Livre blanc

Mobilité d'entreprise : assurer un avenir productif et compétitif

Présentation

Alors que de plus en plus d'organisations adoptent de nouveaux modèles commerciaux liés à la mobilité, au cloud, à l'Internet des objets (IoT) et à l'Internet of Everything (IoE), l'entreprise devient un environnement amorphe. Les smartphones, tablettes et autres terminaux et applications web sont en train de modifier de façon irréversible le travail et le jeu en ligne. Cisco a adopté la vision « Tout type de périphérique ». Dans le cadre de cette vision, les entreprises :

- Offrent à leurs employés un plus grand choix dans les appareils utilisés.
- Assurent une expérience utilisateur cohérente et prévisible
- Augmentent la productivité, la sécurité et la compétitivité en général

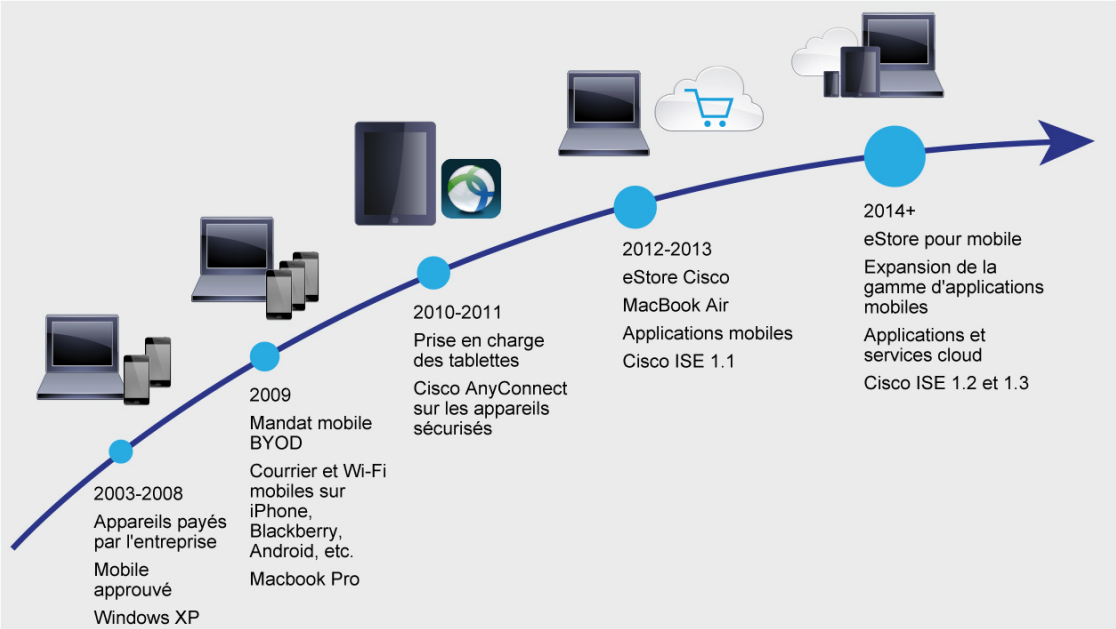
Les entreprises et autres grandes organisations doivent décider si elles permettent à certains utilisateurs, certains appareils et certains emplacements d'accéder aux réseaux, aux données et aux services de l'entreprise. Elles doivent décider également dans quelle mesure cet accès doit être répartir sur plusieurs niveaux, en fonction des besoins de l'entreprise et de ceux des utilisateurs. S'appuyant sur l'expérience de Cisco, ce livre blanc aborde les étapes et les décisions commerciales que les responsables de la sécurité des informations, les responsables IT et les architectes de sécurité des informations doivent considérer lorsqu'ils se lancent dans l'aventure « Tout type de périphérique ».

Introduction

Chaque jour le personnel Cisco utilise plus de 82 000 ordinateurs portables Windows, 32 000 ordinateurs Macintosh, 10 000 machines Linux et 72 000 iPhones, iPads et appareils Windows et Android. Nos plus de 70 000 employés et 30 000 consultants, conseillers et partenaires commerciaux veulent avoir le choix de l'appareil qu'ils utilisent dans le cadre de leur travail. Et ils veulent être libres d'utiliser ces appareils là où ils le souhaitent pour accéder au réseau, aux systèmes, aux applications, aux données et aux services en ligne de l'entreprise. Tandis que tous les ordinateurs portables sont fournis par Cisco, la grande majorité des smartphones et tablettes sont la propriété de leur utilisateur. La plupart des employés Cisco utilisent un ordinateur et un smartphone pour accéder aux services informatiques de la société et plus de 20 % d'entre eux utilisent plus de deux appareils. La diversité de ces appareils augmente de manière exponentielle.

Voici plus de 10 ans que Cisco s'est engagé dans une vision à long terme appelée « Tout type de périphérique » (Figure 1). Elle vise à proposer un choix d'appareils plus vaste tout en assurant une expérience utilisateur commune qui améliore la compétitivité et la sécurité de l'entreprise au niveau international, dans un espace de travail de plus en plus mobile.

Figure 1. Feuille de route « Tout type de périphérique » de Cisco



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

- **La productivité :** les employés Cisco férus de technologie peuvent utiliser leur smartphone, tablette ou ordinateur portable pour travailler, à tout moment et partout, ce qui améliore leur satisfaction et leur productivité.
- **Une main-d'œuvre en pleine évolution :** la génération actuelle de férus de technologie qui intègre la main-d'œuvre 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.
- **L'innovation :** autoriser les travailleurs à utiliser des appareils de nouvelle génération dès leur sortie sur le marché peut générer des gains de productivité supplémentaires. Les utilisateurs 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 département IT de Cisco et la stratégie-produits de Cisco.
- **L'intégration des acquisitions :** les nombreuses entreprises achetées par Cisco rejoignent le groupe avec leurs propres pools d'appareils non standard. La stratégie « Tout type de périphérique » permet d'intégrer rapidement de nouveaux départements et de réduire les risques de sécurité associés.
- **Les coûts d'investissement :** la société Cisco emploie des dizaines de milliers de consultants et de conseillers dans le monde entier, elle doit donc optimiser et réduire les coûts liés à ces prestataires. En appliquant le programme « Tout type de périphérique » à ces consultants et conseillers, Cisco réalise des économies importantes par utilisateur.

Pour soutenir cette initiative de la direction, la stratégie IT de Cisco prend en compte les considérations suivantes :

- Une architecture évolutive pour accueillir tous les appareils approuvés par les plates-formes conformes aux normes du secteur, une connectivité transparente, la couche de sécurité intégrée et la simplicité de gestion.
- La possibilité de répartir de façon flexible le coût de la voix et du matériel en fonction de politiques bien définies et de règles d'utilisation sur les smartphones et les tablettes, les ordinateurs portables de l'entreprise et les services mobiles facultatifs de l'entreprise.

- La gestion des dépenses, pour optimiser de façon proactive les stratégies de dépenses grâce à des relations fortes avec les prestataires de services et des modèles de prix innovants.
- Des cycles de vie d'application robustes, basés sur l'évolution des besoins des utilisateurs et des besoins métier de l'entreprise, avec des applications facilement accessibles dans l'eStore Cisco, un magasin d'applications mobile unique comptant déjà plus de 60 applications.
- Un ancrage social, avec le contenu en libre-service, la communication proactive et l'assistance interactive par les utilisateurs eux-mêmes, mais toujours avec une assistance individuelle si nécessaire.

