10 éléments essentiels pour une stratégie de mobilité d'entreprise sécurisée

Les meilleures pratiques pour protéger les informations d'entreprise sensibles tout en rendant les utilisateurs productifs en tout lieu

CITRIX®

citrix.fr/secure

La mobilité et le BYOD transforment radicalement la façon dont les utilisateurs travaillent et la façon dont les entreprises les prennent en charge. La mobilité, c'est bien plus que le simple accès distant, et les périphériques mobiles ne sont pas de simples gadgets à usage limité. Capables d'utiliser, de stocker et de transmettre des applications et des données au même titre que les ordinateurs traditionnels, les smartphones et les tablettes peuvent être utilisés pour pratiquement toutes les tâches professionnelles. Pour exploiter pleinement les potentialités de la mobilité d'entreprise, les directions informatiques doivent permettre à leurs utilisateurs d'accéder de façon transparente et conviviale à toutes leurs applications et données, depuis tout périphérique.

Les périphériques mobiles imposent également d'adopter la bonne approche sécuritaire afin de protéger les données d'entreprise même lorsqu'elles sont utilisées dans un plus grand nombre d'endroits, souvent via des réseaux non sécurisés, avec un risque significatif de perte ou de vol. Les directions informatiques doivent maintenir la conformité et protéger les données sensibles quels que soient l'endroit et la façon dont elles sont utilisées et stockées, même lorsque des applications personnelles et professionnelles cohabitent sur le même périphérique. Les tendances mobiles émergentes comme les technologies portables ou l'Internet des objets imposent déjà de prendre en compte de nouvelles considérations. Pour toute entreprise, concevoir une stratégie de mobilité véritablement complète et sécurisée constitue désormais une priorité incontournable.

Ce livre blanc présente 10 points essentiels à prendre en considération lors de la conception de votre stratégie de mobilité d'entreprise. Il aborde notamment la sécurité, l'expérience utilisateur, les opérations informatiques et le BYOD. Leader dans le domaine du travail mobile, Citrix propose une solution complète permettant la mise en œuvre d'une mobilité d'entreprise sécurisée et intégrant des technologies de gestion des périphériques mobiles (MDM), de gestion des applications mobiles (MAM), de virtualisation de postes et d'applications et de sécurité de bout en bout depuis le datacenter jusqu'au périphérique. Associées, ces directives, ces meilleures pratiques et ces technologies aideront votre entreprise à tirer pleinement parti de la mobilité.

1. Gérer et protéger ce qui compte le plus

Les utilisateurs accédant aux applications et aux données à partir de multiples périphériques (y compris des tablettes et des smartphones personnels), les directions informatiques ne peuvent plus espérer de façon réaliste contrôler et gérer toutes les facettes de leur environnement. Vous devez en fait vous concentrer sur ce qui compte le plus pour votre entreprise et opter pour les modèles de gestion de la mobilité les plus adaptés à votre activité et à vos scénarios mobiles. Vous avez le choix entre quatre modèles, qui peuvent être utilisés de façon autonome ou associés.

La gestion des périphériques mobiles (MDM) : La MDM vous permet de gérer et de contrôler les périphériques mobiles utilisés pour accéder aux ressources d'entreprise. Avant qu'un périphérique (personnel ou d'entreprise) n'accède au réseau de l'entreprise, vous pouvez vérifier s'il a été débridé ou compromis d'une quelconque façon. Le chiffrement, le verrouillage et la suppression à distance, le VPN mobile, les listes noires applicatives et la

capacité à désactiver de façon sélective des fonctionnalités natives des périphériques garantissent un haut degré de sécurité.

Les conteneurs et hyperviseurs mobiles : Particulièrement utile pour la prise en charge du BYOD, ce modèle vous permet de gérer les applications, les données, les stratégies et les paramètres au sein d'un conteneur situé sur le périphérique, sans aucune interaction avec le contenu personnel éventuellement hébergé. Dans les faits, le périphérique mobile se décompose en deux périphériques virtuels distincts : l'un destiné au travail, l'autre à une utilisation personnelle.

