La vision « Tout périphérique » de Cisco : planifier un avenir productif, sécurisé et compétitif

Ce que vous allez apprendre

Alors que le périmètre du réseau d'entreprise traditionnel continue à s'estomper et que l'entreprise devient progressivement un environnement sans frontières, les téléphones intelligents, les tablettes, les terminaux et les applications Web changent de façon irrémédiable la façon dont les personnes travaillent et jouent en ligne. Cisco a adopté la vision « Tout périphérique » (Any Device) qui élargit le choix de l'employé en matière de périphérique, tout en conservant une expérience utilisateur commune et prévisible qui préserve ou améliore la compétitivité, la productivité et la sécurité générales de l'organisation.

Les entreprises et les grandes organisations doivent décider d'autoriser ou de refuser l'accès de certains utilisateurs, périphériques et emplacements aux réseaux, aux données et aux services de l'entreprise. En s'appuyant sur les expériences et les résultats réels de Cisco, ce livre blanc traite des étapes et des décisions commerciales que les responsables de l'information et de la sécurité ainsi que le service informatique de l'entreprise et les architectes de la sécurité de l'information doivent analyser lorsqu'ils se lancent dans l'aventure « Tout périphérique ».

Introduction

Chaque jour, 80 000 travailleurs d'une multinationale allument une série de périphériques Windows, 17 000 se connectent à des ordinateurs Macintosh, 7 000 utilisent des machines Linux et 35 000 vérifient leur calendrier et leurs courriels sur leur périphérique BlackBerry, iPhone ou Android[1]. Cette multinationale, c'est Cisco Systems, Inc. Nous comptons plus de 70 000 employés et plus de 30 000 contractants, consultants et partenaires commerciaux dans le monde entier, qui aspirent tous à pouvoir mieux choisir les périphériques qu'ils utilisent pour travailler (ainsi que les endroits où ils utilisent ces périphériques pour accéder aux réseaux, aux systèmes, aux applications, aux données et aux services en ligne de l'entreprise). Bien que la vaste majorité des travailleurs de Cisco utilisent un ordinateur et un téléphone intelligent pour accéder aux services informatiques de la société, plus de 20 pour cent d'entre eux utilisent plus de deux périphériques (et la diversité de ces périphériques augmente de façon exponentielle).

Comme indiqué ci-dessus, Cisco a adopté une vision à long terme appelée « Tout périphérique ». Son objectif est de permettre un plus grand choix en matière de périphérique tout en conservant une expérience utilisateur commune et prévisible qui préserve ou améliore la compétitivité et la sécurité générales de l'organisation.

Voici les principales raisons commerciales qui sous-tendent la vision « Tout périphérique » :

- **Productivité :** Cisco permet aux employés mordus de technologie d'utiliser le téléphone intelligent, la tablette ou l'ordinateur portable de leur choix pour effectuer leur travail au sein de la société, quand et où ils le souhaitent. Cette approche améliore leur satisfaction professionnelle et leur productivité. **On estime que leur productivité professionnelle augmente de 30 minutes par jour.**[2]
- **Évolution de la main-d'œuvre :** les membres de la génération actuelle des mordus de technologie qui entrent sur le marché du travail sont habitués à contrôler leurs outils et leur environnement de travail, et souhaitent **choisir la méthode à adopter pour être plus productifs**.
- **Innovation :** permettre aux travailleurs d'utiliser des périphériques de nouvelle génération dès leur sortie peut améliorer la productivité. Ces **travailleurs qui adoptent rapidement les nouvelles technologies sont souvent les précurseurs de changements plus importants sur le marché**, ce qui peut influencer positivement l'adoption informatique et la stratégie produit de Cisco.

1. Mesures Cisco internes, au 2e trimestre de l'exercice 2011
2. Mesures Cisco internes, au mois d'avril 2011

- **Intégration des acquisitions :** les nombreuses entreprises acquises par Cisco viennent compléter notre gamme de périphériques non standard. La vision « Tout périphérique » permet d'intégrer les nouvelles divisions rapidement et de minimiser les risques d'insécurité connexes. **On estime que le temps d'intégration des acquisitions est réduit de 17 semaines.**
- **Coûts en capital :** Cisco emploie des dizaines de milliers de contractants et de consultants de par le monde. Il n'est pas financièrement viable de fournir des ordinateurs portables et des téléphones intelligents détenus par Cisco à cette main-d'œuvre croissante. En faisant migrer les contractants et les consultants vers des périphériques Cisco® Virtualization Experience Client (VXC), Cisco réalise des **économies annuelles estimées à 25 pour cent par utilisateur** (calcul réalisé sur la base du coût total de propriété de nos postes de travail).

D'autres organisations adoptent cette stratégie pour des raisons distinctes, telles que la sécurité des données, l'augmentation de la mobilité et la collaboration sur les environnements de travail, qui expliquent la nécessité d'un accès partagé aux données en temps réel. Comme le choix et le nombre de terminaux augmentent, les entreprises doivent se demander quels actifs ont le droit (ou n'ont pas le droit) d'accéder à leurs applications et à leurs données, tant sur le réseau qu'en dehors. Elles doivent ensuite déterminer comment planifier, suivre, contrôler et appliquer ces politiques.

Le présent document traite des risques, des récompenses et des changements qui touchent les politiques commerciales, informatiques et de sécurité. Il présente également les solutions mises en œuvre par Cisco et d'autres considérations rencontrées jusqu'à présent par Cisco dans son application de la vision « Tout périphérique ».

Étapes de la stratégie « Tout périphérique » de Cisco

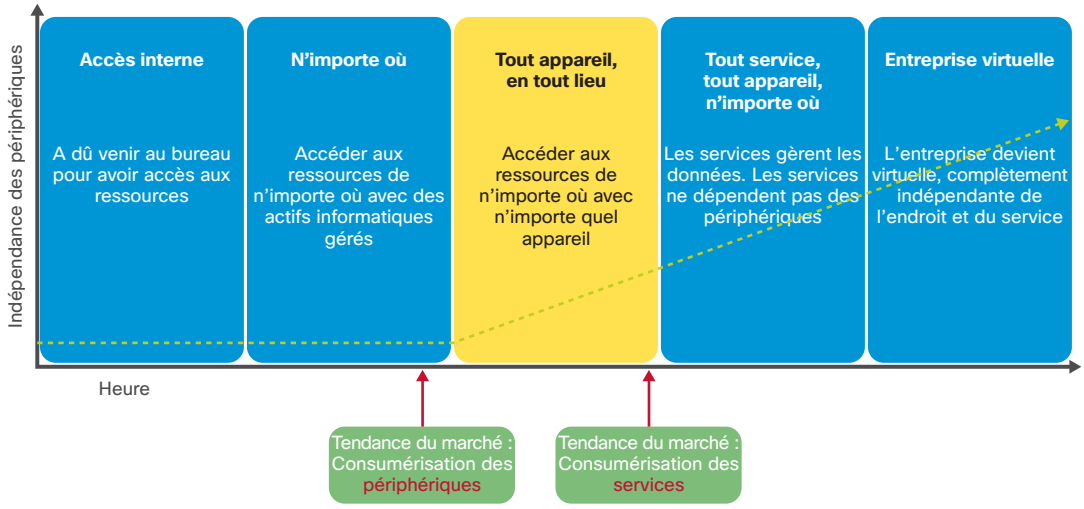
Étape 1 : accès interne

Ces quinze dernières années, l'accès des utilisateurs au réseau Cisco a connu de grands changements. À la fin du dernier millénaire, tous les périphériques informatiques se trouvaient dans les locaux des entreprises et les employés devaient être physiquement dans ces locaux pour avoir un **accès interne** aux ressources informatiques, comme le montre l'étape 1 de la figure 1.

