Gamme McAfee Endpoint Threat Defense and Response

Détection des logiciels malveillants de type « jour zéro », sécurisation du « patient zéro » et neutralisation des attaques avancées

La sophistication croissante des cybermenaces demande une nouvelle génération de produits de protection des terminaux. Les menaces en constante progression et le risque accru de vulnérabilités inconnues contraignent les entreprises à déployer des solutions de sécurité redondantes et non intégrées qui offrent une visibilité limitée et deviennent de plus en plus complexes à gérer. Intel Security résout ce problème grâce à McAfee® Endpoint Threat Defense et McAfee Endpoint Threat Defense and Response. Les deux solutions s'appuient sur une analyse statique et comportementale et sur des informations de cyberveille synthétisées pour prévenir, détecter, corriger et adapter la protection afin de lutter contre les menaces émergentes. Les composants de sécurité unifiés agissent de concert grâce à une approche ouverte et intégrée qui allie une visibilité et une cyberveille partagées à des workflows simplifiés. L'approche de sécurité connectée et les investigations numériques exploitables offrent une infrastructure sécurisée capable d'identifier les menaces de façon rapide et précise et de garder l'avantage sur les pirates potentiels.

Principaux avantages

- Détection, protection et correction avec adaptation proactive des défenses contre les logiciels malveillants de type « jour zéro », des logiciels gris (greyware) et du ransomware
- Protection plus efficace grâce à des réputations dynamiques, à l'analyse comportementale et à l'apprentissage automatique
- Limitation de l'impact sur les utilisateurs et les applications d'entreprise approuvées grâce à une protection renforcée
- Réaction et correction plus rapides d'un nombre accru de menaces grâce à une cyberveille partagée dans tout votre écosystème de sécurité
- Optimisation des procédures d'investigation des incidents et d'application de mesures correctives grâce à des workflows unifiés et à une console de gestion unique : McAfee® ePolicy Orchestrator® (McAfee ePO™)

Neutralisation des logiciels malveillants de type « jour zéro », des logiciels « gris » (greyware) et du ransomware

Gardez une longueur d'avance sur les menaces émergentes grâce à une analyse statique et dynamique des menaces qui tire parti de fonctions avancées d'analyse de la réputation et des comportements pour détecter les exploits potentiels. Exploitez les informations synthétisées de McAfee Threat Intelligence Exchange pour bloquer et confiner immédiatement les menaces et mettre instantanément à jour la réputation des menaces pour prévenir les attaques futures.

McAfee Endpoint Threat Defense et McAfee Endpoint Threat Defense and Response neutralisent les logiciels malveillants de type « jour zéro » en identifiant les similitudes entre les comportements malveillants décelés et tout l'éventail de modèles de menaces Real Protect via une recherche dans le cloud (centres de données hébergés aux États-Unis). Cette technique de classification comportementale permet de mettre au jour des menaces actives susceptibles d'avoir échappé à d'autres logiciels de sécurité. Elle fournit une cyberveille exploitable via le logiciel McAfee ePolicy Orchestrator en vue de l'identification

des menaces de type « jour zéro » et de l'application de mesures correctives en temps réel. La classification basée sur les comportements évolue automatiquement grâce à l'apprentissage automatique dynamique et offre ainsi une protection et une efficacité maximales tout en limitant la fenêtre d'exposition.

Diminution du nombre d'événements et neutralisation accélérée des menaces

Concentrez-vous sur les menaces véritablement importantes en réduisant le nombre d'événements de sécurité, en identifiant automatiquement un nombre accru de menaces, en partageant des informations de cyberveille et en utilisant les alertes proactives pour définir des réponses automatiques. Simplifiez les procédures d'investigation et de neutralisation des menaces grâce à des workflows simplifiés capables d'analyser plus rapidement les événements et étendez la sécurité tout en renforçant la protection à l'échelle de l'entreprise.

Des composants connectés partagent automatiquement les informations de sécurité pertinentes via McAfee Data Exchange Layer. McAfee Threat Intelligence Exchange permet de synthétiser une cyberveille très complète sur les menaces dans tout votre écosystème, y compris McAfee Global Threat Intelligence et d'autres sources externes, puis de partager immédiatement ces informations afin d'adapter automatiquement la protection.

