Approche tout périphérique de Cisco, pour la productivité, la sécurité, la compétitivité

Présentation

Tandis que le périmètre réseau classique des entreprises continue de s'effacer et que les entreprises évoluent de plus en plus dans des environnements sans frontières, les smartphones, tablettes, les autres périphériques se trouvant à l'extrémité et les applications Web changent irrémédiablement la manière dont les utilisateurs travaillent et jouent en ligne. Cisco a adopté la stratégie « Tout périphérique » qui offre aux employés un plus vaste choix de périphériques tout en conservant une expérience utilisateur prévisible commune qui préserve ou améliore la compétitivité, la productivité et la sécurité des entreprises au niveau international.

Les PME-PMI et les grandes entreprises doivent déterminer si elles autorisent ou refusent l'accès de certains utilisateurs, périphériques ou emplacements aux réseaux, aux données et aux services des entreprises. S'appuyant sur les expériences réelles et les résultats de Cisco, ce livre blanc aborde les étapes et les décisions commerciales que les responsables de la sécurité des informations, les responsables des technologies de l'information et les architectes de sécurité des informations doivent considérer lorsqu'ils se lancent dans l'aventure « Tout périphérique ».

Introduction

Chaque jour, 80 000 employés d'une entreprise internationale allument divers périphériques Windows, 17 000 se connectent à des ordinateurs Macintosh, 7 000 utilisent des machines Linux et 35 000 consultent leurs calendriers et e-mails sur leurs smartphones Blackberry, iPhone et Android[1]. Cette société s'appelle Cisco Systems, Inc. Plus de 70 000 employés et 30 000 consultants, conseillers et partenaires commerciaux veulent disposer d'un plus vaste choix en termes de périphériques de travail et de lieu d'utilisation de ces périphériques pour accéder aux réseaux, systèmes, applications, données et services en ligne de l'entreprise. Bien que la grande majorité des employés Cisco utilisent à la fois un ordinateur et un smartphone pour accéder aux services IT de l'entreprise, plus de 20 % utilisent plus de deux périphériques. En outre, la diversité de ces périphériques augmente de manière exponentielle.

Comme nous l'avons mentionné précédemment, Cisco a adopté une stratégie à long terme appelée « Tout périphérique ». Elle vise à proposer un plus vaste choix de périphériques tout en conservant une expérience utilisateur prévisible commune qui préserve ou améliore la compétitivité et la sécurité de l'entreprise au niveau international.

Les principales raisons commerciales à l'origine de la stratégie « Tout périphérique » sont les suivantes :

- **Productivité :** Cisco permet aux employés férus de technologie d'utiliser leurs smartphone, tablette ou ordinateur portable pour travailler, à tout moment et partout, ce qui améliore leur satisfaction et leur productivité. **On estime que la productivité au travail a augmenté de 30 minutes par jour.**[2]
- **Des employés qui changent :** la nouvelle génération actuelle de férus de technologie qui intègre les collaborateurs de Cisco est habituée à contrôler ses outils et son environnement de travail. Elle veut également **choisir la manière dont elle peut améliorer sa productivité**.
- **Innovation :** autoriser les employés à utiliser des périphériques de nouvelle génération dès leur sortie sur le marché peut générer des gains de productivité supplémentaires. Ces **consommateurs précoces annoncent souvent de plus grands changements sur le marché**, ce qui peut exercer une influence positive sur l'adoption de ces produits par le service informatique de Cisco et la stratégie produits de Cisco.

1. Mesures internes de Cisco à compter du 2ème trimestre de l'exercice 2011
2. Mesures internes de Cisco à compter d'avril 2011

- **Intégration des acquisitions :** les nombreuses entreprises achetées par Cisco rejoignent le groupe avec leurs propres pools de périphériques non standard. La stratégie « Tout périphérique » permet d'intégrer rapidement de nouveaux départements et de réduire les risques de sécurité associés. **La réduction du délai d'intégration des acquisitions est estimée à 17 semaines.**
- **Coûts d'investissement :** la société Cisco emploie des dizaines de milliers de consultants et conseillers dans le monde entier. Elle ne peut pas se permettre de fournir des ordinateurs portables et smartphones à cet effectif en pleine croissance. En faisant migrer les appareils de ses consultants et conseillers vers des périphériques Cisco® VXC (Virtualization Experience Client), Cisco réalise des **économies annuelles estimées à 25 % par utilisateur**, selon des estimations basées sur le coût total d'acquisition actuel des postes de travail.

Chaque entreprise a besoin d'un accès partagé à ses données en temps réel pour des raisons distinctes, par exemple pour sécuriser les données, améliorer la mobilité et développer des environnements de travail favorisant la collaboration. Face au nombre croissant des périphériques se trouvant à l'extrémité, les entreprises doivent déterminer quelles ressources elles autoriseront ou non à accéder aux applications et aux données, à l'intérieur comme à l'extérieur de leur réseau. Ensuite, elles doivent définir comment planifier, suivre, appliquer et assumer ces politiques.

Ce document traite des risques, des avantages et des changements concernant les entreprises, les départements IT et les politiques de sécurité, ainsi que des solutions actuellement mises en œuvre par Cisco. Il aborde également les autres facteurs rencontrés par Cisco lors de l'application de la stratégie « Tout périphérique ».

Étapes relatives à l'adoption de la stratégie « Tout périphérique » de Cisco

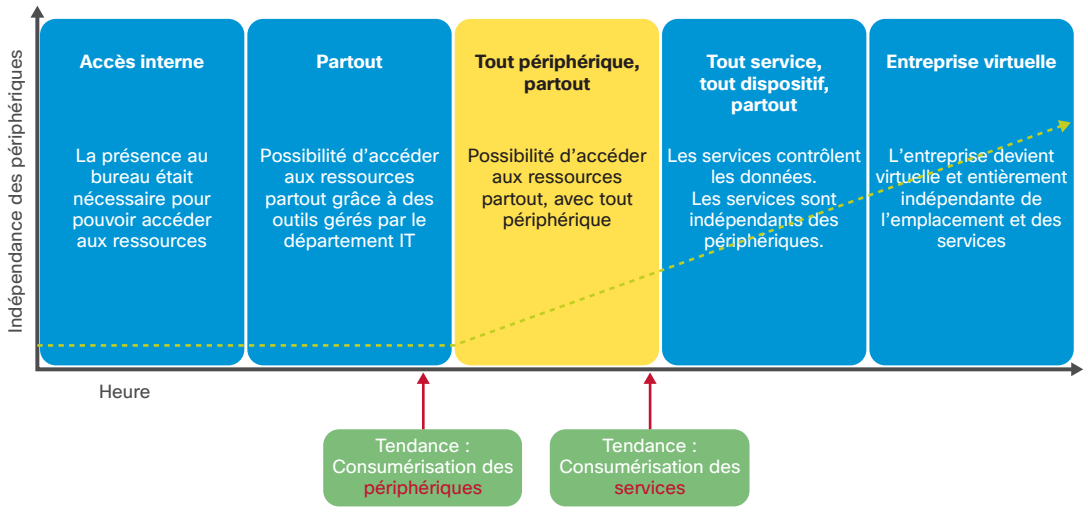
Étape 1 : accès interne

Les 15 dernières années ont été marquées par un changement significatif dans la manière dont les utilisateurs accèdent au réseau Cisco. À la fin du dernier millénaire, tous les périphériques IT se trouvaient au sein de l'entreprise et les employés devaient être physiquement présents dans un bureau pour **accéder en interne** aux ressources IT, comme indiqué dans la première étape de la Illustration 1.

