

L'outil sécurisé de réunions WebEx^{MC}

présenté par



I N T E R C A L L®
GLOBAL CONFERENCING SOLUTIONS

InterCall^{MD}, une filiale de la société West Corporation, en partenariat avec WebEx Communications, Inc., offre des services de conférences Web. Puisque ces services sont animés par WebEx^{MC}, le présent document fait mention du nom, de la plate-forme et des caractéristiques de cette société.

Table des matières

Introduction	3
L'infrastructure sous-jacente	5
L'outil sécurisé de réunions WebEx	7
Accréditation par des tiers.....	11
Conclusion.....	13

Introduction

WebEx^{MC} Communications, Inc. offre des services de collaboration en temps réel à un nombre croissant d'entreprises. Ces dernières ont recours aux applications de **WebEx** à diverses fins, notamment la vente et le marketing, la formation, la gestion de projets et le soutien. **Les clients de WebEx** œuvrent dans toute une variété de secteurs dont la technologie, la finance, la fabrication et les soins de santé. **WebEx** fait de la sécurité des données sa plus grande priorité dans la conception, le déploiement et l'entretien de son réseau, de sa plate-forme et de ses applications, et ses produits satisfont aux exigences de sécurité les plus strictes des entreprises et des organismes gouvernementaux afin qu'ils puissent utiliser couramment et efficacement les services de **WebEx**, tout en ayant la certitude que leurs réunions sont sûres et confidentielles.

Le présent document a pour objet de fournir des renseignements sur les caractéristiques et les fonctions de sécurité des données que comportent les diverses applications **WebEx** et qui sont inhérentes à l'infrastructure de communication sous-jacente de **WebEx** connue sous le nom de **MediaTone^{MC}**. Dans les pages qui suivent, nous examinerons :

WebEx fait de la sécurité des données sa priorité absolue dans la conception, le déploiement et l'entretien de son réseau, de sa plate-forme et de ses applications, et ses produits satisfont aux exigences de sécurité les plus strictes des entreprises et des organismes gouvernementaux.

- **l'infrastructure MediaTone;**
- **l'outil sécurisé de réunions WebEx :**
 - configuration du site,
 - planification d'une réunion,
 - commencer une réunion et se joindre à une réunion,
 - sécurité pendant la réunion,
 - sécurité de la couche transport,
 - compatibilité avec les pare-feu,
 - sécurité après la réunion,
- **l'agrément de sécurité par des tiers.**

On présume que les personnes qui lisent le présent document connaissent bien les fonctions et les services fondamentaux de **WebEx** et comprennent bien le réseau **WebEx MediaTone**. **Voici quelques-unes des applications de réunion et des applications à valeur ajoutée de WebEx :**

- **Meeting Center**, pour une collaboration hautement interactive en équipe;
- **Training Center**, pour offrir une formation efficace sur le Web;
- **Event Center**, pour des séminaires à grande échelle sur le Web;
- **Support Center**, pour des séances de soutien à distance;
- **Sales Center**, pour les réunions de vente en ligne;
- **SMARTtech**, pour créer un réseau géré d'ordinateurs accessibles à distance;
- **GlobalWatch**, pour le contrôle du rendement des réunions.

En outre, **WebEx** offre des services intégrés d'audio conférence, de voix sur IP ainsi que des services de vidéo conférence à un seul point et multi-points.

Les personnes qui lisent le présent document devraient connaître les principaux rôles que proposent les différentes applications, dont ceux d'hôte, de présentateur et de participant :

Hôte

Un hôte organise et amorce les séances **WebEx**. Il dirige également la réunion et, à titre de présentateur initial, il peut accorder des privilèges de présentateur aux participants. Par ailleurs, il amorce la partie audio de la conférence, peut refuser l'accès à la réunion et exclure des participants.

Présentateur

Le présentateur partage des présentations, certaines applications ou le bureau tout entier. Il gère les outils d'annotation et peut accorder et interdire l'accès à distance à des applications communes et au bureau à chacun des participants.