La gestion des applications mobiles (MAM) : Basée sur l'approche de création de conteneurs, la MAM vous permet de centraliser la gestion, la sécurisation et le contrôle de toute application mobile, ainsi que de ses données et paramètres, au sein d'un conteneur. Les stratégies applicatives peuvent prendre en compte plusieurs facteurs : l'authentification, le réseau, la localisation, les mots de passe et le chiffrement.

La virtualisation de postes et d'applications : La sécurité intrinsèque de la virtualisation bénéficie également aux scénarios mobiles. Les applications d'entreprise peuvent être optimisées pour les périphériques mobiles et délivrées à la demande, tandis que les données demeurent bien protégées au sein du datacenter.

2. Penser en premier lieu à l'expérience utilisateur

Les périphériques mobiles ont constitué l'un des principaux moteurs de l'essor de la consumérisation en entreprise, en offrant aux utilisateurs de nouvelles façons performantes de travailler avec les applications et les données dans leur vie de tous les jours. Ils ont de fait mis la barre très haut pour les directions informatiques, qui doivent désormais fournir une expérience similaire en termes de liberté et de convivialité à celle offerte par les technologies grand public. Il peut être utile de s'asseoir un moment avec les utilisateurs et de discuter de leurs besoins et de leurs préférences afin de s'assurer que la stratégie de mobilité adoptée leur offrira vraiment ce qu'ils attendent.

Lorsque vous chercherez à garantir une expérience de qualité supérieure, cherchez des moyens permettant d'offrir à vos utilisateurs plus que ce qu'ils attendent et de fournir des fonctionnalités utiles auxquelles ils n'ont peut-être pas encore pensé. Par exemple :

- Permettre aux utilisateurs d'accéder à leurs applications et données sur tout périphérique, avec l'ensemble de leurs paramètres personnalisés, afin qu'ils soient immédiatement opérationnels.
- Autonomiser les utilisateurs grâce au provisioning en libre-service pour toute application (hébergée, mobile ou SaaS), via une librairie applicative d'entreprise bénéficiant du single sign-on.
- Fournir des clients légers partagés ou d'autres périphériques d'entreprise utilisables par vos employés dont l'accès à certaines applications a été désactivé sur leur périphérique grand public en raison d'exigences de sécurité.
- Automatiser les contrôles pour la gestion et le partage de données (capacité à copier des données d'une application sur une autre, par exemple), afin que les utilisateurs n'aient pas à mémoriser des stratégies spécifiques.
- Définir application par application les fonctionnalités autorisées sur chaque type de périphérique, afin que les employés puissent toujours utiliser des fonctionnalités (impression, caméra, stockage local des données, etc.) sur certaines de leurs applications même lorsque leur direction informatique a décidé de les désactiver sur d'autres applications.

- Permettre aux utilisateurs de synchroniser et de partager facilement leurs fichiers à partir de tout périphérique et de partager des fichiers avec des tiers en envoyant simplement un lien.

En développant votre stratégie de mobilité dans un esprit de collaboration avec vos utilisateurs, vous répondrez mieux à leurs besoins tout en leur faisant comprendre les obligations de votre direction informatique en matière de conformité (besoin de sécuriser les applications et les données, de contrôler l'accès au réseau, de gérer correctement les services, etc.).

3. Eviter le quadruple contournement

Le quadruple contournement représente le pire scénario possible en matière de mobilité d'entreprise : un utilisateur BYOD utilise des données d'entreprise sensibles sur un périphérique grand public en allant directement sur le cloud. Cette approche contourne complètement tous les mécanismes de contrôle et de visibilité de la direction informatique. Ce cas de figure est malheureusement de plus en plus fréquent en entreprise aujourd'hui. Il y a bien sûr de bonnes raisons à cela. Les applications cloud aident les utilisateurs à gagner du temps et à accomplir leur travail plus facilement, et permettent de générer plus facilement de la valeur ajoutée pour l'entreprise. Le problème se pose lorsque ces applications cloud sont utilisées de façon inadéquate avec des données d'entreprise sensibles, compromettant de fait la sécurité et la conformité.

