CLOUDFLARE

LIVRE BLANC

Améliorer le niveau de cybersécurité en période d'incertitude économique

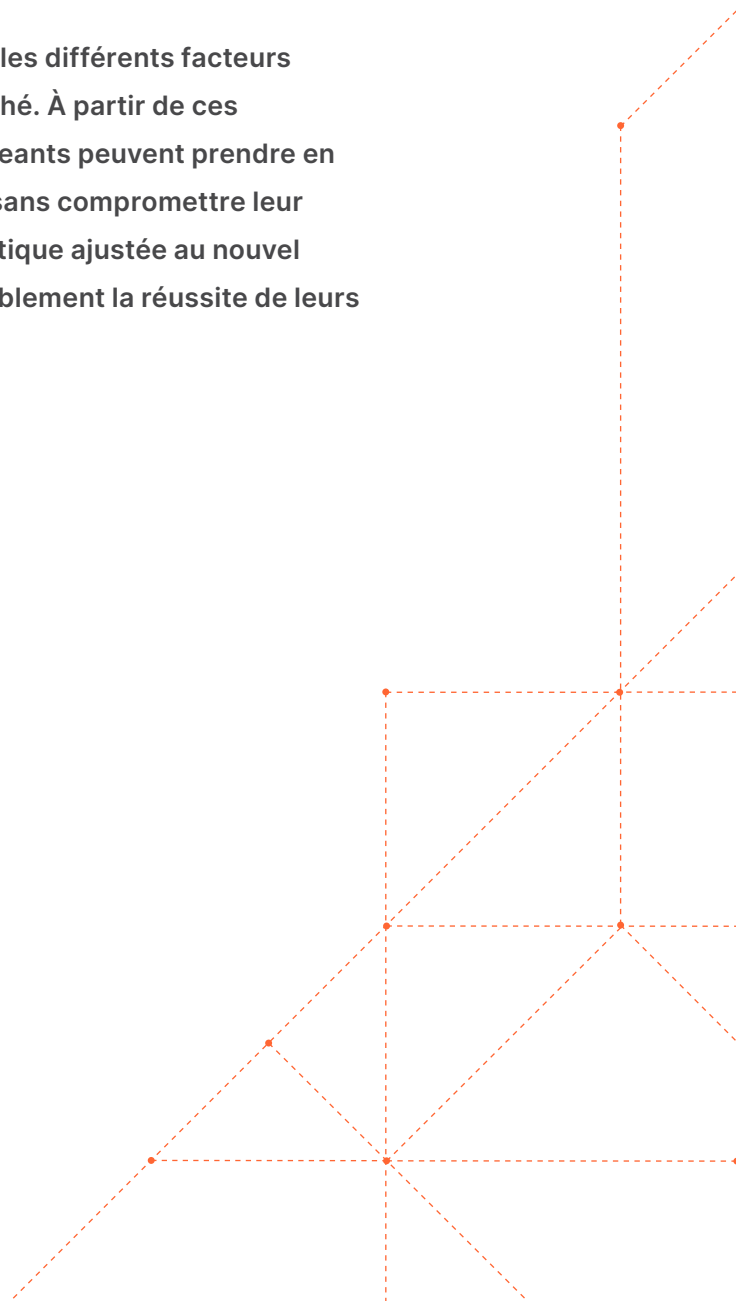
Contenu

Synthèse

Les entreprises sont confrontées à une incertitude économique, tandis que les perspectives deviennent de plus en plus imprévisibles. Cette incertitude, qui se matérialise sous la forme de restrictions budgétaires, contraint les DSI et les responsables techniques à trouver de nouvelles voies à suivre.

Heureusement, les dirigeants peuvent encore s'assurer un bon positionnement à la fin de cette période d'incertitude. Pour affronter les turbulences liées à ce contexte, ils doivent adopter une stratégie proactive, impliquant le réalignement des budgets, la redéfinition des processus pour plus d'efficacité et la poursuite des plans de croissance sans augmentation substantielle des ressources.

Dans cette publication, nous définirons et développerons les différents facteurs à l'origine de ces circonstances et ces conditions de marché. À partir de ces informations, nous définissons cinq mesures que les dirigeants peuvent prendre en vue de rendre leurs pratiques de sécurité plus efficaces, sans compromettre leur niveau de sécurité. Une stratégie d'infrastructure informatique ajustée au nouvel environnement économique leur permet de préparer durablement la réussite de leurs entreprises.