D'autres organisations peuvent avoir leurs propres raisons d'adopter une stratégie « Tout type de périphérique ». Elles peuvent vouloir renforcer la protection des données, augmenter la mobilité ou créer des environnements de travail collaboratif pour partager l'accès aux données en temps réel. Les programmes « Tout type de périphérique » varient également en fonction du secteur et de la réglementation. À mesure que le choix et le nombre des appareils augmentent et que de nouveaux modèles commerciaux redéfinissent la connectivité, les entreprises doivent réfléchir à qui peut accéder aux applications et aux données, aussi bien dans les limites de leur réseau qu'à l'extérieur. Ensuite, elles doivent définir comment planifier, suivre, appliquer et assumer ces politiques.

Ce document aborde les aspects suivants de la vision « Tout type de périphérique » :

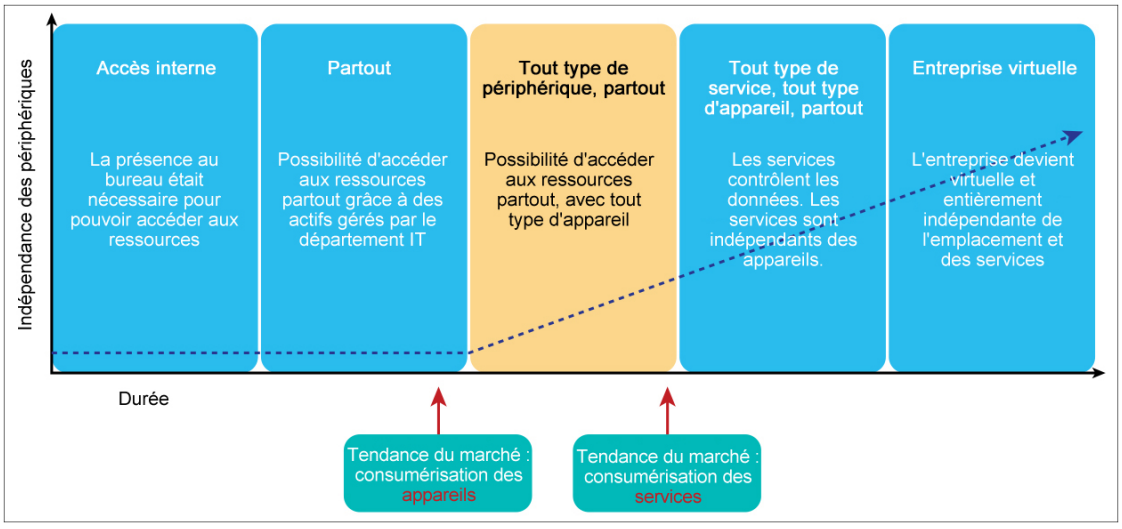
- Risques, avantages et changements dans l'entreprise, le service IT et les politiques de sécurité
- Solutions que Cisco met actuellement en application
- Autres questions auxquelles Cisco a fait face dans le cadre du programme « Tout type de périphérique »

Avec une approche flexible et proactive, les organisations peuvent mettre en place le modèle qui répond le mieux à leurs besoins et évoluer vers un environnement connecté en perpétuelle expansion.

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

Les 15 dernières années ont été marquées par un changement significatif dans la manière dont les utilisateurs accèdent au réseau Cisco (voir Figure 2).

Figure 2. Étapes relatives à l'accès des collaborateurs aux ressources de l'entreprise au cours de l'adoption de la stratégie « Tout type de périphérique »



Étape 1 : accès interne

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 Figure 2.

Politique Cisco sur les appareils 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 appareils sécurisés doivent respecter les exigences suivantes relatives à l'application de la politique et à la gestion des ressources.

Application des politiques

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

- Contrôles d'accès locaux qui imposent des mots de passe forts (complexité)
- Délai d'inactivité de 10 minutes et blocage complet après 10 tentatives infructueuses de connexion
- Chiffrement de tous les appareils et de toutes les données sensibles de Cisco
- Fonctionnalité d'effacement et de verrouillage à distance en cas de désactivation d'un compte employé ou de la perte ou du vol d'un appareil
- Fonctionnalité de gestion de stock pour vérifier la présence des logiciels de sécurité spécifiques, l'application des mises à jour et l'utilisation des applications de l'entreprise et de la version des applications utilisées

Gestion des ressources

Les appareils qui accèdent aux services de l'entreprise doivent subir un certain nombre de contrôles. Les appareils doivent être :

- 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 pour les journaux d'analyse (par exemple, journaux de logiciels de sécurité, authentification et autorisation des utilisateurs et modifications de la configuration)

Étape 2 : Partout

Au fil du temps, les ordinateurs portables et les VPN ont permis aux employés d'être plus mobiles. En outre, les collaborateurs, d'un niveau de plus en plus mondial, ont rendu nécessaire l'adoption de modèles de travail plus flexibles. L'étape 2 illustre comment les environnements de travail et les heures de travail régulières n'entravent plus la productivité, car les collaborateurs plus mobiles accèdent aux ressources IT de l'entreprise depuis divers lieux, par exemple depuis le site d'un client, son domicile, un café ou un hôtel. Avec cette disparition des frontières, les utilisateurs peuvent accéder aux ressources peu importe où ils se trouvent grâce aux services gérés par le service IT.

Étape 3 : Tout type de périphérique, de partout

Ces dernières années, la popularisation des smartphones, des tablettes et des ordinateurs portables a provoqué l'apparition de nouvelles fonctionnalités incroyables, l'amélioration de fonctionnalités existantes, la création de formats plus efficaces et la réduction du cycle de vie des appareils. En conséquence, les employés souhaitent utiliser leur propre appareil pour tout : accéder à leurs e-mails, consulter l'intranet de l'entreprise et utiliser les applications professionnelles de l'entreprise. Ces facteurs sont entrés en jeu assez rapidement, ce qui a exercé une pression sur le département IT de l'entreprise et sur les équipes chargées de la sécurité. En outre, les employés qui ont rejoint Cisco suite à une acquisition ont souhaité continuer à utiliser leur appareil favori dans leur travail, même si le profil de ces appareils ne correspond pas aux critères définis par Cisco.

L'adoption rapide de nouvelles technologies clientes a mené à la mise en œuvre d'approches, d'outils et de technologies venus d'autres entreprises. Cela a créé des communautés d'utilisateurs et a généré une transformation de la façon dont le personnel IT de Cisco assure l'assistance, et de la façon dont les utilisateurs peuvent s'appuyer sur les connaissances de leurs collègues pour résoudre des problèmes courants. Le rôle du service IT de Cisco au sein de ces communautés n'est pas d'agir en tant que propriétaire d'un processus, mais de contribuer en tant qu'entité.

Par exemple, l'adoption de produits Apple chez Cisco est née de l'introduction de ces appareils par les utilisateurs dans l'environnement Cisco. Ils constituaient leur premier choix en termes d'outil et de plate-forme 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 grâce à des alias e-mail, des wikis, à l'intranet et à du contenu vidéo. Lorsque le département IT a commencé à proposer les périphériques Mac dans le cadre de sa procédure d'actualisation des PC, il a adopté le modèle d'assistance autonome mis en place par les utilisateurs Mac, sans perturber ni changer leur communauté. Le département IT a adopté ce modèle, puis l'a utilisé pour mettre au point d'autres services d'assistance autonome.

