Livre blanc

Sécurité sur le web : protégez vos données dans le cloud

Présentation

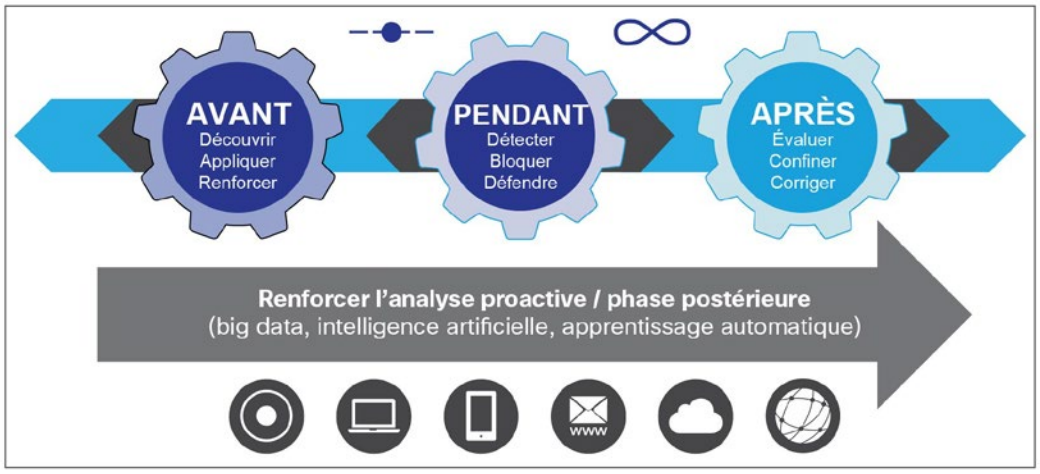
Les équipes de sécurité ne peuvent pas être partout, et pourtant le contexte actuel exige des entreprises qu'elles protègent leurs données sur tous les fronts où une menace risque de se manifester. « Sur tous les fronts », cela inclut les réseaux, les appareils mobiles, les environnements virtuels, le cloud et le data center.

Les menaces modernes sont conçues pour percer chaque défense. Les cybercriminels s'emploient activement à comprendre les types de solutions sécurité déployées. Ils adaptent ensuite le fonctionnement de leurs attaques pour les rendre moins visibles et moins détectables. Selon le **rapport annuel Cisco 2014** sur la sécurité, la plupart de ces acteurs ont pour principal objectif le vol de données à forte valeur.[1]

Parallèlement, l'avènement de l'entreprise multisite et l'émergence de nouveaux modèles commerciaux tels que le cloud computing, la mobilité et les environnements BYOD ont modifié le périmètre de sécurité classique et augmentent la surface d'attaque. Les équipes de sécurité peinent à répondre aux nouvelles exigences. Elles ne savent pas comment catégoriser les menaces à traiter en priorité, et bon nombre d'entre elles leur échappent tout simplement.

Il est dès lors facile de comprendre pourquoi les solutions de sécurité préventives et ciblées ne peuvent garantir une protection adéquate aux entreprises modernes. Aucune méthode de détection n'étant infaillible, certaines menaces sophistiquées et suffisamment furtives parviennent inévitablement à percer toutes les couches d'une défense. Alors, quelle est la réponse ? Des fonctionnalités de sécurité qui permettent une action continue et rétrospective avec la prise en compte du processus d'attaque dans son intégralité, avant, pendant et après.

Figure 1. Le processus d'attaque



[1] Rapport annuel 2014 de Cisco sur la sécurité : http://www.cisco.com/c/en/us/products/security/annual_security_report.html.

© 2015 Cisco et/ou ses filiales. Tous droits réservés. Ceci est un document public de Cisco.

Cisco Cloud Web Security Essentials

Cisco® Cloud Web Security (CWS) permet aux entreprises d'assurer une sécurité continue sur l'ensemble du réseau. Cette solution offre des fonctions leaders sur le marché pour la sécurité et le contrôle des entreprises distribuées. Elle propose l'éventail d'options de déploiement le plus le large actuellement disponible. La version cloud de la solution de sécurisation du web (CWS) permet de sécuriser les terminaux mobiles et les environnements distribués. Elle protège les utilisateurs grâce à des informations sur les menaces collectées au niveau mondial et à des fonctions de défense optimisées. Elle assure également la protection des utilisateurs itinérants.

