Cisco Secure Access

Protégez vos collaborateurs travaillant de manière hybride grâce à une sécurité agile dans le cloud

Juillet 2023

Sommaire

Travail hybride et modèle SSE

La nouvelle ère du travail hybride nécessite de changer d'approche, et le modèle SSE (Security Service Edge) constitue un facteur clé de la stratégie de toute entreprise en matière de sécurité du travail hybride. Le modèle SSE combine plusieurs fonctions de sécurité dans le cloud pour protéger à la fois les collaborateurs, les sous-traitants et les partenaires, où qu'ils se trouvent, et pour sécuriser les ressources stratégiques. Que les sessions impliquent des applications dans des data centers privés, des sites SaaS, peer-to-peer, IaaS ou Internet, le SSE agit comme un « intermédiaire de sécurité » pour identifier et bloquer plusieurs types d'activités malveillantes. Les utilisateurs finaux bénéficient d'une expérience sécurisée et transparente, où qu'ils soient : au bureau, à la maison ou en déplacement. Les solutions SSE doivent répondre à trois exigences principales : offrir une meilleure expérience aux utilisateurs, réduire la complexité IT et renforcer la sécurité.

Présentation du produit

Cisco Secure Access est une solution SSE de sécurité cloud convergée, basée sur une approche Zero Trust, qui fournit un accès fluide, transparent et sécurisé partout, sur tous les appareils. Cette solution regroupe un ensemble global de modules de base, notamment ZTNA, SWG, CASB et FWaaS. La plateforme va ensuite au-delà de ces fonctionnalités et y ajoute la prévention des pertes de données (DLP) multimode, la sécurité DNS, l'isolation du navigateur à distance (RBI), la fonction de sandboxing et la Threat Intelligence de Talos. Le regroupement de ces fonctionnalités sur une même plateforme cloud permet aux entreprises de résoudre de nombreux problèmes de sécurité. Les utilisateurs peuvent désormais accéder en toute sécurité et en toute transparence à toutes les ressources et applications dont ils ont besoin, quels que soient le protocole, le port ou le niveau de personnalisation.

Cisco Secure Access s'appuie sur des structures de données, une gestion des politiques et des contrôles administratifs communs, ce qui facilite l'interopérabilité avec les autres composants. Par exemple, cette solution fonctionne parfaitement avec d'autres offres Cisco, notamment le SD-WAN, la technologie XDR et la supervision de l'expérience numérique, ainsi qu'avec des technologies tierces : les clients profitent donc de meilleurs résultats.

Secure Access applique des dispositifs de cybersécurité modernes, tout en réduisant considérablement les risques, en simplifiant radicalement la complexité opérationnelle de l'IT et en minimisant les tâches des utilisateurs finaux.

Une meilleure expérience pour les utilisateurs

Cisco Secure Access améliore considérablement l'expérience utilisateur, qui devient plus fluide, élimine les risques de contournement des procédures de sécurité nécessaires et augmente la productivité. La solution utilise un client unifié qui simplifie le processus de connexion des utilisateurs. Ils s'authentifient et accèdent directement à l'application souhaitée. Ils sont automatiquement connectés sur le principe du moindre privilège, avec des politiques de sécurité préconfigurées et des mesures d'application adaptables contrôlées par l'administrateur.

Que les sessions utilisent un accès ZTNA ou VPNaaS au niveau d'applications non standard spécifiques, les utilisateurs n'ont rien à faire de plus. Inutile de répéter les tâches de vérification fastidieuses. Les utilisateurs ne ressentent plus aucune confusion concernant la méthode d'accès requise pour les différentes ressources, la nécessité ou non de lancer un client distinct ni toute autre exigence du processus de connexion. L'accès centralisé à toutes les applications facilite considérablement le processus de connexion des utilisateurs, il en garantit également la sécurité – notamment avec la validation de l'état des utilisateurs et des équipements – et il améliore la productivité.