Étape 2 : partout

Au cours du temps, les ordinateurs portables et les VPN ont permis aux employés d'être plus mobiles. En outre, des employés de plus en plus internationaux ont rendu nécessaire l'adoption de modèles de travail plus flexibles. L'étape 2 illustre comment les environnements de travail et les horaires de bureau fixes n'entravent plus la productivité, car des employés plus mobiles accèdent aux ressources informatiques de l'entreprise **partout**, par exemple depuis le site d'un client, son domicile, un café ou un hôtel. L'effacement des frontières géographiques permet aux utilisateurs d'accéder aux ressources partout, grâce à des outils gérés par le département IT.

Illustration 1. Étapes relatives à l'accès des employés aux ressources de l'entreprise au cours de l'adoption de la stratégie « Tout périphérique »



Étape 3 : Tout périphérique, partout

Au cours des dernières années, l'utilisation des smartphones, tablettes et ordinateurs portables s'est banalisée. En outre, de nouvelles fonctionnalités exceptionnelles, la mise à niveau des fonctions, des formats plus efficaces et des cycles de vie plus longs ont été proposés. Les employés ont donc fini par vouloir utiliser leurs propres périphériques pour accéder aux e-mails, à l'intranet et aux applications commerciales de l'entreprise. Ces facteurs sont tous entrés en jeu assez rapidement, ce qui a exercé une pression sur le département IT de l'entreprise. Les employés qui ont rejoint Cisco via une acquisition utilisaient déjà et souhaitaient continuer à utiliser leurs propres périphériques pour travailler. Des milliers de partenaires Cisco extranet avaient également besoin d'accéder à certaines applications. De plus, la mise à disposition de terminaux gérés par le département IT de Cisco impliquait des coûts d'investissement et d'exploitation élevés.

Le département IT de Cisco a reconnu la nécessité d'adopter immédiatement ces technologies de nouvelle génération pour stimuler la productivité. Il a donc choisi d'abandonner l'approche classique qui consiste à limiter et à gérer le déploiement des nouvelles technologies au fur et à mesure qu'elles accèdent à l'environnement de travail. De plus, cette adoption rapide des nouvelles technologies client a entraîné l'introduction et la mise en œuvre d'autres approches, outils et technologies. Ainsi, des communautés d'utilisateurs ont été créées et des changements radicaux ont vu le jour dans la manière dont le département IT gère les problèmes et dans la manière dont les utilisateurs peuvent utiliser les connaissances de leurs pairs pour résoudre des problèmes courants.

Le département IT de Cisco ne contrôle pas ces communautés. Il en fait partie et y contribue au même titre que tout autre membre. Par exemple, l'adoption de produits Apple chez Cisco est née de l'introduction de ces périphériques par les utilisateurs dans l'environnement Cisco. Ils constituaient leur premier choix en termes d'outils et de plates-formes de travail. Les utilisateurs Mac travaillant dans l'environnement Cisco étaient estimés à 3 000 avant que le département IT ne mette officiellement ces outils à leur disposition. Indépendamment du département IT, les utilisateurs Mac ont lancé de nouvelles initiatives pour répondre aux besoins de configuration, d'utilisation et de maintenance au travers d'adresses e-mail, de wikis, de l'intranet et de contenu vidéo. Lorsque le département IT a commencé à proposer les périphériques Mac dans le cadre de sa politique d'actualisation des PC, il a adopté et soutenu le modèle d'assistance autonome mis en place par les utilisateurs Mac, sans perturber ni changer leur communauté. Le département IT a adopté cette structure puis l'a utilisée pour mettre au point d'autres services d'assistance autonome.

L'association de ces facteurs a entraîné la nécessité de développer une nouvelle stratégie de périphériques d'entreprise capable de répondre à la question suivante : *Face à l'effacement des frontières géographiques, comment peut-on permettre aux personnes d'accéder aux ressources de l'entreprise* ***partout****, depuis* ***tout périphérique*** *?*

Tous les employés ne requièrent pas le même niveau ou type d'accès à l'infrastructure de l'entreprise. Certains ont uniquement besoin de services de messagerie et de calendrier sur leur smartphones tandis que d'autres requièrent des privilèges d'accès plus importants. Par exemple, les commerciaux de Cisco peuvent accéder à des outils de commande depuis leur smartphone, ce qui accroît leur capacité à clôturer une vente. Les partenaires extranet de Cisco peuvent utiliser leur propre station de travail pour accéder à un environnement de poste de travail virtuel. Cela permet à Cisco de conserver un plus grand contrôle sur ses ressources.

Étape 4 : Tout service, tout périphérique, partout

Cisco autorise actuellement les utilisateurs à accéder aux ressources hébergées sur site. Dans l'avenir, la consumérisation de services, d'applications, d'espace de stockage et de puissance de traitement offrira une plus grande flexibilité et de meilleurs avantages financiers par rapport aux services IT internes. Pour certains périphériques et dans certains cas d'utilisation, l'accès à des services de cloud externes est déjà nécessaire pour gérer les transactions de l'entreprise (voir la Illustration 2). Cette tendance émergente d'applications et de services sans frontières n'est pas traitée dans ce document. Toutefois, la stratégie « Tout périphérique » de Cisco est une base solide sur laquelle peuvent s'appuyer les futures architectures « **Tout service, tout périphérique, partout** », ainsi que l'idée d'entreprise virtuelle.

Étape 5 : Entreprise virtuelle

L'**entreprise virtuelle** est une évolution logique de l'étape 4, au cours de laquelle une entreprise devient de plus en plus indépendante en termes d'emplacement et de services. Elle dispose d'un modèle d'identité avancé qui permet un contrôle d'accès granulaire et une collaboration externe. De plus, tous les contrôles et fonctionnalités de sécurité s'appliquent aux données de l'entreprise. Nous aborderons la notion d'entreprise virtuelle lorsque nous serons plus engagés dans cette future voie.

