Présentation de solution

McAfee Threat Intelligence Exchange, un atout pour la protection des terminaux

Bénéficiez d'une visibilité et d'un contrôle inégalés sur vos terminaux pour une protection de pointe.

Face aux menaces émergentes actuelles, les entreprises sont confrontées à une série de difficultés opérationnelles et de défis en matière de sécurité. En effet, il est de plus en plus difficile de mettre en œuvre une protection efficace contre les attaques de très faible prévalence, une visibilité sans faille sur les exécutions de fichiers et la possibilité d'étudier les menaces identifiées et d'y répondre de façon appropriée. Si les approches classiques de la protection des terminaux de type défense en profondeur multiniveau permettent d'interrompre le cycle de vie des attaques, ou « chaîne de frappe », les composants de sécurité individuels fonctionnent généralement de façon autonome et isolée. Cela engendre une vue fragmentée de la sécurité, offrant une connaissance du contexte limitée, et se traduit par une visibilité incomplète, une protection moins efficace, des temps de réponse accrus et une sollicitation excessive des ressources informatiques déjà lourdement mises à l'épreuve.

Une protection performante contre les menaces émergentes nécessite des solutions de sécurité qui fonctionnent de concert afin d'identifier les attaques furtives et d'y répondre immédiatement sans dépendre d'une mise en corrélation manuelle, de modifications fastidieuses des stratégies ou des mécanismes classiques de mise à jour des terminaux. La clé réside dans la capacité à séparer le bruit de fond permanent des nouveaux fichiers légitimes, des charges actives d'attaques furtives de faible prévalence qui s'exécutent dans l'environnement. Il est également indispensable de pouvoir partager les informations pertinentes obtenues afin de propager les mesures correctives à l'ensemble de l'infrastructure informatique. Pour ce faire, les solutions de sécurité doivent non seulement filtrer les objets légitimes et malveillants connus, mais également évaluer les fichiers exécutables inconnus pour déterminer un score de réputation en fonction du risque global. L'analyse de la réputation d'un fichier permet la mise en œuvre de mesures de neutralisation des menaces appropriées.

McAfee® Threat Intelligence Exchange offre cette forme innovante de protection des terminaux grâce à un système intelligent qui s'adapte et apprend en fonction de chaque nouvelle menace identifiée et neutralise immédiatement les menaces émergentes. Vous pouvez ainsi personnaliser facilement les informations complètes sur les menaces issues de diverses sources de données. Par ailleurs, les systèmes partagent et échangent désormais des renseignements sur les menaces afin de renforcer leur efficacité collective. La personnalisation locale vous permet de collecter, de remplacer et d'affiner les renseignements transmis par les sources d'informations afin d'adapter la protection de votre environnement et de votre entreprise.

Principaux avantages

Protection adaptative instantanée
Neutralisez les menaces émergentes en quelques millisecondes grâce à une infrastructure de sécurité à mise à jour automatique, qui partage instantanément les informations glanées pour une protection plus rapide et efficace.

Le pouvoir de la connaissance
Déterminez précisément la réputation des fichiers grâce à l'analyse de données locales et modiales variées provenant de diverses sources telles que McAfee Global Threat Intelligence ou VirusTotal, et des informations sur la réputation dérivées localement, propres à votre environnement.

Visibilité et contrôle
Bénéficiez d'informations pertinentes sur tous les fichiers exécutables qui tournent dans votre environnement afin de pouvoir identifier l'endroit où les menaces tentent d'ouvrir une brèche, examiner le point d'origine et isoler l'exposition de façon rapide et précise.

intel Security

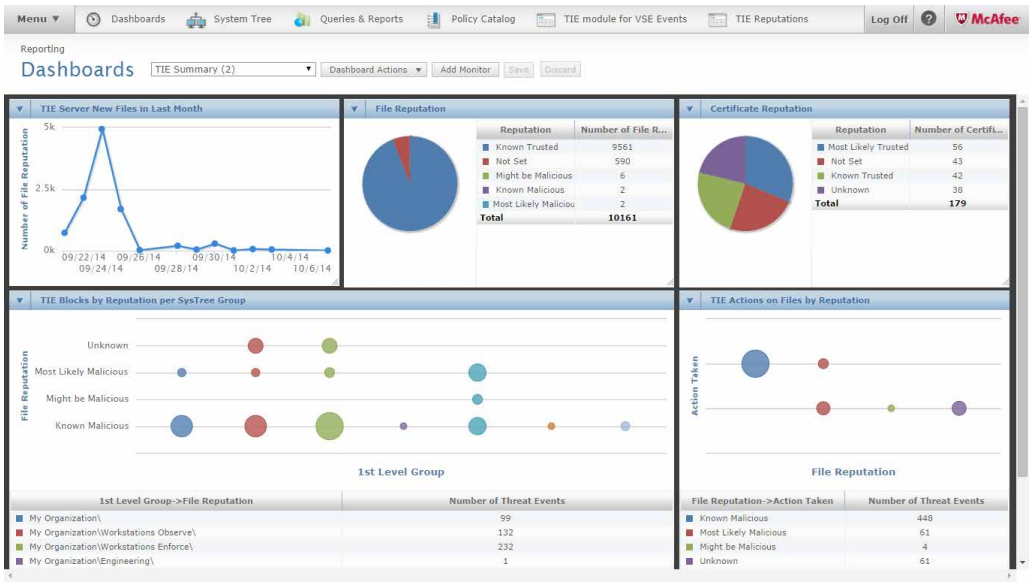

Figure 1. Tableau de bord de McAfee Threat Intelligence Exchange, avec informations directement exploitables

Combler les failles dans la protection

Protection avancée

McAfee Threat Intelligence Exchange offre une nouvelle forme de protection des terminaux qui identifie les risques potentiels dans le bruit de fond des fichiers légitimes et malveillants connus. L'analyse approfondie des fichiers suspects basée sur des données locales, mondiales et propres à l'entreprise permet la prise de décisions intelligentes en matière d'exécution de fichiers visant à détecter et à identifier les attaques de faible prévalence et les logiciels malveillants furtifs. La précision de l'identification est affinée par une logique avancée qui analyse une série de caractéristiques d'exécution et de fichiers, telles que l'emplacement d'exécution du fichier, les métadonnées suspectes ou les tentatives de dissimulation de fichier par compression.

