CLOUDFLARE

E-BOOK

La connectivité cloud

Une approche pour reprendre le contrôle de l'informatique et de la sécurité

Sommaire

Les entreprises perdent le contrôle de l'informatique et de la sécurité

Par le passé, les équipes responsables de l'informatique et de la sécurité se concentraient principalement sur la gestion de l'environnement sur site de leur entreprise. Toutefois, lorsque les besoins opérationnels ont évolué, que les bases de clients sont devenues mondiales et que le télétravail s'est enraciné dans le panorama des entreprises, ces équipes spécialistes de la technologie se sont vues confier des responsabilités dans davantage de domaines : **les déploiements cloud, les applications SaaS et l'Internet public.**

Pris individuellement, chaque domaine connaît déjà plus que sa part de considérations complexes en matière de gestion et de sécurité. Or, la perte de contrôle résulte d'une combinaison de plusieurs facteurs :

- Chacun de ces domaines est différent, tant sur le plan de la finalité première et du modèle opérationnel que sur celui du modèle de sécurité. Ils constituent, dans les faits, des super-silos contenant en eux-mêmes leurs propres silos.
- Les environnements situés hors du périmètre du pare-feu sont intrinsèquement moins visibles pour les équipes responsables de l'informatique et de la sécurité, car l'infrastructure, les points de contrôle des accès et les utilisateurs sont contrôlés par des fournisseurs externes – ou, dans le cas de l'Internet public, ne sont pas contrôlés du tout.
- Au regard de la connectivité, les attentes telles que « any-to-any (point à point), à tout instant et partout » produisent des combinaisons pratiquement infinies d'équipements, de logiciels, de services, de protocoles, de normes, de conventions et d'exigences réglementaires qui, en pratique, sont infinies.

Il n'est guère étonnant que les équipes responsables de la technologie disposent de moins en moins de contrôle tandis qu'elles s'efforcent de réunir ces domaines disparates sous la forme d'un environnement unique, capable de répondre à leurs besoins opérationnels.

Cet aspect complique fortement les tâches cruciales, telles que la gestion des accès des collaborateurs et la définition de politiques de sécurité mondiales, ainsi que la surveillance et l'amélioration des performances des réseaux, et il est difficile de trouver une entreprise au sein de laquelle cette perte de contrôle ne s'est pas installée.

Selon une récente étude de Cloudflare réalisée par Forrester Research, 99 % des entreprises déclarent n'avoir jamais eu autant besoin qu'aujourd'hui d'une connectivité « any-to-any » (c'est-à-dire de point à point) sécurisée et performante.

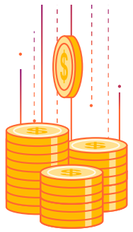
Une nouvelle étude révèle les effets étendus de cette « faille de contrôle » sur l'entreprise dans son ensemble, sous la forme d'une perte de vitesse et de productivité, mais également d'un accroissement des risques et des coûts.

Vitesse et productivité

La perte de contrôle ralentit les entreprises. Les équipes responsables de la technologie passent plus de temps à tester et à sécuriser les systèmes complexes. La dette technologique et la complexification des exigences en matière d'infrastructure s'accumulent. Enfin, les dates de lancement des nouvelles applications sont retardées, laissant aux start-ups plus agiles une chance de remporter le match en matière d'innovation.

Risques

La perte de contrôle amplifie les risques dans divers domaines, tels que la cybersécurité, la conformité aux lois et aux politiques, ou encore la stabilité opérationnelle. Ces risques peuvent s'accumuler lentement, mais les conséquences frappent souvent de manière soudaine et publique, sous la forme d'attaques par rançongiciel dévastatrices, de données dérobées et proposées publiquement à la vente, ou de ralentissements logistiques invalidants.



