McAfee Complete Endpoint Threat Protection

Une protection avancée pour tenir en échec les attaques sophistiquées

Pour faire face aux menaces auxquelles elle est confrontée, votre entreprise a besoin d'une visibilité élevée et d'outils qui lui permettent d'agir et de gérer l'intégralité du cycle de défense contre les menaces. Vous devez doter vos spécialistes de la sécurité de fonctionnalités capables d'agir avec une précision accrue et de fournir des informations plus pertinentes sur les menaces avancées. McAfee® Complete Endpoint Threat Protection offre des mécanismes de défense avancés qui effectuent des analyses, endiguent les menaces et prennent des mesures contre les attaques sophistiquées et de type « jour zéro ». Cette protection essentielle des terminaux intègre des fonctionnalités d'apprentissage automatique et de confinement d'application dynamique pour détecter les menaces de type « jour zéro » en temps quasi réel, puis les classer et les bloquer avant qu'elles n'infectent vos systèmes. Des données d'investigation numérique facilement utilisables et des rapports vous tiennent informé et vous aident à passer d'une approche réactive, où vous vous contentez de réagir aux attaques, à une approche proactive axée sur l'investigation et le renforcement des défenses. Par ailleurs, comme la solution repose sur un cadre extensible, vous pouvez facilement ajouter de nouvelles fonctions de protection avancées, aujourd'hui comme demain, à mesure que le paysage des menaces et vos besoins en matière de sécurité évoluent.

Principaux avantages

- Permet de garder une longueur d'avance sur les menaces « jour zéro », les ransomwares et les logiciels « gris » (greywares) grâce à l'apprentissage automatique et au confinement d'application dynamique
- Accélère l'application des mesures de correction et préserve votre productivité grâce à une analyse et à des actions automatisées
- Simplifie votre environnement, votre déploiement et votre gestion courante grâce à une console de gestion centralisée

Protection automatisée contre les menaces avancées

Il est impératif de bloquer les menaces avancées avant qu'elles aient le temps de s'exécuter. C'est pourquoi McAfee Complete Endpoint Threat Protection inclut les technologies de confinement d'application dynamique et Real Protect[1]. Le composant de confinement d'application dynamique isole automatiquement les logiciels « gris » (greywares) et les menaces « jour zéro » présumées en cas de détection de comportements suspects afin d'éviter qu'ils n'infectent vos systèmes ou n'affectent vos utilisateurs. Real Protect examine et classe les menaces en s'appuyant sur l'apprentissage automatique, et conserve les connaissances ainsi acquises afin de pouvoir appliquer automatiquement les mesures appropriées par la suite.

Conçu pour réduire la complexité

La complexité est l'ennemi de l'efficacité. Désormais, vous ne perdrez plus de temps à gérer de multiples

solutions isolées dotées d'interfaces et de consoles de gestion différentes. McAfee Complete Endpoint Threat Protection est géré à l'aide d'une console unique : le logiciel McAfee® ePolicy Orchestrator® (McAfee ePO™). Grâce à cette console centralisée, vous pouvez renforcer plus rapidement vos défenses, accélérer les déploiements et réduire les tâches de gestion courante. Les clients dont l'environnement héberge des systèmes d'exploitation hétérogènes pourront améliorer leur productivité grâce à des stratégies multiplates-formes pour les systèmes Microsoft Windows, Apple Macintosh et Linux.

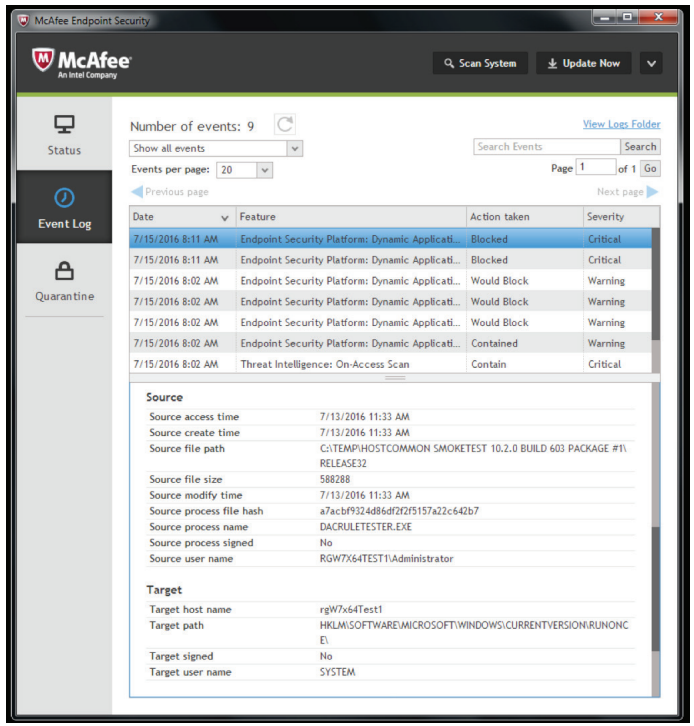

Figure 1. La fonction de confinement d'application dynamique bloque et endigue les menaces en fonction de leur gravité.