La solution de sécurisation du web Cisco présente des outils intuitifs pour créer, appliquer et suivre les politiques régissant les communications entrantes et sortantes avec le web. Elle permet aux entreprises d'avoir le contrôle intégral sur les moyens d'accès aux contenus Internet des utilisateurs. En bref, la solution cloud de sécurité du web donne la possibilité d'établir un périmètre sécurisé dans le cloud. Ce périmètre permet de contrôler et d'appliquer des politiques sensibles au contexte détaillées. En outre :

- il bloque les menaces de manière dynamique en temps réel ;
- il protège le réseau et les utilisateurs des contenus web indésirables ;
- il optimise les ressources du réseau en réduisant la congestion de la bande passante ;
- il offre la possibilité d'avoir un contrôle et des rapports exhaustifs sur l'activité en ligne
- il protège l'entreprise contre les fuites de données.

La solution cloud de sécurisation du web (CWS) s'intègre aux pare-feu Cisco, aux routeurs installées dans les succursales et aux logiciels installés chez les clients pour garantir la sécurité quel que soit l'endroit où les utilisateurs travaillent. Tout le trafic, qu'il provienne du siège social, des succursales ou des teminaux des utilisateurs mobiles ou distants, est acheminé dans le réseau global des data centers. Cisco CWS élimine la liaison, accélère le déploiement des fonctionnalités de sécurisation du web et contribue à optimiser les investissements Cisco existants.

Avec la récente acquisition des entreprises spécialistes de la sécurité Sourcefire et Cognitive Security, Cisco est désormais en mesure de proposer une version améliorée de Cisco CWS pour lutter contre les programmes malveillants sophistiqués, en particulier dans la phase postérieure de l'incident, et d'améliorer la détection en temps réel pendant l'attaque. Cisco propose cette solution avec un abonnement Premium facultatif, décrit ci-dessous.

Cisco CWS Premium

Le bundle premium présente toutes les fonctionnalités contenues dans le bundle Essentials, mais offre par ailleurs deux systèmes novateurs de détection de programmes malveillants: Cognitive Threat Analytics (CTA) et Advanced Malware Protection (AMP). Ces systèmes automatisent la recherche des menaces à risque élevé sur le trafic web de l'entreprise. Cisco CWS Premium propose en outre une protection ciblée et des fonctions d'analyse continue et rétrospective pour aider les entreprises à identifier et à résoudre les menaces les plus sensibles. Par ailleurs, il réduit le délai de détection des menaces déjà actives au sein de leurs réseaux.

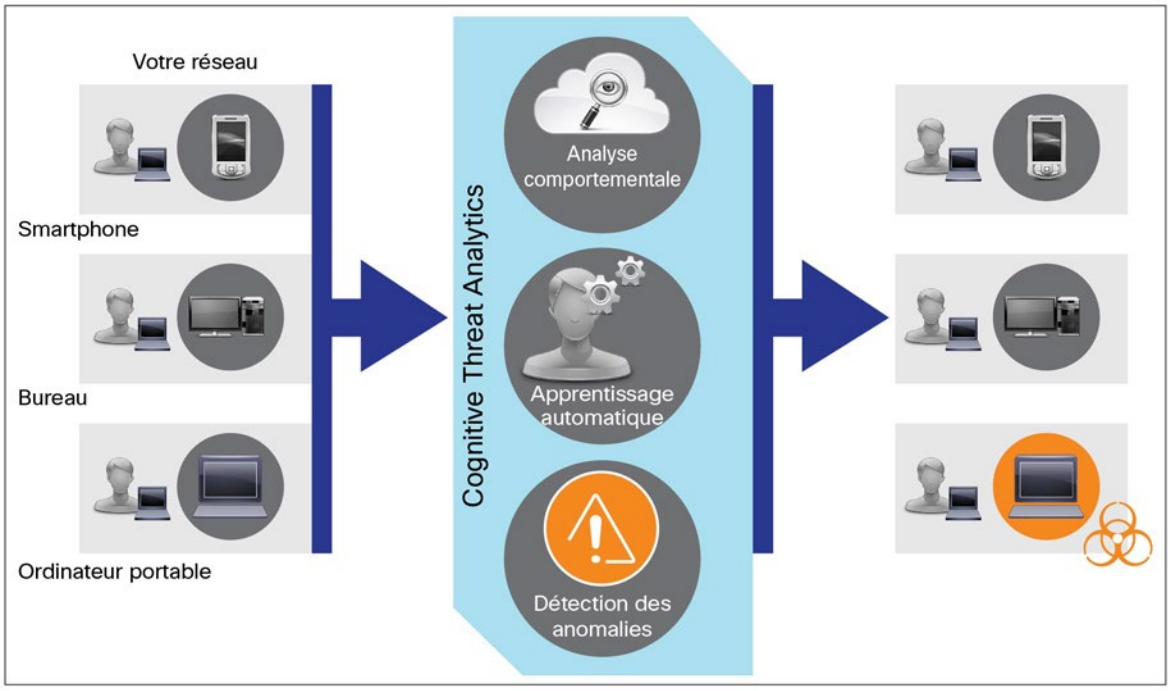
Les équipes de sécurité peuvent désormais assurer une sécurisation continue en protégeant les systèmes tout au long du cycle de l'attaque. La suite de ce document se penche sur ces deux systèmes de détection de logiciels malveillants.

