

Rapport Zscaler sur l'Etat de la Transformation Digitale, EMEA, 2020

Internet est devenu le nouveau réseau d'entreprise,
permettant le travail en tout lieu

Sommaire

1) Résumé analytique	Page 3
2) À propos de cette enquête	Page 5
3) Résultats clés	
A) Internet est devenu le nouveau réseau d'entreprise	Page 6
B) Les scénarios multicloud sont à l'ordre du jour	Page 10
a. Les défis des stratégies multicloud	
C) Les plus grands moteurs de la transformation cloud : la flexibilité et l'évolutivité	Page 13
D) Le plus grand défi de la transformation cloud : la sécurité	Page 14
E) Influence du télétravail sur la transformation cloud	Page 16
F) Défi : sécuriser l'accès distant à l'ère du travail en tout lieu	Page 18
4) Conclusion	Page 22
5) Recommandations	Page 23
À propos de Zscaler	Page 24

Résumé analytique

Avant la pandémie, les entreprises faisaient activement migrer les applications privées vers les cloud publics et permettaient à certains utilisateurs d'accéder aux applications depuis n'importe quel emplacement et n'importe quel appareil. En réaction à la crise mondiale, les employés et les entreprises ont rapidement adopté et dans une mesure encore plus grande ce nouveau style de travail en tout lieu. Cela a créé une prolifération de périmètres de sécurité autour des utilisateurs, des appareils et des applications, les entreprises évaluant les concepts de sécurité émergents pour faire face à ces nouvelles exigences.

Être en télétravail signifie que les employés ont la liberté d'accéder aux données de pratiquement n'importe où, mais cette liberté entraîne également des défis en matière de réduction des risques, car les infrastructures traditionnelles n'ont pas été conçues pour gérer une main-d'œuvre de plus en plus mobile. Les équipes informatiques doivent rapidement et en toute sécurité permettre aux employés de faire du télétravail sans perturber l'entreprise. Cela peut sembler une tâche ardue, mais la solution est dans le cloud : le cloud est ce dont les entreprises ont besoin lorsque l'emplacement n'a plus d'importance.

Pour mieux comprendre la situation sur le terrain Zscaler a commandé l'étude intitulée **"Etat de la Transformation Digitale 2020"** sur les organisations au Royaume-Uni, en France, en Allemagne, aux Pays-Bas, en Italie et en Suède :

- Jusqu'où les organisations sont allées sur le parcours de leur transformation
- Si Internet est déjà devenu le nouveau réseau d'entreprise
- Si le cloud est le nouveau data center.

Ce rapport comprend les principaux résultats de la recherche, des recommandations pour aider les organisations à surmonter les défis communs dans les déploiements cloud complexes, et à répondre aux préoccupations de sécurité pendant leur transformation numérique.

La transformation d'une entreprise nécessite une refonte fondamentale des écosystèmes technologiques. Avec les applications qui migrent vers le cloud et les utilisateurs qui se connectent de partout, le périmètre est devenu sans intérêt et les traditionnels réseaux en étoile sont obsolètes. Il est donc temps de dissocier la sécurité du réseau et de déployer des politiques qui seront appliquées partout où les applications résident et où les utilisateurs se connectent. Les résultats de l'enquête montrent que les entreprises qui déplacent des applications vers le cloud sans adapter leurs infrastructures et leur sécurité ont tendance à se débattre avec la complexité et les imprévisibles exigences de sécurité.

Résumé analytique

Tirer pleinement parti des technologies modernes et contrôler les risques devrait figurer au nombre des priorités clés de la transformation. Les besoins du personnel de plus en plus mobile d'aujourd'hui doivent être pris en compte, notamment une expérience positive et transparente. Si la sécurité des utilisateurs et des applications est plus que jamais importante, la visibilité sur l'ensemble du réseau d'entreprise et sur le trafic des appareils connectés est également devenue essentielle dans la défense des actifs de l'entreprise.

Trois domaines clés pour les télétravailleurs ou travailleurs nomades

Soutenir une poignée de télétravailleurs est une chose, mais comment permettre à un vaste personnel d'accéder en toute sécurité à Internet, au SaaS et aux applications privées alors qu'ils pourraient se trouver n'importe où dans le monde, utilisant n'importe quel appareil ? Pour commencer, vous devez vous concentrer sur trois domaines :

- **Simplicité et évolutivité** : la sécurité réseau traditionnelle est inflexible, ce qui rend la capacité à s'adapter aux fluctuations de capacité extrêmement lente, incroyablement complexe ou tout simplement impossible. Les solutions basées sur le cloud simplifient le déploiement, l'évolutivité et la gestion pour traiter les inévitables changements dans l'environnement commercial.
- **Expérience utilisateur** : les utilisateurs ne devraient pas se préoccuper de la manière dont ils accèdent à une application, de l'appareil qu'ils utilisent ou de l'endroit où s'exécute l'application. Dans un monde tourné vers le travail en tout lieu, une expérience utilisateur sans faille est essentielle à la productivité. Par souci de sécurité, les entreprises doivent tenir compte des limitations de vitesse d'accès lorsqu'elles font un routage du trafic à travers un hub central. L'avenir de la connectivité des utilisateurs passe par des connexions locales rapides, avec un service fourni à la périphérie dans des points de présence mondiaux largement distribués afin de minimiser la latence.
- **Sécurité** : permettre aux utilisateurs de se connecter de n'importe où est formidable, mais si vous les connectez au réseau, vous êtes confronté au risque que des logiciels malveillants se déplacent latéralement et à la possibilité d'attaques DoS. Les entreprises doivent dissocier l'accès aux applications de l'accès au réseau, et la surface d'attaque doit être aussi proche que possible de zéro. Les services ZTNA (Zero Trust Network Access) fournis dans le cloud réduisent cette exposition.

À propos de cette enquête

L'objectif de l'étude Zscaler intitulée "Etat de la transformation digitale 2020" était de comprendre où les entreprises en sont dans leurs efforts de transformation, et si Internet est déjà devenu le nouveau réseau d'entreprise. Nous nous sommes également penchés sur les défis et les obstacles rencontrés au cours de ce parcours. Étant donné que la pandémie de cette année a influencé les projets de transformation digitale et a créé une nécessité d'environnements de travail hybrides au-delà de la crise, nous avons également étudié ces domaines. Nous voulions également savoir comment les entreprises font face à la sécurisation de leurs environnements multi-cloud.

