McAfee ePolicy Orchestrator

La vision et les moyens d'action attendus par les équipes de sécurité

La gestion de la sécurité exige de jongler constamment avec de nombreux outils et de grands volumes de données. Cela confère un avantage aux pirates, qui disposent de plus de temps pour exploiter les failles de protection entre les outils et ainsi occasionner davantage de dommages. En outre, le personnel dédié à la cybersécurité est limité et doit avoir les moyens d'orchestrer de façon simple des environnements pourtant complexes.

Votre équipe doit neutraliser rapidement les menaces sur les équipements de tous types afin de limiter les dégâts, et la direction exige des preuves de l'efficacité du dispositif de sécurité. La plate-forme de gestion McAfee® ePolicy Orchestrator® (McAfee ePO™), disponible sur site et dans le cloud, permet d'accélérer l'exécution des tâches et de limiter le risque d'erreurs humaines. De plus, elle aide les responsables de la gestion de la sécurité à réagir de façon plus rapide et efficace en cas d'attaque.

L'abc de la sécurité

Commençons par examiner les incontournables. Toute architecture de sécurité repose d'abord sur la capacité à surveiller et à contrôler l'intégrité des équipements 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 CIS Benchmarks ainsi que dans la publication spéciale 800-153 du NIST, c'est même indispensable. La console McAfee ePO vous permet de bénéficier d'une visibilité essentielle, mais aussi de définir et d'automatiquement appliquer des stratégies pour conserver un niveau de sécurité élevé. L'orchestration de plusieurs produits devient nettement plus simple du fait que la gestion et la mise en œuvre des stratégies à l'échelle de l'entreprise s'effectuent à partir d'une seule console. Cette fonction fondamentale de gestion de la sécurité est la clé de la conformité de votre sécurité informatique.

Principaux avantages

- Gestion centralisée reconnue pour son efficacité, grâce à sa console unifiée et intégrée très simple d'emploi ; déploiement dans le cloud ou sur site
- Workflows automatisés qui simplifient les tâches d'administration et améliorent l'efficacité
- Plate-forme ouverte et complète qui intègre les solutions McAfee et plus de 150 solutions de tiers pour une réponse aux incidents plus rapide et précise
- Gestion commune de la sécurité pour la grande majorité des équipements disponibles sur le marché
- Utilisation et optimisation de contrôles natifs intégrés aux systèmes d'exploitation (Windows Defender, p. ex.)

Gardez le contact

Une gestion avancée et éprouvée de la sécurité, en toute simplicité

Plus de 36 000 entreprises font confiance à la console McAfee ePO pour gérer leur sécurité, optimiser et automatiser leurs processus de mise en conformité, et améliorer la visibilité sur les équipements, les réseaux et les opérations de sécurité. L'architecture très évolutive de cette console permet aux grandes entreprises de gérer des centaines, voire des milliers de postes, à partir d'un emplacement unique et intégré. L'espace de travail ePO est un véritable tableau de bord qui offre une représentation graphique et synthétique de tout l'environnement. Il permet en outre de gérer correctement les risques en catégorisant notamment le niveau de risque liée aux tâches.

Les administrateurs peuvent accéder au détail d'événements spécifiques pour obtenir des renseignements complémentaires. Cette vue globale accélère la création de rapports, facilite l'exploitation des données disponibles et limite fortement les risques d'erreur même en cas d'interventions manuelles. 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), notre structure d'échange d'informations de pointe, et d'effectuer une intégration 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 d'une plate-forme ouverte 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 d'administration d'un tel arsenal de produits, une gestion unifiée procure incontestablement de nombreux avantages, ne fut-ce qu'en termes de rentabilité opérationnelle. D'après une étude réalisée par MSI en 2018, plus de la moitié des entreprises estiment que l'intégration des outils de sécurité augmenterait leur efficacité de plus de 20 %. Bien conscient de la situation, McAfee a adopté une approche de la gestion de la sécurité fondée sur une plate-forme ouverte. Celle-ci permet de consolider des outils toujours plus nombreux, tout en protégeant l'ensemble de vos ressources, en prenant en charge la cyberveille, en gérant les données à code source libre et en intégrant les produits d'éditeurs tiers. McAfee offre un centre de contrôle centralisé pour assurer la gestion et la conformité d'un large éventail de produits. Les analystes peuvent passer rapidement d'un produit à un autre pour trouver les données critiques dont ils ont besoin et appliquer la mesure ou la 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.

