

Protégez les utilisateurs et les ressources pour votre personnel hybride à l'aide de Cisco Secure Access

La flexibilité pour l'utilisateur et l'adoption rapide du nuage offrent une panoplie d'avantages. Malheureusement, elle étend aussi la surface des menaces, crée des failles de sécurité et a des répercussions sur l'expérience utilisateur.

Le nouveau paradigme du travail



Le travail hybride est là pour de bon

78 %

des organisations soutiennent un mélange d'employés travaillant à distance et au bureau

Source : 2023 Security Service Edge (SSE) Adoption Report (en anglais seulement), Cybersecurity Insiders et Axis



L'adoption du nuage s'est accélérée

50 %

de la charge de travail des organisations est exécutée dans le nuage public

Source : 2023 State of the Cloud Report (en anglais seulement), Flexera



Préoccupations grandissantes concernant la protection des utilisateurs à distance

47 %

des organisations indiquent que le travail à distance est leur principal défi

Source : 2022 Security Visibility Report (en anglais seulement), Cybersecurity Insiders

Les organisations et les équipes de sécurité doivent s'adapter



Pour assurer un accès sécurisé et fluide, les responsables des TI doivent faire ce qui suit :



Simplifier le processus d'accès pour les applications privées



Renforcer les contrôles d'accès de moindre privilège, contextuels et constants



Prévenir les lacunes de visibilité et de couverture de sécurité



Fournir une connectivité sécurisée dans plusieurs types et destinations d'applications



Fournir une expérience utilisateur de qualité supérieure



Éviter la multiplication des outils et la complexité de l'infrastructure

Une approche de cybersécurité convergée

Le service de sécurité en périphérie (SSE) est une approche qui aide les organisations à s'adapter à la nouvelle réalité en améliorant la posture de sécurité générale tout en réduisant la complexité pour l'équipe informatique et les utilisateurs finaux. Le SSE protège les utilisateurs et les ressources et simplifie le déploiement en consolidant de multiples capacités de sécurité, comme la passerelle Web sécurisée, le contrôle d'accès de sécurité infonuagique et la vérification systématique des accès réseau et en les fournissant à partir du nuage. Cela permet une connectivité sécurisée, transparente et directe avec le Web, les services en nuage et les applications privées. La solution Cisco Secure Access comprend tous les éléments ci-dessus et plus encore, afin d'offrir un niveau supérieur de protection et de satisfaction de l'utilisateur.

Les entreprises adoptent une sécurité consolidée en nuage



65 %

planifient l'adoption du SSE au cours des deux prochaines années

Source : 2023 Security Service Edge (SSE) Adoption Report (en anglais seulement), Cybersecurity Insiders et Axis



80 %

disposeront d'un accès unifié au Web, aux services en nuage et à l'accès privé grâce au service d'accès sécurisé en périphérie (SASE) ou au SSE d'ici 2025

Source : Gartner SASE Market Guide-2022 (en anglais seulement)



39 %

considèrent la plateforme de SSE comme la technologie la plus importante pour une stratégie de vérification systématique

Source : 2023 Security Service Edge (SSE) Adoption Report (en anglais seulement), Cybersecurity Insiders et Axis

Avantages de Cisco Secure Access



Simplifie l'expérience de l'utilisateur en réduisant au minimum les étapes manuelles nécessaires pour sécuriser ses activités



Protège en toute sécurité toutes les applications privées, y compris les applications non standard et personnalisées



Améliore l'efficacité de la sécurité grâce à les informations sur les menaces de Cisco, chef de file du marché