Un travail facilité pour le département IT

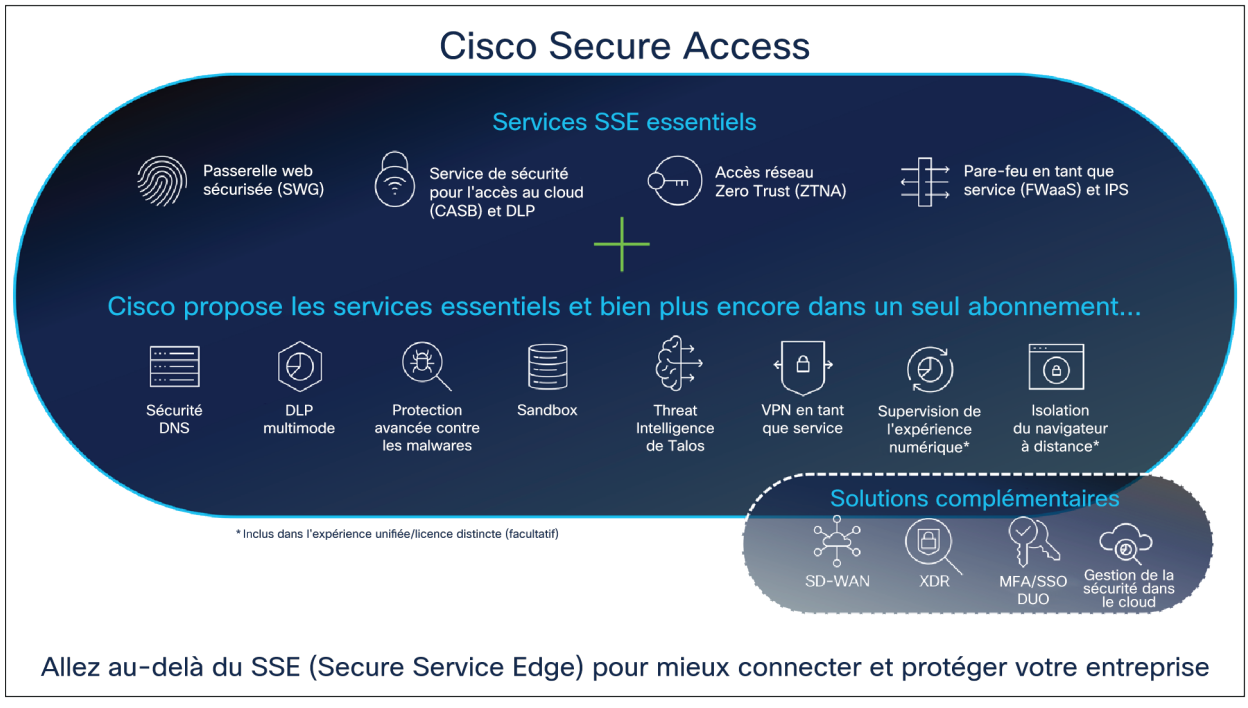
Aujourd'hui, les équipes IT ont du mal à intégrer la multitude d'outils de sécurité à leur disposition. Elles ont besoin de plusieurs consoles de gestion et d'application des politiques, et elles doivent déployer et gérer plusieurs agents logiciels pour chaque équipement de l'utilisateur final. De plus, les rapports, les alertes et les incidents distincts générés par chaque produit de sécurité amplifient le problème.

Cisco Secure Access simplifie et automatise les opérations pour les équipes responsables de la sécurité et de l'IT via une console unique gérée dans le cloud, un client unifié, un processus de création de politiques centralisé et des rapports agrégés. Désormais, au lieu d'avoir à déployer une multitude de produits distincts, le département IT n'a plus qu'à gérer un seul outil. Cela se traduit par un gain mesurable d'efficacité, une réduction des coûts et un environnement IT plus flexible contribuant à l'agilité de l'entreprise. Le département IT peut désormais détecter et bloquer plus rapidement les menaces, accélérer les enquêtes et réduire les tâches de remédiation, tout en gagnant en visibilité sur l'activité des utilisateurs finaux, avec un nombre de tâches d'agrégation manuelles réduit.

Une solution plus sûre pour tout le monde

Cisco Secure Access offre une sécurité de pointe aux utilisateurs et aux ressources sur site. Les capacités étendues de son approche architecturale de défense en profondeur protègent votre environnement contre un ensemble éclectique de menaces de cybersécurité. Les utilisateurs finaux sont protégés contre les fichiers infectés, les sites web malveillants, mais aussi le phishing et les ransomwares. Les équipes responsables de l'IT et de la sécurité peuvent réduire la surface d'exposition aux attaques, appliquer des contrôles sur le principe du moindre privilège, valider l'intégrité des utilisateurs et des équipements, et éliminer les failles de sécurité dans les environnements distribués.