Participant

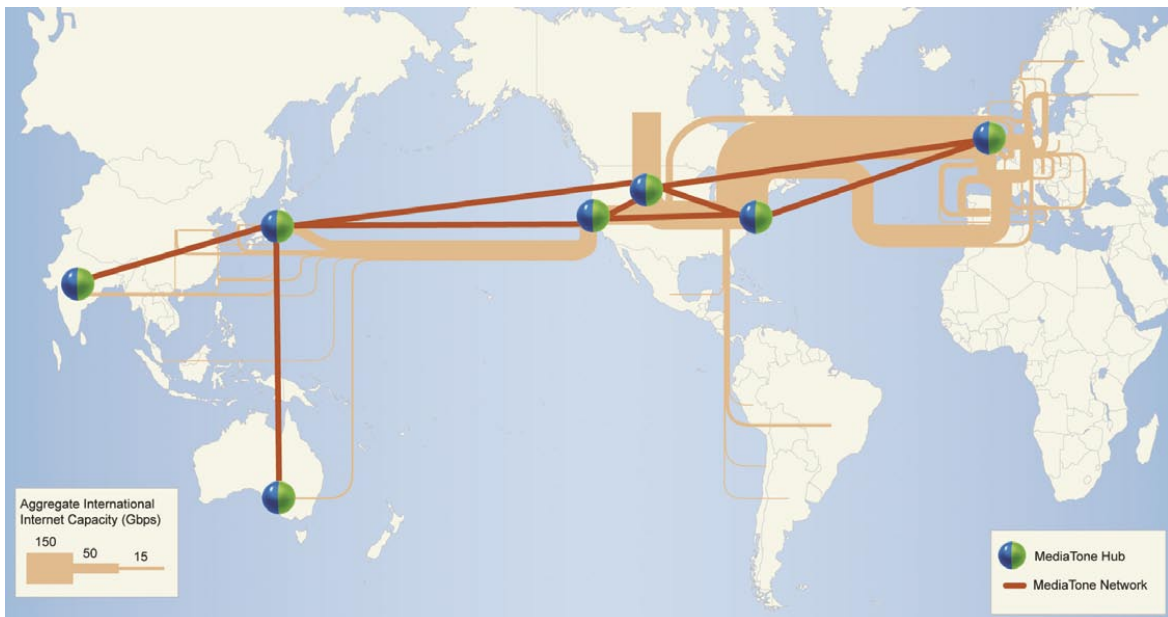
Un participant assume des responsabilités minimales et consulte habituellement le contenu des séances.

À moins d'indication contraire, les sujets abordés dans le présent document s'appliquent également à tous les services et à toutes les applications **WebEx**.

L'infrastructure sous-jacente

Le réseau WebEx MediaTone

Le réseau **WebEx MediaTone** est une infrastructure de communication construite spécialement pour les communications en temps-réel sur Internet. Ce réseau comprend une série de centres de données répartis aux quatre coins du monde et stratégiquement situés à proximité d'importants points d'accès à Internet. **Le trafic de WebEx** est acheminé entre les centres de données de **WebEx** au moyen de fibres optiques spécialisées à large bande.



Architecture commutée

WebEx est la seule société à mettre en place un réseau mondial de commutateurs **MediaTone** haute vitesse. Grâce à cette architecture, les données d'une séance provenant de l'appareil du présentateur et acheminées à celui des participants sont commutées — jamais stockées en permanence — par l'intermédiaire du réseau **WebEx MediaTone**. Cette architecture se distingue des autres solutions de réunions sur le Web qui fonctionnent selon un modèle de stockage et de transmission, avec un serveur qui stocke en permanence des données potentiellement délicates dans le matériel du fournisseur. **Ainsi, les séances WebEx** sont complètement transitoires et fonctionnent selon le même principe qu'une conversation téléphonique sur le réseau public. En plus d'avantages exclusifs sur le plan de la sécurité, cette architecture offre également une infrastructure de réunions extrêmement évolutive et hautement disponible, qui ne souffre pas des limites matérielles inhérentes aux solutions reposant sur un serveur installé chez le client.

