謀
RESEARCH
Influence et analyse
via les médias sociaux

Décembre 2016

CISCO ONE SIMPLIFIE LA SÉCURITÉ D'ENTREPRISE À L'ÈRE NUMÉRIQUE

LIVRE BLANC

Préparé par
Zeus Kerravala

ZK Research
Une division de Kerravala
Consulting

PRÉSENTATION DE L'AUTEUR

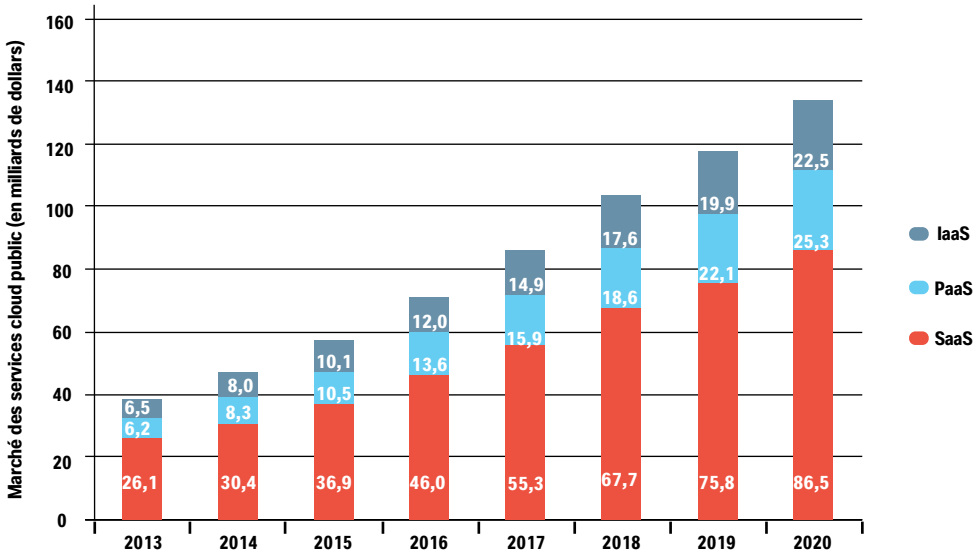
Zeus Kerravala est le fondateur et analyste en chef de ZK Research. Il apporte des conseils tactiques et stratégiques à ses clients pour les guider dans l'environnement des affaires actuel mais aussi sur le long terme. Il fournit des études et des analyses à différents acteurs : les gestionnaires réseaux et IT des entreprises utilisatrices, les fournisseurs de matériels informatiques, de logiciels et de services IT, et les membres de la sphère financière souhaitant investir dans les entreprises de sa compétence.

INTRODUCTION : LES ENTREPRISES NUMÉRIQUES DOIVENT REPENSER LEURS STRATÉGIES DE SÉCURITÉ

À l'heure du tout numérique, l'environnement IT doit évoluer rapidement pour répondre aux besoins des entreprises. Désormais, les réseaux sont définis par logiciel, les applications résident dans le cloud, les employés utilisent leurs propres appareils sur leurs lieux de travail et l'Internet des objets (IoT) est en plein essor. Toutes ces transitions technologiques développent la capacité d'une entreprise à faire preuve de dynamisme et de réactivité pour agir rapidement. Néanmoins, tout un pan de l'écosystème IT doit encore évoluer : la sécurité. Dans ce domaine, les principaux changements à prendre en compte sont les suivants :

