

janvier 2021

ETUDE DE MARCHÉ

Réseaux cloud : une accélération de la transition

La confiance des leaders mondiaux de l'informatique dans le cloud augmente malgré les préoccupations liées à la sécurité. »

Sommaire

Introduction : l'évolution constante du paysage cloud	3
Résultats clés	4-9
Les professionnels de l'informatique font de plus en plus confiance au cloud	4
Les entreprises sont confrontées à des contraintes croissantes en matière d'accès au cloud	5
L'infrastructure réseau actuelle est de plus en plus coûteuse	6
Les professionnels de l'informatique recherchent une connectivité plus facile et plus économique	7
La sécurité est au cœur des réseaux cloud	8
Les professionnels de l'informatique attendent des fournisseurs de services cloud qu'ils jouent un rôle essentiel avec les solutions SD-WAN	9
Conclusion : sécuriser la périphérie du réseau	10
Barracuda en quelques mots	11

Introduction

L'évolution constante du paysage cloud

Le cloud public stimule l'innovation numérique. Alors que les sociétés informatiques du monde entier continuent à transformer radicalement leurs infrastructures, à faire évoluer le mode de prestation des services et à gérer les problèmes de sécurité, l'utilisation du cloud et la dépendance envers celui-ci ne cessent de croître. Outre les opérations quotidiennes, le cloud public est désormais considéré, par de nombreuses entreprises, comme un prérequis à la croissance axée sur l'innovation.

Ce rapport analyse en détail le cloud public, les contraintes d'accès, les problèmes de sécurité, les solutions émergentes et divers problèmes connexes.

Méthodologie

Barracuda a demandé au cabinet d'études indépendant Censuwide de mener une enquête auprès des décideurs informatiques responsables de l'infrastructure cloud de leur entreprise. Plus de 800 personnes ont participé à l'enquête mondiale, représentant des entreprises de toutes tailles et de différents secteurs, notamment la construction, l'éducation, la finance, la santé, la technologie, la production industrielle, la vente au détail et les transports. L'enquête a été réalisée en octobre 2020.

Résultats clés

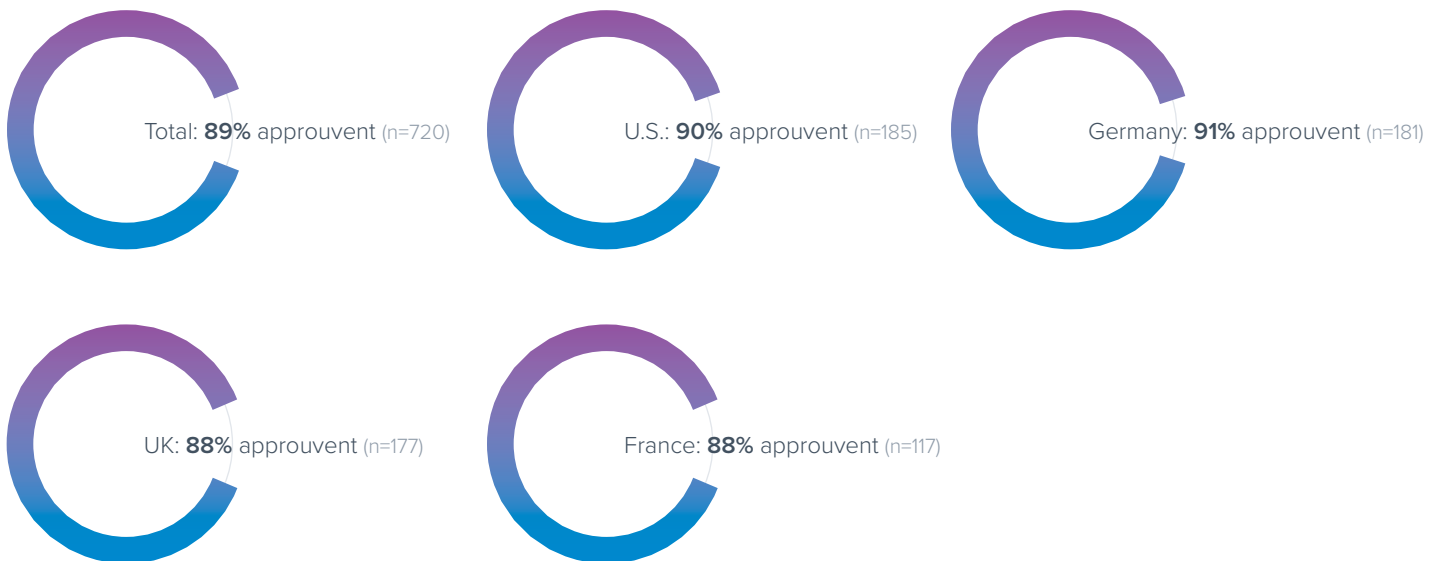
CONSTAT N°1

Les professionnels de l'informatique font de plus en plus confiance au cloud

90 % des personnes interrogées déclarent que leur entreprise comprend le modèle de responsabilité partagée pour la sécurité du cloud utilisé par Amazon Web Services et Microsoft Azure. Le fournisseur de services cloud est responsable de la sécurité du cloud, tandis que l'entreprise est responsable de la sécurité de ce qu'elle met dans le cloud.