Étape 2 : n'importe où

Avec le temps, les ordinateurs portables et les RPV ont accru la mobilité des travailleurs, et la mondialisation croissante de la main-d'œuvre a rendu nécessaire l'élaboration de modèles de travail plus flexibles. L'étape 2 montre comment les environnements de travail et les horaires de bureau traditionnels cessent alors de limiter la productivité, dans la mesure où une main-d'œuvre plus mobile peut désormais accéder aux ressources informatiques de l'entreprise à partir de **n'importe où**, que ce soit depuis le site d'un client, le domicile d'un employé, un café ou un hôtel. Cette dissolution des frontières physiques permet aux utilisateurs d'accéder aux ressources depuis n'importe où à l'aide de leurs périphériques informatiques.

Figure 1. Les étapes de l'accès de la main-d'œuvre au cours de l'adoption de la vision « Tout périphérique »



Étape 3 : n'importe quel périphérique, n'importe où
Ces dernières années, en raison de la banalisation des téléphones intelligents, des tablettes et des ordinateurs portables (en plus de l'apparition de nouvelles fonctionnalités épatantes, de mises à niveau pour de nouvelles fonctions, de formats plus efficaces et de la réduction des cycles de vie des périphériques), les employés souhaitent utiliser leurs propres périphériques dans toutes les tâches, de l'accès à la messagerie et à l'intranet de la société à l'utilisation des applications de l'entreprise. Les services informatiques ont dû faire face à de nouveaux défis en raison de l'entrée en jeu relativement rapide de ces facteurs. Les employés qui ont rejoint Cisco par le biais d'une acquisition utilisaient déjà leurs propres périphériques pour le travail et souhaitaient continuer. Des milliers de partenaires extranet de Cisco ont également demandé un accès à certaines applications. Or, fournir des terminaux informatiques gérés par Cisco est une solution qui aurait entraîné des coûts d'infrastructures et de fonctionnement élevés.

Le service informatique de Cisco a reconnu la nécessité d'opter pour l'utilisation instantanée de ces technologies de nouvelle génération afin de favoriser la productivité, plutôt que d'utiliser l'approche traditionnelle de limitation et de gestion du déploiement de nouvelles technologies lors de l'embauche des employés. En outre, cette adoption rapide des nouvelles technologies client a entrainé l'émergence et la mise en œuvre d'autres approches, outils et technologies d'entreprise qui ont créé des communautés d'utilisateurs et permis une modification de la prise en charge des services informatiques. Les utilisateurs finaux sont désormais en mesure d'utiliser les connaissances de leurs pairs pour résoudre les problèmes courants.

Le rôle du service informatique de Cisco au sein de ces entreprises n'est pas de posséder, mais de participer et de contribuer en tant que pair. Par exemple, l'introduction de produits Apple au sein de Cisco a tout d'abord eu lieu grâce aux utilisateurs qui apportaient ces périphériques au travail, car il s'agissait des outils et des plates-formes qui leur convenaient le mieux pour travailler. Cisco comptait environ 3 000 utilisateurs de produits Mac avant que le service informatique ne mette ces outils à la disposition du plus grand nombre. Indépendamment du service informatique, les utilisateurs de produits Mac ont été à l'origine d'un nouvel effort pour fournir une aide à la configuration, à l'utilisation et à la maintenance par le biais d'alias de messagerie, de wikis, de l'intranet et de commentaires vidéo. Lorsque le service informatique de Cisco a commencé à proposer les produits Mac comme option dans le cadre de sa politique d'actualisation du parc informatique, il a adopté et pris en charge le modèle autonome sans perturber ou modifier la communauté Mac. Le service informatique a utilisé cette base pour développer des services plus autonomes.

Ensemble, ces facteurs ont démontré la nécessité d'une nouvelle stratégie d'entreprise pour les périphériques. Cette stratégie devait répondre à une question fondamentale, mais urgente : *alors que la frontière des périphériques s'estompe, comment pouvons-nous permettre aux personnes d'accéder aux ressources de l'entreprise à partir de* ***n'importe quel périphérique*** *et depuis* ***n'importe où****?*

Tous les travailleurs n'ont pas besoin du même niveau et du même type d'accès à l'infrastructure de l'entreprise. Certains travailleurs ont seulement besoin d'accéder aux services de messagerie et de calendrier sur leur téléphone intelligent, alors que d'autres ont besoin de niveaux d'accès plus importants. Par exemple, les vendeurs de Cisco peuvent accéder à des outils de commande à partir de leur téléphone intelligent, ce qui améliore leur capacité à clôturer une vente. Les partenaires extranet de Cisco peuvent utiliser leur propre poste de travail pour accéder à un environnement de postes de travail virtuels, ce qui permet à Cisco de garder un contrôle important sur nos actifs d'entreprise.

Étape 4 : n'importe quel service, n'importe quel périphérique, depuis n'importe où
Cisco autorise actuellement les utilisateurs à accéder aux ressources d'entreprise hébergées dans les locaux. À l'avenir, la consumérisation des services (applications, espace de stockage et puissance de calcul) offrira plus de flexibilité et d'avantages financiers que les services informatiques en interne. Certains périphériques et scénarios nécessitent déjà un accès à des services en nuage externe pour les transactions d'entreprise (voir la figure 2). Bien que cette nouvelle tendance vers les applications et les services sans frontières dépasse le champ d'action du présent document, la vision « Tout périphérique » de Cisco est une base solide pour les futures infrastructures concernées par la stratégie **« N'importe quel service, n'importe quel périphérique, depuis n'importe où »** et, en fin de compte, pour la création de l'entreprise virtuelle.

Étape 5 : l'entreprise virtuelle
L'**entreprise virtuelle** est une évolution logique de l'étape 4, dans laquelle l'entreprise devient de plus en plus indépendante vis-à-vis des emplacements physiques et des services. L'entreprise a un modèle identitaire mature qui permet un contrôle de l'accès granulaire et une collaboration externe, et l'ensemble des contrôles et des fonctions de sécurité est appliqué aux données de l'entreprise. Nous reparlerons de l'entreprise virtuelle lorsque nous nous approcherons de cet état futur.