Introduction

Depuis quelques années, les responsables informatiques doivent affronter des crises successives, tandis qu'ils planifient et exécutent leur stratégie. Ils ont dû réagir à une pandémie mondiale et à ses effets secondaires, à des pénuries affectant la chaîne d'approvisionnement, à l'intensification d'un conflit en Europe de l'Est et à l'éventualité d'une récession. Selon les termes de l'économiste de Stanford Paul Romer, « Il est regrettable de manquer l'occasion qu'offre une crise » (source). Les choix qu'ont faits les directeurs de l'information pour soutenir leur personnel à distance offriront des avantages durables et imprévus, en rendant leurs lieux de travail attrayants et propices au télétravail. De même, à l'heure où les dirigeants sont confrontés à une détérioration des perspectives économiques, les choix qu'ils font en matière de sécurité, de connectivité réseau, d'accès à distance, de stockage, de développement et d'infrastructure aideront leurs entreprises à ressortir plus fortes et mieux positionnées pour une croissance durable et sécurisée à l'avenir.

L'essor du télétravail s'est accompagné d'une explosion des rançongiciels et des cybermenaces sophistiquées, qui ont atteint de nouveaux sommets en termes d'impact sur les revenus, d'ampleur et de sophistication (source). L'évaporation de ce qu'il restait du périmètre du réseau, associée à une augmentation historique des renouvellements de personnel, a engendré des lacunes en matière de sécurité et des retards dans les projets informatiques stratégiques. Ceci a contraint les organisations à repenser à la fois leur approche du recrutement et de la fidélisation, mais également leur stratégie de contrôle des accès à leurs systèmes et machines. Bien que la pandémie ait donné lieu à une augmentation spectaculaire de la cybercriminalité (source), elle a également ouvert les yeux des organisations et de leurs conseils d'administration sur l'urgente nécessité d'une cybersécurité efficace. L'heure est maintenant venue d'adopter une approche plus stratégique du laborieux déploiement d'une infrastructure de travail hybride sécurisée, productive et disponible.

Voici cinq choses que vous pouvez faire pour réduire les risques pour votre activité sans dépasser votre budget et améliorer la capacité de votre entreprise à gérer les menaces émergentes qui se profilent à l'horizon :

1. Réalisez un audit des outils de sécurité existants afin d'identifier les chevauchements de fonctionnalités

Les entreprises ont tout intérêt à consolider leurs fournisseurs de solutions de sécurité. Bien qu'aucun outil ne puisse apporter à lui seul la solution miracle dont rêvent les RSSI, de nombreux opérateurs de sécurité estiment que leur entreprise perd de l'argent en utilisant un trop grand nombre d'outils qui, par ailleurs, offrent une défense insuffisante. Le recours à une multitude d'outils de différents fournisseurs signifie que vos collaborateurs consacrent un temps précieux à l'acquisition, à la mise en œuvre, à la gestion, au dépannage et au support d'un grand nombre de systèmes déconnectés, plutôt qu'à la sécurisation de votre infrastructure et de vos données. D'ailleurs, une enquête réalisée en juin 2022 lors de l'édition annuelle de la RSA Conference a établi que « la moitié (53 %) des entreprises interrogées ont l'impression d'avoir gaspillé plus de 50 % de leur budget consacré à la cybersécurité sans être en mesure de remédier aux menaces. 43 % des personnes interrogées disent que la première difficulté à laquelle ils se heurtent en matière de détection et d'élimination des menaces est la surabondance d'outils, tandis que 10 % des entreprises ne disposent pas d'outils efficaces pour remédier aux menaces relatives à la cybersécurité » (source). Il suffirait de se débarrasser d'une poignée de ces outils pour améliorer la sécurité, tout en faisant gagner un temps précieux à vos collaborateurs.

En transférant les investissements des dépenses en capital vers les dépenses d'exploitation, vous pouvez également améliorer immédiatement la trésorerie à court terme et éviter de vous enfermer dans des investissements pluriannuels qui entravent l'agilité opérationnelle. Une approche de la simplification consiste à réduire la dépendance à l'égard des équipements traditionnels. La transition des boîtiers traditionnels vers les solutions « en tant que service » peut contribuer à assurer que vos initiatives les plus prioritaires continuent à bénéficier d'un financement, même en cas de diminution des budgets. L'adoption du modèle « en tant que service » vous permet également de bénéficier des cycles d'innovation intrinsèquement plus rapides des logiciels et d'éliminer la problématique de l'application fréquente de correctifs sur les matériels anciens. Déléguer les responsabilités liées à l'innovation et la mise en œuvre de correctifs permet à votre équipe de se concentrer sur les activités vraiment différenciatrices de votre entreprise. Face à l'incertitude, la simplification et la consolidation stratégiques sont des facteurs de réussite à long terme.