Méthodologie de l'enquête

Quoi

Atomik Research, pour le compte de Zscaler, a mené une enquête en ligne auprès d'entreprises basées au Royaume-Uni, en Allemagne, en France, aux Pays-Bas, en Suède et en Italie et comptant 3000 employés ou plus.

Qui

Au total, 606 DSI, RSSI ou responsables de l'architecture réseau impliqués dans des projets de transformation cloud ont été interrogés.

QUEL EST L'ÉTAT DE LA MIGRATION DE VOS APPLICATIONS/SERVICES VERS LE CLOUD ?

Total	Total N=606	Royaume- Uni N=101	Allemagne N=101	France N=101	Pays-Bas N=101	Suède N=101	Italie N=101
Nous avons achevé à 100 % la migration vers le cloud.	39%	38%	40%	49%	46%	23%	41%
Nous avons migré certains services/applications vers le cloud.	61%	62%	60%	51%	54%	77%	59%

Données démographiques

RÉPONDANTS PAR INTITULÉ DE POSTE

Total	Total N=606	Royaume- Uni N=101	Allemagne N=101	France N=101	Pays-Bas N=101	Suède N=101	Italie N=101
CIO	40%	52%	30%	47%	28%	23%	62%
CISO	37%	28%	43%	32%	32%	62%	26%
Responsable de l'architecture réseau	23%	20%	27%	21%	40%	15%	12%

RÉPONSES PAR TAILLE D'ENTREPRISE

Total	Total N=606	Royaume- Uni N=101	Allemagne N=101	France N=101	Pays-Bas N=101	Suède N=101	Italie N=101
3000 à 4999 employés	53%	58%	47%	52%	51%	70%	41%
5000 à 9999 employés	33%	24%	45%	37%	39%	26%	31%
Plus de 10.000 employés	13%	18%	9%	11%	10%	4%	29%

Résultats clés

A) Internet est devenu le nouveau réseau d'entreprise

L'objectif général du rapport était de déterminer à quel point les projets de transformation des entreprises répondantes sont avancés, et comment elles font face au nouveau monde du cloud et de la mobilité. Deux tiers des entreprises répondantes ont migré la majorité de leurs applications professionnelles vers le cloud, et près d'un quart des entreprises (22 %) hébergeaient plus des trois quarts de leurs applications chez un fournisseur de cloud. L'Italie est en tête avec 53 % d'entreprises ayant transféré plus de la moitié de leurs applications vers le cloud, suivie de près par le Royaume-Uni (50 %), l'Allemagne et la France (45 % chacun), puis la Suède (30 %). Les résultats de l'enquête indiquent qu'Internet a atteint le statut de nouveau réseau d'entreprise et que le cloud est devenu le nouveau data center.

Quel est le pourcentage de vos applications commerciales d'entreprise s'exécutant dans le cloud ?

Total	Royaume-Uni	Allemagne	France	Pays-Bas	Suède	Italie
Total 100%	100%	100%	100%	100%	100%	100%
Moins de 25 %	1%	4%	0%	4%	0%	0%
26 - 50%	33%	35%	26%	32%	55%	20%
51 - 75%	44%	45%	45%	44%	30%	53%
Plus de 75 %	22%	17%	30%	21%	15%	27%

Deux tiers des entreprises ont déplacé la majorité de leurs applications d'entreprise vers le cloud.

Résultats clés

Un tableau plus diversifié est présenté à travers les pays ayant fait l'objet du sondage lorsque nous avons demandé quelles applications avaient été mises en œuvre dans le cloud. Dans l'ensemble, les bases de données commerciales, le stockage de données/partage de fichiers, la sécurité Internet et les portails B2B semblent tout aussi importants, les applications financières étant légèrement en tête. La Suède mène le peloton avec près de deux tiers des personnes interrogées qui ont répondu qu'elles disposaient de bases de données commerciales (67 %), financières (66 %) et de sécurité Internet (68 %) dans le cloud, tandis que le Royaume-Uni est en tête avec le stockage/partage de fichiers (58 %) et la France prend les devants pour ce qui est de la sécurité Internet (55 %) et des portails B2B (56 %). En Allemagne, les systèmes ERP (49 %) et les portails B2B (44 %) sont couramment utilisés dans le cloud.

Quel est le pourcentage de vos applications commerciales d'entreprise s'exécutant dans le cloud ?

SUR QUEL MARCHÉ ÊTES-VOUS BASÉ ?

Total	Total N=606	Royaume- Uni N=101	Allemagne N=101	France N=101	Pays-Bas N=101	Suède N=101	Italie N=101
Suite Office	45%	39%	37%	50%	47%	52%	45%
Bases de données commerciales	50%	43%	42%	50%	44%	67%	51%
Stockage des données/ partage des fichiers	50%	58%	42%	50%	46%	60%	41%
Impression	31%	29%	40%	34%	37%	27%	19%
ERP	37%	46%	49%	45%	32%	23%	27%
Sécurité Internet	50%	42%	46%	55%	40%	68%	52%
Employés et culture (ressources humaines)	33%	35%	38%	40%	34%	31%	21%
Finances	51%	34%	43%	51%	61%	66%	50%
Outils de développement et d'ingénierie	37%	43%	33%	37%	36%	43%	34%
Portails B2B	50%	50%	44%	56%	50%	58%	40%

(Plusieurs réponses étaient possibles).

Les entreprises suédoises ont fait les plus grands progrès dans l'adoption du cloud, deux tiers ayant déplacé leurs bases de données commerciales, leurs finances et leur sécurité Internet vers le cloud.

Résultats clés

Un tiers des entreprises allemandes a tendance à conserver la suite Office (34 %) et la sécurité Internet (29 %) en interne, alors qu'à travers l'Europe, l'impression (27 %), les employés et la culture – ressources humaines – (26 %) ainsi que les outils de développement et d'ingénierie (25 %) sont toujours conservés dans le data center d'entreprise. Les entreprises suédoises sont les plus prudentes : 37 % d'entre elles n'ont aucune intention de déplacer leurs services d'impression dans le cloud. Environ un tiers des entreprises italiennes prévoient non seulement de conserver leur stockage de données/partage de fichiers en interne, mais également les outils de développement et d'ingénierie.

Quelles applications comptez-vous garder sur votre réseau d'entreprise ?

