McAfee Threat Intelligence Exchange

Lutter contre les attaques ciblées via le partage des données de cyberveille

McAfee® Threat Intelligence Exchange permet une détection et une neutralisation adaptatives des menaces en exploitant les données de cyberveille sur l'ensemble de vos solutions de sécurité pour terminaux, passerelles, réseaux et centres de données, et ce en temps réel. La combinaison et le partage instantané d'informations mondiales de cyberveille importées et de données collectées en local permettent aux solutions de sécurité d'agir de concert en échangeant et en tirant parti des renseignements partagés. Ainsi, McAfee Threat Intelligence Exchange ramène le délai entre la détection et la neutralisation de l'attaque de plusieurs jours, semaines ou mois à quelques millisecondes.

Principaux avantages

- La protection adaptative contre les menaces ramène le délai entre l'identification et la neutralisation d'une attaque ciblée avancée de plusieurs jours, semaines ou mois à quelques millisecondes.
- La cyberveille collaborative fournit des informations collectives sur les menaces provenant de sources de données mondiales combinées à des données de cyberveille locales.
- Vous bénéficiez d'une visibilité immédiate sur la présence d'attaques ciblées avancées au sein de l'entreprise.
- Les informations de sécurité pertinentes sont partagées en temps réel entre les solutions de sécurité pour terminaux, passerelles, réseaux et centres de données.

Création d'un écosystème de cyberveille collaboratif

McAfee Threat Intelligence Exchange utilise McAfee Data Exchange Layer pour partager des informations et offrir une sécurité intégrée. Les données combinées issues de plusieurs sources de cyberveille sont instantanément transmises à l'ensemble des solutions de sécurité connectées, y compris les solutions d'éditeurs tiers.

Lorsque les composants de sécurité fonctionnent main dans la main, toute information pertinente pouvant aider à la détection et à la neutralisation des menaces est immédiatement envoyée à l'ensemble des terminaux, passerelles, centres de données, services de cloud et autres points de contrôle de la sécurité de votre environnement. L'intégration extrêmement simple, grâce à McAfee Data Exchange Layer, réduit considérablement les coûts de mise en œuvre et d'exploitation, tout en offrant une efficacité opérationnelle et une sécurité inégalées.

Conçu comme un cadre ouvert, McAfee Data Exchange Layer permet à tous les composants de sécurité, y compris ceux d'éditeurs tiers, de rejoindre dynamiquement l'écosystème McAfee Threat Intelligence Exchange. Le coût total de possession est donc réduit et vous pouvez optimiser davantage la valeur des investissements déjà consentis dans des produits et solutions de sécurité, grâce à des composants désormais capables de communiquer entre eux.

La prévention collaborative et adaptative des menaces constitue une approche inédite de la sécurité informatique d'entreprise, en ce sens qu'elle jette un pont entre vos systèmes disparates et assure une réelle coordination de la sécurité. Pour surmonter les obstacles posés par les limites organisationnelles et budgétaires, les équipes chargées de la sécurité doivent être en mesure d'automatiser le partage des données de cyberveille et d'appliquer des protections et des stratégies de prévention de façon proactive à tous les niveaux du réseau.

intel Security

Principaux avantages (suite)

- Vous disposez des données nécessaires pour prendre des décisions concernant des types de fichiers inconnus en fonction du contexte du terminal (attributs des fichiers, des processus et de l'environnement) et de données de cyberveille collectives.
- McAfee Data Exchange Layer simplifie l'intégration. De plus, l'alliance de solutions Intel Security et tierces, en permettant l'exploitation en temps réel des données de cyberveille, entraîne une réduction des coûts de mise en œuvre et d'exploitation.

En transformant l'infrastructure de sécurité en un système collaboratif, les administrateurs de la sécurité peuvent détecter les menaces, partager des informations sur celles-ci et immuniser leur environnement. McAfee Threat Intelligence Exchange accroît considérablement la résilience et le contrôle dans la lutte contre les attaques émergentes et ciblées.

Adaptation et immunisation contre les menaces

Chaque information partagée, issue des multiples points de contrôle de votre réseau, contribue à l'amélioration des connaissances dans la lutte contre les menaces ciblées. Ces menaces étant conçues pour viser un objectif précis, les entreprises ont besoin d'un système de surveillance local pour identifier les tendances et toute attaque spécifique subie. Combinées aux renseignements de cyberveille mondiaux, les données contextuelles locales ainsi recueillies favorisent une meilleure prise de décision par rapport aux fichiers inconnus et réduisent les délais de protection et de détection.