Centres de données

Le contenu des séances WebEx est commuté à l'aide du matériel WebEx situé dans les centres de données que WebEx possède et exploite partout dans le monde. Les centres de données de WebEx se trouvent notamment à Mountain View (Californie), à Denver (Colorado), à Reston (Virginie), à Londres (Royaume-Uni) et à Tokyo (Japon). Chaque centre fonctionne jour et nuit, sept jours sur sept. WebEx compte également des nœuds de communication à Melbourne (Australie) et à Bangalore (Inde).

L'accès aux installations est strictement réservé aux personnes recensées sur la liste d'approbation d'accès gérée par l'équipe de sécurité de WebEx, décrite ci-après. Des dispositifs de sécurité biométriques complètent le système de contrôle d'accès.

Le personnel de sécurité de WebEx consacre beaucoup de temps à recevoir de la formation sur tous les aspects de la sécurité organisationnelle auprès des fournisseurs et des spécialistes du secteur afin de demeurer à la fine pointe des tendances en matière de sécurité.

Personnel de sécurité

WebEx a un service consacré exclusivement à la sécurité qui relève directement du directeur principal de l'information de la Société. Cette équipe comprend un analyste légiste accrédité GIAC, deux professionnels agréés de la sécurité des systèmes d'information, un analyste d'intrusions accrédité GIAC et un professionnel de la gestion des systèmes d'information. Le personnel de sécurité de WebEx consacre beaucoup de temps à recevoir de la formation sur tous les aspects de la sécurité organisationnelle auprès des fournisseurs et des spécialistes du secteur afin de demeurer à la fine pointe des tendances en matière de sécurité.

La séparation des responsabilités du personnel de sécurité de celles des autres employés de WebEx est un facteur important qui a permis à WebEx d'obtenir les accréditations WebTrust et SAS-70 de type II (décrites plus loin dans le présent document).

L'outil sécurisé de réunions **WebEx**

L'hôte a accès aux fonctions de sécurité suivantes :

- commencer/planifier les réunions **WebEx**;
- accorder/révoquer des privilèges de présentateur;
- accorder/révoquer des privilèges d'hôte;
- mettre fin à une séance de partage d'application pour tous les participants à la réunion;
- restreindre l'accès à une réunion en cours;
- exclure des participants;
- mettre fin à la réunion;
- activer/désactiver la fonction de discrétion pour les participants à l'aide des fonctions intégrées de téléconférence;
- prendre des notes à l'aide de la fonction intégrée de prise de notes ou accorder ce privilège à un participant et envoyer ces notes à chaque participant avant de conclure la réunion.

Le présentateur a accès aux fonctions de sécurité suivantes :

- consulter la liste des participants à la séance;
- permettre/interdire aux participants de sauvegarder ou d'imprimer des présentations ou des documents partagés pendant la séance;
- permettre/interdire aux participants de changer de page dans une présentation ou un document partagé;
- permettre/interdire aux participants d'annoter le contenu de la séance;
- permettre/interdire aux participants d'envoyer des messages textuels aux autres participants, au présentateur ou aux deux;
- permettre/interdire aux participants d'enregistrer la séance;
- céder temporairement le contrôle d'une application partagée à certains participants;
- suspendre temporairement le partage d'une application ou du bureau pour que les participants ne puissent pas voir le contenu partagé pendant cette période, par exemple lorsque le présentateur désire accéder en toute sécurité et confidentialité à des parties délicates de l'application;
- des fonctions en instance de brevet qui garantissent la confidentialité des échanges (clavardage, prise de notes et gestion des participants) entre l'hôte et le présentateur.