Plus des trois quarts des personnes interrogées utilisent plusieurs fournisseurs de services cloud, tels qu'Amazon Web Services, Microsoft Azure et Google Cloud Platform. Près de 80 % d'entre elles déclarent que leur entreprise a déployé un réseau basé sur Azure.

Mon entreprise comprend le modèle de responsabilité partagée pour la sécurité du cloud.



Résultats clés

CONSTAT N°2

Les entreprises sont confrontées à des contraintes croissantes en matière d'accès au cloud

La majorité des personnes interrogées, dans toutes les régions, s'efforcent de garantir une disponibilité sans faille et un accès permanent aux applications cloud. 60 % d'entre elles ont envisagé Microsoft ExpressRoute ou AWS Direct Connect, mais ces solutions n'étaient pas disponibles ou s'avéraient trop coûteuses pour l'ensemble de leurs sites.

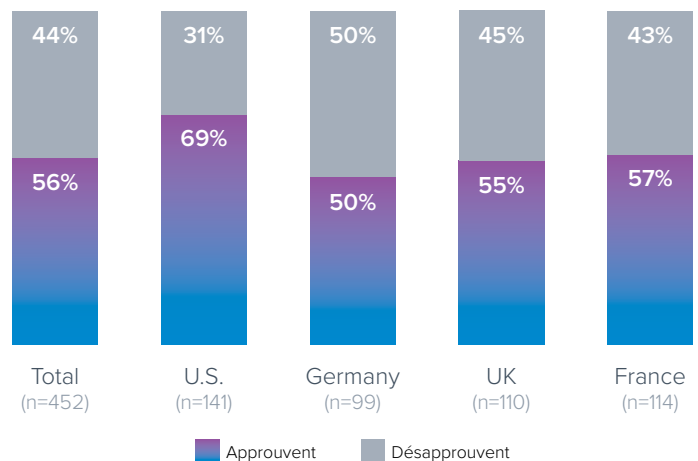
Et un nombre encore plus important — près de 70 % — ont rencontré des problèmes de latence et de performances avec des applications SaaS, telles qu'Office 365. Le pourcentage était le plus élevé aux États-Unis (80%) et le plus bas au Royaume-Uni (53%). Cette tendance va s'accroître, car les charges de travail entraînent une utilisation croissante du cloud et une plus grande dépendance envers celui-ci.

Tandis que les entreprises ont de plus en plus recours au cloud, elles se heurtent à un certain nombre de contraintes. Par exemple, les temps d'arrêt sont toujours cités comme un problème. Bien que ce soit rare, les infrastructures cloud tombent en panne. Les interruptions de service du point de terminaison lui-même, comme le fournisseur d'accès Internet ou le fournisseur de connectivité, sont plus fréquentes. Les entreprises qui ont besoin d'une haute disponibilité ou de temps de fonctionnement garantis ont besoin de fournisseurs de basculement et de connexions fiables pour éviter cette contrainte.

La bande passante est une contrainte bien plus courante. En informatique d'entreprise, les fichiers de données, y compris les fichiers vidéo et multimédias courants, peuvent être volumineux et ils ont tous un impact important sur la bande passante.

Les entreprises qui utilisent un réseau traditionnel pour acheminer le trafic via un datacenter centralisé (souvent pour des raisons de sécurité) constatent que leurs utilisateurs et leurs réseaux sont confrontés à une augmentation de la latence et à l'incapacité de répondre aux exigences du trafic.

Nous luttons pour garantir une disponibilité transparente et un accès «permanent» aux applications cloud.