Sécurisation du terminal « patient zéro »

Détectez les logiciels de type « jour zéro » et empêchez-les d'apporter des modifications aux terminaux. Le confinement dynamique d'applications surveille le comportement des logiciels « gris » (greyware) et bloque les modifications d'origine malveillante afin d'arrêter les exploits avant qu'ils puissent s'exécuter. Sécurisez les terminaux connectés ou non au réseau et isolez les comportements malveillants grâce à une protection invisible pour les utilisateurs.

Opérationnalisation des processus de sécurité à des fins d'évolutivité et d'adaptation

L'application de stratégies, l'investigation des incidents et la mise en œuvre de mesures correctives sont rationalisées grâce à McAfee ePO, une console de gestion centralisée qui offre une visibilité sur tous les systèmes afin que vous puissiez évaluer rapidement l'état de sécurité des terminaux et activer la protection en temps réel. Réduisez les tâches de surveillance, de recherche et de réponse grâce à des workflows unifiés et à des mesures correctives applicables en un clic sur un terminal unique ou dans toute l'infrastructure. Avec McAfee Endpoint Threat Defense et McAfee Endpoint Threat Defense and Response, tirez parti de l'apprentissage automatique pour mettre à jour les modèles de classification basée sur les comportements et partager instantanément la cyberveille avec tous les composants de sécurité afin qu'ils puissent agir de façon conjointe et unifiée contre les menaces émergentes. Prévenez les attaques futures et exploitez les réponses préconfigurées pour confiner les menaces potentielles. Vous pourrez dès lors réaffecter votre personnel à d'autres tâches de gestion de la sécurité plus stratégiques.

Détection, priorisation et neutralisation des attaques avancées

McAfee Endpoint Threat Defense and Response permet de déterminer l'origine, l'ampleur et l'impact d'une attaque. Il s'appuie sur la technologie McAfee Active Response pour offrir une visibilité sur les événements actuels et historiques des terminaux de votre infrastructure. Les indicateurs d'attaque sont identifiés et priorisés avec un contexte très étoffé pour accélérer la réponse.

Vous pouvez traquer les menaces avec précision, vitesse et agilité et neutraliser celles qui cherchent à se propager dans votre environnement, celles qui attendent dans l'ombre ou celles qui ont effacé leurs traces pour échapper à la détection. Une visibilité et un contrôle basés sur les connaissances peuvent déterminer l'endroit où les menaces tentent de s'infiltrer et permettent à vos intervenants de confiner et de neutraliser immédiatement ces menaces, réduisant ainsi la fenêtre d'exposition à quelques minutes ou secondes au lieu de plusieurs mois.

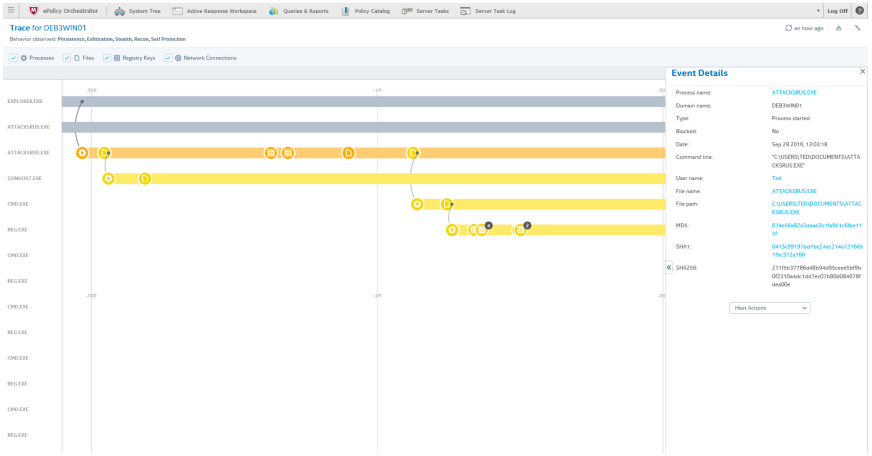

Figure 1. L'environnement de défense contre les menaces établit l'origine et le comportement des incidents suspects pour accélérer les interventions sur incidents.