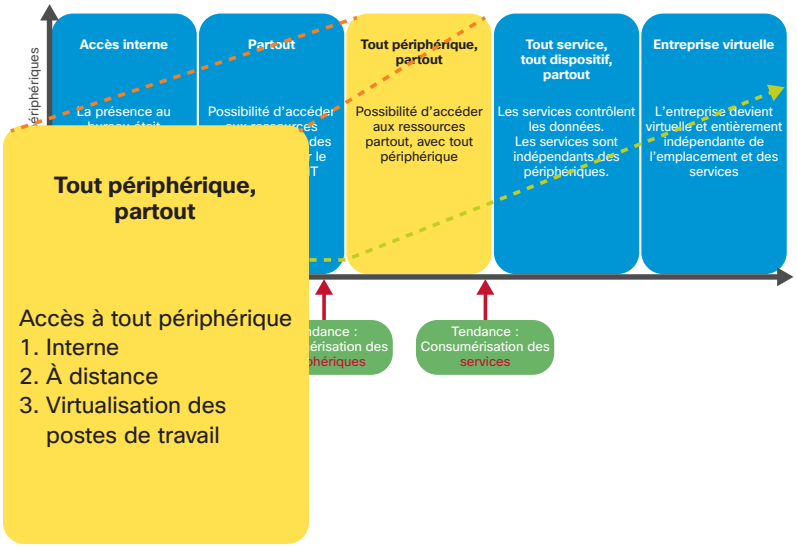
Accès sur tout périphérique, partout

Ce paragraphe décrit les étapes suivies par Cisco pour proposer une architecture « Tout périphérique » plus avancée, y compris la manière dont la stratégie « Tout périphérique » a défié les normes de sécurité classiques et les solutions déployées par Cisco sur son réseau.

Lors de l'implémentation de solutions « Tout périphérique », Cisco s'est concentré sur trois cas d'utilisation :

- Accès distant
- Accès interne
- Accès aux postes de travail virtualisés

Illustration 2. Trois manières d'accéder au réseau de l'entreprise avec tout périphérique



Accès distant depuis tout périphérique

Étape 1 : Accès à un serveur proxy depuis tout périphérique

Face à l'adoption massive de smartphones mobiles au cours des 5 dernières années, le département IT de Cisco devait rapidement trouver une solution pour autoriser l'accès aux ressources de l'entreprise depuis des périphériques comme Palm, Windows Mobile, Nokia, iPhone, Android et autres. Bien que cet accès comportait des avantages en termes de productivité, il posait aussi des risques significatifs (voir le panneau situé sur le côté : Risques potentiels de la stratégie « Tout périphérique »). Cisco a opté pour une approche pragmatique en fournissant aux périphériques mobiles un ensemble de services contrôlés (messagerie et calendrier) via l'accès à un serveur proxy. Les utilisateurs peuvent choisir leur périphérique tandis que Cisco applique des politiques de sécurité qui optimisent la sécurité et la confidentialité des données. Par exemple, les utilisateurs doivent configurer et saisir un PIN à quatre chiffres pour accéder à leur messagerie ou à leur calendrier. Le service est verrouillé au bout de dix tentatives de connexion infructueuses, et la session de l'utilisateur expire après 10 minutes d'inactivité. De plus, en cas de perte ou de vol d'un smartphone, l'employé doit simplement appeler le représentant du service d'assistance Cisco qui peut émettre une commande d'effacement des données pour le périphérique.

Bien que cette approche ne protège pas des fraudes, l'entreprise aurait été encore plus en danger si elle ne l'avait pas adoptée. Les périphériques mobiles accédaient continuellement au réseau de l'entreprise via une connexion LAN sans fil (WLAN). De plus, certains utilisateurs choisissaient des fonctionnalités d'accès échappant au contrôle de l'entreprise, telles que la messagerie instantanée de Yahoo et Gmail. Cisco n'avait donc quasiment pas de contrôle sur l'état de sécurité de son réseau avant le déploiement de ce service. En permettant aux utilisateurs d'accéder à leur messagerie depuis des périphériques mobiles, Cisco leur a fourni une offre d'accès séduisante avec une fonctionnalité de contrôle d'accès simple, mais efficace. Jusqu'à présent, Cisco a protégé environ 35 000 périphériques portables[3] grâce à cet accès mobile à la messagerie. Les exigences de sécurité augmenteront à mesure que Cisco permettra d'accéder à d'autres ressources de l'entreprise depuis les smartphones.

3. Mesures internes de Cisco à compter de mai 2011

Étape 2 : Accès à distance complet depuis tout périphérique

Après avoir mis en œuvre les services de messagerie mobiles pour les périphériques portables, le département IT de Cisco a commencé à étendre l'accès à distance à tous les périphériques portables. Traditionnellement, les employés distants dotés d'ordinateurs portables fournis par le département IT accédaient au réseau de l'entreprise Cisco à l'aide de VPN. Cependant, les employés demandaient de plus en plus à pouvoir utiliser divers ordinateurs Mac, Windows et Linux, qu'ils soient fournis ou non par le département IT. En outre, face à la popularité croissante des tablettes PC, les utilisateurs de ces périphériques souhaitaient aussi disposer d'un accès à distance. Ces demandes ont posé un problème de taille au paradigme Cisco en matière de sécurité pour les ressources contrôlées par le service informatique.

Par conséquent, Cisco a introduit le concept de « périphérique sécurisé ». Un périphérique sécurisé peut être de tout type, mais doit respecter certaines normes de sécurité pour bénéficier d'un accès à distance complet au réseau de l'entreprise. Cisco définit les périphériques sécurisés à l'aide des principes architecturaux suivants :

- Contrôle de l'état de sécurité des périphériques : Cisco doit pouvoir identifier chaque périphérique qui pénètre dans le réseau de l'entreprise et l'associer à un utilisateur spécifique. Il doit aussi pouvoir contrôler l'état de sécurité des périphériques utilisés pour se connecter aux services de l'entreprise. Cette fonctionnalité est importante pour les équipes Cisco chargées de la gestion des incidents.
- Authentification et autorisation des utilisateurs : Cisco exige que les utilisateurs de l'entreprise soient authentifiés. L'authentification permet d'identifier les utilisateurs tout en empêchant l'accès non autorisé à leurs informations d'identification. En outre, Cisco empêche l'authentification des anciens employés et bloque leur accès aux ressources et aux données de l'entreprise.
- Stockage des données sécurisé : les activités utilisées pour les services de l'entreprise (par exemple, la lecture des e-mails, l'accès aux documents ou la collaboration à l'aide de la plate-forme de collaboration d'entreprise Cisco Quad™) doivent garantir la protection de toutes les données stockées localement sur le périphérique. Les utilisateurs doivent pouvoir stocker des données de l'entreprise sur le périphérique et y accéder sans risquer de les divulguer, ce qui pourrait donner lieu à un accès non autorisé.