© 2015 Cisco et/ou ses filiales. Tous droits réservés. Ceci est un document public de Cisco.

Cognitive Threat Analytics

Développé par Cognitive Security, Cognitive Threat Analytics (CTA) est un système d'analyse comportementale du réseau en temps quasi réel. Il utilise l'apprentissage automatique et des statistiques avancées pour repérer toute activité inhabituelle sur le réseau, signe d'une infection. Cette solution n'étant pas soumise à des jeux de règles, aucune intervention humaine n'est requise pour « ajuster » la technologie. Dès qu'il est activé, CTA commence à rechercher les menaces. Les données sont corrélées dans le cloud pour améliorer la vitesse, l'agilité et la profondeur des capacités de détection des menaces de CTA.

Figure 2. Présentation de CTA



CTA s'améliore au fil des comportements observés. Il s'adapte au fur et à mesure qu'il identifie de nouveaux biais de commande-contrôle non détectés jusqu'alors par le secteur de la sécurité. Il évalue le comportement des entités (par exemple, d'utilisateurs individuels) sur le réseau et utilise des méthodes d'analyse du comportement pour anticiper le comportement probable de ces entités. CTA utilise des méthodes d'analyse du comportement du réseau à long terme pour mettre en corrélation des activités à première vue isolées. Il compare ensuite ces données corrélées aux comportements d'utilisateurs individuels du réseau du client afin de détecter plus rapidement les menaces.

Peu importe le type de menace détecté, CTA signale le moindre comportement suspect, significatif ou prolongé. CTA fonctionne comme une équipe de sécurité qui tente d'identifier un voleur à l'étalage avant qu'il n'ait pu agir : que fait cette personne de différent par rapport aux autres acheteurs ? Elle porte un grand sac au lieu de pousser un caddie ? Elle tente de sortir par une porte dérobée au lieu de sortir par la porte principale ? Même si le comportement suspect s'avère justifié, cela vaut la peine de vérifier.

© 2015 Cisco et/ou ses filiales. Tous droits réservés. Ceci est un document public de Cisco.

CTA repère les anomalies et oriente ensuite les analystes de sécurité vers les problèmes potentiels, ce qui permet à la fois de réduire leur charge de travail et de définir la priorité des menaces. Il complète également la technologie de sécurité Cisco existante, améliorant la précision de ces solutions et leur capacité à détecter les comportements inconnus ou inhabituels sur le réseau. Les fonctions de sécurité Cisco sont ainsi étendues jusqu'à la phase postérieure de l'attaque. Mais surtout, CTA permet de bénéficier d'une sécurité qui s'adapte à l'évolution constante des menaces.

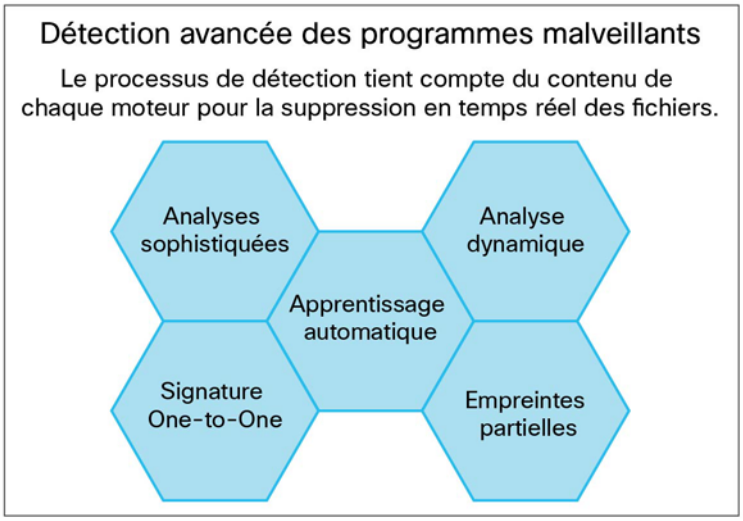
Advanced Malware Protection (AMP)

La solution Advanced Malware Protection (AMP) de Sourcefire est le deuxième système de détection intégré à Cisco CWS Premium. AMP ne se fie pas aux signatures de programmes malveillants, dont la création pour chaque nouveau malware peut prendre des semaines, voire des mois. À la place, il utilise les analyses de réputation de fichiers, de sandboxing et rétrospectives pour identifier et stopper les menaces à tous les stades de l'attaque.

