

Cisco Secure Access

Le travail hybride est là pour de bon.

Table des matières

Protéger les utilisateurs et les ressources, peu importe où

Cisco Secure Access est une solution de sécurité infonuagique (SSE) convergente qui est meilleure pour les utilisateurs, plus simple pour les TI et plus sécuritaire pour tout le monde. Elle renforce la cybersécurité moderne tout en offrant une expérience transparente et sans friction, car les utilisateurs se connectent de n'importe où, grâce à une approche d'accès commun.

Secure Access simplifie les opérations des TI au moyen d'une console unique gérée dans le nuage, d'un client unifié, d'une création centralisée de politiques et de rapports agrégés. Des capacités de sécurité étendues convergées en une seule solution (ZTNA, SWG, CASB, FWaaS, sécurité DNS, RBI et autres) réduisent les risques de sécurité en appliquant des principes de vérification systématique et en mettant en œuvre des politiques de sécurité granulaires. Les informations sur les menaces de Talos, chef de file du marché, alimentent un blocage inégalé des menaces afin de réduire les risques et d'accélérer les enquêtes.

Les entreprises de tous types connaissent un changement fondamental dans la manière dont leurs utilisateurs accèdent aux différentes ressources. Les employés, les sous-traitants et les partenaires se trouvent désormais souvent en dehors du périmètre de sécurité de l'entreprise et utilisent de plus en plus d'applications et de bases de données hébergées dans le nuage.

Il en résulte une expérience sous-optimale pour les travailleurs hybrides, une complexité accrue pour les TI et la sécurité, et des lacunes en matière de sécurité. Les utilisateurs finaux sont frustrés par la diversité des méthodes de connexion et la lourdeur des processus de sécurité. Les équipes des TI et de la sécurité sont confrontées à un trop grand nombre d'outils de sécurité et à des portails de gestion disparates. Les cyberattaques sont de plus en plus fréquentes et complexes et ciblent une surface de menace élargie, ce qui accroît les risques pour la sécurité. Pour surmonter ces obstacles, les entreprises adoptent des services de sécurité consolidés basés sur le nuage avec le Service de sécurité en périphérie (SSE).

Avantages

- Offrez à l'utilisateur final un accès unifié, transparent et sécurisé à n'importe quelle application, port ou protocole.
- Simplifiez les opérations des TI au moyen d'une console unique, d'une gestion simplifiée des politiques et de rapports agrégés.
- Réduisez les risques grâce à une protection avancée en matière de cybersécurité, à des principes de vérification systématique et à des politiques de sécurité granulaires.
- Maintenez la continuité des activités et évitent les répercussions financières et sur la réputation d'une violation.
- Permettez un travail sans friction partout.
- Obtenez une visibilité sur l'utilisation des applications en nuage, leurs niveaux de risque et les opérations des TI dans l'ombre.

Une meilleure sécurité infonuagique pour les utilisateurs, plus simple pour les TI et plus sécuritaire pour tout le monde

Cisco Secure Access protège l'accès au Web, aux services en nuage, aux applications de logiciel-service (SaaS) et aux applications privées. Grâce aux principes de moindre privilège, la solution authentifie les utilisateurs de manière dynamique. Elle évalue la position de l'appareil grâce à des renseignements contextuels

afin de garantir la sécurité. Plusieurs couches de sécurité complexes protègent vos utilisateurs et vos ressources contre un large éventail de cyberattaques telles que les menaces malveillantes, l'exfiltration de données, l'hameçonnage, les rançongiciels et les fichiers infectés.

Cisco Secure Access offre une flexibilité inégalée en matière de sécurisation d'accès à toutes les applications privées (et non à certaines d'entre elles). La solution ZTNA, basée ou non sur le client, sécurise de manière transparente l'accès aux applications standard avec l'accès le moins privilégié, à partir d'appareils gérés et non gérés.

Pour les applications où la solution ZTNA n'est pas prise en charge (p. ex. : multipoint, client à client, ports ou protocoles hors normes), Cisco Secure Access offre une capacité de réseau privé virtuel à la demande (VPNaaS) de secours, sans les problèmes typiques de matériel, de gestion et des utilisateurs finaux. Un seul client unificateur est utilisé pour les solutions ZTNA et VPNaaS, ce qui permet à l'utilisateur final de bénéficier d'une expérience simple et unifiée.

Cisco Secure Access intègre tous les modules de sécurité pertinents en une seule solution fournie dans le nuage. Inutile d'assembler plusieurs outils de sécurité. De plus, un tableau de bord unique simplifie la gestion des TI et de la sécurité et réduit les coûts d'administration.

L'efficacité de la sécurité est primordiale. Secure Access est soutenu par Cisco Talos, un des fournisseurs les plus importants et les plus fiables de recherche de pointe en matière de sécurité à l'échelle mondiale. La solide équipe d'experts de Talos, composée de chercheurs et d'experts en science des données à plein temps, de l'apprentissage automatique et de l'intelligence artificielle, voit ce qui se passe dans le paysage des menaces, intervient sur ces données rapidement et de manière significative, et assure la protection.

- Secure Access est proposé en deux formules, avec des décomptes d'utilisateurs privés et sécurisés indépendants, pour une plus grande flexibilité pour les clients.
- Essentials : Le forfait de base comprend un accès Internet sécurisé, un accès privé sécurisé, une passerelle Web sécurisée (SWG), la vérification systématique des accès réseau (ZTNA), un contrôle d'accès de sécurité infonuagique (CASB), un pare-feu de couche 3/4, l'isolation du navigateur à distance (RBI) (limité) et plus
- Avantage : Capacité Essentials plus pare-feu de couche 7, IPS, DLP, RBI (intégral), et plus.