	Total N=606	Royaume- Uni N=101	Allemagne N=101	France N=101	Pays-Bas N=101	Suède N=101	Italie N=101
Total							
Suite Office	25%	30%	34%	25%	26%	21%	18%
Bases de données commerciales	22%	27%	22%	20%	26%	10%	28%
Stockage des données/ partage des fichiers	23%	15%	27%	19%	30%	14%	36%
Impression	27%	29%	25%	26%	25%	37%	22%
ERP	19%	18%	12%	21%	23%	23%	16%
Sécurité Internet	23%	29%	29%	19%	28%	14%	21%
Employés et culture (ressources humaines)	26%	20%	25%	25%	31%	29%	24%
Finances	21%	29%	27%	27%	13%	12%	27%
Outils de développement et d'ingénierie	25%	18%	22%	22%	28%	21%	33%
Portails B2B	22%	22%	22%	22%	16%	21%	32%
Autre, veuillez préciser	6%	4%	6%	4%	3%	4%	

Non seulement l'on a migré les applications commerciales vers le cloud, mais le personnel est également de plus en plus mobile. Plus de la moitié des entreprises européennes (53 %) ont plus de cinquante pour cent de leur personnel en télétravail. Dans un tiers des organisations (36 %), au moins un quart de l'effectif est à distance. Les Pays-Bas sont en tête sous le rapport du personnel en télétravail, 44 % des entreprises ayant plus de la moitié de leur effectif travaillant à distance, et près d'un tiers des entreprises ayant au moins 25 % de leur personnel travaillant du domicile. En Italie (35 %) et au Royaume-Uni (33 %), un quart du personnel n'a pas de bureau fixe, tandis qu'en Suède (44 %) et en Allemagne (42 %), près de la moitié du personnel est en télétravail.

Résultats clés

Les entreprises déplaçant leurs applications vers des fournisseurs de services cloud et offrant un modèle de travail flexible à la majorité de leurs employés, le lieu de travail du futur est déjà une réalité aujourd'hui. Les entreprises qui adoptent cette approche sont en première ligne pour devenir des entreprises sans frontières, où il n'y a plus de périmètre d'entreprise entourant le personnel. Au lieu de cela, chacun fonctionne comme s'il était sa propre filiale. Cet abandon progressif de la culture de bureau 9 h - 17 h a de sérieuses implications. Comment l'effectif peut-il être efficacement géré sans contact direct au quotidien ? Comment les équipes pourront-elles collaborer efficacement et comment mesurer la productivité du personnel ? Outre les implications en matière de RH et de gestion du personnel, le nouveau style de travail de l'entreprise doit être efficacement sécurisé. Lorsque les données ont quitté le data center et que le personnel travaille en dehors du périmètre de l'entreprise, l'organisation est exposée.

Quel pourcentage de votre personnel n'a pas de bureau (par exemple utilisateurs nomades/bureau à domicile) ?

Total	Royaume-Uni	Allemagne	France	Pays-Bas	Suède	Italie	
100%	100%	100%	100%	100%	100%	100%	
25 % ou moins	11%	20%	15%	10%	9%	5%	8%
26-50 %	36%	34%	42%	31%	30%	44%	36%
51-75 %	33%	29%	30%	31%	44%	31%	35%
76-100 %	20%	18%	14%	29%	18%	21%	22%

Dans plus de la moitié des entreprises européennes interrogées, la majorité des salariés n'ont pas d'espace de travail fixe au sein des bureaux de leur entreprise.

B) Les stratégies multicloud sont à l'ordre du jour

Avant que les entreprises n'entament leurs projets de transformation cloud, les applications d'entreprise étaient hébergées au sein du réseau d'entreprise où elles pouvaient être contrôlées et surveillées. Actuellement, les entreprises saisissent l'opportunité de déplacer leurs applications vers des sites plus économiques et plus rentables. Si les applications peuvent être hébergées n'importe où, les entreprises peuvent décider de modifier ou non l'emplacement des applications à tout moment sans affecter le service pour l'utilisateur final. Les stratégies multicloud sont en plein essor car les entreprises utilisent Internet comme nouveau réseau d'entreprise et travaillent avec plus d'un fournisseur de services cloud.

En moyenne, près de la moitié (49 %) des personnes interrogées ont déclaré opérer dans un environnement multicloud composé de deux fournisseurs de services cloud, tels qu'Amazon Web Services, Microsoft Azure ou Google. Un tiers des entreprises ont déjà trois fournisseurs. La Suède (52 %) et les Pays-Bas (42 %) sont les plus diversifiés, ayant déjà adopté trois fournisseurs de services cloud, suivis par le Royaume-Uni (30 %). En Italie et en Allemagne, la plupart des répondants travaillent avec deux fournisseurs de services cloud.

L'une des raisons d'un scénario multicloud est que les départements métiers imposent généralement le fournisseur cloud en fonction des exigences spécifiques des applications utilisées. Cela signifie que c'est généralement l'application qui choisit le cloud, et non l'inverse. Les applications d'entreprise trouveront leurs exigences mieux adaptées à un seul fournisseur cloud que les applications industrielles avec leurs cas d'utilisation spécifiques pour les développeurs.

Combien de fournisseurs de services cloud (tels que AWS, Azure, Google, SAP, etc.) utilisez-vous dans votre entreprise ?

	Total N=606	Royaume- Uni N=101	Allemagne N=101	France N=101	Pays-Bas N=101	Suède N=101	Italie N=101
Un	13%	22%	20%	11%	10%	7%	7%
Deux	49%	49%	44%	60%	45%	34%	64%
Trois	33%	27%	30%	23%	42%	52%	23%
Plus de trois	5%	3%	7%	6%	4%	7%	6%

Résultats clés

a) Les défis des stratégies multicloud

Le cloud est censé simplifier l'infrastructure d'une entreprise. Cependant, avec des scénarios multicloud, les décideurs des services informatiques sont confrontés à différents défis. Les problèmes les plus courants sont la sécurisation de l'accès aux réseaux multicloud (36 %), la configuration de réseaux multicloud (35 %) et, selon 32 % des personnes interrogées, l'augmentation des coûts au sein des réseaux MPLS. Ces défis ont un point commun : comment la structure architecturale peut-elle répondre aux exigences du personnel, d'accéder de manière transparente et sécurisée aux environnements multicloud sans augmenter les coûts et la complexité ?

	TOTAL	
TOTAL	529	100%
Configuration des réseaux multicloud	183	35%
Complexité de l'administration	156	29%
Accès pour les filiales	144	27%
Bande passante pour les filiales	155	29%
Accès pour les utilisateurs à distance	145	27%
Expérience utilisateur incohérente	162	31%
Perte de contrôle sur l'accès des utilisateurs aux applications	125	24%
Sécurisation de l'accès aux réseaux multicloud	189	36%
Performance d'accès aux applications cloud	148	28%
Gestion des fusions et acquisitions	129	24%
Coûts en hausse pour les réseaux MPLS	169	32%
Réaction lente aux événements de sécurité	139	26%

(Jusqu'à trois réponses étaient possibles).

