de dimensionner le déploiement en fonction des besoins.
- Elle pérennise l'investissement en sécurité grâce à une conception évolutive, conçue pour accompagner le développement de l'entreprise ou l'augmentation du trafic Internet.
- Elle protège les investissements existants en proposant une migration gratuite d'une solution intégrée vers un déploiement distribué.
- Elle réduit les dépenses d'investissement grâce à une architecture modulaire et extensible.

Récompenses et certifications

La gamme de produits FireEye Network Security s'est distinguée au travers de nombreuses récompenses et certifications décernées par des acteurs du secteur de la sécurité et par des instances officielles :

- En 2018, Frost & Sullivan a confirmé la position de leader incontesté de FireEye, avec une part de marché de 46 %, soit plus que les 10 concurrents suivants réunis[2].
- FireEye Network Security a reçu quantité de prix et distinctions du SANS Institute, SC Magazine, CRN et bien d'autres.
- Elle fut même la toute première solution du marché à bénéficier de la certification SAFETY (Support Anti-Terrorism By Fostering Effective Technologies) du ministère américain de la Sécurité intérieure.

1 Forrester (mai 2016), The Total Economic Impact Of FireEye
2 Frost & Sullivan (2018), Marché mondial des sandbox Advanced Malware (prévisions 2022).

Tableau 1. Spécifications de FireEye Network Security, appliance intégrée

	NX 2500	NX 2550	NX 3500	NX 4500	NX 5500	NX 6500
Systèmes d'exploitation pris en charge	Linux macOS X Microsoft Windows	Linux macOS X Microsoft Windows	Linux macOS X Microsoft Windows	Linux macOS X Microsoft Windows	Linux macOS X Microsoft Windows	Linux macOS X Microsoft Windows
Performances*	Jusqu'à 50 Mbit/s ou 100 Mbit/s	Jusqu'à 250 Mbit/s	Jusqu'à 500 Mbit/s	Jusqu'à 1 Gbit/s	Jusqu'à 2,5 Gbit/s	Jusqu'à 5 Gbit/s
Interface de surveillance réseau	4 x 1 GigE bypass	4 x 10 GigE SFP+ 4 x 1 GigE bypass	4 x 10 GigE SFP+ 4 x 1 GigE bypass	8 x 10 GigE SFP+ 4 x 1 GigE bypass	8 x 10 GigE SFP+ 4 x 1 GigE bypass	8 x 10GigE SFP+ 2 x 40 GigE QSFP+
Mode de fonctionnement des ports réseau	Surveillance instantanée, fail open, fail close (bypass matériel) ou TAP/SPAN	Surveillance instantanée, fail open, fail close (bypass matériel) ou TAP/SPAN	Surveillance instantanée, fail open, fail close (bypass matériel) ou TAP/SPAN	Surveillance instantanée, fail open, fail close (bypass matériel) ou TAP/SPAN	Surveillance instantanée, fail open, fail close (bypass matériel) ou TAP/SPAN	Surveillance instantanée ou TAP/SPAN
Haute disponibilité	Non disponible	Non disponible	Non disponible	Disponible	Disponible	Disponible
Interfaces de gestion (panneau arrière)	2 ports 10/100/1000 BASE-T	2 x 1 GigE	2 x 1 GigE	2 x 1 GigE	2 x 1 GigE	2 x 1 GigE
Port IPMI	Panneau avant	Panneau arrière	Panneau arrière	Panneau arrière	Panneau arrière	Panneau arrière
Écran LCD et clavier (panneau avant)	Non disponible	Non disponible	Non disponible	Non disponible	Non disponible	Non disponible
Port VGA	Non	Oui	Oui	Oui	Oui	Oui
Ports USB	2 ports USB de type A (panneau avant)	4 ports USB de type A (tous à l'arrière)	4 ports USB de type A 2 avant, 2 arrière	4 ports USB de type A 2 avant, 2 arrière	4 ports USB de type A 2 avant, 2 arrière	2 ports USB de type A
Port série (panneau arrière)	115 200 bit/s, pas de parité, 8 bits, 1 bit d'arrêt (connecteur RJ45, câble adaptateur RJ45–D-sub inclus)	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	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	Un seul disque dur SATA interne fixe de 1 To, 3,5 pouces	2 disques durs de 4 To, 3,5 pouces, SAS3, 7,2 KRPM, RAID 1, remplaçable	2 disques durs de 4 To, 3,5 pouces, SAS3, 7,2 KRPM, RAID 1, remplaçable	2 disques durs de 4 To, 3,5 pouces, SAS3, 7,2 KRPM, RAID 1, remplaçable	2 disques durs de 4 To, 3,5 pouces, SAS3, 7,2 KRPM, RAID 1, remplaçable	2 disques durs de 10 To 3,5 pouces, SAS3, 7,2 KRPM RAID 1, remplaçable
Châssis	Montage en baie 1U, s'intègre en baie 19 pouces	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	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 50 x 4,32 cm	43,7 x 65 x 4,32 cm	43,8 x 62 x 8,84 cm	43,8 x 62 x 8,84 cm	43,8 x 62 x 8,84 cm	43,7 x 78,7 x 8,9 cm
Alimentation en courant alternatif	Interne, non redondante, fixe, 250 W à 90 - 264 VCA, 3,5 - 1,5 A, embase secteur IEC 60320-C14, 50 - 60 Hz	Redondante (1+1) 750 W à 100 - 240 VCA, 8 - 4,5 A, embase secteur IEC 60320-C14 50 - 60 Hz, remplaçable	Redondante (1+1) 800 W à 100 - 240 VCA, 10,5 - 4 A, embase secteur IEC 60320-C14, 50 - 60 Hz, remplaçable	Redondante (1+1) 800 W à 100 - 240 VCA, 10,5 - 4 A, embase secteur IEC 60320-C14, 50 - 60 Hz, remplaçable	Redondante (1+1) 800 W à 100 - 240 VCA, 10,5 - 4 A, embase secteur IEC 60320-C14, 50 - 60 Hz, remplaçable	1000 W redondant (1+1) ; 100-240 VCA 10,5 - 4 A, 50-60 Hz, embase secteur IEC60320-C14, remplaçable

