McAfee Advanced Threat Defense au service des solutions IPS réseau

Renforcez votre protection contre les logiciels malveillants furtifs.

Principaux avantages

- Détecte et bloque automatiquement les logiciels malveillants avancés et les attaques furtives dissimulées dans le trafic réseau, puis applique les mesures correctives appropriées.
- Renforce la sécurité réseau grâce à une véritable analyse statique du code et à la mise en place d'un environnement sandbox propre à la cible, sans augmentation de la charge de traitement IPS.
- Bloque les menaces en mode Plug-and-Play, sans intervention humaine.

Le système de prévention des intrusions (IPS) basé sur le réseau est le pilier de toute architecture de sécurité d'entreprise. Déployé en mode intrabande parallèlement à une passerelle et à une protection basée sur l'hôte, ce type de système surveille le trafic réseau et le comportement des terminaux au moyen d'une série de techniques permettant de détecter les attaques et de les contrer.

Aujourd'hui, cependant, on note une recrudescence des menaces inconnues de type « jour zéro » parvenant à contourner les mécanismes de défense traditionnels. Furtives, bien camouflées, remarquablement adaptatives et généralement bien ciblées, ces attaques sophistiquées ont beau constituer une minorité du paysage des menaces en perpétuelle évolution, elles n'en sont pas moins redoutables et terriblement coûteuses.

Pour s'en protéger, certaines entreprises intègrent des systèmes d'analyse dynamique à leur infrastructure IPS sous forme d'appliances sandbox hors bande. Celles-ci lancent les exécutables suspects dans un environnement virtuel sécurisé et examinent leur comportement d'exécution dans le but de déceler toute intention malveillante. Malheureusement, l'avantage que pourrait présenter cette méthode en termes de précision de détection est très souvent réduit à néant par une intégration insatisfaisante et des procédures d'intervention manuelles.

La plupart des appliances sandbox, par exemple, alertent uniquement les analystes en sécurité lorsqu'une nouvelle attaque a été détectée. Ces derniers doivent alors créer manuellement de nouvelles règles de blocage à destination du pare-feu et du système IPS, puis seulement commencer à identifier et à corriger tous les terminaux contaminés pendant l'analyse en environnement restreint (sandbox) hors bande. Parmi les autres handicaps les plus courants des solutions existantes, on relève les suivants :

- Forte augmentation des coûts due à l'installation d'une appliance sandbox par capteur IPS
- Dépendance par rapport à un environnement d'exécution virtuel générique susceptible de négliger certains comportements d'attaque propres à la cible
- Recours à la seule analyse dynamique, rendant l'environnement sandbox vulnérable à diverses stratégies malveillantes qui détectent les environnements sécurisés et retardent l'exécution des comportements révélateurs

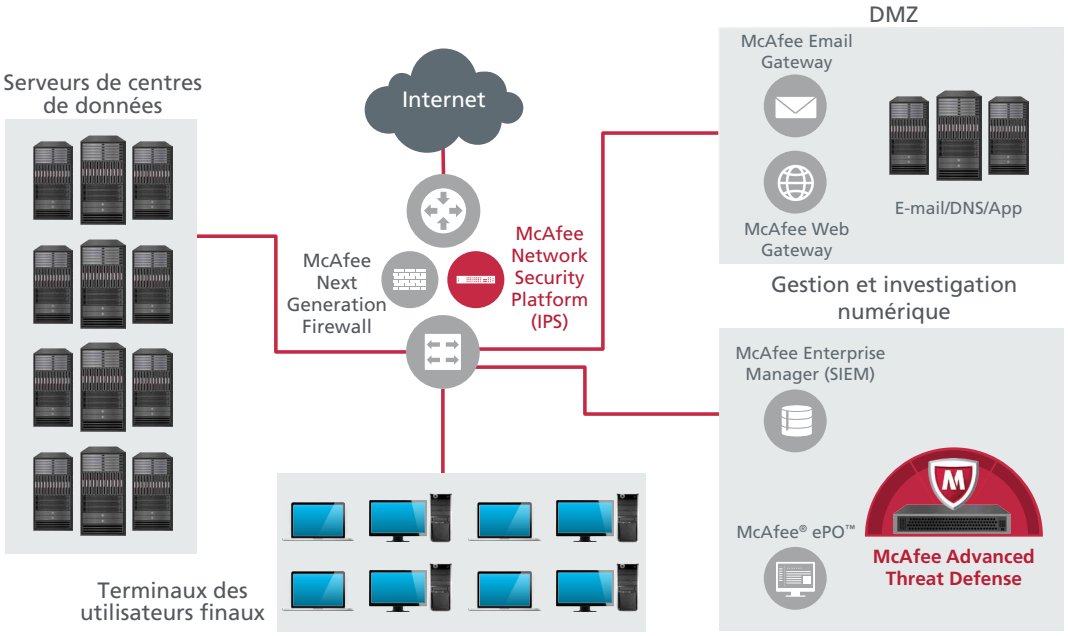
L'approche Security Connected : l'intégration entre IPS et sandbox

