Cisco Secure Access

Protégez votre main-d’œuvre hybride grâce à une sécurité agile en nuage

Juillet 2023

Table des matières

Protégez votre main-d'œuvre hybride grâce à une sécurité agile en nuage

Travail hybride et service de sécurité en périphérie

La nouvelle ère du travail hybride nécessite une approche révisée de la sécurité, et le service de sécurité en périphérie (SSE) est un outil clé de la stratégie de travail hybride de toute entreprise. Le SSE combine plusieurs fonctions de sécurité dans le nuage pour protéger les employés, les sous-traitants ou les partenaires qui travaillent de n'importe quel endroit et pour protéger les ressources essentielles. Que les sessions comprennent des applications dans des centres de données privés, des emplacements de logiciel-service, du poste à poste, de l'infrastructure ou Internet, le SSE agit comme « intermédiaire de sécurité » pour déceler et prévenir plusieurs types d'activités malveillantes. Les utilisateurs finaux sont assurés d'une expérience utilisateur sécurisée et transparente, peu importe où ils travaillent : au bureau, à la maison ou sur la route. Les solutions de SSE doivent répondre à trois exigences principales : offrir une expérience utilisateur supérieure, réduire la complexité des TI et améliorer l'efficacité de la sécurité.

Présentation du produit

Cisco Secure Access est une solution de sécurité en nuage convergée, fondée sur le principe de vérification systématique, qui offre un accès fluide, transparent et sécurisé de n'importe quoi à n'importe où. Cette solution ouvre la voie à un ensemble global de modules de base, notamment ZTNA, SWG, CASB et FWaaS. La plateforme va au-delà de ces fonctionnalités et ajoute la DLP multimode, la sécurité DNS, l'isolement de navigateur distant (RBI), la fonction de bac à sable et les informations sur les menaces de Talos. En tirant parti de ces capacités, le tout sur une seule plateforme en nuage, les entreprises peuvent résoudre divers problèmes de sécurité. Les utilisateurs peuvent désormais accéder de manière sécurisée et transparente à toutes les ressources et applications dont ils ont besoin, peu importe le protocole, le port ou le niveau de personnalisation.

Cisco Secure Access offre des contrôles d'administration, des structures de données et une gestion des politiques communs qui facilitent l'interopérabilité avec d'autres composants synergétiques. Par exemple, cette solution fonctionne parfaitement avec d'autres offres de Cisco, notamment le SD-WAN, la XDR et la supervision de l'expérience numérique, ainsi qu'avec les technologies tierces pour améliorer les résultats pour les clients.

Cisco Secure Access met en application des mesures de cybersécurité modernes, tout en réduisant foncièrement les risques, en simplifiant dramatiquement la complexité opérationnelle des TI et en réduisant au minimum les tâches effectuées par les utilisateurs finaux.

Meilleur pour les utilisateurs

Cisco Secure Access améliore radicalement l'expérience de l'utilisateur afin d'éliminer les frictions, contre le contournement potentiel des procédures de sécurité nécessaires et augmente la productivité. La solution utilise un client unifié qui simplifie la façon dont les utilisateurs se connectent; ils s'authentifient et accèdent directement à

l'application souhaitée. Une telle fonction « tout accès » les connecte automatiquement aux concepts de moindre privilège, aux politiques de sécurité préconfigurées et aux mesures d'application de la loi adaptables que l'administrateur contrôle.

Que les sessions utilisent la ZTNA ou le VPNaaS pour des applications hors norme précises, les utilisateurs n'ont pas besoin de prendre des mesures supplémentaires. Cela permet d'éviter de répéter encore et encore les fastidieuses tâches de vérification. La confusion chez les utilisateurs quant à la méthode d'accès requise pour les différentes ressources, le lancement d'un client distinct ou la spécification d'un processus de connexion différent est éliminée. L'accès centralisé à toutes les applications facilite grandement le processus de connexion des utilisateurs, garantit la sécurité, y compris la validation de la posture de l'utilisateur et de l'appareil, et améliore la productivité.