Renseignements complets sur les menaces

McAfee Threat Intelligence Exchange intègre plusieurs sources de données sur les menaces, telles que McAfee Global Threat Intelligence, les résultats d'analyse de fournisseur tiers agrégés par le service VirusTotal ou des informations locales propres à votre environnement pour déterminer avec précision le score de réputation en fonction du risque d'un fichier.

Architecture instantanée

McAfee Threat Intelligence Exchange permet à votre architecture de s'adapter instantanément aux menaces en propageant les informations pertinentes issues de chaque menace identifiée à tous les terminaux via la couche d'échange de données, et cela sans qu'il soit nécessaire d'envoyer un échantillon pour analyse ou d'attendre une mise à jour des signatures antivirus. Il permet également d'automatiser entièrement la réponse adaptative pour obtenir un processus en boucle fermée, ou de l'utiliser de façon interactive pour une protection contre les logiciels malveillants, les fichiers à haut risque ou tout simplement les applications indésirables. Le résultat final réduit considérablement le délai de neutralisation des menaces émergentes et d'application des mesures correctives.

Principaux avantages (suite)

Réduction considérable du coût total de possession
McAfee Threat Intelligence Exchange transforme les assemblages disparates de technologies de sécurité en un système coordonné unique offrant une simplicité accrue, une rapidité instantanée et des connaissances éclairées afin de réduire les coûts d'exploitation, de rationaliser la protection et la réponse aux incidents, et de permettre à l'équipe informatique d'affecter ses ressources aux priorités stratégiques plutôt qu'à des interventions tactiques urgentes.

Exploitation de la couche d'échange de données du cadre d'implémentation Security Connected
McAfee Threat Intelligence Exchange exploite la couche d'échange de données (DXL), une structure de communication bidirectionnelle ultrarapide permettant le partage d'informations et de contexte entre les différentes technologies de sécurité connectées. La structure de la couche d'échange de données est hautement évolutive et offre des transactions à faible latence via une connectivité réseau persistante, permettant ainsi des communications et des actions instantanées sur tous les terminaux comptables. Les produits connectés présents sur la couche d'échange de données s'inscrivent auprès de la structure et publient dessus en toute simplicité, sans nécessiter d'efforts d'intégration complexes basés sur une API ou de 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, indépendamment du fournisseur ou de l'architecture sous-jacente.

Base de connaissance de réponse aux incidents
McAfee Threat Intelligence Exchange stocke les données historiques de réputation et d'exécution des fichiers pour examiner en profondeur les attaques de faible prévalence, les fichiers suspects et les menaces générales, et y répondre de façon appropriée. Il permet d'identifier rapidement la présence d'une menace dans votre environnement, son emplacement et son étendue, ainsi que la première ou la seule instance d'une charge active « patient zéro ».

Contrôle flexible
McAfee Threat Intelligence Exchange permet d'affiner, de remplacer et d'importer facilement les résultats de réputation et les mesures d'identification, vous permettant ainsi de prendre le contrôle intégral de votre environnement. Par exemple, les informations de réputation des fichiers peuvent être classées localement afin de remplacer et d'ajuster immédiatement les stratégies de traitement des fichiers. Les stratégies peuvent être personnalisées pour les groupes et les systèmes afin d'offrir un large spectre de mise en œuvre aligné sur la valeur des actifs. Par ailleurs, les informations pertinentes provenant d'outils tiers peuvent facilement être importées pour agir sur l'ensemble de l'environnement.

Déploiement et gestion simplifiés
L'intégration entre McAfee Threat Intelligence Exchange, le module logiciel McAfee VirusScan® Enterprise et le logiciel McAfee ePolicy Orchestrator® (McAfee ePO™) est entièrement transparente. La couche d'échange de données permet de configurer automatiquement les produits, limitant ainsi le risque d'erreur et éliminant les nombreuses interventions manuelles.

Écosystème Security Connected
McAfee Threat Intelligence Exchange connecte vos composants de sécurité disparates pour partager les informations contextuelles pertinentes et offrir une protection adaptative contre les menaces. Offrant un écosystème Security Connected évolutif intégrant l'analyse des menaces avancées aux solutions de protection du réseau, de la passerelle et des terminaux, McAfee Threat Intelligence Exchange exploite toutes les contre-mesures disponibles pour neutraliser les menaces.

Figure 2. Processus de la solution McAfee Threat Intelligence Exchange

En savoir plus

McAfee Threat Intelligence Exchange assure une surveillance accrue des fichiers inconnus (« fichiers gris ») et un contrôle administratif local des terminaux afin de permettre une prise de décision rapide quant au traitement à leur apporter. Offrant un écosystème de sécurité intégrant 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.

- **http://www.mcafee.com/fr/products/threat-intelligence-exchange.aspx**
- **http://www.mcafee.com/fr/products/virusscan-enterprise.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