McAfee Network Security Platform

Une plate-forme de protection contre les menaces complète, intelligente et avancée

McAfee® Network Security Platform est un système de détection et de prévention des intrusions (IDPS) de nouvelle génération qui identifie et bloque les logiciels malveillants sophistiqués sur le réseau. Grâce à diverses techniques avancées de détection et d'émulation, il va au-delà de la simple mise en correspondance de modèles pour offrir une protection très performante contre les attaques furtives. Pour répondre aux besoins des réseaux les plus exigeants, cette plate-forme prend en charge des débits supérieurs à 30 Gbit/s avec une seule appliance (et jusqu'à 100 Gbit/s en cas de pile). La gamme de solutions intégrées de McAfee optimise les opérations de sécurité en combinant la cyberveille en temps réel de McAfee® Global Threat Intelligence avec des données contextuelles riches sur les utilisateurs, les équipements et les applications. Cette approche permet une réponse rapide et précise aux attaques propagées par le réseau.

Principaux avantages

- Détection et blocage rapides des menaces pour une protection sans faille des applications et des données
- Solution évolutive ultraperformante pour les environnements dynamiques
- Gestion centralisée assurant visibilité et contrôle
- Détection avancée avec analyse antimalware sans signatures
- Déchiffrement SSL à l'entrée et en sortie pour l'inspection du trafic web

Protection contre les menaces furtives actuelles

La numérisation a transformé le paysage de la sécurité. Le cloud, la mobilité et l'IoT offrent une connectivité encore inégalée sans véritable périmètre à protéger. En très peu de temps, la quantité et la gravité des risques ont connu une croissance exponentielle. De nombreuses entreprises se concentrent désormais sur la protection des données, pour laquelle une stratégie efficace de sécurité des réseaux est essentielle. Les réseaux sont aujourd'hui confrontés à des attaques furtives avancées capables de contourner les méthodes de détection traditionnelles. De ce fait, les applications et les données sont exposées à des violations de sécurité et à des périodes d'indisponibilité qui paralysent l'entreprise. Malheureusement, la plupart des entreprises ne disposent pas des ressources financières et opérationnelles nécessaires pour implémenter et gérer la combinaison d'outils et de technologies indispensable à une défense adéquate.

McAfee Network Security Platform combine des fonctionnalités intelligentes de prévention des menaces et une gestion intuitive de la sécurité afin de garantir une détection plus précise et d'optimiser les opérations de sécurité. Aucune technologie de détection des logiciels

Gardez le contact

malveillants ne peut, à elle seule, refouler toutes les attaques. C'est pourquoi McAfee Network Security Platform intègre en couches plusieurs moteurs de détection, avec et sans signatures, pour empêcher les logiciels malveillants de mettre à mal le réseau. Grâce à une combinaison de technologies avancées telles que l'analyse complète des protocoles, l'analyse des menaces basée sur la réputation et l'analyse du comportement, il effectue une inspection approfondie du trafic réseau. La solution peut ainsi détecter et prévenir les rappels de logiciels malveillants, les attaques par déni de service (DoS), les menaces « jour zéro » et d'autres menaces avancées.

Sécurité intégrée

McAfee Network Security Platform s'intègre avec McAfee® Advanced Threat Defense, qui combine analyse statique de code, analyse dynamique (sandboxing) et apprentissage automatique pour détecter les menaces « jour zéro », notamment les ransomwares ou les attaques utilisant des techniques de contournement. McAfee Network Security Platform tire également parti du service d'évaluation de la réputation des fichiers de McAfee Global Threat Intelligence et assure une intégration en temps réel avec McAfee® ePolicy Orchestrator® et McAfee® Enterprise Security Manager pour une corrélation instantanée des événements réseau sur l'ensemble des sources pertinentes. La solution combinée intègre des informations sur les équipements, sur les utilisateurs et sur le niveau de sécurité des terminaux, des évaluations des vulnérabilités ainsi qu'une mine d'autres renseignements qui aident les entreprises à mieux appréhender la gravité des menaces et leurs facteurs de risques métier.

Performances et disponibilité

McAfee Network Security Platform offre un haut niveau de sécurité sans sacrifier les performances. La solution allie une architecture d'inspection à un seul passage, basée sur les protocoles, à un matériel spécialisé à la hauteur des exigences des opérateurs de télécommunication. Elle permet ainsi d'inspecter les données à plus de 100 Gbit/s. Son architecture efficace préserve les performances, quels que soient les paramètres de sécurité, alors que les autres solutions IPS peuvent entraîner une réduction de débit allant jusqu'à 50 % lors de l'utilisation de stratégies où la sécurité est prioritaire sur les performances.

McAfee Network Security Platform offre également des modes actif-actif et actif-passif avec reprise automatique dynamique, vous permettant de respecter les SLA de haute disponibilité tout en évitant les goulets d'étranglement des appliances plus lentes ou des solutions autonomes surchargées.

Plate-forme matérielle évolutive et protection de l'investissement

Les appliances des séries NS7500 et NS9500 de McAfee offrent aux clients la flexibilité nécessaire pour acheter ce dont ils ont besoin dans l'immédiat, puis faire évoluer facilement leur débit via une licence logicielle en fonction de leurs besoins. Il est également possible d'empiler plusieurs appliances de la série NS9500 de McAfee pour gagner en capacité.