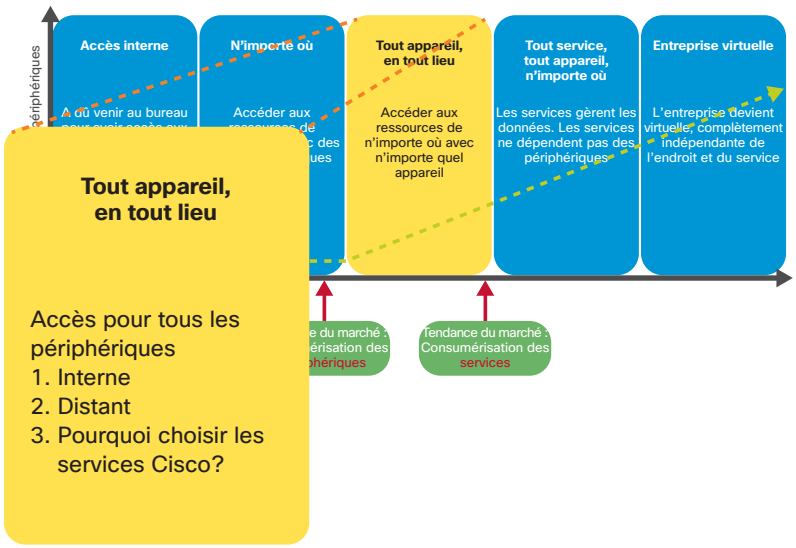
Accès depuis n'importe quel périphérique et depuis n'importe où

Cette section explore les étapes franchies par Cisco pour parvenir à une architecture « Tout périphérique » plus mature, notamment la façon dont la vision « Tout périphérique » compromet les normes de sécurité traditionnelles, ainsi que les solutions que Cisco a déployées sur notre réseau.

En mettant en œuvre plusieurs solutions « Tout périphérique », Cisco s'est concentré sur trois scénarios :

- Accès à distance
- Accès interne
- Accès à la virtualisation des postes de travail

Figure 2. Trois façons d'accéder au réseau de l'entreprise avec la vision « Tout périphérique »



Accès à distance à partir de n'importe quel périphérique

Étape 1 : Accès proxy à partir de n'importe quel périphérique

L'adoption massive des téléphones intelligents au cours des cinq dernières années a augmenté la pression sur le service informatique de Cisco qui a dû autoriser l'accès aux ressources d'entreprise à partir de périphériques tels que Palm, Windows Mobile, Nokia, iPhone, Android et d'autres. Bien que l'autorisation de cet accès ait eu des effets positifs sur la productivité pour Cisco, elle impliquait également des risques importants (voir la barre latérale : « Potential Any Device Risks » [Risques potentiels de la vision Tout périphérique]). Cisco a opté pour une approche pragmatique en fournissant une série de services contrôlés (messagerie et calendrier) sur des périphériques mobiles par le biais d'un accès proxy. Les utilisateurs peuvent choisir leur périphérique, tandis que Cisco applique des politiques de sécurité qui maximisent la sécurité et la confidentialité des données. Par exemple, les utilisateurs doivent configurer et entrer un code PIN à quatre chiffres pour accéder à leur messagerie ou à leur calendrier. Dix tentatives infructueuses verrouillent le service et la connexion expire après dix minutes d'inactivité. Si un téléphone intelligent est perdu ou volé, le travailleur doit tout simplement appeler le représentant du centre d'assistance de Cisco, qui peut envoyer une commande de nettoyage au périphérique.

Bien que cette approche ne soit pas toujours infaillible, le fait de ne pas proposer cette solution aurait entraîné des risques encore plus importants pour l'organisation. De nombreux périphériques mobiles accèdent en permanence au réseau de l'entreprise par le biais d'un LAN sans fil (WLAN) (en plus de ceux qui accèdent à des fonctions non contrôlées par l'entreprise, telles que Yahoo IM et Gmail), Cisco n'avait donc pratiquement aucun contrôle sur notre sécurité avant le déploiement de ce service. En permettant un accès mobile à la messagerie, Cisco a fourni aux utilisateurs un service d'accès intéressant qui intègre un contrôle simple mais efficace. Quelque 35 000 périphériques mobiles protégés[3] bénéficient actuellement d'un accès mobile à la messagerie de Cisco. Lorsque Cisco offre un nouvel accès à d'autres ressources d'entreprise par le biais des téléphones intelligents, les exigences de sécurité sont adaptées en conséquence.

3. Mesures Cisco internes, au mois de mai 2011

Étape 2 : accès à distance complet depuis n'importe quel périphérique

Après avoir mis en œuvre les services de messagerie mobile pour les périphériques mobiles, le service informatique de Cisco a abordé la mise à niveau et l'extension de l'accès à distance pour tous les périphériques portables. Traditionnellement, les télétravailleurs disposant d'un ordinateur portable fourni par le service informatique accédaient au réseau de l'entreprise Cisco à l'aide d'un RPV. Toutefois, le nombre de demandes de travailleurs souhaitant utiliser des ordinateurs Mac, Windows et Linux, qu'ils soient fournis par le service informatique ou non, a augmenté. En outre, la popularité grandissante des tablettes a également engendré des demandes d'accès à distance de la part des utilisateurs de ces périphériques. Ces demandes ont représenté un défi important pour la politique de sécurité de Cisco en ce qui concerne les actifs contrôlés par le service informatique.

En conséquence, Cisco a lancé le concept de « périphérique de confiance ». Un périphérique de confiance peut être n'importe quel type de périphérique, mais il doit respecter certains critères de sécurité pour obtenir un accès distant complet au réseau de l'entreprise. Cisco se base sur les principes architecturaux suivants pour définir la notion de périphérique de confiance :

- **Assurance de l'état de la sécurité du périphérique :** Cisco doit être capable d'identifier des périphériques uniques lorsqu'ils accèdent au réseau de l'entreprise et de les associer à un utilisateur spécifique, ainsi que de contrôler l'état de la sécurité des périphériques utilisés pour se connecter aux services de l'entreprise. Cette fonctionnalité est essentielle pour l'équipe de gestion des incidents de Cisco.
- **Authentification et autorisation des utilisateurs :** Cisco exige que les utilisateurs de l'entreprise soient authentifiés. L'authentification identifie les utilisateurs tout en empêchant les accès non autorisés aux identifiants des utilisateurs. En outre, Cisco évite l'authentification des travailleurs ne travaillant plus pour la société et les empêche d'accéder aux actifs et aux données de l'entreprise.
- **Stockage sécurisé des données :** les activités utilisées pour les services de l'entreprise (par exemple, la lecture de courriels, l'accès aux documents ou la collaboration à l'aide de la plate-forme de collaboration d'entreprise Cisco Quad™) doivent sécuriser les données stockées localement sur le périphérique. Les utilisateurs doivent être capables d'accéder à des données et de les stocker sur le périphérique sans risquer de perdre des données d'entreprise, une situation qui pourrait entraîner un accès non autorisé.

