McAfee ePolicy Orchestrator

Une console centralisée pour consulter des informations pertinentes sur la sécurité, les partager et agir sans délai

La gestion de la sécurité exige de jongler constamment avec de nombreux outils et de grands volumes de données. Cela confère un avantage au pirate informatique, qui dispose de plus de temps pour exploiter les failles de protection entre les outils et venir perturber vos activités. En outre, le personnel dédié à la cybersécurité est limité et doit avoir les moyens d'en gérer toute la complexité. La plate-forme de gestion McAfee® ePolicy Orchestrator® (McAfee ePO™) permet d'accélérer l'exécution des tâches et de limiter le risque d'erreurs humaines, sans compter qu'elle motive les responsables à gérer la sécurité de façon plus rapide et efficace.

L'abc de la sécurité

Commençons par l'essentiel. Toute architecture de sécurité repose d'abord sur la capacité à surveiller et à contrôler l'intégrité des terminaux et des systèmes. Selon les recommandations formulées dans certaines normes du secteur en matière de contrôles de sécurité et confidentialité, p. ex. dans les documents **CIS** Controls et **NIST SP 800-53**, c'est même indispensable. La console McAfee ePO vous permet de bénéficier d'une visibilité essentielle, mais aussi de définir et automatiquement appliquer des stratégies pour conserver un niveau de sécurité élevé dans l'entreprise. La gestion et la mise en œuvre des stratégies sur l'ensemble des produits de sécurité de l'entreprise sont réalisées au moyen d'une seule console, ce qui réduit la complexité généralement associée à l'administration de plusieurs produits. Cette sécurité fondamentale est la clé de la conformité de votre sécurité informatique.

Une gestion avancée et éprouvée de la sécurité

Plus de 30 000 entreprises s'en remettent à la console McAfee ePO pour gérer leur sécurité, optimiser et automatiser leurs processus de conformité, et améliorer la visibilité sur les opérations réseau, de sécurité et des terminaux. Les grandes entreprises font confiance à l'architecture très évolutive de la console McAfee ePO, qui leur permet de gérer des centaines, voire des milliers de postes, à partir d'un emplacement unique. La console McAfee ePO offre à l'administrateur responsable de la sécurité la possibilité de simplifier la gestion des stratégies, d'importer des sources de cyberveille externes grâce à Data Exchange Layer (DXL), et d'effectuer une intégration

Gardez le contact

bidirectionnelle des stratégies sur un large éventail de produits. Ce gain d'efficacité opérationnelle allège la charge d'administration des processus et de partage des données, favorisant une intervention plus rapide.

L'efficacité pour lutter contre la prolifération des outils

Une étude d'ESG révèle que 40 % des entreprises utilisent entre 10 et 25 outils, et 30 % entre 26 et 50 outils, pour gérer des milliards de nouvelles menaces et une multitude d'équipements. Compte tenu de la complexité de gestion d'un tel arsenal de produits, une gestion unifiée procure incontestablement de nombreux avantages, ne fut-ce qu'en termes de rentabilité opérationnelle, pour de nombreuses tâches. Bien conscient de la situation, McAfee a adopté une approche collaborative (« Together is power ») en matière de gestion de la sécurité. Celle-ci permet de consolider la prolifération des outils tout en protégeant l'ensemble de vos ressources, en prenant en charge la cyberveille, en gérant les données open source et en intégrant les produits d'éditeurs tiers. McAfee offre un centre de commande et de contrôle centralisé pour assurer la gestion et la conformité d'un large éventail de produits. Vous pouvez passer rapidement d'un produit à un autre pour trouver les données critiques dont vous avez besoin et appliquer la mesure ou stratégie requise. La console McAfee ePO vous permet également d'investir dans des technologies de nouvelle génération et de les intégrer avec des ressources existantes au sein d'une infrastructure unique.