Politique relative aux périphériques sécurisés

Il est nécessaire de transcrire les principes relatifs aux architectures en spécifications techniques afin d'aider les entreprises à adopter des solutions pouvant être mises en œuvre. Les périphériques sécurisés doivent respecter les exigences suivantes relatives à l'application de la politique et à la gestion des ressources :

Application de la politique

Les périphériques qui accèdent aux services de l'entreprise doivent passer les contrôles de sécurité suivants avant de se connecter. En cas de suppression non autorisée de ces contrôles, l'accès aux ressources de l'entreprise doit être bloqué :

- Contrôles d'accès local avec mots de passe sécurisés (complexité), délai d'inactivité de 10 minutes et verrouillage après 10 tentatives de connexion infructueuses
- Chiffrement des données incluant le chiffrement des périphériques et des supports amovibles
- Fonctionnalité d'effacement et de verrouillage à distance en cas de désactivation d'un compte employé ou de perte ou vol d'un périphérique
- Fonctionnalité de suivi des stocks pour vérifier la présence de logiciels de sécurité spécifiques, mises à jour de correctifs et applications de l'entreprise

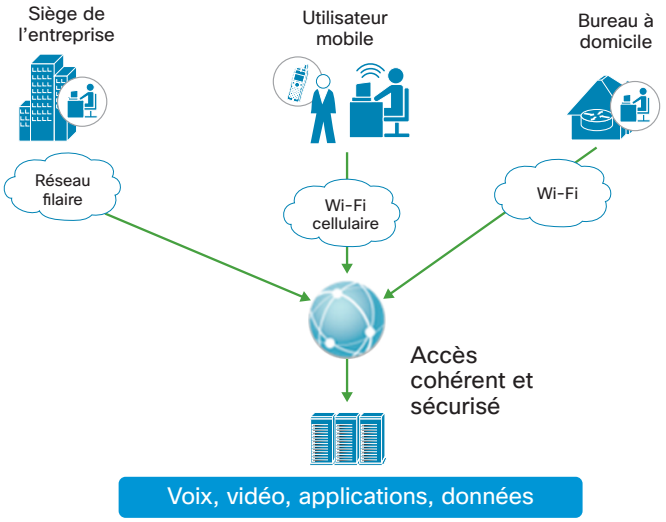
Gestion des ressources

Les périphériques qui accèdent aux services de l'entreprise doivent respecter les contrôles suivants :

- Particulièrement identifiables lorsque l'identification n'est pas usurpée de façon commune
- Autorisés de manière explicite et individuelle à accéder aux ressources de l'entreprise, avec un enregistrement et un suivi associés à un utilisateur spécifique
- Capables de bloquer l'accès aux ressources de l'entreprise
- Capables de produire des données de journaux d'analyse (par exemple, journaux de logiciels de sécurité, authentification et autorisation des utilisateurs et modifications de la configuration)

Face au nombre si élevé d'utilisateurs qui choisissent eux-mêmes leurs périphériques mobiles et les connectent au réseau de l'entreprise, le réseau devient vulnérable et met en péril les ressources IT et les données. La solution Cisco AnyConnect™ Secure Mobility inclut un client VPN, les appareils Cisco ASA (Adaptive Security Appliance) en guise de pare-feu et de tête de réseau VPN, ainsi que la sécurité Web de Cisco basée sur le cloud ou sur site. Elle répond à ce problème en offrant une expérience de connectivité intelligente, transparente et toujours active grâce à une application des politiques de sécurité complète, préventive et sensible au contexte. Elle permet aussi une mobilité sécurisée sur les périphériques mobiles gérés et non gérés (Illustration 3).

Illustration 3. Cisco AnyConnect Secure Mobility



Le client VPN SSL (Secure Sockets Layer) Cisco AnyConnect répond à grand nombre des problèmes de sécurité liés à l'utilisation, par les employés Cisco, de périphériques non contrôlés et non gérés par le département IT. Le département IT de Cisco autorise uniquement l'accès aux périphériques enregistrés. Pour s'assurer qu'un périphérique tentant d'établir une session VPN SSL est enregistré, l'application Cisco AnyConnect compare le certificat du périphérique avec son numéro de série. Pour enregistrer un périphérique, il est nécessaire de l'associer à une personne, ce qui facilite les recherches liées à la sécurité et permet de responsabiliser les utilisateurs.

Le département IT de Cisco utilise les appareils ASA (Adaptive Security Appliance) de la gamme Cisco ASA 5500 pour vérifier la conformité des périphériques avec les normes de sécurité de l'entreprise. Par exemple, les utilisateurs Cisco doivent configurer un mot de passe de verrouillage d'écran pour pouvoir établir une connexion VPN. Cisco AnyConnect empêche les utilisateurs autres que les employés de Cisco de se connecter au réseau de l'entreprise à l'aide de périphériques trouvés. Si un employé informe le département IT de Cisco qu'il a perdu un périphérique, le département IT peut immédiatement désactiver toutes les sessions VPN actives et empêcher toute connexion VPN ultérieure depuis ce périphérique. Le service informatique de Cisco peut aussi désactiver facilement le compte d'un employé quittant l'entreprise.[4] La sécurité sur les iPhones et sur les périphériques mobiles Nokia et Android est encore plus draconienne, car les certificats de ceux-ci sont distribués par une solution de gestion de périphérique mobile. Cette solution permet d'appliquer les politiques de sécurité de manière plus rigoureuse, de gérer les stocks et d'effacer les périphériques à distance en cas de perte ou de désactivation d'un compte employé.

Cisco œuvre actuellement à l'intégration du client Cisco AnyConnect à la solution Cisco ScanSafe pour garantir une sécurité Web basée sur le cloud. Il est également en train de l'intégrer à l'appareil de sécurité Web Cisco IronPort™ afin de garantir une sécurité Web sur site. Ces solutions complémentaires protègent les utilisateurs des programmes malveillants basés sur le Web, qu'ils soient connectés ou non via une session VPN SSL active. La solution Cisco ScanSafe bloque les infections de programmes malveillants, ce qui permet de maintenir protégés les périphériques et le réseau de l'entreprise, même si les utilisateurs visitent des URL malveillantes lorsqu'ils ne sont pas connectés au réseau de l'entreprise ni à un VPN.

