McAfee Active Response

Un outil complet de détection des menaces et de réponse aux incidents pour les terminaux

De nos jours, les entreprises sont confrontées à un paysage des menaces en évolution aussi rapide que constante. Les attaques informatiques sont mises au point et diffusées à des cadences effrénées. Certaines attaques sont conçues sur mesure pour cibler des entreprises individuelles en exploitant des informations très précises, ce qui améliore leur efficacité et réduit les possibilités de détection. De plus en plus souvent, les pirates passent outre les technologies de prévention. Des outils intégrés et conviviaux capables de mieux détecter leur présence mais aussi d'assurer une investigation et une résolution rapides de l'incident sont désormais une exigence fondamentale pour les entreprises proactives, soucieuses de leur sécurité. Les solutions de détection et de réponse aux incidents les plus performantes améliorent l'efficacité du dispositif de sécurité alors même qu'elles capturent de plus en plus d'informations à partir d'un nombre croissant de systèmes. Grâce à des fonctionnalités prédéfinies de premier ordre, à une interaction automatisée avec les solutions de gestion de la sécurité existantes et à une capacité de personnalisation étendue, McAfee® Active Response limite fortement le rayon d'action des auteurs d'attaques et leurs possibilités de nuire à vos actifs informatiques et à votre image de marque.

Principaux avantages

- **Automatisation —** La solution collecte et surveille le contexte et les états des systèmes de façon à détecter les modifications susceptibles de correspondre à des indicateurs d'attaque, et identifie même les composants d'attaque à l'état de sommeil. Elle envoie ensuite les informations recueillies aux équipes chargées de l'analytique, des opérations et des investigations numériques.
- **Adaptabilité —** Lorsque vous recevez une alerte, vous pouvez adapter la solution aux changements dans les méthodologies d'attaque. Vous pouvez automatiser la collecte des données, les alertes et les réponses aux objets suspects, et personnaliser votre configuration en fonction de vos workflows.
- **Continuité —** Fonctionnant en continu, des collecteurs persistants activent des déclencheurs lors de la détection d'événements d'attaque, signalant ainsi à vos systèmes et à vous-même la présence d'une activité d'attaque placée sous surveillance.

Un paysage des menaces en pleine mutation

Désormais conscientes qu'une compromission est possible à chaque instant, les entreprises doivent se préparer à y faire face par la détection précoce des attaques, l'identification des activités malveillantes en cours ou encore la découverte d'indicateurs d'attaques (IoA). De même, elles doivent reconnaître que de nouvelles technologies sont indispensables pour combler les failles en matière de visibilité, de découverte, de détection et de réponse aux incidents.

Limites des approches actuelles de réponse aux incidents

Lorsqu'ils doivent enquêter sur un incident potentiel ou avéré dans une entreprise tout entière, les équipes

d'intervention et les administrateurs de la sécurité sont entravés dans leur travail par deux facteurs : le temps et l'échelle de l'opération. Même si un grand nombre d'informations détaillées sont collectées par des systèmes ou outils existants, celles-ci sont très longues à rassembler et à analyser. Or, la vitesse est un facteur critique de la collecte de données. Dès lors, des compromis importants sont consentis dans la nature des données recueillies, ainsi que dans le nombre de systèmes sources. De plus, en raison de leur volume, les données deviennent de plus en plus difficiles à traiter pour en extraire les informations pertinentes.

Les outils de réponse aux incidents les plus communément utilisés sont des scripts écrits par les équipes d'intervention elles-mêmes. Ces outils jettent les bases de la collecte des données qui seront ensuite exploitées dans le cadre d'analyses plus larges. La masse de connaissances accumulée, de même que les outils associés, est relativement évoluée ; toutefois, la capacité d'exploitation de ces informations à grande échelle et à la vitesse requise est limitée. Et faute de pouvoir réaliser une investigation immédiate portant sur des indicateurs d'attaques spécifiques, à l'échelle de l'entreprise, les équipes d'intervention manquent d'envergure dans leurs initiatives de recherche et de réponse aux incidents. Ces dernières sont en général limitées artificiellement de manière à répondre aux exigences de délais, ce qui se traduit par des carences importantes dans l'intervention. Elles se heurtent aux limites des outils actuels, de sorte que les équipes d'intervention elles-mêmes s'en trouvent handicapées dans leur travail.