Les stratégies informatiques et la sensibilisation des utilisateurs ne suffisent pas à prévenir ce quadruple contournement. En effet, soyons réaliste ! Si c'est la meilleure solution pour répondre à un besoin et que la direction informatique est peu susceptible de le découvrir, ça se produira ! Il est donc indispensable d'inciter les utilisateurs à collaborer avec la direction informatique et d'utiliser son infrastructure, tout particulièrement lorsqu'il s'agit d'applications et de données sensibles. La meilleure incitation possible, c'est une expérience de qualité supérieure, délivrée de façon proactive et spécialement conçue pour mieux répondre aux besoins que les solutions alternatives non gérées.

4. Accorder une grande attention à votre stratégie de mise à disposition de service

Les utilisateurs mobiles s'appuient sur de nombreux types d'applications : non seulement des applications mobiles personnalisées, mais également des applications mobiles natives tierces, des applications Windows mobilisées et des solutions SaaS. En concevant votre stratégie de mobilité, vous devrez penser au large éventail d'applications employé par les utilisateurs et groupes d'utilisateurs de votre entreprise, ainsi qu'à la façon dont il faudra y accéder à partir des périphériques mobiles.

Les utilisateurs peuvent accéder de quatre façons à leurs applications depuis un périphérique mobile :

Expérience de périphérique natif : Dans ce scénario, le périphérique de l'utilisateur n'est absolument pas géré. Chacun achète ses propres applications, peut mélanger librement des données personnelles et professionnelles et peut travailler via tout réseau. Tout comme pour le quadruple contournement décrit précédemment, il s'agit là d'une approche non sécurisée extrêmement risquée, qui ne devrait jamais être autorisée pour les données sensibles.

Expérience d'accès virtualisé : Des applications et des données virtuelles, ainsi que des postes de travail virtuels le cas échéant, sont hébergés au sein du datacenter et mis à disposition via un protocole d'affichage distant. La direction informatique peut gérer l'accès et garantir une sécurité totale, tout en permettant aux utilisateurs d'exécuter des applications Windows sur des plateformes mobiles. Aucune donnée ne quitte à

un quelconque moment le datacenter, limitant ainsi significativement les besoins de protection sur le périphérique lui-même. Cette méthode repose sur la connectivité, qui limite les scénarios d'utilisation en mode hors-ligne.

Expérience conteneurisée : L'entreprise crée un conteneur sur le périphérique, au sein duquel toutes les applications mobiles d'entreprise (y compris les applications personnalisées et les applications mobiles natives tierces) seront conservées bien séparées de tout autre contenu. La direction informatique pourra gérer les applications et données qui doivent aller dans le conteneur tout en permettant aux utilisateurs de provisionner leurs propres applications via une librairie applicative d'entreprise. Les applications peuvent être mises à jour, provisionnées et modifiées automatiquement à partir de stratégies informatiques définies. Les paramètres réseau de type SSL, chiffrement ou VPN spécifiques à certaines applications peuvent également être intégrés au conteneur afin de permettre aux utilisateurs de se connecter facilement et d'une façon appropriée quels que soient les paramètres. Le conteneur peut être supprimé à distance en cas de perte, de vol ou de mise à jour du périphérique, ou si l'employé quitte l'entreprise.

Expérience d'entreprise totalement gérée : Cette approche préserve un contrôle complet sur le périphérique mobile grâce à des stratégies intégrées (suppression à distance, restrictions géographiques, expiration des données ou autres mesures de sécurité). Toutes les applications mobiles sont choisies de façon explicite et provisionnées par la direction informatique, sans aucune possibilité de personnalisation. Si cette approche s'avère hautement sécurisée et particulièrement adaptée à certaines entreprises et à certains scénarios spécifiques, elle génère une expérience extrêmement contraignante, totalement incompatible avec le BYOD.