Risques potentiels de la stratégie « Tout périphérique »

Les entreprises doivent prévoir de se protéger contre les risques potentiels liés à la stratégie « Tout périphérique », à savoir :

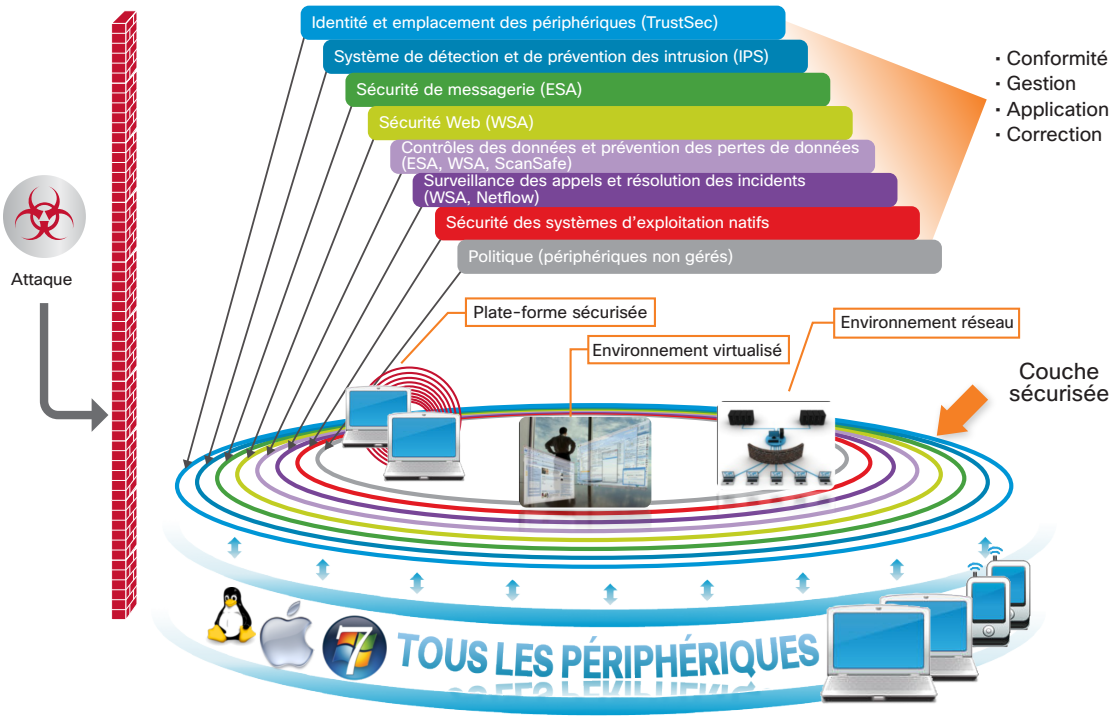
- Perte du contrôle des données d'entreprise stockées sur le périphérique, y compris les données réglementaires ou de clients
- Perte du contrôle de l'emplacement des périphériques :
  - Lorsque la sécurité générale des périphériques est moins contrôlée, le risque d'incidents est plus élevé et l'infrastructure et les services Cisco sont plus vulnérables aux attaques
  - Il se peut que les périphériques ne soient pas conformes aux modèles de politiques et aux modèles opérationnels, ce qui peut porter préjudice aux relations commerciales ou nuire aux exigences légales et réglementaires
- Une visibilité réduite sur les périphériques connectés au réseau (c'est-à-dire sur leur emplacement, leur propriétaire et leur utilisateur) entraîne des problèmes en termes de sécurité, de licence, d'assurance réglementaire et juridique et de contrôle.

4. Consultez le document www.cisco.com/web/about/ciscoitatwork/downloads/ciscoitatwork/pdf/Cisco_IT_Case_Study_AnyConnect_Deployment.pdf

Accès interne depuis tout périphérique Cisco

Étape 1 : Priorité au contrôle des programmes malveillants basés sur le réseau
Les périphériques appartenant à l'entreprise jouent un rôle essentiel dans la préservation de la sécurité et de l'intégrité des données de l'entreprise. Cisco protège de manière exceptionnelle ses environnements à hébergement géré grâce à l'installation et à la gestion de plusieurs couches de protection sur ses propres ordinateurs déployés. Cette protection inclut des fonctionnalités antispam, antispyware, antivirus géré, un système de prévention des intrusions basé sur hôte et une fonction de gestion des correctifs. Or, comme Cisco utilise de moins en moins les environnements à hébergement géré et les périphériques appartenant à l'entreprise, il doit déplacer ces contrôles de terminaux vers le réseau géré. Actuellement, pour protéger son réseau, Cisco utilise des outils tels que les appareils de sécurité Web Cisco IronPort, les appareils de sécurité de messagerie électronique Cisco IronPort, les systèmes Cisco de prévention des intrusions, ainsi que des systèmes de protection NetFlow développés par des tiers, une protection contre les programmes malveillants de type « zero day » et des outils de gestion des événements.

Illustration 4. Contrôles de sécurité réseau dans un environnement « Tout périphérique » de Cisco



Installé à la périphérie d'Internet, un serveur proxy de sécurité tel que l'appareil de sécurité Web Cisco IronPort permet de réduire significativement les menaces entrantes provenant des réseaux filaires et sans fil. Le déploiement de l'appareil de sécurité Web Cisco IronPort répond aux exigences de sécurité réseau de la stratégie « Tout périphérique » de Cisco tout en protégeant l'entreprise. Lors de son déploiement initial au niveau des passerelles Internet Cisco dans la région Est des États-Unis, l'appareil de sécurité Web a bloqué plus de 3 millions de transactions malveillantes[5] en 45 jours[6].

L'appareil de sécurité de messagerie électronique Cisco IronPort est une passerelle de messagerie dotée d'un système avancé de prévention des menaces pour lutter contre les spams, virus, programmes malveillants et attaques ciblées. L'appareil inclut des contrôles du trafic sortant, la prévention de la perte des données, l'application des politiques d'utilisation acceptable et le chiffrement basé sur messages. L'intégration de la sécurité de messagerie au sein du réseau protège de nombreux périphériques et améliore la productivité. Par exemple, en un mois, l'appareil de sécurité de messagerie électronique Cisco IronPort a bloqué 280 millions[7] de messages électroniques destinés à des adresses Cisco.com, ce qui représente 88 % des tentatives.

5. Y compris les téléchargements de programmes malveillants, les logiciels de piratage de navigateur, les logiciels de publicité indésirable, les enregistrements effectués par les réseaux de zombies etles connexions de chevaux de Troie (porte dérobée)
6. Du 14 avril au 31 mai 2011
7. Données du 1er trimestre de l'exercice 2011

Cisco compte également sur les fonctionnalités de détection du système de prévention des intrusions Cisco pour fournir des services intelligents de surveillance réseau et d'envoi d'alertes. Le département IT et l'équipe de sécurité des informations de Cisco peuvent effectuer rapidement tout type d'analyse sur les menaces, ce qui leur permet d'identifier le terminal et de résoudre le problème. Comme le système de prévention des intrusions Cisco est accessible depuis des appareils dédiés ou intégré dans le pare-feu, les commutateurs et les plates-formes de routage Cisco, il est déployé sur tous les sites Cisco du monde entier. L'étendue de ce déploiement permet à l'équipe Cisco chargée de la résolution des incidents de sécurité informatique (CSIRT) de réagir rapidement à tout incident survenant dans l'ensemble du réseau. Comme le département IT de Cisco est passé de périphériques loués et gérés à des périphériques fournis par l'utilisateur, il est désormais capital de pouvoir contrôler minutieusement la couche réseau. Face à la perte de visibilité sur les périphériques, il est nécessaire d'investir dans des technologies capables de fournir des informations complètes en temps réel sur les menaces au niveau de la couche réseau.