2. Concentrez-vous sur les données, et pas seulement sur les outils

Les équipes de direction devraient s'intéresser davantage à une meilleure intégration non seulement des outils, mais également des données dans tous leurs ensembles d'outils de sécurité, afin de permettre une meilleure identification des modèles et des anomalies. Traditionnellement, les équipes de sécurité ont continué à ajouter des suites d'outils au fil du temps, sans prendre en compte les conséquences à long terme d'un trop grand nombre d'ensembles de données disséminés dans un trop grand nombre d'emplacements. Souvent, il en découle un patchwork de produits dont l'interopérabilité est faible ou nulle, ainsi qu'une opacité des données entraînant des informations moins exploitables et moins précises, qui introduisent à leur tour des risques d'erreur humaine. Par ailleurs, pour une équipe, la nécessité d'extraire plusieurs ensembles de données, de les fusionner, puis d'exécuter des requêtes peut représenter une perte de temps, mais également un gaspillage de ressources. Au lieu de cela, ces ressources pourraient être affectées à des initiatives opérationnelles plus stratégiques.

Même si les équipes sont en mesure de trouver des solutions créatives pour résoudre les difficultés d'interopérabilité (telles que la fusion manuelle des ensembles de données ou l'importation et l'exportation de fichiers CSV), il est important de tenir compte du fait qu'au-delà de l'efficacité, la valeur des outils de sécurité réside dans les données que ces systèmes assimilent, créent et mettent à la disposition du personnel chargé de la défense de l'infrastructure. Si vos données sont disséminées aux quatre coins de votre infrastructure et ne sont ni classifiées, ni sécurisées, ni soigneusement gérées, cela peut altérer la pertinence des informations que vous pouvez en extraire. C'est particulièrement le cas si des données résident dans des instances d'informatique fantôme (Shadow IT) pouvant avoir été entièrement omises. La consolidation des ensembles d'outils et une réflexion attentive à l'interopérabilité de votre pile de sécurité vous permettent de limiter les erreurs humaines et de mieux sécuriser vos données. En effet, même si vous avez investi dans les meilleurs outils actuellement disponibles, des ensembles de données cloisonnés et fantômes se traduisent par des informations insatisfaisantes.

Du point de vue de l'efficacité, il est important de prendre en compte qu'à l'ère de la sécurité Zero Trust (« Ne jamais faire confiance, toujours vérifier »), la multiplication des outils signifie que les équipes passent plus de temps à se connecter, à s'authentifier et à accéder aux systèmes avant de commencer à travailler. Si un collaborateur n'a besoin d'interagir qu'avec un nombre limité de systèmes, cela lui permet de gagner du temps et d'intervenir plus rapidement. Il est essentiel d'avoir conscience que les données contenues dans ces systèmes, ainsi que le nombre de systèmes auxquels un collaborateur doit accéder pour exécuter une tâche, vont au final favoriser ou grever la capacité des équipes à répondre, plutôt que réagir, aux menaces en temps opportun.

3. Envisagez l'adoption de modèles « en tant que service » dans le cloud pour une innovation maximale et une complexité minimale

Chaque entreprise a besoin d'innover pour rester compétitive, mais si la cybersécurité n'est pas son secteur d'activité, elle ne disposera pas du temps, du budget ou des ressources nécessaires pour suivre l'évolution des vulnérabilités CVE, des tendances des attaques et des correctifs critiques indispensables pour préserver la sécurité de l'ensemble de son infrastructure. L'adoption de modèles « en tant que service », lorsqu'elle est possible, permet aux dirigeants de bénéficier d'une innovation continue sans devoir faire de compromis ou prendre des décisions difficiles concernant leur dette technique.

Il est aussi important de noter que certains services de sécurité facturent des frais de dépassement des limites de trafic ou des frais de bande passante. Examinez attentivement ce que votre entreprise paie chaque mois ou chaque année, afin de déterminer si ces dépenses sont supérieures à ce que vous pensiez. Si c'est le cas, vous pouvez saisir cette opportunité pour rechercher d'autres solutions ne facturant pas les dépassements. Ainsi, non seulement vous économiserez de l'argent, mais vos dépenses à long terme seront plus prévisibles, ce qui permettra à votre équipe de mieux planifier l'avenir.