Configuration du site de réunions WebEx

Le module d'administration de site **WebEx** permet aux clients d'appliquer leurs politiques de sécurité à l'ensemble de leur site **WebEx**. Par exemple, la fonction permettant au présentateur de partager son bureau peut être désactivée sur un site particulier. Les autorisations accordées à ce niveau s'appliquent à toutes les séances créées sur ce site. Les autres fonctions de sécurité relatives à la configuration d'administration du site comprennent :

- l'interdiction de répertorier les réunions;
- la saisie obligatoire de l'adresse électronique des participants;
- la saisie obligatoire d'un mot de passe sûr;
- les critères de définition d'un mot de passe sûr par le client;
- les restrictions d'accès au site — l'administrateur du site peut décider que l'authentification est obligatoire pour tous les utilisateurs, tant les hôtes que les participants. Il peut ainsi s'assurer que toute personne accédant au site, que ce soit pour consulter des renseignements (p. ex., la liste des réunions) ou accéder à une réunion sur le site, a préalablement été authentifiée;
- l'approbation obligatoire des demandes de « mot de passe oublié »;
- l'obligation d'attribuer un mot de passe à chaque réunion.

Planification d'une réunion

Outre les paramètres de sécurité définis au niveau du site, un hôte peut préciser les restrictions d'accès en fonction des paramètres suivants :

(Nota : Les hôtes ne peuvent pas annuler les paramètres définis au niveau du site.)

• Réunion répertoriée ou non répertoriée

— Cette option permet aux hôtes d'inscrire ou non leurs réunions au calendrier des réunions de leur site. Les réunions qui ne sont pas inscrites ne figurent jamais au calendrier et ne sont accessibles qu'en suivant le lien inclus dans l'invitation envoyée par courriel ou en saisissant le numéro précis de la réunion sur la page d'accès à la réunion. Dans un cas comme dans l'autre, l'hôte doit explicitement informer les participants de l'existence de la réunion.

• Réunion ouverte ou protégée par mot de passe

— L'hôte peut demander aux participants de saisir un mot de passe avant de se joindre à la réunion et peut également exclure le mot de passe de la réunion des courriels d'invitation.

• Inscription

— Afin de mieux limiter l'accès, l'hôte peut utiliser une « liste de contrôle d'accès » par le biais de la fonction d'inscription, en précisant que seuls les utilisateurs invités à participer à la réunion peuvent s'y joindre, à condition de s'être inscrits et d'avoir été explicitement acceptés par l'hôte.

— Si cette mesure n'est pas déjà activée au niveau du site, l'hôte peut choisir de ne pas envoyer de courriels d'invitation. Cela lui permet de mieux gérer la diffusion des renseignements d'accès à la réunion.

Les clients WebEx peuvent combiner à leur guise les fonctions précédemment décrites pour créer un environnement WebEx adapté à leurs propres politiques de sécurité.

Commencer une réunion et se joindre à une réunion

Les réunions WebEx doivent être ouvertes par un hôte. Celui-ci doit authentifier son identité à l'aide de son identifiant et de son mot de passe pour accéder au site WebEx. Une fois identifié, il peut commencer une réunion WebEx. L'hôte détient le premier niveau de contrôle de la réunion et en est le présentateur initial. À ce titre, il peut à tout moment accorder à l'un ou l'autre des participants des droits d'animateur ou de présentateur et les révoquer. Il peut également mettre fin à la séance à tout moment pour tous les participants ou exclure ceux de son choix.

Le site WebEx peut être configuré de manière à permettre aux participants de se joindre à la réunion avant l'hôte. Avant l'arrivée de l'hôte, les participants ne peuvent pas partager de présentations ni utiliser les autres fonctions du service de réunions, à l'exception de la fonction de clavardage.

Sécurité pendant la réunion

Pendant la réunion, la sécurité est d'abord assurée par l'outil WebEx Meeting Service Manager. Cet outil est conçu pour offrir en temps réel et de manière sécurisée du contenu média riche à chaque participant à une séance WebEx. Tout le contenu qu'un présentateur partage avec les participants au cours d'une séance WebEx n'est qu'une représentation des données originales. Ce contenu est codé et optimisé à des fins de partage au moyen du format UCF (Universal Communications Format), une technologie exclusive à WebEx.