Pour la majorité des entreprises, l'association d'un accès virtuel et d'une expérience conteneurisée permettra de prendre en charge l'éventail complet d'applications et de scénarios souhaités par les utilisateurs. Cette approche permet en outre aux directions informatiques de préserver la visibilité et le contrôle, tout en garantissant aux utilisateurs une expérience supérieure. Ces derniers peuvent accéder aux applications hébergées et aux applications mobiles natives (de même qu'aux applications SaaS de type Salesforce ou NetSuite) via un single sign-on d'entreprise unifié. Lorsqu'un employé quitte l'entreprise, sa direction informatique peut immédiatement désactiver son compte pour supprimer l'accès à toutes les applications hébergées, mobiles natives et SaaS utilisées sur le périphérique.

5. Automatiser l'atteinte des résultats escomptés

L'automatisation ne se contente pas de simplifier la vie des directions informatiques, elle leur permet également de délivrer une meilleure expérience. Pensez un peu à la valeur ajoutée que l'automatisation peut apporter pour répondre aux besoins de mobilité les plus courants :

- Un employé remplace un périphérique égaré ou change son périphérique contre un nouveau. En cliquant simplement sur une unique URL, toutes les données de travail et applications d'entreprise seront disponibles sur le nouveau périphérique, totalement configuré, personnalisé et opérationnel. De même, un nouvel employé ou sous-traitant est intégré tout aussi facilement, avec toutes ses applications mobiles d'entreprise provisionnées au sein d'un conteneur hébergé sur n'importe quel périphérique personnel ou d'entreprise. Le single sign-on (SSO) permet un accès transparent aux applications SaaS et hébergées.
- Lorsqu'un employé passe d'un endroit à un autre et d'un réseau à un autre, des contrôles d'accès adaptatifs et sensibles au contexte reconfigurent automatiquement les applications afin de garantir une sécurité appropriée, avec une transparence totale pour l'utilisateur.

- Un membre du conseil d'administration se rend à une réunion avec une tablette à la main. Tous les documents pour la réunion sont automatiquement chargés sur le périphérique, configurés par la direction informatique pour un accès en lecture seule, et limités en cas de besoin à une utilisation via une application conteneurisée. Les documents particulièrement sensibles peuvent être paramétrés pour disparaitre automatiquement du périphérique dès que la personne quitte la salle de réunion.
- Lorsque les employés changent de fonction au sein de l'entreprise, les applications associées à leur nouveau poste sont automatiquement rendues disponibles, tandis que celles devenues inutiles disparaissent. Les licences SaaS tierces font instantanément l'objet d'une demande de réattribution.

Un moyen permettant de parvenir à ce type d'automatisation consiste à s'appuyer sur Active Directory. En premier lieu, il faut lier chaque fonction à un conteneur correspondant. Tout utilisateur exerçant cette fonction héritera automatiquement de ce conteneur et de toutes les applications et données, de tous les paramètres et privilèges qui lui sont associés. Sur le périphérique lui-même, vous pouvez vous servir de la MDM pour définir et installer de façon centralisée des mots de passe et des codes PIN WiFi, des certificats utilisateur, une authentification à deux facteurs et tout autre élément nécessaire à la prise en charge de ces processus automatisés.

6. Définir le réseau de façon explicite

A différentes applications et à différents scénarios correspondront différents besoins en termes de réseau : site intranet ou Microsoft SharePoint, portail partenaire externe, application sensible exigeant une authentification SSL mutuelle, etc. Appliquer les paramètres de sécurité les plus élevés sur le périphérique dégrade inutilement l'expérience de l'utilisateur. D'autre part, demander aux utilisateurs d'appliquer différents paramètres pour chaque application peut s'avérer encore plus fastidieux pour ces derniers.