Le périmètre réseau se réduit. Traditionnellement, la sécurité de l'entreprise passait par le déploiement d'un pare-feu au niveau du seul point d'entrée dans l'entreprise : la connexion à Internet. Aujourd'hui, l'essor du cloud computing (figure 1), de l'IoT et du BYOD a érodé le périmètre réseau et créé des centaines de nouveaux points d'entrée. Par exemple, le cloud permet aux branches d'activité d'acquérir elles-mêmes les services dont elles ont besoin. L'étude ZK Research de 2016 sur les intentions d'achats en matière de réseaux montre en effet que 96 % des entreprises possèdent des services cloud qui n'ont pas été acquis par le département IT, et cette indépendance est problématique pour l'équipe de sécurité. D'autres angles morts apparaissent avec l'IoT, dans la mesure où l'équipe chargée de la technologie opérationnelle déploie des terminaux spécifiques. Avec ces tendances, de nouveaux points d'entrée dans l'entreprise voient le jour. Selon les estimations de ZK Research, la surface d'attaque a été multipliée par 10 au cours des cinq dernières années.

Figure 1 : La croissance rapide des services cloud lance de nouveaux défis à la sécurité



ZK Research, prévisions mondiales 2016 pour le cloud

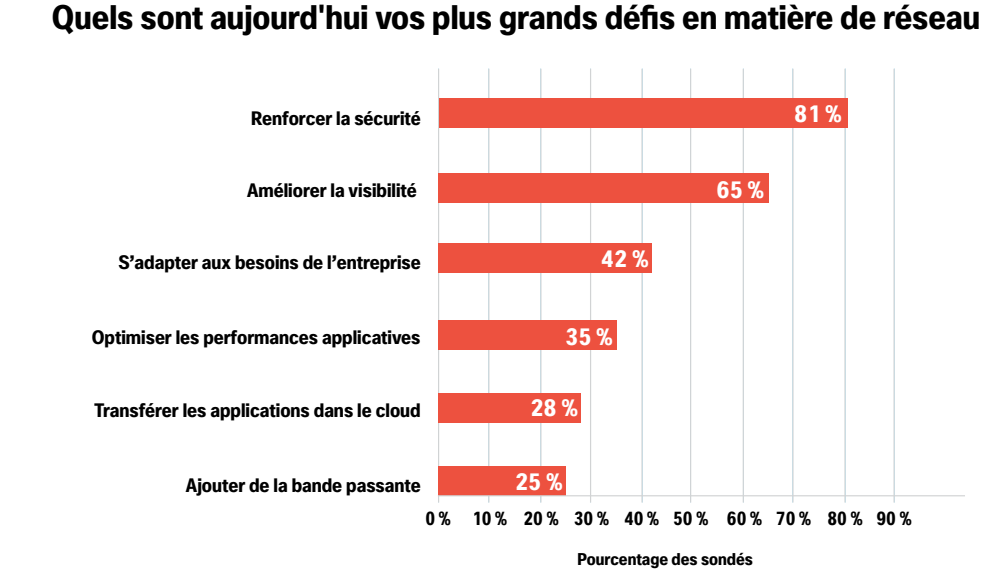
Le paysage des menaces évolue. D'après l'enquête ZK Research de 2016 sur la sécurité, la protection du périmètre réseau mobilise à elle seule 90 % des budgets

de sécurité. Pourtant, seulement 20 % des attaques se focalisent sur ce point. Les entreprises doivent se concentrer sur de nouvelles vulnérabilités, comme l'hameçonnage, l'espionnage du réseau, les attaques sur mobiles et les bugs logiciels. À l'heure de la transformation numérique, les cyberattaques se révèlent bien plus lucratives. Le paysage des menaces devrait donc continuer d'évoluer à un rythme exponentiel.

La sécurité se complexifie. Face à l'augmentation de la surface d'attaque et à l'apparition de menaces plus sophistiquées, les entreprises déploient davantage de produits ciblés en différents points de l'infrastructure. L'enquête ZK Research de 2016 sur la sécurité révèle que les grandes entreprises recourent en moyenne à 32 fournisseurs de solutions de sécurité, et à plus de 100 pour certaines d'entre elles. La multiplication de ces outils ne se traduit pas forcément par une amélioration de la sécurité, elle peut même, au contraire, introduire des politiques incohérentes. D'autre part, ZK Research constate qu'il faut en moyenne plus de 100 jours pour découvrir une violation de sécurité. Et en dépit des dizaines de milliards de dollars dépensés chaque année pour de nouveaux produits, la sécurité reste aujourd'hui le grand défi des gestionnaires réseaux (figure 2). Enfin, la pléthore de produits ciblés ralentit fortement la mise en œuvre de nouvelles politiques ou même de simples changements et elle peut aussi créer des écarts de sécurité dus à la configuration et à l'essai obligatoires de tous ces équipements.