L'outil WebEx Meeting Service Manager :

- ne peut être appelé qu'à partir d'un navigateur Web et ne peut pas être lancé de manière indépendante;
- est numériquement signé par Verisign;
- est le seul moyen possible de participer à une séance WebEx;
- est entièrement dépendant des connexions établies pour chaque séance avec le réseau WebEx MediaTone;
- exécute un processus exclusif qui code toutes les données partagées;

Pour mieux comprendre le format UCF, il est utile de le comparer au format PDF. Ce dernier est une représentation codée et allégée de l'objet original. Le contenu codé ne contient aucun élément original, mais seulement une représentation de ces éléments qui est interprétée par le visualiseur Adobe Acrobat. L'outil WebEx Meeting Service Manager fonctionne de la même manière. Sur l'appareil du présentateur, WebEx Meeting Service Manager crée une représentation codée l'objet original, qu'il envoie aux participants à la séance. Les représentations codées ne contiennent aucun élément de la présentation source et ne peuvent être lues que par l'outil WebEx Meeting Service Manager. Cette méthode unique procure deux avantages importants : une moins grande utilisation de la bande passante, les éléments codés étant souvent de deux à trois fois plus légers que le document source, et une plus grande sécurité, car aucun texte en clair ni contenu original ne sort de l'appareil du présentateur.

Une fois que WebEx Meeting Service Manager a codé le contenu de la présentation sur l'appareil du présentateur, il lui attribue un identifiant connu uniquement de lui et de l'outil Meeting Service Manager de chaque participant. WebEx utilise ce moyen pour empêcher des pirates de reconstituer le contenu des séances. Ces techniques protègent contre la reconstruction des données transmises au cours des séances WebEx.

- crypte tout le contenu des présentations partagées au moyen de la norme de cryptage AES;
- crypte la connexion au réseau **MediaTone** à l'aide de la norme de cryptage SSL 128 bits;
- fournit une identification visuelle de chaque participant à la réunion.

*Chaque séance **WebEx** comporte un ensemble particulier de paramètres générés par le commutateur **MediaTone**. Chaque participant authentifié doit avoir accès à ces paramètres, de même qu'au témoin de séance exclusif pour pouvoir se joindre à une séance **WebEx**.*

Il est impossible de participer à une séance **WebEx** sans ne étroite coordination entre le Meeting Service Manager et le réseau de commutation **MediaTone**. Puisque les données d'une séance **WebEx** sont partagées par l'intermédiaire du Meeting Service Manager, qui doit établir une connexion avec le réseau de commutation **MediaTone**, ces caractéristiques de sécurité s'appliquent pendant toute la durée de la séance. En résumé, chaque séance est dynamique et comprend l'établissement d'une liaison entre le Meeting Service Manager et le commutateur **MediaTone**.

Chaque connexion à **WebEx** Meeting Service Manager doit être authentifiée avant que soit créée la connexion avec le commutateur **MediaTone** pour participer à une séance **WebEx**. Le processus d'authentification fait appel à un témoin unique par client et par séance afin de confirmer l'identité de chaque participant qui tente de se joindre à une séance **WebEx**. Chaque séance **WebEx** comporte un ensemble particulier de paramètres générés par le commutateur **MediaTone**. Chaque participant authentifié doit avoir accès à ces paramètres, de même qu'au témoin de séance exclusif pour pouvoir se joindre à une séance **WebEx**.

Sécurité de la couche transport

Outre tous les dispositifs de sécurité évoqués pour la couche application et pour assurer le maximum de sécurité, **WebEx** crypte par défaut tout le contenu des présentations à l'aide de l'algorithme AES (Advanced Encryption Standard) et offre la possibilité de sécuriser complètement le contenu des séances en cryptant la voie de communication entre l'outil **WebEx** Meeting Service Manager et le commutateur **MediaTone** à l'aide du tunnel de cryptage SSL (Secure Sockets Layer) de 128 bits.