Tableau 1. Spécifications de FireEye Network Security, appliance intégrée (suite)

	NX 2500	NX 2550	NX 3500	NX 4500	NX 5500	NX 6500
Puissance maximale	85 W	265 W	426 W	519 W	658 W	660 W
Dissipation thermique maximale	290 BTU/h	904 BTU/h	1 454 BTU/h	1 771 BTU/h	2 245 BTU/h	2 252 BTU/h
Temps moyen de bon fonctionnement	108 944 h	54 200 h	65 466 h	57 766 h	52 802 h	54 041 h
Poids de l'appliance seule/avec emballage	7,3 kg / 12,79 kg	13,5 / 18,5 kg	17 / 26,6 kg	19,2 / 28,8 kg	19,2 / 29 kg	20 / 32,2 kg
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	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	IEC 60950 EN 60950-1 UL 60950 CSA/CAN-C22.2
Certifications de sécurité	FIPS 140-2 Niveau 1 CC NDPP v1.1	FIPS 140-2 Niveau 1 CC NDPP v1.1	FIPS 140-2 Niveau 1 CC NDPP v1.1	FIPS 140-2 Niveau 1 CC NDPP v1.1	FIPS 140-2 Niveau 1 CC NDPP v1.1	FIPS 140-2 Niveau 1 CC NDPP vw1.1
Conformité aux normes EMC	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	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	Sécurité : EN 60950, C22.2, UL 60950, IEC 60950, CAN/CSA-C22.2, K 60950, AS/NZS 60950, GB 4943.1, J60950, SI60950 EMC : FCC (article 15, sous-article B, classe A), ICES-003, EN55032, VCCI V-3, EN 55024, EN 61000, CNS 13438, CISPR32, KN 32, KN 35
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	Directive RoHS 2011/65/UE REACH Directive DEEE 2012/19/UE	Directive RoHS 2011/65/UE REACH Directive DEEE 2012/19/UE	RoHS, REACH, DEEE, Réglementation sur les minéraux de conflits
Température de fonctionnement	0 ~ 40 °C	0 ~ 40 °C	0 ~ 40 °C	0 ~ 40 °C	0 ~ 40 °C	0 ~ 40 °C
Température à l'arrêt	-20 ~80 °C	-30 ~ 70 °C	-40 ~ 70 °C	-40 ~ 70 °C	-40 ~ 70 °C	-30 ~ 70 °C
Plage d'humidité relative tolérée	5 ~ 85 % @ 40 °C, sans condensation	10 ~ 95 % @ 40 °C, sans condensation	10 ~ 95 % @ 40 °C, sans condensation	10 ~ 95 % @ 40 °C, sans condensation	10 ~ 95 % @ 40 °C, sans condensation	10 ~ 90 % @ 40 °C sans condensation
Taux d'humidité relative à l'arrêt	5 ~ 85 % @ 40 °C, sans condensation	10 ~ 95 % @ 60 °C, sans condensation	10 ~ 95 % @ 60 °C, sans condensation	10 ~ 95 % @ 60 °C, sans condensation	10 ~ 95 % @ 60 °C, sans condensation	10 ~ 95 % @ 55 °C sans condensation
Altitude maximale de fonctionnement	3 000 m .	3 000 m .	3 000 m .	3 000 m .	3 000 m .	3 000 m .