Tout fichier non identifié détecté sur votre réseau est analysé localement par McAfee Threat Intelligence Exchange. Si la menace est avérée, les mécanismes de défense sont activés en temps réel sur l'ensemble des systèmes. De plus, l'information est conservée de sorte que la menace sera immédiatement détectée si elle se présente sur un autre équipement ou serveur.

Par exemple, si la présence d'un fichier malveillant est décelée au niveau de la passerelle, l'information est transmise à McAfee Threat Intelligence Exchange par le biais de McAfee Data Exchange Layer, atteignant vos terminaux et centres de données en quelques millisecondes. Ces derniers disposent alors de tous les renseignements nécessaires pour une immunisation proactive contre la menace. En outre, si une tentative de compromission d'un terminal est bloquée, révélant ainsi la présence d'un logiciel malveillant, la passerelle et les autres composants de sécurité en sont instantanément avertis, de façon à sécuriser tout le périmètre contre la menace.

Exploitation des données de cyberveille en temps réel

Désormais, vous pouvez combiner les données de cyberveille issues de sources mondiales importées, notamment McAfee Global Threat Intelligence (McAfee GTI), à des informations sur les menaces provenant de tiers et à des indicateurs de compromission partagés tels que les fichiers STIX (Structured Threat Information eXpression). McAfee Global Threat Intelligence recueille des données locales historiques et en temps réel auprès des terminaux, centres de données, passerelles et réseau, mais aussi auprès de la solution de sandboxing McAfee Advanced Threat Defense. Ces données globales et locales combinées sont ensuite rendues exploitables et partagées en temps réel sur l'ensemble de l'écosystème de sécurité.

McAfee Threat Intelligence Exchange offre aux administrateurs la possibilité de personnaliser facilement les données de cyberveille complètes issues de sources mondiales (comme McAfee GTI), de données tierces et de fichiers STIX importés. Ces informations sont ensuite associées à des données de cyberveille locales provenant d'événements historiques et en temps réel survenus sur les terminaux, passerelles, solutions de sandboxing et autres composants de sécurité. Les administrateurs de la sécurité peuvent assembler, remplacer, compléter et ajuster ces informations complètes de façon à personnaliser la protection de leur environnement et de leur organisation (par exemple, listes noires et blanches de fichiers, ou certificats attribués à l'entreprise et utilisés par celle-ci).

Ces données de cyberveille hiérarchisées et optimisées localement offrent une protection immédiate contre les attaques futures. De plus, des métadonnées descriptives sur les objets clés sont conservées et intégrées dans les renseignements collectifs recueillis. Ensemble, les administrateurs et les produits de gestion des événements et des informations de sécurité (SIEM) peuvent exploiter les informations collectées pour identifier instantanément les systèmes présentant un risque élevé de compromission d'après l'activité malveillante antérieure.

Les attaques ciblées avancées, un défi de taille

Conçues pour contrecarrer les mécanismes de détection et pour s'implanter à long terme au sein de l'entreprise afin d'exfiltrer des données de valeur, les attaques ciblées avancées continuent de frapper durement les entreprises. Selon des données récemment publiées dans l'étude de Verizon *2015 Data Breach and Investigations Report* (Rapport d'enquête 2015 sur les compromissions de données), 70 à 90 % des échantillons de logiciels malveillants sont propres à chaque entreprise, faisant de la détection des indicateurs de menaces uniques le plus grand défi de notre époque[1].

Pour plus d'informations, visitez notre site à l'adresse **www.mcafee.com/fr/products/threat-intelligence-exchange.aspx**.

Une protection de premier plan pour les terminaux

Grâce au module McAfee VirusScan® Enterprise dédié, McAfee Threat Intelligence Exchange offre une prévention des menaces innovante pour les terminaux. Au moyen de règles configurables, ce module prend des décisions précises en matière d'exécution de fichiers et tire parti des renseignements combinés issus du contexte local des terminaux (attributs des fichiers, des processus et de l'environnement) et des informations de cyberveille collectives les plus récentes disponibles (prévalence dans l'entreprise, ancienneté, réputation, etc.).

Les administrateurs ont la possibilité de définir des conditions d'exécution d'après leurs exigences spécifiques en personnalisant le module VirusScan Enterprise de McAfee Threat Intelligence Exchange en fonction du niveau de tolérance au risque sur le terminal propre à l'entreprise. Ils peuvent ainsi fixer des conditions très strictes et appliquer une politique de tolérance zéro pour les fichiers inconnus ou encore définir des règles qui empêchent l'accès à tout fichier dont la réputation n'est pas connue et acceptable.