Les équipes de sécurité peuvent obtenir une visibilité sur les activités non autorisées comme le Shadow IT et l'utilisation d'applications non autorisées, et les bloquer. En masquant les ressources internes et en empêchant les hackers de détecter leur présence, le département IT renforce la sécurité. Toutes ces fonctionnalités s'appuient sur la Threat Intelligence de Cisco Talos, avec sa télémétrie inégalée, ses nombreuses études et son intelligence artificielle avancée, pour identifier et stopper les menaces, et pour accélérer la remédiation. En maîtrisant les risques, les entreprises assurent la continuité des activités et évitent tout impact potentiel sur leur réputation ou leurs finances.



Fonctionnalités et bénéfices

Tableau 1. Fonctionnalités et bénéfices

Fonctionnalité	Bénéfice
Accès réseau Zero Trust (ZTNA)	Offrez un accès granulaire propre aux applications privées dans les data centers sur site ou dans les environnements cloud/IaaS. Basée sur des politiques de contrôle d'accès définies, cette fonctionnalité utilise le principe du moindre privilège et des informations contextuelles pour refuser l'accès par défaut de manière granulaire, et pour faciliter l'accès des utilisateurs aux applications lorsque des droits leur sont explicitement accordés, peu importe où ils se trouvent. • Deux méthodes d'accès : accès basé sur le client et accès par navigateur sans client, politique d'accès granulaire basée sur les utilisateurs et les applications, authentification SAML, fournisseur d'identités intégré et contrôle d'accès contextuel • L'accès basé sur le client s'appuie sur le client unifié Cisco Secure • Établit un accès sécurisé après une vérification de l'intégrité du périphérique • Authentifie les utilisateurs via un tunnel sécurisé et chiffré, qui ne leur permet que de voir les applications et les services auxquels ils sont autorisés à accéder • Le proxy d'application permet un accès à distance transparent et sécurisé sans exposer les applications à Internet Il masque même les informations réseau des applications privées pour les clients qui accèdent à ces applications Cela empêche les hackers d'apprendre quoi que ce soit de la reconnaissance IP, même s'ils ont compromis un périphérique client • Empêche les déplacements latéraux des hackers • Permet de mettre en œuvre des politiques de contrôle d'accès propres à l'emplacement et aux périphériques pour empêcher les appareils potentiellement compromis de se connecter à ses services • Les administrateurs attribuent des privilèges d'accès aux sous-traitants et aux employés uniquement sur les ressources dont ils ont besoin, sans aucune possibilité de déplacement latéral • Les administrateurs peuvent configurer des profils d'intégrité pour le type et la version du système d'exploitation des terminaux, le type et la version du navigateur, et les informations de géolocalisation à utiliser dans la décision d'accès • Fournit à l'utilisateur des informations utiles expliquant pourquoi l'accès lui a été refusé
VPNaaS	Toutes les applications privées ne peuvent pas bénéficier d'un accès ZTNA. L'option cloud VPNaaS est incluse pour un accès à distance sécurisé ainsi qu'un accès Internet protégé pour le trafic Internet non web. • Exemples de fonctionnalités : prise en charge de divers cas d'usage (tunnellisation fractionnée, passage de tout le trafic dans le tunnel, communication peer-to-peer, détection des réseaux de confiance, certificat BYO, DNS fractionné, DNS fractionné dynamique) ; plusieurs méthodes d'authentification (SAML, certificat, Radius, LDAP) ; convivial pour l'utilisateur (toujours sur le VPN, démarrage avant l'ouverture de session) ; simplification des opérations IT (pool d'adresses IP locales, plusieurs profils VPN) • Les utilisateurs distants peuvent accéder aux applications privées via la fabric Security Access à partir du client Cisco Secure • Le contrôle d'accès basé sur l'identité est disponible avec l'authentification SAML via le fournisseur d'identités du client • L'intégrité des terminaux est également évaluée. Cela permet d'appliquer un contrôle d'accès granulaire aux ressources privées