Fonctionnalités de la gamme McAfee Endpoint Threat Defense and Response

Composant	Avantage	Avantages pour les clients	Différenciation	McAfee Endpoint Threat Defense	McAfee Endpoint Threat Defense and Response
Confinement[1] dynamique d'applications	Sécurisation du terminal « patient zéro » par le blocage des modifications que les logiciels « gris » (greyware) tentent d'apporter aux terminaux connectés ou non au réseau	• Analyse des menaces potentielles sans sacrifier le terminal « patient zéro » • Protection optimisée, sans impact sur les utilisateurs ou les applications approuvées • Réduction du délai entre la détection et le confinement avec intervention manuelle minimale • Sécurisation du terminal « patient zéro » et isolement du réseau pour le mettre à l'abri des infections	• Intégration à l'infrastructure Intel Security pour offrir une protection et une efficacité optimales • Fonctionnalité constamment active, avec ou sans connexion Internet, et qui ne nécessite aucune analyse ou information externe • Fonctionnement transparent pour l'utilisateur • Mode d'observation offrant une visibilité instantanée sur les comportements d'exploits potentiels dans l'environnement	√	√
Real Protect	Classification des comportements basée sur l'apprentissage automatique pour bloquer les logiciels malveillants « jour zéro » avant qu'ils ne s'exécutent et interrompre directement l'exécution des menaces qui avaient précédemment échappé à la détection	• Détection plus efficace d'un nombre accru de logiciels malveillants, y compris ceux difficiles à identifier, comme les logiciels de demande de rançon (ransomware) • Identification, analyse et neutralisation automatiques des menaces, sans intervention manuelle • Adaptation des défenses à l'aide de la classification automatisée et d'une infrastructure de sécurité connectée	• Analyse comportementale statique et dynamique pour une protection plus efficace qu'une approche mononiveau • Interception des logiciels malveillants qu'il est uniquement possible de détecter à l'aide d'une analyse dynamique des comportements • Intégration étroite permettant de partager les mises à jour de réputation en temps réel et d'améliorer l'efficacité de tous les composants de sécurité	√	√

Fiche technique de la gamme

Composant	Avantage	Avantages pour les clients	Différenciation	McAfee Endpoint Threat Defense	McAfee Endpoint Threat Defense and Response
McAfee Threat Intelligence Exchange	Connexion des composants de sécurité afin de partager des informations contextuelles et d'offrir une visibilité et un contrôle à l'échelle de l'entreprise pour mettre en place une protection adaptative contre les menaces	• Identification du terminal « patient zéro » et partage instantané des informations dans tout le système de sécurité pour éviter toute infection ultérieure • Diminution du coût total de possession et opérationnalisation de la sécurité des terminaux • Connexion des composants de sécurité pour créer un circuit de protection en boucle fermée qui réunit des technologies de sécurité indépendantes en un système coordonné unique	• Synthétisation des flux McAfee Global Threat Intelligence et des informations de cyberveille locales et d'autres sources • Définition des éléments approuvés et non fiables à l'aide des informations de cyberveille locales ou issues d'autres sources • Établissement instantané de relations entre les informations de réputation des menaces des terminaux, du réseau, de l'environnement web et des solutions de cloud • Extraction d'informations de cyberveille exploitables et détaillées pour adapter les défenses	√	√
McAfee Data Exchange Layer	Couche d'échange de données pour intégrer et optimiser la communication avec les produits Intel Security et d'autres solutions d'éditeurs tiers	• Réduction des risques et des temps de réponse • Diminution des frais généraux et des coûts d'exploitation du personnel • Processus optimisés et recommandations pratiques	• Partage des informations sur les menaces entre tous les produits de sécurité • Partage instantané des informations de menace collectées au niveau du premier terminal infecté avec les autres terminaux pour prévenir les infections et mettre à jour la protection	√	√
Plate-forme de gestion McAfee ePO	Console centralisée unique qui offre des fonctionnalités de gestion des stratégies évolutives, flexibles et automatisées pour identifier et résoudre les problèmes de sécurité	• Workflows de sécurité simplifiés et unifiés pour une amélioration avérée de l'efficacité • Visibilité centralisée sur tous les systèmes pour évaluer directement le niveau de sécurité et la protection en temps réel • Déploiement rapide et gestion de la protection Intel Security grâce à la mise en œuvre de stratégies personnalisées • Diminution du délai de réponse grâce à des requêtes, des tableaux de bord et des réponses dynamiques et automatisés	• Contrôle granulaire, coûts réduits et gestion accélérée de la sécurité opérationnelle grâce à une seule console • Tableaux de bord avec fonction glisser-déposer pour améliorer la visibilité en temps réel dans tout l'écosystème • Kits de développement logiciel à architecture ouverte pour faciliter l'adoption rapide des futures innovations en matière de sécurité	√	√