Les entreprises sont confrontées à un dilemme commun : comment la structure architecturale peut-elle répondre aux exigences du personnel, d'accéder de manière transparente et sécurisée aux environnements multicloud sans augmenter les coûts et la complexité ?

Résultats clés

Dans une perspective pays par pays, les défis sont plus diversifiés. La configuration reste l'un des problèmes les plus courants pour 40 % des personnes interrogées en Allemagne et 38 % aux Pays-Bas et en Suède, tandis que l'expérience utilisateur incohérente est mieux classée, avec 41 % en Allemagne et 40 % aux Pays-Bas. Environ un tiers des entreprises ont des difficultés avec la bande passante pour les filiales, d'après 35 % des répondants en Allemagne, 33 % aux Pays-Bas et en Italie, suivis par 31 % en France. Un obstacle tout aussi important pour un tiers des entreprises semble être l'accès distant pour les utilisateurs finaux, choix effectué par 32 % en Allemagne et 35 % en Italie, ce qui n'est pas surprenant étant donné que l'expérience utilisateur incohérente était déjà classée comme l'un des principaux défis dans l'ensemble.

À quels défis êtes-vous confrontés dans votre configuration du réseau multicloud ?

Total	Total N=529	Royaume- Uni N=79	Allemagne N=81	France N=90	Pays-Bas N=91	Suède N=94	Italie N=94
Configuration des réseaux multicloud	35%	33%	40%	23%	38%	38%	35%
Complexité de l'administration	29%	29%	36%	21%	29%	33%	30%
Accès pour les filiales	27%	28%	31%	19%	32%	31%	23%
Bande passante pour les filiales	29%	22%	35%	31%	33%	22%	33%
Accès pour les utilisateurs à distance	27%	29%	32%	21%	24%	23%	35%
Expérience utilisateur incohérente	31%	24%	41%	32%	40%	31%	17%
Perte de contrôle sur l'accès des utilisateurs aux applications	24%	23%	32%	23%	21%	28%	16%
Sécurisation de l'accès aux réseaux multicloud	36%	30%	35%	38%	26%	38%	46%

D'où viennent les défis ?

Les entreprises sont susceptibles de se heurter à la complexité des configurations multicloud et aux problèmes de sécurité si elles s'en tiennent à leurs infrastructures de réseau traditionnelles en étoile, lorsqu'elles déplacent des applications vers le cloud. La transformation des applications, des réseaux et de la sécurité doit aller de pair pour éviter les problèmes courants. Les entreprises doivent se poser les questions suivantes :

Défi n°1 | Complexité et bande passante : comment adapter l'architecture réseau pour accéder de manière transparente et en toute sécurité aux environnements multicloud sans latence ?

Défi n°2 | Expérience utilisateur : comment faire correspondre les exigences de sécurité avec la configuration d'un réseau architectural, de sorte qu'un utilisateur n'ait plus besoin d'interagir manuellement ?

Défi n°3 | Accès distant : comment soutenir la présence d'un grand nombre d'employés répartis, ayant besoin d'un accès sécurisé à plusieurs environnements ?

C) Les plus grands moteurs de la transformation cloud : la flexibilité et l'évolutivité

Nous avons posé des questions sur les moteurs et les défis dans la première édition du rapport sur l'état de la transformation en 2019 et avons constaté certains changements dans les réactions de cette année, qui seraient dus à la pandémie mondiale. Lorsqu'on leur a demandé quels étaient les trois principaux moteurs de la transformation en 2019, les réponses les plus fréquentes étaient l'introduction de processus plus efficaces (38 %), l'octroi d'une plus grande flexibilité aux employés (37 %), la capacité de se concentrer sur les compétences de base (36 %), l'amélioration des marges bénéficiaires (36 %) et l'augmentation des économies de coûts (35 %).

En 2020, l'octroi d'une plus grande flexibilité aux employés est passé à 42 % (soit une hausse de 5 points de pourcentage), suivi de la capacité à s'adapter à la demande, d'une complexité réduite de l'administration sur site, et de la stratégie commerciale visant à se concentrer sur les compétences essentielles (tous à 40 %). L'accroissement des économies de coûts est passée à 38 % et l'amélioration des marges bénéficiaires est restée stable à 36 %.

Il existe des différences considérables au niveau de chaque pays. Le Royaume-Uni et les Pays-Bas considèrent la capacité à s'adapter à la demande (41 % et 42 % respectivement) comme plus importante cette année, alors que les aspects financiers, tels que l'augmentation des économies de coûts (41 %) ou l'amélioration de la marge bénéficiaire (42 % au Benelux) étaient dominants en 2019. Cependant, le plus important pour les entreprises britanniques est la stratégie commerciale qui consiste à se concentrer sur les compétences de base (43 %). La flexibilité pour les employés est la plus importante pour environ la moitié des entreprises en Allemagne (51 %), suivie par la capacité à s'adapter à la demande. Pour les décideurs informatiques français, des processus plus efficaces (41 %) et une amélioration des marges (40 %) sont les facteurs les plus importants, tandis que plus de la moitié des entreprises néerlandaises souhaitent réduire la complexité de l'administration sur site (54 %).

Quels ont été les principaux moteurs du transfert de vos applications professionnelles vers le cloud ?

Total	Total	Royaume-Uni	Allemagne	France	Pays-Bas	Suède	Italie
Introduire des processus plus efficaces	38%	36%	30%	41%	31%	43%	49%
Donner plus de flexibilité aux employés	42%	37%	51%	37%	37%	48%	44%
Capacité à s'adapter à la demande	40%	41%	46%	37%	42%	45%	31%
Complexité réduite de l'administration sur site	40%	36%	42%	39%	54%	28%	34%
Stratégie d'entreprise pour se concentrer sur les compétences de base	40%	43%	39%	33%	42%	41%	43%
Améliorer la marge bénéficiaire	36%	37%	40%	40%	30%	43%	30%
Accroître les économies de coûts	38%	38%	43%	34%	31%	38%	44%

D) Le plus grand défi de la transformation cloud : la sécurité

Dans l'enquête de l'année dernière, la sécurité était en tête de liste des principaux obstacles à la transformation dans toutes les régions pour près d'un quart des décideurs (23 %), le Royaume-Uni étant le plus préoccupé (28 %), suivi de l'Allemagne (26 %). Vient ensuite la complexité des projets de transformation, mentionnée par 13 % des décideurs, suivie de près par le manque d'expertise (12 %).

