Le commerce et la sécurité : comment protéger les données des clients tout en réalisant des économies de temps et d'argent

Présentation

Dans le secteur du commerce, les environnements IT connaissent des changements technologiques sans précédent. Alors que les enseignes sont soumises à des exigences croissantes, leur clientèle attend d'elles des services performants et sécurisés. Mais les commerçants sont également la cible de pirates organisés et bien établis, à l'affût de la moindre faiblesse des réseaux et des systèmes de point de vente (POS). La conséquence fâcheuse de bon nombre d'attaques est le vol de données de carte de crédit et autres informations client.

Ce livre blanc passe en revue les défis auxquels sont confrontés les réseaux du secteur du commerce et présente une solution de sécurité Cisco® qui assure une protection efficace, à jour et fiable : Cisco Cloud Web Security (CWS).

Les menaces qui pèsent sur les environnements IT du secteur du commerce se multiplient

Mettre en place des réseaux en magasin offrant les performances et la sécurité requises n'est pas une mince affaire. Du simple contrôle de l'accès Internet en magasin aux exigences complexes en matière de respect des normes PCI DSS (Payment Card Industry Data Security Standard), les commerçants doivent réfléchir à l'avance à la manière dont ils vont gérer le trafic réseau. Pour être efficaces, les solutions de sécurité doivent assurer le contrôle des réseaux installés en magasin tout en prenant en compte leur évolution galopante. Qui plus est, elles doivent s'adapter à la complexité croissante des menaces.

Les attaques et atteintes majeures à la sécurité des environnements IT du secteur du commerce continuent à se multiplier en dépit des efforts des experts du secteur et des professionnels de la sécurité. Les victimes sont aussi bien des géants de la vente que de grandes chaînes de restaurants franchisés (voir la figure 1). Les cybercriminels visent toujours les systèmes de paiement. Ces attaques, qui portent atteinte à l'image de marque des enseignes, sapent la confiance des clients. Parallèlement, les dédommagements et les efforts mis en œuvre pour tenter d'atténuer l'impact de ces attaques se chiffrent parfois en centaines de millions de dollars.

Figure 1. Les violations de données les plus importantes de l'histoire des États-Unis (en fonction du coût des attaques)

Sources : Bloomberg, Privacy Rights Clearinghouse et Breach Level Index

L'accès Wi-Fi invité et les expériences d'achat mobile interactif en magasin ont conduit à la prolifération de nouvelles offres, parmi lesquelles de nombreuses applications d'achat et l'accès réseau en magasin. Bien que ces services en magasin représentent un bénéfice indéniable pour les clients, l'envers de la médaille est moins rose pour les commerçants dont les réseaux deviennent plus complexes, mettant à rude épreuve leurs ressources IT. Les services en ligne élargissent également le champ d'attaque, exposant davantage les entreprises aux cybercriminels qui scrutent les points faibles et s'attaquent aux vulnérabilités des réseaux. C'est la raison pour laquelle il est primordial pour les commerçants d'investir dans la protection des données de leurs clients, non seulement au niveau des succursales, mais aussi du siège.

L'Internet des objets (IoT) est une autre tendance informatique que les commerçants doivent aujourd'hui gérer. L'IoT représente un réseau d'objets physiques connectés à Internet via une technologie intégrée, capable d'interagir avec le réseau interne et l'environnement externe. Par exemple, un commerçant peut diffuser sur les terminaux mobiles des consommateurs des informations en temps réel concernant des produits susceptibles de les intéresser, en se basant sur des données client contextuelles obtenues à partir de biens présentés en magasin.

Mais l'IoT propose également d'autres applications métier, dont le suivi en temps réel des stocks entrants grâce aux radio-étiquettes ou encore l'accès des fournisseurs de la chaîne d'approvisionnement aux systèmes internes et aux données en vue d'accélérer les opérations. La multitude des terminaux constituant l'IoT contribue ainsi à multiplier les technologies essentielles dans le magasin. Dans de nombreux cas, ces terminaux n'intègrent aucune mesure de protection et il est donc nécessaire d'en ajouter après-coup.

Étant donné les marges bénéficiaires qui sont en jeu dans le secteur du commerce, les entreprises n'ont d'autre choix que de s'adapter à l'évolution constante des menaces tout en proposant à leur clientèle des expériences d'achat innovantes et personnalisées. De plus en plus, il est nécessaire de mettre à niveau les systèmes POS ou d'investir dans des technologies de sécurité afin de contrôler le risque de perte de données. Mais face à la prolifération des menaces, le secteur du commerce ne reste pas les bras croisés. Ainsi, de nombreuses enseignes se sont récemment regroupées dans le cadre d'une initiative baptisée « Retail Cyber Intelligence Sharing Center » (R-CISC).