Ensemble, ces développements sont le signal du besoin d'une nouvelle stratégie d'entreprise en ce qui concerne les terminaux, qui doit répondre à une question fondamentale, mais néanmoins impérative : alors que de nouveaux modèles commerciaux liés à la mobilité, au cloud, à l'IoT et à l'IoE se développent, comment pouvons-nous offrir un accès sûr aux ressources de l'entreprise depuis tout type d'appareil, et de partout ?

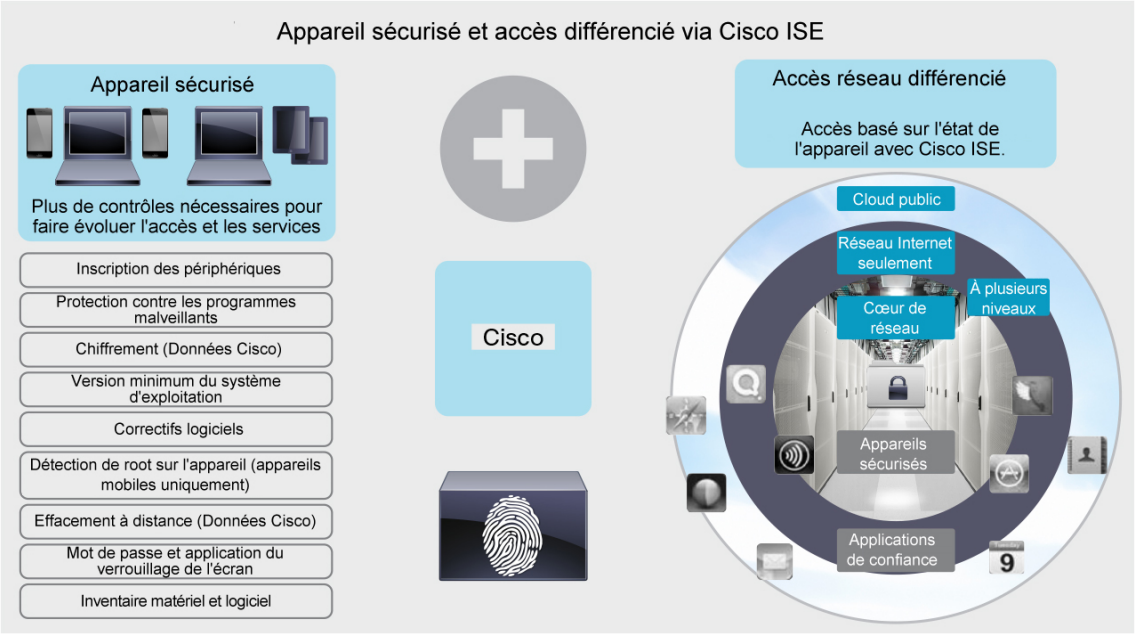
Risques potentiels de la stratégie « Tout périphérique »

Les entreprises doivent envisager de se protéger contre les risques liés à la stratégie « Tout type de périphérique », notamment :

- Perte du contrôle des données d'entreprise stockées sur le périphérique, y compris les données réglementaires ou de clients
- Perte de contrôle sur l'état des appareils :
  - Un niveau inférieur de contrôle sur la sécurité globale des appareils peut augmenter les risques d'intrusion et créer un vecteur d'attaque ciblant l'infrastructure et les services
  - Les appareils ne sont pas toujours conformes aux règles de sécurité et aux modèles opérationnels. Cela peut détériorer les relations professionnelles, se répercuter sur les exigences légales ou réglementaires et augmenter le coût de l'assistance technique
- Une visibilité réduite sur les appareils connectés au réseau (géolocalisation, propriétaire et utilisateur) entraîne des problèmes sur les plans de la sécurité, des licences, de la conformité réglementaire et juridique et des audits.

Tous les travailleurs 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 smartphone, tandis que d'autres requièrent des niveaux d'accès supérieurs. Par exemple, les commerciaux de Cisco peuvent accéder à des outils de commande depuis leur smartphone, ce qui augmente leur capacité à clôturer une vente. Cette situation a engendré plusieurs niveaux d'accès réseau en fonction de la confidentialité et de l'emplacement des données consultées, comme illustré dans la Figure 3. Le point de départ est que les employés ont besoin d'utiliser des « des applications de confiance » dans le cadre de leurs activités professionnelles. Dès lors que les employés ont besoin d'un accès au cœur de réseau, ils doivent utiliser des « appareils sécurisés ». Les mesures de protection sur l'appareil doivent être optimisées au-delà du simple enregistrement de l'appareil, de l'utilisation de mot de passe, du verrouillage de l'écran et de l'effacement du contenu à distance. Elles doivent prévoir le respect des règles de sécurité imposées par le moteur Cisco® ISE.

Figure 3. Accès réseau différencié



Étape 4 : Tout service, tout périphérique, partout

Cisco permet actuellement aux utilisateurs d'accéder aux ressources de l'entreprise hébergées en local ou dans le cloud. Pour adopter une approche « Tout type de périphérique », l'entreprise doit se doter de certains éléments basiques que sont une connectivité transparente, des normes pour les appareils sécurisés, une seule boutique d'applications mobiles, un modèle de sécurité axé sur les menaces et un modèle d'assistance en libre-service dynamique. La productivité de l'entreprise sous-tend la vision « Tout type de périphérique ». Elle augmente proportionnellement à la satisfaction des employés.

Étape 5 : Entreprise virtuelle

L'entreprise virtuelle, évolution logique de l'étape 4, dépend de moins en moins de la localisation et des services. À ce stade, le modèle d'identité de l'entreprise a atteint une certaine maturité qui permet un contrôle précis des accès et offre un certain niveau de collaboration externe. Les contrôles et fonctions de sécurité sont entièrement appliqués aux données de l'entreprise. Nous aborderons la notion d'entreprise virtuelle lorsque nous serons plus engagés dans cette voie.

Concrétiser l'approche « Tout type de périphérique » : un examen détaillé de la stratégie de Cisco

Il fut un moment où les employés Cisco accédaient par leurs propres moyens à leur messagerie électronique et à leurs fichiers de travail via leur smartphone ou leur tablette. Réalisant qu'une simple politique BYOD était insuffisante, Cisco a élaboré une stratégie plus globale « Tout type de périphérique ». Elle prenait en considération les terminaux mobiles fournis par Cisco et ceux achetés par les employés. Elle soulevait également les questions d'accès aux applications, d'exigences de sécurité et d'expérience utilisateur.

Valeur commerciale de l'application Cisco SalesMobile

Durant le premier mois du lancement de l'application SalesMobile, les résultats ont été les suivants :

- 561 671 325 $ de chiffre d'affaires traité
- Approbation des transactions 40 % plus rapide
- Adoption virale via l'eStore Cisco

« Je dois avouer que j'ai un faible pour cette application. Le fait de pouvoir approuver les transactions en déplacement facilite le processus de vente ! » - Directeur commercial régional Cisco

« Cette application est fort sympathique et très facile à utiliser. Il était temps ! » - Directeur pays Cisco

Axée sur la mobilité business-to-employee (B2E), l'infrastructure et les technologies Cisco sont intégrées à des solutions de partenaires solides, dans le cadre d'une stratégie capable d'évoluer selon les besoins de l'entreprise et des utilisateurs. Ce programme Cisco a permis de réduire les coûts, d'améliorer la productivité des utilisateurs et leur niveau de satisfaction, et d'atténuer les risques pour la sécurité. Cette section étude la démarche suivie par Cisco pour concrétiser sa vision d'une architecture « Tout type de périphérique » aboutie. Elle explique notamment en quoi cette approche a remis en question les normes de sécurité traditionnelles et décrit les solutions que Cisco a déployées.