Il n'est pas surprenant que la sécurité occupe toujours la première place avec une importance d'ailleurs plus grande cette année – 42 % des répondants à travers l'Europe ont fait état de difficultés dans ce domaine. Les coûts et le manque d'expertise interne ont été cités par plus d'un tiers des personnes interrogées (36 %), suivis de près par la complexité (35 %). Au niveau de chaque pays, l'Italie (50 %) est la plus préoccupée par la sécurité, suivie du Royaume-Uni et de l'Allemagne (46 %), puis de la Suède (43 %).

Les plus grands défis en France sont les coûts (47 %), suivis par la culture d'entreprise (35 %). Aux Pays-Bas, les préoccupations des salariés concernant le maintien de leur emploi (40 %) sont toujours dominantes, comme l'année dernière. L'insécurité professionnelle a également été soulevée comme un problème par des répondants britanniques (43 %) et suédois (39 %). Ceci est en corrélation avec les difficultés rencontrées dans les deux pays en ce qui concerne le manque d'expertise interne, de même qu'en Suède (44 %) et aux Pays-Bas (37 %). Cette question est également classée dans le haut de l'échelle en Italie (42 %) et en Allemagne (41 %). L'expertise en matière de cloud semble moins problématique en France, où elle n'est mentionnée que par 25 % des entreprises, et au Royaume-Uni, où elle n'est évoquée que par 32 % des répondants.

Ces résultats montrent que si le cloud procure des avantages aux utilisateurs finaux et aux entreprises, il entraîne également d'énormes bouleversements pour les architectes réseau chargés de superviser cette migration transformationnelle. Il est tout à fait compréhensible que ce changement perturbe les architectes réseau qui luttent pour se forger un avenir dans un écosystème résolument tourné vers le cloud.

Dans notre enquête de 2019, 23 % des entreprises interrogées ont déclaré que la sécurité était leur plus grande préoccupation. En 2020, ce chiffre est passé à 42 %.

Résultats clés

Le réseau d'entreprise est sous la responsabilité de l'architecte réseau, mais le cloud sape son importance, ce qui à son tour atténue le travail des architectes réseau. Cependant, on pourrait être tenté de conclure que le problème n'est pas un manque de compréhension technique autour du cloud, mais plutôt une réticence à changer. S'accrocher aux anciens styles de travail peut préserver un sentiment de pertinence pour les architectes réseau. Des architectes plus visionnaires pourraient voir des possibilités d'adapter leur expertise au nouveau style d'architecture réseau pour valider à nouveau leurs positions et apporter la connaissance de l'entreprise aux déploiements dans le cloud.

Quels ont été les principaux défis liés à la migration de vos applications professionnelles vers le cloud ?

Total	Total N=606	Royaume- Uni N=101	Allemagne N=101	France N=101	Pays-Bas N=101	Suède N=101	Italie N=101
Coût	36%	28%	37%	47%	39%	32%	38%
Complexité	35%	38%	43%	34%	34%	33%	32%
Préoccupations en matière de sécurité	42%	46%	46%	32%	36%	43%	32%
Manque d'expertise interne sur le cloud	36%	32%	41%	25%	37%	44%	42%
Engagement actuel en faveur des solutions sur site	32%	28%	39%	28%	38%	41%	22%
Inquiétude des employés quant à la conservation de leur emploi	34%	43%	31%	30%	40%	39%	25%
Culture d'entreprise	30%	32%	35%	35%	25%	27%	25%

E) Influence du télétravail sur la transformation cloud

Avant la crise du coronavirus, le « lieu de travail du futur » était un sujet largement discuté mais souvent au bas de la liste des priorités. Du jour au lendemain, la pandémie a radicalement changé la façon dont les entreprises travaillent, obligeant les équipes informatiques à rapidement transférer le personnel des bureaux vers le domicile, puis à passer aux solutions de travail à distance pour assurer la continuité d'activité et préserver la productivité de l'entreprise.

Le télétravail a nécessité des ajustements importants pour les organisations et les employés. Cependant, l'introduction de mesures de distanciation sociale a fait que les modèles de lieu de travail flexibles sont devenus une réalité bien plus rapidement que ce que de nombreuses entreprises auraient jamais imaginé. Que les employés aient perçu ou non leur expérience de télétravail comme positive ou négative se résume souvent à une chose : le statut de la transformation cloud au sein de leur entreprise. En transférant les applications et les données vers le cloud, et en passant à une infrastructure compatible avec le cloud, les entreprises ont pu jeter les bases d'un travail agile.

Nous avons voulu savoir comment les entreprises ont réagi à la pandémie mondiale en ce qui concerne leurs projets de transformation cloud et avons constaté que près d'un quart (22 %) des entreprises européennes étaient déjà passées à une stratégie 100 % cloud. Alors que 33 % affirmaient que leur transformation cloud n'a pas été affectée, un nombre égal a déclaré que la pandémie a accéléré leur migration vers le cloud. Les projets cloud ont été ralentis dans seulement 12 % des entreprises.

Sur la base d'une évaluation pays par pays, 61 % des répondants en Italie ont déclaré que la pandémie n'avait pas affecté leur feuille de route pour le cloud, mais les entreprises allemandes et néerlandaises ont redéfini les priorités des projets et les ont fait avancer respectivement dans 60 % et 50 % des entreprises interrogées. Le Royaume-Uni (33 %) et la France (34 %) ont indiqué que, dans environ un tiers des entreprises, la COVID-19 n'a pas affecté leur feuille de route pour le cloud, tandis qu'un quart des entreprises ont accéléré leurs projets (23 % au Royaume-Uni et 28 % en France). En Suède, un peu moins d'un tiers a décidé d'aller de l'avant comme prévu et de faire avancer les projets (31 %).

Résultats clés

Comment la crise sanitaire mondiale a-t-elle influencé le rythme des projets de transformation cloud au cours des derniers mois ?

Total	Total N=606	Royaume- Uni N=101	Allemagne N=101	France N=101	Pays-Bas N=101	Suède N=101	Italie N=101
Nous avons déjà mis en place une stratégie 100 % cloud avant la pandémie.	22%	26%	17%	29%	20%	23%	18%
La COVID n'a pas affecté notre feuille de route de transformation cloud.	33%	33%	10%	34%	27%	31%	61%
Les priorités des projets cloud ont été avancées.	33%	23%	60%	28%	50%	31%	9%
Les priorités des projets cloud ont été ralenties.	12%	18%	13%	10%	4%	16%	11%
Aucune réponse	0%	1%	0%	0%	0%	0%	1%

Nous voulions avoir une idée de la façon dont les entreprises prévoient de s'adapter au télétravail comme étant la nouvelle norme. Près de la moitié (48 %) des personnes interrogées s'attendent à ce que, dans les 12 prochains mois, l'on note une augmentation d'entre 25 à 50 % du nombre de télétravailleurs. Ceci est vrai pour 27 % des personnes interrogées au Royaume-Uni et pour 49 % en Allemagne.