Politique relative aux périphériques de confiance

Les principes d'architecture doivent être traduits en spécifications techniques pour aider les organisations à implémenter des solutions applicables. Les périphériques de confiance doivent respecter les exigences suivantes en matière d'application de la politique et de gestion des actifs :

Application de la politique

Les périphériques qui accèdent à des services d'entreprise doivent valider la mise en œuvre des contrôles de sécurité suivants avant la connexion. La suppression non autorisée de ces contrôles doit désactiver l'accès aux ressources de l'entreprise :

- Contrôles d'accès locaux appliquant un mot de passe fort (complexe), expiration après 10 minutes d'inactivité et verrouillage après 10 échecs de tentative de connexion.
- Cryptage des données comprenant le cryptage des périphériques et des supports multimédias mobiles.
- Fonctions de nettoyage et de verrouillage à distance dans les cas de licenciement d'un employé, ou de perte/vol d'un périphérique.
- Fonction de suivi de l'inventaire pour vérifier la présence d'un logiciel de sécurité spécifique, de correctifs et d'applications d'entreprise.

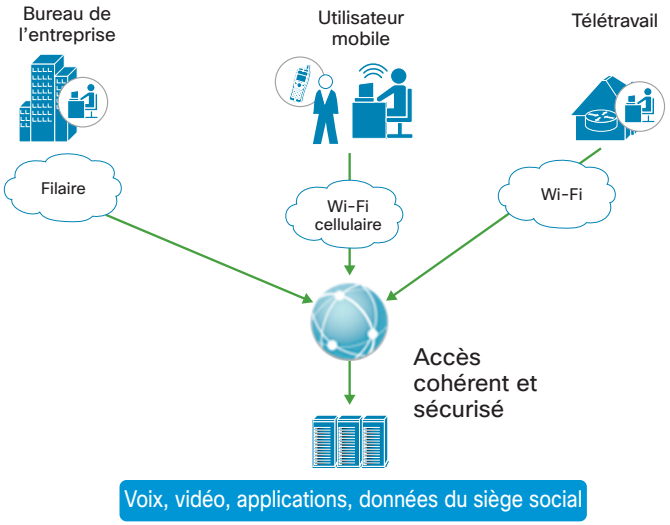
Gestion des actifs

Les périphériques qui accèdent à des services d'entreprise doivent respecter les contrôles suivants :

- Le périphérique doit être identifiable de façon unique selon une méthode empêchant les usurpations triviales.
- Le périphérique doit être explicitement et individuellement autorisé à accéder à l'entreprise. Il doit être enregistré et permettre le traçage jusqu'à un utilisateur spécifique.
- L'accès à l'entreprise doit pouvoir être bloqué.
- Des journaux de données judiciaires (par exemple, sur les logiciels de sécurité, l'authentification et l'autorisation des utilisateurs et les changements de configuration) doivent pouvoir être générés s'ils sont nécessaires pour une enquête.

De nombreux utilisateurs choisissent leurs propres périphériques mobiles et accèdent au réseau de l'entreprise depuis ceux-ci, le réseau devient donc vulnérable aux brèches de sécurité, ce qui menace les actifs informatiques et les données. La solution de mobilité sécurisée Cisco AnyConnect™ (qui inclut un client RPV, les appareils de sécurité adaptatifs de Cisco en tant que pare-feu, une tête de réseau RPV et des dispositifs de sécurité Web dans les locaux ou en nuage) répond à cette inquiétude en proposant une expérience de connectivité intelligente, transparente et toujours active avec une application de la politique de sécurité contextuelle, exhaustive et préventive et une mobilité sécurisée sur les périphériques mobiles gérés et non gérés d'aujourd'hui (voir la figure 3).

Figure 3. Mobilité sécurisée Cisco AnyConnect™



Le client RPV Secure Sockets Layer (SSL) Cisco AnyConnect résout de nombreux problèmes de sécurité associés à l'octroi de la flexibilité nécessaire aux employés de Cisco pour utiliser des périphériques qui ne sont pas contrôlés ou gérés par le service informatique. Le service informatique de Cisco autorise uniquement les périphériques enregistrés à se connecter au réseau. Pour s'assurer qu'un périphérique qui tente de créer une session RPV SSL est enregistré, l'application Cisco AnyConnect compare le certificat du périphérique et son numéro de série. Le fait d'exiger l'enregistrement des périphériques associe le périphérique à une personne, ce qui permet de réaliser des enquêtes de sécurité et de vérifier les droits de l'utilisateur.

Le service informatique utilise les appareils de sécurité adaptatifs de la gamme Cisco ASA 5500 pour vérifier la conformité des périphériques par rapport aux normes de sécurité de l'entreprise. Par exemple, les utilisateurs Cisco ne peuvent pas établir une connexion RPV avant d'avoir configuré un mot de passe de verrouillage de l'écran. L'application Cisco AnyConnect permet d'éviter que les personnes qui ne font pas partie du personnel se connectent au réseau Cisco au moyen de périphériques perdus. Si un employé signale un périphérique égaré au service informatique de Cisco, celui-ci peut immédiatement mettre un terme aux sessions RPV et empêcher d'autres connexions RPV à partir de ce périphérique. Le service informatique de Cisco peut également supprimer facilement le compte des employés qui quittent la société.[4] La sécurité sur les périphériques mobiles iPhone, Nokia et Android est encore plus stricte, car leurs certificats sont distribués par une solution de gestion des périphériques mobiles. Cette solution permet une mise en œuvre plus précise des politiques de sécurité, de la gestion des stocks et du nettoyage à distance d'un périphérique en cas de perte ou de départ d'un employé.

Cisco effectue actuellement l'intégration du client Cisco AnyConnect avec la solution Cisco ScanSafe pour la sécurité Web en nuage et les dispositifs de sécurité Web (WSA) Cisco IronPort™ pour la sécurité Web dans les locaux. Ces solutions complémentaires protègent les utilisateurs des programmes Web malveillants, qu'ils soient connectés par le biais d'une connexion RPV SSL active ou non. La solution Cisco ScanSafe bloque les infections par des programmes malveillants, ce qui sécurise les périphériques (et le réseau de l'entreprise), même si les utilisateurs se connectent à des URL dangereuses lorsqu'ils ne sont pas sur le réseau ou connectés par le biais d'un RPV.

