Messages AMP Everywhere

Le problème	Les entreprises sont sous attaque permanente et chaque jour des incidents se produisent, les plus graves faisant les gros titres des médias. Une communauté internationale de hackers crée des programmes malveillants sophistiqués qu'elle diffuse par le biais d'attaques et de vecteurs multiples dans les entreprises de toutes tailles. Ces attaques dynamiques peuvent échapper aux meilleurs outils de détection ponctuelle, comme les anciens pare-feu et systèmes de prévention des intrusions. À la base, ces outils ont été conçus pour inspecter le trafic et les fichiers au point d'entrée du réseau, une mission qu'ils accomplissent efficacement. Toutefois, ils n'offrent qu'une visibilité minimale sur l'activité des programmes malveillants. Dans l'incapacité de se protéger contre ce qu'ils ne voient pas, les professionnels de la sécurité ne peuvent pas constater l'étendue d'éventuelles intrusions, ni intervenir rapidement pour maîtriser les programmes malveillants avant qu'ils ne provoquent des dommages considérables. La détection ponctuelle ne sera jamais efficace à 100 % à elle seule. Il suffit qu'un fichier malveillant passe à travers les mailles du filet pour que la sécurité de votre réseau soit compromise. L'entreprise a besoin d'une solution capable de prendre en compte efficacement tout le cycle de vie des programmes malveillants à tous les stades de l'attaque. Celle-ci devra détecter les incidents et y répondre, sans grever le budget ni nuire à l'efficacité opérationnelle.
Le message	Les programmes malveillants sont de plus en plus complexes, les attaques ciblées se multiplient et les cybercriminels commettent leurs méfaits par le biais de multiples vecteurs. D'après le rapport annuel Cisco 2015 sur la sécurité, les cybercriminels : • changent très fréquemment de tactiques et d'outils, disparaissent d'un réseau avant d'être arrêtés ou changent rapidement de méthode pour y pénétrer ; • conçoivent des programmes malveillants qui reposent sur des outils en lesquels les utilisateurs ont confiance ou qu'ils considèrent comme inoffensifs afin d'infecter durablement leurs machines, sous leurs propres yeux ; • s'emploient à dissimuler leur présence ou à se fondre dans le paysage de l'entreprise ciblée, en prenant parfois des semaines ou des mois pour s'infiltrer dans les bases de données et l'infrastructure. Et ce n'est que lorsqu'ils sont prêts qu'ils passent à l'action. Les entreprises doivent adopter des systèmes de protection aussi complets que les attaques dont elles sont victimes. Ces solutions doivent être capables d'éradiquer les programmes malveillants évasifs, d'identifier les attaques connues et les comportements malveillants, et de fournir une visibilité sur les multiples points d'entrée dans l'entreprise, depuis les appareils mobiles et les terminaux jusqu'aux points de contrôle du réseau. Pour gagner la bataille contre les programmes malveillants toujours plus sophistiqués, la protection doit être omniprésente, permanente et rétrospective. La solution Cisco® Advanced Malware Protection (AMP) ne se limite pas à une simple détection ponctuelle. Elle contrôle et protège de façon *totale* et *permanente* les fichiers et leurs activités, à la recherche des premiers signes de comportements malveillants. Elle vous offre la visibilité et le contrôle nécessaires pour intercepter les malwares avancés qui auraient échappé aux autres couches de sécurité. Votre entreprise est entièrement protégée tout au long du processus, c'est-à-dire avant, pendant et après l'attaque. La solution intègre de nombreuses fonctionnalités : une détection continue et de prise en compte des attaques de type « zero-day », des stratégies évoluées d'analyse, une grande capacité d'information sur les programmes malveillants et des fonctionnalités puissantes qui peuvent être déployées sur plusieurs vecteurs d'attaque dans le but de se protéger de manière proactive et réagir rapidement aux attaques les plus complexes.
La solution	Cisco AMP est une solution intégrée qui repose sur la collecte d'informations. Elle vise à analyser les programmes malveillants sophistiqués et à s'en prémunir. Disponible sur abonnement, elle se gère via une console en ligne facile à utiliser et se déploie sur de nombreux vecteurs d'attaque et points de contrôle en tant que : • solution pour réseaux, intégrée dans les pare-feu Cisco ASA et dans les appliances de sécurité du réseau Cisco FirePOWER qui couvrent une grande variété de tailles de réseaux et de capacités de traitement ; • solution pour terminaux PC, Mac, terminaux mobiles et environnements virtuels ; • appliance virtuel de cloud privé sur site, au sein d'environnements soumis à des contraintes drastiques en matière de confidentialité des données ; • fonctionnalité intégrée dans les appliances de sécurisation du cloud, de la messagerie et du web ; • solution autonome de gestion des données sur les attaques et d'analyse dynamique des programmes malveillants via AMP Threat Grid, déployée comme appliance ou sur la base d'un abonnement à un service dans le cloud, et développée grâce à la technologie issue de l'acquisition de ThreatGRID par Cisco en juin 2014.