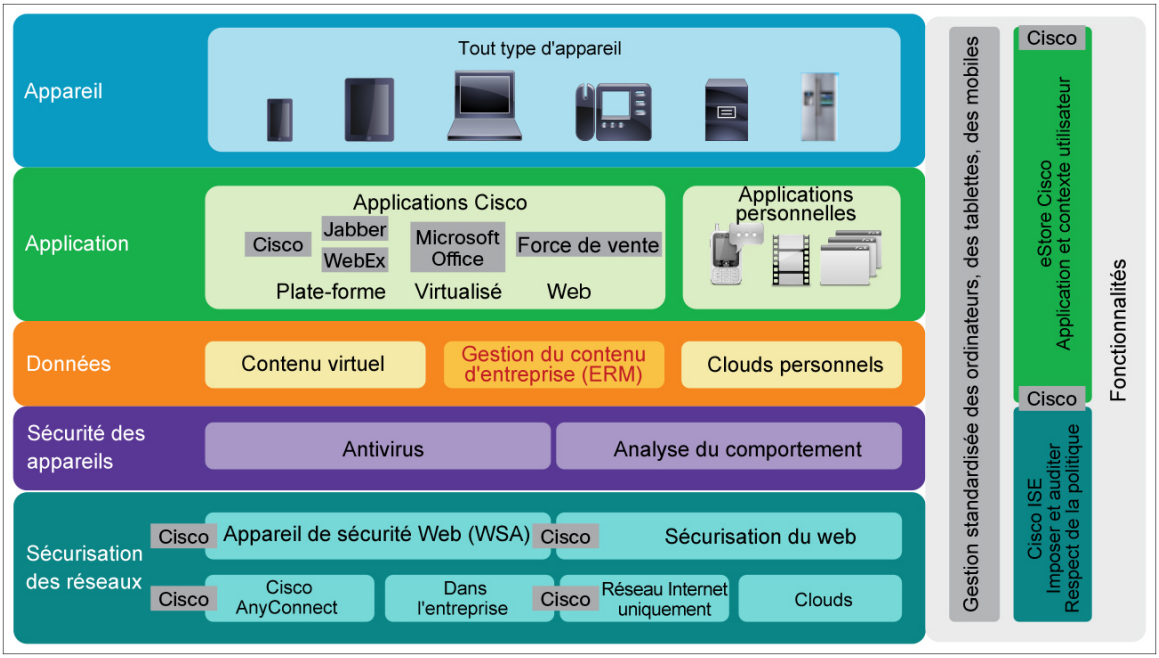
Présentation de l'architecture

Actuellement, tous les employés Cisco peuvent se connecter au réseau avec n'importe quel appareil, à condition qu'il réponde aux normes de sécurité définies par Cisco. Ces appareils peuvent être fournis par Cisco, s'il s'agit d'ordinateurs portables, ou être achetés par les employés. Cela concerne les iPhones, les iPads, les appareils Android ou les appareils Windows. La plupart des employés s'achètent leur propre smartphone ou tablette qu'ils choisissent eux-mêmes. L'employé ou Cisco prend en charge l'abonnement aux services, selon la fonction occupée par l'employé. Les employés utilisent ces appareils tout au long de leur journée de travail. Ils peuvent recevoir des appels sur leur numéro professionnel attribué à leur téléphone et ils peuvent synchroniser le calendrier, les e-mails et les contacts de leur appareil avec l'environnement Microsoft Exchange de l'entreprise. Ils peuvent utiliser des applications de collaboration, comme Cisco WebEx® et Cisco Jabber®. Ils peuvent également établir une connexion VPN hautement sécurisée à l'intranet pour consulter des pages Web internes, approuver des ventes, entrer des notes de frais, trouver la salle de réunion disponible la plus proche, etc.

La solution « Tout type de périphérique » s'appuie sur des technologies Cisco déjà déployées :

- les réseaux d'accès filaire, sans-fil et VPN
- le moteur Cisco ISE qui impose des règles de sécurité en fonction de l'utilisateur demandeur, du type d'appareil, de la méthode et du moment auquel l'accès est demandé
- les communications unifiées et les applications de collaboration, notamment Cisco Unified Communications Manager, Cisco WebEx et Cisco Jabber. Ces applications sont hébergées sur les plates-formes Cisco Unified Computing System™ (Cisco UCS®).

Figure 4. Architecture High-Level



Conception

Cisco a conçu la solution pour fournir un accès hautement sécurisé aux outils de collaboration et à l'intranet avec un minimum de développement et de test côté IT afin d'économiser les ressources IT internes et d'accélérer le déploiement. Grâce aux fonctions natives de chiffrement, d'e-mail, de calendrier et de gestion des contacts de chaque appareil, Cisco élimine le besoin de développement et de test en interne de solutions de tiers, habituellement nécessaires lorsque les fabricants mettent à jour leur système d'exploitation.

Microsoft ActiveSync synchronise les applications natives d'e-mail, de calendrier et de contacts des appareils avec Microsoft Exchange. ActiveSync offre également des fonctions de sécurité de base, comme l'utilisation d'un code PIN pour déverrouiller l'appareil et permettre l'effacement de contenu à distance.

Conception des applications

Le cycle de vie du projet comporte la planification, le déploiement, la mise en œuvre et l'utilisation. Tout au long de ce cycle de vie, l'équipe IT Cisco en charge de la mobilité a travaillé avec les équipes IT Cisco responsables des applications de messagerie Windows, Windows Exchange, Cisco WebEx, Cisco Jabber et le client Cisco AnyConnect® Secure Mobility.

Le principe directeur de la conception d'applications est d'offrir une expérience utilisateur qui soit au minimum aussi simple sur un smartphone ou une tablette que sur un ordinateur portable. Pour parvenir à ce résultat, l'équipe exploite les fonctions natives du système d'exploitation de l'appareil (e-mail, calendrier, chiffrement, etc.) dans toute la mesure du possible. Lorsqu'une autre étape est nécessaire, par exemple pour établir une connexion VPN, Cisco cherche à réduire le nombre d'actions demandées à l'employé. Par exemple, Cisco AnyConnect installe automatiquement une connexion VPN hautement sécurisée dès qu'un employé ouvre une autre application, par exemple le navigateur web, une application personnalisée ou Cisco Jabber. AnyConnect se lance en une à deux secondes et reste connecté jusqu'à l'arrêt du smartphone ou de la tablette.

L'équipe utilise des API pour automatiser les tâches de gestion, par exemple pour veiller à ce que les nouveaux utilisateurs rejoignent le bon groupe Active Directory. Les API intègrent également la plate-forme EMAN de gestion d'entreprise développée en interne à Active Directory, la solution de gestion des appareils mobiles MDM et au client Cisco AnyConnect Secure Mobility.