Liste de produits gérés par McAfee ePO (exemple)

Produits McAfee	Produits d'autres éditeurs
McAfee Endpoint Protection (Prévention contre les menaces, Contrôle Web, Pare-feu)	Guidance Software : enCase Enterprise
McAfee Drive Encryption	Avecto : Privilege Guard
McAfee File and Removable Media Protection	AccessData : AccesData Enterprise
McAfee Active Response	Autonomic Software : Power Manager, Patch Manager
McAfee Management for Optimized Virtual Environments (McAfee MOVE)	Xerox MFP
McAfee Data Loss Prevention (McAfee DLP)	DXL
McAfee Policy Auditor	
McAfee Enterprise Security Manager	
McAfee Threat Intelligence Exchange	
McAfee Application Control	
McAfee Cloud Workload Security	
McAfee Advanced Threat Defense	
McAfee Content Security Reporter	
McAfee Database Activity Monitoring	

Scénarios d'utilisation possibles : Gestion centralisée des produits de sécurité avec la console McAfee ePO

Produit et technologie	Scénario de gestion centralisée	Avantage
McAfee ePO McAfee Endpoint Security	McAfee Endpoint Security détecte un fichier malveillant connu sur un terminal. La console McAfee ePO définit une stratégie plus stricte sur le terminal pour le mettre en quarantaine. Toutes les opérations sont effectuées dans une interface de gestion commune.	Confinement rapide d'un terminal compromis
McAfee ePO McAfee DLP McAfee Enterprise Security Manager	McAfee Enterprise Security Manager détecte l'exfiltration d'un volume important de données sur un terminal et le marque dans la console McAfee ePO. Cette dernière applique ensuite des stratégies de prévention des fuites de données pour bloquer ces données et avertit l'utilisateur de la non-conformité d'une telle action.	Application automatique de stratégies de prévention des fuites de données

Exemples d'intégration

Produit et technologie	Scénario d'intégration	Avantage
McAfee ePO McAfee Endpoint Security DXL Cisco Identity Service Engine (ISE) Cisco PxGrid	McAfee Endpoint Security marque un hôte suspect. La console McAfee ePO peut déclencher des analyses supplémentaires. Ces informations sont communiquées à Cisco ISE via PxGrid et la plate-forme d'échange DXL (console McAfee ePO). Cisco ISE peut isoler l'hôte jusqu'à ce qu'il soit jugé acceptable.	Protection proactive renforcée
Avecto Defendpoint McAfee ePO DXL McAfee Threat Intelligence Exchange	Déployez et gérez la solution de gestion des privilèges la plus réputée du marché, Avecto Defendpoint, à partir de McAfee ePO. Avecto Defendpoint s'appuie sur les données de réputation d'applications fournies par McAfee Threat Intelligence Exchange pour modifier les configurations.	Complexité réduite Pas d'infrastructure supplémentaire et donc un coût de possession réduit Modifications des accès avec privilèges basées sur la cyberveille
Rapid7 Nexpose McAfee ePO DXL	McAfee ePO partage la liste des ressources avec Nexpose. La console ePO vous permet d'accéder et de comprendre votre exposition aux risques et de définir des stratégies en conséquence. Les données sur les vulnérabilités sont partagées avec la communauté d'éditeurs DXL.	Réduction de la complexité Vue complète et fiable du niveau de sécurité et priorisation des mesures à appliquer pour réduire le risque à partir d'un seul tableau de bord
Check Point NGTX Check Point NGTP McAfee ePO DXL McAfee Active Response McAfee Enterprise Security Manager	Cette intégration simplifie le partage bidirectionnel et en temps réel de la cyberveille entre le réseau et les terminaux. Les événements sont partagés avec la communauté DXL.	Délai de détection plus rapide Blocage et neutralisation des attaques

Les entreprises équipées de plates-formes intégrées sont mieux protégées et peuvent intervenir plus rapidement que celles qui en sont dépourvues.

