

# Cisco Secure Access

Le travail hybride n'est pas prêt de disparaître

---

# Sommaire

Une protection qui vous suit partout	3
Bénéfices	3
Une sécurité cloud plus efficace pour les utilisateurs, plus simple pour les équipes IT et plus sûre pour tous	3
Revoir ses objectifs SSE à la hausse	4
Évaluez votre niveau de préparation à l'approche SSE	5
Contactez-nous dès aujourd'hui	5

---

## Une protection qui vous suit partout

Cisco Secure Access est une solution SSE convergée de sécurité cloud plus intéressante pour les utilisateurs, plus facile à gérer pour les équipes IT et plus sûre pour tout le monde. Elle permet de bénéficier d'une cybersécurité moderne tout en offrant une expérience de connexion simple et fluide aux utilisateurs, quel que soit leur équipement et où qu'ils se trouvent, via une approche d'accès commune.

Secure Access simplifie les opérations IT grâce à une console unique gérée dans le cloud, un client unifié, une création de politiques centralisée et la génération de rapports combinés. Les fonctionnalités de sécurité étendues regroupées dans une même solution (ZTNA, SWG, CASB, FWaaS, sécurité DNS, RBI, etc.) réduisent les risques en appliquant les principes Zero Trust et des politiques de sécurité granulaires. La Threat Intelligence de Talos assure un niveau inégalé de blocage des menaces pour réduire les risques et accélérer les recherches en cas de faille.

Les entreprises de tous types constatent actuellement un changement radical dans la façon dont leurs utilisateurs accèdent aux ressources. De nombreux collaborateurs, prestataires externes et partenaires opèrent désormais en dehors du périmètre de sécurité de l'entreprise, et utilisent un éventail de plus en plus large d'applications et de bases de données hébergées dans le cloud.

Ce phénomène nuit au bon fonctionnement des dispositifs de protection et se traduit par une expérience parfois frustrante pour les collaborateurs travaillant de manière hybride, mais aussi par une complexité accrue du point de vue des équipes IT et des responsables de la sécurité. Les méthodes de connexion hétéroclites et les processus de sécurité fastidieux sont peu appréciés des utilisateurs. Les équipes chargées de l'IT et de la sécurité sont pénalisées quand elles doivent gérer un trop grand nombre d'outils et de portails de gestion disparates. De plus en plus fréquentes, les attaques en ligne gagnent également en sophistication et la surface d'exposition s'étend, d'où une augmentation des risques. Pour surmonter ces obstacles, les entreprises font converger leurs services de sécurité cloud avec l'approche Security Service Edge (SSE).

## Bénéfices

- Accès unifié, fluide et sécurisé aux applications, aux ports et aux protocoles
- Opérations IT simplifiées grâce à une console unique, une gestion plus facile des politiques et des rapports combinés
- Risques réduits grâce à une cybersécurité avancée, à l'approche Zero Trust et à des politiques de sécurité granulaires
- Continuité de vos activités préservée pour éviter l'impact négatif d'une faille de sécurité sur vos finances ou votre réputation
- Tâches simplifiées partout
- Visibilité accrue sur l'utilisation des applications cloud, leurs niveaux de risque et le Shadow IT

## Une sécurité cloud plus efficace pour les utilisateurs, plus simple pour les équipes IT et plus sûre pour tous

Cisco Secure Access protège l'accès au web, aux services cloud, au SaaS et aux applications privées. La solution s'appuie sur le principe du moindre privilège pour authentifier dynamiquement les utilisateurs. Elle évalue les moyens de défense des équipements à l'aide d'informations contextuelles pour mieux les protéger. Plusieurs niveaux de sécurité protègent vos utilisateurs et vos ressources contre de nombreuses cyberattaques – des menaces, des tentatives d'exfiltration de données, des attaques par hameçonnage, des ransomwares ou des fichiers infectés.

---

Cisco Secure Access offre une flexibilité de pointe en matière de sécurisation de l'accès à toutes les applications privées (et pas seulement à certaines d'entre elles). Il s'agit d'une solution ZTNA avec ou sans client qui sécurise facilement l'accès aux applications standard en se basant sur l'approche du moindre privilège, que l'équipement soit géré par le département IT de l'entreprise ou non.

Pour les applications où le modèle ZTNA n'est pas pris en charge (des ports ou protocoles non standard, multipoint ou client à client, par exemple), Cisco Secure Access offre une fonctionnalité VPNaaS de secours, sans les difficultés souvent associées au matériel, à la gestion et aux utilisateurs finaux. Un seul client unificateur est utilisé pour l'architecture client ZTNA et le VPNaaS afin d'offrir une expérience simple et unifiée aux utilisateurs finaux.