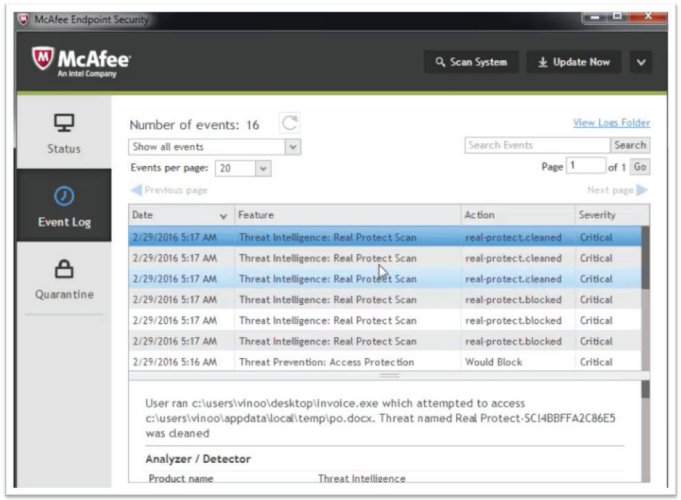

Figure 2. Real Protect utilise l'apprentissage automatique pour détecter en temps quasi réel les logiciels malveillants de type « jour zéro » qui échappent souvent à la détection des analyses basées sur les signatures.

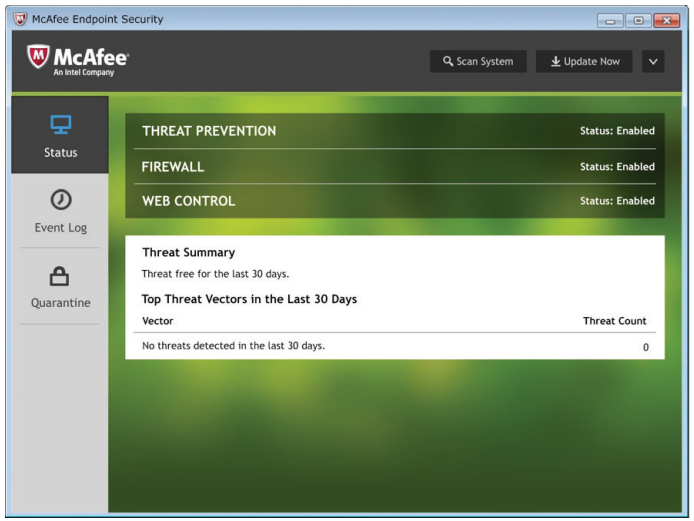

Figure 3. Une interface utilisateur intuitive pour faciliter la tâche des administrateurs et des utilisateurs

Un cadre flexible adapté aux besoins d'aujourd'hui et de demain

McAfee Complete Endpoint Threat Protection vous offre un cadre collaboratif et connecté, ainsi qu'une sécurité en temps quasi réel alliant plusieurs technologies de protection. Une telle approche permet non seulement une analyse plus efficace des menaces, mais aussi le partage des données d'investigation numérique collectées avec d'autres dispositifs de défense afin qu'ils fonctionnent de manière plus intelligente. Grâce à une couche de communication commune, les systèmes de protection des terminaux de base peuvent échanger des données avec des systèmes de défense contre les menaces avancées pour bénéficier d'informations plus pertinentes et d'une détection plus précise et immédiate dès le premier contact avec la menace.

Par ailleurs, une telle approche confère plus de flexibilité en matière de déploiement puisque vous pouvez directement installer tous les composants inclus dans la solution achetée. Vous pouvez ensuite sélectionner les fonctionnalités à configurer et à activer immédiatement et reporter l'activation d'autres défenses à plus tard au moyen d'une simple modification de la stratégie.

Enfin, ce cadre vous permet d'étendre votre protection à mesure que vos besoins évoluent grâce à une architecture conçue pour intégrer des technologies supplémentaires.