Composant	Avantage	Avantages pour les clients	Différenciation	McAfee Endpoint Threat Defense	McAfee Endpoint Threat Defense and Response
McAfee Active Response	Visibilité sur les menaces, chronologies, traque des menaces présentes et passées et détection proactives, avec possibilité d'application immédiate de mesures correctives et d'adaptation de la protection	• Recherche rapide de données en temps réel et historiques sur les menaces pour déterminer l'envergure de l'attaque, accélérer les investigations et diminuer le temps de réponse • Automatisation des réponses aux menaces et protection en temps réel, sans intervention manuelle • Priorisation des menaces selon la gravité et l'urgence • Utilisation de la surveillance continue et des collecteurs personnalisables pour rechercher des indicateurs d'attaques en cours d'exécution, inactifs ou susceptibles d'avoir été supprimés	• Visibilité instantanée sur des tentatives d'exploits inconnus et des comportements à risque qui ont été exécutés dans l'environnement sans être détectés par les technologies de protection • Investigation de la chronologie des événements sur chaque terminal avec la fonction de recherche en direct intégrée sur tous les terminaux afin de traquer les menaces • Action en un clic pour protéger, corriger et adapter la protection, ce qui permet de ramener tous les outils et les étapes nécessaires à une seule opération		✓

Spécifications

McAfee Endpoint Threat Defense	McAfee Endpoint Threat Defense and Response
Plates-formes prises en charge : • Microsoft Windows : 7, To Go, 8, 8.1, 10, 10 November, 10 Anniversary • Mac OS X version 10.5 ou ultérieure • Linux : dernières versions de RHEL, SUSE, CentOS, OEL, Amazon Linux et Ubuntu **Serveurs :** • Windows Server (2003 SP2 ou ultérieur, 2008 SP2 ou ultérieur et 2012), Windows Server 2016 • Windows Embedded (Standard 2009, Point of Service 1.1 SP3 ou ultérieur) • Citrix Xen Guest • Citrix XenApp 5.0 ou ultérieur	**Plates-formes prises en charge :** • Microsoft Windows : 7, 8, 8.1, 10, 10 Anniversary • RedHat 6.5 • CentOS 6.5 • Windows Server 2008, 2012 et 2016

1. McAfee Endpoint Threat Defense and Response inclut des centres de données hébergés situés aux États-Unis et utilisés pour valider l'authentification des clients, vérifier la réputation des fichiers et stocker des données en rapport avec la détection et la traque de fichiers suspects. Même si elle n'est pas indispensable, une connexion au cloud permet d'améliorer les performances de la fonction de confinement dynamique d'applications. Pour bénéficier des fonctionnalités complètes de confinement dynamique d'applications, de McAfee Active Response et de Real Protect, vous avez besoin d'un accès au cloud et d'un contrat de support actif. En outre, ces fonctionnalités sont soumises aux conditions générales du service de cloud.

En savoir plus

Pour en savoir plus sur les avantages de McAfee Endpoint Threat Defense, consultez notre site à l'adresse : **www.mcafee.com/fr/products/endpoint-threat-defense.aspx**.

Pour en savoir plus sur les avantages de McAfee Endpoint Threat Defense and Response, consultez notre site à l'adresse : **www.mcafee.com/fr/products/endpoint-threat-defense-response.aspx**.

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