En limitant les différents réseaux à des applications ou à des conteneurs spécifiques, avec des paramètres distincts définis pour chacun, vous pouvez mettre en place des réseaux spécifiques à chaque application sans exiger d'actions supplémentaires de la part de vos utilisateurs. Ceux-ci n'ont qu'à cliquer sur une application et peuvent commencer à travailler, pendant que des tâches comme l'authentification, l'acceptation de certificats ou l'ouverture d'un VPN spécifique à une application se lancent automatiquement en arrière-plan conformément aux stratégies définies.

7. Protéger par-dessus tout les données sensibles

Dans bon nombre d'entreprises, la direction informatique ne sait pas où résident les données les plus sensibles et doivent donc traiter toutes les données avec le même niveau de protection, ce qui constitue une approche à la fois coûteuse et inefficace. La mobilité vous offre l'opportunité de protéger vos données de façon plus sélective, à partir d'un modèle de classification répondant à vos besoins commerciaux et de sécurité spécifiques.

De nombreuses entreprises s'appuient sur un modèle relativement simple, qui classe les données en trois catégories (publiques, confidentielles et à diffusion restreinte) et prend également en compte le périphérique et la plateforme utilisés. D'autres entreprises adoptent un modèle de classification bien plus complexe qui prend aussi en compte de nombreux autres facteurs comme la fonction de l'utilisateur et sa localisation. Il existe une façon de mettre en œuvre un modèle relativement simple :

Les données publiques auxquelles n'est associé aucun degré de confidentialité ou de conformité peuvent bénéficier d'une mobilité illimitée et d'une utilisation sans restriction, en tout lieu et sur tout périphérique. Inutile pour les utilisateurs de passer par l'infrastructure de l'entreprise : vous pouvez configurer des paramètres réseau propres à chaque application pour permettre aux utilisateurs de se connecter de la manière qui leur semble la plus pratique.

Les données confidentielles qui ne sont pas destinées à être rendues publiques, mais représentent un certain risque en cas de fuite, exigent un plus haut degré de protection. Dans ce cas, vous pouvez fournir un accès virtuel via le réseau de l'entreprise pour les périphériques BYOD ou grand public, et n'autoriser une mobilité totale des données que pour les périphériques d'entreprise dotés de fonctionnalités MDM telles que le chiffrement et la suppression à distance, ou pour les périphériques spéciaux, spécifiquement conçus pour protéger les données en contexte hostile. Certaines entreprises peuvent considérer que l'approche avec conteneur est suffisante pour ce type de données. Dans ce cas, les données peuvent bénéficier d'une mobilité totale sur tout périphérique mobile si elles sont stockées uniquement au sein d'un conteneur distinct, qui pourra être sécurisé et contrôlé par la direction informatique.

Les données à diffusion restreinte posant un risque avéré de non-conformité, de dégradation significative de l'image de l'entreprise, de perte de chiffre d'affaires et autres conséquences néfastes doivent faire l'objet de toute votre attention. La mobilité complète des données devra être limitée aux périphériques spéciaux pour contexte hostile, et l'accès virtuel autorisé sur les périphériques d'entreprise. Les périphériques BYOD et grand public ne bénéficieront d'aucun accès, ou pourront dans certaines circonstances et après vérification soigneuse bénéficier d'un accès virtuel avec conteneurs.

Le modèle ci-dessus tient compte à la fois de la classification des données et du type de périphérique. vous pouvez également souhaiter intégrer d'autres considérations à votre stratégie de sécurité, comme par exemple la plateforme du périphérique, la localisation géographique ou la fonction de l'utilisateur. Certaines entreprises et de nombreuses administrations préfèrent créer un éventail plus large de catégories de données plus spécifiques, chacune dotée de ses propres règles.

En configurant l'accès réseau via votre infrastructure d'entreprise pour les données confidentielles et à diffusion restreinte, vous pouvez bénéficier d'informations précises sur la façon dont vos employés utilisent l'information et ainsi évaluer l'efficacité de votre modèle de sensibilité des données et de votre stratégie de contrôle mobile.