Tableau 2. Performances de l'IPS de FireEye Network Security, appliance intégrée

	NX 2500	NX 2550	NX 3500	NX 4500	NX 5500	NX 6500
Performances IPS max.	Jusqu'à 50 Mbit/s ou 100 Mbit/s	Jusqu'à 250 Mbit/s	Jusqu'à 500 Mbit/s	Jusqu'à 1 Gbit/s	Jusqu'à 2,5 Gbit/s	Jusqu'à 5 Gbit/s
Connexions simultanées max.	15 000 ou 80 000	80 000	160 000	500 000	1 000 000	2 000 000
Nouvelles connexions par seconde	750/s ou 4 000/s	4 000/s	8 000/s	10 000/s	20 000/s	40 000/s

Tableau 3. Spécifications de FireEye Network Smart Node, appliance physique

	NX 1500	NX 2500	NX 2550	NX 3500	NX 4500	NX 5500	NX 6500
Systèmes d'exploitation pris en charge	Linux macOS X Microsoft Windows	Linux macOS X Microsoft Windows	Linux macOS X Microsoft Windows	Linux macOS X Microsoft Windows	Linux macOS X Microsoft Windows	Linux macOS X Microsoft Windows	Linux macOS X Microsoft Windows
Performance	Jusqu'à 50 Mbit/s	Jusqu'à 100 Mbit/s ou 250 Mbit/s	Jusqu'à 500 Mbit/s	Jusqu'à 1 Gbit/s	Jusqu'à 2 Gbit/s	Jusqu'à 5 Gbit/s	Jusqu'à 10 Gbit/s
Interface de surveillance réseau	4 ports 10/100/1000 BASE-T	4 x 1 GigE bypass	4 x 10 GigE SFP+ 4 x 1 GigE bypass	4 x 10 GigE SFP+ 4 x 1 GigE bypass	8 x 10 GigE SFP+ 4 x 1 GigE bypass	8 x 10 GigE SFP+ 4 x 1 GigE bypass	8 x 10GigE SFP+ 2 x 40 GigE QSFP+
Mode de fonctionnement des ports réseau	Surveillance instantanée, fail close ou TAP	Surveillance instantanée, fail open, fail close (bypass matériel) ou TAP/ SPAN	Surveillance instantanée, fail open, fail close (bypass matériel) ou TAP/ SPAN	Surveillance instantanée, fail open, fail close (bypass matériel) ou TAP/ SPAN	Surveillance instantanée, fail open, fail close (bypass matériel) ou TAP/ SPAN	Surveillance instantanée, fail open, fail close (bypass matériel) ou TAP/ SPAN	Surveillance instantanée ou TAP/ SPAN
Haute disponibilité	Non disponible	Non disponible	Non disponible	Non disponible	Non disponible	Non disponible	Non disponible
Interfaces de gestion (panneau arrière)	2 ports 10/100/1000 BASE-T	2 x 1 GigE	2 x 1 GigE	2 x 1 GigE	2 x 1 GigE	2 x 1 GigE	2 x 1 GigE
Port IPMI	Non disponible	Panneau avant	Panneau arrière	Panneau arrière	Panneau arrière	Panneau arrière	Panneau arrière
Écran LCD et clavier (panneau avant)	Non disponible	Non disponible	Non disponible	Non disponible	Non disponible	Non disponible	Non disponible
Port VGA	Non disponible	Non disponible	Oui	Oui	Oui	Oui	Oui
Ports USB	2 ports USB de type A	2 ports USB de type A (panneau avant)	4 ports USB de type A (tous à l'arrière)	4 ports USB de type A 2 avant, 2 arrière	4 ports USB de type A 2 avant, 2 arrière	4 ports USB de type A 2 avant, 2 arrière	2 ports USB de type A

Tableau 3. Spécifications de FireEye Network Smart Node, appliance physique (suite)