Coûts

La perte de contrôle réclame un lourd tribut en termes d'opportunité : l'incapacité des équipes spécialistes de la technologie à se concentrer sur les initiatives permettant d'ajouter de la valeur à l'entreprise. Le coût est également déterminé par la nécessité d'engager davantage de collaborateurs (et d'acheter davantage d'outils) afin d'apporter un semblant d'ordre aux environnements technologiques complexes.

« La vaste majorité de notre parc informatique exécute MacOS et bon nombre de nos développeurs les plus essentiels travaillent sous Linux. La compatibilité limitée de [nos fournisseurs de gestion des accès] a souvent retardé nos lancements, et leur capacité à fonctionner avec Linux était non existante. »

Head of Security, cabinet de conseil en matière de cloud

« Nous dépensions beaucoup d'argent, mais nous n'avions pas de visibilité sur notre empreinte numérique mondiale. Nous ne disposions d'aucune information sur la manière dont nous étions attaqués, le moment où ces attaques survenaient ou l'identité de ceux qui s'en prenaient à nous. »

Global Director of Governance, Risk, Compliance, and Security, fournisseur de pièces automobiles

« Nous connaissons une croissance très rapide et les réglementations internationales en matière de confidentialité évoluent en permanence. Nous avons besoin d'agilité et de la capacité d'évoluer rapidement et efficacement. Les solutions que nous utilisions n'étaient pas suffisamment robustes pour supporter notre croissance. »

Chief Technical Officer, entreprise de technologies de protection de la confidentialité

La connectivité cloud :

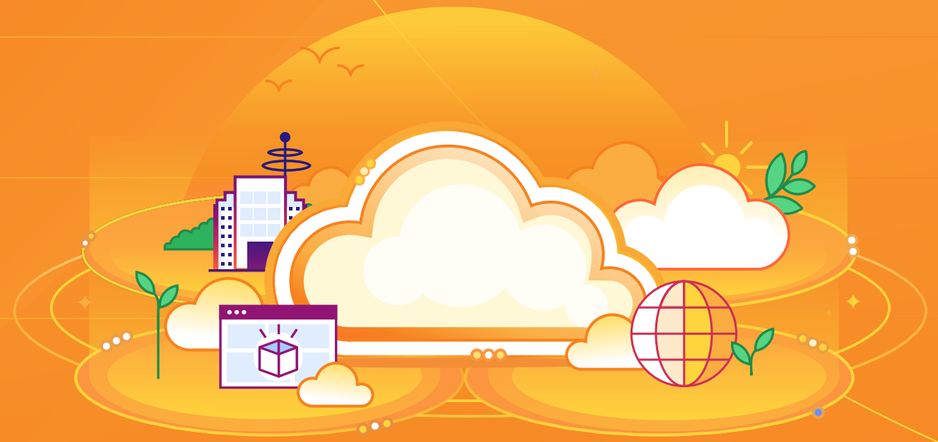
une nouvelle approche pour connecter, protéger et accélérer votre entreprise

Les entreprises ne peuvent remédier à la faille de contrôle dans leur environnement informatique en déployant des optimisations isolées et des produits dédiés plus nombreux. Une nouvelle approche est nécessaire.

Elles ont besoin d'un type de cloud différent, capable d'assurer une connectivité sécurisée, performante et de point à point (« any-to-any »). Ce cloud doit pouvoir s'intégrer à tous les réseaux, proposer une programmabilité totale afin de prendre en charge n'importe quel scénario d'utilisation, tout en assurant une visibilité et un contrôle unifiés sur l'ensemble des domaines dont le service informatique est responsable.

Ce nouveau modèle de cloud s'appelle la **connectivité cloud**. Grâce à son architecture programmable, à ses possibilités d'intégration à l'ensemble des réseaux, à son intelligence et à ses innovations intégrées, sans oublier son interface unifiée, ce modèle offre les avantages suivants aux entreprises :

- La possibilité de faire évoluer sans effort les ressources de sécurité, de connectivité réseau et d'amélioration des performances, afin de répondre à n'importe quelle exigence opérationnelle.
- Une connectivité transparente pour tous vos domaines : réseaux sur site, déploiements cloud, applications SaaS et Internet public.
- Davantage de ressources et d'heures de travail à investir dans l'innovation stratégique en matière d'informatique et de sécurité.
- Une meilleure prévisibilité lors du lancement de nouveaux produits et services ou de mises à jour technologiques.
- Une meilleure expérience pour vos clients, afin de renforcer votre avantage concurrentiel.
- Une meilleure expérience pour vos collaborateurs, avec pour résultat une amélioration de la productivité, de l'efficacité et de l'agilité opérationnelle.