Plutôt que d'utiliser le port 80 du pare-feu (trafic Internet HTTP normal) pour traverser le pare-feu, SSL utilise le port 443 (trafic HTTPS). Cela permet aux clients de restreindre l'accès au port 80 sans incidence sur le trafic **WebEx**.

Enfin, les participants à une réunion **WebEx** se branchent au réseau **WebEx MediaTone** par l'intermédiaire d'une connexion logique; il n'y a pas de connexion de poste à poste entre les appareils locaux. La connexion logique est gérée par **WebEx** Meeting Service Manager et est réservée exclusivement aux communications liées à la séance **WebEx**. Il est par conséquent impossible d'utiliser cette connexion pour toute autre tâche que celles qu'autorise **WebEx** Meeting Service Manager.

Compatibilité avec les pare-feu

WebEx Meeting Service Manager communique avec le commutateur WebEx pour établir une connexion fiable et sécurisée. Au moment de l'instanciation, WebEx Meeting Service Manager détermine le meilleur mode de communication. Durant le processus d'établissement de cette connexion, WebEx Meeting Service Manager tente de se connecter en mode TCP (port 1270) ou HTTP/HTTPS (port 80/443). Le port 1270 est très souvent bloqué par un pare-feu; dans ce cas, WebEx Meeting Service Manager fait passer toutes les communications WebEx dans un tunnel HTTP/HTTPS. Si le site WebEx comprend une connexion SSL, tout le trafic est transporté en HTTPS (port 443). Quelle que soit la connexion établie au moment de l'instanciation, grâce à cette communication entre le Meeting Service Manager et le commutateur WebEx, aucune configuration spéciale des pare-feu n'est nécessaire pour autoriser les séances WebEx.

Les seuls renseignements relatifs à une séance que WebEx conserve sont les EDR (Event Detail Records), qu'il utilise aux fins d'établissement de rapports et de facturation.

Sécurité après la réunion

Une fois la réunion terminée, aucun renseignement sur la séance n'est conservé dans les commutateurs MediaTone ni dans les ordinateurs des participants. Si un hôte choisit d'enregistrer une séance, l'enregistrement sera placé soit sur un appareil client, soit dans la zone sécurisée MyRecordings, qui est distincte de l'environnement de communication partagée WebEx. Ce procédé est comparable à celui des messageries vocales et du téléphone. Les messages vocaux sont stockés en permanence à l'écart du réseau de communication principal, d'où ils proviennent pourtant. Le réseau même ne conserve aucun contenu, qui se trouve uniquement dans les messages enregistrés.

Les seuls renseignements relatifs à une séance que WebEx conserve sont les dossiers contenant les détails de l'événement (EDR). WebEx les utilise aux fins d'établissement de rapports et de facturation. Les EDR sont stockés dans la base de données d'exploitation de WebEx et sont accessibles aux clients depuis leur site WebEx dès qu'ils se sont branchés au moyen de leur identifiant d'hôte. Ils peuvent également être téléchargés depuis le site WebEx ou par l'intermédiaire des interfaces applicatives WebEx.

Accréditation par des tiers

Les seuls renseignements relatifs à une séance que **WebEx** conserve sont les dossiers contenant les détails de l'événement (EDR), qu'il utilise aux fins d'établissement de rapports et de facturation.



Pour obtenir de plus amples renseignements sur **Web Trust**, consulter le site <http://www.webtrust.org>

SAS-70 est le cadre de référence qui permet à **WebEx** de divulguer ses activités et ses processus de contrôle selon un modèle de rapport uniforme.



Pour obtenir de plus amples renseignements sur SAS-70, consulter le site <http://www.sas70.com/>

L'engagement de WebEx

WebEx considère que la confidentialité et la sécurité sont de la plus haute importance pour ses clients et ses partenaires. **C'est pourquoi WebEx** s'engage à :

- consulter des vérificateurs **WebTrust** et SAS-70 spécialement formés et accrédités pour examiner ses politiques et méthodes de sécurité;
- appliquer les normes commerciales les plus élevées en vigueur sur Internet;
- faire vérifier périodiquement son environnement de production afin de s'assurer du respect des normes.