L'équipe utilise également des API de l'eStore Cisco pour automatiser le provisionnement des services. L'eStore est basé sur le catalogue de services Cisco Prime™ et Cisco Process Orchestrator. Il est intégré à MDM, à Active Directory et à Cisco ISE. Cette intégration permet à Cisco d'automatiser certains processus comme l'identification de l'employé pour déterminer s'il peut accéder au service, l'envoi d'une notification par e-mail au sujet du service au responsable de l'employé, le provisionnement du service et la gestion du cycle de vie du service.

Récupération après sinistre

Cisco emploie la même architecture de récupération après sinistre pour l'e-mail et l'accès VPN que celle utilisée pour tous les autres services aux employés. Les serveurs de messagerie électronique et les têtes de réseau VPN Cisco AnyConnect sont déployés dans le data center virtuel Metro (MVDC), selon une configuration actif-actif avec équilibrage de charge. Si la connexion à un site est interrompue, sa charge de travail bascule sur le serveur d'un autre site. Les modifications apportées à l'architecture de la solution sont appliquées simultanément à tous les data centers et minutieusement testés.

Déploiement

La mise en œuvre du programme Cisco « Tout type de périphérique » s'est déroulée sur différentes phases :

1. Automatisation du provisionnement des services de messagerie électronique et de téléphonie portable (2008)
2. Déploiement de Microsoft ActiveSync pour que les employés puissent synchroniser les contacts et l'e-mail avec les iPhones et les appareils Android (2009).
3. Début de l'utilisation du client Cisco AnyConnect Secure Mobility pour la connexion au VPN à partir de certains appareils personnels (2011)
4. Développement de l'eStore, un guichet unique pour le provisionnement des services BYOD (2012)
5. Mise en service de l'eStore (2013)

Cisco a mené un projet pilote dans un bâtiment de San José. L'équipe a utilisé l'infrastructure sans fil existante du bâtiment, deux serveurs d'infrastructure de clé publique (PKI) existants dans un data center Cisco et un cluster Cisco ISE existant dans un autre data center Cisco.

Après ce projet pilote, Cisco a mis en place ce programme pays par pays. Dans chaque pays, Cisco a ajouté de nouvelles fonctions, une par une. Les dirigeants ont été invités à informer les employés du programme.

Sécurité

Dans la mesure où un nombre grandissant d'appareils de plus en plus divers se connectent, la problématique de la sécurité s'intensifie. Les pirates informatiques profitent des plus petites failles de sécurité de l'environnement pour l'attaquer. Afin de contrer ces efforts, Cisco a adopté une approche de sécurité axée sur les menaces. Nos solutions s'intègrent les unes aux autres pour faire face aux différents vecteurs d'attaque et offrir une protection en tout moment et en tout lieu, dès lors qu'une menace existe.

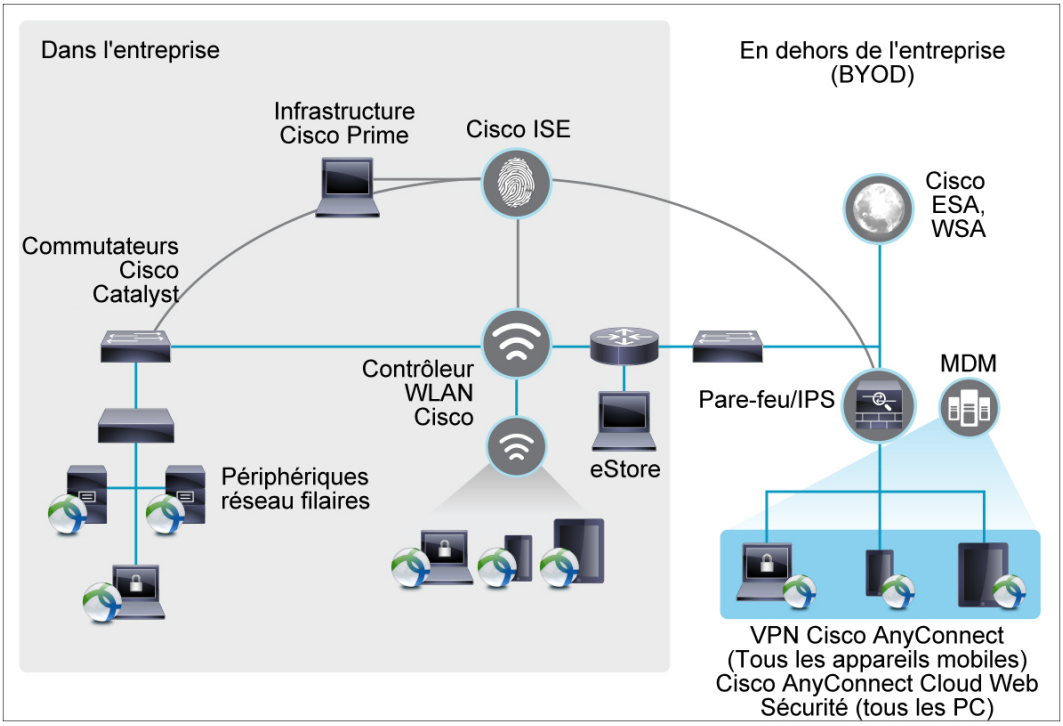
Cisco utilise les capacités natives de chiffrement du système d'exploitation de chaque appareil pour protéger les données, comme les contacts et les e-mails.

L'architecture de l'accès utilisateur comprend les éléments suivants, représentés dans la Figure 5 :

- Pare-feu Cisco ASA : Cisco protège ses data centers avec le pare-feu de nouvelle génération Cisco ASA. Il est doté d'un système d'inspection dynamique d'entreprise, de fonctions de visibilité et de contrôle des applications et d'un VPN d'accès à distance, ainsi que du clustering avancé garantissant un accès hautement sécurisé et performant et un excellent niveau de disponibilité.
- Cisco IPS : Cisco utilise Cisco IPS pour identifier, classer et bloquer le trafic malveillant issus de nombreux vecteurs de menace, dont les réseaux, les serveurs et les terminaux de bureau. Le pare-feu Cisco ASA et Cisco IPS sont progressivement remplacés par le pare-feu Cisco ASA avec fonctionnalités FirePOWER™. Cette solution regroupe le pare-feu de la gamme Cisco ASA 5500 (avec visibilité et contrôle des applications), le système de prévention des intrusions (NGIPS) de nouvelle génération Sourcefire® et AMP pour garantir une défense intégrée contre les menaces.
- Solution MDM : Cisco utilise une application MDM tierce pour vérifier l'état des appareils et distribuer ses applications. L'outil MDM s'assure que l'appareil est enregistré et conforme aux règles de sécurité. Pour être conforme, l'appareil doit utiliser une version approuvée du système d'exploitation, un code PIN avec une longueur minimale, un délai d'expiration de 10 minutes, une fonction d'effacement du contenu à distance, le chiffrement, un programme anti-logiciels malveillants et une fonction d'inventaire du contenu.
- Cisco ISE : une fois que l'outil MDM a vérifié si l'appareil mobile est conforme à la politique de sécurité, Cisco ISE applique la politique en refusant l'accès aux appareils non conformes. Si un employé essaye d'accéder aux ressources internes à partir d'un appareil personnel, Cisco ISE contrôle cet accès.
- Client Cisco AnyConnect Secure Mobility : les employés qui souhaitent accéder à l'intranet depuis un appareil mobile doivent télécharger le client Cisco AnyConnect Secure Mobility. AnyConnect® offre une connexion sécurisée vers l'intranet avec IPSec IKEv2 (Internet Key Exchange) et SSL. Les clients se connectent via les dispositifs de sécurité adaptatifs Cisco ASA qui authentifient l'utilisateur et chiffrent le flux de données mobile de sorte qu'il ne puisse pas être lu s'il est intercepté.
- Dispositif de sécurité Internet Cisco (WSA) : examine toutes les demandes d'accès aux sites Web externes à partir des appareils sur lesquels est installé le client Cisco AnyConnect Secure Mobility. WSA évalue les sites Web sur la base de leur réputation et de leur contenu. En fonction de la politique de sécurité interne de Cisco, il peut bloquer ou surveiller l'accès à certains sites Web ou certaines fonctions, comme la conversation en ligne, la messagerie, la vidéo et l'audio. Le service IT de Cisco bloque seulement environ 2 % des demandes de site Web, ce qui représente tout de même 6 à 7 millions de demandes par jour. La plupart des sites sont bloqués en raison d'informations concernant leur réputation. 2 % (soit 500 000 par jour) sont bloqués car ils présentent des risques de logiciels malveillants, comme des chevaux de Troie ou des programmes de téléchargement de chevaux de Troie. Pour une protection complète contre les logiciels malveillants, la solution Cisco Advanced Malware Protection (AMP) fait maintenant partie des appareils WSA et sera intégrée à l'architecture Cisco. Cisco AMP assure la détection et le blocage des logiciels malveillants, l'analyse permanente et l'envoi d'alertes rétrospectives. Cisco prévoit d'utiliser Cisco Cloud Web Security pour les utilisateurs hors site.