Le talon d'Achille du secteur du commerce

D'après le rapport d'enquête 2013 sur les compromissions de données publié par Verizon, les commerces de détail et les restaurants représentaient le deuxième secteur le plus ciblé par les attaques en 2013. Même si les clients continuent d'acheter auprès d'un commerçant qui a été victime d'une infraction, un rapport publié par le Retail News Insider en 2014 indique qu'ils sont susceptibles de troquer la carte de crédit au profit d'argent liquide, entraînant dès lors une diminution des dépenses.

Selon un autre rapport publié en 2014 par le groupe Interactions Consumer Experience Marketing, des indices révèlent que les pirates qui s'en prennent aux commerces ne sont pas si créatifs qu'on pourrait s'y attendre. Selon les constatations, « comparativement à d'autres secteurs, les cybercriminels qui ont attaqué des commerces de détail ont utilisé un nombre restreint de méthodes pour subtiliser des données ». Ainsi, 97 % des attaques consistaient en la falsification des systèmes de paiement.

Détecter les failles est une véritable gageure pour le secteur du commerce. En règle générale, les programmes malveillants restent tapis dans l'environnement IT jusqu'à ce qu'une tierce partie (généralement les services de détection des fraudes ou de répression criminelle) détecte des signes d'activité suspecte. Selon une étude de 3 ans réalisée par Verizon Enterprise Solutions et citée dans un article du Bloomberg Businessweek en 2014, à peine 31 % des entreprises détectent des atteintes à la sécurité par leurs propres moyens de surveillance. Pour les commerçants, ce chiffre tombe à 5 %.

Le tableau 1 présente quatre exemples des plus importantes violations de données au cours de l'année 2014, ainsi que la durée pendant laquelle les programmes malveillants sont restés silencieusement dans l'environnement IT avant d'être mis au jour.

Tableau 1. Les caractéristiques des principales violations d'accès aux réseaux en 2014

Attaque	Durée	Méthode d'attaque	Point faible
Magasin de spiritueux américain	17 mois	Logiciels malveillants dits « low-and-slow »	Technologie
Chaîne canadienne et américaine de boutiques d'artisanat	8 à 9 mois	Systèmes POS trafiqués	Processus
Chaîne canadienne et américaine de magasins d'aménagement intérieur	6 mois	Programme malveillant sur mesure conçu pour échapper à la détection et attaquer les registres	Sécurité non considérée comme une priorité ; fonctionnalités inutilisées
Vente aux enchères en ligne	3 mois	Base de données piratée	Personnel et technologie

Sources : Sophos, Bank Info Security, Krebs on Security, Bloomberg News, Private WiFi.com et Huffington Post

Des capacités et des exigences IT fonctionnelles croissantes

À mesure que les environnements et réseaux IT des commerçants se complexifient, leur gestion se complique également. Dans le secteur informatique, le manque croissant de personnel qualifié s'ajoute à la difficulté de gérer ces environnements connectés à Internet en magasin. Pour faire face à cette pénurie, particulièrement dans le domaine de la cybersécurité, des groupes informatiques centralisent la gestion et l'exploitation de l'environnement IT des magasins.

La difficulté majeure est que les réseaux installés en magasin ont été initialement conçus pour relier les terminaux de point de vente aux serveurs en arrière-plan et au WAN de l'entreprise. Ces réseaux, destinés à traiter un trafic peu dense, sont aujourd'hui sollicités à de nombreuses fins : marketing, accès des collaborateurs à l'intranet et à l'Internet, applications IoT, systèmes d'alarme et de vidéosurveillance, mais aussi accès Wi-Fi invité.

Cette tendance s'accompagne de l'apparition d'une kyrielle de nouvelles technologies proposées aux commerçants. Déployées en magasin, elles offrent une forte valeur ajoutée aux consommateurs qui ne voudront bientôt plus s'en passer. Ces solutions consomment davantage de bande passante et nécessitent donc le traitement d'un volume de données plus important encore. Sans oublier que la difficulté à prévoir les besoins en bande passante, qui varient d'une installation à l'autre, complique encore un peu plus les choses. Si ces exigences dépendent de la taille de chaque magasin, elles varient également suivant l'utilisation des différentes technologies.