	Entreprises avec plates-formes intégrées	Entreprises sans plates-formes intégrées
Victimes de moins de cinq compromissions l'année dernière	78 %	55 %
Menaces détectées en huit heures	80 %	54 %

2016 Penn Schoen Berland

Des workflows extensibles pour optimiser les processus

La base de données McAfee ePO offre des fonctionnalités de gestion flexibles et automatisées. Celles-ci vous permettent d'identifier, de gérer et de réagir face aux vulnérabilités, à l'évolution du niveau de sécurité et aux menaces connues, le tout à partir d'une même console. Vous pouvez définir la manière dont la console McAfee ePO doit lancer des alertes et des actions en fonction du type et de la criticité des événements de sécurité au sein de votre environnement, mais aussi de vos stratégies et outils. La plate-forme McAfee ePO favorise l'optimisation des opérations de développement et de sécurité, car elles permet de créer des workflows automatisés entre vos systèmes informatiques et dispositifs de sécurité, afin de corriger rapidement les problèmes. Vous pouvez l'utiliser pour déclencher des mesures de correction qui seront appliquées par vos systèmes, notamment l'affectation de stratégies plus strictes. L'utilisation de ses API web permet de limiter les tâches manuelles.

Scénarios d'utilisation courants

- Gagnez du temps et évitez les tâches fastidieuses et redondantes en planifiant la production de rapports de conformité de la sécurité adaptés à chaque partie prenante.
- La console McAfee ePO peut être facilement intégrée à vos fonctions et processus métier grâce à des API bien conçues. Celles-ci vous permettent d'accéder à une mine d'informations et d'accélérer les workflows (intégration de systèmes de gestion de tickets d'incident, d'applications web ou de portails en libre-service).
- Préservez votre niveau de sécurité en déployant des solutions de sécurité et des agents au fur et à mesure que de nouveaux équipements sont ajoutés à votre réseau d'entreprise, par la synchronisation de la console McAfee ePO et d'Active Directory.

« Plate-forme de gestion d'une efficacité inégalée, McAfee ePolicy Orchestrator est l'outil de gestion sous-jacent de tous les produits de sécurité de l'entreprise. Elle offre la puissance et la flexibilité recherchées par tous les acheteurs d'entreprise. Couvrant de nombreux aspects de la sécurité, les fonctionnalités sont étroitement intégrées grâce à une cyberveille et un moteur de stratégies communs. »

— Forrester Wave : Endpoint Security Suites (Suites de protection des terminaux), 2016

Neutralisation et correction rapides

Les fonctionnalités avancées intégrées de McAfee ePO améliorent l'efficacité de l'équipe responsable des opérations de sécurité lorsqu'elle doit neutraliser une menace ou apporter des modifications pour rétablir la conformité. La fonction Réponses automatiques de McAfee ePO peut déclencher une action donnée, basée sur un événement spécifique. Ces actions peuvent être de simples notifications ou des mesures de correction approuvées.

Scénarios d'utilisation communs pour les réponses automatiques

- Envoi d'e-mails ou de SMS de notification aux administrateurs en cas de nouvelles menaces, d'erreurs critiques, selon des seuils déterminés
- Application de stratégies en cas d'événements de menace ou côté client, p. ex. pour bloquer les communications externes lorsqu'un système est potentiellement compromis (pour empêcher les activités de commande et de contrôle) ou pour éviter l'exfiltration de données ou les transferts sortants jusqu'à ce que l'administrateur ait modifié la stratégie
- Marquage des systèmes et application de mesures de correction supplémentaires, p. ex. des analyses de la mémoire à la demande en cas de détection de menaces
- Déclenchement de fichiers exécutables enregistrés pour l'exécution de scripts externes et de commandes serveur, p. ex. la génération d'un ticket dans le centre de service ou l'intégration à d'autres processus métier
- Mise en quarantaine automatique du terminal doublée de l'application de stratégies plus strictes