McAfee apporte désormais la solution à tous ces problèmes en proposant une architecture qui intègre McAfee Network Security Platform, une sonde IPS sophistiquée hautes performances, à McAfee Advanced Threat Defense, le système de détection de logiciels malveillants avancés le plus puissant et le plus complet du marché. McAfee Network Security Platform inspecte le trafic intrabande et bloque les menaces grâce à un ensemble de technologies de détection des logiciels malveillants, optimisées pour une exécution en temps réel. La solution McAfee Advanced Threat Defense exécute une série d'examens plus approfondis mais plus gourmands en ressources, qui s'appuient notamment sur la mise en place d'un environnement sandbox propre à la cible et la réalisation d'une véritable analyse statique du code. Ensemble, ces deux systèmes détectent et bloquent les menaces avancées furtives et encore inconnues. Pour une solution complète de bout en bout, il est également possible d'ajouter McAfee Real Time afin de rapidement identifier et corriger tout système contaminé par des logiciels malveillants avancés.

- *Détection* — Des technologies d'analyse innovantes fonctionnent de concert pour détecter les menaces sophistiquées de façon précise et rapide, sur plusieurs protocoles.
- *Blocage* — Étroitement intégrés, les produits de sécurité McAfee bloquent instantanément les tentatives d'infiltration et isolent les terminaux infectés.
- *Correction* — La solution McAfee balaie automatiquement tout l'environnement à la recherche de tentatives d'infiltration et applique les mesures correctives nécessaires aux terminaux touchés.

Déploiement centralisé

Évolutivité et coût de possession moindre



Reposant sur l'approche d'intégration de la sécurité d'entreprise Security Connected, la solution McAfee Advanced Threat Defense pour IPS réseau offre un large éventail d'avantages opérationnels et défensifs uniques sur le marché :

- *Blocage Plug-and-Play des menaces* — Toute attaque détectée par McAfee Advanced Threat Defense est automatiquement bloquée par McAfee Network Security Platform sans qu'aucune intervention humaine ne soit nécessaire, ce qui permet de gagner en rapidité.
- *Intégration des rapports et des workflows* — Les rapports générés par McAfee Advanced Threat Defense sont automatiquement intégrés aux workflows de McAfee Network Security Platform, éliminant ainsi le besoin de basculer d'un écran à l'autre au cours des investigations.
- *Visibilité des terminaux* — McAfee Advanced Threat Defense peut accéder aux données des terminaux stockées sur McAfee Network Security Platform et les utiliser pour améliorer la vitesse et la précision de la détection des menaces.