8. Bien clarifier les fonctions et les responsabilités

Qui sera responsable de la mobilité d'entreprise au sein de votre organisation ? Dans la plupart des entreprises, la mobilité continue à faire l'objet d'une approche ad hoc, souvent mise en œuvre par une commission contrôlant l'ensemble des fonctions informatiques, depuis l'infrastructure jusqu'aux applications en passant par le réseau. Etant donné le rôle stratégique de la mobilité en entreprise et vu la complexité de la matrice des utilisateurs et des besoins informatiques à satisfaire, il est crucial de définir clairement la structure organisationnelle, les fonctions et les processus associés à la mobilité. Chacun doit comprendre qui est responsable de la mobilité et comment celle-ci sera gérée de façon globale entre les différentes fonctions informatiques.

La responsabilité des périphériques mobiles eux-mêmes doit elle aussi être clairement établie, tout particulièrement dans les entreprises où la mobilité et le BYOD vont de pair. Votre stratégie BYOD doit couvrir la zone d'ombre située entre les périphériques d'entreprise totalement gérés et les périphériques personnels des utilisateurs réservés strictement à leur usage privé. Par exemple :

- Qui est responsable des sauvegardes pour un périphérique BYOD ? Qui assure le support et la maintenance pour le périphérique, et qui paye quoi ?
- Comment la propriété intellectuelle créée sera-t-elle gérée si un sous-traitant recherche des données ou se connecte à partir d'un périphérique personnel ?
- Quelles sont les implications en matière de confidentialité pour le contenu personnel lorsque quelqu'un utilise le même périphérique à des fins professionnelles ?

Les utilisateurs et les directions informatiques doivent parfaitement comprendre leurs responsabilités et rôles respectifs afin d'éviter tout malentendu. Définir votre programme BYOD de façon explicite et faites signer un document d'engagement aux participants avant qu'ils ne commencent à utiliser leurs périphériques personnels au travail.

9. Intégrer la conformité à vos solutions

A l'échelle mondiale, les entreprises sont tenues de respecter plus de 300 normes, réglementations ou lois liées à la confidentialité et à la sécurité, auxquelles s'ajoutent plus de 3 500 contrôles spécifiques. Mais respecter ces obligations ne suffit pas : vous devez en outre documenter et prouver votre conformité et permettre la mise en œuvre d'audits complets. Sans parler de vos stratégies d'entreprise internes. Il se peut que vous ayez déjà résolu les problèmes de conformité au sein de votre réseau. Dans ce cas, la dernière chose que vous souhaiterez sera bien de laisser la mobilité d'entreprise créer un vaste nouveau problème à résoudre. Assurez-vous que vos plateformes et périphériques mobiles bénéficient d'une conformité transparente aux obligations réglementaires, normes de votre secteur et stratégies de sécurité internes, depuis le contrôle d'accès basé sur des stratégies et une classification jusqu'au stockage sécurisé des données. Votre solution doit permettre une tenue complète de journaux et la publication de comptes-rendus afin de vous permettre de répondre rapidement, efficacement et avec succès aux demandes d'audit.

10. Se préparer à l'Internet des objets

Ne concevez pas vos stratégies uniquement pour aujourd'hui. Essayez de vous figurer ce que sera la mobilité d'entreprise dans quelques années. Les technologies portables comme Google Glass ou les montres intelligentes continueront à bouleverser la façon dont les gens utilisent les technologies mobiles. Elles garantiront une expérience plus humaine et intuitive, tout en permettant la prise en charge de nouveaux scénarios d'utilisation. Des véhicules connectés (notamment des véhicules sans conducteur) utiliseront des données et des services cloud sous de nouvelles formes afin d'aider les gens à aller là où ils veulent aller plus facilement et plus efficacement. Des systèmes de contrôle industriel (ICS) utiliseront et échangeront des données d'entreprise aussi bien en arrière-plan que dans le cadre de flux humains. Les innovations de ce type continueront à renforcer le potentiel de la mobilité, mais elles génèreront également de nouvelles implications dans les domaines de la sécurité, de la conformité, de la gestion et de l'expérience utilisateur.