Alors que les entreprises sont fermement engagées sur la voie de la numérisation, la sécurité est, en l'état, excessivement complexe et les méthodes appliquées sont trop lentes pour répondre aux besoins actuels. Quelle que soit leur taille, les entreprises doivent maintenant repenser leur stratégie de sécurité en tenant compte des exigences de l'ère numérique.

Figure 2 : La sécurité reste le plus grand défi de la plupart des entreprises



ZK Research, étude 2016 sur les intentions d'achats en matière de réseaux

CHAPITRE II : COMPRENDRE LE MODÈLE LOGICIEL CISCO ONE

Les entreprises numériques s'appuient sur des technologies centrées sur le réseau, comme l'IoT, le cloud computing et la mobilité. Par conséquent, les réseaux se sont développés et doivent proposer davantage de fonctionnalités. La complexité des processus d'achat, de déploiement et de gestion des logiciels nécessaires à leur exploitation n'a donc fait que croître. Pourtant, plusieurs difficultés pèsent sur la gestion et l'acquisition de ces logiciels, notamment les suivantes :

Le processus de commande et de gestion des licences logicielles pour les dispositifs réseau devenant plus complexe, il est difficile de veiller à ce que les bonnes fonctions soient disponibles au bon endroit du réseau ;

Les logiciels réseau étant généralement mis à niveau lors du renouvellement des équipements, les entreprises peuvent passer à côté de nouvelles opportunités ;

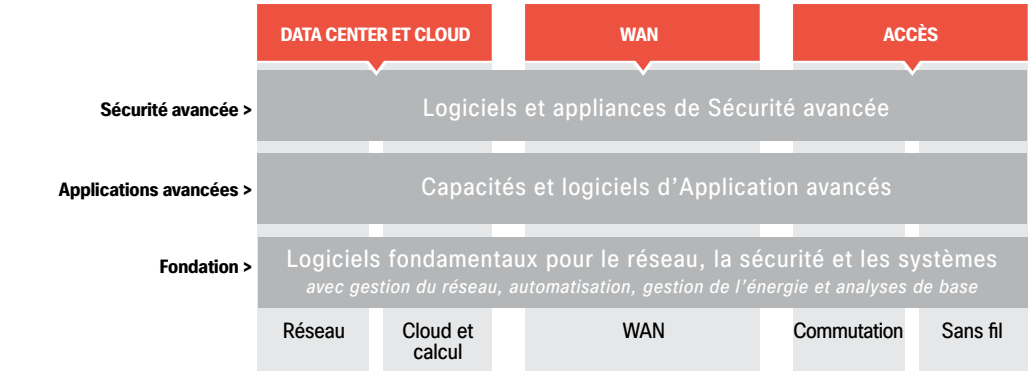
L'actualisation périodique de l'infrastructure réseau entraîne une fluctuation des dépenses difficilement prévisible au budget.

Avec Cisco ONE, les clients disposent d'une solution simple et flexible pour acquérir des logiciels destinés aux data centers, aux réseaux WAN et aux réseaux d'accès. Ce modèle dissocie l'achat des logiciels de l'acquisition des plates-formes matérielles sous-jacentes.

Cisco ONE simplifie le processus d'approvisionnement et de gestion du réseau en donnant au client la possibilité d'acheter toutes les licences de fonction sous forme de pack, puis d'activer les licences au cas par cas, selon les besoins. Il est plus avantageux puisqu'il réduit la complexité, protège les investissements et propose de nouvelles fonctionnalités et des modèles d'achat flexibles.