- Cisco Email Security Appliance (ESA) : ESA inspecte tout les e-mails qui ne proviennent pas de Cisco, indépendamment de l'appareil utilisé pour accéder à la messagerie. Il bloque les messages des spammeurs connus et vérifie également la présence de contenu douteux ou d'autres anomalies. Sur les 5,6 millions d'e-mails que Cisco reçoit tous les jours, près des deux tiers sont bloqués. Environ 15 % des e-mails avec du contenu marketing sont autorisés, mais le serveur ESA les étiquette comme étant « marketing » ou « éventuel spam ». Pour faire face aux menaces de logiciels malveillants avancés, Cisco AMP est désormais intégré aux appareils ESA et le sera également à l'architecture Cisco.

Figure 5. Architecture de sécurité pour le BYOD, accès filaire et sans fil



Gestion

Le service IT de Cisco fournit tous les services « Tout type de périphérique » d'après le modèle ITaaS. Il offre aux utilisateurs les services IT selon l'usage qu'ils font de l'infrastructure et des applications, contrairement à une approche ad hoc, basée sur un besoin spécifique ou sur la demande d'un utilisateur. Cisco a créé un tableau de bord des métriques de service qui sont analysées tous les mois. Ces métriques comprennent le taux d'adoption, le coût total d'acquisition (TCO), le nombre de dossiers d'assistance technique, le niveau de satisfaction des utilisateurs et la conformité aux normes de sécurité. Si une métrique est inférieure aux objectifs du programme, Cisco en étudie les causes et applique les corrections nécessaires.

- Infrastructure Cisco PRIME : le service IT de Cisco utilise cette application pour une visibilité du réseau de bout en bout. Cette visibilité s'étend des terminaux (appareils personnels compris) jusqu'au data center sur le réseaux filaires et sans fil. La visibilité de bout en bout aide les équipes IT de Cisco à comprendre, à identifier et à résoudre les problèmes liés aux applications et aux services.

- Cisco Prime Service Catalog et Cisco Process Orchestrator : les employés Cisco peuvent télécharger des applications mobiles comme Cisco Jabber et Cisco WebEx via l'eStore Cisco, le déploiement interne Cisco Prime Service Catalog et Cisco Process Orchestrator. L'eStore automatise le processus de provisionnement. Il vérifie les critères d'éligibilité, génère une demande d'approbation, provisionne le service et contrôle le cycle de vie du service.

Gestion des demandes de service

Au départ, Cisco a mis en place un site intranet où les employés pouvaient ajouter leurs appareils personnels au réseau. Maintenant, les employés font la demande de services de mobilité via la communauté Mobility de WebEx Social, au travers une interface intuitive. Le système EMAN interne du service IT assure le provisionnement, mais les employés n'ont aucune interaction avec le logiciel. (Cisco prévoit d'éliminer ce système EMAN.)

Si un employé demande à ce que Cisco prenne en charge son forfait de téléphonie portable, la demande est transmise au vice-président responsable de cet employé, pour approbation. Si cet employé paye son forfait, l'eStore envoie un e-mail au responsable de l'employé indiquant que le service est provisionné.

Gestion des configurations

La gestion des configurations s'applique aux appareils et aux applications.

Chaque fois qu'un fabricant met à jour le matériel ou le logiciel de son appareil, le service IT Cisco teste la mise à jour dans l'environnement Cisco. L'objectif est de s'assurer que les changements n'affectent pas la sécurité et que l'appareil reste compatible avec WebEx, Jabber et les autres applications mobiles.

Cisco met aussi régulièrement à jour WebEx Social, EMAN, l'outil MDM et l'eStore pour qu'ils soient compatibles avec de nouveaux appareils, de nouveaux systèmes d'exploitation et de nouvelles applications. Par exemple, quand Apple a présenté son iOS 7 en septembre 2013, Cisco a dû mettre à jour son logiciel client et sa tête de réseau VPN Cisco AnyConnect. Cisco ajoute de nouvelles applications dans l'eStore tous les mois et s'assure que les applications sont hautement sécurisées et offrent une expérience utilisateur satisfaisante.

Gestion de la capacité

Cisco collecte des métriques sur ce programme depuis 2009. Cisco ASA fait état du nombre d'utilisateurs d'AnyConnect. Cisco ISE génère des rapports sur l'utilisation des appareils, par exemple les utilisateurs et les types d'appareil. Ces informations aident à estimer de façon exacte la demande. Cisco peut ainsi réadapter son infrastructure et décider des types d'appareils qui pourront être utilisés. Par exemple, les métriques ont très tôt montré que les appareils Symbian n'étaient plus très utilisés. Le service IT de Cisco a donc cessé de développer une version Symbian des clients mobiles.

Gestion des fournisseurs

Le département IT de Cisco et Cisco Global Procurement négocient les forfaits mensuels auprès des opérateurs. L'équipe surveille les tarifs pour s'assurer que les forfaits voix et données avec remise continuent à diminuer au même rythme que les forfaits de services mobiles grand public. Par ailleurs, Cisco renégocie régulièrement ses contrats avec les revendeurs pour faire bénéficier ses employés de remises sur les appareils qu'ils achètent.

Considérations relatives à l'infrastructure IT

Le programme « Tout type de périphérique » dispense le département IT de Cisco d'avoir à gérer les appareils mobiles, il continue à s'occuper de certains aspects :

- Forfaits de téléphonie mobile payés par l'entreprise : en collaboration avec Cisco Global Procurement, le département IT de Cisco gère environ 35 000 comptes auprès de plus de 100 opérateurs. Bande passante pour vidéo mobile : la bande passante dans les studios de Cisco TV, où les employés ont tendance à se connecter à plusieurs appareils, a déjà été optimisée. Cisco prévoit une augmentation de la demande en bande passante vidéo une fois que les applications vidéo mobiles seront ajoutées à l'eStore pour permettre aux employés d'assister aux réunions comme s'ils y étaient physiquement.
- Couverture sans-fil : l'équipe chargée de la mise en réseau suit le nombre d'appareils sans fil qu'utilise chaque employé. Ceci permet au département IT de Cisco d'adapter la capacité du réseau pour offrir une meilleure expérience utilisateur.
- Espaces d'adressage IP.