Gestion des terminaux à tout moment et en tout lieu

McAfee Threat Intelligence Exchange offre une prévention des menaces adaptative et une simplicité de gestion de la sécurité avec une couverture mondiale. La solution communique avec les terminaux où qu'ils soient et permet de gérer les stratégies en matière de menaces, les fonctions de détection, les mises à jour de sécurité ainsi que les investigations à distance. Les divers composants de sécurité opèrent comme s'ils ne faisaient qu'un, indépendamment des frontières physiques. Quel que soit leur emplacement, les produits de protection des terminaux, les solutions au niveau de la passerelle et autres produits de sécurité partagent immédiatement les données de sécurité pertinentes, de façon à offrir une prévention des menaces adaptative.

Incapables de distribuer immédiatement les modifications de stratégies, le contenu et les mises à jour logicielles vers les terminaux, les autres solutions de gestion de la sécurité laissent les entreprises exposées à des risques accrus pendant un certain laps de temps. Grâce à McAfee Data Exchange Layer, McAfee Threat Intelligence Exchange est en mesure de maintenir une connexion permanente malgré les obstacles qui se présentent sur le réseau. La solution supprime le délai d'exposition aux risques de manière efficace, ne laissant aucun terminal sur la touche.

Tous les avantages de la collaboration

Requête d'analyse de la réputation en un seul clic

Dès qu'un fichier inconnu est détecté par l'un des composants de sécurité (passerelle, terminal ou réseau) de l'entreprise, sa réputation peut être déterminée aisément en fonction de ses attributs et des données de cyberveille composites en votre possession.

Analyse avancée des menaces
En cas de doutes concernant un fichier, celui-ci peut être transféré automatiquement de McAfee Threat Intelligence Exchange vers McAfee Advanced Threat Defense pour obtenir instantanément des informations supplémentaires sur de nouvelles menaces potentielles. Ensemble, les solutions tirent parti des données analytiques sur les menaces issues de l'analyse de code statique et dynamique pour déterminer la réputation d'un fichier donné. Ce processus est entièrement automatisé, documenté et partagé collectivement via McAfee Data Exchange Layer pour garantir la protection de l'ensemble de l'écosystème de sécurité.

Gestion des événements de sécurité
McAfee Enterprise Security Manager permet de réaliser une analyse plus approfondie lors de l'examen des indicateurs de compromission identifiés par McAfee Threat Intelligence Exchange. L'accès aux informations de sécurité historiques et la possibilité de créer des listes de surveillance automatisées assurent à l'entreprise une sécurité plus performante.

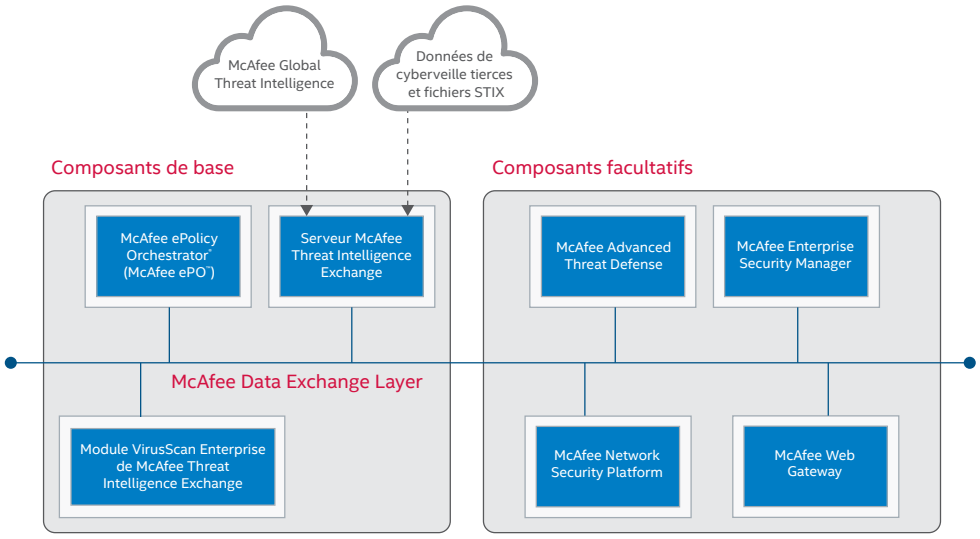

Figure 1. L'intégration extrêmement simple via McAfee Data Exchange Layer réduit les coûts de mise en œuvre et d'exploitation, et assure une efficacité opérationnelle exceptionnelle, tout en marquant un pas en avant dans l'évolution de la plate-forme McAfee Security Connected.

1. http://www.verizonenterprise.com/DBIR/2015/

McAfee. Part of Intel Security.
Tour Pacific
13, Cours Valmy - La Défense 7
92800 Puteaux
France
+33 1 47 62 56 09 (standard)
www.intelsecurity.com

62276ds_threat-intelligence-exchange_0216