Accordez toute votre attention aux discussions en cours sur ce type de technologies émergentes et concevez votre stratégie de mobilité autour de principes de base applicables à tout type de périphérique mobile et de scénario. De cette façon, vous limiterez la fréquence des itérations et des modifications de stratégie, qui peuvent susciter la confusion et frustrer les utilisateurs.

La solution Citrix pour une mobilité d'entreprise sécurisée

Leader dans le domaine du travail mobile, Citrix propose une solution complète permettant la mise en œuvre d'une mobilité d'entreprise sécurisée, avec l'expérience simple et conviviale que vos utilisateurs demandent. Intégrant des technologies complètes de MDM, de MAM, de création de conteneurs et de virtualisation de postes et d'applications, cette solution offre une grande liberté pour prendre en charge la mobilité sécurisée de la façon la plus appropriée pour chaque type de donnée, de scénario et de fonction au sein de votre entreprise.

La solution Citrix pour une mobilité d'entreprise sécurisée comprend les produits suivants :

XenMobile : XenMobile offre des fonctionnalités MDM et MAM complètes destinées à la gestion de la mobilité d'entreprise sécurisée. Les directions informatiques peuvent fournir un accès en un seul clic aux applications mobiles, Web, Windows et du datacenter à partir d'une librairie applicative unifiée, y compris à des applications de productivité

intégrée, en offrant une superbe expérience utilisateur. XenMobile fournit également des applications de messagerie, de navigation et d'agenda sécurisées et d'entreprise, afin d'éviter les failles de sécurité inévitablement liées aux applications grand public. La direction informatique bénéficie d'options de provisioning et de contrôle des applications, des données et des périphériques basés sur l'identité, de déprovisioning de compte automatique pour les utilisateurs licenciés et la suppression sélective à distance des données et applications sur les périphériques perdus. La technologie intégrée de conteneur d'applications Citrix MDX offre des fonctionnalités comme le chiffrement de données, l'authentification par mot de passe, le verrouillage et la suppression sécurisés, des stratégies interapplicatives et des micro VPN pour les applications mobiles.

XenDesktop et XenApp : XenDesktop et XenApp permettent aux directions informatiques de transformer des applications Windows et des postes de travail Windows complets en services à la demande délivrés sur tout périphérique. Les applications et les données sont gérées au sein du datacenter, ce qui permet à la direction informatique d'assurer la protection des données, la conformité, le contrôle d'accès et l'administration des utilisateurs de façon centralisée, aussi bien sur des périphériques personnels que sur des périphériques d'entreprise, le tout dans un environnement unifié. XenApp permet également de mobiliser facilement les applications Windows pour une utilisation sur smartphones et tablettes et d'adapter leurs interfaces afin qu'elles se comportent comme des applications mobiles natives sur un périphérique mobile, garantissant ainsi une expérience optimisée.

ShareFile : ShareFile vous permet de délivrer un service robuste et sécurisé de synchronisation et de partage de fichiers, capable de répondre à tous les besoins de mobilité et de collaboration de votre personnel. Une expérience riche de type grand public permet aux utilisateurs de stocker et de synchroniser facilement leurs données sur tous leurs périphériques à partir de n'importe quel point du réseau. La direction informatique peut maintenir un haut degré de gestion et de contrôle pour le partage et la synchronisation de fichiers, grâce à une liberté totale quant au choix de l'endroit où les données seront stockées, à des stratégies efficaces de sécurisation des périphériques, à des fonctionnalités d'audit complètes et à l'intégration avec Microsoft Active Directory.