Résultats clés

CONSTAT N°3

L'infrastructure réseau actuelle est de plus en plus coûteuse

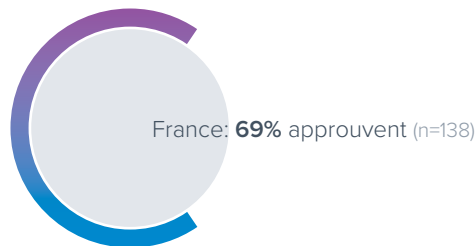
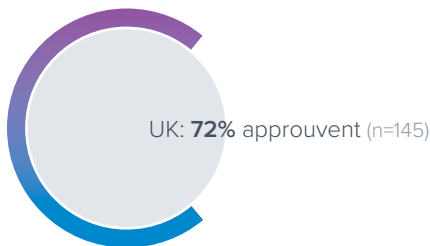
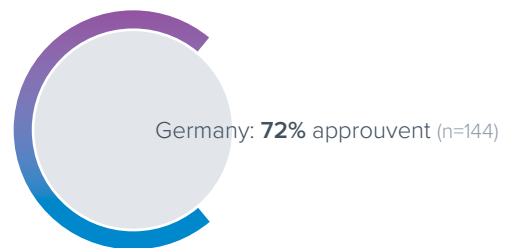
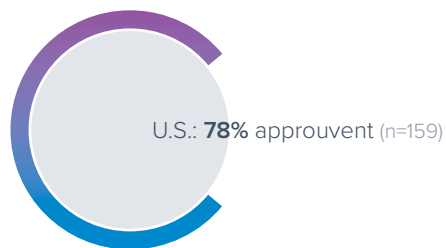
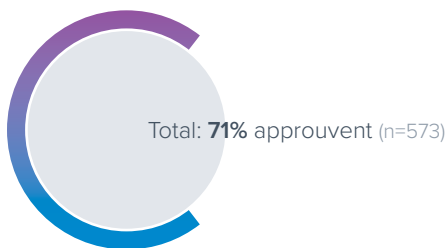
71% des personnes interrogées utilisent des méthodes d'accès traditionnelles, telles que le MPLS, dans le réseau de leur entreprise.

62 % d'entre elles déclarent que leurs coûts MPLS augmentent fortement en raison des pics saisonniers des charges de travail. Un pourcentage similaire (61%) déclare que les lignes MPLS sont coûteuses et peu flexibles pour les besoins des entreprises. Ce sentiment était le plus répandu aux États-Unis (72%) et le moins courant au Royaume-Uni (53%).

Les lignes dédiées et louées, telles que les lignes MPLS, sont la solution que la plupart des entreprises utilisent

traditionnellement pour interconnecter les infrastructures réseau, en particulier pour l'Internet et le cloud. Alors que les lignes MPLS étaient une bonne idée il y a quelques années, elles constituent un obstacle au cloud computing intensif. Ces lignes sont fixes, ce qui signifie qu'elles souffrent de plafonds de débit. Pour couronner le tout, la location de ces lignes se fait généralement sur le long terme et pénalise souvent les entreprises qui ont besoin d'une bande passante supplémentaire et plus rapide. De plus, les solutions MPLS ne s'adaptent pas aux variations du débit. Il en résulte souvent une inadéquation des capacités, si bien que les entreprises se rendent compte qu'elles paient souvent plus cher qu'elles ne le devraient pour assurer une capacité supplémentaire dont elles n'ont pas besoin 24 h/24.

Nous utilisons des méthodes d'accès traditionnelles (telles que MPLS) dans le réseau de l'entreprise.



Résultats clés

CONSTAT N°4

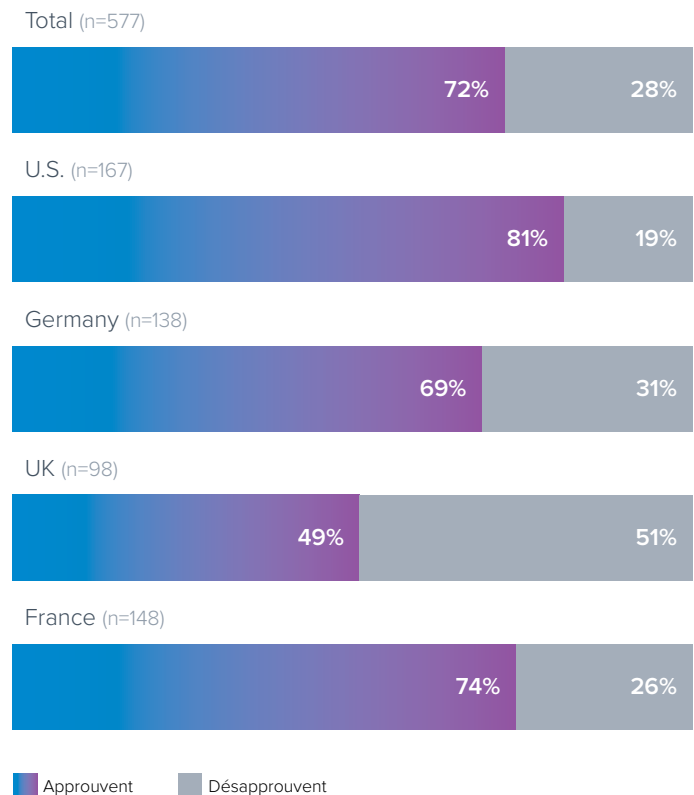
Les professionnels de l'informatique recherchent une connectivité plus facile et plus économique