Un outil complet de détection et de réponse aux incidents pour les terminaux

McAfee Active Response assure une détection continue des menaces avancées et une réponse aux incidents immédiate pour permettre aux équipes de sécurité de surveiller l'état de protection, d'améliorer le niveau de détection et d'étendre les capacités d'intervention. Pour ce faire, la solution dispose de fonctions telles que la découverte proactive, l'analyse détaillée, l'investigation numérique, la génération de rapports complets ainsi que le traitement des alertes et l'exécution des actions suivant une échelle de priorités. Optimisé de manière à répondre à des critères rigoureux en matière de détection et de réponse aux incidents pour les terminaux, McAfee Active Response emploie des collecteurs de données prédéfinis et personnalisables par l'utilisateur pour mener des recherches approfondies sur tous les systèmes. L'objectif est d'identifier non seulement les indicateurs d'attaque présents dans des processus actifs, mais également ceux en sommeil et même ceux qui ont déjà été supprimés. McAfee Active Response permet de rechercher les indicateurs d'attaque au moment présent, mais aussi de définir des alertes et des actions conformes aux objectifs de sécurité, par l'intermédiaire de déclencheurs fournissant des instructions si ces indicateurs se manifestent à nouveau à l'avenir.

McAfee Active Response est la preuve de l'efficacité de l'architecture de sécurité intégrée de McAfee, conçue pour neutraliser davantage de menaces plus rapidement et en mobilisant moins de ressources dans un monde toujours plus complexe. La solution vous offre une visibilité continue et des informations pertinentes sur

Configuration système requise

Configuration matérielle minimale
Le serveur peut être installé sur une machine virtuelle si nécessaire. La configuration matérielle minimale recommandée pour le serveur McAfee Active Response est la suivante :

- 4 processeurs Intel Xeon X5675, 3,07 GHz
- 8 Go de mémoire RAM
- SSD 120 Go

Infrastructure de services requise

- McAfee ePO 5.1.1 ou version ultérieure
- McAfee Agent 5.0 (extension) ou version ultérieure
- Data Exchange Layer 2.0.0.405 (logiciel de courtage) ou version ultérieure

Navigateurs web pris en charge

- Microsoft Internet Explorer 9 et versions ultérieures
- Google Chrome 17 et versions ultérieures
- Mozilla Firefox 10.0 et versions ultérieures

Infrastructure client requise

- McAfee Agent 5.0.0.2710 ou version ultérieure pour terminaux Linux
- McAfee Agent 5.0.0.2610 ou version ultérieure pour terminaux Microsoft Windows
- Data Exchange Layer 2.0.0.405 (clients) ou version ultérieure pour tous les terminaux managés

vos terminaux, pour que vous puissiez identifier plus rapidement les compromissions. Elle procure en outre les outils nécessaires pour corriger les problèmes au plus vite et de la façon la plus efficace pour votre entreprise. La gestion est assurée par McAfee® ePolicy Orchestrator® (McAfee ePO™) en association avec la couche d'échange de données Data Exchange Layer (DXL) : vous disposez ainsi d'une évolutivité et d'une extensibilité unifiées, sans être obligé de faire appel à du personnel supplémentaire pour administrer le produit.