Risques potentiels pour tous les périphériques

Les organisations doivent savoir gérer les risques potentiels suivants pour tous les périphériques :

- Perte de contrôle sur les données d'entreprise stockées sur le périphérique, notamment les données règlementaires ou sur la clientèle.
- Perte de contrôle sur la posture du périphérique :
  - La baisse du contrôle sur l'ensemble de la sécurité du périphérique augmente potentiellement le risque d'exploitation et crée un vecteur d'attaque contre l'infrastructure et les services de Cisco.
  - Il est possible que les périphériques ne soient pas conformes aux modèles politiques et opérationnels, ce qui peut nuire aux relations commerciales ou enfreindre les exigences juridiques ou règlementaires.
- La perte de visibilité sur les périphériques connectés au réseau (c'est-à-dire sur l'endroit où ils se trouvent et l'entité qui les détient et les utilise) engendre des défis pour la sécurité, les licences, l'assurance juridique et législative et les audits.

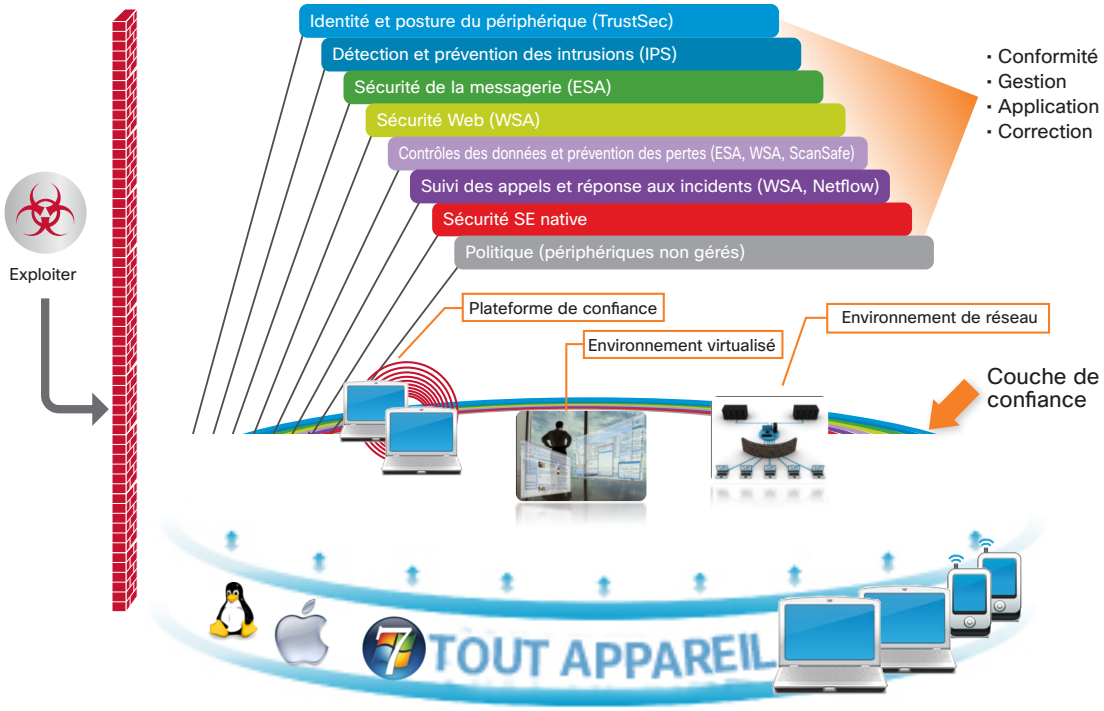
4. Consultez : www.cisco.com/web/about/ciscoitatwork/downloads/ciscoitatwork/pdf/Cisco_IT_Case_Study_AnyConnect_Deployment.pdf

Accès interne par le biais de la stratégie « Tout périphérique » de Cisco

Étape 1 : priorité au contrôle des programmes malveillants sur le réseau

Les périphériques appartenant à la société sont des outils importants pour le maintien de la sécurité et de l'intégrité des données d'entreprise. Cisco effectue un travail colossal pour la protection de nos environnements d'hébergement administrés en installant et en gérant différents niveaux de défense sur les ordinateurs déployés de l'entreprise (notamment un programme anti-pourriel, une protection anti-logiciel espion, un antivirus administré, un programme de prévention des intrusions sur l'hôte et une solution de gestion des correctifs). Toutefois, dans la mesure où Cisco abandonne progressivement les environnements d'hébergement administrés et les périphériques détenus par l'entreprise, ces contrôles doivent s'éloigner des terminaux et être intégrés dans le réseau administré. Cisco utilise actuellement des outils comme les dispositifs de sécurité Web (WSA) Cisco IronPort, la solution de sécurité de la messagerie (ESA) Cisco IronPort Cisco et les systèmes Cisco de prévention des intrusions (IPS), auxquels s'ajoutent notamment des systèmes de protection développés par des tiers pour NetFlow, une protection instantanée contre les programmes malveillants et des outils de gestion des événements utilisés pour protéger notre réseau (voir la figure 4).

Figure 4. Contrôles de la sécurité du réseau dans un environnement Cisco « Tout périphérique »



Un proxy de sécurité tel que le dispositif WSA Cisco IronPort situé à la périphérie d'Internet réduit de façon significative les menaces entrantes des réseaux filaires et sans fil. Tout en répondant aux exigences de sécurité de la stratégie « Tout périphérique » de Cisco, le déploiement du dispositif WSA Cisco IronPort protège également l'entreprise. Lors de son déploiement initial sur les passerelles Internet de Cisco dans l'est des États-Unis, le dispositif WSA a bloqué plus de 3 000 000 de transactions malveillantes[5] en 45 jours[6].

La solution ESA Cisco IronPort est une passerelle de messagerie dotée d'un système de pointe pour la prévention des menaces comme les pourriels, les virus, les programmes malveillants et les attaques ciblées. Elle comprend des contrôles à la sortie avec un système de prévention de la perte des données, une politique relative à l'utilisation acceptable et un cryptage des messages. L'intégration de la solution de sécurité de la messagerie au réseau ne se contente pas de protéger les périphériques. Elle améliore également la productivité. Par exemple, en un mois, la solution ESA Cisco IronPort a bloqué 280 millions[7] de courriels envoyés à des adresses Cisco.com (soit 88 pour cent des tentatives d'envois de messages).