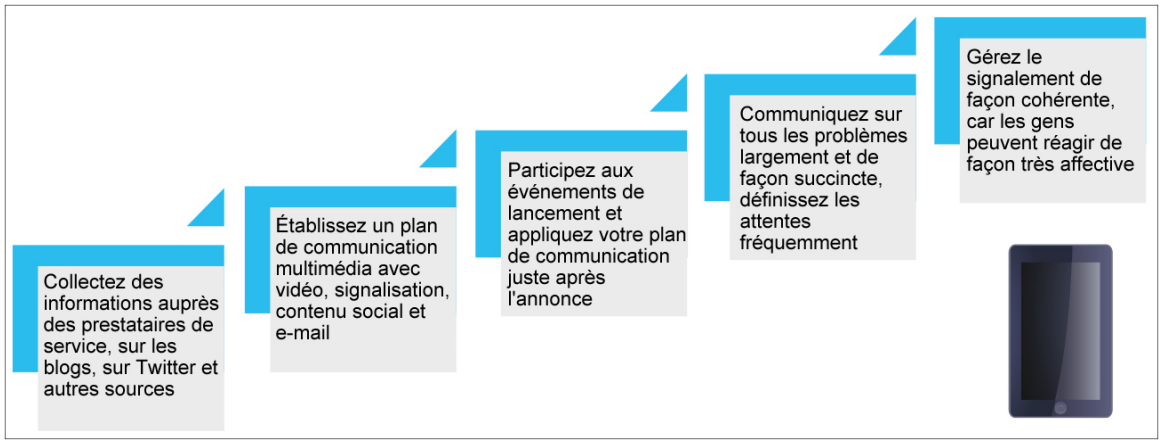
Gestion des licences logicielles

La plupart des applications mobiles de l'eStore sont gratuites, ce qui dispense le département IT de Cisco d'avoir à gérer des licences logicielles. Cependant, il doit gérer les comptes cloud de chaque employé. Lorsque de nouveaux employés rejoignent Cisco, les services cloud auxquels ils peuvent accéder sont automatiquement installés, notamment la messagerie électronique, l'accès VPN, WebEx, Jabber et autres. Lorsque les employés quittent Cisco, leurs comptes sont automatiquement fermés.

Gestion du cycle de vie

Les médias sociaux et d'autres sources d'actualités aident Cisco à se tenir informé en temps voulu des mises à niveau matérielles et logicielles (Figure 6). Par exemple, Cisco a eu connaissance de la version IOS 8 plusieurs mois avant son lancement et a pu commencer à utiliser la version bêta dès qu'elle a été disponible. Le département IT a commencé à la tester avec les applications mobiles Cisco et a ouvert une discussion WebEx Social sur ce qui fonctionnait ou ne fonctionnait pas. Le jour de la sortie officielle, Cisco a mis en place un blog mis à jour dynamiquement pour partager en temps réel les mises à jour Cisco et l'avis des utilisateurs.

Figure 6. Gestion du cycle de vie



Gestion des services

Chaque mois, Cisco génère des métriques sur le taux d'adoption des nouveaux appareils et des nouveaux logiciels, les dossiers d'assistance technique, les scores de satisfaction utilisateur, le coût par utilisateur, les dépenses liées aux opérateurs et le nombre d'appareils entièrement sécurisés. Ces informations permettent à Cisco de déterminer quand optimiser la capacité du réseau et quand proposer de nouvelles applications dans l'eStore. Elles sont diffusées via une communauté WebEx Social interne dans la mesure où d'autres équipes Cisco sont concernées par ces informations. Par exemple, les ingénieurs se réfèrent aux courbes d'adoption pour décider d'une stratégie produit.

Cisco surveille constamment la communauté Mobility sur WebEx Social pour être au fait des problèmes et des suggestions. Grâce à une collaboration étroite avec l'équipe de l'application WebEx, le service IT est en mesure d'offrir une expérience utilisateur au minimum aussi simple sur un smartphone ou une tablette que sur un ordinateur portable.

Services et assistance

Assistance en cas d'incident

En dépit d'une augmentation de 82 % du nombre d'utilisateurs entre 2011 et 2013, le nombre de dossiers d'assistance a diminué de 33 % au cours de cette même période. Cela s'explique par le fait que les employés obtiennent une assistance via la communauté Mobility dans WebEx Social et disposent notamment d'une fonction en libre-service pour les démarches suivantes :

- Choix de l'appareil et du forfait de services mobiles
- Obtention de l'autorisation de la direction
- Inscription et installation de nouveaux services
- Services sur plusieurs appareils
- Dépannage et problèmes courants
- Gestion des coûts imprévus (en particulier lors de déplacements)
- Perte ou vol du téléphone
- Changement de téléphone

Les employés qui ne trouvent pas de réponse à leur question dans WebEx Social peuvent ajouter une question ou envoyer un e-mail à une des listes de diffusion actives. Environ six membres du personnel IT de Cisco gèrent et modèrent les réponses et publient du contenu via ces différents canaux. Cisco encourage les utilisateurs à participer aux activités de la communauté.

Les employés peuvent également appeler le centre Cisco Global Technical Response Center (service d'assistance interne) pour les problèmes urgents ou nécessitant l'intervention d'un spécialiste dans tel ou tel appareil. Cependant, Cisco encourage les employés à résoudre eux-mêmes leurs problèmes, une méthode qu'ils privilégient d'ailleurs en raison de l'immédiateté de la réponse. Preuve à l'appui : le taux de satisfaction des employés a augmenté de 28 % depuis que Cisco a créé la communauté WebEx Social.

Équipe d'assistance

Une petite équipe veille à ce que les terminaux se connectent sans problème au réseau, qu'ils soient sécurisés et accèdent aux services stratégiques. En outre, au minimum deux personnes sont affectées à l'assistance technique de chaque application mobile proposée dans l'eStore. Le responsable de la maintenance travaille en collaboration avec Global Technical Response Center, Cisco Employee Connection, Global Business Services et Global Information Services.

Financement

Cisco a conçu le programme « Tout type de périphérique » pour qu'il soit autofinancé via une combinaison de financement privé et de refacturation aux différentes divisions.

Financement initial

À l'exception de la bande passante évoquée précédemment, le programme ne nécessite pas l'acquisition de nouvelles infrastructures, car il utilise les architectures de réseau, de data center, de collaboration et de sécurité déjà en place. Cisco a installé environ 10 % de points d'accès sans fil supplémentaires. La seule application ajoutée est le logiciel tiers MDM.

Les frais liés aux opérateurs représentent 90 % du coût du programme. Les frais d'infrastructure et les frais de gestion des services Cisco AnyConnect Secure Mobility représentent les 10 % restants. La charge de travail du service IT a diminué en dépit de l'ajout de dizaines de milliers de nouveaux appareils au réseau. En 2013, Cisco a géré ce service avec environ 33 % de personnel en moins qu'en 2009.