Comment envisagez-vous que le pourcentage du personnel sans bureau (utilisateurs nomades/bureau à domicile) dans votre entreprise change au cours des 12 prochains mois ?

Total	Total N=606	Royaume- Uni N=101	Allemagne N=101	France N=101	Pays-Bas N=101	Suède N=101	Italie N=101
Restera stable	14%	8%	7%	8%	3%	36%	24%
Augmentera de 10 %	19%	14%	6%	29%	16%	19%	33%
Augmentera de 25 %	24%	27%	27%	24%	30%	17%	22%
Augmentera de 50 %	23%	27%	49%	14%	32%	10%	10%
Augmentera de 75 %	5%	7%	6%	5%	6%	0%	5%
Nous envisageons 100 % du personnel en télétravail	1%	1%	1%	2%	0%	1%	2%
Le personnel en télétravail va décroître	13%	17%	5%	19%	14%	18%	5%

F) Le défi : sécuriser l'accès distant à l'ère du télétravail

La sécurité ayant été citée comme l'un des principaux obstacles à la transformation cloud, nous avons voulu savoir quels systèmes de sécurité les entreprises utilisent pour connecter leurs travailleurs mobiles aux applications d'entreprise. Les solutions traditionnelles, telles que Remote Desktop Protocol (RDP), étaient utilisées par un tiers des entreprises (33 %), suivies de près par les solutions d'accès distant VPN (30 %). Moins d'un cinquième des entreprises (19 %) utilisaient une solution de gestion des identités et des accès (IAM) et seulement 17 % avaient adapté un concept zero trust.

Comment vos employés mobiles et distants accèdent-ils aux applications d'entreprise sur le réseau ou dans le cloud ?

SUR QUEL MARCHÉ ÊTES-VOUS BASÉ ?

Total	Royaume-Uni N=101	Allemagne N=101	France N=101	Pays-Bas N=101	Suède N=101	Italie N=101	
Via une solution d'accès distant VPN	30%	36%	16%	52%	22%	18%	38%
Via le protocole RDP (Remote Desktop Protocol)	33%	45%	24%	37%	44%	18%	32%
Via une solution zero trust	17%	9%	35%	7%	32%	13%	9%
Via la gestion de l'identité et de l'accès (IAM)	19%	11%	26%	4%	3%	51%	22%

En jetant un regard plus granulaire, d'énormes différences sont devenues apparentes. Alors que plus de la moitié des décideurs informatiques en France s'appuyaient encore sur les accès distant VPN, 51 % d'experts suédois avaient en place une solution IAM. En Allemagne et aux Pays-Bas, environ un tiers des entreprises avaient déployé un modèle zero trust. Au Royaume-Uni, la solution dominante (à 45 %) était le RDP, suivi du VPN à 36 %. En Italie, le VPN venait en tête avec 38 %.

Près de la moitié des entreprises en Italie (48 %), en France (46 %) et au Royaume-Uni (45 %) étaient persuadées d'avoir en place une infrastructure sécurisée d'accès distant, tandis que les Pays-Bas (44 %) et la Suède (41 %) n'étaient pas aussi confiants. L'Allemagne (43 %), la Suède (38 %) et les Pays-Bas (34 %) évaluaient déjà de nouvelles solutions de sécurité en fonction des exigences du nombre croissant du personnel en télétravail. À travers l'Europe, 34 % des entreprises suivaient la même stratégie, mais seulement 4 % avaient des plans concrets pour passer vers une nouvelle solution dans les 12 à 24 prochains mois.

Résultats clés

Dans quelle mesure votre entreprise est-elle convaincue que le personnel en télétravail peut accéder en toute sécurité aux applications du réseau d'entreprise et au cloud ?

Total	Total N=606	Royaume- Uni N=101	Allemagne N=101	France N=101	Pays-Bas N=101	Suède N=101	Italie N=101
Nous sommes persuadés d'avoir en place une infrastructure sécurisée d'accès distant	33%	45%	22%	46%	22%	18%	48%
Nous ne sommes pas certains d'avoir en place une infrastructure sécurisée d'accès distant	29%	18%	29%	28%	44%	41%	16%
Nous évaluons de nouvelles solutions de sécurité en fonction des exigences du nombre croissant du personnel en télétravail	34%	34%	43%	24%	34%	38%	32%
Nous projetons de mettre en place, au cours des 12 à 24 prochains mois, une nouvelle solution de sécurité pour le personnel distant en pleine expansion	4%	4%	7%	3%	1%	4%	5%

Étant donné que 34 % des entreprises évaluent de nouvelles solutions, nous avons voulu savoir si elles envisageaient de migrer vers un modèle SASE (Secure Access Service Edge) basé sur le cloud, lequel de manière dynamique autorise ou refuse les connexions au service en fonction des politiques définies par l'entreprise.

Plus d'un tiers des entreprises européennes (36 %) connaissaient déjà le cadre et disposaient de plans pour une transition complète en une seule étape, tandis qu'un peu plus d'un quart (26 %) n'avaient encore aucun plan et que près d'un cinquième (19 %) prévoyaient une transition lente vers SASE. Les partisans les plus progressistes du concept étaient l'Allemagne et la Suède, avec près de la moitié des leurs entreprises prévoyant d'adopter le SASE (49 %), suivies de 41 % des entreprises des Pays-Bas. Nous avons également constaté que 11 % des entreprises étaient déjà en train de mettre en œuvre l'approche SASE. En France, à peu près le même nombre d'entreprises envisageaient de maintenir leur solution existante (28 %) que celles qui planifiaient une lente migration (27 %). Le même nombre avait des plans pour une transition rapide. Et seulement une petite minorité (4 %) à travers l'Europe n'était pas encore familiarisée avec le concept.

Près de la moitié des entreprises allemandes et suédoises prévoient d'adopter le modèle SASE, suivies par les Pays-Bas avec 41 %.

Résultats clés

Comment décririez-vous la connaissance et/ou l'adoption de SASE par votre organisation ?