Cisco ONE s'articule autour de trois domaines distincts : Data center et cloud, WAN et Accès. Chaque domaine se décline en trois ensembles de fonctions différents : Fondation, Applications avancées et Sécurité avancée (figure 3). Le détail des différents domaines de Cisco ONE est consultable sur le site *www.cisco.com/go/one*.

Figure 3 : Cisco ONE offre aux clients une gamme complète de solutions



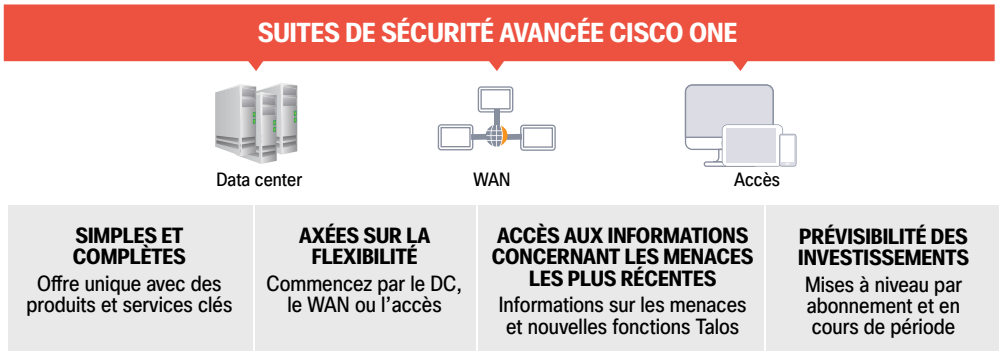
Cisco, 2016

CHAPITRE III : LOGICIELS CISCO ONE POUR LA SÉCURITÉ AVANCÉE

Cette offre, présentée à la figure 4, étend les avantages de Cisco ONE à la sécurité avancée. Pour renforcer les défenses du data center, du WAN et du réseau d'accès, elle propose des suites prédéfinies simples, composées de produits et services de sécurité phares, et dédiées à chaque domaine.

En choisissant d'acquérir une solution de sécurité avancée par le biais de Cisco ONE, les clients bénéficient des avantages suivants :

Figure 4 : Cadres de sécurité avancée Cisco ONE



ZK Research et Cisco, 2016

Des suites simples et complètes : Pour chaque domaine (data center, WAN et accès), Cisco ONE fournit une offre unique de produits et services de sécurité clés. Par exemple, l'offre prédéfinie pour le data center comprend la protection avancée contre les programmes malveillants, la prévention des intrusions nouvelle génération, le filtrage des URL et des services de pare-feu virtualisés.

Une flexibilité intrinsèque : Les clients peuvent commencer à déployer la solution dans un domaine particulier, même si la sécurité avancée Cisco ONE est plus avantageuse en optant pour une approche globale, avec un déploiement dans les trois domaines. En outre, Cisco ONE prend en charge les appareils physiques aussi bien que virtuels (actuellement pour l'accès, prochainement pour le data center et le WAN).

Les informations les plus récentes sur les menaces : Les clients ont accès à Cisco Talos, une source d'information de premier plan, compatible avec les fonctionnalités des différentes offres Cisco ONE. La sécurité avancée Cisco ONE offre également de nouvelles fonctions.

La prévisibilité des investissements : Les trois offres sont proposées sous forme d'abonnement pour une période d'un an, de trois ans ou de cinq ans et permettent ainsi d'anticiper les flux de trésorerie. Les clients peuvent aussi effectuer une mise à niveau vers un appareil plus récent en cours d'abonnement, en bénéficiant d'un report des avantages correspondant à la période inutilisée.

La plupart des entreprises concentrent leur action sur le périmètre réseau et laissent souvent de côté la sécurité interne du data center.