Plus simple pour les TI

Les équipes des TI actuelles ont du mal à intégrer une multitude d'outils de sécurité, ont besoin de plusieurs consoles de gestion et moteurs de stratégie, et doivent déployer et gérer de nombreux agents logiciels pour chaque appareil de l'utilisateur final. Ces défis sont amplifiés par la production de rapports, les alertes et les incidents distincts qui découlent de chaque produit de sécurité.

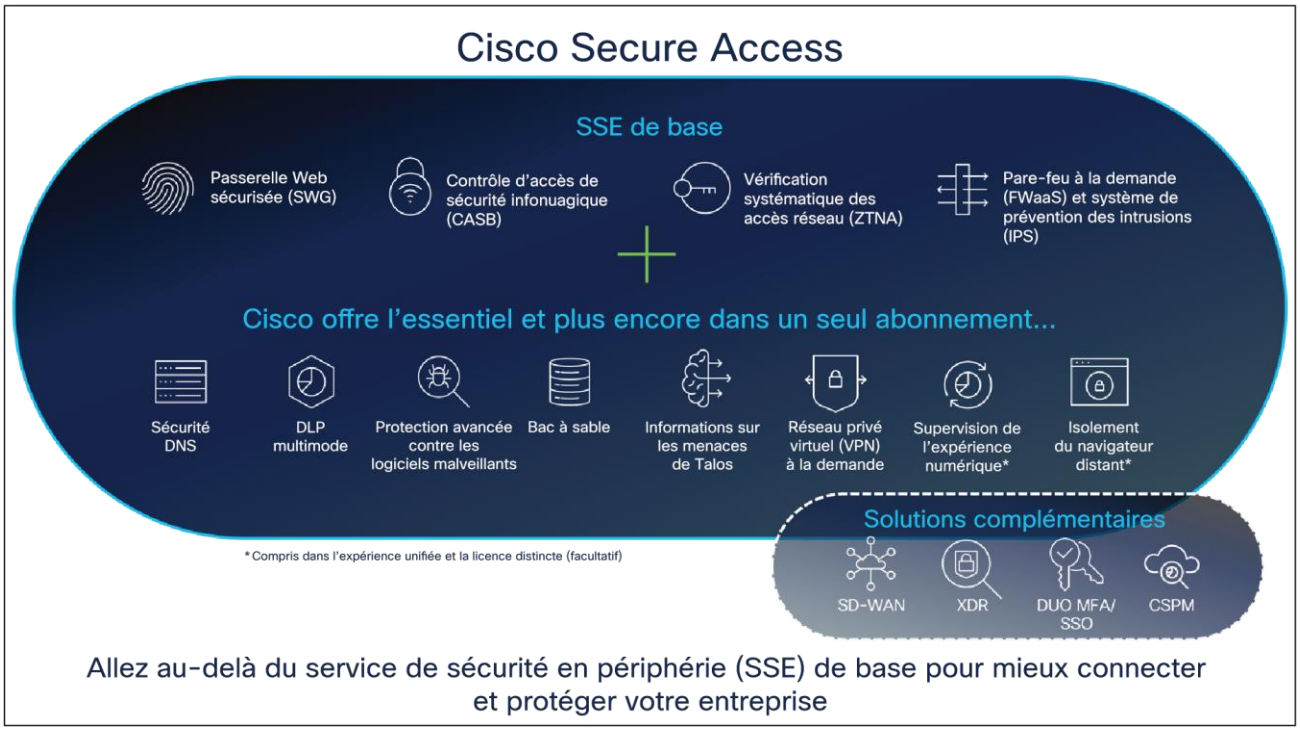
Cisco Secure Access simplifie et automatise les opérations pour les équipes de sécurité et des TI au moyen d'une console unique gérée dans le nuage, d'un client unifié, d'un processus centralisé de création de politiques et de rapports agrégés. Maintenant, au lieu de déployer de nombreux produits disparates, les TI ont seulement à gérer un outil. Cela se traduit par des gains d'efficacité mesurables, entraînant des réductions de coûts et un environnement informatique flexible qui prend en charge une agilité d'entreprise améliorée. Les services des TI peuvent désormais détecter et bloquer plus rapidement les menaces, accélérer les enquêtes et réduire au minimum les tâches de correction, tout en améliorant la visibilité sur les activités des utilisateurs finaux avec moins de tâches d'agrégation manuelles.