Total	Total N=606	Royaume- Uni N=101	Allemagne N=101	France N=101	Pays-Bas N=101	Suède N=101	Italie N=101
Nous n'avons pas encore entendu parler/discuté de SASE	4%	5%	2%	8%	6%	0%	5%
Nous avons entendu parler du SASE, mais n'avons pas l'intention d'adopter cette approche	26%	18%	23%	28%	34%	35%	21%
Nous avons entendu parler du SASE, et nous avons des plans pour passer lentement à cette approche (par exemple, des filiales, suivies d'entités mobiles, puis les sièges sociaux, etc.)	19%	33%	11%	27%	14%	7%	26%
Nous avons entendu parler du SASE, et nous planifions la transition pour toutes nos entités en même temps	36%	27%	49%	27%	41%	49%	23%
Nous sommes en train de passer à une approche SASE	11%	15%	14%	8%	6%	10%	13%
Nous sommes déjà passés à une approche SASE	3%	3%	2%	3%	0%	0%	13%

Explorant davantage les bénéfices potentiels d'une approche SASE, la moitié des personnes interrogées dans la zone EMEA ont déclaré que le principal avantage est la réduction du risque de menaces à la sécurité et de perte de données; 39 % ont cité l'amélioration de la visibilité et du contrôle du réseau sur tous les utilisateurs et toutes les plate-formes cloud, et 38 % ont déclaré que cela permet à l'équipe informatique d'être un moteur de croissance et de contribuer au résultat net. Plus d'un tiers (36 %) ont mentionné une complexité réduite/une agilité accrue de l'infrastructure.

La moitié des répondants britanniques ont déclaré que le principal avantage est que cela permet à l'équipe informatique d'être un moteur de croissance et de contribuer au résultat net, suivi par la réduction de la complexité/augmentation de l'agilité à 42 %.

Résultats clés

Les répondants des cinq marchés restants ont tous déclaré que le principal avantage était la réduction du risque de menaces de sécurité et de perte de données à travers les données distribuées (48 % en Allemagne, 47 % en France, 54 % aux Pays-Bas, 76 % en Suède et 45 % en Italie). Les décideurs informatiques allemands ont également déclaré qu'il était important pour eux d'améliorer la visibilité et le contrôle du réseau pour tous les utilisateurs et les plate-formes cloud, à 44 % (contre 43 % pour la Suède), et de permettre aux services informatiques de devenir un moteur de croissance (43 %).

Lesquels de ces potentiels avantages du SASE sont les plus intéressants pour le service informatique de votre organisation ?

Total	Total N=606	Royaume- Uni N=101	Allemagne N=101	France N=101	Pays-Bas N=101	Suède N=101	Italie N=101
Capacité à évoluer globalement et dynamiquement en fonction de la demande	31%	31%	33%	33%	34%	29%	29%
Complexité réduite/agilité accrue des infrastructures	36%	42%	37%	29%	38%	34%	40%
Une meilleure expérience utilisateur, non affectée par la latence	30%	25%	33%	25%	34%	34%	28%
Risques réduits des menaces de sécurité et de pertes de données à travers les données distribuées	50%	33%	48%	47%	54%	76%	45%
Permet à l'équipe informatique d'être un moteur de croissance et de contribuer au résultat final	38%	50%	43%	34%	33%	34%	37%
Visibilité et contrôle réseau améliorés sur l'ensemble des utilisateurs et des plate-formes cloud	39%	43%	44%	35%	37%	43%	32%
Coûts informatiques réduits	32%	34%	42%	32%	23%	20%	41%
Aucun	0%	0%	0%	1%	0%	0%	1%

La moitié des entreprises britanniques ont déclaré que le principal avantage du SASE est qu'il permet aux équipes IT d'être au cœur de la croissance et de contribuer à la rentabilité

Conclusion

Auparavant, les applications d'entreprise étaient hébergées au sein du réseau de l'entreprise où elles pouvaient être contrôlées et surveillées par l'entreprise. L'adoption des technologies du cloud a pris de l'ampleur et le télétravail devient la nouvelle norme. Cependant, les entreprises risquent de se heurter à la complexité des configurations multicloud ainsi qu'aux problèmes de sécurité si elles s'accrochent à leurs traditionnelles infrastructures de réseau en étoile.

Le modèle SASE défini par Gartner semble trouver un écho auprès des entreprises européennes pour améliorer la sécurité et rétablir la visibilité et le contrôle du réseau pour tous les utilisateurs et réseaux. SASE repose sur le concept selon lequel le fait de se fier au data center comme centre de gravité du réseau d'une entreprise n'a aucun sens dans un monde où de plus en plus d'applications migrent vers le cloud et où les utilisateurs accèdent aux réseaux partout et à tout moment, à partir d'une multitude d'appareils.

L'idée du service à la périphérie (Service Edge) rapproche le calcul et les services au plus près des utilisateurs, ce qui garantit une latence minimale entre le terminal et l'application. Ce modèle contraste nettement avec les services par connectivité réseau, car il est simple, évolutif et flexible, avec une faible latence et une sécurité élevée.

SASE aura des répercussions considérables sur les services informatiques des entreprises. Les services seront à la périphérie, loin des mécanismes ou des fonctionnalités internes du réseau. De ce fait, les utilisateurs n'ont besoin de savoir ni où se trouve un réseau, ni où est hébergée une application. Internet devenant le nouveau réseau, la dépendance au réseau physique va diminuer et il y aura moins de dépendance à l'IT en tant que service interne d'une entreprise.

Sur la base de la recommandation de Gartner selon laquelle les entreprises orientées vers un monde cloud et mobile doivent restructurer les modèles d'accès à leurs services, nous avons voulu, dans la dernière partie de l'enquête, savoir dans quelle mesure les entreprises sont avancées dans le suivi du cadre SASE. Comme nous l'avons vu, une majorité d'entreprises acceptent déjà le cloud comme nouveau réseau d'entreprise, et plus de 66 % des répondants ont plus de 50 % de leurs applications dans le cloud. Nous voulions donc savoir s'ils progressent de la même manière dans l'adaptation de leur infrastructure de sécurité pour répondre aux exigences de l'ère du cloud.

Le personnel mobile ne s'inquiète pas quant au point de stockage de ses applications. Ils exigent un accès transparent quel que soit l'emplacement où ils travaillent et peu importe l'endroit où sont hébergées les applications. En outre, les professionnels de l'IT doivent se sentir à l'aise avec le fait qu'ils doivent reprendre le contrôle dans un paysage de plus en plus mobile où le périmètre traditionnel n'existe plus.