À l'origine, le modèle de sécurité de la plupart des réseaux installés en magasin était conçu pour protéger le trafic réseau interne. Or, la quasi-totalité des commerces prend désormais en charge les communications vers l'extérieur du réseau, que ce soit pour collaborer avec les partenaires commerciaux et fournisseurs ou pour accéder à Internet.

S'ils veulent protéger leur réseau comme il se doit, les commerçants devront déployer de nouvelles solutions de prévention et de détection permettant de distinguer de manière plus précise les terminaux et les utilisateurs. Ces solutions devront également proposer des fonctions avancées d'utilisation du réseau. Parallèlement, des politiques d'utilisation acceptable devront être appliquées. Étant donné les types de programmes malveillants et d'attaques dont fait l'objet ce secteur, il est évident que tous les terminaux connectés aux réseaux des magasins se trouvent dans un environnement hostile.

Comment définir l'environnement susceptible aux menaces ? Les pirates cherchent toujours la voie offrant le moins de résistance pour s'implanter dans un environnement, ce qui inclut généralement les terminaux de point de vente. Malheureusement, la plupart des systèmes POS leaders sont composés d'éléments matériels, de composants logiciels et de systèmes d'exploitation facilement mis à mal en cas d'attaques banales. Même si les fournisseurs de ces systèmes proposent des correctifs adéquats, les coûts d'exploitation engendrés pour corriger des centaines de milliers de terminaux POS sont considérables. Qui plus est, ces mises à jour doivent généralement être effectuées manuellement.

Les connexions classiques des systèmes POS à l'Internet public sont une porte ouverte au risque. Dans ce type de configuration, qui autorise les opérations à distance, les systèmes POS en arrière-plan se trouvent dans un local différent, et l'assistance est assurée à distance. Dans ce cas, il faut faire un choix entre rationaliser la gestion des terminaux et réduire le risque d'attaques basées sur le réseau. Or, ce compromis n'est ni juste ni nécessaire.

Les systèmes de sécurisation Web classiques requièrent l'installation d'une passerelle centralisée au niveau du siège social. Chaque magasin ou succursale dirige l'ensemble du trafic vers le point d'agrégation central où il est contrôlé avant d'être autorisé à accéder à Internet. Étant donné l'augmentation du trafic (entrant et sortant) dans les magasins, cette approche nécessite d'importantes quantités de bande passante alors que celle-ci est limitée. La conformité est également un facteur important à prendre en compte, dans la mesure où l'informatique des magasins est soumise aux normes PCI DSS. Afin de se conformer à la réglementation et de réussir les évaluations annuelles, les entreprises doivent mettre en œuvre des contrôles du réseau proactifs pour protéger les connexions et garantir la sécurité des systèmes qui traitent les données des titulaires de cartes.

Pour résumer, les réseaux en magasin étaient auparavant généralement conçus dans l'unique but de connecter les systèmes POS au WAN de l'entreprise. Ces solutions étaient généralement déployées à l'intérieur du périmètre de sécurité de l'entreprise. Cependant, de récentes failles de sécurité dont ont été victimes différentes enseignes commerciales et impliquant des systèmes POS semblent indiquer que cette architecture réseau n'est plus viable.

Les lacunes courantes des environnements IT

En raison des délais serrés dans lesquels les commerçants doivent résoudre les problèmes liés à la sécurité, ils estiment généralement qu'une solution ciblée suffit à protéger leurs ressources essentielles. Toutefois, un modèle de sécurité cohésif doit proposer plus qu'une solution spécifique et doit mettre en œuvre des contrôles de sécurité du réseau suffisants pour répondre à la fois aux problèmes actuels et aux exigences de demain.

La différence entre une solution ciblée ou spécifique et une solution de sécurité complète peut être illustrée par le déploiement d'une connexion Internet directe avec les magasins. Lors du déploiement d'une connexion Internet directe, un pare-feu est ajouté pour protéger le réseau du magasin. Ce pare-feu peut être déployé selon deux modèles.