Étape 2 : Renforcement du contrôle d'accès des périphériques
Auparavant, l'équipe CSIRT de Cisco comptait énormément sur les systèmes IT (tels que les systèmes de gestion des stocks et des ressources et les systèmes de gestion des hôtes) pour associer les périphériques impliqués dans des incidents à des utilisateurs. Si un périphérique présentait un risque, l'équipe CSIRT de Cisco pouvait le rechercher dans les systèmes de gestion des stocks matériels et logiciels, l'associer à un utilisateur particulier et indiquer à cet utilisateur de résoudre le problème. Cette solution n'est pas possible dans l'univers « Tout périphérique ». Pour mettre en œuvre la stratégie « Tout périphérique », l'équipe CSIRT de Cisco a remodelé ses systèmes IT. Par exemple, les enregistrements DHCP (Dynamic Host Configuration Protocol) et les adresses MAC sont associés aux identifiants de connexion des applications et non aux identifiants de connexion des périphériques pour aider à déterminer l'identité des utilisateurs.

Dans un avenir proche, l'architecture Cisco TrustSec® permettra de résoudre ce problème. Elle inclura un contrôle d'accès basé sur des politiques, une mise en réseau axée sur l'identité, ainsi que des services d'intégrité et de confidentialité des données. Grâce au protocole 802.1x, la connexion réseau Cisco TrustSec identifie les utilisateurs et les associe à leurs périphériques. Elle permet également à Cisco de fournir un accès distinct dans un environnement de réseau dynamique. De plus, elle assure la conformité des politiques de sécurité pour un nombre de plus en plus élevé de consommateurs et de périphériques pouvant être mis en réseau. Par exemple, la technologie Cisco TrustSec peut exploiter le modèle de sécurité propre aux périphériques sécurisés. Lorsque des périphériques sont considérés sécurisés, Cisco leur accorde un accès complet aux ressources de l'entreprise sur le réseau interne. De plus, la plate-forme ISE (Cisco Identity Services Engine) de Cisco, qui associe le contrôle d'identité et le contrôle d'accès, offre une architecture de nouvelle génération pour la gestion de l'identité et des politiques.

Accès aux postes de travail virtualisés depuis tout périphérique

La mobilité et les nouveaux périphériques ont accéléré l'adoption de la stratégie « Tout périphérique » de Cisco. Une autre question a rapidement émergé : comment intégrer les acquisitions d'entreprise et gérer les relations extérieures extra-territoriales et hors site ?

Au cours des dernières années, Cisco a fait l'acquisition de nombreuses entreprises dont l'intégration a posé des problèmes au département IT et aux services de sécurité des informations de Cisco. Toutes les entreprises achetées disposaient de leurs propres périphériques et de leurs politiques et normes de sécurité spécifiques qui étaient souvent bien différents de ceux utilisés chez Cisco. L'équipe de sécurité des informations de Cisco était chargée de s'assurer que les périphériques de terminaux respectaient les politiques et les normes Cisco. Il n'y avait que deux solutions possibles, chacune présentant ses propres inconvénients. La première consistait à remplacer les périphériques issus des acquisitions par des périphériques fournis et pris en charge par le département IT de Cisco puis à former les employés à leur utilisation. Ce processus aurait entraîné une transition coûteuse et longue qui aurait affecté la productivité pendant des semaines ou des mois. La deuxième option était de conserver les périphériques existants tout en risquant de dégrader la sécurité de l'ensemble de l'entreprise. Une autre solution était nécessaire.

Le passage à l'externalisation affectait également les politiques de l'entreprise. Il y a quinze ans, l'externalisation se limitait aux tâches simples. Aujourd'hui, elle est utilisée dans la plupart des activités de l'entreprise et peut concerner de nombreux processus commerciaux. L'effectif externe actuel de Cisco est supérieur à 45 000 personnes dont 17 000 gèrent des activités quotidiennes sur 350 sites d'entreprises tierces. Cisco entretient également des relations avec des partenaires externes de plus de 200 entreprises tierces différentes.

Actuellement, la plupart de l'effectif externe se trouvant sur et hors site est doté de périphériques pris en charge par le département IT de Cisco et conformes à ses politiques. En matière d'externalisation extra-territoriale et hors site, le département IT de Cisco gère une infrastructure extranet qui prend en charge toutes les connexions réseau des entreprises tierces. Le département IT de Cisco gère 70 % de

l'ensemble des connexions extranet de bout en bout, y compris les périphériques, la connectivité WAN et le réseau distant sur les sites des entreprises tierces. Cependant, comme l'externalisation est devenue plus volumineuse et complexe, ce modèle ne répond plus aux attentes de l'entreprise en termes de coût total d'acquisition et de temps nécessaire pour acquérir des compétences.

La virtualisation des postes de travail et les fonctionnalités de sécurité réseau décrites précédemment permettront de résoudre ce problème tout en offrant des avantages significatifs (voir le panneau situé sur le côté : « Avantages et inconvénients de la virtualisation des postes de travail »). Cisco prévoit que la virtualisation des postes de travail entraînera des économies de coût de plus de 20 % et une amélioration de 40 à 60 % du temps nécessaire pour acquérir des compétences dans le cadre des acquisitions et des lieux d'externalisation extra-territoriaux et hors site. Ce service centralisé, entièrement évolutif et indépendant de l'emplacement permettra aussi d'améliorer la sécurité des données et la conformité des périphériques. Cisco a déjà lancé aux États-Unis un projet pilote de virtualisation des postes de travail avec 2 000 utilisateurs. Il s'appliquera à d'autres sites à travers le monde au cours de l'année 2011.