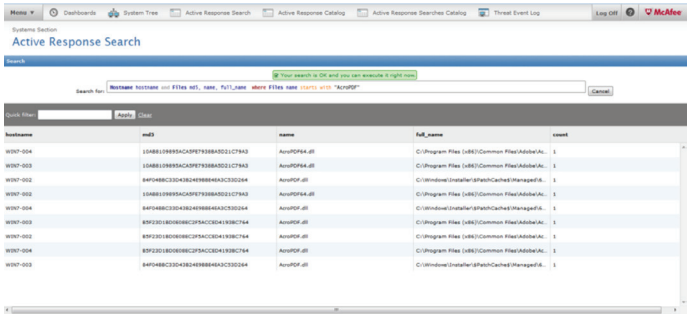

Figure 1. Interface utilisateur de la recherche McAfee Active Response

Fonctionnalité	Avantage	Avantages pour les clients	Différenciation
Collecteurs	Les collecteurs permettent aux utilisateurs de trouver et de visualiser des données précises sur leurs systèmes.	Les collecteurs offrent des fonctionnalités permettant des recherches approfondies sur les systèmes. Ils assurent une visibilité sur les attaques ou compromissions critiques potentielles, afin de recueillir et de visualiser des données issues de ces systèmes. À l'aide de divers langages de script courants, les utilisateurs peuvent personnaliser facilement leurs propres collecteurs et réponses aux incidents, ce qui optimise la configuration et l'adaptation.	Non seulement McAfee Active Response détecte les fichiers exécutables ou en cours d'exécution, mais il identifie aussi le code en sommeil et même le code supprimé par le pirate pour effacer toute trace de son passage. McAfee Active Response peut rechercher des fichiers, des flux réseau, des entrées de Registre et des mappages de processus.
Déclencheurs	Les déclencheurs permettent aux responsables de la sécurité de surveiller en continu un événement ou changement d'état critique avec un jeu d'instructions valable tant au moment présent qu'à l'avenir.	Les mesures d'intervention sont activées par un déclencheur défini à l'avance, générant un événement ou exécutant des actions. McAfee Active Response est capable d'agir au-delà des pics d'activité statiques et d'opérer en mode continu de réponse aux incidents.	McAfee Active Response peut détecter les menaces dans l'immédiat et déclencher des actions pour faire face aux menaces susceptibles de se manifester à l'avenir.
Réactions	Les réactions consistent en des actions préconfigurées et personnalisables qui peuvent être appliquées lorsque les conditions d'un déclencheur sont remplies. Cela vous permet de débusquer et de neutraliser les menaces.	Les réactions permettent aux utilisateurs d'exécuter certaines actions, telles que rechercher des fichiers supprimés du système par hachage (MD5 et SHA1), déterminer si des hôtes sont activement connectés à une adresse IP ou se sont connectés à une adresse IP par le passé, ou rechercher des fichiers malveillants non-PE qui n'ont fait l'objet d'aucun accès ou n'ont pas été déclenchés sur le système (recherche d'un PDF malveillant sur un système où il a été copié dans le système de fichiers sans être ouvert).	McAfee Active Response est préconfiguré pour agir sur la base des résultats de recherche et tenir compte d'actions personnalisées définies par l'utilisateur afin de répondre à un besoin spécifique.

Configuration système requise (suite)

Systèmes d'exploitation clients pris en charge

- Microsoft Windows
  - Windows 8.0 version de base (32 et 64 bits)
  - Windows 8.1 version de base U1 (32 et 64 bits)
  - Windows Server 2012 version de base R2 U1 (64 bits)
  - Windows Server 2008 R2 Entreprise SP1 (64 bits)
  - Windows Server 2008 R2 Standard SP1 (64 bits)
  - Windows 7 Entreprise jusqu'au SP1 (32 et 64 bits)
  - Windows 7 Professionnel jusqu'au SP1 (32 et 64 bits)
- CentOS 6.5 (32 bits)
- RedHat 6.5 (32 bits)

Fonctionnalité	Avantage	Avantages pour les clients	Différenciation
Gestion centralisée à l'aide du logiciel McAfee ePO	Cet environnement à console unique offre des fonctions complètes de gestion et d'automatisation.	Les administrateurs peuvent exploiter McAfee ePO au sein de l'architecture de sécurité intégrée de McAfee pour exécuter des réponses automatisées en fonction de déclencheurs et de résultats de recherche, et pour juguler les menaces. La gestion unifiée offre une visibilité accrue sur la sécurité, sans charge d'administration supplémentaire. Ainsi, les aspects opérationnels sont simplifiés et l'investissement en temps du personnel administratif est réduit.	La gestion et l'intervention à partir d'une console unique constituent un facteur de différenciation important. Nous pouvons ainsi protéger de manière centralisée une variété de plates-formes avec une série de contrôles de sécurité puissants, dont ceux de McAfee Active Response.
Architecture de sécurité intégrée	L'architecture de sécurité intégrée exploite notre couche Data Exchange Layer pour rationaliser la communication avec d'autres produits de McAfee.	Grâce aux concepts novateurs, aux processus optimisés et aux recommandations pratiques de l'architecture de sécurité intégrée de McAfee, McAfee Active Response réduit les risques et le temps de réponse des entreprises, tout en allégeant les frais généraux et les coûts d'exploitation du personnel.	

En savoir plus

Pour en savoir plus sur les avantages de McAfee Active Response, consultez notre site à l'adresse : **www.mcafee.com/fr/products/active-response.aspx**.

McAfee
Together is power.

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