Les trois abonnements incluent les services d'assistance logicielle, qui comprennent les mises à jour et mises à niveau logicielles, l'accès à l'assistance technique et les nouvelles fonctions logicielles.

Avec cette offre, Cisco se distingue des autres fournisseurs en couvrant davantage de composantes du réseau (data center, WAN et accès) et en sécurisant à la fois l'intérieur du réseau et son périmètre.

Pour aider ses clients à tirer plus rapidement parti de Cisco ONE, Cisco offre un ensemble de services aux entreprises, avec les composants suivants :

Les services de démarrage rapide sont personnalisés pour Cisco ONE afin d'intégrer rapidement les nouvelles fonctionnalités dans l'entreprise. Les techniciens apportent conseils d'expert et assistance tout au long du processus afin de réduire les risques tout en accélérant la rentabilisation. Ces prestations comprennent la mise en œuvre des nouveaux services, l'installation des logiciels, la configuration, la personnalisation, l'automatisation des tâches, la migration, l'intégration et les tests.

Les services d'optimisation couvrent la phase d'adoption et la gestion du changement pour veiller à la réussite de la transformation tout en optimisant les résultats de l'entreprise.

CHAPITRE IV : SÉCURITÉ AVANCÉE CISCO ONE POUR LE DATA CENTER

Le data center est le centre névralgique de la plupart des entreprises, tant il abrite l'ensemble de ses applications, données et éléments de propriété intellectuelle stratégiques. Il est donc logiquement la cible privilégiée des pirates. Sa protection est souvent un défi, car les attaques peuvent se déclencher au sein même du data center ou passer par une « porte dérobée », pour peu qu'un système ayant accès au data center ne soit pas sécurisé. La plupart des entreprises concentrent leur action sur le périmètre réseau et laissent souvent de côté la sécurité interne du data center. Les chiffres ci-après, tirés de l'enquête ZK Research de 2016 sur la sécurité, démontrent clairement qu'il est nécessaire de donner plus d'importance à la sécurisation du data center :

Actuellement, 90 % des budgets de sécurité sont dépensés sur le périmètre réseau, mais seulement 20 % des violations de sécurité se produisent à ce niveau ;

Le délai moyen de détection d'une violation dans le data center est de 100 jours ;

Le trafic est-ouest représente 70 % du trafic de data center et s'accroît rapidement. Il contourne les mécanismes de sécurité placés au cœur du réseau ;

53 % des sondés désactivent les fonctions de sécurité sur le périmètre réseau pour favoriser les performances et rendent, par la même occasion, le data center plus vulnérable.

Avec l'offre Sécurité avancée Cisco ONE pour le data center, les clients peuvent contrer les menaces qui pèsent aujourd'hui sur cette partie du réseau :

Elle permet d'instaurer des politiques segmentées par le biais d'un pare-feu virtualisé ;

Elle contribue à empêcher et maîtriser les menaces connues et inconnues grâce à la prévention des intrusions nouvelle génération ;

Elle favorise la détection et le blocage des programmes malveillants furtifs et des attaques 0-day avec la protection avancée du réseau ;

Elle fournit des filtres de réputation et de catégorie concernant plus de 280 millions de sites Web dans au moins 80 catégories ;

Elle vous donne les moyens de défendre votre entreprise contre les menaces venues de l'extérieur comme de l'intérieur, sachant qu'un nombre croissant d'attaques sont déclenchées en son sein.

La figure 5 présente les fonctions de la sécurité avancée Cisco ONE pour le data center.