Plus sécuritaire pour tout le monde

Cisco Secure Access offre une efficacité de pointe en matière de sécurité, tant pour les utilisateurs finaux que pour les ressources sur site. Les capacités étendues de son approche architecturale de défense en profondeur protègent contre un ensemble diversifié de menaces à la cybersécurité. Les utilisateurs finaux sont protégés contre les risques tels que les fichiers infectés, les sites Web malveillants ainsi que l'hameçonnage et les rançongiciels. Les équipes des TI et de sécurité peuvent réduire la surface d'attaque, appliquer des contrôles de moindre privilège, activer la validation de la posture et éliminer les failles de sécurité dans les environnements distribués.

Les équipes de sécurité peuvent obtenir de la visibilité sur les opérations informatiques de l'ombre et l'utilisation des applications non autorisées, et bloquer de telles activités. En masquant les ressources internes et en empêchant les pirates de découvrir leur présence, le service des TI offre une couche de sécurité supplémentaire. Toutes ces fonctionnalités sont soutenues par les informations sur les menaces de Cisco Talos avec sa télémétrie inégalée, ses recherches approfondies et son intelligence artificielle avancée pour repérer et prévenir les menaces, et accélérer les mesures correctives. En maîtrisant les risques, les organisations maintiennent la continuité des activités et évitent les répercussions financières et sur la réputation d'une violation.

Cisco Secure Access



Fonctionnalités et avantages

Tableau 1. Fonctionnalités et avantages

Fonctionnalité	Avantage
Vérification systématique des accès réseau (ZTNA)	Fournissez un accès granulaire et propre aux applications privées dans les centres de données sur site ou dans des environnements en nuage ou d'infrastructure-service. Fondée sur des stratégies de contrôle d'accès définies, elle utilise les principes du moindre privilège et des analyses contextuelles pour refuser l'accès par défaut de manière granulaire, et négocie l'accès des utilisateurs aux applications lorsqu'il est explicitement accordé, quel que soit l'emplacement. • Deux méthodes d'accès : accès fondé sur le client et fondé sur un navigateur sans client, politique d'accès granulaire fondée sur l'utilisateur et l'application, authentification SAML, fournisseur d'identité (IdP) intégré et contrôle d'accès contextuel. • L'accès fondé sur le client tire parti de la solution Cisco Secure Client unifiée. • Établit un accès sécurisé après une vérification de la posture d'appareil. • Authentifie les utilisateurs au moyen d'un tunnel chiffré sécurisé, leur permettant de voir uniquement les applications et les services auxquels ils ont l'autorisation d'accéder. • Le mandataire d'application fournit un accès à distance transparent et sécurisé sans exposer les applications à Internet. Il masque même les détails du réseau des applications privées pour les clients qui y accèdent. Cela empêche les agresseurs d'apprendre quoi que ce soit de la reconnaissance IP, même s'ils ont compromis un appareil client. • Empêche le mouvement latéral de l'agresseur. • Met en œuvre des stratégies de contrôle d'accès propres à l'emplacement et aux appareils afin d'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 pour les ressources auxquelles ils ont besoin d'accéder, sans aucune