Leçons retenues par Cisco

La conception et la mise en œuvre d'une stratégie « Tout périphérique » constitue un changement radical pour toute entreprise. Une telle transformation est mieux accueillie et a plus de chances de réussir avec une structure de gestion cohérente. Au cours de la mise en œuvre de la stratégie « Tout périphérique » sur l'ensemble de l'entreprise, le département IT et les responsables de la sécurité des informations de Cisco ont beaucoup appris :

- La mise en œuvre de la stratégie « Tout périphérique » mobilise plusieurs secteurs dont les départements chargés des postes de travail, de la sécurité, de l'infrastructure réseau et des communications.
- Les entreprises doivent recruter un responsable principal unique qui sera chargé de constituer l'équipe pluridisciplinaire, de former les responsables, et de fournir les résultats et les mesures.
- Ne sous-estimez pas les efforts requis pour segmenter les utilisateurs et mener une analyse des utilisateurs. Cette analyse doit servir à déterminer les droits d'accès des utilisateurs aux services. Il s'agit de la première étape lors de la mise en œuvre de la stratégie « Tout périphérique ».

Les entreprises investissent énormément pour respecter les réglementations en vigueur en matière de sécurité, d'intégrité, de confidentialité et de contrôle des données. En 2010, Cisco a actualisé son code de déontologie pour y ajouter les instructions d'utilisation des périphériques privés. De plus, le département de la sécurité des

Avantages et inconvénients de la virtualisation des postes de travail

La virtualisation des postes de travail est un modèle informatique qui centralise les programmes, applications, services et données. Bien que l'expérience utilisateur soit quasiment similaire à celle enregistrée avec un ordinateur classique, les données, le système d'exploitation et les applications ne résident pas entièrement sur le périphérique de l'utilisateur final. Ce modèle informatique également appelé VDI (Virtual Desktop Infrastructure) offre de nombreux avantages potentiels :

- Expérience cohérente : les utilisateurs utilisent la même interface sur tous les périphériques compatibles VDI.
- Amélioration de la productivité : les utilisateurs peuvent accéder aux données et aux applications partout, depuis tout périphérique compatible VDI. L'accès aux applications est souvent plus rapide car l'environnement VDI se trouve dans le data center.
- Risque réduit de programmes malveillants : les départements IT peuvent s'assurer que les applications sont actualisées, que les correctifs sont constamment mis à jour et qu'ils sont bien installés par les utilisateurs.
- Risque réduit de perte de données et de vol de propriété intellectuelle : les données sont centralisées, sauvegardées et disponibles, même en cas de panne, de perte ou de vol du périphérique.
- Délai de commercialisation plus rapide : les utilisateurs importants, tels que le personnel issu d'une entreprise rachetée et les partenaires disposant de leurs propres périphériques, peuvent être intégrés plus rapidement dans l'environnement de l'entreprise.
- Compatibilité des applications : la virtualisation des postes de travail rend les applications de l'entreprise compatibles avec un environnement d'exploitation connu.
- Prise en charge plus facile : il est plus facile de mettre à disposition un poste de travail virtuel qu'un nouveau PC, et la virtualisation se prête bien à un modèle pris en charge de manière centralisée par le département IT.

Or, la virtualisation des postes de travail n'est peut-être pas adaptée à toutes les applications ou communautés d'utilisateurs. Les principaux inconvénients sont les suivants :

- Ne convient pas à certaines applications : il existe actuellement des problèmes avec les applications à bande passante élevée telles que les applications de conception assistée par ordinateur, vidéo et de communications unifiées.
- Ne convient pas à certains périphériques : l'expérience utilisateur en matière de virtualisation des postes de travail n'est pas adaptée à certains périphériques comme les smartphones ou tablettes dotés de petits écrans.
- Plates-formes limitées : la plupart des solutions de virtualisation de postes de travail prennent principalement en charge les périphériques Windows.
- Environnements à latence élevée : VDI fonctionne difficilement dans les environnements réseau à latence élevée.

informations change actuellement un grand nombre de ses politiques de sécurité pour les axer davantage sur les données. Pourtant, dans certains cas, ces investissements peuvent aller à l'encontre de la stratégie « Tout périphérique ». Par exemple, Cisco emploie des médecins et des infirmiers sur site pour fournir des services de santé à ses employés. Les tablettes à écran tactile jouent un rôle essentiel pour ces professionnels de la santé car ils peuvent les transporter de patient à patient dans une structure de soins et les utiliser en association avec le système de conférences Cisco TelePresence® pour diagnostiquer et traiter les patients à distance. Néanmoins, ces tablettes sont soumises à la loi américaine HIPAA (Health Insurance Portability and Accountability). Cisco n'autorise pas ces professionnels de la santé à utiliser leurs propres tablettes dans ce contexte. En outre, Cisco veille au respect des protocoles de sécurité et de gestion des données uniquement pour les périphériques appartenant à l'entreprise.

Premières étapes dans la mise en œuvre de votre propre stratégie « Tout périphérique »

Comme Cisco s'est aventuré dans la stratégie « Tout périphérique », il a identifié 13 secteurs d'activités importants concernés par ce nouveau modèle. Le tableau 1 présente ces secteurs d'activités et fournit une liste de questions qui ont aidé Cisco et peuvent également vous aider, lors de la mise en œuvre de votre stratégie, à identifier les problèmes potentiels et à déterminer la meilleure manière d'y remédier. Lisez ces questions et répondez-y le plus honnêtement possible lors de la mise en œuvre de votre propre stratégie.

Tableau 1. Questions à poser pour la mise en œuvre de la stratégie « Tout périphérique »

Secteur d'activités	Questions relatives aux activités de l'entreprise auxquelles vous devez répondre
Continuité des activités et reprise sur sinistre	· Souhaitez-vous que les périphériques n'appartenant pas à l'entreprise puissent accéder ou non au plan de continuité des activités ? · Souhaitez-vous pouvoir effacer à distance tout périphérique accédant au réseau s'il a été volé ou perdu ?
Gestion des hôtes (application de correctifs)	· Les périphériques n'appartenant pas à l'entreprise seront-ils autorisés à accéder aux flux de gestion des hôtes de l'entreprise ?
Gestion de la configuration des clients et validation de la sécurité des périphériques	· Comment souhaitez-vous valider et maintenir actualisée la conformité des périphériques aux protocoles de sécurité ?
Stratégies d'accès à distance	· Qui doit être autorisé à accéder à quels services et plates-formes sur quels périphériques ? · Les employés externes doivent-ils obtenir les mêmes droits d'accès que les autres aux périphériques, aux applications et aux données ?
Licences logicielles	· Souhaitez-vous modifier les politiques pour qu'elles autorisent l'installation de logiciels sous licence de l'entreprise sur des périphériques n'appartenant pas à l'entreprise ? · Les contrats de licence des logiciels existants prennent-ils en compte les utilisateurs qui accèdent à la même application logicielle depuis plusieurs périphériques ?
Exigences relatives au chiffrement	· Les périphériques n'appartenant pas à l'entreprise doivent-ils respecter les exigences en vigueur en matière de chiffrement de disque ?
Authentification et autorisation	· Souhaitez-vous que les périphériques n'appartenant pas à l'entreprise adhèrent aux modèles Active Directory de Microsoft ou soient autorisés à y adhérer ?
Gestion de la conformité réglementaire	· Quelle sera la politique de l'entreprise à propos de l'utilisation de périphériques qui ne lui appartiennent pas dans des situations dangereuses ou quand les exigences de conformité sont élevées ?
Gestion des incidents et recherches	· Comment les solutions de sécurité et de confidentialité informatiques géreront-elles les incidents et les recherches liés aux périphériques n'appartenant pas à l'entreprise ?
Interopérabilité des applications	· Comment l'entreprise gèrera-t-elle les tests d'interopérabilité des applications avec les périphériques qui ne lui appartiennent pas ?
Gestion des ressources	· L'entreprise a-t-elle besoin de modifier la manière dont elle identifie ses propres périphériques afin de pouvoir identifier ceux qui ne lui appartiennent pas ?
Assistance	· Quelles seront les politiques de l'entreprise relatives à l'assistance des périphériques qui ne lui appartiennent pas ?