NetScaler : NetScaler est un contrôleur de mise à disposition d'applications tout-en-un qui permet de sécuriser, de contrôler et d'optimiser la mise à disposition des applications, des postes de travail et des services sur tout périphérique. La compatibilité étendue avec les systèmes d'exploitation mobiles permet un accès VPN SSL complet pour les principaux périphériques et systèmes d'exploitation mobiles (notamment Apple, Google et Microsoft). La prise en charge du Micro VPN SSL vous permet de définir des paramètres de connexion spécifiques pour chaque application sans exiger d'actions supplémentaires de la part des utilisateurs. Le contrôle d'accès, l'audit et les rapports assurent la conformité et la protection des données. Le contrôle et la visibilité de bout en bout permettent une meilleure orchestration de l'intégralité de votre infrastructure et la répartition efficace des charges entre les différents composants de la mobilité Citrix.

Conclusion

La mobilité d'entreprise s'est rapidement étendue et ne s'applique plus uniquement à quelques groupes d'utilisateurs et scénarios bien précis. Elle est aujourd'hui devenue un élément fondamental de l'informatique d'entreprise. Lorsque vous concevrez votre stratégie de mobilité d'entreprise, assurez-vous de prendre en compte l'éventail complet des besoins de vos utilisateurs et de votre direction informatique. Les utilisateurs attendent un accès transparent et convivial à leurs données et applications, depuis tout périphérique et avec une expérience encore meilleure que celle dont ils bénéficient chez eux. Les directions informatiques doivent être capables de maintenir le bon degré de contrôle, de protection et de conformité pour chaque type de données, sans pour autant restreindre inutilement la possibilité pour l'utilisateur de choisir sa façon de travailler. Les solutions Citrix

offrent les fonctionnalités complètes dont vous avez besoin pour prendre en charge votre stratégie de mobilité d'entreprise. Elles comprennent XenMobile pour la MDM, la MAM et la création de conteneurs ; XenDesktop et XenApp pour la virtualisation ; ShareFile pour la synchronisation et le partage sécurisés des fichiers ; NetScaler pour la sécurisation, le contrôle et l'optimisation de la mise à disposition des services sur les périphériques mobiles. En utilisant de façon astucieuse les modèles disponibles et les technologies de sécurité et d'accès aux données et aux applications sur périphériques mobiles, vous pouvez mettre en place la stratégie de mobilité complète dont votre entreprise aura besoin aujourd'hui et dans les années à venir.

Ressources supplémentaires

Etude de cas : Comment quatre entreprises ont relevé avec succès le défi de la mobilité d'entreprise

Délivrer des informations d'entreprise en toute sécurité sur les périphériques Android et iOS

Les 10 incontournables pour une mobilité d'entreprise sécurisée

Gestion de la mobilité d'entreprise : Adopter le BYOD via la mise à disposition sécurisée des applications et données

Siège social
Fort Lauderdale, Floride, États-Unis

Siège Silicon Valley
Santa Clara, Californie, États-Unis

Siège Europe, Moyen-Orient, Afrique
Schaffhausen, Suisse

Centre de développement Inde
Bangalore, Inde

Siège Division en ligne
Santa Barbara, Californie, États-Unis

Siège Pacifique
Hong Kong, Chine

Siège Amérique latine
Coral Gables, Floride, Etats-Unis

Centre de développement Royaume-Uni
Chalfont, Royaume-Uni

À propos de Citrix
Citrix (NASDAQ:CTXS) est l'entreprise de référence dans le domaine de la virtualisation, des réseaux et des infrastructures cloud permettant aux individus de travailler et de collaborer différemment. Les solutions cloud de Citrix aident les directions informatiques et les fournisseurs de services à bâtir, gérer et sécuriser des espaces de travail virtuels offrant des applications, postes de travail, données et services de qualité, accessibles à tous, quel que soit l'appareil, le réseau ou la plate-forme cloud. Cette année, Citrix célèbre 25 ans d'innovation qui rend aujourd'huid' l'informatique plus accessible et les employés plus productifs grâce à de nouvelles méthodes de travail. Le chiffre d'affaires annuel de l'entreprise a atteint 2,9 milliards de dollars en 2013. Les produits Citrix sont utilisés dans le monde entier par plus de 330 000 entreprises et plus de 100 millions d'utilisateurs. Pour en savoir plus www.citrix.fr.