Fonctionnalité	Avantage
	capacité de déplacement latéral. • Les administrateurs peuvent configurer des profils de posture 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 renseignements utiles expliquant la cause du refus d'accès
Réseau privé virtuel à la demande (VPNaaS)	Les applications privées ne peuvent pas toutes être couvertes par la ZTNA. L'option VPNaaS en nuage est incluse pour un accès à distance sécurisé ainsi qu'un accès Internet sécurisé pour le trafic Internet autre que le Web. • Voici quelques exemples de fonctionnalités : prise en charge des scénarios (prise en charge de la tunnellisation fractionnée et de tous les tunnels, communication de poste à poste, détection des réseaux de confiance, certificat d'appareil personnel, DNS fractionné, DNS fractionné dynamique); plusieurs méthodes d'authentification (SAML, certificat, Radius, LDAP); la facilité d'utilisation de l'utilisateur (VPN toujours en fonction, commencer avant la connexion); simplification des opérations informatiques (groupe d'adresses IP locales, nombreux profils de VPN) • Permet aux utilisateurs à distance d'accéder à des applications privées par l'intermédiaire de la trame d'accès de sécurité à l'aide de Cisco Secure Client. • Le contrôle d'accès fondé sur l'identité est disponible au moyen de l'authentification SAML par l'entremise du fournisseur d'identité du client. • La posture du terminal est également évaluée; cela permet un contrôle d'accès granulaire aux ressources privées.

Fonctionnalité	Avantage
Passerelle Web sécurisée (mandataire intégral)	Consignez et inspectez tout le trafic Web sur les ports 80/443 pour plus de transparence, de contrôle et de protection. Les tunnels IPSec, les fichiers PAC et le chaînage des mandataires sont utilisés pour transférer le trafic pour une visibilité complète, des contrôles au niveau des adresses URL et des applications, et une protection avancée contre les menaces. • Filtrage du contenu par catégorie ou adresse URL spécifique pour bloquer les destinations qui enfreignent les politiques ou les règlements de conformité. • Analyse de tous les fichiers téléchargés pour rechercher des programmes malveillants et d'autres menaces. • La fonction de bac de sable avec Cisco Secure Malware Analytics analyse les fichiers inconnus (voir la section dédiée à Cisco Secure Malware Analytics). • Blocage de types de fichiers (p. ex., blocage du téléchargement de fichiers .exe). • Déchiffrement SSL complet ou sélectif pour protéger contre les attaques cachées et les infections chronophages. • Contrôles granulaires des applications pour bloquer des activités d'utilisateur particulières dans certaines applications (p. ex., les téléchargements de fichiers vers Dropbox, les pièces jointes vers Gmail, les publications ou les partages sur Facebook). • Rapports détaillés comprenant les adresses URL complètes, l'identité du réseau, les actions d'autorisation ou de blocage, ainsi que l'adresse IP externe.
Contrôle d'accès de sécurité infonuagique (CASB)	Exposez l'informatique de l'ombre en détectant et en produisant des rapports sur les applications en nuage en cours d'utilisation. Gérez l'adoption du nuage, réduisez les risques et bloquez l'utilisation d'applications en nuage offensantes, non productives, risquées ou inappropriées. • Prévention de la perte de données (DLP) pour empêcher l'exfiltration de données sensibles de l'entreprise et dans le nuage (voir la section distincte sur la prévention des pertes de données). • Rapports sur la catégorie de prestataire, le nom de l'application et le volume d'activité pour chaque application découverte. • Détails de l'application et renseignements sur les risques, comme le niveau de réputation des sites Web, la viabilité financière et les certifications de conformité pertinentes. • Détection de programmes malveillants en nuage pour détecter et supprimer les programmes malveillants des applications de stockage des fichiers en nuage et s'assurer que les applications continuent d'être sans programme malveillant. • Capacité de bloquer ou d'autoriser des applications en nuage précises. • Restrictions relatives aux détenteurs pour contrôler les instances des applications de logiciel-service auxquelles tous les utilisateurs ou certains groupes ou particuliers peuvent accéder.
Prévention de la perte de données (DLP)	Prévention de la perte de données multimode. Analysez les données sensibles en ligne pour offrir une visibilité et un contrôle sur les données sensibles qui quittent votre entreprise. Fonctionnalité de prévention de la perte de données fondée sur l'API pour l'analyse hors bande des données stockées dans le nuage. Comprend des politiques et des rapports unifiés. • Plus de 190 classificateurs de contenu intégrés, y compris le RGPD, PCI-DSS, HIPAA, PII et PHI. • Classificateurs de contenu intégrés personnalisables avec seuil et proximité pour affiner l'analyse et réduire le nombre de faux positifs. • Dictionnaires définis par l'utilisateur avec des phrases personnalisées (comme les noms de code de projet). • Détection et production de rapports sur l'utilisation des données sensibles et rapports détaillés pour aider à détecter les mauvaises utilisations. • Inspection du contenu du trafic Web et des applications en nuage, et mise en application des politiques sur les données.