	NX 1500	NX 2500	NX 2550	NX 3500	NX 4500	NX 5500	NX 6500
Port série (panneau arrière)	115 200 bit/s, pas de parité, 8 bits, 1 bit d'arrêt (connecteur RJ45, câble adaptateur RJ45–D-sub inclus)	115 200 bit/s, pas de parité, 8 bits, 1 bit d'arrêt (connecteur RJ45, câble adaptateur RJ45–D-sub inclus)	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	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	Un seul disque dur SATA interne fixe de 500 Go, 2,5 pouces	Un seul disque dur SATA interne fixe de 1 To, 3,5 pouces	2 disques durs de 4 To, 3,5 pouces, SAS3, 7,2 KRPM, RAID 1, remplaçable	2 disques durs de 4 To, 3,5 pouces, SAS3, 7,2 KRPM, RAID 1, remplaçable	2 disques durs de 4 To, 3,5 pouces, SAS3, 7,2 KRPM, RAID 1, remplaçable	2 disques durs de 4 To, 3,5 pouces, SAS3, 7,2 KRPM, RAID 1, remplaçable	2 disques durs de 10 To 3,5 pouces, SAS3, 7,2 KRPM RAID 1, remplaçable
Châssis	Format poste de travail	Montage en baie 1U, s'intègre en baie 19 pouces	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	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	28 x 17,5 x 4,4 cm	43,7 x 50 x 4,32 cm	43,7 x 65 x 4,32 cm	43,8 x 62 x 8,84 cm	43,8 x 62 x 8,84 cm	43,8 x 62 x 8,84 cm	43,7 x 78,7 x 8,9 cm
Alimentation en courant alternatif	Adaptateur secteur externe 12 V à 5 A, 60 W, 90 - 264 VCA,, embase secteur IEC 60320-C14, 50 - 60 Hz, remplaçable	Interne, non redondante, fixe, 250 W à 90 - 264 VCA, 3,5 - 1,5 A, embase secteur IEC 60320-C14, 50 - 60 Hz	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) 800 W à 100 - 240 VCA 9 - 4,5 A, embase secteur IEC 60320-C14 50 - 60 Hz, remplaçable	Redondante (1+1) 800 W à 100 - 240 VCA 9 - 4,5 A, embase secteur IEC 60320-C14 50 - 60 Hz, remplaçable	Redondante (1+1) 800 W à 100 - 240 VCA, 10,5 - 4 A, embase secteur IEC 60320-C14, 50 - 60 Hz, remplaçable	Redondante (1+1) 1000 W à 100 - 240 VCA, 10,5 - 4 A, embase secteur IEC 60320-C14, 50 - 60 Hz, remplaçable
Puissance maximale	24 W	85 W	265 W	426 W	519 W	658 W	660 W
Dissipation thermique maximale	82 BTU/h	290 BTU/h	904 BTU/h	1 454 BTU/h	1 771 BTU/h	2 245 BTU/h	2 252 BTU/h
Temps moyen de bon fonctionnement	193 772 h	108 944 h	54 200 h	65 466 h	57 766 h	52 802 h	54 041 h
Poids de l'appliance seule/avec emballage	1,7 kg / 2,95 kg	7,3 kg / 12,79 kg	13,5 kg / 18,5 kg	17 kg / 26,6 kg	19,2 / 28,8 kg	19,2 / 29 kg	20 kg 32,2 kg
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	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	IEC 60950 EN 60950-1 UL 60950 CSA/CAN-C22.2	IEC 60950 EN 60950-1 UL 60950 CSA/CAN-C22.2
Certifications de sécurité	FIPS 140-2 Niveau 1 CC NDPP v1.1	FIPS 140-2 Niveau 1 CC NDPP v1.1	FIPS 140-2 Niveau 1 CC NDPP v1.1	FIPS 140-2 Niveau 1 CC NDPP v1.1	FIPS 140-2 Niveau 1 CC NDPP v1.1	FIPS 140-2 Niveau 1 CC NDPP v1.1	FIPS 140-2 Niveau 1 CC NDPP v1.1

Tableau 3. Spécifications de FireEye Network Smart Node, appliance physique (suite)