Principaux avantages (suite)

- Protection haute disponibilité et reprise après sinistre
- Appliances virtuelles également disponibles
- Intégration avec la gamme de solutions McAfee pour la sécurité des équipements jusqu'au cloud

Visibilité et contrôle

Prenez des décisions éclairées concernant les applications et protocoles de votre réseau. McAfee Network Security Platform a été la première solution IDPS à allier la prévention des menaces avancées et la reconnaissance des applications au sein d'un moteur d'exécution de décisions de sécurité. La solution met en corrélation les activités liées aux menaces et l'utilisation des applications, notamment une visibilité au niveau de la couche 7 sur plus de 2 000 applications et protocoles. Vous pouvez ainsi prendre des décisions avisées concernant les applications que vous autorisez sur votre réseau.

En plus de l'identification des applications, McAfee Network Security Platform offre une visibilité sur les utilisateurs et sur les équipements. En diagnostiquant les comportements anormaux sur le réseau, il détecte les hôtes et les utilisateurs à risque, dont les réseaux de robots (botnets) actifs, et les définit comme prioritaires.

Gestion intelligente et évolutive de la sécurité

Rentabilisez de façon optimale votre investissement en sécurité grâce à la gestion intelligente de la sécurité réseau. McAfee Network Security Manager propose une gestion web évolutive, qui peut couvrir de deux à plusieurs centaines d'appliances de sécurité du réseau. La solution procure en outre des workflows de notification progressive qui aiguillent les administrateurs vers les alertes qui nécessitent leur attention. À cela s'ajoutent des tableaux de bord de sécurité conviviaux qui priorisent automatiquement les événements en fonction de la pertinence et de la gravité des alertes.

Fonctionnalités supplémentaires

Prévention des menaces avancées

- Le déchiffrement SSL en entrée prend en charge les algorithmes de chiffrement DH (Diffie-Hellman) et ECDH (Elliptic-Curve Diffie-Hellman) grâce à une solution de clé partagée avec agent, sans impact sur les performances des sondes — en attente de brevet pour la série NS.
- Déchiffrement SSL en sortie (série NS)
- Moteur d'émulation McAfee® Gateway Anti-Malware
- Moteur d'émulation pour code JavaScript incorporé dans les PDF
- Moteur d'analyse comportementale pour Adobe Flash
- Moteur d'inspection approfondie des fichiers Microsoft Office
- Fonctions avancées de protection contre les contournements
- Analyse dans le cloud et analyse de la réputation sur mobiles

Protection contre les rappels des réseaux de robots et logiciels malveillants

- Détection des rappels « fast-flux » de domaines DNS/DGA
- Redirection vers un serveur DNS sinkhole
- Détection heuristique des robots
- Corrélation d'attaques multiples
- Base de données de contrôles et de commandes

Prévention avancée des intrusions

- Défragmentation IP et réassemblage des flux TCP
- Signatures McAfee, définies par l'utilisateur et à code source libre

- Prise en charge native des signatures Snort (série NS)
- Listes d'autorisation et de blocage optimisées avec prise en charge du format STIX (Structured Threat Information eXpression) (série NS de McAfee)
- Mise en quarantaine de l'hôte et limitation du débit
- Inspection des environnements virtuels
- Intégration avec McAfee Advanced Threat Defense
- Prise en charge de la décompression des réponses HTTP

Prévention des attaques par déni de service (DoS) et par déni de service distribué (DDoS)

- Détection heuristique et basée sur des seuils
- Limitation des connexions basée sur l'hôte
- Détection basée sur les profils, avec autoapprentissage

McAfee Global Threat Intelligence

- Réputation des fichiers, des adresses IP et des URL
- Réputation des applications et des protocoles
- Géolocalisation
- Élaboration de listes d'autorisation basées sur les catégories McAfee Global Threat Intelligence

Haute disponibilité

- Modes actif-actif et actif-passif avec capacité de basculement avec état
- Fonction externe de prévention de défaillance fail-open (mode actif)
- Fonction intégrée de prévention de défaillance fail-open

Prise en charge des protocoles de tunnellisation

- IPv6
- Tunnels IPv4 dans IPv4, IPv4 dans IPv6, IPv6 dans IPv4 et IPv6 dans IPV6
- MPLS
- GRE
- Double marquage VLAN QinQ

McAfee® Network Security Manager

- Gestion multiniveau couvrant jusqu'à 1 000 sondes
- Authentification des utilisateurs (RADIUS et LDAP)
- Basculement et restauration automatiques
- Reprise après sinistre des données de configuration critiques
- Gestion hiérarchique centralisée des stratégies
- Tableau de bord relatif à la mémoire détaillant l'utilisation de la mémoire par équipement

En savoir plus

Pour en savoir plus et obtenir des informations sur les options des appliances physiques, consultez la fiche de spécifications de McAfee Network Security Platform.

Consultez ce livre blanc (en anglais) pour en savoir plus sur les caractéristiques indispensables d'un système de détection et de prévention des intrusions (IDPS).

11-13 Cours Valmy - La Défense 7
92800 Puteaux, France
+33 1 4762 5600
www.mcafee.com/fr