L'anatomie de la connectivité cloud

La connectivité cloud est un nouveau type de cloud qui connecte **toutes les ressources** et **tous les utilisateurs** à l'environnement informatique, **partout** où ils se trouvent.

Toutefois, il est tout aussi important de s'attacher à ce qu'elle n'est **pas**. De nombreuses plateformes dans le cloud proposent des services de sécurité, des services réseau ou des services pour développeurs depuis le cloud. Or, sans la possibilité de couvrir l'ensemble de ces scénarios d'utilisation ou de se connecter facilement à chaque domaine de l'environnement informatique, ces plateformes ne constituent qu'un nouveau silo.

L'entreprise se retrouve alors avec un énième nouvel outil à intégrer, une visibilité réduite et un plus grand nombre d'incohérences au niveau de la gestion, soit autant d'exemples répandus de perte de contrôle.

À l'inverse, la connectivité cloud possède les **qualités architecturales** suivantes, tout en servant les utilisateurs/domaines suivants :

Qualités architecturales :

- Intégration native et universelle à Internet
- Intelligence et innovations transversales intégrées
- Architecture composable et programmable
- Interface unifiée et simplifiée

Domaines et utilisateurs connectés et protégés :

- Collaborateurs hybrides et sur site
- Développeurs
- Clients
- Partenaires et sous-traitants
- Déploiements multi-cloud
- Réseaux hybrides et sur site

Examen approfondi : l'architecture de la connectivité cloud

Une architecture composable et programmable :

La connectivité cloud est fondamentalement conçue pour être adaptable et compatible. Plus spécifiquement :

- Chaque méthode de connectivité et chaque service cloud sont interopérables les uns avec les autres, dans chaque emplacement réseau.
- La connectivité des couches 1 à 7 est entièrement programmable par API, partout et à tous les niveaux.
- La connectivité cloud est découplée de la pile technologique (aux extrémités) et de l'emplacement.
- Vous pouvez développer vos propres fonctions serverless prenant en charge les API sur les mêmes serveurs tous les autres services de la solution de connectivité cloud.

Par conséquent, les entreprises peuvent :

- Refuser tout compromis en matière de sécurité, de connectivité réseau et d'innovation lorsqu'elles basculent entre les clouds (IaaS, PaaS, SaaS), les réseaux sur site ou les utilisateurs (client, collaborateur, partenaire).
- Orchestrer et automatiser les services avec n'importe quel système tiers.
- Personnaliser les règles de régionalisation des données afin de répondre aux exigences en matière de conformité, de confidentialité et de souveraineté.

Une intégration native et universelle à Internet :

L'architecture de la connectivité cloud est profondément intégrée à Internet. De manière plus spécifique, elle propose :

- Une infrastructure située dans un grand nombre de villes et de points d'échange Internet (IXP), pas uniquement quelques datacenters par région.
- Le contrôle total sur une requête, de la source à la destination, pas uniquement via une couche superposée ou sous-jacente définie par logiciel.
- Une connectivité réseau capable d'évoluer indéfiniment à la demande, dans n'importe quel emplacement, sans étape de configuration lors de la mise en place ou de l'exploitation.
- Des services toujours disponibles sur chaque serveur, tout en étant indépendants des fournisseurs de cloud et de la géolocalisation, quelle que soit l'origine.
- Une connectivité depuis n'importe quelle source automatiquement routée vers chaque datacenter, afin d'assurer une disponibilité permanente du service.