	NX 1500	NX 2500	NX 2550	NX 3500	NX 4500	NX 5500	NX 6500
Conformité aux normes EMC	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	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	Sécurité : EN 60950, C22.2, UL 60950, IEC 60950, CAN/CSA-C22.2, K 60950, AS/NZS 60950, GB 4943.1, J60950, SI60950 EMC : FCC (article 15, sous-article B, classe A), ICES-003, EN55032, VCCI V-3, EN 55024, EN 61000, CNS 13438, CISPR32, KN 32, KN 35
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	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	RoHS, REACH, DEEE, Réglementation sur les minéraux de conflits
Température de fonctionnement	0 ~ 40 °C	0 ~ 40 °C	0 ~ 40 °C	0 ~ 40 °C	0 ~ 40 °C	0 ~ 40 °C	0 ~ 40 °C
Température à l'arrêt	-20 ~ 80 °C	-20 ~ 80 °C	-30 ~ 70 °C	-40 ~ 70 °C	-40 ~ 70 °C	-40 ~ 70 °C	-30 ~ 70 °C
Plage d'humidité relative tolérée	10 ~ 95 % @ 40 °C, sans condensation	5 ~ 85 % @ 40 °C, sans condensation	10 ~ 95 % @ 40 °C, sans condensation	10 ~ 95 % @ 40 °C, sans condensation	10 ~ 95 % @ 40 °C, sans condensation	10 ~ 95 % @ 40 °C, sans condensation	10 ~ 90 % @ 40 °C, sans condensation
Taux d'humidité relative à l'arrêt	10 ~ 95 % @ 60 °C, sans condensation	5 ~ 95 % @ 40 °C, sans condensation	10 ~ 95 % à 60 °C, sans condensation	10 ~ 95 % à 60 °C, sans condensation	10 ~ 95 % à 60 °C, sans condensation	10 ~ 95 % à 60 °C, sans condensation	10 ~ 95 % @ 55 °C, sans condensation
Altitude maximale de fonctionnement	3 000 m .	3 000 m .	3 000 m .	3 000 m .	3 000 m .	3 000 m .	3 000 m .

Tableau 4. Spécifications IPS de FireEye Network Security Smart Node, appliance physique

	NX 1500	NX 2500	NX 2550	NX 3500	NX 4500	NX 5500	NX 6500
Performances IPS max.	Jusqu'à 50 Mbit/s	Jusqu'à 100 / 250 Mbit/s	Jusqu'à 500 Mbit/s	Jusqu'à 1 Gbit/s	Jusqu'à 2 Gbit/s	Jusqu'à 5 Gbit/s	Jusqu'à 10 Gbit/s
Connexions simultanées max.	15 000	80 000	160 000	500 000	1 000 000	2 000 000	4 000 000
Nouvelles connexions par seconde	750/s	4 000/s	8 000/s	10 000/s	20 000/s	40 000/s	80 000/s

Tableau 5. Spécifications IPS de FireEye Network Security Smart Node, appliance virtuelle

	VA-NXS 1500	VA-NXS 2500	VA-NXS 2550	VA-NXS 4500	VA-NXS 6500
Systèmes d'exploitation pris en charge	Linux macOS X Microsoft Windows	Linux macOS X Microsoft Windows	Linux macOS X Microsoft Windows	Linux macOS X Microsoft Windows	Linux macOS X Microsoft Windows
Performances*	Jusqu'à 50 Mbit/s	Jusqu'à 100 Mbit/s	Jusqu'à 250 Mbit/s	Jusqu'à 500 Mbit/s	Jusqu'à 1 Gbit/s
Interface de surveillance réseau	1 – 8	1 – 8	1 – 8	1 – 8	1 – 8
Ports de gestion réseau	1 ou 2	1 ou 2	1 ou 2	1 ou 2	1 ou 2
Mode de fonctionnement des ports réseau	En mode blocage actif, SPAN	En mode blocage actif, SPAN	En mode blocage actif, SPAN	En mode blocage actif, SPAN	En mode blocage actif, SPAN
Cœurs de processeur	3	6	8	8	16
Mémoire	10 Go	16 Go	16 Go	32 Go	32 Go
Capacité des disques	384 Go	384 Go	384 Go	512 Go	512 Go
Cartes réseau	VMXNet 3, vNIC	VMXNet 3, vNIC	VMXNet 3, vNIC	VMXNet 3, vNIC	VMXNet 3, vNIC
Prise en charge d'hyperviseur	VMware ESXi 6.0 (ou ultérieur) et KVM 1.5.3 (ou ultérieur)	VMware ESXi 6.0 (ou ultérieur) et KVM 1.5.3 (ou ultérieur)	VMware ESXi 6.0 (ou ultérieur) et KVM 1.5.3 (ou ultérieur)	VMware ESXi 6.0 (ou ultérieur) et KVM 1.5.3 (ou ultérieur)	VMware ESXi 6.0 (ou ultérieur) et KVM 1.5.3 (ou ultérieur)
Certifications de sécurité	FIPS 140-2 Niveau 1 CC NDPP v1.1 (en cours)	FIPS 140-2 Niveau 1 CC NDPP v1.1 (en cours)	FIPS 140-2 Niveau 1 CC NDPP v1.1 (en cours)	FIPS 140-2 Niveau 1 CC NDPP v1.1 (en cours)	FIPS 140-2 Niveau 1 CC NDPP v1.1 (en cours)