Fonctionnalité	Bénéfice
Passerelle web sécurisée (proxy complet)	Enregistrez et inspectez tout le trafic web sur les ports 80/443 pour renforcer la transparence, le contrôle et la protection. Utilisez les tunnels IPsec, les fichiers PAC et le chaînage des proxys en vue de transférer le trafic pour une visibilité totale, des contrôles au niveau des URL ou des applications ainsi qu'une protection avancée contre les menaces. • Le filtrage du contenu par catégories ou par URL permet de bloquer les destinations qui enfreignent les politiques ou les réglementations en matière de conformité • Analysez tous les fichiers téléchargés pour détecter les programmes malveillants et autres menaces • La fonction de sandboxing de Cisco Secure Malware Analytics analyse les fichiers inconnus (voir la section dédiée à Cisco Secure Malware Analytics) • Blocage de types de fichiers (par exemple, blocage du téléchargement des fichiers .exe) • Le déchiffrement SSL systématique ou sélectif permet de vous protéger contre les attaques dissimulées et les infections chronophages • Le contrôle granulaire des applications permet de bloquer des activités spécifiques des utilisateurs dans certaines applications (par exemple, les chargements de fichiers vers Dropbox, les pièces jointes dans Gmail et les publications ou partages sur Facebook) • Des rapports détaillés précisant les adresses URL complètes, l'identité du réseau, l'autorisation ou le blocage des actions, ainsi que l'adresse IP externe
Service de sécurité pour l'accès au cloud (CASB)	Détectez et signalez les applications cloud en cours d'utilisation pour lever le voile sur le Shadow IT. Gérez l'adoption des technologies cloud, réduisez les risques et bloquez l'utilisation d'applications cloud non productives, risquées ou inappropriées. • Prévention des pertes de données (DLP) pour empêcher l'exfiltration de données sensibles de quitter l'entreprise et de se retrouver dans le cloud (voir la section DLP distincte) • Rapports indiquant la catégorie du fournisseur, le nom de l'application et le volume d'activités pour chaque élément détecté • Détails de l'application et informations sur les risques, telles que le score de réputation web, la viabilité financière et les certifications de conformité associées • Détection cloud des programmes malveillants pour les supprimer des applications de stockage de fichiers dans le cloud et s'assurer que les données contenues dans les applications restent exemptes de programmes malveillants. • Possibilité de bloquer ou d'autoriser certaines applications cloud • Restrictions sur les détenteurs pour contrôler les instances d'applications SaaS auxquelles tous les utilisateurs ou des groupes/individus spécifiques peuvent accéder
Prévention des pertes de données (DLP)	Prévention des pertes de données multimode. Analysez les données sensibles en ligne pour offrir une visibilité et un contrôle sur celles qui émanent de votre entreprise. Fonctionnalité DLP basée sur les API pour l'analyse hors bande des données au repos dans le cloud. Inclut des politiques et des rapports unifiés. • Plus de 190 classificateurs de contenu intégrés, notamment RGPD, PCI-DSS, HIPAA, PII et PHI • Classificateurs de contenu intégrés personnalisables avec paramètres de seuil et de proximité pour ajuster et réduire les faux-positifs • Dictionnaires définis par l'utilisateur avec des expressions personnalisées (comme les noms de code de projet) • Détection et création de rapports sur l'utilisation des données sensibles, et rapports détaillés pour identifier les utilisations abusives • Inspection du contenu du trafic web et des applications cloud, et application des politiques relatives aux données

Fonctionnalité	Bénéfice
Pare-feu en tant que service (FWaaS)	Offre une visibilité et un contrôle sur le trafic non web provenant de requêtes Internet, sur tous les ports et protocoles. Inclut les applications mobiles, le partage de fichiers peer-to-peer, la collaboration (par exemple, Webex ou ZOOM), O365 ou tout trafic non web ou non DNS. • Déploiement, gestion et reporting via le tableau de bord unique et unifié Security Access • Politiques personnalisables (IP, port, protocole, application et IPS) • Pare-feu de couche 3/4 pour consigner toutes les activités et bloquer le trafic indésirable à l'aide de règle d'adresse IP, de port et de protocole • Ressources de calcul cloud évolutives qui éliminent les problèmes de capacité des appliances • Visibilité et contrôle des applications de couche 7 pour identifier une base croissante de plus de 2 800 applications non web et les bloquer ou les autoriser de manière sélective • Déchiffrement du trafic avant l'inspection
Système de prévention des intrusions (IPS)	Le système de prévention des intrusions examine les flux de trafic réseau et prévient l'exploitation des vulnérabilités en ajoutant une couche de prévention des menaces, fondée sur la technologie SNORT 3 et la détection basée sur les signatures. • Dans un tableau de bord unifié, créez des politiques pour examiner le trafic et prendre des mesures automatisées afin d'intercepter et de supprimer les paquets dangereux avant qu'ils n'atteignent le réseau • Protection au niveau du trafic Internet et du trafic privé • Configuration des options et des politiques d'accès pour différents profils personnalisés en fonction de la destination du trafic • Base étendue et grandissante de plus de 40 000 signatures de Cisco Talos • Signatures disponibles dans des modèles prédéfinis et personnalisables • Détection et blocage de l'exploitation des vulnérabilités
Cisco Secure Malware Analytics	Combine des fonctions avancées de sandboxing avec la Threat Intelligence pour fournir une solution unifiée qui protège les entreprises contre les programmes malveillants. Fournit un accès à l'intégralité de la console Secure Malware Analytics, permettant l'exécution de fichiers malveillants dans un glovebox, le suivi des actions d'exécution et la capture de l'activité réseau générée par le fichier. Avec Investigate en plus, les analystes peuvent aller plus loin et découvrir les domaines, les adresses IP et les ASN malveillants associés aux actions d'un fichier afin d'obtenir une vue complète de l'infrastructure, des tactiques et des techniques des hackers. • Possibilité de détecter les méthodes d'attaque cachées et de signaler les fichiers malveillants • Source unique d'informations corrélées pour accélérer la recherche des menaces et la réponse aux incidents • API à intégrer avec la technologie XDR et les systèmes SIEM couramment utilisés pour enrichir les données de sécurité • Notification rétrospective en cas de modification de la disposition du fichier (correcte à l'origine, jugée malveillante par la suite)