Par conséquent, les entreprises bénéficient :

- D'une faible latence pour tout utilisateur, application et infrastructure réseau connectés à Internet.
- De l'absence d'équipements matériels ou virtuels à activer, gérer ou faire évoluer.
- D'un plan de contrôle pour l'ensemble des services, exécuté sur tous les serveurs, afin d'assurer une cohérence opérationnelle de 100 %.

Intelligence et innovations intégrées

Une solution de connectivité cloud propose :

- L'absence de chaînage de services interne ou externe aux datacenters.
- Des fonctions d'amélioration de la sécurité, des performances, de la confidentialité et de la conformité sont intégrées, plutôt que mises en œuvre a posteriori.
- Un système transversal d'information sur les menaces, qui identifie la plupart des attaques existantes et les ressources que vous essayez de protéger.
- Un système d'information sur les menaces transversal qui supervise l'ensemble des chemins Internet et peut accélérer n'importe quelle requête en l'aiguillant vers l'itinéraire le plus rapide.

Par conséquent, les entreprises bénéficient des avantages suivants :

- De meilleures informations sur les menaces, notamment via des modèles d'apprentissage automatique (Machine Learning) continuellement renforcés.
- Une meilleure connectivité et une meilleure expérience utilisateur.
- L'absence de compromis – par exemple, la nécessit de devoir désactiver des services de sécurité pour assurer la disponibilité ou la conformité d'une application.
- Un développement plus rapide, car les fonctions de sécurité, d'amélioration des performances et de la conformité sont intégrées aux nouvelles applications serverless.

Interface unifiée et simplifiée

Une solution de connectivité cloud propose :

- Une interface de gestion unifiée sur l'ensemble d'une plateforme produit intégrée.
- Des fonctions de journalisation consolidées, dotées d'intégrations à tous les services de stockage de journaux dans le cloud et toutes les plateformes d'analyse des données (par exemple, SIEM).

Par conséquent, les entreprises bénéficient :

- De processus simplifiés en termes de mise à jour des politiques, de création de comptes utilisateur et d'autres tâches de sécurité quotidiennes.
- Des processus simplifiés en termes de configuration et de gestion des ressources professionnelles (sur site ou dans le cloud), ainsi que des autres tâches réseau quotidiennes.
- D'une formation plus rapide des collaborateurs.
- De procédures plus simples en matière de dépannage et de support client.
- D'une consolidation des fournisseurs plus efficace.

Scénarios d'utilisation de la connectivité cloud

Pour comprendre de quelle manière la connectivité cloud peut aider une entreprise à connecter efficacement l'ensemble de ses équipements et de ses utilisateurs à son environnement informatique, prenons l'exemple d'une enseigne de prêt-à-porter fictive nommée Acme Inc. Les opérations d'Acme couvrent sept pays, avec 40 magasins physiques et une activité d'e-commerce florissante. L'entreprise dispose de sept agences et emploie 3 000 personnes, dont 30 % sont en télétravail, partiel ou total.

Scénario d'utilisation : rationaliser la sécurité réseau de l'entreprise

Les opérations multinationales et les effectifs hybrides d'Acme constituent un terreau fertile pour une perte de contrôle. L'établissement de connexions sécurisées entre une diversité d'endroits, d'appareils, d'applications et d'éléments d'infrastructure peut rapidement devenir une tâche particulièrement chronophage.

Grâce à la connectivité cloud, Acme peut à la fois sécuriser et connecter l'ensemble de ces composants réseau sur une plateforme unique, sans intégrations complexes ni solutions de contournement, peut-être même en conservant une approche SASE (Secure Access Service Edge, service d'accès sécurisé en périphérie).

Scénario d'utilisation : créer une stratégie de sécurité cohérente sur l'ensemble du catalogue en ligne

Acme gère de nombreux sites web pour ses diverses marques et régions, sans même parler des cohortes d'API qui se connectent à ces sites par l'intermédiaire de services tiers. Sans infrastructure unifiée en matière de sécurité, Acme ne dispose pas d'une visibilité précise et cohérente sur les menaces visant son catalogue en ligne – un exemple classique de perte de contrôle.