Analyse de la réputation des fichiers

La fonction de réputation des fichiers permet de consulter des bases de données de fichiers afin de déterminer si un fichier est « sain », réputé malveillant ou inconnu. AMP capture une « empreinte » de chaque fichier lorsqu'il transite par le service Cisco CWS et interroge la base cloud de sécurité adaptative et collective de Cisco et Sourcefire pour avoir une note de réputation, ou « score ». Sur la base de la note reçue, AMP peut ensuite bloquer automatiquement les fichiers malveillants et appliquer les politiques définies par l'administrateur. La figure 3 illustre les différents moteurs fonctionnant en temps réel pour détecter des programmes malveillants sophistiqués et déterminer la réputation des fichiers.

Figure 3. Advanced Malware Protection (AMP)



Analyse en sandbox des fichiers

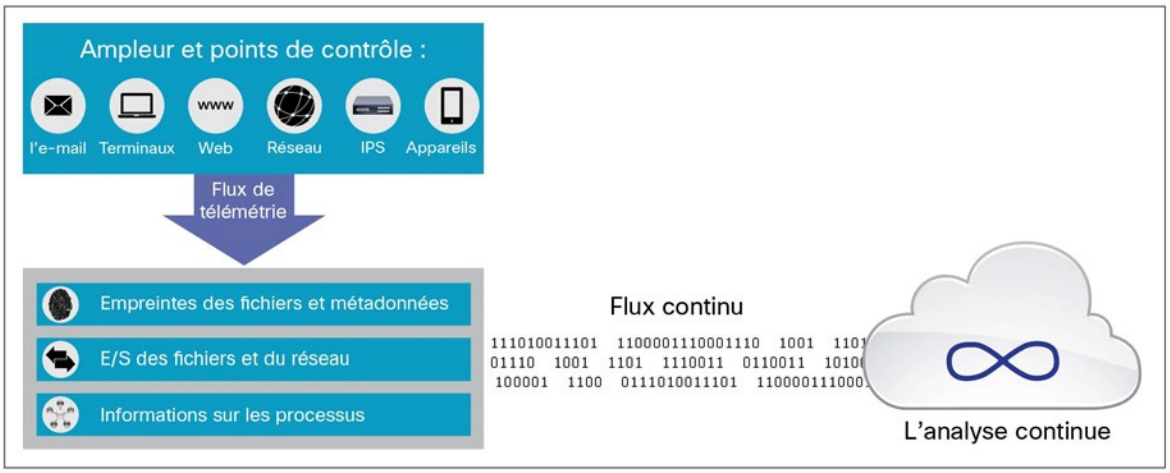
Le sandboxing des fichiers est une caractéristique essentielle d'AMP, donc de CWS Premium. Il permet à AMP d'analyser les fichiers inconnus qui traversent le réseau. Dans un environnement de sandbox extrêmement sécurisé, AMP recueille des informations précises sur le comportement d'un fichier et associe ensuite ces données à une analyse humaine et automatique des données afin de déterminer le niveau de menace qu'il représente. Ces informations sont ensuite ajoutées au réseau collectif d'informations Cisco et Sourcefire basé dans le cloud pour alimenter dynamiquement le jeu de données cloud d'AMP. La fonction de génération active de rapports permet aux équipes de sécurité de consulter des rapports détaillés et faciles à lire concernant les fichiers analysés.

© 2015 Cisco et/ou ses filiales. Tous droits réservés. Ceci est un document public de Cisco.

Analyse rétrospective des fichiers

Probablement la plus importante fonction d'AMP, l'analyse rétrospective des fichiers permet aux entreprises de « remonter dans le temps » pour déterminer précisément quand une attaque s'est produite et évaluer ensuite les dommages. L'analyse rétrospective des fichiers permet de vérifier en continu les fichiers qui ont emprunté la passerelle de sécurité grâce aux renseignements livrés en temps réel par le réseau d'informations Cisco et Sourcefire dans le cloud.