Fonctionnalité	Bénéfice
Isolation du navigateur à distance (RBI)	L'isolation du navigateur à distance protège les utilisateurs et les entreprises contre les menaces basées sur les navigateurs. Elle déplace l'exécution de l'activité de navigation de l'utilisateur vers une instance de navigateur virtualisée à distance basée dans le cloud pour se protéger contre les menaces Internet. Le code du site web est exécuté séparément et seul un flux visuel sécurisé arrive jusqu'à l'utilisateur. Ceci est totalement transparent pour l'utilisateur final. Pas besoin de se préoccuper des programmes malveillants qui n'ont pas encore été détectés. • Isolation du trafic web entre les périphériques de l'utilisateur et les menaces s'appuyant sur le navigateur • Protection contre les menaces zero-day • Contrôles granulaires pour différents profils de risque • Déploiement rapide sans modification de la configuration du navigateur existante • Évolutivité à la demande pour protéger facilement les utilisateurs supplémentaires • Protection des collaborateurs qui ont besoin d'accéder à des sites Internet présentant des risques connus. La productivité n'est pas réduite par les blocages et les utilisateurs sont protégés
Sécurisation de la couche DNS	Applique le filtrage au niveau de la couche DNS pour bloquer les requêtes vers des destinations malveillantes et indésirables avant qu'une connexion ne soit établie. Bloque les menaces sur n'importe quel port ou protocole avant qu'elles n'atteignent le réseau et les terminaux. • Protège l'accès Internet de tous les périphériques de votre réseau, sur tous vos sites ainsi que pour tous les utilisateurs itinérants • Fournit des rapports détaillés sur l'activité DNS par type de menace ou de contenu web, et l'action appliquée • Conserve les journaux de toutes les activités • Accélère le déploiement sur des milliers de sites et pour des milliers d'utilisateurs pour une protection immédiate
Threat Intelligence de Talos	Talos, l'un des fournisseurs mondiaux majeurs d'études sur la sécurité, analyse quotidiennement des centaines de milliards de requêtes DNS et d'autres données télémétriques. Il exécute en permanence des modèles d'intelligence artificielle, statistiques et d'apprentissage automatique dans cette immense base de données pour fournir des informations sur les cybermenaces et améliorer les taux de réponse aux incidents. • Détecter les domaines, adresses IP, URL et programmes malveillants avant même qu'ils soient utilisés dans le cadre d'une attaque • Hiérarchiser l'analyse des incidents • Accélérer les recherches et les ripostes en cas d'incident • Anticiper l'origine des futures attaques en identifiant et en cartographiant les infrastructures des hackers