Notre plate-forme ouverte propose différentes méthodes d'intégration (écriture de scripts, utilisation ou non d'API, ou encore intervention minime grâce à DXL, notre structure de communication à code source libre).

Principaux avantages (suite)

- Évolutivité permettant de prendre en charge des centaines voire des milliers d'équipements, avec une couverture qui s'étend des équipements au cloud

Selon des analystes, c'est le logiciel McAfee ePO qui incite de nombreuses entreprises à choisir McAfee et à y rester fidèles.

Avantages d'une plate-forme intégrée
Les entreprises équipées de plates-formes intégrées sont mieux protégées et peuvent intervenir plus rapidement que celles qui en sont dépourvues.

Entreprises dotées d'une plate-forme intégrée

- 78 % ont été victimes de moins de cinq compromissions l'année dernière.
- 80 % ont détecté les menaces dans un délai de huit heures.

Vous pouvez ainsi choisir celle qui répond le mieux à vos besoins, tout en évitant les personnalisations fastidieuses et le recours à divers services. Le programme McAfee® Security Innovation Alliance (SIA) accélère le développement de produits de sécurité interopérables et simplifie leur intégration aux environnements complexes des clients. En outre, il procure un écosystème de sécurité connecté, réellement intégré, pour une rentabilisation optimale des investissements des clients en matière de sécurité. Le programme SIA compte actuellement plus de 150 intégrations de partenaires.

De plus, la structure de communication Data Exchange Layer (DXL) connecte et optimise les actions des divers produits de sécurité d'éditeurs différents et des solutions développées en interne ou à code source libre. L'intégration entre Cisco pxGrid et DXL vous donne accès à toutes les données issues de 50 autres technologies de sécurité. McAfee ePO est un composant essentiel pour la gestion de notre plate-forme ouverte robuste.

La sécurité des équipements étendue avec la gestion d'outils natifs

Extensible, la plate-forme McAfee ePO est capable de gérer de nombreux équipements, y compris ceux dotés de contrôles natifs. En plus de cogérer les outils de sécurité intégrés dans Microsoft Windows 10, la solution McAfee les optimise pour garantir une protection maximale, tout en permettant aux entreprises de tirer parti des fonctions système natives de Microsoft. Le logiciel McAfee ePO gère McAfee® MVISION Endpoint, qui combine des fonctionnalités d'apprentissage automatique conçues pour renforcer la sécurité native des systèmes d'exploitation Microsoft, tout en vous épargnant la complexité et les coûts qu'engendrerait une console de gestion supplémentaire. De plus, il assure une gestion commune à l'aide de stratégies harmonisées entre tous les équipements, y compris ceux qui exécutent Microsoft Windows 10, de façon à garantir cohérence et simplicité dans l'environnement d'entreprise hétérogène.

Cohérence grâce aux workflows automatisés

McAfee ePO offre des fonctionnalités de gestion flexibles et automatisées. Celles-ci vous permettent d'identifier et de gérer les vulnérabilités, les changements dans votre niveau de sécurité et les menaces connues, ainsi que d'appliquer les mesures nécessaires, le tout à partir d'une même console. Une étude de MSI commanditée par McAfee en 2018 a révélé que les entreprises s'attendent à ce que l'automatisation de tâches reproductibles ou répétitives leur procure un gain de temps d'environ 25 % par jour. Grâce au logiciel McAfee ePO, vous pouvez facilement déployer et mettre en œuvre des stratégies de sécurité à partir d'une vue unique, en activant quelques étapes se succédant de manière logique. Cette vue propose des données contextuelles pertinentes à mesure que vous exécutez les différentes tâches, et affiche chaque étape ainsi que les relations entre chacune d'entre elles. La gestion est par conséquent moins complexe et moins sujette aux erreurs. 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 d'après vos stratégies et outils. La plate-forme McAfee ePO favorise l'optimisation

Entreprises dépourvues d'une plate-forme intégrée

- 55 % seulement ont été victimes de moins de cinq compromissions l'année dernière.
- 54 % à peine ont détecté les menaces dans un délai de huit heures.

