Guide de l'acheteur SASE

Comment choisir une plateforme SASE qui donne la priorité à la sécurité des données ?

Forcepoint

Sommaire

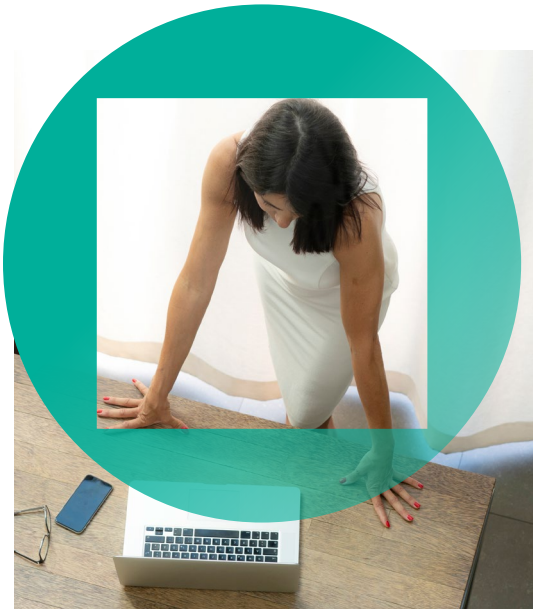
Résumé analytique

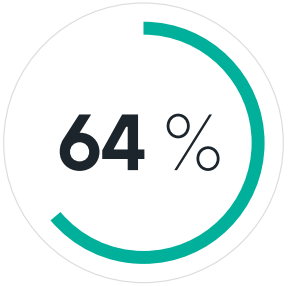
Travailler à distance signifie aujourd'hui « travailler n'importe où » – à domicile, dans un bureau ou partout où les déplacements sont autorisés. Les nouveaux défis consistent à connecter les personnes aux données dont elles ont besoin et à assurer une sécurité cohérente partout où elles sont utilisées.

Les personnes, les applications et les données se situent désormais souvent en dehors des frontières traditionnelles de l'entreprise. Mais les équipes chargées de la sécurité doivent continuer à assurer une sécurité cohérente là où elle est nécessaire, tout en favorisant la productivité du personnel où qu'il se trouve, tout en réduisant la charge opérationnelle. L'architecture Secure Access Service Edge (Service d'Accès Sécurisé vers l'Extérieur, ou SASE) de Gartner est une solution d'avenir convaincante, conçue pour rassembler des technologies de réseau et de sécurité disparates sous forme de services convergents fournis depuis le cloud.

Certaines solutions SASE se concentrent sur la connexion des personnes aux applications ; cependant, l'accès est simplement la manière dont les personnes obtiennent les données dont elles ont besoin pour accomplir leur travail en toute sécurité. La cybersécurité doit également protéger l'utilisation de ces données, de la périphérie au cloud.

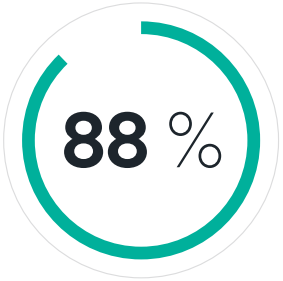
Utilisez ce guide pour comprendre les différentes approches de sécurisation des SASE et les capacités que vous devez attendre d'une plateforme SASE, et la confiance à lui apporter.



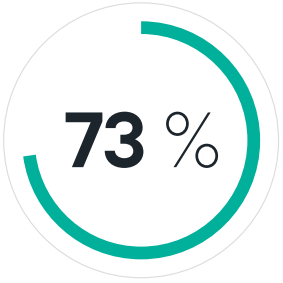


64 % des entreprises affirment qu'assurer la sécurité des réseaux est plus difficile de nos jours[1]

53 % des employés travaillent à distance, contre seulement 20 % avant le COVID[1]



88 % des utilisateurs d'un SASE sont convaincus d'avoir une visibilité sur l'ensemble de l'utilisation du cloud dans l'entreprise[1]