Tableau 6. Spécifications IPS de FireEye Network Security Smart Node, appliance virtuelle

	VA-NXS 1500	VA-NXS 2500	VA-NXS 2550	VA-NXS 4500	VA-NXS 6500
Performances IPS max.	Jusqu'à 50 Mbit/s	Jusqu'à 100 Mbit/s	Jusqu'à 250 Mbit/s	Jusqu'à 500 Mbit/s	Jusqu'à 1 Gbit/s
Connexions simultanées max.	15 000	80 000	80 000	160 000	500 000
Nouvelles connexions par seconde	750/s	4 000/s	4 000/s	8 000/s	10 000/s

Tableau 7. Tailles des AMI prises en charge par FireEye Network Security sur AWS

Modèle	Débit	vCPU	Mémoire	Disques	Interfaces réseau	Type d'instance AWS
NX4500v	500 Mbit/s	8	32 Go	512 Go (EBS)	Un port de gestion, un port de soumission et deux ports de surveillance (4 au total)	M5.2xlarge
NX6500v	1 Gbit/s	16	64 Go	512 Go (EBS)	Un port de gestion, un port de soumission et six ports de surveillance (8 au total)	M5.4xlarge

Tableau 8. Spécifications de FireEye MVX Smart Grid

	VX 5500	VX 12550
Systèmes d'exploitation pris en charge	Linux macOS X Microsoft Windows	Linux macOS X Microsoft Windows
Performances*	Jusqu'à 2 Gbit/s	Jusqu'à 14 Gbit/s
Haute disponibilité **	N+1	N+1
Interfaces de gestion (panneau arrière)	1 x 10/100/1000 Mbit/s BASE-T	1 x 10/100/1000 Mbit/s BASE-T
Ports cluster (panneau arrière)	3 x 10/100/1000 Mbit/s BASE-T	1 x 10/100/1000 Mbit/s BASE-T, 2 x 10 Gbit/s BASE-T, 4 ports 10 GigE SFP+
Port IPMI (panneau arrière)	Inclus	Inclus
Écran LCD et clavier (panneau avant)	Non disponible	Sans LCD
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 SAS3 de 2 To, RAID 1, 3,5 pouces, remplaçables	2 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	43,7 x 65 x 4,32 cm	43,7 x 78,7 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) 1000 W, 100 - 240 VCA, 1,5 - 4 A, embase secteur IEC 60320-C14, 50 - 60 Hz, remplaçable
Puissance maximale	285 W	660 W
Dissipation thermique maximale	972 BTU/h	2594 BTU/h
Temps moyen de bon fonctionnement	54 200 h	54 041 h
Poids de l'appliance seule/avec emballage	12,2 kg / 17,2 kg	20 kg / 32,2 kg
Certification de sécurité	FIPS 140-2 Niveau 1, CC NDPP v1.1 (en attente)	FIPS 140-2 Niveau 1, CC NDPP v1.1 (en attente)
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

Tableau 8. Spécifications de FireEye MVX Smart Grid

	VX 5500	VX 12550
Conformité aux normes EMC	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
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
Température de fonctionnement	0 ~ 40 °C	0 ~ 40 °C
Température à l'arrêt	-30 ~ 70 °C	-30 ~ 70 °C
Plage d'humidité relative tolérée	10 ~ 95 % à 40 °C, sans condensation	10 ~ 90 % à 40 °C, sans condensation
Taux d'humidité relative à l'arrêt	10 ~ 95 % à 60 °C, sans condensation	10 ~ 95 % à 55 °C, sans condensation
Altitude maximale de fonctionnement	3000 m .	3000 m .

Services de support

FireEye propose des formules de support simples et flexibles qui vous permettent d'exploiter tout le potentiel des produits et services FireEye. Il existe quatre niveaux de services de support : Platinum, Platinum Priority Plus, Government et Government Priority Plus. Pour en savoir plus sur le support FireEye, référez-vous aux services de support FireEye.

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 cyberveille. 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.

FIREEYE™