Grâce à la connectivité cloud, Acme peut suivre toutes les menaces depuis un panneau unique, avant d'appliquer efficacement les nouvelles politiques et les modifications des politiques à l'ensemble du catalogue.

Scénario d'utilisation : accélérer le développement et les tests

Acme lance constamment de nouvelles fonctionnalités et expériences sur l'ensemble de son catalogue en ligne. Toutefois, les ingénieurs et les responsables web risquent de crouler sous le fardeau des tâches de dimensionnement d'applications, d'intégrations de produits de sécurité et d'amélioration des performances et d'autres tâches de déploiement chronophages, au risque d'opposer l'un à l'autre le contrôle et la vitesse.

Grâce à la connectivité cloud, toutes les considérations ci-dessus sont soit intégrées, soit entièrement automatisées. Il est donc plus simple pour les équipes d'Acme de se concentrer sur le développement et les tests.

Scénario d'utilisation : tous les cas ci-dessus

Contrairement à de nombreux services, une solution de connectivité cloud peut répondre à l'ensemble des scénarios d'utilisation ci-dessus en s'appuyant sur une infrastructure et une interface utilisateur uniques. Dans une telle situation, l'efficacité de la solution s'en trouverait d'ailleurs amplifiée. Une sécurité réseau plus efficace aiderait les équipes responsables de l'informatique et du web à gérer plus facilement la présence en ligne. L'intégration de services d'amélioration de la sécurité, des performances et du développement améliorerait, dans son ensemble, l'agilité du moteur d'innovation de l'entreprise. La connectivité cloud devient une plateforme pour tous les objectifs de transformation numérique d'Acme.

Un meilleur contrôle sur l'environnement informatique bénéficie à l'entreprise

Fonctionnalité de la connectivité cloud	Avantages pour l'équipe technologique	Avantages étendus pour l'entreprise
Meilleure connectivité pour chaque utilisateur, application et réseau	• Les utilisateurs peuvent facilement utiliser leurs outils préférés • Moins de tickets transmis au support informatique	• Adoption facilitée des technologies innovantes • Risque d'informatique fantôme (Shadow IT) réduit
Simplification des tâches quotidiennes de gestion de la sécurité et des réseaux	• Gestion facilitée des politiques de sécurité, des profils utilisateur, des règles de routage, etc.	• Plus de temps pour travailler sur les technologies innovantes • Réponse plus agile aux menaces émergentes
Meilleur système d'information sur les menaces	• Réponse aux menaces plus rapide et plus efficace	• Réduction des risques organisationnels
Circulation facilitée entre les infrastructures cloud et sur site	• Application de n'importe quel service de sécurité à n'importe quelle infrastructure • Intégrations plus rapides	• Transformation numérique plus rapide • Contrôle facilité des données critiques
Orchestration et automatisation des services avec n'importe quel système tiers	• Intégrations plus rapides • Adoption facilitée des meilleurs services cloud du marché	• Transformation numérique plus rapide • Meilleure productivité des collaborateurs
Aucun équipement virtuel à activer, gérer ou faire évoluer	• Développement logiciel plus efficace	• Lancement plus rapide de produits numériques • Meilleure expérience numérique pour le client
Plan de contrôle unique pour l'ensemble des services, exécuté sur tous les serveurs	• Gestion facilitée de l'informatique et de la sécurité • Réduction de la lassitude liée aux alertes de sécurité	• Plus de temps pour travailler sur les technologies innovantes • Réduction des risques organisationnels
Sécurité, performances et conformité sans compromis	• Réponse facilitée aux exigences de conformité • Pas de nécessité de désactiver les services de sécurité pour réduire le risque pour la conformité	• Expansion régionale et verticale facilitée • Réduction des risques organisationnels