73 % des utilisateurs confirmés de SASE vont supprimer les VPN[1]

Deux types de SASE

Un SASE fait disparaître les accumulations disparates de matériel de réseau et de sécurité et les remplace par des services cloud convergents qui suivent principalement deux écoles de pensée :

SASE centré sur l'accès

- **Avantages :** Comme son nom l'indique, la sécurité SASE centrée sur l'accès se concentre principalement sur la connexion sécurisée des utilisateurs aux applications et aux données, que ce soit sur le web, dans le cloud ou dans des centres de données privés internes. Généralement fourni sous forme de cloud, ce type de SASE permet un contrôle centralisé des personnes autorisées à utiliser les systèmes essentiels de l'entreprise et protège contre les attaques de malware, de ransomware et les autres menaces avancées.
- **Problèmes potentiels :** Les SASE centrés sur l'accès ont tendance à se concentrer sur la connexion des utilisateurs aux applications dont ils ont besoin pour interagir avec les données de l'entreprise, mais ne fournissent pas de contrôle continu sur l'utilisation de ces données.En outre, certaines solutions se comportent comme des produits à fonction unique gérés à distance, nécessitant plusieurs agents de terminaux pour différents services de sécurité, ce qui entraîne une prolifération d'agents menant à des conflits.

SASE centré sur les données :

- **Avantages :** Donner priorité aux données, au sein d'une stratégie SASE, permet de contrôler en permanence la manière dont les données sont utilisées et d'assurer la sécurité d'accès aux données pour les utilisateurs. En outre, quelques solutions SASE ont évolué pour comprendre comment les utilisateurs interagissent avec les données, les systèmes numériques et physiques ; ces solutions sont capables d'identifier les comportements à risques pouvant conduire à des intrusions. En plaçant les données au cœur du SASE, on active l'application automatisée des politiques de sécurité en fonction du risque que présente chaque utilisateur à un moment donné. L'objectif du SASE centré sur les données est de rendre l'application des politiques uniforme, partout – sur les terminaux, dans le réseau, sur le web et dans le cloud, ce qui rend cette approche idéale pour les entreprises distribuées où les employés travaillent et utilisent des services cloud au-delà des limites physiques de l'entreprise.
- **Problèmes potentiels :** Même si vous pouvez mettre en œuvre toutes les plateformes SASE progressivement, une capacité à la fois, une approche SASE centrée sur les données est plus efficace lorsque la sécurité des données est considérée comme une priorité par l'ensemble de l'entreprise. Pour tirer le meilleur d'une telle approche, les politiques de sécurité relatives aux informations sensibles et à la propriété intellectuelle doivent être comprises et soutenues par la direction, de même que les processus et procédures opérationnels.

5 étapes vers le SASE

1.

Protégez les travailleurs à distance, sur le web comme dans le cloud.

La sécurité de votre SASE doit permettre aux salariés d'effectuer leur travail en toute sécurité, et ne doit pas entraver leur productivité. L'ubiquité de ces travailleurs ne doit pas les empêcher d'avoir la liberté de travailler en toute sécurité depuis n'importe quel endroit et à tout moment.

2.

Contrôler l'accès au cloud et aux applications privées sans VPN

Chaque utilisateur ne doit avoir accès qu'aux ressources qu'il est explicitement autorisé à utiliser, sous la visibilité et le contrôle total de votre entreprise.

3.

Protéger l'utilisation des données, où que celles-ci se trouvent

Votre SASE doit assurer un contrôle permanent de la manière dont les données critiques et les propriétés intellectuelles sont utilisées une fois téléchargées à partir des applications. Cela permet d'éviter que les données ne soient transférées de manière inappropriée vers le cloud, le web ou des comptes personnels - de manière involontaire ou malveillante.

4.