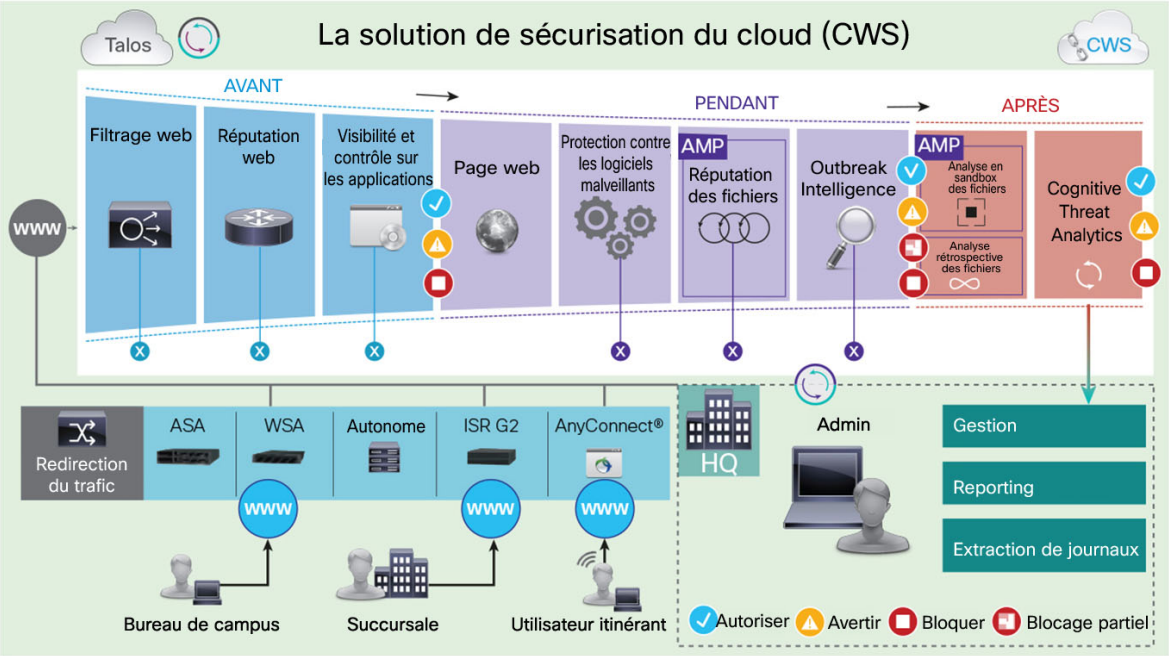
1. Des règles peuvent être définies au niveau du routeur WAN pour diriger le trafic Internet vers le nouveau pare-feu.
2. Les terminaux connectés au réseau du magasin peuvent utiliser le pare-feu comme passerelle par défaut, éliminant ainsi le contrôle ou la surveillance du réseau. Lors du déploiement d'une connexion Wi-Fi en magasin, si le trafic n'est pas correctement dirigé vers un point de contrôle, il est impossible de garantir qu'il n'y aura pas de fuite de données de l'entreprise sur Internet. Par ailleurs, il n'existe aucune garantie que les politiques d'utilisation acceptable sont respectées en permanence.

De manière générale, la multiplication de produits ciblés donne lieu à une situation où le risque réel pour l'entreprise devient difficile à contrôler, à discerner ou à gérer.

Les menaces qui pèsent sur les commerçants font les gros titres depuis plusieurs années. En 2006, à la suite d'une importante faille de sécurité, les données de près d'un million de cartes de crédit ont été compromises. Les pirates ont exploité des faiblesses du système de sécurité des magasins pour accéder aux informations de carte de crédit ainsi qu'à d'autres données client. Une fois la faille repérée, les pirates s'infiltrent sur les réseaux d'entreprise, faisant alors main basse sur les données privées.

Étant donné la capacité des pirates informatiques à partager leurs tactiques et à automatiser leurs attaques, ils n'hésitent pas à cibler de grandes enseignes en s'attaquant au maillon le plus faible de la chaîne, qui est le plus souvent un point de vente dont les contrôles sont moins performants.