Figure 4. Processus d'analyse rétrospective d'AMP



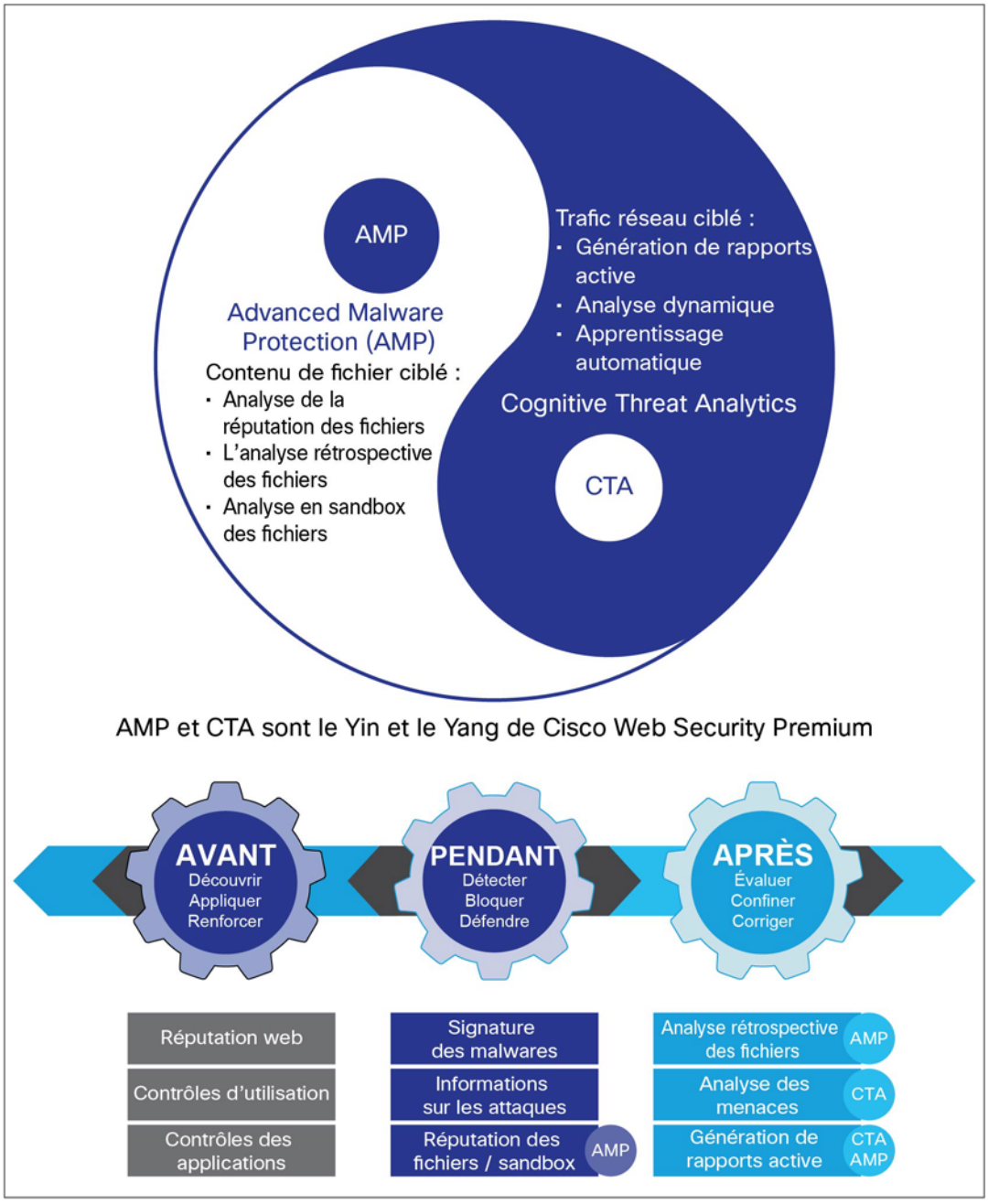
Il peut arriver que l'analyse rétrospective d'AMP révèle qu'un fichier considéré comme « sain » lorsqu'il a traversé les lignes de défense est en réalité un programme malveillant sophistiqué habilement déguisé. Dans ce cas, AMP alerte immédiatement l'administrateur de la sécurité et identifie quel utilisateur sur le réseau est susceptible d'avoir été contaminé et à quel moment. Les équipes de sécurité peuvent ainsi réagir rapidement à l'attaque, avant qu'elle se répande.