Fonctionnalité	Avantage
Pare-feu à la demande (FWaaS)	Offre une visibilité et un contrôle du trafic non lié au Web provenant de demandes allant vers Internet, sur l'ensemble des ports et des protocoles. Comprend les applications mobiles, la transmission du fichier de poste à poste, la collaboration (p. ex., Webex ou ZOOM), O365 ou tout trafic non lié au Web ou au DNS. • Déploiement, gestion et production de rapports au moyen du tableau de bord unique et unifié Security Access. • Politiques personnalisables (politiques d'adresse IP, de port, de protocole, d'application et d'IPS). • Pare-feu de couche 3 ou 4 pour consigner toutes les activités et bloquer le trafic indésirable à l'aide de règles d'adresse IP, de port et de protocole. • Les ressources informatiques en nuage évolutives éliminent les problèmes de capacité des appareils. • Visibilité et contrôle des applications de couche 7 pour repérer une base croissante de plus de 2 800 applications non liées au Web et bloquer ou autoriser de manière sélective. • Déchiffre le trafic avant l'inspection.
Système de prévention des intrusions (IPS)	Le système IPS examine le flux de trafic réseau et empêche les exploitations de vulnérabilité grâce à une couche supplémentaire de prévention des menaces fondée sur la technologie SNORT 3 et la détection fondée sur les signatures. • À l'aide d'un tableau de bord unifié, créez des politiques pour examiner le trafic et prenez des mesures automatisées pour détecter et supprimer les paquets dangereux avant qu'ils atteignent le réseau. • Fournit une protection d'IPS pour le trafic Internet et privé. • Configurez les politiques d'accès et les options pour différents profils personnalisés selon la destination du trafic. • Utilisez une base étendue et croissante de plus de 40 000 signatures de Cisco Talos. • Les signatures sont offertes dans des modèles prédéfinis, qui sont personnalisables. • Détection et blocage de l'exploitation des vulnérabilités.
Cisco Secure Malware Analytics	Combine une fonction de bac à sable avancée avec les informations sur les menaces dans une seule solution unifiée pour protéger les entreprises contre les programmes malveillants. Donne accès à l'ensemble de la console Secure Malware Analytics, permettant l'exécution de fichiers malveillants dans une boîte à gants, le suivi des actions d'exécution des fichiers et la capture de l'activité réseau générée par le fichier. Lorsqu'ils sont combinés avec Investigate, les analystes de sécurité peuvent aller plus loin et découvrir des domaines, des adresses IP et des ASN malveillants associés aux actions d'un fichier afin d'obtenir la vue la plus complète possible de l'infrastructure, des tactiques et des techniques d'un agresseur. • Capacité à détecter les méthodes d'attaque cachées et à signaler les fichiers malveillants. • Source unique et corrélée d'informations pour accélérer la recherche de menaces et l'intervention en cas d'incident. • API à intégrer à la XDR et aux SIEM couramment utilisés pour enrichir les données de sécurité. • Notification rétrospective si la disposition du fichier change (bonne à l'origine/plus tard considérée comme malveillante).