Figure 5 : Sécurité avancée Cisco ONE pour le data center

ABONNEMENTS	LICENCES DÉTAILLÉES	MATÉRIEL (vendu séparément)
Abonnements ASA 5585-X*	ASA 5585-X Firepower (IPS, URL, AMP) Contexte de sécurité	Appliance ASA 5585-X
Abonnements Firepower 4100/9300*	Firepower 9300/4100 Firepower Threat Defense (IPS, URL, AMP)	Appliance Firepower 9300/4100

*L'abonnement comprend à la fois l'assistance et les licences logicielles pour profiter des mises à jour des logiciels et des signatures, des crédits pour les mises à niveau en cours d'abonnement, et de l'accès aux fonctions et informations les plus récentes concernant les menaces.

Cisco, 2016

CHAPITRE V : SÉCURITÉ AVANCÉE CISCO ONE POUR LE WAN ET LA PÉRIPHÉRIE

Dans de nombreuses entreprises, l'activité se concentre dans les filiales. Selon les estimations de ZK Research, ces dernières regroupent 84 % des employés et constituent le principal lieu de travail et d'interaction avec la clientèle. L'augmentation du nombre d'employés rattachés à une filiale a un lourd impact sur le réseau puisque le nombre d'équipements utilisés croît de manière exponentielle avec l'essor du BYOD. Selon l'enquête ZK Research de 2016 sur la consumérisation, 82 % des entreprises ont déjà adopté un plan BYOD et les employés des filiales utilisent chacun trois appareils personnels en moyenne. Cette pratique crée de nouveaux risques de sécurité, en témoignent 75 % des sondés de l'enquête ZK Research de 2016 sur la sécurité, qui citent la sécurité mobile comme leur principal problème en la matière.

Une autre tendance a accentué les exigences de sécurité dans les filiales : l'utilisation croissante des applications cloud. Pour améliorer les performances du SaaS (logiciel proposé comme un service), les entreprises permettent aux employés d'accéder au cloud directement depuis la filiale, sans passer par le WAN. Sur les douze derniers mois,

cette utilisation combinée des équipements personnels et des applications cloud dans les filiales a multiplié par cinq le nombre de points d'entrée pour les attaques.

La sécurité des filiales doit impérativement évoluer pour faire face à la numérisation croissante du monde. Pour y parvenir, les entreprises doivent veiller à ce qu'elles réunissent les caractéristiques suivantes :

Accès à distance sécurisé ;

Sécurité unifiée du réseau filaire et sans fil ;

Protection des données contre la falsification, l'accès non autorisé et l'espionnage ;

Accès Internet direct et sécurisé.

Au sein de l'offre Sécurité avancée de Cisco ONE, la solution Défense contre les menaces pour le WAN et la périphérie est conçue pour optimiser la sécurité des filiales :

Elle offre un accès à distance et un VPN pour les terminaux clients hautement sécurisés ;

Elle contribue à empêcher et maîtriser les menaces connues et inconnues grâce à la prévention des intrusions nouvelle génération ;

Elle favorise la détection et le blocage des programmes malveillants furtifs et des attaques 0-day avec la protection avancée du réseau ;
Elle fournit des filtres de réputation et de catégorie concernant plus de 280 millions de sites Web dans au moins 80 catégories.

La figure 6 présente la structure de la solution Sécurité avancée de Cisco ONE : Défense contre les menaces pour le WAN et la périphérie.

Figure 6 : Sécurité avancée Cisco ONE : Défense contre les menaces pour le WAN et la périphérie

ABONNEMENTS	LICENCES DÉTAILLÉES	MATÉRIEL REQUIS (vendu séparément)
Abonnements ASA 5500-X*	ASA 5500-X Firepower (IPS, URL, AMP), AnyConnect Plus	Appliances ASA 5506, 5508, 5516, 5525, 5545, 5555

*L'abonnement comprend à la fois l'assistance et les licences logicielles pour profiter des mises à jour des logiciels et des signatures, des crédits pour les mises à niveau en cours d'abonnement, et de l'accès aux fonctions et informations les plus récentes concernant les menaces.