La solution propose plus qu'une simple stratégie de détection et assure une protection à tous les stades de l'attaque : avant, pendant et après.

Avant l'attaque, AMP renforce la protection du réseau contre les attaques connues et inconnues grâce aux informations collectées à l'échelle mondiale. La base de sécurité adaptative et collective Cisco et les flux de contenu de grande qualité d'AMP Threat Grid vous fournissent des données complètes et contextuelles pour vous protéger contre les attaques d'aujourd'hui.

Pendant l'attaque, la solution AMP associe ces informations à des signatures de fichiers connues et à la technologie d'analyse dynamique des programmes malveillants de Cisco AMP Threat Grid. Elle peut ainsi identifier et bloquer les fichiers qui enfreignent les règles et les fichiers malveillants qui tentent d'infiltrer le réseau.

Cisco AMP se démarque par ses actions après l'attaque. La solution analyse en permanence l'ensemble des fichiers et du trafic à la recherche de comportements malveillants même après l'inspection initiale. Désormais, en cas de comportement malveillant d'un fichier après l'incident, la solution le détecte et offre aux équipes chargées de la sécurité la visibilité et le contrôle nécessaires pour y répondre rapidement. Vous bénéficiez ainsi d'une protection rétrospective, c'est-à-dire la faculté de consigner l'activité de chaque fichier sur le système, puis de remonter jusqu'à l'origine d'une menace potentielle, d'examiner son comportement et de disposer des fonctionnalités de traitement intégrées visant à l'éliminer.

Détecter les incidents de manière continue

- *Une visibilité améliorée* : la solution Cisco AMP va bien au-delà de la détection ponctuelle. Elle capture et analyse en continu l'activité des fichiers et le trafic. Vous bénéficiez ainsi d'une protection rétrospective qui consiste à revenir en arrière et à étudier les processus, l'activité des fichiers et les communications afin de cerner l'ampleur d'une infection, de déterminer ses causes premières et de l'éliminer.

- *Une analyse continue* : le système Cisco AMP déclenche des alertes rétrospectives s'il identifie un fichier malveillant, même si ce dernier a déjà transité sur le réseau ou le terminal depuis plusieurs heures ou plusieurs jours. Vous pouvez ainsi prendre les mesures qui s'imposent et minimiser les dommages.

- *Une détection et un blocage des tentatives d'exploit* : si elle est déployée en ligne, la solution AMP est à même de détecter et de bloquer des tentatives d'attaque côté client. Elle vous protège également contre les tentatives d'exploit qui visent Adobe Acrobat, Java, Flash et d'autres applications clientes couramment ciblées.

Répondre et réagir

- *Une détection des attaques connues et inconnues* : la solution bloque l'entrée des fichiers malveillants dans le système et analyse localement les fichiers inconnus. Les fichiers transmis à AMP Threat Grid sont analysés grâce à des indicateurs comportementaux et à des milliards d'objets malveillants.

- *Une réponse rapide* : Cisco AMP permet d'identifier facilement l'enchaînement des événements associés à la propagation des programmes malveillants pour contenir rapidement le problème. AMP vous permet de cibler des applications, des fichiers, des programmes malveillants et d'autres causes premières. Briser la chaîne d'attaque se fait rapidement et simplement.