Prévention des intrusions : McAfee Network Security Platform

McAfee Network Security Platform est une gamme d'appliances intégrées de prévention des intrusions (IPS) qui identifient et bloquent les menaces sophistiquées sur le réseau, notamment les logiciels malveillants avancés, les menaces « jour zéro », les attaques par déni de service et les réseaux de robots (botnets). Alliant une architecture d'inspection à un seul passage ultraperformante à un matériel spécialisé à la hauteur des exigences des opérateurs de télécommunication, McAfee Network Security Platform atteint des vitesses d'analyse de 40 Gbit/s avec une seule appliance et garantit une efficacité et une précision exceptionnelles, quels que soient les paramètres de sécurité. Ses fonctionnalités d'analyse embarquées incluent des signatures personnalisées, des analyses complètes des protocoles, des analyses de réputation, des analyses approfondies des fichiers avec émulation et détection du code JavaScript, ainsi qu'une mise en corrélation du comportement des menaces et de l'utilisation des applications basée sur une visibilité au niveau de la couche 7 sur plus de 1 500 applications et protocoles.

Une combinaison parfaite

- Valorisez vos investissements de sécurité existants.
- Limitez le remaniement de votre architecture réseau.
- Élargissez et automatisez votre protection.
- Réduisez au maximum les actions correctives et les investigations grâce à un blocage en ligne fiable.
- Simplifiez les workflows grâce à l'interface McAfee Network Security Platform.

Security Connected

La plate-forme Security Connected de McAfee offre un cadre unifié à des centaines de produits et services, permettant ainsi aux nombreux partenaires d'échanger leurs connaissances, de partager des données contextuelles en temps réel et de collaborer pour assurer la sécurité des informations et des réseaux. Grâce aux concepts novateurs, aux processus optimisés et aux recommandations pratiques de cette plate-forme, toute entreprise est désormais en mesure de réduire les risques auxquels elle est exposée ainsi que son temps de réponse, mais aussi d'alléger les frais généraux et les coûts d'exploitation de son personnel.

Toutefois, la fonctionnalité la plus puissante de McAfee Network Security Platform est sans doute sa capacité à intégrer et à exploiter les données et le potentiel des autres solutions de sécurité McAfee. L'intégration avec les solutions suivantes est particulièrement importante :

- Real Time for McAfee® ePolicy Orchestrator® (McAfee ePO) fournit une visibilité en temps réel sur les terminaux et les fonctionnalités de gestion nécessaires à l'isolation et à l'éradication des attaques.
- McAfee Enterprise Security Manager, une solution révolutionnaire de gestion des événements et des informations de sécurité (SIEM) fournit un aperçu en temps réel de l'environnement informatique interne, lui-même mis en corrélation avec le contexte extérieur. La base de données optimisée de McAfee Enterprise Security Manager collecte des milliards d'entrées de journal et les compare à d'autres flux de données pertinents, ce qui permet d'accéder et d'exploiter rapidement une mine de données de sécurité collectées sur plusieurs années. Non seulement elle calcule les lignes de base de tous les flux de données entrants afin d'identifier les anomalies et les menaces potentielles avant même qu'elles ne se développent, mais elle simplifie également la gestion de la conformité grâce à des centaines de tableaux de bord prédéfinis et des rapports spécifiques.
- McAfee Advanced Threat Defense est le composant de détection des logiciels malveillants de cette solution.

Environnement sandbox : McAfee Advanced Threat Defense

McAfee Advanced Threat Defense est une solution multiniveau de détection des logiciels malveillants qui empile une série évolutive de moteurs d'inspection et de fonctionnalités analytiques, suivant une séquence progressive exigeant une puissance de calcul croissante. Cette approche unique et efficace allie une détection de très haute précision à une grande fiabilité et à un débit extrêmement élevé. Les fonctionnalités analytiques embarquées de McAfee Advanced Threat Defense présentent les caractéristiques suivantes :