Figure 2. Le fonctionnement de Cisco Cloud Web Security

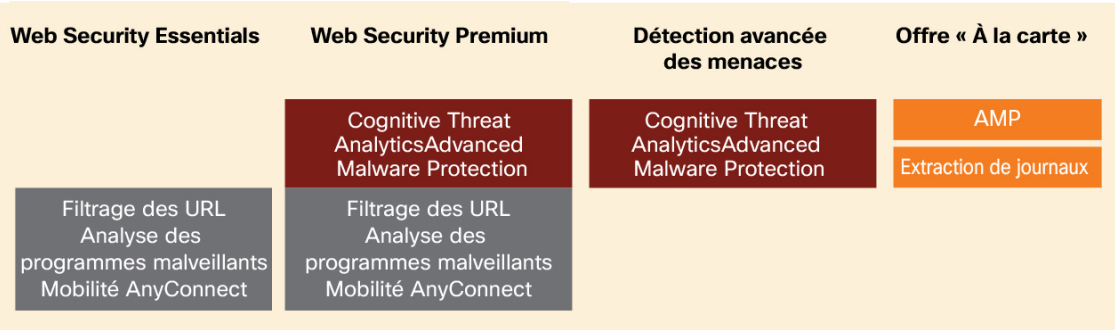


Protection et contrôle flexibles

Cisco a développé un ensemble de produits et de fonctionnalités répondant aux besoins en matière de sécurité et de mise en réseau pour les environnements IT du secteur du commerce. Ces solutions vont des points d'accès sans fil au routage, en passant par la commutation et les services de sécurité avancée basés sur le cloud.

La figure 3 présente les options disponibles lors de l'achat de Cisco CWS.

Figure 3. Les options disponibles lors de l'achat de Cisco CWS



Les solutions leaders du marché Cisco Web Security Appliance (WSA) et Cisco Cloud Web Security (CWS) proposent des modèles de déploiement flexibles assurant la sécurité des contenus sur site et dans le cloud. L'adoption de Cisco WSA pour protéger le réseau au niveau du siège et de Cisco CWS pour le protéger au niveau des filiales permet de renforcer la protection et de répondre aux exigences de sécurité IT tout en évitant d'investir dans de nouveaux équipements pour chacune des succursales. Grâce à son intégration directe avec diverses technologies conçues pour l'environnement commercial, dont les pare-feu Cisco ASA (Adaptive Security Appliance),

les routeurs Cisco ISR (Integrated Services Routers) et le client Cisco AnyConnect®, la solution Cisco CWS vous permet de tirer parti des investissements et des processus d'assistance aux opérations existants pour renforcer la protection et améliorer l'assistance opérationnelle.

Cisco met la protection des connexions Internet à la portée des magasins sans nécessiter de matériel supplémentaire et en ne réacheminant le trafic que si la politique de l'entreprise l'exige. Le trafic à faible risque accède directement à Internet, tandis que le reste du trafic est envoyé vers le site central pour un contrôle approfondi.

Pour assurer une protection contre les menaces connues et émergentes, Cisco CWS recherche les attaques en utilisant des techniques diverses, dont des signatures de programmes malveillants classiques et des filtres de réputation des fichiers et des sites, ainsi que des filtres d'attaque. Mais Cisco CWS ne s'arrête pas là. Il intègre également l'écosystème leader du marché « Collective Security Intelligence » (CSI), qui comprend le groupe de renseignements de sécurité et de recherche Talos. Le travail conjoint de Cisco CSI et de Talos vise à s'assurer que les utilisateurs tirent parti des dizaines de milliers de clients qui utilisent la technologie Cisco.

Cisco CWS propose des rapports détaillés comportant des données courantes sur la sécurité des informations, ainsi qu'une analyse complète de la consommation et de l'utilisation de la bande passante. Dans les environnements où la bande passante est limitée, cette visibilité est un outil essentiel pour optimiser les performances. Une autre fonctionnalité avancée permet de générer un rapport détaillé sur les habitudes de navigation Wi-Fi des utilisateurs « invités », offrant une visibilité sur et une protection contre la comparaison de prix avec les boutiques en ligne et la consultation de contenus offensants. Les fonctions de génération de rapports de Cisco CWS sont donc non seulement utiles pour l'équipe de sécurité IT, mais également pour l'entreprise dans son ensemble.

Et peut-être plus important encore, en tant que solution cloud, Cisco CWS (figure 2) permet d'adapter et d'optimiser en toute simplicité les capacités de bande passante de toute entreprise. Le résultat : des réductions des coûts immédiates et quantifiables, et une efficacité nettement accrue des capacités de gestion du risque au niveau du magasin. Ces économies sont réalisées en transférant la gestion et le contrôle du trafic d'un système matériel en local vers des systèmes cloud. Par ailleurs, en appliquant le modèle de logiciel en tant que service (SaaS) pour réguler le trafic sur la base de politiques, Cisco CWS réduit considérablement la charge appliquée au matériel réseau en magasin.

L'utilité de Cisco CWS pour les entreprises du secteur du commerce

Cet exemple concret montre comment Cisco CWS peut protéger une entreprise des menaces actuelles : un responsable de la sécurité IT a été chargé de protéger une chaîne de 1 500 magasins qui déploie dans ses différents points de vente une technologie permettant aux clients d'accéder à Internet pour bénéficier d'un panel de services supplémentaires. Ce responsable sait qu'il existe une vague d'attaques par programmes malveillants sophistiqués visant à compromettre les systèmes en magasin (dont les terminaux POS). Il souhaite donc que ces attaques soient détectées et corrigées rapidement et efficacement. De plus, bon nombre de magasins ont une bande passante limitée et la solution doit optimiser les connexions réseau de chaque point de vente.