Les décisions technologiques sont essentielles pour obtenir la productivité et la protection de l'entreprise, ainsi que pour donner aux leaders informatiques la possibilité de mener à bien la transformation. Les technologies traditionnelles centrées sur le réseau et sur lesquelles les équipes s'appuient depuis plus de 30 ans, telles que les accès distants VPN, ont frustré les utilisateurs et sont maintenant utilisées comme canal pour les cyberattaques. Dans un monde désormais tourné vers le travail en tout lieu, les équipes IT doivent passer à une solution d'accès basée sur le cloud, dans leurs efforts d'adaptation aux besoins de l'entreprise dans un environnement en constante mutation.

Recommandations

Avant même la crise de la COVID-19, le « lieu de travail du futur » était un sujet largement abordé, mais souvent au bas de la liste des priorités. Cependant, l'introduction de mesures de distanciation sociale a fait que les modèles de lieu de travail flexibles sont devenus une réalité bien plus rapidement que ce que de nombreuses entreprises auraient jamais imaginé. Que les employés aient perçu ou non leur expérience de télétravail comme positive ou négative se résume souvent à une chose : le statut de la transformation cloud au sein de leur entreprise.

En transférant les applications et les données vers le cloud, et en passant à une infrastructure compatible avec le cloud, les entreprises ont pu jeter les bases d'un travail agile. Le modèle SASE de Gartner décrit le dispositif de sécurité d'un tel environnement de travail mobile ainsi que les moyens de surmonter les difficultés telles que la limitation de la bande passante, l'incohérence de l'expérience utilisateur et le manque de visibilité.

Pour mettre en œuvre un personnel distant productif et sécurisé, les entreprises devraient évaluer leur infrastructure en fonction des exigences technologiques suivantes :

- **Expérience des utilisateurs** – Pour offrir la meilleure expérience utilisateur et éviter les tickets au support informatique, les solutions d'accès doivent prendre en charge divers types d'appareils et avoir une présence importante et distribuée. Plus de points de présence signifie moins de latence et une expérience utilisateur plus rapide et plus productive pour ceux qui travaillent à domicile, de même que lorsqu'ils retourneront au bureau.
- **Politiques basées sur l'identité** – Connecter un utilisateur autorisé à une application spécifique en fonction du contexte (identité, posture des appareils, etc.), et jamais au réseau. Cela permettra de fournir un moyen de connexion plus granulaire, de réduire les mouvements latéraux sur le réseau et de minimiser l'exposition à Internet des ressources commerciales critiques.
- **Simplicité et évolutivité** – Exploitez les technologies fournies dans le cloud et qui s'intègrent bien pour simplifier la gestion. Par exemple, pensez aux plate-formes SASE (Secure Access Service Edge), qui incluent les services ZTNA (Zero Trust Network Access), CASB (Cloud Access Security Broker), et plus encore. Les plate-formes SASE s'intègrent aux fournisseurs d'identité modernes, tels qu'Okta, Azure Activity Directory et Ping Identity, ainsi qu'aux logiciels de gestion des terminaux utilisateurs, tels que CrowdStrike et Carbon Black. Étant donné que la plate-forme est fournie dans le cloud, le service informatique peut facilement augmenter le nombre d'utilisateurs distants sans avoir à se soucier de la capacité.
- **Visibilité** – Les services en ligne d'accès au cloud fournissent de nombreuses informations sur qui accède à quelles applications, à partir de quel appareil et d'où. Cela inclut l'inspection des données chiffrées dans le protocole SSL. Les logs de trafic peuvent ensuite être acheminés vers Splunk, Sumo Logic ou vers un autre service syslog pour permettre de minimiser le temps de correction en cas de violation et réagir rapidement en cas d'activité suspecte.

À propos de Zscaler

Le plus grand cloud du monde - une plate-forme de sécurité née dans et pour le cloud

La plate-forme Zscaler a été construite dès le départ pour permettre aux clients de passer en toute sécurité au monde moderne – un monde dans lequel le cloud est le nouveau data center et Internet le nouveau réseau où les échanges ont lieu. C'est aussi un monde où les employés peuvent travailler en toute sécurité de n'importe où. La plate-forme Zscaler a été développée pour garantir que les entreprises pourraient fonctionner en toute sécurité et rester productives alors que les applications quittent le data center et que les utilisateurs s'éloignent du réseau.

Distribué à travers plus de 150 data centers dans le monde, Zero Trust Exchange de Zscaler, basé sur SASE, est la plus grande plate-forme de sécurité cloud au monde. Elle alimente les quatre solutions Zscaler, notamment Zscaler Internet Access, qui sécurise les connexions à Internet et aux applications SaaS et protège contre les cybermenaces; Zscaler Private Access, qui fournit un accès zero trust aux applications privées dans le cloud et au data center sans VPN; Zscaler Cloud Protection, qui sécurise les charges de travail en utilisant la micro-segmentation et en identifiant les mauvaises configurations du cloud; et Zscaler Digital Experience, qui fournit une visibilité sur le chemin complet entre l'utilisateur et l'application pour identifier les problèmes de performance. Chaque année depuis 2011, Zscaler est un leader du Magic Quadrant de Gartner pour les passerelles Web sécurisées.

Avec plus de 10 ans d'expérience dans le développement, l'exploitation et l'évolutivité du cloud, Zscaler sert des entreprises clientes du monde entier, y compris 450 des entreprises Forbes Global 2000. Le cloud Zscaler traite 120 milliards de transactions par jour, bloquant 100 millions de menaces et de violations de politiques. En plus de protéger les clients, il leur permet de réduire les coûts, de diminuer la complexité et d'améliorer l'expérience utilisateur en éliminant les piles d'appliances de passerelle qui créent des latences.

Zscaler a été fondée en 2008 avec pour mission de faire du cloud un lieu sûr pour faire des échanges et une expérience plus productive pour les utilisateurs en entreprise. La plate-forme de sécurité dédiée de Zscaler met en place les défenses et les contrôles de l'entreprise là où se produisent les connexions – Internet – de manière à ce que chaque connexion soit rapide et sécurisée, peu importe comment et où les utilisateurs se connectent ou alors où sont hébergées leurs applications et charges de travail.

Zscaler a accompagné des centaines d'entreprises dans leur transformation numérique de manière sécurisée. Contactez-nous pour faciliter votre transformation.

Plus d'informations :

Regardez la vidéo de deux minutes pour découvrir les avantages d'une architecture basée sur le cloud.

Découvrez comment Zscaler a aidé Siemens dans sa transformation numérique.

[zscaler.fr](https://www.zscaler.fr)