Pour faire face aux contraintes, les entreprises se tournent vers les réseaux nouvelle génération. Dans les quatre régions, 88% des répondants connaissent le WAN virtuel de Microsoft. Plus de 7 sur 10 prévoient de mettre en œuvre une solution SD-WAN au cours des 12 prochains mois pour résoudre les problèmes de connectivité dans le cloud. Ce nombre était le plus élevé aux États-Unis (81%) et le plus bas au Royaume-Uni (49%).

Dans le même temps, 58% de tous les répondants affirment que leur entreprise hésite à adopter une solution SD-WAN par crainte qu'elle soit complexe et coûteuse. Ce pourcentage était le plus bas en Allemagne (54%) et nettement plus élevé au Royaume-Uni (74%).

Les offres de produits récentes changent cette perception en combinant la sécurité des points de terminaison, l'accès zero trust et une gestion simplifiée.

Mon entreprise envisage d'implémenter SD-WAN dans les 12 prochains mois comme solution pour résoudre les problèmes de connectivité au cloud.



Résultats clés

CONSTAT N°5

La sécurité est au cœur des réseaux cloud

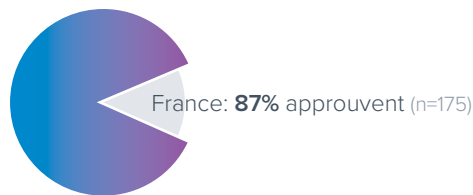
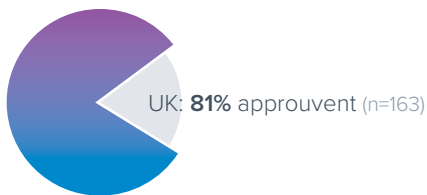
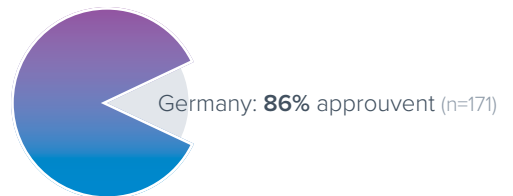
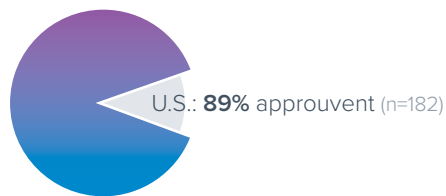
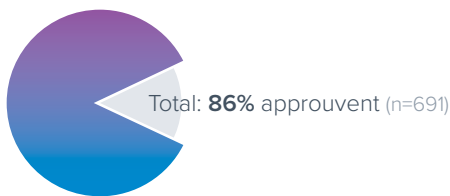
Un total de 86% des entreprises dans les quatre régions disposent de solutions distinctes pour la mise en réseau et la sécurité. Également, un total de 91% de tous les répondants estiment que la sécurité doit être intégrée à l'ensemble du réseau, et pas seulement appliquée au datacenter.

Un total de 71% d'entre elles considèrent la sécurité comme une préoccupation majeure de leur entreprise lors du déploiement d'une solution SD-WAN. Cette préoccupation était la plus élevée aux États-Unis (81%) et plus faible en Allemagne (65%), au Royaume-Uni (62%) et en France (62%). Plus de 80 % connaissent la notion de Secure Access Service Edge (SASE) et affirment que leur entreprise voit l'intérêt de mettre en œuvre une solution qui exploite la sécurité zero trust à la périphérie du

réseau. Les différences régionales vont de 88% en France à 78% au Royaume-Uni.

Dans l'environnement actuel, les réseaux sont fluides, souvent hybrides, et le cloud présente de nouveaux défis de sécurité. Les données sortent désormais du réseau d'entreprise étroitement contrôlé, et les applications orientées cloud et l'accès à distance fournissent de nouveaux vecteurs d'attaque et de perte de données. Alors que la plupart des solutions de sécurité réseau considèrent la connectivité et la sécurité comme des activités distinctes, les solutions réseau qui adoptent le protocole SASE et combinent l'accès, la connectivité et la sécurité facilitent la mise en réseau cloud.