Fonctionnalité	Bénéfice
Détection des programmes malveillants	Détecte et supprime les programmes malveillants des applications de stockage de fichiers dans le cloud. Renforce la protection en détectant et en supprimant les fichiers malveillants avant qu'ils n'atteignent un terminal. • Améliore l'efficacité des administrateurs de la sécurité : une fois activés, tous les fichiers des services cloud sont hachés et envoyés automatiquement pour être analysés et rechercher la présence de programmes malveillants. Tout fichier contenant un programme malveillant est signalé afin qu'un administrateur puisse remédier au problème, notamment par une mise en quarantaine et/ou la suppression dudit fichier • Prend en charge Box, Dropbox, Webex et Microsoft 365
Une seule console de gestion et de création de rapports	Création de politiques de sécurité unifiées, notamment des règles basées sur l'intention. Gestion d'Internet, des applications SaaS publiques et de l'accès aux applications privées. Fournit une journalisation complète et la possibilité d'exporter les journaux vers le SOC de l'entreprise, etc. • Permet de définir la politique pour tous les utilisateurs et toutes les applications de manière centralisée. Simplifie le processus de création des politiques de sécurité et favorise la cohérence dans la définition des politiques pour l'ensemble de l'entreprise • Avec des sources (utilisateurs, périphériques) et des ressources (applications, destination) unifiées, la politique de sécurité suit les utilisateurs, quels que soient le point de liaison et l'application à laquelle ils accèdent • Réduit les activités en cours de gestion des politiques • Améliore la visibilité et le délai de détection grâce à des rapports agrégés • Simplifie le processus global d'enquête des analystes du SOC/responsables de la sécurité
Connecteurs d'applications	Les connecteurs d'applications simplifient les tâches administratives relatives à la configuration d'une connectivité sécurisée au niveau des applications privées. Ils connectent Cisco Secure Access aux data centers des clients. • Réduisez la dépendance de l'équipe SSE vis-à-vis des équipes réseau pour les modifications au niveau des périphériques et des règles de pare-feu • Évitez les complexités, telles que la configuration du routage dynamique ou le chevauchement des sous-réseaux • Dans des scénarios tels qu'une fusion, les réseaux sont souvent séparés avec des adresses IP qui se chevauchent, etc. L'utilisation de tunnels devient alors complexe. Les connecteurs d'applications peuvent agir comme un bouclier contre cette complexité • Protégez les applications privées en masquant leur emplacement (adresse IP) et en autorisant uniquement les connexions via des politiques Zero Trust dans Security Access

Options des offres

Cisco Secure Access est une solution SSE complète. Elle est disponible dans un seul abonnement pour améliorer la sécurité et la productivité. Il est proposé dans des offres qui permettent aux clients de choisir facilement le niveau de protection et de couverture adapté aux besoins de leur entreprise. Il existe actuellement deux offres : Cisco Secure Access Essentials et Cisco Secure Access Advantage.

Tableau 2. Offre de base

Catégorie	Fonctionnalités	Secure Access Essentials	Secure Access Advantage
Secure Access	Accès Internet sécurisé • Sécurité pour l'itinérance • Intégration du SD-WAN pour l'accès direct à Internet • VPNaaS	✓	✓
	Accès privé sécurisé • Accès ZTNA basé sur le client • Accès ZTNA sans client • VPNaaS	✓	✓
Sécurité de base	Pare-feu cloud pour le contrôle de couches 3 et 4 des applications web et privées	✓	✓
	Passerelle web sécurisée (trafic web proxy, filtrage des URL, filtrage du contenu, contrôles avancés des applications)	✓	✓
	Service de sécurité pour l'accès au cloud (CASB) : détection des applications cloud, évaluation des risques, blocage, détection des programmes malveillants dans le cloud ; contrôles des détenteurs	✓	✓
	Isolation du navigateur à distance (risqué*)	✓	✓
	Secure Malware Analytics (sandbox)	Limité	Illimité
Sécurité avancée	Pare-feu cloud de couche 7		✓
	Protection IPS		✓
	Prévention des pertes de données (DLP) pour les applications web		✓
	Isolation du navigateur à distance (tous**)		✓
Assistance	Accès amélioré à l'assistance Cisco 24 h/24, 7 j/7 par e-mail et par téléphone	✓	✓

* Risqué : isole les sites web non catégorisés et les catégories de sécurité (y compris potentiellement dangereux)

** Tous : isole les destinations choisies, y compris les catégories de contenu et de sécurité, les listes de destinations, les applications, les éléments non catégorisés, etc.

En savoir plus

Pour en savoir plus, rendez-vous sur : Cisco Secure Access.

Siège social aux États-Unis
Cisco Systems, Inc.
San José. CA

Siège social en Asie-Pacifique
Cisco Systems (États-Unis) 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 de fax sont répertoriés sur le site web de Cisco, à l'adresse : **www.cisco.com/go/offices**.

Imprimé aux États-Unis C78-3777960-00 07/23