FIREEYE™

FICHE PRODUIT

File Protect

Détection et élimination des malwares sur les plateformes de contenus et de stockage en ligne

EN BREF

- Détecte les malwares latents qui échappent aux moteurs antivirus traditionnels
- Se déploie en mode de quarantaine active (mode de protection) ou en analyse uniquement (mode de surveillance)
- Offre des analyses récursives, programmées et spontanées pour les plateformes de stockage compatibles CIFS et NFS
- Fournit une protection proactive de Microsoft SharePoint et OneDrive
- Analyse une grande variété de types de fichiers (PDF, documents Microsoft Office, fichiers multimédias, etc.)
- S'intègre à FireEye Endpoint Security pour rationaliser les conventions de nommage et la priorisation des réponses à incident
- Partage les renseignements sur les menaces au travers de FireEye Central Management et du cloud FireEye DTI

Présentation

FireEye File Protect protège les données d'une grande variété de fichiers contre les attaques issues du cloud, du web mail, d'outils de transfert de fichiers, de périphériques de stockage portables, voire de plateformes de partage de fichiers et de référentiels de contenus. File Protect analyse ces supports de stockage pour détecter et mettre en quarantaine les malwares capables de contourner les solutions IPS, les antivirus, les passerelles et les pare-feu de nouvelle génération.

Problématiques des malwares présents sur les plateformes de stockage en ligne

De nos jours, les cyberattaques avancées s'appuient sur des malwares sophistiqués et des tactiques dites APT (Advanced Persistent Threat) pour percer les systèmes de défense et se propager latéralement sur les plateformes de stockage en ligne et les référentiels de contenus. Elles peuvent ainsi établir leur présence sur le réseau et infecter de nombreux systèmes, même hors ligne. Beaucoup de contenus d'entreprises sont particulièrement exposés à ces malwares car les dispositifs de défense traditionnels des data centers ne font pas le poids face à ces attaques qui s'introduisent souvent sur le réseau par des moyens légitimes. Les cybercriminels profitent de ces vulnérabilités pour installer des malwares sur les plateformes de stockage en réseau et infiltrer du code malveillant dans les vastes datastores des entreprises. Ce faisant, ils parviennent à établir une menace persistante même après l'application de mesures correctives.

Importance d'une protection efficace des contenus de fichiers

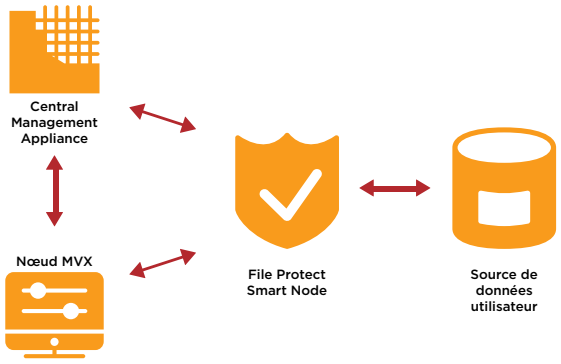
En l'absence d'un mécanisme de détection des malwares dissimulés dans les contenus, les auteurs d'APT peuvent exploiter les ressources réseau pour exfiltrer des informations propriétaires et causer des dommages sévères. File Protect analyse les plateformes de stockage en ligne à l'aide du moteur breveté FireEye Multi-Vector Virtual Execution™ (MVX), qui détecte le code malveillant zero-day incorporé dans les types de fichiers courants (PDF, MS Office, vCards, ZIP/RAR/TNEF, etc.) et le contenu multimédia (QuickTime, MP3, Real Player, JPG, PNG, etc.). Sa méthode consiste à effectuer des analyses récursives, programmées et spontanées des plateformes de partage de fichiers en réseau et des datastores accessibles pour identifier et mettre en quarantaine les malwares détectés. Les attaques avancées se trouvent ainsi stoppées à un moment charnière de l'attaque.

Détection des menaces inconnues et zero-day

File Protect inspecte chaque fichier pour y détecter l'éventuelle présence d'exploits zero-day ou de code malveillant. Le moteur FireEye MVX analyse le trafic dans un environnement virtuel sécurisé, à la recherche des attaques zero-day, multi-flux et autres menaces par contournement. Il stoppe les phases d'infection et de compromission d'une chaîne d'attaque en identifiant des exploits et malwares encore inconnus.

La puissance de MVX Smart Grid

L'architecture flexible et évolutive de FireEye MVX Smart Grid démultiplie l'efficacité de FireEye Network Security dans les environnements cloud hybrides ou privés. MVX Smart Grid sépare le moteur MVX du matériel et des nœuds Smart Nodes™ virtuels pour renforcer la sécurité des campus, des succursales et des utilisateurs à distance. IPS, analytique, analyse statique, Threat Intelligence appliquée... Smart Nodes s'appuie sur diverses techniques de surveillance du trafic Internet pour détecter et bloquer les menaces, avec l'appui du moteur MVX pour l'analyse dynamique des données.