5. Y compris des téléchargements, des logiciels de détournement de navigateur, des logiciels publicitaires non souhaités, des contrôles de botnet et des chevaux de Troie de type porte dérobée.
6. Du 14 avril au 31 mai 2011
7. Données du premier trimestre de l'exercice 2011

Cisco se base également sur les fonctionnalités de détection des systèmes de prévention des intrusions de Cisco pour contrôler les renseignements et diffuser des alertes sur nos réseaux. Le service informatique et le service de sécurité de Cisco peuvent rapidement exploiter les renseignements relatifs aux menaces, ce qui nous permet de les identifier et d'y répondre sans dépendre d'un terminal. Les systèmes de prévention des intrusions de Cisco sont disponibles sur les appareils dédiés ou sont intégrés au pare-feu, au commutateur et aux plates-formes de routage de Cisco et sont donc déployés dans chaque emplacement de Cisco dans le monde. Cette couverture permet à l'équipe Cisco chargée de traiter les incidents liés à la sécurité informatique (CSIRT) d'agir rapidement pour chaque incident survenu sur l'ensemble du réseau. Dans la mesure où le service informatique de Cisco passe d'un système de périphériques prêtés et administrés à des périphériques fournis par les utilisateurs, la capacité à inspecter attentivement la couche réseau devient essentielle. En raison de la diminution de la visibilité sur les périphériques, il convient d'investir dans des technologies qui permettent d'évaluer la situation de façon exhaustive et en temps réel pour détecter les menaces sur la couche réseau.

Étape 2 : renforcer le contrôle de l'accès des périphériques
Par le passé, l'équipe CSIRT de Cisco se basait en grande partie sur les systèmes informatiques (tels que le stock, la gestion des actifs et les systèmes de gestion des hôtes) pour associer les périphériques impliqués dans les incidents et leurs utilisateurs. Si un périphérique était impliqué dans un incident, l'équipe CSIRT de Cisco le recherchait dans les systèmes de gestion du matériel et des logiciels, l'associait à un utilisateur particulier et communiquait avec cet utilisateur pour résoudre le problème. Cette solution n'est pas applicable dans un monde « Tout périphérique ». L'équipe CSIRT de Cisco a largement remodelé les systèmes informatiques pour la stratégie « Tout périphérique » en associant par exemple les enregistrements DHCP (Dynamic Host Configuration Protocol) et les adresses MAC aux renseignements de connexion des applications, et non des périphériques, pour faciliter l'identification de l'utilisateur.

Dans un futur proche, l'architecture Cisco TrustSec® (qui fournit un contrôle de l'accès basé sur une politique, un réseau basé sur les identités et des services d'intégrité et de confidentialité des données) permettra de résoudre ce problème. Grâce au protocole 802.1x, les renseignements de connexion au réseau Cisco TrustSec identifient les utilisateurs et les associent à leurs périphériques. Elles permettent également à Cisco de fournir un accès différencié à un environnement de réseau dynamique et assurent la conformité d'un nombre croissant de consommateurs et de périphériques ayant accès au réseau. Par exemple, les technologies Cisco TrustSec peuvent tirer parti des normes de sécurité d'un périphérique de confiance. Lorsque des périphériques sont considérés comme « de confiance », ils bénéficient d'un accès total aux ressources de l'entreprise sur le réseau interne. En outre, la plate-forme de services d'identité (ISE) de Cisco (c'est-à-dire, la solution de contrôle de l'accès et de l'identité de Cisco) fournit une architecture de nouvelle génération pour la gestion de l'identité et des politiques.

Accès à la virtualisation des postes de travail à partir de n'importe quel périphérique

La mobilité et les nouveaux périphériques ont accéléré la stratégie « Tout périphérique » de Cisco et une troisième question s'est rapidement posée : comment intégrer les acquisitions et gérer les relations d'externalisation à l'étranger et hors des locaux?

Ces dernières années, Cisco a acquis de nombreuses entreprises dont l'intégration a été un défi pour le service informatique et les organisations de sécurité de Cisco. Chaque entreprise acquise avait ses propres périphériques et ses propres politiques et normes de sécurité, qui étaient souvent différents de ceux en vigueur chez Cisco. L'équipe chargée de la sécurité de l'information de Cisco devait s'assurer que les terminaux étaient conformes à la politique et aux normes de Cisco. Seules deux solutions étaient possibles et chacune d'entre elles entraînait différents défis. La première solution consistait à remplacer les périphériques de la société acquise par des périphériques fournis et pris en charge par le service informatique de Cisco, et à former les travailleurs à leur utilisation. Ce processus allait engendrer une transition coûteuse et longue qui affecterait la productivité pendant des semaines, voire des mois. La deuxième solution consistait à conserver les périphériques existants, au risque d'affecter la sécurité de l'ensemble de l'entreprise. Une autre solution devait être trouvée.

Les politiques de l'entreprise étaient également concernées par l'arrivée de l'externalisation. Il y a quinze ans, l'externalisation se limitait à quelques tâches simples. Aujourd'hui, elle est utilisée dans la plupart des secteurs de l'organisation et peut concerner de nombreux processus commerciaux. La main-d'œuvre actuelle de Cisco dépasse les 45 000 personnes, dont 17 000 effectuent leurs activités quotidiennes à partir de 350 sites tiers. Cisco a également des relations avec des sous-traitants dans plus de 200 entreprises différentes.

Aujourd'hui, la majorité de la main-d'œuvre sur site et à l'extérieur a reçu des périphériques pris en charge par le service informatique de Cisco et conformes à la politique de Cisco. Pour l'externalisation à l'étranger et en dehors des locaux, le service informatique de Cisco possède une infrastructure extranet qui prend en charge toutes les connexions réseau tierces. Le service informatique de Cisco gère 70 pour cent de l'ensemble des connexions extranet de bout en bout, notamment les périphériques, la connectivité WAN et le réseau distant pour les sites tiers. Toutefois, comme l'externalisation de Cisco a gagné en volume et en complexité, ce modèle ne répond plus aux attentes de l'entreprise en matière de coût total de possession et de temps nécessaire à l'acquisition des capacités.

La virtualisation des postes de travail, ainsi que les fonctionnalités de sécurité du réseau décrites précédemment dans le présent document permettront de relever ces défis tout en offrant des avantages importants (voir la barre latérale « Benefits and Challenges of Desktop Virtualization » [Avantages et défis de la virtualisation des postes de travail]). Cisco prévoit que la virtualisation des postes de travail permettra de réaliser des économies de plus de 20 pour cent et d'améliorer le temps nécessaire à l'acquisition des capacités de 40 à 60 pour cent pour les acquisitions et les sites d'externalisation à l'étranger et hors des locaux. Ce service centralisé, évolutif et indépendant de tout site permettra également d'améliorer la sécurité des données et la conformité des périphériques. Cisco a déjà commencé une activité pilote de virtualisation des postes de travail avec 2 000 utilisateurs aux États-Unis et d'autres sites du monde entier ont suivi dans le courant de l'année 2011.