Cloudflare tient ses promesses en termes de connectivité cloud

Le réseau Cloudflare constitue la première plateforme de connectivité cloud du monde. Il aide les responsables des technologies dans les entreprises à réduire le temps passé, les risques et les coûts liés à la gestion de leurs collaborateurs, leurs appareils, leurs systèmes, leurs applications, leurs clouds et leurs réseaux. Il a été conçu depuis le départ pour proposer aux clients, aux collaborateurs et aux développeurs des entreprises une expérience unifiée au sein d'un environnement éminemment complexe et distribué en matière de puissance de calcul, de stockage et d'applications.

Il tient cette promesse grâce aux caractéristiques suivantes :

Une architecture composable et programmable : tous les services Cloudflare peuvent s'exécuter sur chaque serveur de notre réseau et sont totalement indépendants de tout matériel spécifique. En outre, il est particulièrement simple de personnaliser les règles de routage, les politiques d'accès et le code grâce à notre service de développement serverless, Workers (qui s'exécute partout où opèrent également nos autres services

Une portée universelle, mondiale et Internet-native : le réseau Cloudflare couvre plus de 300 villes à travers le monde et est interconnecté à plus de 12 500 FAI, services cloud et entreprises. Cette particularité lui permet d'être présent à environ 50 ms de 95 % de la population mondiale connectée à Internet.

Intelligence et innovations transversales : Cloudflare achemine approximativement 20 % du trafic web mondial et bloque plus de 140 milliards de menaces chaque jour. Ce réseau et notre système d'information sur les menaces soutiennent l'ensemble de notre catalogue de services d'amélioration de la sécurité, des performances, de la confidentialité, de la conformité et du développement.

Une interface unifiée et simplifiée : celle-ci vous permet de gérer votre sécurité Zero Trust, votre connectivité réseau, vos services d'amélioration de la sécurité et des performances des applications, vos services de développement, votre conformité, votre confidentialité et bien d'autres aspects depuis une interface unique.

Les entreprises mondiales utilisent Cloudflare pour reprendre le contrôle de l'informatique et de la sécurité

« La technologie d'informations statistiques sur la sécurité de Cloudflare me montre exactement ce qui se passe sur l'ensemble de notre empreinte numérique… La capacité d'entrer dans une salle de réunion et d'annoncer "Voici les attaques que nous subissons, voici d'où elles viennent et voici comment nous allons les bloquer" est un outil particulièrement puissant. »

GPC

« Nous savons si un appareil sur le réseau a été infecté par un logiciel malveillant. Nous pouvons couper instantanément une connexion, sécuriser nos systèmes importants et appliquer des mesures correctives à une machine infectée. L'intégration de Cloudflare à Crowdstrike renforce notre stratégie de sécurité générale… Nous avons [également] constaté des avantages en termes de satisfaction des développeurs et de maintenance simplifiée. »

STAX

« Comme Cloudflare Workers dispose d'une architecture fortement distribuée, je n'ai pas besoin de passer du temps avec mon équipe à chercher comment garantir une disponibilité maximale aux fonctionnalités que nous développons. Notre délai de mise sur le marché a été accéléré de manière spectaculaire, et nous savons que tout ce que nous codons via Workers sera conforme à nos contrats de niveau de service (SLA) au regard de la disponibilité élevée »

onetrust

« Cloudflare simplifie la migration de nos propriétés sur site vers le cloud. À mesure que nous faisons appel à différents services cloud publics, Cloudflare nous sert de point de contrôle indépendant et unifié, en nous offrant la flexibilité stratégique nécessaire au choix de la solution cloud la plus adaptée à notre travail et la possibilité d'effectuer facilement des modifications en aval. »

Handelsblatt MEDIA GROUP

Sommaire

Téléphone : +33 75 7 90 52 73
E-mail : enterprise@cloudflare.com
Site web : www.cloudflare.com/fr-fr/

RÉV. : BDES-5059.2023SEP19