WebTrust

Ernst & Young LLP a remis à **WebEx** le sceau **WebTrust**. **WebTrust** est un sceau de confiance décerné aux entreprises qui respectent en permanence certaines normes établies par l'American Institute of Chartered Public Accountants (AICPA) et l'Institut canadien des comptables agréés (ICCA), qui sont reconnues à l'échelle mondiale.

Le principe de sécurité **WebTrust** définit un objectif global pour la sécurité des données transmises sur Internet et stockées dans des systèmes de commerce électronique. Au cours d'une vérification **WebTrust**, le vérificateur évalue si le principe a été respecté en fonction des critères **WebTrust**. Avalisé par l'AICPA et l'ICCA, **WebTrust** est le seul sceau qui peut garantir aux gens d'affaires qu'ils peuvent faire confiance à une entreprise et lui confier ce qu'ils ont de plus précieux : leurs renseignements privés.

La vérification indépendante est la clé de voûte de **WebTrust**. Contrairement à tout autre sceau prétendant protéger les données privées des consommateurs ou des entreprises, **WebTrust** est le seul sceau administré par un tiers. **WebEx** se soumet chaque année à un processus de renouvellement d'accréditation pour conserver le sceau **WebTrust**.

SAS-70 de type II

Ernst & Young LLP effectue chaque année une vérification SAS 70 de type II et fournit à **WebEx** le rapport correspondant. Le Statement on Auditing Standards (SAS) n° 70 pour les organismes de services est une norme de vérification reconnue à l'échelle internationale élaborée par l'American Institute of Certified Public Accountants (AICPA). La vérification SAS-70 de type II, largement reconnue, atteste que les activités de contrôle de **WebEx** ont été soumises à une vérification approfondie. Le rapport permet à **WebEx** de démontrer qu'elle a recours à des dispositifs de contrôle et de protection appropriés pour manipuler et traiter les données appartenant à ses clients.

La norme SAS-70 est le cadre de référence qui permet à **WebEx** de divulguer ses activités et ses processus de contrôle selon un modèle de rapport uniforme. La vérification SAS-70 de type II et le rapport correspondant attestent qu'un vérificateur indépendant (**Ernst & Young**) examine en permanence les dispositifs de contrôle et de protection dont **WebEx** s'est dotée pour assurer la confidentialité et la sécurité des données de ses clients. Ce rapport SAS-70 de type II peut être communiqué aux équipes de vérification et de sécurité des entreprises clientes en vertu d'un accord de confidentialité.

Remarques sur la conformité à l'HIPAA

WebEx n'est pas une entreprise liée au secteur de la santé et elle n'exerce aucun contrôle sur la sélection du contenu partagé par les utilisateurs pendant les réunions **WebEx**. Cependant, le réseau **WebEx MediaTone** est conçu de telle manière qu'aucun renseignement partagé au cours d'une réunion **WebEx** n'est stocké ou conservé dans les commutateurs **WebEx**. Alliée aux caractéristiques de sécurité décrites ci-dessus, cette architecture permet aux entités régies par l'HIPAA (*Health Insurance Portability and Accountability Act*) de se conformer facilement aux directives réglementaires se rapportant à l'utilisation, à la divulgation et au stockage de renseignements médicaux.

Conclusion

Partout dans le monde, des entreprises et des organismes gouvernementaux utilisent chaque jour les applications et les services de WebEx. Cela ne serait pas possible si WebEx ne veillait pas à intégrer des normes et des principes de sécurité à la conception et à l'exploitation de son infrastructure et de ses services. La sécurité des données demeure la priorité absolue de WebEx, lui permettant d'atteindre son objectif, soit de fournir les services de communication électronique en temps réel les plus efficaces et les plus sûrs.

© 2005 WebEx Communications, Inc. WebEx, WebEx MediaTone et le logo WebEx sont des marques déposées de WebEx Communications, Inc. Tous droits réservés. Toutes les autres marques citées sont la propriété de leurs détenteurs respectifs.

WP-SO-041405