Fonctionnalité	Avantage
Isolement du navigateur distant (RBI)	RBI protège les utilisateurs et les organisations contre les menaces fondées sur les navigateurs. Cela déplace l'exécution de l'activité de navigation de l'utilisateur vers une instance de navigateur virtualisée en nuage à distance pour assurer la protection contre les menaces Internet. Le code du site Web est exécuté séparément et seul un flux visuel sécuritaire est fourni à l'utilisateur. Cette opération est entièrement transparente pour l'utilisateur final. Vous n'avez plus à vous soucier des logiciels malveillants qui n'ont pas encore été détectés. • Isolement du trafic Web entre les appareils de l'utilisateur et les menaces fondées sur le navigateur. • Protection contre les menaces du jour zéro. • Contrôles granulaires pour différents profils de risque. • Déploiement rapide sans modification de la configuration existante du navigateur. • Évolutivité à la demande pour protéger facilement des utilisateurs supplémentaires. • Protégez les employés qui peuvent avoir besoin d'accéder à des sites Internet à risque connus. La productivité n'est pas réduite en raison des blocages et les utilisateurs restent en sécurité.
Sécurité de couche DNS	Applique le filtrage au niveau de la couche DNS pour bloquer les demandes vers des destinations malveillantes et indésirables avant qu'une connexion ne soit établie. Bloque les menaces sur n'importe quel port ou protocole, avant même qu'elles atteignent le réseau ou les terminaux. • Protège l'accès Internet sur tous les appareils réseau, les bureaux et les utilisateurs en itinérance. • Fournit des rapports détaillés sur l'activité DNS par type de menace de sécurité ou de contenu Web et les mesures prises. • Conserve des journaux de toutes les activités. • Déploiement accéléré à des milliers d'emplacements et d'utilisateurs pour fournir une protection immédiate.
Informations sur les menaces Talos	Talos, l'un des principaux fournisseurs mondiaux de recherches de pointe sur la sécurité, analyse quotidiennement des centaines de milliards de requêtes DNS et d'autres données télémétriques. Talos exécute en permanence des modèles d'intelligence artificielle, de statistiques et d'apprentissage automatique dans cette base de données massive pour fournir des informations sur les cybermenaces et améliorer les taux d'intervention en cas d'incident. • Découvrez les adresses URL, les adresses IP, les programmes malveillants et les domaines malveillants avant qu'ils ne soient utilisés dans des attaques. • Donnez la priorité aux enquêtes sur les incidents. • Accélérez les enquêtes et les interventions en cas d'incident. • Prévoyez l'origine des futures attaques en localisant et en cartographiant les infrastructures des agresseurs.