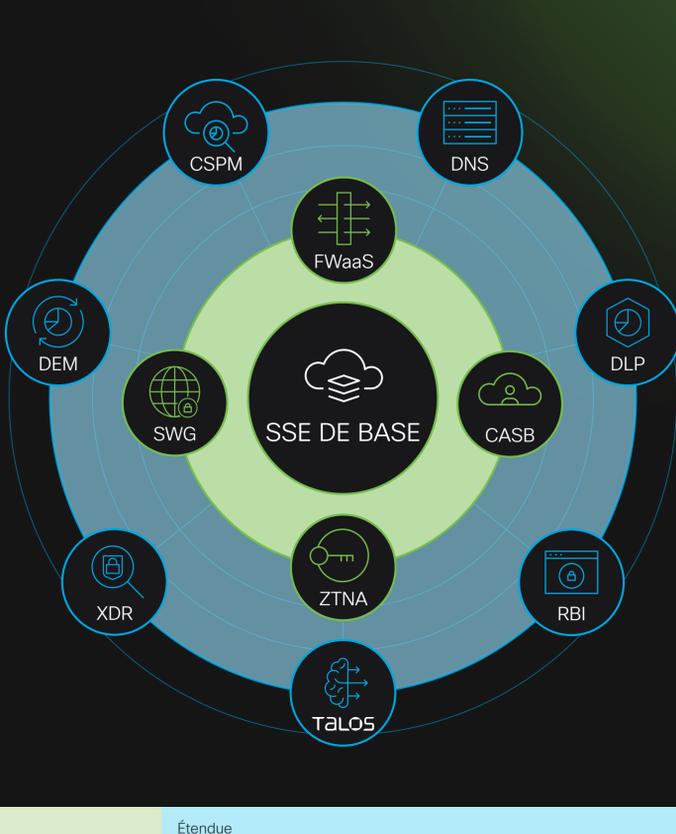


Garantit une vérification systématique grâce à des contrôles granulaires basés sur l'utilisateur, l'appareil, l'emplacement et l'application



Simplifie la gestion et améliore la facilité d'utilisation grâce à une console d'administration unifiée

La visibilité étendue de Cisco de la convergence de la sécurité



Base	Étendue	
FWaaS : Pare-feu à la demande	DNS : Serveur de noms de domaine	XDR : Détection et intervention étendues
CASB : Contrôle d'accès de sécurité infonuagique	DLP : Prévention de la perte de données	DEM : Supervision de l'expérience numérique
ZTNA : Vérification systématique des accès réseau	RBFI : Isolement du navigateur distant	CSPM : Gestion de la posture de sécurité dans le nuage
SWG : Passerelle Web sécurisée	Talos : Informations sur les menaces de Talos	

Découvrez comment Cisco Secure Access peut élever votre sécurité à un niveau supérieur



La sécurité convergée de Cisco réduit les risques et offre de la valeur



Sécurité renforcée

Les risques sont atténués dans l'ensemble du paysage des menaces grâce à une surface d'attaque considérablement réduite. Les activités malveillantes sont repérées et bloquées efficacement, et les incidents sont résolus rapidement pour assurer la continuité des activités.

30 % d'augmentation de l'efficacité de la sécurité

1 M \$ de réduction des coûts liés aux violations (sur environ trois ans)

Source : Forrester Total Economic Impact (TEI) Study for Cisco Umbrella SIG/SSE, 2022 (en anglais seulement)



Avantages concernant le coût et la valeur

Les équipes NetOps et SecOps bénéficient d'une sécurité convergée à partir d'une plateforme infonuagique unique qui offre une expérience facile et sécurisée partout où votre entreprise travaille.

231 % de ROI sur trois ans

2 M \$ de profits nets, VAN de trois ans

<12 mois de délai de récupération

Source : Forrester Total Economic Impact (TEI) Study for Cisco Umbrella SIG/SSE, 2022 (en anglais seulement)

Si vous êtes à la recherche d'une solution de SSE ou d'une solution de SASE unifiée complète, laissez Cisco accélérer votre parcours de sécurité.

Vous trouverez de plus amples renseignements sur

Cisco Secure Access : Services de sécurité convergée natifs du nuage

Cisco+ Secure Connect : Solution de SASE unifiée, clé en main et gérée dans le nuage