Conclusions de Cisco

L'élaboration et la mise en œuvre de la stratégie « Tout périphérique » représentent un changement important pour n'importe quelle organisation. La présence d'une structure de gouvernance cohérente permet une transition plus en douceur et plus efficace. Le service informatique et les professionnels de la sécurité de Cisco ont tiré de nombreuses leçons de l'adoption de cette stratégie « Tout périphérique » par l'ensemble de l'entreprise :

- L'adoption de la stratégie « Tout périphérique » nécessite un effort pluridisciplinaire de la part des services en charge des postes de travail, de la sécurité, de l'infrastructure réseau et des communications.
- Les organisations doivent recruter un seul parrain-cadre qui sera responsable de l'organisation de l'équipe interfonctionnelle, de la formation des responsables et de la rédaction de rapports sur les résultats et les mesures.
- Ne sous-estimez pas les efforts nécessaires pour segmenter la population de vos utilisateurs et conduire une analyse des utilisateurs. Cette analyse doit déterminer quels utilisateurs ont accès à quels services et doit être la première action à effectuer lorsque vous lancez votre stratégie « Tout périphérique ».

Avantages et défis de la virtualisation des postes de travail

La virtualisation des postes de travail est un modèle informatique qui centralise les programmes, les applications, les services et les données. Bien que l'expérience des utilisateurs soit similaire à une expérience informatique 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 l'infrastructure de postes de travail virtuels ou VDI) présente de nombreux avantages potentiels :

- Expérience cohérente : les utilisateurs profitent de la même interface sur tous les périphériques de l'infrastructure VDI.
- Productivité accrue : les utilisateurs peuvent accéder aux données et aux applications à partir de n'importe quel périphérique de l'infrastructure VDI, où qu'ils se trouvent. Souvent, l'accès aux applications est accéléré, car l'environnement VDI se trouve dans un centre de données.
- Réduction des risques de programmes malveillants : le service informatique peut s'assurer que les applications sont à jour, que les correctifs sont plus rigoureux et que les utilisateurs installent les correctifs.
- Réduction du risque de perte de données et de propriété intellectuelle : les données sont centralisées, sauvegardées et disponibles, même si le périphérique tombe en panne ou est perdu ou volé.
- Accès plus rapide au marché : les utilisateurs importants (tels que les utilisateurs découlant d'une acquisition et les partenaires possédant leurs propres périphériques) peuvent être intégrés plus rapidement dans l'environnement de l'entreprise.
- Compatibilité des applications : la virtualisation des postes de travail peut servir de passerelle de compatibilité pour exécuter des applications d'entreprise dans un environnement de fonctionnement connu.
- Facilité de prise en charge : la mise en service d'un poste de travail virtuel est plus rapide que l'acquisition d'un nouvel ordinateur personnel. Par ailleurs, la virtualisation s'intègre bien dans un modèle de prise en charge informatique centralisé.

La virtualisation des postes de travail n'est cependant peut-être pas la solution pour toutes les applications ou toutes les communautés d'utilisateurs. Les problèmes suivants peuvent notamment se poser :

- Problème d'adaptation à certaines applications : actuellement, il existe des problèmes avec certaines applications à large bande, telles que la conception assistée par ordinateur, la vidéo et les communications unifiées.
- Problème d'adaptation à certains périphériques : l'expérience de l'utilisateur de la virtualisation des postes de travail ne s'adapte pas à certains périphériques, tels que les téléphones mobiles ou les tablettes avec un petit écran.
- Plates-formes limitées : la plupart des solutions de virtualisation des postes de travail se concentrent principalement sur les périphériques Windows.
- Environnements à forte latence : la VDI ne fonctionne pas correctement sur les environnements à forte latence.

Les organisations doivent effectuer des investissements suffisants pour respecter les règlementations applicables relatives à la sécurité, à l'intégrité, à la confidentialité et à l'audit des données. En 2010, Cisco à mis à jour son code d'éthique professionnelle pour inclure des recommandations sur l'utilisation des périphériques personnels. L'équipe chargée de la sécurité de l'information réécrit actuellement bon nombre de ses politiques de sécurité pour se concentrer davantage sur les données. Toutefois, dans certains cas, ces investissements peuvent aller à l'encontre de la vision « Tout périphérique ». Par exemple, Cisco emploie des médecins et des infirmières dans les locaux pour proposer des services de soins de santé aux employés. Les tablettes à écran tactile sont un outil précieux pour ces praticiens. Ils peuvent l'utiliser lors de la consultation des patients dans une structure de soins, en conjonction avec le système de conférence Cisco TelePresence® pour diagnostiquer et traiter des patients à distance. Toutefois, ces tablettes sont exposées à des données relevant de la loi américaine sur l'assurance maladie (HIPAA). Cisco n'autorise pas les travailleurs de la santé à utiliser leur tablette personnelle dans ce cadre et s'assure que les protocoles de gestion de la sécurité et des données sont respectés, avec des périphériques fournis par la société uniquement.

Premières étapes de votre propre stratégie « Tout périphérique »

Lorsque Cisco s'est lancé dans l'aventure « Tout périphérique », nous avons identifié 13 domaines professionnels majeurs qui sont affectés par ce nouveau paradigme. Le tableau 1 présente ces domaines prioritaires et fournit une liste de questions qui ont aidé Cisco (et qui pourront vous aider lorsque vous commencerez à appliquer votre stratégie) à reconnaître et à surmonter des problèmes potentiels et à déterminer comment aborder au mieux ces considérations au fil de votre travail. Étudiez ces questions et soyez honnêtes dans vos réponses lorsque vous élaborez votre stratégie.

Tableau 1. Questions à se poser pour l'application de la stratégie « Tout périphérique »

Domaine professionnel	Questions professionnelles à se poser
Planification de la continuité opérationnelle et reprise après sinistre	· La planification de la continuité opérationnelle doit-elle autoriser ou refuser l'accès des périphériques extérieurs à l'entreprise? · Doit-il exister une fonction de nettoyage à distance pour le périphérique accédant au réseau s'il est perdu ou volé?
Gestion de l'hôte (correction)	· Les périphériques extérieurs à l'entreprise peuvent-ils être ajoutés à des flux de gestion des hôtes d'entreprise existants?
Gestion de la configuration du client et validation de la sécurité du périphérique	· Comment la conformité du périphérique aux protocoles de sécurité sera-t-elle validée et tenue à jour?
Stratégie d'accès à distance	· Qui doit avoir accès à quels services et plates-formes sur quels périphériques? · Un collaborateur externe a-t-il le droit d'utiliser les mêmes périphériques, applications et données?
Licences logicielles	· La politique doit-elle être modifiée pour autoriser l'installation de logiciels de l'entreprise sur des périphériques n'appartenant pas à l'entreprise? · Les accords existants pour les logiciels s'appliquent-ils aux utilisateurs qui accèdent à la même application logicielle par le biais de plusieurs périphériques?
Exigences relatives au cryptage	· Les périphériques n'appartenant pas à l'entreprise doivent-ils respecter les exigences existantes relatives au cryptage des disques?
Authentification et autorisation	· Les périphériques n'appartenant pas à l'entreprise doivent-ils être ajoutés ou être autorisés à être ajoutés aux modèles Microsoft Active Directory existants?
Gestion du respect des règlementations	· Quelle sera la politique de l'organisation sur l'utilisation des périphériques n'appartenant pas à l'entreprise dans des scénarios de conformité élevée ou de risques élevés?
Gestion des incidents et enquêtes	· Comment les services de politique de sécurité et de confidentialité informatique de l'entreprise vont-ils gérer les incidents et les enquêtes avec les périphériques n'appartenant pas à l'entreprise?
Interopérabilité des applications	· Comment l'organisation va-t-elle gérer les tests d'interopérabilité des applications avec les périphériques n'appartenant pas à l'entreprise?
Gestion des actifs	· L'organisation doit-elle modifier la manière dont elle identifie les périphériques qu'elle possède pour identifier également ceux qu'elle ne possède pas?
Prise en charge	· Quelle sera la politique de l'organisation en matière de prise en charge des périphériques n'appartenant pas à l'entreprise?