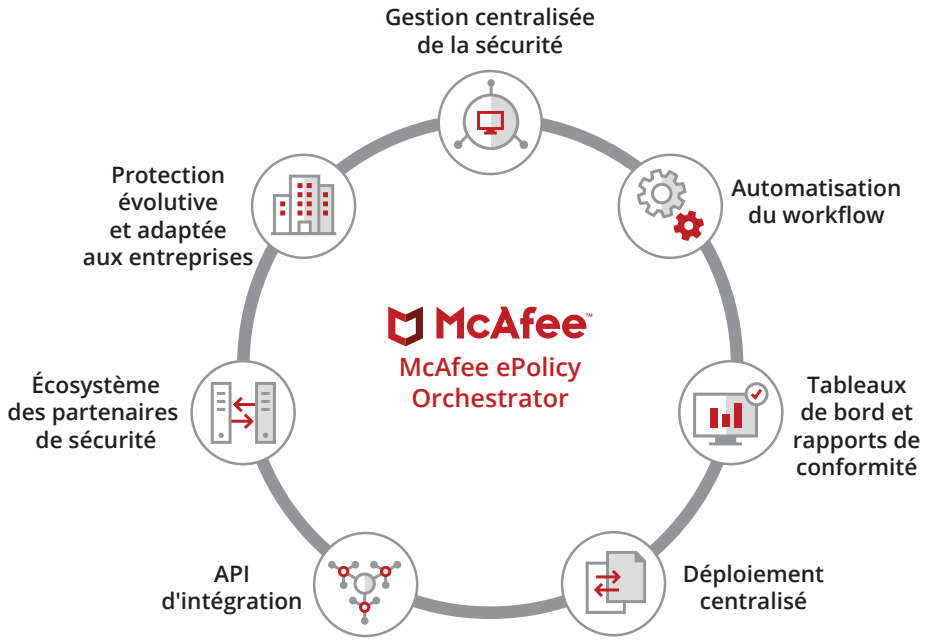

Figure 1. Gestion des stratégies grâce à la console McAfee ePO.

Sécurisation de toute l'entreprise avec la console McAfee ePO

Gestion centralisée de la sécurité

- Console unique pour bénéficier d'une gestion centralisée et d'une visibilité sur des centaines de milliers de postes dans toute l'entreprise
- Infrastructure ouverte pour une gestion globale de la sécurité des systèmes protégés par des solutions McAfee et d'autres éditeurs
- Plate-forme extensible qui intègre et tire parti de l'infrastructure informatique existante pour améliorer l'efficacité opérationnelle

Accélération des temps de réponse en toute sécurité

- Vues et informations complètes pour résoudre les problèmes de sécurité internes et externes de façon proactive
- Déploiement centralisé rapide des mises à jour et des définitions de sécurité pour garantir la protection des terminaux contre les dernières menaces
- Temps de réponse accélérés grâce à des tableaux de bord directement exploitables et à des fonctions avancées de requête et de génération de rapports

Réduction de la complexité et optimisation des processus

- Infrastructure de sécurité rapidement opérationnelle grâce à une configuration assistée, à des flux de gestion de stratégies automatisés et à des tableaux de bord prédéfinis
- Affectation de stratégies par marqueurs pour attribuer avec précision des profils de sécurité prédéfinis à des systèmes ou à des groupes de systèmes en fonction de leur rôle au sein de l'entreprise ou de leur niveau de risque
- Catalogue de tâches et fonctionnalités de gestion automatisée pour rationaliser les processus administratifs et réduire la charge de travail
- Agent unique pour gérer plusieurs produits de protection des terminaux et ainsi réduire le risque de conflit sur ceux-ci

Évolutivité au fil des déploiements au sein de l'entreprise

- Architecture adaptée aux entreprises et capable de prendre en charge des centaines de milliers d'équipements sur un serveur unique
- Solution éprouvée, capable de gérer des environnements informatiques complexes et hétérogènes
- Rapports d'entreprise qui agrègent les données pour offrir une vue unifiée de votre état de sécurisation et de votre conformité

« Le logiciel McAfee ePO se démarque des autres solutions. Cette plate-forme unique répond à tous les besoins de protection des terminaux. Je bénéficie d'une visibilité totale sur tous les produits McAfee depuis une seule et même console. Grâce à ses tableaux de bord conviviaux et ses fonctionnalités intégrées, toutes les tâches et opérations sont simplifiées : rapports, visibilité, déploiement, mise à jour, gestion, prise de décisions, etc. »

— Christopher Sacharok, ingénieur responsable de la sécurité des informations, Computer Sciences Corporation

McAfee
Together is power.

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