L'avenir

La stratégie « Tout périphérique » mise en œuvre chez Cisco constitue un investissement continu et durable. Au cours des prochaines années, Cisco continuera de déplacer les données et les applications importantes des périphériques vers le réseau ou vers le cloud, de renforcer la sécurité réseau et d'intégrer les contrôles d'identité et de politiques sur les périphériques lorsqu'ils se connectent au réseau. Les prochaines étapes de ce plan permettront de résoudre les problèmes liés à la stratégie « Tout périphérique » dans les secteurs d'activités suivants :

Interopérabilité des applications

Environ 60 % des périphériques qui se connectent actuellement au réseau Cisco sont des postes de travail Windows. Cependant, ce pourcentage diminue au fur et à mesure que la popularité des autres périphériques augmente. Avec le temps, Cisco aura moins de contrôle sur le type ou les versions des logiciels installés sur les périphériques, ce qui augmente les risques de problèmes d'interopérabilité entre les applications, navigateurs, versions et environnements d'exécution. La prédominance des applications Web a simplifié le problème, mais ne l'a pas résolu. Le nombre de postes de travail, smartphones et tablettes différents continue d'augmenter tout comme celui des environnements de navigateur. Les dirigeants de Cisco ont lancé une initiative de normalisation des navigateurs, basée sur les normes W3C (World Wide Web Consortium). Les normes industrielles relatives au développement Web facilitent l'interopérabilité des applications dans un environnement comprenant différents navigateurs, systèmes d'exploitation et périphériques.

Cisco s'appuie également sur la virtualisation des postes de travail pour présenter un environnement d'exploitation compatible avec chaque système d'exploitation. Un projet pilote de virtualisation des postes de travail, regroupant actuellement des milliers d'utilisateurs, doit être mis en œuvre auprès de 18 000 employés d'ici juillet 2012.

Licences logicielles

Comme la plupart des entreprises, Cisco utilise des systèmes de gestion des ressources pour effectuer le suivi des licences logicielles. Cisco doit répondre à de nombreuses questions relatives aux politiques en ce qui concerne les divers cas de concession de la licence logicielle « Tout périphérique ».

- Les utilisateurs seront-ils autorisés à installer des logiciels de l'entreprise sur leurs propres périphériques ?
- Les contrats conclus avec les distributeurs de logiciels autoriseront-ils l'installation des logiciels de l'entreprise sur des périphériques qui ne lui appartiennent pas ?
- Cisco devra-t-il effectuer un suivi des périphériques n'appartenant pas à l'entreprise, et si oui, comment ?

Cisco mène des recherches sur l'utilisation des informations recueillies par la technologie Cisco TrustSec, telles que l'identité des utilisateurs et les adresses MAC, pour mettre en œuvre un système de gestion des ressources qui effectue un suivi de l'ensemble des périphériques et déployer des mécanismes de génération de rapports détaillés qui prennent en compte les ressources matérielles et logicielles n'appartenant pas à l'entreprise.

Continuité des activités et reprise sur sinistre

Cisco emploie des personnes qui ont accès aux ressources internes et qui travaillent sur les sites d'entreprises tierces, ainsi que de nombreux consultants qui travaillent dans les bureaux Cisco du monde entier. Qui est chargé de veiller à la sécurité et à l'intégrité de ces données ? Cisco sauvegarde ses PC Windows de manière centralisée. Or, un grand nombre de ses partenaires refusent que leurs ressources confidentielles soient sauvegardées sur le système d'une entreprise tierce. Si les utilisateurs ne sont pas inclus dans les services de continuité des activités de l'entreprise, quel autre système est utilisé pour que ces utilisateurs puissent continuer à travailler rapidement en cas de panne ? La virtualisation des postes de travail peut être une solution. Elle permet de ne plus stocker de données sensibles sur les périphériques.

Cisco a commencé à gérer les interactions de ses utilisateurs sur l'ensemble du réseau. L'entreprise se dirige en toute confiance vers un avenir où un nombre réduit d'applications et de données résident sur les postes de travail grâce à l'association de la virtualisation des postes de travail et des services SaaS (Software as a Service) ou du cloud computing. Certains sites et applications de l'entreprise suivront une approche davantage tournée vers les transactions. Celle-ci permettra de gérer, de sauvegarder et d'effectuer un suivi des utilisateurs, des actions et des données, de manière cohérente. Cette évolution permettra au département IT de Cisco d'adopter ultérieurement la stratégie efficace et sécurisée « Tout service, tout périphérique, partout », puis à terme, de virtualiser l'entreprise.

Informations complémentaires

Cisco avance à grands pas vers la mise en œuvre d'un environnement « Tout service, tout périphérique, partout » au sein de son entreprise. Il continuera à partager ses expériences et les leçons qu'il a apprises pour vous aider à surmonter les problèmes susceptibles de survenir au cours du processus. Les connaissances et la méthodologie utilisées par Cisco pour faire migrer son entreprise et ses environnements IT vers un environnement « Tout périphérique » et au-delà peuvent s'appliquer à d'autres entreprises de petite ou moyenne taille.

Contactez votre représentant Cisco pour savoir quelle stratégie adopter pour préparer vos infrastructures commerciale, informatique et de sécurité à migrer vers des architectures « Tout périphérique ».

Pour plus d'informations sur les solutions Cisco compatibles avec la stratégie « Tout périphérique », consultez les rubriques suivantes :

- Client Cisco AnyConnect Secure Mobility
- Stratégies de virtualisation
- Technologie Cisco TrustSec
- Appareils de sécurité de messagerie électronique Cisco IronPort
- Appareils de sécurité Web Cisco IronPort

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

Siège social en Asie-Pacifique
Cisco Systems (USA) 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 Web de Cisco, à l'adresse **www.cisco.com/go/offices**.

C11-681837-00 08/11