Le responsable de la sécurité déploie des routeurs de périphérie Cisco ISR dans chaque magasin. Ces périphériques prennent en charge les fonctionnalités de l'IWAN Cisco pour protéger et optimiser la bande passante au niveau de chaque succursale. L'IWAN permet de gérer la bande passante en utilisant des connexions Internet à moindre coût plutôt que de coûteuses connexions à des réseaux privés. Il offre également un chemin de migration progressif qui permet à l'entreprise d'effectuer la transition depuis des connexions réseau privées à son rythme. Afin de s'assurer que les terminaux mobiles se connectent au bon réseau dans chaque magasin, Cisco ISE (Identity Services Engine) protège les différents systèmes en déterminant quels utilisateurs et terminaux peuvent accéder à certaines parties des réseaux.

Pour protéger le trafic Web, l'entreprise utilise Cisco CWS Premium pour l'accès direct à Internet, qui peut être déployé via les routeurs de périphérie Cisco ISR, sans nécessiter de matériel supplémentaire. Cisco CWS Premium intègre Cisco Advanced Malware Protection (AMP) et Cognitive Threat Analytics (CTA), dont les fonctions avancées mettent tous les utilisateurs à l'abri des menaces potentielles. CTA est un système d'analyse des comportements du réseau en temps quasi réel qui tire parti de l'apprentissage automatique et de statistiques avancées pour identifier toute activité inhabituelle sur un réseau afin de détecter d'éventuelles attaques. AMP utilise des analyses de réputation de fichiers, de sandboxing et rétrospectives pour identifier et stopper les menaces déjà présentes sur le réseau.

Avec ces produits de sécurité Cisco, la chaîne de 1 500 magasins peut à présent gérer l'utilisation de sa bande passante, les niveaux d'accès utilisateur, la défense contre les menaces et la sécurité du contenu. Il ne s'agit là que d'une des combinaisons possibles de produits de sécurité Cisco. En l'occurrence, le responsable de la sécurité IT répond aux objectifs de l'entreprise en termes de réseau et de sécurité en ce qui concerne son réseau distribué.

Les atouts de Cisco CWS

Une entreprise qui utilise la solution Cisco intégrée pour protéger ses réseaux peut appliquer une politique commune, détecter des attaques sophistiquées et optimiser l'utilisation de la bande passante du WAN. Cisco CWS Premium, intégré aux routeurs de périphérie Cisco ISR, permet également de surveiller les botnets. L'entreprise peut ainsi s'assurer que la sécurité de ses terminaux POS n'est pas compromise et transférer des données à son siège sans risque. L'achat groupé de solutions offre à l'entreprise une opportunité supplémentaire de réaliser des économies.

Les différents modules et services étant conçus pour s'intégrer les uns aux autres, l'ajout d'éléments supplémentaires se fait en douceur. Cisco estime que cela réduit de 40 % le temps nécessaire au personnel IT pour configurer et mettre en œuvre la solution. L'entreprise bénéficie également d'un niveau de sécurité élevé et constant sur son réseau à travers le monde, ce qui lui permet de continuer à se développer et de se concentrer sur son activité au lieu de se préoccuper des pirates qui cherchent à s'infiltrer sur les réseaux de ses magasins.

Conclusion

Les commerçants peuvent réduire de manière substantielle les frais d'exploitation liés à la surveillance, à la gestion et à la maintenance de leurs réseaux grâce à des outils cloud tels que Cisco CWS. Parfaitement intégré aux solutions Cisco ASA et Cisco ISR, CWS élimine intelligemment la nécessité d'appliquer des politiques de sécurité en local, réduisant dès lors les besoins en bande passante de chaque point de vente. Reconnue comme solution leader du marché par Gartner, Cisco CWS propose une approche intelligente pour faire bénéficier les réseaux de magasins des fonctions de sécurité les plus efficaces sans pour autant en compliquer le fonctionnement.

Pour en savoir plus

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

Siège social aux États-Unis
Cisco Systems, Inc.
San Jose, 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 sont répertoriés sur le site de Cisco, à l'adresse **www.cisco.com/go/offices**.

Imprimé aux États-Unis C11-733817-00 02/15