À l'avenir

La stratégie « Tout périphérique » chez Cisco est un investissement continu et sur le long terme pour l'avenir. Au cours des prochaines années, Cisco poursuivra son plan de transfert des données et des applications importantes des périphériques vers le réseau ou le nuage, de renforcement de la sécurité du réseau et d'intégration des contrôles de l'identité et de la politique sur les périphériques lorsqu'ils interagissent avec le réseau. Les prochaines étapes de ce plan permettront de relever les défis du « Tout périphérique » dans les domaines d'activités suivants :

Interopérabilité des applications

Bien que 60 pour cent des périphériques qui se connectent actuellement au réseau Cisco soient des postes de travail Windows, ce pourcentage diminue en raison de la popularité croissante des autres périphériques. À l'avenir, Cisco aura moins de contrôle sur le type ou les versions des logiciels installés sur les périphériques, ce qui augmente le risque de problèmes d'interopérabilité entre les applications, les navigateurs, les versions et les environnements d'exécution. La prévalence des applications Web a simplifié le problème, mais ne l'a pas résolu. Si la diversité des postes de travail, des téléphones intelligents et des tablettes continue de croître, il en va de même pour le nombre d'environnements de navigation. Les dirigeants de Cisco ont encouragé une initiative « navigateur standard » pour les applications Web internes, basée sur les normes World Wide Web Consortium (W3C). Les normes de développement Web du secteur facilitent l'interopérabilité des applications dans un écosystème qui inclut différents navigateurs, systèmes d'exploitation et terminaux.

Cisco se base également sur la virtualisation des postes de travail pour présenter un système opérationnel compatible sur n'importe quel système d'exploitation. Une virtualisation pilote des postes de travail, qui couvre actuellement des milliers d'utilisateurs, devrait être mise à la disposition de 18 000 travailleurs avant juillet 2012.

Licences logicielles

Comme la plupart des entreprises, Cisco utilise des systèmes de gestion des actifs pour assurer le suivi des licences logicielles. Cisco doit répondre à des questions politiques concernant certains scénarios de licences logicielles dans le cadre du « Tout périphérique », telles que :

- Les utilisateurs seront-ils autorisés à installer des logiciels de l'entreprise sur leur propre périphérique?
- Les contrats existants avec des fournisseurs de logiciels autorisent-ils l'installation des logiciels de l'entreprise sur les périphériques n'appartenant pas à l'entreprise?
- Cisco doit-il suivre les périphériques n'appartenant pas à l'entreprise et, si oui, comment?

Cisco étudie l'utilisation des renseignements collectés par la technologie Cisco TrustSec (telles que l'identité et l'adresse MAC de l'utilisateur) afin de mettre en œuvre un système de gestion des actifs qui suit tous les périphériques, et des mécanismes de rapport détaillés qui tiennent compte des actifs matériels et logiciels n'appartenant pas à l'entreprise.

Planification de la continuité des activités et reprise après sinistre

Cisco emploie des travailleurs disposant d'actifs de l'entreprise et travaillant sur les sites d'autres sociétés, ainsi que des collaborateurs qui travaillent dans des bureaux de Cisco dans le monde entier. Qui doit s'assurer de la sécurité et de l'intégrité des données? Cisco sauvegarde ses ordinateurs personnels Windows de façon centralisée, mais de nombreux autres partenaires ne souhaitent pas que leur propriété intellectuelle soit sauvegardée sur un système tiers. Si des utilisateurs ne sont pas intégrés aux services de continuité des activités de l'entreprise, quelles autres dispositions sont prévues pour que ces utilisateurs reprennent le travail rapidement après une interruption de service? Une des solutions possibles est la virtualisation des postes de travail, qui peut dissocier les données sensibles des périphériques.

Cisco a commencé à gérer les interactions de nos utilisateurs par le biais du réseau. La société évolue résolument vers un avenir où de moins en moins d'applications et de données seront conservées sur les postes de travail en utilisant une combinaison de solutions de virtualisation des postes de travail et de logiciels-services ou d'informatique en nuage. Certaines applications ou sites de l'entreprise passeront à une approche davantage basée sur les transactions, par laquelle les utilisateurs, les actions et les données pourront être gérés, suivis et sauvegardés de façon cohérente. Cette évolution mènera le service informatique de Cisco vers un avenir « N'importe quel service, n'importe quel périphérique, depuis n'importe où » efficace et sécurisé, et finalement, vers la création de l'entreprise virtuelle.

Renseignements complémentaires

Cisco s'efforce de mettre en œuvre un environnement « N'importe quel service, n'importe quel périphérique, depuis n'importe où » pour notre organisation et nous allons continuer à partager nos expériences et ce que nous avons appris pour vous aider à résoudre les problèmes qui peuvent apparaître au cours du processus. Les connaissances et la méthodologie utilisées par Cisco pour faire évoluer notre entreprise et notre environnement informatique vers le « Tout périphérique » et au-delà peuvent être appliquées à d'autres organisations, grandes et petites.

Discutez avec votre représentant Cisco pour déterminer comment positionner votre infrastructure opérationnelle, informatique et de sécurité de façon stratégique pour préparer une évolution vers des architectures « Tout périphérique ».

Pour plus de renseignements sur les solutions de Cisco qui permettent le « Tout périphérique », consultez :

- Client de mobilité sécurisée Cisco AnyConnect
- Stratégies de virtualisation
- Technologie Cisco TrustSec
- Dispositifs de sécurité de messagerie IronPort de Cisco
- Appareils Cisco IronPort Web Security

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

Siège social – Asie
Cisco Systems (USA) Pte. Ltd.
Singapour

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

Cisco a plus de 200 bureaux dans le monde. Vous trouverez les adresses, ainsi que les numéros de téléphone et de télécopieur sur le site Web de Cisco, à l'adresse **www.cisco.com/go/offices**.

C11-681837-00 08/11