Source : 2016 Penn Schoen Berland

Gain de temps

D'après une étude réalisée par MSI en 2018, les clients estiment qu'une intégration de leurs outils de sécurité leur procurerait un gain de temps de 20 %.

Les avantages de l'intégration

- Amélioration de l'efficacité des outils et des processus : 61 %
- Réduction de la complexité et des interventions manuelles, permettant aux professionnels de la sécurité de se concentrer sur les tâches nécessitant un esprit critique : 61 %
- Amélioration de la visibilité par la présentation des données sous la forme de modèles et en contexte : 58 %
- Optimisation des workflows pour des réponses rapides : 57 %

Source : Étude réalisée par MSI, 2018

des opérations de développement et de sécurité, car elle permet de créer des workflows automatisés entre vos systèmes informatiques et dispositifs de sécurité, afin de corriger rapidement les problèmes. Vous pouvez utiliser la console McAfee ePO pour déclencher des mesures de correction qui seront appliquées par vos systèmes informatiques, notamment l'affectation de stratégies plus strictes. L'utilisation de ses API web permet de limiter les tâches manuelles. Il est possible d'exiger qu'une stratégie ou tâche nouvellement créée ou mise à jour soit soumise à une procédure d'approbation pour pouvoir être envoyée en mode Push, une mesure de contrôle qualité qui réduit encore le risque d'erreurs.

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.
- Intégrez facilement la console McAfee ePO à vos fonctions et processus métier existants en tirant parti de ses API robustes, de façon à accroître votre visibilité et à accélérer les workflows. La console s'intègre par exemple à des systèmes de gestion des tickets, applications web ou portails en libre-service.
- Préservez votre niveau de protection en déployant des solutions de sécurité avec apprentissage automatique ou avec agent au fur et à mesure que de nouveaux terminaux sont ajoutés à votre réseau d'entreprise, par la synchronisation de la console McAfee ePO et d'Active Directory.

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

« McAfee ePO a été l'un des pionniers de l'intégration de l'automatisation et de l'orchestration de la sécurité. (...) De nos jours, les professionnels de la sécurité ont besoin des performances de la solution ePO traditionnelle, mais sous une forme simplifiée, qui leur garantisse à la fois efficience et efficacité. (...) L'espace de travail SaaS de MVISION combine analyse, gestion des stratégies et événements selon des modalités qui répondent aux besoins des grandes et moyennes entreprises. »

— Frank Dickinson, Vice-président de la recherche en produits de sécurité, IDC

- 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 de la charge de travail ou du conteneur (n'importe quel équipement) avec application de stratégies plus strictes

Gestion de la sécurité dans le cloud

Les entreprises doivent pouvoir déployer les solutions de protection contre les menaces avancées plus facilement et rapidement. Elles sont nombreuses à se rendre compte du gain d'efficacité qu'offre la gestion de la sécurité dans le cloud, en éliminant les coûts et les tâches de maintenance associés à une infrastructure sur site. McAfee ePO peut être implémenté à partir du cloud, partout et à tout moment, selon deux options de déploiement : McAfee ePO sur Amazon Web Services (AWS) ou McAfee MVISION ePO. L'un comme l'autre peuvent être opérationnels en moins d'une heure.