- *L'automatisation du confinement* : en suivant l'activité du web, des e-mails, des terminaux et des appareils du réseau, AMP reconnaît automatiquement les fichiers et les applications, et se charge ensuite d'effectuer un filtrage généralisé en appliquant les politiques de contrôle prédéfinies.

Se donner les moyens de sécuriser

- *L'amélioration de vos investissements dans vos solutions de sécurité* : AMP Threat Grid s'intègre avec vos technologies de sécurité pour automatiser l'envoi d'informations à des fins d'analyse et de création de rapports.

- *Une corrélation puissante* : la solution AMP illustre les risques associés à une attaque en cours. Elle crée des listes hiérarchisées et automatisées des appareils potentiellement infectés en se basant sur des informations relatives aux événements émanant de plusieurs sources.

	• *Une analyse contextuelle des programmes malveillants* : la solution AMP identifie l'activité des programmes malveillants, notamment le trafic HTTP et DNS associé, les flux TCP/IP, les processus affectés et l'activité du registre. Les équipes en charge de la sécurité peuvent ainsi en apprendre davantage sur les risques potentiels pour leurs réseaux et réduire le nombre d'incidents causés par des programmes malveillants. Toutes ces fonctionnalités vous offrent une visibilité complète sur le réseau dans son ensemble et vous fournissent les informations nécessaires pour répondre aux questions essentielles, notamment : • D'où proviennent ces programmes malveillants ? • Quels systèmes ont été affectés ? • Que fait le fichier malveillant ? • Comment l'arrêter ? Grâce à ces informations, vous pouvez prendre des décisions plus éclairées, réduire considérablement le temps consacré à la détection, au confinement et à l'élimination des programmes malveillants de votre réseau, et enfin éviter de futures attaques similaires. Votre entreprise profite donc d'une protection plus efficace et plus complète. **Présentation de la solution en 100 mots** La solution Cisco Advanced Malware Protection (AMP) protège le réseau avant, pendant et après une attaque. Elle propose une détection continue, des alertes rétrospectives, une capacité proactive de renseignement, des stratégies évoluées d'analyse et des fonctionnalités puissantes pour vous protéger de manière proactive et répondre rapidement aux plus complexes des attaques d'aujourd'hui. Avant l'attaque, elle renforce les défenses du réseau en utilisant la grande base mondiale d'informations contextuelles sur les attaques. Pendant l'attaque, elle utilise ces informations ainsi que les signatures de fichiers connues et des fonctions d'analyse dynamique pour bloquer l'intrusion de programmes malveillants. Après l'attaque, Cisco AMP affiche les données issues de l'historique des activités des fichiers pour une visibilité et un contrôle inédits sur l'environnement. **Présentation de la solution en 50 mots** La solution Cisco AMP protège le réseau avant, pendant et après l'attaque. Elle propose une détection continue, des alertes rétrospectives, une capacité proactive d'information, des stratégies évoluées d'analyse et des fonctionnalités puissantes qui se déploient sur les multiples vecteurs d'attaque pour vous protéger de manière proactive et répondre rapidement aux plus complexes des attaques d'aujourd'hui. **Présentation de la solution en 25 mots** Cisco AMP propose une détection continue, des alertes rétrospectives, une capacité proactive d'information, des stratégies évoluées d'analyse et des fonctionnalités puissantes pour vous protéger de manière proactive et répondre rapidement aux plus complexes des attaques d'aujourd'hui.
Thèmes et messages clés	**<u>Informations générales sur la solution AMP</u>** La solution AMP détecte les attaques et y répond. • Elle ne se limite pas à une simple détection ponctuelle. Elle surveille le système en permanence, identifie les comportements malveillants et fournit des moyens de réponse. • La solution AMP permet aux entreprises de mieux gérer les incidents grâce aux fonctions de sécurité rétrospective. • Améliorez la détection des attaques grâce aux informations les plus à jour sur les programmes malveillants d'AMP Threat Grid qui alimentent votre infrastructure de sécurité. • La solution AMP est conçue pour empêcher les attaques et éradiquer rapidement les fichiers malveillants, et vous protège à tous les stades de l'attaque. **<u>Messages clés relatifs aux fonctionnalités</u>** **Détection continue et sécurité rétrospective** La solution AMP ne se limite pas aux fonctions classiques de détection ponctuelle. Elle propose des alertes rétrospectives et une analyse dynamique des programmes malveillants connus et inconnus afin de bloquer ceux qui tentent de passer au travers de vos systèmes de défense. Même si les fichiers contournent un point de