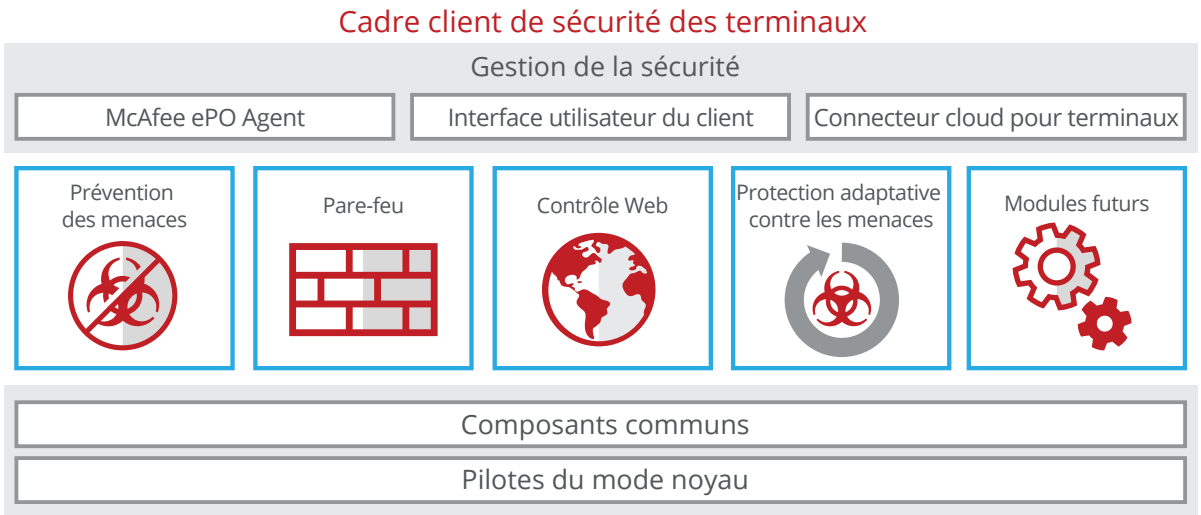

Figure 4. Cadre client de sécurité des terminaux de McAfee

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
- Plates-formes Linux 32 et 64 bits : 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

FICHE TECHNIQUE

Composant	Avantage	Avantages pour les clients	Différenciation
Confinement d'application dynamique	Sécurisation du terminal « patient zéro » grâce au blocage des modifications que les logiciels « gris » (greywares) tentent d'apporter aux terminaux	▪ Protection optimisée, sans impact sur les utilisateurs finaux 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	▪ 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 menaces « jour zéro » avant qu'elles 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 (ransomwares) ▪ 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	▪ 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
Prévention des menaces	Solution de protection complète capable de détecter, de bloquer et de neutraliser les logiciels malveillants rapidement, grâce à plusieurs niveaux de protection	▪ Blocage des logiciels malveillants connus et inconnus grâce à l'analyse heuristique, comportementale et à l'accès ▪ Simplification des stratégies et des déploiements grâce à une protection pour postes de travail et serveurs Windows, Mac et Linux ▪ Amélioration des performances en passant l'analyse des processus approuvés et en priorisant les processus suspects	Protection antimalware multiniveau qui collabore avec le pare-feu et les défenses de l'environnement web pour offrir des analyses et une prévention des menaces plus efficaces
Pare-feu intégré	Protection des terminaux contre les réseaux de robots, les attaques par déni de service distribué (DDoS), les fichiers exécutables non approuvés, les menaces APT et les connexions Internet à risque	▪ Protection des utilisateurs et de la productivité grâce à la mise en œuvre de stratégies ▪ Préservation de la bande passante par le blocage des connexions entrantes indésirables et le contrôle des demandes sortantes ▪ Sensibilisation des utilisateurs par des messages d'information sur les réseaux et fichiers exécutables fiables, ainsi que sur les fichiers ou connexions à risque	Stratégies basées sur l'application et l'emplacement pour protéger les postes de travail et les ordinateurs portables, en particulier lorsqu'ils ne sont pas connectés au réseau d'entreprise

Composant	Avantage	Avantages pour les clients	Différenciation
Contrôle Web	Navigation sur Internet sans risque grâce à une protection et à un filtrage spécifiques au Web et spécialement conçus pour les terminaux	▪ Diminution des risques et protection de la conformité grâce à des messages d'avertissement des utilisateurs avant qu'ils n'accèdent à des sites web malveillants ▪ Prévention des menaces et protection de la productivité par l'autorisation ou le blocage de l'accès aux sites web ▪ Blocage des téléchargements dangereux avant leur exécution	Protection des systèmes Windows et Mac et de nombreux navigateurs
Data Exchange Layer	Couche d'échange de données pour intégrer et optimiser la communication avec les produits McAfee et d'autres solutions d'éditeurs tiers	▪ Réduction des risques et des temps de réponse grâce à l'intégration ▪ Diminution des frais généraux et des coûts d'exploitation du personnel ▪ Processus optimisés et recommandations pratiques	Partage d'informations sur les principales menaces entre les composants de sécurité
Gestion par 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 et flexibilité accrues pour la prise de mesures en toute confiance ▪ Déploiement et gestion rapides d'un seul agent grâce à la mise en œuvre de stratégies personnalisables ▪ Diminution du délai de réponse grâce à des rapports et à des tableaux de bord intuitifs	▪ Contrôle accru, coûts réduits et gestion accélérée de la sécurité opérationnelle grâce à une seule console ▪ Interface reconnue dans tout le secteur pour sa convivialité et ses performances ▪ Tableaux de bord avec fonction glisser-déposer pour une visibilité sur tout l'écosystème de sécurité ▪ Plate-forme ouverte pour faciliter l'adoption rapide des innovations en matière de sécurité

En savoir plus

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

1. La solution inclut des centres de données hébergés situés aux États-Unis et utilisés pour vérifier la réputation des fichiers et stocker des données en rapport avec les détections de fichiers suspects. Même si elle n'est pas indispensable, une connexion au cloud permet d'améliorer les performances de la fonction de confinement d'application dynamique. Pour bénéficier des fonctionnalités complètes de confinement d'application dynamique 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.

McAfee Together is power.

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