Financement régulier

La division de chaque employé se voit facturer un montant de frais de service mensuels, pour compenser les frais de développement, de gestion et de provisionnement des services « Tout type de périphérique ». Le montant facturé aux divisions a permis à Cisco d'adapter la capacité de l'infrastructure face à l'augmentation du nombre d'appareils de 20 000 à 66 000 en quatre ans. Ces frais sont réajustés tous les ans par rapport aux coûts réels de l'infrastructure et aux coûts prévisionnels liés à la prise en charge de nouveaux utilisateurs.

Cisco a négocié des contrats avec plus de 100 opérateurs mobiles dans le monde. Les employés qui peuvent prétendre à un forfait smartphone payé par Cisco sont ajoutés au plan d'entreprise, s'il en existe un. L'opérateur facture directement les frais à Cisco. Les directeurs reçoivent un rapport faisant état de factures atteignant des montants exceptionnellement importants pour des employés. Dans la mesure où chaque service règle une partie de la facture, les directeurs ont tout intérêt à inviter ces employés à réduire leur utilisation ou à changer de forfait.

La plupart des employés payent leur propre forfait, le forfait familial, les frais de résiliation, les frais de dépassement de forfait voix ou données, ainsi que les services mobiles supplémentaires. Ces options ne s'appliquent pas à un compte mobile d'entreprise pris en charge par Cisco. Cisco informe les employés de la disponibilité de forfaits proposés aux personnes qui ne voyagent pas à l'extérieur du pays ou à celles se déplaçant de façon occasionnelle ou régulière.

Leçons retenues par Cisco

La conception et la mise en œuvre d'une stratégie « Tout type de périphérique » est un changement important pour toute organisation. Une telle transformation sera acceptée plus volontiers et plus efficacement si une structure de gouvernance uniforme est en place. Dans cette démarche d'adoption de la vision « Tout type de périphérique » à l'échelle de l'entreprise, les dirigeants, le département IT et les spécialistes sécurité de Cisco ont beaucoup appris. Voici les enseignements tirés.

Enseignements sur le plan commercial :

- La mise en œuvre de la stratégie « Tout type de 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 multidisciplinaire, de former les responsables et de fournir les résultats et les mesures.
- La mise en œuvre du programme « Tout type de périphérique » se répercute sur toute l'organisation. Tous les intéressés doivent comprendre le volume de travail que représente l'élaboration de politiques, ainsi que les enjeux de cette stratégie.

Résumé des métriques 2011-2013

Réduction des coûts :

- 500 000 $ économisés tous les ans en dépenses d'achat d'appareils en encourageant le BYOD pour les smartphones et les tablettes
- Réduction des frais d'opérateurs annuels bruts de 30 % en revalidant les services payés par l'entreprise
- Réduction du nombre de dossiers d'assistance de 40 % en deux ans, grâce au déploiement de l'assistance sur les médias sociaux et notamment sur la communauté WebEx Social

Métriques de service :

- Augmentation de 82 % du nombre d'appareils et augmentation de 203 % de l'utilisation des données
- Augmentation de 28 % du nombre d'utilisateurs à un coût par utilisateur inférieur de 25 %
- Amélioration du taux de satisfaction client (+ 28 %)

- 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 type de périphérique ».
- Contrôlez les coûts en réévaluant régulièrement si les utilisateurs doivent bénéficier de forfaits payés par l'entreprise, en tenant compte des commentaires et en offrant aux employés des conseils pour réduire les frais d'itinérance, d'utilisation des données et l'utilisation de la téléphonie mobile.
- Informez en continu les utilisateurs sur la sécurisation de leurs appareils via des forums de discussion, des guides utilisateur, les bonnes pratiques, des vidéos et des formations.
- Élaborez des politiques et des procédures d'effacement des informations sensibles lorsque les employés quittent la société et exigez que les employés se conforment à ces procédures.
- Pour encourager l'assistance en libre-service, offrez du contenu mis à jour, facilement accessible et simple à comprendre.

Enseignements sur le plan technique :

- Avertissez les utilisateurs au sujet des cartes SIM (Subscriber Identity Module) et des frais imprévus imputables au changement de cartes SIM entre les téléphones de différents fabricants. Mettez en place des systèmes pour éviter cette pratique.
- Assurez-vous que l'espace d'adressage sans fil dans les bureaux est suffisant pour prendre en charge un nombre grandissant d'utilisateurs mobiles. Ajoutez des espaces d'adressage IP sans fil dans les lieux les plus fréquentés.
- Testez les nouvelles applications mobiles et les portails en libre-service auprès d'employés occupant différentes fonctions. Pensez à inclure des employés qui ne font pas partie du service IT, ainsi que des employés de différents pays.

- Pour le réseau sans fil destiné aux invités, pensez à installer des processus de communication multicanal pour les utilisateurs et l'équipe d'assistance.
- Préparez des déploiements limités pour tester la compatibilité et offrir un espace de formation pratique pour faciliter l'assistance et la transition vers une utilisation généralisée.
- Si possible, utilisez des ressources d'ingénierie et d'assistance situées partout dans le monde pour optimiser les coûts et les niveaux de service.
- Tenez-vous informé des tendances du secteur, des nouvelles technologies et des nouvelles normes pour mieux assurer la compatibilité, l'assistance et l'évolution de votre service.

Premières étapes de la démarche « Tout type de périphérique »

Lorsque Cisco a entrepris la démarche « Tout type de périphérique », 13 secteurs d'activités importants concernés par ce nouveau modèle ont été identifiés. Le tableau 1 présente ces secteurs d'activités et fournit une liste de questions qui ont aidé Cisco (et peuvent également vous aider) à identifier les problèmes potentiels et à déterminer la meilleure approche pour y remédier. Réfléchissez à ces questions et répondez de manière objective.

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

Secteur d'activités	Questions relatives aux activités de l'entreprise auxquelles vous devez répondre
Continuité des activités et récupération après 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 travailleurs 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 IT géreront-elles les incidents et les recherches liés aux appareils n'appartenant pas à l'entreprise ? • Comment l'équipe de gestion des incidents obtiendra-t-elle les données nécessaires à l'enquête ?
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 appareils qui ne lui appartiennent pas ?
Services juridiques	• Existe-t-il une législation locale qui exige certains changements et certaines politiques ? • Les contrats de licence utilisateur final (EULA) internes sont-ils mis à jour en conséquence ?

Pour en savoir plus

Cisco a déjà commencé à mettre en œuvre l'approche d'un environnement « tout type de service, tout type de périphérique, partout » basé sur le choix des employés. Nous continuerons à partager notre expérience pour aider le personnel IT, le personnel de sécurité de l'information et les architectes de la sécurité de l'information à anticiper les problèmes. Les connaissances et la méthodologie adoptées par Cisco pour transformer son organisation et son environnement IT en une architecture « Tout type de périphérique » et au-delà peuvent s'appliquer à d'autres entreprises, quelle que soit leur taille.

Contactez votre représentant Cisco pour savoir quelle stratégie adopter afin de préparer vos infrastructures commerciales, IT et de sécurité à migrer vers une architecture « Tout type de périphérique ».

Pour plus d'informations sur les solutions de sécurité Cisco axées sur l'approche « Tout type de périphérique », consultez la page : http://www.cisco.com/go/security.

Siège social aux États-Unis
Cisco Systems
San José, 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 de Cisco, à l'adresse : **www.cisco.com/go/offices**.

Imprimé aux États-Unis C11-681837-01 01/15