contrôle de sécurité, la solution continue de surveiller et d'analyser le trafic et l'activité de tous les fichiers (quels qu'ils soient) sur les terminaux, les appareils mobiles et le réseau, tout en consignant chacun de leurs mouvements. Si un fichier inconnu ou précédemment considéré comme inoffensif commence à avoir un comportement suspect, Cisco AMP envoie immédiatement aux équipes de sécurité alerte rétrospective et indicateur de compromission, tout en leur indiquant exactement ce qui s'est produit. Vous pouvez tout savoir sur cette attaque : la provenance du programme malveillant, ses diverses destinations, les systèmes affectés et l'activité du malware à l'instant présent. Cette fonctionnalité rétrospective, c'est-à-dire la faculté de consigner l'activité de chaque fichier sur le système, puis de remonter jusqu'à l'origine d'un malware potentiel et de voir son comportement, permet aux équipes de sécurité de bénéficier de la visibilité nécessaire pour identifier rapidement une attaque et des moyens de l'éliminer. Elle peut considérablement accélérer l'identification, la désactivation et l'éradication du programme malveillant (même les attaques de type « zero-day ») et empêcher des attaques similaires de se reproduire.

Nouveautés relatives au lancement du 7 avril

- Les utilisateurs d'AMP pour Endpoints peuvent désormais envoyer leurs propres indicateurs de compromission (IoC) depuis les terminaux pour détecter des attaques ciblées. Ces « IoC de terminaux » permettent aux équipes de sécurité d'effectuer des enquêtes plus précises sur les attaques complexes moins connues et propres à leur environnement. Les attaques ciblées se multiplient et les hackers créent des programmes malveillants qui visent des applications et des entreprises spécifiques. Prendre en compte les IoC de terminaux une protection inédite.

- La fonctionnalité de faible prévalence de la solution AMP pour terminaux affiche tous les fichiers qui ont été exécutés dans l'entreprise par nombre croissant d'instances. En général, les fichiers exécutés par un grand nombre d'utilisateurs ne posent pas de problème, tandis que ceux exécutés uniquement par un ou deux utilisateurs peuvent être malveillants. La fonctionnalité de faible prévalence peut vous aider à éliminer les attaques non détectées auxquelles seul un petit nombre d'utilisateurs a été exposé. Vous pouvez ensuite utiliser l'outil d'AMP retraçant la trajectoire des programmes pour tout savoir sur le fichier, et la fonctionnalité d'analyse d'AMP Threat Grid pour déterminer si les fichiers de faible prévalence sont effectivement des menaces.

Informations sur les menaces et analyses avancées

Cisco AMP utilise la plus vaste base de données et d'analyses sur les attaques collectées en temps réel, fournie par la base de sécurité adaptative et collective Cisco, notamment par Talos Security Intelligence and Research Group. La solution met en corrélation automatiquement et continuellement à la fois les fichiers, le comportement, les données télémétriques et les activités avec cette solide base d'informations contextuelles afin de détecter les programmes malveillants et les indicateurs de compromission. Les fonctions d'analyse automatisées d'AMP profitent aux équipes de sécurité qui consacrent ainsi moins de temps à rechercher les signes d'une attaque et bénéficient en permanence d'un panorama des menaces à jour pour rapidement comprendre, hiérarchiser, bloquer et éradiquer les attaques sophistiquées qui touchent leur entreprise.

Nouveautés relatives au lancement du 7 avril

- L'intégration récente d'AMP Threat Grid dans les solutions Cisco AMP vous donne accès à des flux de contenus très précis sur les attaques, ce qui vous permet de générer des informations contextuelles propres à votre entreprise. Les flux d'informations sont aux formats standard pour s'intégrer en toute fluidité dans les solutions de sécurité existantes, améliorant considérablement la capacité de l'entreprise à détecter et à empêcher d'autres attaques.

