Présentation de solution

Sécurité à l'unisson

Cyberveille adaptative pour une réaction rapide aux menaces émergentes

Lorsqu'elles tentent de mettre en place une défense efficace contre les menaces émergentes actuelles, les entreprises sont confrontées à de nombreuses difficultés sur le plan opérationnel et de la sécurité. Les attaques ciblées avancées et « jour zéro » utilisent des charges actives encore jamais observées. Les logiciels malveillants (*malware*) polymorphes posent des problèmes similaires. À elles seules, les contre-mesures traditionnelles basées sur les signatures ne sont pas suffisantes pour détecter les charges actives avancées.

Pour combattre efficacement les menaces émergentes, les entreprises ont besoin d'un système de sécurité qui combine des fonctionnalités d'évaluation basées sur le comportement, la réputation et les signatures au niveau du réseau et des terminaux. Et si chacune de ces couches technologiques se montre individuellement performante dans la détection des menaces, il est important qu'elles agissent de manière concertée pour partager les informations, acquérir des connaissances et s'adapter à l'unisson afin de faire face aux menaces en mutation. Les communications manuelles entre les solutions destinées au réseau et aux terminaux sont lentes à s'exécuter et, dans tous les cas, ne sont pas suffisamment rapides pour contrer les menaces actuelles.

McAfee® Threat Intelligence Exchange et McAfee Advanced Threat Defense fonctionnent de concert pour assurer une protection automatisée et adaptative contre les menaces émergentes. Indépendamment du premier point de contact avec un fichier malveillant inconnu, lorsque la dangerosité de ce dernier est attestée, l'environnement connecté tout entier est informé immédiatement. Dès que McAfee Advanced Threat Defense identifie un fichier comme malveillant, McAfee Threat Intelligence Exchange publie cette information via la mise à jour de réputation exécutée par la couche d'échange de données Data Exchange Layer (DXL) à l'intention de tous les systèmes de contre-mesures au sein de l'entreprise. Les terminaux sur lesquels McAfee Threat Intelligence Exchange est installé disposent d'une protection proactive si le même fichier se présente à nouveau. De plus, les passerelles intégrées à McAfee Threat Intelligence Exchange empêcheront le fichier de pénétrer dans l'entreprise. Enfin, lorsque des fichiers à la réputation inconnue sont détectés sur les terminaux dotés de McAfee Threat Intelligence Exchange, ils sont soumis à McAfee Advanced Threat Defense pour déterminer si l'objet est malveillant, ce qui élimine les « angles morts » générés par la distribution hors bande des charges actives.

Principaux avantages

- Endiguement plus rapide de l'attaque grâce à une intervention automatisée et adaptative
- Visibilité, agilité et contrôle plus performants par la collaboration entre les produits pour le réseau et les terminaux
- Réponse aux incidents intelligente grâce à des informations concluantes sur la réputation et les exécutions de fichiers
- Amélioration de la sécurité et réduction du coût total de possession, par une intégration et une implémentation simplifiées

Combler les failles dans la protection

Identification des charges actives furtives

McAfee Threat Intelligence Exchange et McAfee Advanced Threat Defense fonctionnent de manière coordonnée pour analyser les objets suspects, indépendamment du premier point de contact. Lorsque de nouveaux fichiers sont sur le point de s'exécuter, ils sont soumis à une série d'examens de la part des divers composants connectés de cette solution collaborative : règles au niveau des terminaux, réputation au niveau de l'environnement local et mondial, analyse dynamique et analyse statique du code approfondies. Cette approche connectée de l'analyse des menaces permet une identification plus précise des logiciels malveillants furtifs qui passeraient sinon inaperçus.

intel Security

Détection plus performante grâce à une analyse des menaces basée sur le comportement
McAfee Advanced Threat Defense propose une classification fondée sur la réputation, avec des fonctionnalités innovantes de déconstruction des logiciels malveillants, notamment une décompression robuste qui déjoue les techniques de contournement pour exposer le code exécutable d'origine et déterminer le comportement attendu. Ensemble, l'analyse statique du code et l'analyse dynamique offrent une méthode d'évaluation complète et constituent la technologie de détection des menaces avancées la plus puissante du marché.

Visibilité et contrôle, du terminal au réseau
McAfee Advanced Threat Defense peut également recevoir des échantillons de logiciels malveillants collectés au niveau des points d'entrée du réseau par d'autres produits de l'environnement. En retour, ces composants réseau peuvent partager les nouvelles informations glanées sur ces échantillons via McAfee Threat Intelligence Exchange. Ce partage de renseignements et de données de réputation montre bien tous les avantages de l'intégration de la sécurité des terminaux et du réseau, telle qu'elle est assurée par la plate-forme Security Connected de McAfee. De plus, McAfee Threat Intelligence Exchange gère une base de connaissances qui indique l'emplacement d'exécution des derniers objets concernés au sein de l'environnement de terminaux, pour proposer une visibilité probante sur les instances futures.