Cisco, 2016

CHAPITRE VI : SÉCURITÉ AVANCÉE CISCO ONE POUR L'ACCÈS

La périphérie d'accès au réseau de l'entreprise devient de plus en plus complexe. La croissance des équipements personnels et des applications cloud crée de nombreux angles morts susceptibles de favoriser la violation du réseau. En outre, l'IoT se généralise et de nombreux équipements sont désormais rattachés à la périphérie d'accès au réseau, notamment des caméras de vidéosurveillance, des éclairages à LED, des systèmes CVCA et des équipements propres à l'activité de l'entreprise. D'après l'étude ZK Research de 2016 sur les intentions d'achats en matière de réseaux, 70 % des gestionnaires réseaux ont peu, voire pas du tout, confiance dans les équipements attachés à la périphérie du réseau.

En outre, les cybercriminels concentrent leurs actions sur les utilisateurs et les applications en recourant à des programmes malveillants, notamment par des campagnes d'hameçonnage élaborées. Une fois que ces menaces ont pénétré le réseau, elles peuvent y rester cachées pendant plusieurs mois pour réunir des informations avant de finalement exfiltrer des données précieuses. L'enquête ZK Research de 2016 sur la sécurité révèle d'autres chiffres intéressants concernant la périphérie d'accès :

90 % des entreprises ont déjà subi une violation de sécurité dont 46 % au cours de l'année passée ;

50 % des entreprises utilisent des terminaux mobiles infectés par des programmes malveillants ;

Le délai moyen de détection d'une violation sur la couche d'accès est de 100 jours ;

96 % des entreprises utilisent des applications qui n'ont pas été validées par le département IT ;

Les employés utilisent en moyenne quatre applications grand public dans le cadre de leur travail quotidien.

Les entreprises ont besoin d'une approche simplifiée pour sécuriser la périphérie d'accès.

Les entreprises ont besoin d'une approche simplifiée pour sécuriser la périphérie d'accès, afin que les employés puissent exploiter les informations dont ils ont besoin à tout moment et en tout lieu, avec l'équipement de leur choix. Les équipes de sécurité ont également besoin de davantage de visibilité pour détecter le trafic anormal et éventuellement identifier une violation.

Au sein de l'offre Sécurité avancée de Cisco ONE, la solution Politique et défense contre les menaces pour l'accès est conçue pour accroître la sécurité tout en offrant aux utilisateurs un accès approprié qui soit plus simple. Elle offre les avantages suivants :

Accès hautement sécurisé, déterminé par l'identité et l'équipement utilisé, accès centralisé basé sur l'identité et le contexte quel que soit l'emplacement ;

Prise en charge de la visibilité, de la conformité et de la gestion du périphérique mobile ;

VPN et terminal hautement sécurisé avec Cisco AnyConnect Apex.

La figure 7 présente la structure de la solution Sécurité avancée de Cisco ONE : Politique et défense contre les menaces pour l'accès.

Figure 7 : Sécurité avancée Cisco ONE : Politique et défense contre les menaces pour l'accès

ABONNEMENTS	LICENCES DÉTAILLÉES	MATÉRIEL REQUIS (vendu séparément)
Abonnements ISE et AnyConnect*	ISE-Apex, ISE-Plus, AnyConnect Apex	Appliance ISE

*L'abonnement comprend à la fois l'assistance et les licences logicielles pour profiter des mises à jour des logiciels et des signatures, des crédits pour les mises à niveau en cours d'abonnement, et de l'accès aux fonctions et informations les plus récentes concernant les menaces.

Cisco, 2016

CHAPITRE VII : CONCLUSIONS ET RECOMMANDATIONS

L'ère de l'entreprise numérique se conjugue désormais au présent avec l'arrivée de nombreuses innovations technologiques, comme l'IoT, le cloud et la mobilité. Ces technologies permettent aux entreprises d'être plus dynamiques et distribuées, et d'atteindre de nouveaux sommets d'efficacité et de productivité. Les entreprises qui sauront passer rapidement au numérique seront plus rentables et acquerront un avantage compétitif. Les autres auront du mal à survivre.

