Cisco AMP pour Endpoints

Détectez les menaces même les plus insidieuses

Presque toutes les solutions de sécurité des terminaux sur le marché prétendent bloquer 99 % des malwares. Mais qu'en est-il du 1 % de menaces qui leur échappe ? Aussi faible soit-il, ce pourcentage peut causer des ravages sur votre réseau. Si vous comptez uniquement sur les technologies classiques ne permettant qu'une action ponctuelle, telles que les antivirus, ces menaces peuvent passer inaperçues pendant des mois.

La protection des utilisateurs est plus importante que jamais

La mobilité et la flexibilité du personnel occupent une place centrale dans les entreprises. Qu'ils soient directement connectés au réseau de leur société ou non, les collaborateurs peuvent désormais travailler à tout moment sur un vaste éventail de terminaux : les ordinateurs portables, les tablettes, les smartphones, etc. Aujourd'hui, les réseaux sont conçus pour permettre l'accès à distance même aux données les plus sensibles.

Malheureusement, les hackers exploitent également ce filon. Ils ciblent les collaborateurs et les données précieuses auxquelles ils accèdent sur leurs terminaux avec des menaces spécialement conçues pour contourner les outils classiques de sécurité. Comment votre entreprise peut-elle donc continuer à innover, à s'engager sur la voie du numérique et à favoriser la mobilité sans nuire à la sécurité ?

Une solution de nouvelle génération pour la sécurité de vos terminaux

Cette solution de nouvelle génération pour la sécurité de vos terminaux combine des fonctions de prévention, de détection et de traitement des incidents, en exploitant la puissance de l'analytique cloud. Cisco® AMP pour Endpoints est un connecteur léger qui fonctionne sur les équipements Windows, Mac, Linux, Android et iOS. Cette solution peut utiliser le cloud public ou être déployée dans un cloud privé. AMP surveille et analyse en continu toute activité liée aux fichiers et aux processus sur votre réseau afin de détecter les 1 % de menaces que les autres solutions n'identifient pas. AMP ne perd jamais de vue l'emplacement d'un fichier ni son activité. Si un fichier qui semblait sain lors de l'inspection initiale présente un comportement malveillant, AMP possède un historique complet du comportement de la menace afin de la détecter, de la maîtriser et de l'éliminer.

Bénéfices

Cisco® AMP pour Endpoints assure la protection complète de vos terminaux contre les attaques les plus sophistiquées. Il empêche les attaques et bloque les malwares au point d'entrée, puis détecte, maîtrise et corrige rapidement les menaces avancées qui contournent les premières lignes de défense et s'infiltrent dans votre réseau.

- **Prévenir :** renforcer les défenses en utilisant des informations détaillées sur les menaces à l'échelle mondiale et bloquer en temps réel les malwares sans fichier ou cachés dans des fichiers.
- **Détecter :** surveiller et enregistrer en continu toutes les activités des fichiers pour détecter rapidement les programmes malveillants furtifs.
- **Réagir :** accélérer les recherches et éliminer automatiquement les malwares sur tous les PC, Mac, systèmes Linux, serveurs et terminaux mobiles (Android et iOS).

Étapes suivantes

Contactez un conseiller ou un partenaire Cisco pour tout connaître de Cisco AMP pour Endpoints et savoir comment protéger votre entreprise des cyberattaques avancées. Rendez-vous sur notre site web pour en savoir plus.

C45-731874-12 04/18

Bloquez les malwares

AMP pour Endpoints repose sur une approche cloud, impiquant la collecte d'informations sur les menaces et l'analyse des fichiers. Le cloud AMP reçoit en permanence des données en provenance de Cisco Talos et de Cisco Threat Grid, le plus grand ensemble de flux d'informations sur les menaces en temps réel sur le marché. Cette approche cloud permet à AMP d'analyser les fichiers en fonction des toutes dernières informations disponibles sur les menaces afin de vous protéger contre les malwares, qui évoluent constamment.

Comme la lutte contre les malwares requiert des techniques distinctes, AMP comporte plus de 15 mécanismes intégrés de détection et de protection pour empêcher que les attaques ne nuisent à votre entreprise. Parmi ces mécanismes figurent la protection contre les activités malveillantes (qui bloque les ransomwares), la prévention des exploits sans fichier, l'analyse des nouvelles menaces via l'apprentissage automatique, le sandboxing et bien plus encore. Si un fichier semble suffisamment sûr pour passer tous ces mécanismes, AMP l'accepte, puis le surveille en permanence afin de s'assurer qu'il n'implique aucun comportement malveillant.

Éliminez les angles morts

Avec Cisco AMP pour Endpoints, vous bénéficiez d'une vue d'ensemble de vos terminaux, quel que soit leur système d'exploitation. AMP offre également une meilleure visibilité sur le trafic anormal lié aux objets connectés (IoT) sur lesquels aucun connecteur ne peut être déployé, y compris les imprimantes, les thermostats et les caméras de sécurité.

Nous savons que les cybercriminels se limitent rarement à un seul vecteur d'attaque. AMP pour Endpoints partage les informations sur les menaces dans l'ensemble de votre environnement, unifiant ainsi la sécurité entre les terminaux, le réseau, la messagerie, le cloud et le web. Grâce à ces intégrations, AMP permet de détecter une menace dans une zone de votre environnement, puis de la bloquer automatiquement à tous les emplacements où la menace apparaît. AMP compare automatiquement les fichiers, les données de télémétrie, le comportement et les activités pour contrer les attaques avancées de manière proactive sur tous les vecteurs d'attaque possibles.

Détectez les menaces inconnues

La technologie intégrée de sandboxing d'AMP analyse le comportement des fichiers suspects et les compare à d'autres sources d'informations. L'analyse des fichiers génère des informations détaillées pour mieux comprendre comment maîtriser la propagation des attaques et bloquer les attaques futures.

Lorsqu'un fichier est jugé malveillant, AMP réduit considérablement le délai et les ressources nécessaires pour l'analyser. Il fournit automatiquement des informations répondant aux questions les plus pressantes, notamment :

- Que s'est-il passé ?
- D'où provient ce malware ?
- Où est-il allé ?
- Quelle action le malware est-il en train d'effectuer ?
- Comment l'arrêter ?

La console de gestion web d'AMP permet de bloquer l'exécution d'un fichier sur tous les terminaux en quelques clics. Étant donné que Cisco AMP connaît tous les terminaux sur lesquels le fichier est passé, il peut également mettre le fichier en quarantaine pour tous les utilisateurs. Avec AMP, éliminer un programme malveillant est une véritable intervention chirurgicale qui ne provoque pas de dommage collatéral sur les systèmes ni sur l'entreprise.