- Détection basée sur les signatures des virus, vers, logiciels espions (spyware), robots (bots), chevaux de Troie, attaques par débordement de mémoire tampon et attaques combinées, à l'aide d'une base de connaissances créée et gérée par McAfee Labs dont le contenu avoisine actuellement les 150 millions de signatures.
- Détection basée sur la réputation utilisant le réseau McAfee Global Threat Intelligence pour déceler les nouvelles menaces.
- Émulation et analyse statique en temps réel permettant de détecter rapidement les logiciels malveillants et les menaces « jour zéro » non identifiables au moyen des techniques basées sur les signatures et la réputation.
- Analyse statique complète qui reconstitue la logique du code pour évaluer l'état des attributs et des jeux d'instruction, et effectuer un examen approfondi du code source sans l'exécuter. Ouvrant tous les types de fichiers compressés afin d'effectuer une analyse minutieuse et une classification des logiciels malveillants qu'ils contiennent, les fonctionnalités de décompression permettent aux entreprises de mieux comprendre les logiciels malveillants auxquels elles ont affaire et leur impact sur les activités. L'analyse statique complète du code offre un aperçu critique des comportements dépendant de la saisie et des chemins d'exécution masqués ou différés qui ne s'exécutent généralement pas pendant l'analyse dynamique et sont négligés par les solutions d'isolement en sandbox moins exhaustives.
- Analyse dynamique dans un environnement restreint de type sandbox qui exécute le code du fichier suspect dans un environnement virtuel en temps réel et en observe le comportement. McAfee Advanced Threat Defense est une solution sandbox unique en son genre dans la mesure où elle reconstitue l'environnement de l'hôte cible à l'aide de machines virtuelles en temps réel, en se basant sur des requêtes envoyées au logiciel McAfee ePO. Le fait de pouvoir analyser le comportement d'un fichier dans les conditions exactes de l'hôte ciblé permet de générer des résultats précis de manière rapide et efficace, révélant ainsi les comportements anormaux qui n'auraient peut-être pas été décelés dans un environnement plus générique. Étant donné que la plupart des attaques avancées sont conçues pour échapper à la détection pendant une exécution en environnement sandbox, McAfee Advanced Threat Defense inclut un éventail de techniques innovantes garantissant l'exécution du code pendant l'analyse dynamique.

Ces techniques fonctionnent de concert pour identifier efficacement plusieurs types de logiciels malveillants connus et inconnus. La combinaison d'analyses statiques et dynamiques permet donc de déceler les logiciels malveillants avancés et dissimulés qui échappent en principe à la vigilance des moteurs d'analyse plus légers.

Faciles à configurer, les appliances McAfee Advanced Threat Defense effectuent uniquement les analyses qui n'ont pas été exécutées sur les sondes IPS en aval, éliminant ainsi tous les problèmes de dégradation des performances dus aux inspections redondantes. Grâce à leur évolutivité, elles sont en outre capables de gérer jusqu'à 250 000 objets par jour, ce qui permet à un seul système de détection des logiciels malveillants avancés de prendre en charge plusieurs sondes McAfee Network Security Platform. McAfee Network Security Platform et les appliances McAfee Advanced Threat Defense bénéficient par ailleurs d'une gestion centralisée via une interface web fournie par McAfee Network Security Manager.

Une solution en boucle fermée efficace pour la prévention des menaces avancées

La combinaison des logiciels McAfee Network Security Platform et McAfee Advanced Threat Defense offre une protection IPS réseau extraordinairement performante, doublée de capacités exceptionnellement efficaces en matière de détection et d'éradication des logiciels malveillants avancés. Cette solution en boucle fermée automatisée détecte les attaques sophistiquées, les bloque et corrige les systèmes hôtes contaminés, le tout sans aucune intervention manuelle des opérateurs réseau ou des analystes en sécurité généralement débordés.

Pour plus d'informations sur les solutions McAfee de protection des réseaux contre les menaces avancées furtives, contactez votre représentant McAfee ou rendez-vous sur www.mcafee.com/fr/products/advanced-threat-defense.aspx.

McAfee S.A.S.
Tour Franklin, La Défense 8
92042 Paris La Défense Cedex
France
+33 1 47 62 56 00 (standard)
www.mcafee.com/fr

61051brf_atd-network-ips_0514_fnl_ETMG