Cisco Secure Access intègre tous les modules de sécurité utiles dans une solution cloud unique. Vous n'avez plus besoin d'assembler vous-même une solution constituée de différents outils de sécurité. En outre, un tableau de bord unique simplifie la gestion de l'IT et de la sécurité, tout en réduisant vos coûts d'administration.

L'efficacité de la sécurité représente un enjeu crucial. Secure Access repose sur Cisco Talos, l'un des fournisseurs de solutions de sécurité de pointe les plus importants et les plus fiables au monde. Avec son équipe d'experts à temps plein composée de chercheurs et de spécialistes des données exploitant des technologies d'apprentissage automatique et d'intelligence artificielle, Talos dispose d'une excellente visibilité sur les menaces en ligne et prend des mesures rapides et efficaces pour renforcer votre protection.

- Secure Access est proposé en deux packages, avec un décompte indépendant d'utilisateurs pour l'accès sécurisé privé ou Internet, pour une flexibilité accrue.
- Essentials : package de base comprenant l'accès Internet sécurisé, l'accès privé sécurisé, les technologies SWG, ZTNA et CASB, le pare-feu de couche 3 ou 4, l'isolation (partielle) du navigateur à distance et d'autres fonctions.
- Advantage : en plus des fonctions Essentials, ce package inclut le pare-feu de couche 7, les technologies IPS et DLP, l'isolation (complète) du navigateur à distance et bien plus encore.

## Revoir ses objectifs SSE à la hausse

Cisco Secure Access n'en reste pas à l'approche classique d'autres fournisseurs de solutions de sécurité. Il s'agit d'une solution de sécurité cloud fournie en tant que service qui offre plusieurs avantages essentiels.

### **Cisco fournit :**

- Un accès sécurisé à toutes les applications, y compris celles qui impliquent des protocoles non standard et celles qui sont basées sur des architectures multicanaux ou de client à client
- Une console de gestion unique pour tous les modules de sécurité
- Des fonctionnalités de sécurité complètes de pointe qui évitent d'avoir à accumuler des outils coûteux provenant de plusieurs fournisseurs, garantissent la cohérence des règles et sont facilement maîtrisables
- Une architecture cloud native résiliente avec une évolutivité étendue du nombre d'utilisateurs, un traitement efficace en un seul passage pour des réponses plus rapides et des délais d'exécution raccourcis afin d'assurer une prise en charge rapide de toute nouvelle fonctionnalité
- Une répartition automatique de la charge et un rééquilibrage du trafic pour améliorer les performances des clients

## Évaluez votre niveau de préparation à l'approche SSE

Répondez à un bref questionnaire pour faire un point sur votre situation à l'aide de notre [outil d'évaluation en ligne](#).

### Cisco Secure Access

**Services SSE essentiels**

- Passerelle web sécurisée (SWG)
- Service de sécurité pour l'accès au cloud (CASB) et DLP
- Accès réseau Zero Trust (ZTNA)
- Pare-feu en tant que service (FWaaS) et IPS

**Cisco propose les services essentiels et bien plus encore dans un seul abonnement.**

- Sécurité DNS
- DLP multimode
- Protection avancée contre les malwares
- Sandbox
- Threat Intelligence de Talos
- VPN en tant que service
- Supervision de l'expérience numérique\*
- Isolation du navigateur à distance\*

**Solutions complémentaires**

- SD-WAN
- XDR
- MFA/SSO DUO
- Gestion de la sécurité dans le cloud

\* Inclus dans l'expérience unifiée/licence distincte (facultatif)

Contactez-nous dès aujourd'hui

En savoir plus sur Cisco Secure Access. Rendez-vous sur <https://www.cisco.com/site/fr/fr/products/security/secure-access/index.html>

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](http://www.cisco.com/go/offices).

Cisco et le logo Cisco sont des marques commerciales ou des marques déposées de Cisco Systems, Inc. et/ou de ses filiales aux États-Unis et dans d'autres pays. Pour consulter la liste des marques commerciales Cisco, visitez le site : [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Les autres marques mentionnées dans les présentes sont la propriété de leurs détenteurs respectifs. L'utilisation du terme « partenaire » n'implique pas de relation de partenariat commercial entre Cisco et d'autres entreprises. (1110R)