J'ai des solutions distinctes pour le réseau et la sécurité, c'est-à-dire des produits qui se concentrent spécifiquement sur le réseau ou la sécurité.



Résultats clés

CONSTAT N°6

Les professionnels de l'informatique attendent des fournisseurs de services cloud qu'ils jouent un rôle essentiel avec les solutions SD-WAN

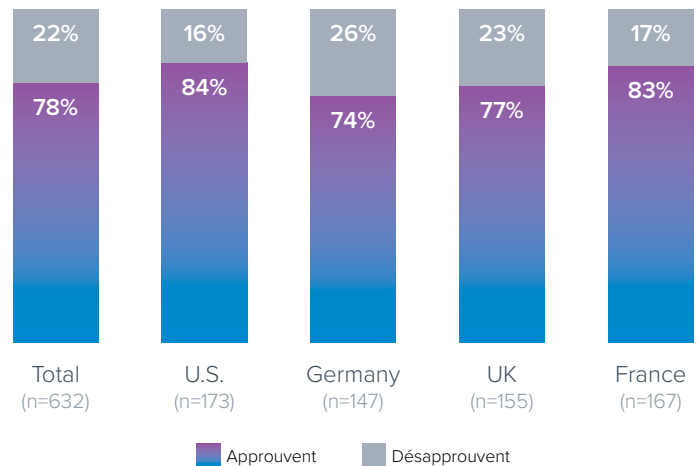
Globalement 78% des professionnels de l'informatique, dans les quatre pays, préfèrent largement déployer une solution SD-WAN unifiée et sécurisée dans le cloud.

En outre, plus des trois quarts de tous les répondants envisagent d'évaluer :

- Une solution de connectivité cloud qui utilise Microsoft Global Network comme réseau backbone (80%)
- Une solution SD-WAN intégrée dans l'infrastructure d'un fournisseur de services cloud (76%)
- Une solution de connectivité pouvant fonctionner en parallèle avec l'infrastructure réseau et de sécurité existante (78%)

De nombreuses entreprises sont confrontées à des infrastructures vieillissantes, ce qui fait du SD-WAN un choix logique pour alléger les contraintes de performance et de coût inhérentes à ces architectures anciennes.

Je préférerais déployer une solution unifiée de SD-WAN / sécurité dans le cloud.



Conclusion

sécuriser la périphérie du réseau

Les solutions Secure Access Service Edge (SASE) sont relativement nouvelles, mais elles constituent le prochain changement d'infrastructure logique pour les entreprises axées sur le cloud. Très flexibles, les solutions SASE permettent aux entreprises de toutes tailles et de tous types, d'améliorer la connectivité, de simplifier la gestion et de renforcer la sécurité.

Comme l'infrastructure est axée sur le cloud, le niveau d'intégration d'une solution SASE avec un fournisseur cloud est essentiel. Les entreprises affichent une nette préférence pour les solutions SD-WAN qui sont directement intégrées à l'infrastructure d'un fournisseur de cloud public. Elles considèrent également que la possibilité d'établir une connectivité sur le backbone d'un réseau cloud, tel que le Microsoft Global Network, est un autre avantage intéressant de la mise en œuvre d'une solution SD-WAN basée sur le cloud.

Enfin, la sécurité reste une préoccupation primordiale. La plupart des personnes interrogées considèrent que l'accès zero trust est implicite dans les déploiements, et elles recherchent des solutions qui unifient l'accès, la sécurité et la mise en réseau, et qui ne traitent pas ces facteurs comme des entités distinctes.

En déployant une solution native tout-en-un qui combine sécurité et optimisation du réseau pour créer une infrastructure SD-WAN sécurisée, les entreprises peuvent tirer pleinement parti du cloud public.

La sécurité reste une préoccupation primordiale. La plupart des personnes interrogées considèrent que l'accès zero trust est implicite dans les déploiements, et elles recherchent des solutions qui unifient l'accès, la sécurité et la mise en réseau, et qui ne traitent pas ces facteurs comme des entités distinctes.

Barracuda en quelques mots

Rendre le monde plus sûr est notre objectif chez Barracuda.

Nous pensons que chaque entreprise doit se doter de solutions cloud, faciles à acquérir, à déployer et à utiliser, tout en gardant leur niveau de sécurité. Nous protégeons les e-mails, les réseaux, les données et les applications avec des solutions innovantes et évolutives, qui s'adaptent à la croissance de nos clients.

Plus de 200 000 entreprises à travers le monde font confiance à Barracuda pour les protéger – elles restent sereines face aux risques qui sont toujours là – et peuvent se concentrer sur le développement de leur business.

Pour en savoir plus, rendez-vous sur barracuda.com.