- AMP Threat Grid analyse chaque mois des millions d'échantillons en fonction de 350 indicateurs comportementaux, ce qui représente des milliards d'objets. Suite à cela, la solution établit un indice de dangerosité facilement compréhensible pour aider les équipes de sécurité à définir des priorités et à prendre des décisions plus avisées. L'immensité de l'échelle de couverture contre les menaces de tous horizons permet aux équipes de sécurité d'en apprendre davantage sur les risques potentiels pour leurs réseaux et de mieux se protéger des programmes malveillants.

- Selon le rapport annuel de 2015 de Cisco sur la sécurité, les vulnérabilités sont omniprésentes sur le réseau d'une entreprise. Or, les équipes de sécurité ne savent pas comment identifier les hôtes les plus vulnérables ou les failles à éliminer en priorité. La nouvelle fonction relative aux vulnérabilités d'AMP pour terminaux affiche la liste des hôtes qui contiennent un logiciel vulnérable, la liste des logiciels vulnérables sur chaque hôte et les hôtes les plus exposés. Grâce à sa capacité de renseignement sur les

	menaces et à ses outils d'analyse de sécurité, AMP identifie le logiciel vulnérable ciblé par le programme malveillant et l'attaque potentielle associée, et vous fournit une liste des hôtes à traiter par ordre de priorité. **De puissantes fonctionnalités** Disponible sur abonnement, la solution Cisco AMP se gère via une console en ligne facile à utiliser. Vous pouvez la déployer sur plusieurs plates-formes et satisfaire diverses exigences en termes de besoins de performance et de stockage. Vous pouvez la déployer comme bon vous semble, là où elle répond le mieux à vos besoins spécifiques en matière de sécurité. La solution peut être déployée : • En tant que solution réseau : o Intégrée dans un pare-feu dédié Cisco ASA en tant que composant du Cisco ASA avec fonctionnalités FirePOWER (AMP sur ASA avec fonctionnalités FirePOWER) o Intégrée dans les appliances de sécurité du réseau Cisco FirePOWER dédiés couvrant une grande variété de capacités de réseaux et de capacités de traitement (AMP for Networks) • En tant que solution de terminal pour les PC, les Mac, les appareils mobiles et les environnements virtuels (AMP for Endpoints) • En tant qu'appliance virtuel de cloud privé sur site dans des environnements soumis à des contraintes drastiques en matière de confidentialité des données (appliance virtuel de cloud privé AMP) • En tant que fonctionnalité intégrée dans les appliances de sécurisation du cloud, de la messagerie et du web • En tant que solution autonome de gestion des données sur les menaces et d'analyse dynamique des programmes malveillants via AMP Threat Grid, déployée en tant qu'appliance ou sur la base d'un abonnement cloud • En outre, AMP for Endpoint peut désormais être lancé et chargé sur les terminaux à partir de AnyConnect 4.1, la solution VPN d' accès à distance. **Nouveautés relatives au lancement du 7 avril** Réseau • AMP sur ASA doté des fonctionnalités FirePOWER • Appliances AMP for Networks dédiés • Appliance AMP Threat Grid Terminal • Mac Contenu • Améliorations ESA/WSA/CWS Gestion sur site • Cloud privé 2.0
Services de sécurité	Les innombrables fonctionnalités de Cisco AMP peuvent être utilisées en tant que service avec la solution Cisco Managed Threat Defense (MTD). Cisco MTD est une solution de sécurité totalement gérée qui repose sur une analytique prédictive en temps réel pour détecter plus rapidement les attaques, optimiser la sécurité et la maîtrise du réseau, et assurer une protection contre les programmes malveillants sophistiqués sur les réseaux étendus des entreprises. Les services de résolution des incidents de sécurité de Cisco reposent sur les informations collectées par les solutions AMP et Cisco TALOS ainsi que sur l'expertise d'une équipe dédiée afin d'aider les entreprises à se préparer, à gérer, à traiter et à dépasser les attaques rapidement et efficacement.