Fonctionnalité	Avantage
Détection de programmes malveillants en nuage	Détecte et supprime les programmes malveillants des applications de stockage de fichiers en nuage. Renforce la protection de sécurité en détectant et en corrigeant les fichiers malveillants avant qu'ils n'atteignent un terminal. • Augmente l'efficacité et l'efficience des administrateurs de la sécurité – une fois activée, tous les fichiers des services en nuage sont hachés et envoyés automatiquement pour analyse des programmes malveillants. Tout fichier contenant un programme malveillant sera signalé afin qu'un administrateur de la sécurité puisse y remédier, y compris la mise en quarantaine ou la suppression. • Prend en charge Box, Dropbox, Webex et Microsoft 365.
Console de gestion et de production de rapports unique	La création de politiques de sécurité unifiées, y compris les règles fondées sur les intentions, et la gestion d'Internet, des applications de logiciel-service publiques et de l'accès aux applications privées. Fournit une journalisation complète et la possibilité d'exporter les journaux vers le centre des opérations de sécurité de l'entreprise, etc. • Endroit unique pour définir la politique de tout utilisateur pour n'importe quelle application. Simplifie le processus des politiques de sécurité des bâtiments et favorise la cohérence dans la définition des politiques pour l'ensemble de l'entreprise. • Une source unifiée (utilisateurs, appareils) et des ressources unifiées (applications, destination) permet de s'assurer que la politique de sécurité suit les utilisateurs, peu importe le point d'attache et peu importe l'application à laquelle il accède. • Réduit les activités courantes de gestion des politiques. • Améliore la visibilité et le délai de détection grâce à la production de rapports agrégés. • Simplifie le processus global d'enquête du centre des opérations de sécurité et de l'analyste de sécurité.
Connecteurs d'application	Les connecteurs d'application simplifient les tâches administratives pour la configuration d'une connectivité sécurisée aux applications privées. Ils connectent Cisco Secure Access aux centres de données des clients. • Réduisez la dépendance de l'équipe de SSE aux équipes de réseau pour les modifications des appareils et des règles de pare-feu. • Évitez les complexités de routage, comme la configuration du routage dynamique ou le chevauchement des sous-réseaux. • Dans des scénarios comme une fusion, les réseaux restent souvent séparés et leurs adresses IP se chevauchent, etc. L'utilisation des tunnels devient complexe. Les connecteurs d'applications peuvent contourner cette complexité. • Protège les applications privées en masquant leur emplacement (adresse IP) et en autorisant uniquement les connexions dans le cadre des politiques de vérification systématique dans Security Access.

Choix de forfaits

Cisco Secure Access est la solution de SSE la plus large qui soit. Elle est offerte dans un seul abonnement pour obtenir de meilleurs résultats en matière de sécurité et une productivité accrue. Elle est offerte sous forme de forfaits qui permettent aux clients de choisir facilement le niveau de protection et de couverture qui convient aux besoins de leur organisation. Il existe actuellement deux forfaits : Cisco Secure Access Essentials et Cisco Secure Access Advantage.

Tableau 2. Offre de base

Catégorie	Fonctionnalités	Secure Access Essentials	Secure Access Advantage
Accès sécurisé	Accès sécurisé à Internet • Sécurité d'itinérance • Intégration de l'accès Internet direct (DIA) du réseau étendu défini par logiciel (SD-WAN) • Réseau privé virtuel à la demande (VPNaaS)	✓	✓
	Accès privé sécurisé • Vérification systématique des accès réseau (ZTNA) fondée sur le client • Vérification systématique des accès réseau (ZTNA) sans client • Réseau privé virtuel à la demande (VPNaaS)	✓	✓
Sécurité de base	Pare-feu en nuage pour les contrôles de couche 3 et 4 des applications Web et privées	✓	✓
	Passerelle Web sécurisée (trafic Web de mandataire, filtrage des URL, filtrage du contenu, contrôles avancés des applications)	✓	✓
	CASB – découverte des applications en nuage, évaluation des risques, blocage, détection des programmes malveillants en nuage; contrôles du détenteur	✓	✓
	Isolement du navigateur distant (RBI) (à risque*)	✓	✓
	Secure Malware Analytics (fonction de bac de sable)	Limité	Illimité
Sécurité avancée	Pare-feu fourni en nuage de la couche 7		✓
	Protection de l'IPS		✓
	Prévention de la perte de données (DLP) pour les applications Web		✓
	Isolement du navigateur distant (tout**)		✓
Soutien	Accès au soutien amélioré de Cisco 24 heures sur 24, 7 jours sur 7, par courriel et par téléphone	✓	✓

* À risque : isolez les sites Web non catégorisés et les catégories de sécurité (y compris les sites potentiellement dangereux)

** Tout : isolez toute destination choisie, y compris les catégories de contenu et de sécurité, les listes de destinations, les applications, les applications non catégorisées, etc.

Pour en savoir plus

Pour en savoir plus, consultez la page Cisco Secure Access.

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

Siège social en Asie-Pacifique
Cisco Systems (USA) Pad 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 télécopieur 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