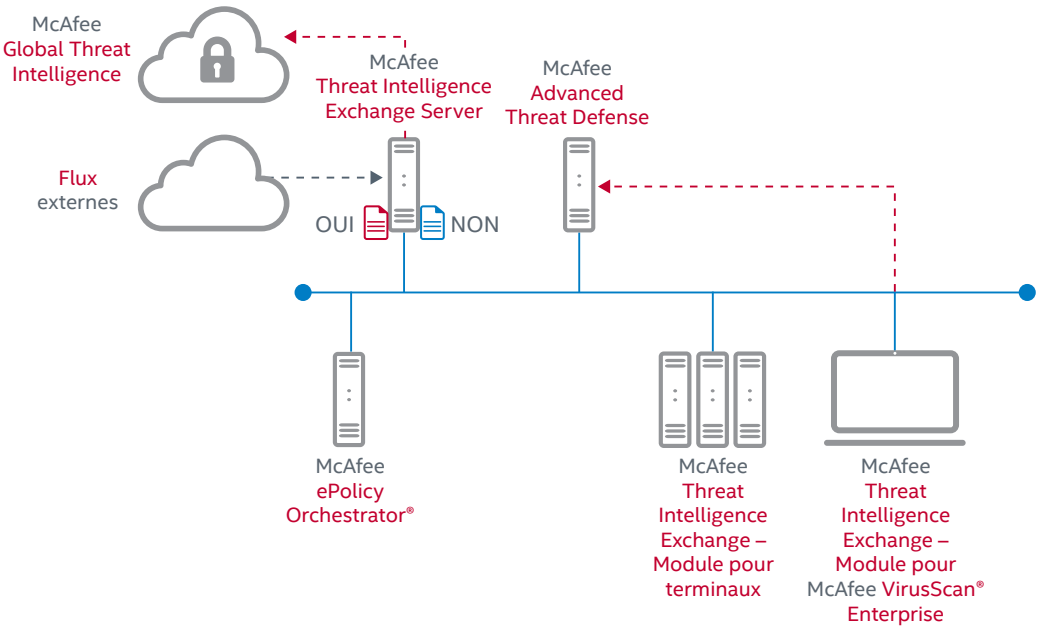

Figure 1. Synthèse des données de réputation et des renseignements sur les menaces issus du cloud, du réseau et des terminaux

Sécurité connectée grâce à la couche McAfee Data Exchange Layer (DXL)
McAfee Threat Intelligence Exchange est la première solution à utiliser la couche Data Exchange Layer de McAfee, une structure de communication bidirectionnelle à la fois légère et ultrarapide, qui permet l'exploitation d'informations de sécurité et la mise en place d'une protection adaptative grâce à l'intégration des produits et au partage des données contextuelles. Les produits connectés par cette couche d'échange de données s'inscrivent auprès de la structure et lui transmettent des informations en toute simplicité, sans nécessiter ni procédures d'intégration complexes à l'aide d'API ni configurations fastidieuses. Cette innovation marque le début d'une nouvelle ère dans le domaine de la sécurité, où tous les composants s'assemblent pour former un système cohésif unique.

Réponse adaptative aux incidents

Une fois que McAfee Advanced Threat Defense analyse et classifie un fichier, les résultats sont envoyés à McAfee Threat Intelligence Exchange. La réputation du nouveau fichier, qu'elle soit bonne ou mauvaise, est communiquée instantanément à tous les systèmes de contre-mesures liés par McAfee Threat Intelligence Exchange dans l'environnement. De cette manière, toute instance future du fichier sera repérée, et tous les composants intégrés à McAfee Threat Intelligence Exchange pourront prendre les mesures requises en fonction des stratégies définies, à savoir autoriser le fichier, le bloquer ou en supprimer la menace. Cette réponse adaptative offre une protection immédiate à l'environnement tout entier — réseau, passerelle et terminaux. L'agilité de la réaction est augmentée, tandis que la durée nécessaire à l'endiguement et à la correction diminuent, sans qu'il faille modifier l'architecture réseau.

Déploiement et gestion aisés

L'intégration entre McAfee Threat Intelligence Exchange et McAfee Advanced Threat Defense s'effectue de façon transparente au niveau de la couche Data Exchange Layer. Conçue comme un cadre ouvert, cette couche permet aux composants de sécurité de rejoindre dynamiquement le réseau McAfee Threat Intelligence Exchange, sans nécessiter l'emploi de nombreuses API ou des configurations de produits complexes. Résultat : le risque d'erreurs est réduit et les tâches manuelles fastidieuses sont éliminées.

CONNECTER
Intégrer facilement les terminaux et équipements réseau pour une collaboration harmonieuse et le partage des informations de sécurité.

PROTÉGER
Utiliser toutes les fonctions connectées pour analyser les objets suspects, indépendamment du premier point de contact.

RÉPONDRE
Étudier les nouvelles instances rencontrées par rapport à l'historique avec une visibilité exceptionnelle, grâce à une base de données centralisée, afin d'exercer un meilleur contrôle sur l'environnement.

S'ADAPTER
Appliquer une réponse automatisée, immédiate et unifiée aux menaces émergentes sur tous les terminaux et équipements réseau.

Figure 2. Intégration transparente au niveau de la couche Data Exchange Layer via le cadre Security Connected

En savoir plus

McAfee Threat Intelligence Exchange et McAfee Advanced Threat Defense constituent deux outils essentiels pour relier des composants de sécurité disparates, protéger votre environnement, réagir face aux incidents de sécurité et appliquer automatiquement les adaptations nécessaires en fonction des menaces émergentes. Offrant un écosystème de sécurité qui intègre fonctionnalités d'analyse des menaces avancées, produits de sécurité du réseau et solutions de protection des terminaux, McAfee fournit la visibilité à l'échelle de l'entreprise et le contexte requis pour contrer les menaces, tout en réduisant les temps de réponse et en simplifiant les procédures de correction.

- **www.mcafee.com/fr/products/threat-intelligence-exchange.aspx**
- **www.mcafee.com/fr/products/advanced-threat-defense.aspx**
- **www.mcafee.com/fr/enterprise/security-connected/index.aspx**

McAfee. Part of Intel Security.
Tour Franklin, La Défense 8
92042 Paris La Défense Cedex
France
+33 1 47 62 56 00 (standard)
www.intelsecurity.com