McAfee Cloud Threat Detection

Renforcement des protections McAfee® pour déterminer la dangerosité des logiciels malveillants avancés et exposer les menaces

Un large éventail d'outils d'analyse McAfee récents, dont les solutions d'apprentissage automatique, permettent d'identifier les logiciels malveillants et de passer directement à l'action, en mettant à jour les défenses pour contrer les attaques similaires futures.

Les entreprises mènent un combat incessant face à des logiciels malveillants toujours plus intelligents conçus pour contourner les systèmes de défense traditionnels. Les solutions de détection avancées sont utiles, mais elles peuvent paraître complexes et onéreuses pour des entreprises disposant d'effectifs et de ressources de sécurité limités. En outre, comme la plupart ne s'intègrent pas avec l'infrastructure de protection, l'entreprise reste plus longtemps vulnérable tandis que les équipes d'intervention tentent de trouver la parade.

De quoi les entreprises ont-elles besoin ? D'une solution de détection avancée abordable et ultrasimple à déployer et à utiliser : McAfee® Cloud Threat Detection. Ce nouveau service pratique s'intègre avec les solutions de sécurité McAfee existantes pour déterminer la dangerosité des logiciels malveillants avancés et exposer les menaces furtives. Comme il s'agit d'un service de cloud, il vous permet de tirer parti de ressources de calcul considérables capables d'appliquer les dernières techniques d'analyse. Vous pouvez ainsi améliorer votre capacité de détection et valoriser vos investissements de sécurité existants.

Une détection intégrée à la protection

Les solutions McAfee constituent votre première ligne de défense. Elles détectent les logiciels malveillants connus et probables grâce notamment à des outils avancés d'émulation et d'analyse de la réputation. Et si elles ne parviennent pas à déterminer si un fichier est malveillant, elles peuvent le transférer vers le cloud pour une analyse plus poussée.

Des ordinateurs en butte à des logiciels malveillants émergents et furtifs

Le service McAfee Cloud Threat Detection a recours à des moteurs d'analyse statiques pour extraire les détails des fichiers. Grâce à la prise en charge d'un très large éventail de types de fichiers, ils fournissent tout le contexte nécessaire concernant les logiciels « gris » (greywares) et identifient de façon précise les fichiers malveillants et non infectés. En plus, le service procède également à une analyse comportementale lors de l'exécution du fichier dans un environnement restreint (sandbox). Toutes les actions du logiciel malveillant sont enregistrées, examinées et évaluées pour déterminer l'intention malveillante. Le fichier a-t-il généré un

Principaux avantages :

- Réduction du risque de dommages posé par les menaces inconnues à votre entreprise
- Exploitation de la puissance des Big Data et de l'apprentissage automatique
- Rentabilisation des investissements en sécurité
- Simplification du déploiement de l'analyse des menaces avancées

dossier aléatoire, écrit un nouveau fichier dans celui-ci et supprimé le fichier d'origine ? Dissimule-t-il des transmissions vers des URL inconnues ou suspectes dans le trafic vers des sites connus comme Google, Amazon ou Facebook ? Ce ne sont que quelques exemples de comportement que le service McAfee Cloud Threat Detection peut utiliser pour classer un fichier inconnu. Ces processus mettent également au jour les métadonnées, les URL, les noms de fichier, les emplacements de dossiers, etc. qui sont ensuite communiqués aux clients afin qu'ils puissent enquêter et déterminer si d'autres ordinateurs ont été compromis.

Apprentissage automatique supervisé

Géré et optimisé par McAfee Labs, le cycle d'analyse s'appuie à chaque étape sur les connaissances de nos analystes, les grands volumes de données (Big Data) et l'apprentissage automatique. Les connaissances issues de plus de 25 années de collecte et d'analyse de données et de 2 milliards de fichiers ont contribué au développement et à l'apprentissage de modèles de classification exhaustive dans notre système de Big Data dans le cloud. Des recherches poussées et l'interprétation constante des résultats d'inspection alimentent notre système d'apprentissage automatique pour affiner ces modèles à mesure que les techniques et les comportements des logiciels malveillants évoluent.

La précision avant tout

L'expérience nous a enseigné qu'un faux négatif ou positif peut avoir des répercussions graves et coûter cher. C'est pourquoi nos systèmes incluent des mécanismes de contrôle et d'évaluation qui comparent les résultats aux certificats de signature et fichiers système les plus critiques afin de garantir l'authenticité et la fiabilité des verdicts. Au terme de la détection des menaces émergentes par des outils d'analyse avancés, nous comparons et recoupons les résultats avec des artefacts de logiciels malveillants ainsi que des attributs contextuels et comportementaux pour minimiser les faux positifs. C'est là un des avantages majeurs de l'association de l'analyse dans le cloud et de nos ressources antimalware étendues.

La détection en action

McAfee Cloud Threat Detection communique chaque verdict au système d'origine, qui applique alors une stratégie telle que la mise en quarantaine d'un ordinateur ou l'activation de mécanismes de protection pour contrer des attaques similaires. Des indicateurs de compromission et des rapports détaillés facilitent l'investigation et fournissent les informations requises pour répondre à l'attaque et en corriger les effets. Les menaces identifiées permettent de mettre à jour les réputations dans McAfee Global Threat Intelligence (McAfee GTI) de façon à accélérer la protection de toutes les entreprises avec des solutions intégrées avec McAfee GTI. La fonctionnalité de soumission manuelle favorise les investigations et permet aux analystes de transférer facilement les fichiers pour une analyse ponctuelle.

Solutions intégrées

- McAfee® ePolicy Orchestrator® Cloud
- McAfee Network Security Platform
- McAfee Threat Intelligence Exchange
  - McAfee Endpoint Protection
- McAfee Web Gateway et Web Gateway Cloud Service

Un service rapide, abordable et adapté aux petites entreprises

Comme il s'agit d'un service dans le cloud, il vous suffit de saisir une clé partagée chiffrée dans votre produit McAfee intégré pour activer le service. Si vous possédez des systèmes distribués, il n'est pas nécessaire de réacheminer le trafic vers un centre de données : envoyez-le simplement dans le cloud. Nos experts se chargent de la maintenance régulière et implémentent les mises à jour et les mises à niveau de façon transparente. S'agissant d'un abonnement couvrant toutes les solutions McAfee intégrées dont le prix est fonction du volume, aucun investissement initial n'est nécessaire et le principal obstacle à l'achat pour les PME, à savoir le coût, est éliminé.

Pour en savoir plus, consultez la page **www.mcafee.com/fr/products/cloud-threat-detection.aspx**.

McAfee
Together is power.

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