- Avec McAfee ePO sur AWS, les entreprises peuvent tirer parti d'un grand nombre de services AWS natifs, comme l'allocation automatique des ressources, et d'Amazon RDS. Elles n'ont donc plus à acheter et à gérer une base de données distincte. Les administrateurs peuvent se concentrer sur les tâches de sécurité primordiales, sans se soucier de l'infrastructure. McAfee ePO sur AWS gère McAfee® Endpoint Security, McAfee® Data Loss Prevention, McAfee® Cloud Workload Security, DXL ainsi que des solutions d'autres éditeurs qui lui sont intégrées.
- McAfee® MVISION ePO étend les avantages de McAfee ePO grâce à son modèle SaaS. Celui-ci simplifie considérablement la gestion de la plate-forme, de sorte que vous pouvez vous consacrer pleinement aux tâches de sécurité critiques. Les mises à jour sont distribuées vers la plate-forme de façon transparente et en continu. Une fois l'agent déployé, les produits de sécurité requis sont automatiquement déployés sur tous les équipements de l'entreprise. Non seulement il devient inutile de les installer ou de les mettre à jour manuellement pour chaque équipement, mais cette automatisation améliore la mise en œuvre des stratégies de protection. Les entreprises peuvent ainsi gérer McAfee MVISION Endpoint et DXL à l'aide d'une seule console et à partir de n'importe quel emplacement. McAfee MVISION ePO permet à vos équipements de fournir des renseignements essentiels à votre SIEM. Grâce à ces données pertinentes et facilement accessibles, vos analystes peuvent affiner la traque des menaces et l'application des mesures correctives.

« 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

Produits McAfee gérés par McAfee ePO

Produits McAfee*
McAfee® Endpoint Protection (Prévention contre les menaces, Contrôle Web, Pare-feu)
McAfee MVISION Endpoint ajoute des fonctions de protection contre les menaces avancées à Windows Defender
McAfee® MVISION Mobile
McAfee® Drive Encryption
McAfee® File and Removable Media Protection
McAfee® Active Response
McAfee® Management for Optimized Virtual Environments (McAfee MOVE)
McAfee Data Loss Prevention (McAfee DLP)
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
Data Exchange Layer (DXL)

**Pour McAfee ePO en version déployée sur site*

Flexibilité de déploiement

Déploiement	Principal avantage
McAfee ePO sur site	Contrôle total des données et fonctionnalités
McAfee ePO sur AWS	Aucune maintenance du matériel, alors qu'elle est requise avec une solution déployée sur site
McAfee MVISION ePO (solution SaaS ePO*)	Offre SaaS multiclient qui élimine entièrement la maintenance de l'infrastructure et la gestion des mises à niveau

**Les fonctionnalités ePO ne sont pas toutes disponibles dans McAfee MVISION ePO.*

Scénarios d'utilisation : Gestion centralisée de la sécurité par la console McAfee ePO

Produit et technologie	Scénario d'utilisation	Avantage
McAfee MVISION ePO McAfee MVISION Endpoint Microsoft Windows 10	McAfee MVISION ePO gère McAfee MVISION Endpoint, qui renforce les contrôles natifs de Microsoft Windows 10 à l'aide de fonctions de protection avancée. Une plate-forme de gestion commune et des stratégies cohérentes pour Microsoft Windows et McAfee Endpoint Security vous permettent de facilement détecter et contrer les menaces avancées.	Protection renforcée pour les contrôles natifs de Microsoft Windows, et gestion plus efficace de la sécurité
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 des terminaux infectés
McAfee ePO McAfee Data Loss Prevention 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 (via la console McAfee ePO). Cisco ISE peut isoler l'hôte jusqu'à ce qu'il soit jugé acceptable.	Protection proactive renforcée
Rapid7 Nexpose McAfee ePO DXL	McAfee ePO partage la liste des ressources avec Nexpose. Vous pouvez ensuite consulter la console ePO pour comprendre votre exposition aux risques, et y 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 également partagés avec la communauté DXL. La lame logicielle Check Point Anti-Bot bloque le trafic de commande et de contrôle, et envoie des alertes à McAfee ePO, ainsi qu'aux autres solutions de sécurité tierces intégrées, par l'intermédiaire de sujets DXL communs. Sur la base de ces renseignements, McAfee lance automatiquement un workflow adapté de correction des terminaux. Les solutions de Check Point et de McAfee sont également capables de détecter et de prévenir les attaques « jour zéro », mais aussi de les convertir ensuite en attaques connues, qu'elles émanent du réseau ou du terminal. Grâce à l'échange en temps réel d'une cyberveille stratégique, cette intégration permet aux produits de Check Point et de McAfee de détecter, bloquer et neutraliser les menaces de façon automatisée.	▪ Délai de détection plus rapide ▪ Blocage et neutralisation des attaques

McAfee Together is power.

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