Relever la barre en matière de SSE

Cisco Secure Access va au-delà de l'approche traditionnelle adoptée par d'autres fournisseurs de sécurité. Notre sécurité infonuagique est fournie en tant que service et offre plusieurs avantages décisifs.

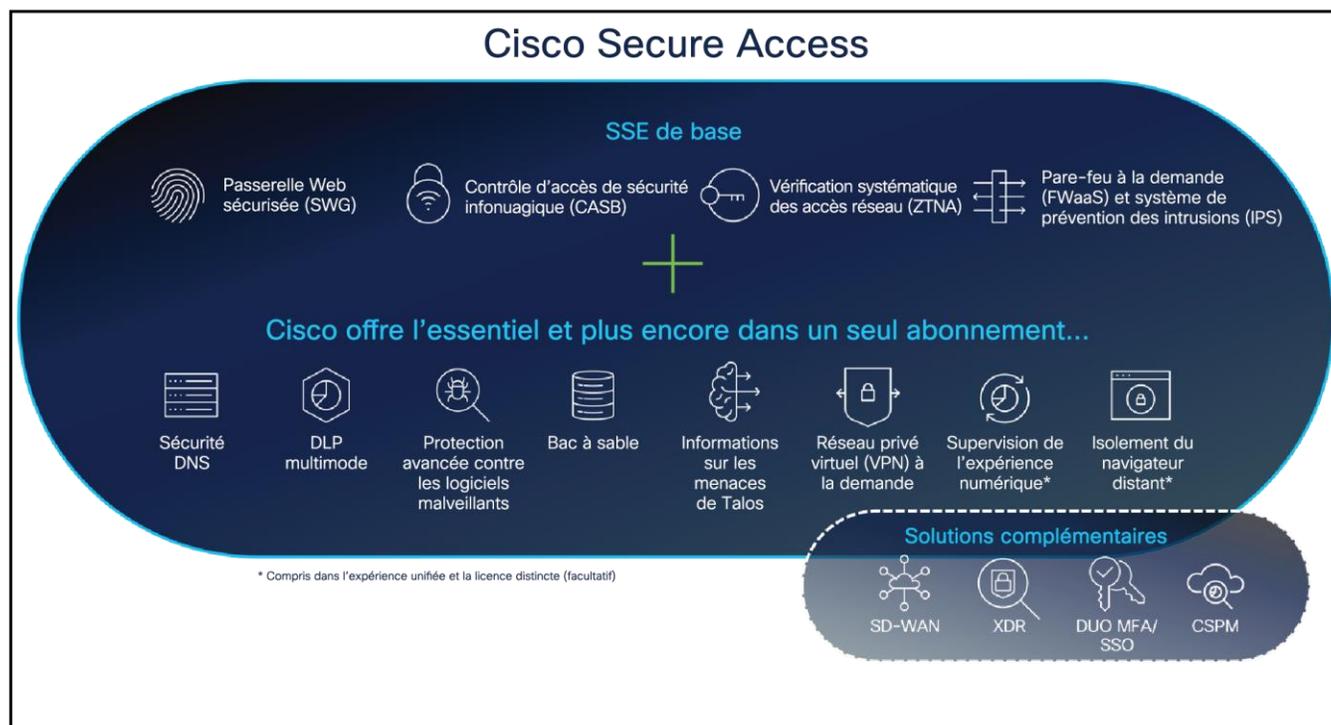
Cisco offre :

- un accès sécurisé à toutes les applications, y compris celles qui impliquent des protocoles hors normes et celles qui sont basées sur des architectures multicanaux et client à client;
- une console de gestion unique et unifiée pour tous les modules de sécurité;
- des capacités de sécurité complète de pointe qui éliminent le besoin d'outils coûteux provenant de plusieurs fournisseurs, assurent la cohérence des ensembles de règles et nécessitent une courbe d'apprentissage minimale;
- une architecture infonuagique résiliente dotée d'une grande évolutivité pour le nombre d'utilisateurs finaux, d'un traitement efficace en un seul passage pour des interventions plus rapides et de délais d'exécution plus courts pour la prise en charge rapide de nouvelles fonctionnalités;

- une répartition automatique de la charge et un rééquilibrage du trafic favorisant un meilleur rendement pour les clients.

Évaluez votre état de préparation en matière de SSE

Répondez à un court questionnaire pour voir où vous en êtes avec l'[outil d'évaluation en ligne](#)



Commencez dès maintenant

En savoir plus sur Cisco Secure Access. Rendez-vous sur le site

<https://www.cisco.com/site/ca/fr/products/security/secure-access/index.html>

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.

Cisco et le logo Cisco sont des marques de commerce ou marques de commerce déposées de Cisco ou de ses filiales aux États-Unis et dans d'autres pays. Pour voir la liste des marques commerciales Cisco, rendez-vous à l'adresse : www.cisco.com/go/trademarks. Les autres marques commerciales mentionnées dans le présent document sont la propriété de leurs détenteurs respectifs. L'utilisation du terme « partenaire » n'implique pas de relation de partenariat entre Cisco et une autre entreprise. (1110R)