Conclusion

Doté de CTA et d'AMP, Cisco CWS Premium s'inscrit dans le cadre de la stratégie de Cisco qui vise à aider les entreprises à faire face aux problèmes de sécurité connus et émergents. Il les aide à détecter, à comprendre et à neutraliser les menaces grâce à une analyse continue et à des informations sur la sécurité livrées en temps réel depuis le cloud et partagées sur toutes les solutions de sécurité pour une efficacité accrue. L'association de ces trois solutions aide les entreprises à identifier de nouveaux biais de contrôle-commande jusqu'alors non détectés par les solutions de sécurité classiques et à faire face aux problèmes de sécurité tout au long du cycle des attaques.

© 2015 Cisco et/ou ses filiales. Tous droits réservés. Ceci est un document public de Cisco.

Figure 5. Solution cloud de sécurisation du web avec AMP et CTA : pour agir sur le processus d'attaque dans son intégralité



Avant : découvrir, appliquer, renforcer

Cisco CWS propose des fonctions permettant de connaître la réputation des sites, des contrôles d'utilisation et d'applications (y compris pour les microapplications), des signatures de programmes malveillants et des informations sur les attaques afin de garantir la sécurité avant et pendant un incident.

© 2015 Cisco et/ou ses filiales. Tous droits réservés. Ceci est un document public de Cisco.

Pendant : détecter, bloquer, défendre

Le moteur AMP améliore la sécurité pendant l'attaque grâce à ses fonctions de réputation et d'analyse en sandbox des fichiers. Il bloque automatiquement les fichiers malveillants et applique les politiques définies par l'administrateur sur la base de la réputation connue du fichier. Il analyse les fichiers inconnus qui passent par Cisco CWS et alimente en conséquence la base d'informations sur les menaces. Ces fonctions aident les analystes de la sécurité à catégoriser les menaces à examiner en priorité.

Après : évaluer, confiner, corriger

Les moteurs CTA et AMP assurent l'analyse continue et la résolution des problèmes lors de la phase critique postérieure à l'incident. CTA permet d'analyser en temps réel les comportements sur le réseau afin d'identifier les événements suspects. Parallèlement, l'analyse rétrospective des fichiers d'AMP permet de résoudre le problème des fichiers malveillants qui percent les premières lignes de défense du périmètre. Les fonctionnalités actives de création de rapports d'AMP offrent une bonne visibilité sur la réputation et le comportement des fichiers qui ont pénétré le réseau. Les équipes de sécurité peuvent identifier et évaluer plus facilement l'étendue de l'attaque et y réagir rapidement.

L'apprentissage automatique qui s'opère au niveau de CTA et d'AMP au cours de la phase postérieure de l'attaque sert ensuite à améliorer les capacités de détection en temps quasi réel de Cisco CWS Premium en cas d'attaque.

Pour en savoir plus

Pour tout savoir de Cisco Cloud Web Security Essentials et Cloud Web Security Premium, rendez-vous à http://www.cisco.com/go/cws.

Pour plus d'informations sur CTA, rendez-vous sur http://www.cisco.com/go/cognitive.

Pour plus d'informations sur AMP, rendez-vous sur http://www.cisco.com/go/amp.

Siège social aux États-Unis
Cisco Systems, Inc.
San José, Californie

Siège social en Asie-Pacifique
Cisco Systems (États-Unis) Pte, Ltd.
Singapour

Siège social en Europe
Cisco Systems International BV Amsterdam.
Pays-Bas

Cisco compte plus de 200 agences à travers le monde. Les adresses, numéros de téléphone et numéros de fax de nos bureaux sont indiqués sur le site web Cisco, à l'adresse suivante : **www.cisco.com/go/offices**.

Cisco et le logo Cisco sont des marques de commerce ou des marques déposées de Cisco et/ou de ses filiales aux États-Unis et dans d'autres pays. Pour consulter la liste des marques commerciales Cisco, rendez-vous à l'adresse : www.cisco.com/go/trademarks. Les autres marques commerciales mentionnées dans le présent document sont la propriété de leurs détenteurs respectifs. L'utilisation du terme « partenaire » n'implique pas de relation de partenariat entre Cisco et une autre entreprise. (1110R)

Imprimé aux États-Unis C11-734836-00 06/15

© 2015 Cisco et/ou ses filiales. Tous droits réservés. Ceci est un document public de Cisco.