Connecter et protéger les bureaux et les sites distants

Les utilisateurs des sites distants doivent disposer d'un accès rapide et sécurisé au web, au cloud et aux applications privées sans les coûts ou la complexité induits par des lignes MPLS privées ou par la redirection du trafic vers le siège. Une intégration facile avec les services SASE est cruciale pour une gestion évolutive.

5.

Surveiller en permanence les risques posés par les utilisateurs

Pour contrôler l'utilisation des données, en particulier sur les appareils distants et les services cloud, il faut comprendre en permanence ce que font les gens, et savoir si leur comportement crée des risques qui pourraient se transformer en violations.

Ce qu'il faut rechercher dans un SASE centré sur les données

En fusionnant plusieurs capacités au cœur d'une plateforme cloud unique, votre SASE comble les lacunes qui existaient auparavant avec des produits à fonction unique disparates, réduit les coûts et améliore l'efficacité en assurant la sécurité partout où les données sont utilisées. La différence entre les approches SASE centrées sur l'accès et celles centrées sur les données se résume à la question de savoir si les données sont protégées en permanence après qu'on y ait accédé. Lors de votre évaluation, tenez compte des capacités suivantes. Recherchez des fonctionnalités de niveau supérieur qui permettent d'automatiser et de gérer les données, et, dans votre SASE, donnez toujours la priorité aux données.

Capacités essentielles

- **Protection des données :** Un SASE centré sur les données doit fournir une protection pour l'accès et l'utilisation des informations sensibles et de la propriété intellectuelle. Recherchez des solutions SASE qui offrent un ensemble unique de politiques de sécurité des données pouvant être appliquées partout de manière uniforme, des terminaux jusqu'au réseau, au web et au cloud. Les contrôles du trafic à l'échelle de l'entreprise garantissent que les données ne peuvent pas sortir des appareils des employés de manière inappropriée, par exemple en étant déplacées vers un service cloud ou une clé USB, en étant imprimées ou copiées.
- **Protection contre les menaces :** Les défenses sont stratifiées et combinent la protection de la périphérie, l'inspection approfondie du contenu, la détection avancée des malwares et l'isolation du navigateur à distance pour se protéger contre les assaillants externes. Vous pouvez mettre en ligne vos bureaux distants rapidement et en toute sécurité grâce à une protection complète effectuée directement depuis le cloud, sans aucun équipement matériel.
- **Sécurité des applications :** Le SASE a été développé pour fournir visibilité et contrôle sur les applications, repérer la shadow IT et les appareils gérés ou non par l'entreprise, grâce à des fonctionnalités comme le filtrage des URL, l'inspection approfondie du contenu et la visibilité des applications dans le cloud. Le blocage de l'utilisation de tout service cloud non autorisé empêche les employés de déjouer les politiques de sécurité. Un audit complet et un contrôle granulaire de l'utilisation et des activités des applications simplifient la conformité dans le cloud.

- **Sécurité réseau :** Une sécurité complète englobant des services de firewall à la fois sur site et dans le cloud permet d'activer un accès sécurisé à Internet, d'inspecter le trafic crypté et de se défendre contre les menaces réseau avancées.
- **Connectivité réseau :** SD-WAN connecte les succursales directement à Internet, là où les services SASE peuvent assurer une sécurité sans faille. Un agent terminal connecte de la même manière les employés distants.

Fonctionnalités de niveau supérieur

- **Des politiques unifiées de sécurisation des données** vous donnent la capacité de définir des politiques de sécurité juste une seule fois, que vous pouvez ensuite appliquer partout, des terminaux jusqu'au cloud.
- **Des agents unifiés** couvrent tous les terminaux, permettant d'accéder en toute sécurité aux ressources, d'appliquer des politiques et de surveiller l'activité des appareils des utilisateurs.
- **Des fonctions de déploiement flexibles** intègrent des contrôles riches basés sur le contexte, une application hybride sur les sites ayant des exigences particulières (par exemple, la conformité aux réglementations sur la souveraineté des données), et sécurisent le SD-WAN sans nécessiter de produits supplémentaires.
- **L'application de politiques basées sur le risque** personnalise automatiquement la sécurité en fonction du risque que présente le comportement de chaque utilisateur lorsqu'il utilise des données, des applications et des systèmes.