Cette évolution technologique a cependant un prix : la complexité croissante de la sécurité. Les méthodes de sécurité traditionnelles, concentrées exclusivement sur le périmètre réseau, ne sont désormais plus suffisantes : l'essentiel des attaques esquive aujourd'hui la périphérie du réseau. Les architectures de sécurité doivent évoluer et il est nécessaire de se concentrer davantage sur le réseau interne et plus particulièrement sur les nouvelles cibles privilégiées des cybercriminels : le data center, les filiales et la périphérie d'accès.

Centrée sur les menaces, l'approche de Cisco répond de manière idéale à ces contraintes. En transformant le réseau en détecteur et aussi en outil de sécurisation, elle permet de repérer rapidement les menaces à partir des anomalies du réseau pour les placer ensuite en quarantaine avant qu'elles ne puissent se propager latéralement et causer plus de dommages.

Parallèlement au déploiement de son architecture avancée, Cisco simplifie l'achat de fonctions de sécurité avancée pour le data center, les filiales et la périphérie d'accès grâce à son offre Cisco ONE. En choisissant d'acquérir une solution logicielle de sécurité par le biais de Cisco ONE, les clients bénéficient des avantages suivants :

Suites logicielles simples et complètes, prédéfinies pour chaque domaine ;

Possibilité de commencer par le domaine de leur choix ;

Accès aux fonctions et informations les plus récentes concernant les menaces ;
Prévisibilité des investissements grâce aux offres d'abonnement.

Pour que les clients puissent mieux sécuriser leurs réseaux, Cisco ONE leur permet d'acquérir des fonctionnalités logicielles adaptées à leurs besoins présents, tout en protégeant leurs investissements futurs. Avec Cisco ONE, Cisco se différencie également de nombreux autres fournisseurs de produits ciblés, puisque les clients peuvent couvrir davantage de points du réseau et profiter d'une sécurité approfondie.

La migration vers le modèle Cisco ONE devrait être la priorité absolue de toute entreprise souhaitant améliorer sa sécurité. Par conséquent, les recommandations de ZK Research sont les suivantes :

Repenser la sécurité à l'ère numérique. Les méthodologies de sécurité traditionnelles ont été mises au point à une époque où l'IT avait la mainmise sur les applications, les terminaux et le lieu de travail des utilisateurs. Cette époque est révolue et l'IT ne dispose plus d'un tel contrôle. Les entreprises doivent adopter une approche centrée sur les menaces, qui valorise le réseau (l'actif omniprésent dans l'entreprise), surveille l'ensemble du trafic et identifie rapidement les violations de sécurité.

Minimiser le nombre de fournisseurs de solutions de sécurité. L'enquête ZK Research de 2016 sur la sécurité montre que les entreprises font appel à 32 fournisseurs de solutions de sécurité en moyenne. Une telle multiplicité de prestataires aboutit à un environnement ingérable, truffé de nombreux angles morts, de faux-positifs et d'informations incohérentes. L'objectif devrait être de minimiser le nombre de fournisseurs de solutions de sécurité pour améliorer les performances et simplifier la gestion. Bien qu'il soit sans aucun doute nécessaire de recourir à plusieurs prestataires, les entreprises doivent choisir un fournisseur principal capable de mobiliser un large écosystème de partenaires pour offrir une interopérabilité transparente.

Les clients devraient envisager Cisco ONE pour la sécurité de leur réseau. Ce livre blanc en atteste, Cisco ONE est plus avantageux que les modèles d'achat traditionnels en termes de coût mais aussi d'innovation. ZK Research estime que Cisco ONE est le modèle d'achat optimal pour la sécurité du data center, du WAN et de l'accès à l'ère numérique.

CONTACT

zeus@zkresearch.com

Mobile : +1 301-775-7447
Bureau : +1 978-252-5314