Protection de Microsoft OneDrive et SharePoint

File Protect analyse continuellement le contenu pour signaler la présence de malwares dans les référentiels OneDrive et SharePoint et procéder à leur mise en quarantaine permanente. La plateforme exploite le protocole WebDAV pour s'intégrer en toute sécurité aux services SharePoint et protéger les workflows métiers qui utilisent les référentiels SharePoint.

Personnalisation à l'aide de règles YARA

La prise en charge des règles YARA permet à File Protect d'analyser d'importants volumes de fichiers à la recherche de menaces visant l'entreprise de manière spécifique.

Priorisation simplifiée des réponses à incident

Grâce à l'intégration de FireEye Endpoint Security, chaque objet malveillant peut être analysé plus en détail afin de déterminer si les antivirus en place ont été capables de détecter le malware bloqué par File Protect. Cela permet aux entreprises d'établir efficacement les priorités lors du suivi des réponses à incident, tout en établissant des conventions de nommage communes pour les malwares connus.

Partage des informations sur les malwares

Les produits FireEye s'intègrent à la plateforme Central Management pour bénéficier d'une Threat Intelligence dynamique en temps réel qui les aide à protéger le réseau local. Ces renseignements peuvent être diffusés via le cloud FireEye Dynamic Threat Intelligence (DTI), ce qui permet d'avertir tous les abonnés à l'échelle mondiale des menaces émergentes.

Taux quasi nul de faux positifs, sans aucune règle à définir

Contrairement aux systèmes IPS, File Protect ne nécessite aucun paramétrage. La solution propose des options de déploiement flexibles, notamment une surveillance en mode analyse uniquement ou en mode de mise en quarantaine active. Les entreprises peuvent ainsi connaître la quantité de malwares présents sur les plateformes de stockage en ligne et bloquer toute propagation latérale.

Content Smart Nodes : une protection où il faut, quand il faut

FireEye Content Smart Nodes offre aux RSSI et responsables de contenus la flexibilité d'une solution virtuelle de protection des contenus critiques. Associé à MVX Smart Grid, Content Smart Nodes se déploie en toute transparence à n'importe quelle échelle, là où vous en avez réellement besoin.

Déploiements flexibles

Solution idéale pour tout type d'environnement réseau, File Protect donne aux entreprises la possibilité de choisir entre des appliances FireEye Content Smart Nodes virtuels ou des appliances matérielles traditionnelles déployées sur site.

Tableau 1. FireEye Content Smart Nodes

	FX 2500V
Systèmes d'exploitation pris en charge	Microsoft Windows, MacOS X
Performance	40 000 fichiers par jour
Ports de l'interface réseau	Ether 1, Ether 2
Cœurs de processeur	2
Mémoire	8 Go
Capacité des disques	512 Go
Prise en charge d'hyperviseur	VMware ESXi 6.0 ou ultérieur

Tableau 2. Spécifications techniques

	FX 6500
Performances*	Jusqu'à 70 000 fichiers par jour
Ports de l'interface réseau	4 x 1 GigE BaseT
Port IPMI (panneau arrière)	Inclus
Ports USB (panneau 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
Capacité de stockage	4 disques durs de 2 To, RAID 10, 3,5 pouces, remplaçables
Châssis	Montage en baie 2U, s'intègre en baie 19 pouces
Dimensions du châssis (L x P x H)	438 x 620 x 88,4 mm
Alimentation en courant alternatif	Redondante (1+1) 800 W à 100 - 240 VCA, 9 - 4,5 A, embase secteur IEC 60320-C14, 50 - 60 Hz, remplaçable
Consommation électrique maximale	530 W
Dissipation thermique maximale	1 808 BTU/h
Temps moyen de bon fonctionnement	53 742 h
Poids de l'appliance seule/avec emballage	20,2 kg / 29,8 kg
Certifications de sécurité	IEC 60950 EN 60950-1 UL 60950 CSA/CAN-C22.2
Certifications EMC/EMI	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 réglementaire	Directive RoHS 2011/65/UE, REACH, Directive DEEE 2012/19/UE
Température de fonctionnement	0 ~ 40 °C
Plage d'humidité relative tolérée	10 ~ 95 % à 40 °C, sans condensation
Altitude maximale de fonctionnement	3 000 m

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

FireEye, France
4, place de la Défense,
Paris La Défense Cedex 92974
+33 1 58 58 01 76
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.

FIREEYE™