Les principales questions à se poser :

1. Quelles mesures devrez-vous prendre pour effectuer la transition vers un modèle de main-d'œuvre hybride ?
2. Comment les travailleurs distants accèdent-ils aujourd'hui à votre cloud et à vos applications privées ?
3. Qu'avez-vous dû changer dans votre infrastructure ou vos opérations pour la prise en charge du travail à domicile (TAD) ?
4. Comment comptez-vous gérer le TAD ?
5. Quelles applications cloud votre entreprise autorise-t-elle aujourd'hui ?
6. Avez-vous une visibilité sur les applications non approuvées qui ont des capacités de partage de données ?
7. Pouvez-vous contrôler la sécurité dans le cloud/Internet de vos travailleurs à distance ?
8. Cherchez-vous des moyens de consolider le matériel en périphérie de votre réseau (dans les bureaux, les filiales, etc.) ?
9. Quelle est votre stratégie pour sécuriser l'accès aux applications internes et privées ?
10. Comment protégez-vous ou contrôlez-vous les données, et quels sont les écarts entre les exigences réglementaires et vos capacités ?
11. Quel est le niveau de risque de votre entreprise face aux « pertes » de données dans le cloud, à leur exposition publique ou à leur exfiltration directe ?
12. Si vous deviez repartir à zéro, que feriez-vous différemment pour sécuriser l'accès au cloud, aux données et aux réseaux ?

Le but recherché : Protéger les données – où qu'elles se trouvent

Les travailleurs d'aujourd'hui, où qu'ils soient, auront plus d'autonomie au sein de votre entreprise décentralisée. Le monde a changé à jamais, offrant des options semblant infinies pour accéder aux ressources et aux services, et se protéger contre des menaces de plus en plus sophistiquées ou contre des failles accidentelles.

En tant que professionnel de la sécurité, vous devez faciliter cette transformation sans vous laisser enfermer dans des solutions ponctuelles qui ne peuvent pas évoluer au sein de cet univers numérique sans frontière. Le fait que vous lisiez ces lignes signifie que vous essayez de trouver de nouveaux moyens de soutenir efficacement la productivité, tout en protégeant vos employés et vos données critiques où qu'ils se trouvent. L'adoption d'une approche native cloud et hybride est la manière la plus efficace d'assurer la sécurité.

Trouvez un partenaire qui peut vous aider à identifier rapidement les possibilités pour créer un cadre de sécurité intégré, étape par étape. Un partenaire qui vous donne l'agilité nécessaire pour vous adapter à un environnement en constante évolution.

En tant que professionnel de la sécurité, vous devez faciliter cette transformation sans vous laisser enfermer dans des solutions ponctuelles qui ne peuvent pas évoluer au sein de cet univers numérique sans frontière.

Prochaines étapes

En savoir plus et télécharger notre *livre blanc* 5 étapes vers le SASE.

Télécharger maintenant

[1] Rapport ESG Research Insights, Quantifying the Benefits of SASE (Quantifier les avantages du SASE), mars 2021

Forcepoint

forcepoint.com/contact

À propos de Forcepoint

Forcepoint est l'entreprise leader en cybersécurité pour la protection des utilisateurs et des données. Son objectif est de protéger les entreprises tout en stimulant la transformation et la croissance numériques. Nos solutions à facteur humain s'adaptent en temps réel à la façon selon laquelle les individus interagissent avec les données, et offrent un accès sécurisé tout en permettant aux employés de créer de la valeur. Basé à Austin, au Texas, Forcepoint crée des environnements sûrs et fiables protégeant des milliers de clients dans le monde entier.