FIREEYE™

FICHE PRODUIT

FireEye Endpoint Security

Neutralisez les attaques grâce à une CTI de terrain

POINTS FORTS

- Prévention contre la majeure partie des cyberattaques ciblant les terminaux d'un environnement
- Détection et blocage des intrusions pour en réduire l'impact
- Détection plus rapide des menaces grâce au traitement prioritaire des alertes réelles
- Utilisation d'un agent unique et léger pour minimiser l'impact sur les utilisateurs finaux
- Protections et fonctionnalités offertes par les modules téléchargeables
- Conformité PCI-DSS, HIPAA, etc.
- Déploiement sur site ou dans le cloud

À l'origine, les solutions traditionnelles de protection des terminaux ne sont pas conçues pour lutter contre des attaques sophistiquées ou des menaces de type APT. Or, une protection efficace des terminaux passe par une solution capable d'analyser et de réagir rapidement devant de telles menaces.

FireEye Endpoint Security s'appuie sur le meilleur des produits de sécurité traditionnels pour y ajouter la technologie, l'expertise et la Cyber Threat Intelligence (CTI) signées FireEye. Objectif : vous protéger efficacement face aux cyberattaques actuelles. Conçu sur un modèle de défense en profondeur (Defense-in-Depth), Endpoint Security s'appuie sur une architecture modulaire dotée de moteurs préconfigurés et de modules téléchargeables pour protéger, détecter et gérer les agents.

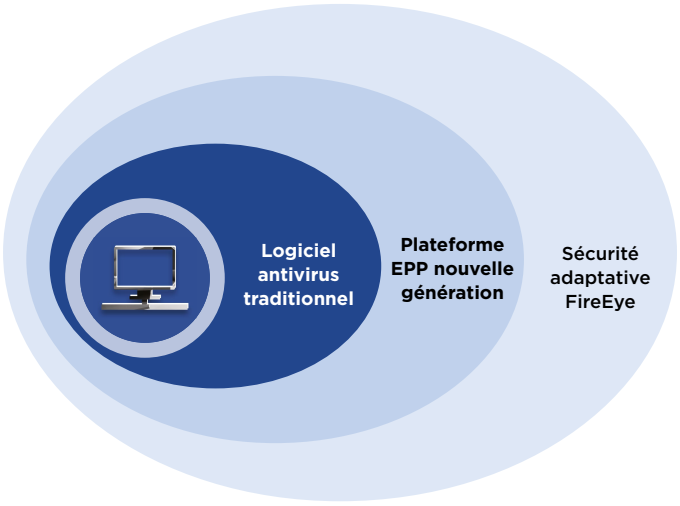
Pour bloquer les malwares courants, Endpoint Security utilise un moteur EPP (Endpoint Protection Platform) basé sur les signatures. Pour les menaces émergentes qui n'ont pas encore été caractérisées par une signature, MalwareGuard fait appel à des technologies de machine learning nourries par une CTI de terrain. Face aux menaces APT, les fonctionnalités EDR (Endpoint Detection and Response) déploient un moteur d'analyse des comportements capable de détecter toute activité suspecte. Notre moteur d'indicateurs de compromission (IOC) se base sur une CTI en temps réel pour détecter les menaces furtives. Pour ajouter de nouveaux moteurs et fonctionnalités, vous pouvez télécharger des modules sur FireEye Market.

Malgré la meilleure des protections, les intrusions sont inévitables. Pour réduire au maximum les perturbations, Endpoint Security apporte une réponse rapide au moyen d'un jeu d'outils complet :

- Recherche et investigation des menaces connues et inconnues sur des dizaines de milliers de terminaux en quelques minutes
- Identification des vecteurs utilisés par une attaque pour infiltrer un terminal
- Confirmation d'une attaque passée (et encore active) sur un terminal donné
- Établissement de la chronologie et de la durée de compromission du terminal, et suivi de l'incident
- Identification des terminaux et systèmes à mettre en quarantaine pour prévenir toute propagation

L'informatique est un formidable outil pédagogique pour nos étudiants. Grâce à FireEye Endpoint Security, nous sommes en mesure d'assurer la disponibilité, la performance et la sécurité de notre parc informatique. Ceci est crucial pour réaliser notre mission.

– James D. Perry II
RSSI, Université de Caroline du Sud



Les dirigeants pensent souvent qu'un virus, quel qu'il soit, est la fin du monde. FireEye me permet de présenter des preuves concrètes de la nature du problème et de démontrer la façon dont nous avons pu gérer et isoler la menace. Cette capacité à expliquer les choses telles qu'elles sont permet de relâcher la pression sur tous les acteurs concernés.

– Michael Hennessy, Directeur des services technologiques
Alpha Grainer Manufacturing, Inc

Principales caractéristiques

- Agent unique basé sur un modèle de défense en profondeur visant à minimiser la configuration et optimiser la détection et le blocage
- Analyse et neutralisation des menaces au sein d'un workflow FireEye Endpoint Security unique
- Protection 100 % intégrée contre les malwares (antivirus), machine learning, analyse comportementale, indicateurs de compromission (IOC) et visibilité sur les terminaux
- Triage Summary et Audit Viewer pour l'inspection et l'analyse exhaustives des menaces

Fonctionnalités supplémentaires

- Enterprise Security Search pour localiser et interpréter toute activité suspecte ou malveillante
- Data Acquisition pour une inspection et une analyse approfondie des terminaux sur une période donnée
- Visibilité de bout en bout permettant aux équipes de sécurité de rechercher, d'identifier et d'évaluer le niveau de gravité des menaces
- Fonctions de détection et de réponse visant à détecter, investiguer et confiner les terminaux infectés pour accélérer l'intervention
- Interface intuitive pour une interprétation et une réponse rapides à toute activité suspecte sur un terminal

Systèmes d'exploitation et environnements pris en charge	
Windows	Windows 7, 8, 8.1, 10 Server 2008R2, 2012R2, 2016, 2019
Mac	OS X 10.9+
Linux	Red Hat Enterprise Linux 6.8+, 7.2+, 8 CentOS 6.8+, 7.2+, 8 Ubuntu 14.04, 16.04, 18.04 SUSE 11.3, 11.4, 12.2, 12.3, 15 Open SUSE 15.1 Amazon AMI 2018.3, AMI2 Oracle Linux 6.10 et 7.6

Options de déploiement : équipement physique sur site, appliance virtuelle sur site, service cloud 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 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.