Les services de cette nature proposés via le cloud offrent également à votre entreprise la possibilité de se développer ou de se recentrer en fonction des besoins, sans investir dans des racks de matériel coûteux, dont la gestion du cycle de vie est problématique. En cette période d'incertitude, les entreprises doivent rester agiles et réactives face aux fluctuations des conditions du marché. Lorsque la trésorerie est une préoccupation, la capacité de minimiser les coûts, voire de les éliminer complètement est un avantage stratégique qui peut faire la différence entre la survie et la prospérité – quelles que soient les conditions du marché.

4. Transformez l'expérience de vos collaborateurs

Forbes indique : « Notre enquête révèle que les processus de connexion complexes, en plusieurs étapes, sont une source de frustration pour les employés : ils leur font perdre leur temps, grèvent leur productivité et les incitent à abandonner des tâches essentielles liées à leur travail… Ironiquement, près de 40 % déclarent avoir remis à plus tard, délégué, voire complètement ignoré la mise en place de nouvelles applications de sécurité au travail en raison de la lourdeur des processus de connexion. Cela revient à protéger votre domicile avec le portail le plus solide, le plus haut et le plus sécurisé que l'on puisse acheter (renforcé par des dragons crachant des rayons laser), puis à le laisser ouvert la nuit. » Non seulement il est inefficace et difficile pour le personnel responsable de la défense de l'infrastructure de se souvenir de quel outil héberge quelle fonction, mais la multiplication des tableaux de bord et des emplacements où résident les données entraîne des risques de sécurité majeurs et des lacunes en matière de visibilité pour n'importe quelle entreprise. Celles qui souhaitent garder une longueur d'avance sur les menaces de cybersécurité doivent être conscientes que chaque clic et chaque frappe de clavier nécessitent du temps et de l'énergie précieux et détournent l'attention des événements critiques auxquels le personnel doit répondre. Afin d'offrir aux collaborateurs une expérience améliorée et rationalisée, les dirigeants doivent impérativement examiner de près le nombre d'outils que doivent utiliser le personnel responsable de la défense de l'infrastructure pour effectuer son travail efficacement, de même que ce qu'il est possible d'éliminer ou de consolider pour réduire le temps dont ces collaborateurs ont besoin pour répondre, pas seulement réagir, à un événement de sécurité critique.

Dans le cas des collaborateurs n'exerçant pas de fonctions techniques et n'intervenant pas dans la défense de l'infrastructure, il ne faut pas négliger le fait que les télétravailleurs souhaitant accroître leur productivité personnelle peuvent se tourner vers l'informatique fantôme (Shadow IT) ou des méthodes de contournement. Bien que les contrôles Zero Trust fournissent des perspectives prometteuses pour la création d'entreprises plus sécurisées, en particulier dans un environnement distant, il est évident que toutes les approches ne sont pas équivalentes. Plus il est complexe pour un collaborateur d'accéder aux ressources dont il a besoin, plus il sera tenté de trouver un moyen de contourner les contrôles de sécurité, plutôt que de les respecter. Les dirigeants doivent non seulement s'efforcer de comprendre l'efficacité des produits de sécurité, mais également tenir compte de la facilité d'utilisation : ignorer l'expérience des collaborateurs revient à augmenter le risque global pour l'entreprise.

5. Identifiez les coûts dissimulés et les possibilités d’amélioration des performances dans votre pile de cybersécurité actuelle

Plutôt que les outils eux-mêmes, c'est la façon dont vous les configurez et les gérez qui peut faire toute la différence. Vous devez envisager de demander à vos équipes d'effectuer un audit des configurations et personnalisations actuelles afin d'identifier des possibilités d'optimiser les performances. S'il s'avère impossible d'améliorer ces dernières, vous pouvez rechercher des solutions conçues dès le départ dans cette optique. En effet, un objectif de performances ajouté après coup permet rarement d'atteindre le but recherché par les dirigeants. En matière de performances réseau, n'oubliez pas qu'il est impossible de défaire et refaire le code d'une architecture insatisfaisante. De la même façon que les possibilités de redessiner les plans d'un immeuble sont limitées une fois les fondations en place, les réseaux doivent être intégralement créés dans l'optique de performances optimales.

L’accès à la puissance d'un réseau périphérique mondial, capable de traiter et gérer les données au plus près de la source, confère aux entreprises un avantage stratégique, aujourd'hui et à l'avenir. Selon la publication MIT Technology Review, « Le traitement de volumes de données peut entraîner des problèmes de performances. En réponse, de nombreuses entreprises se tournent vers l'informatique de périphérie (“edge computing”), permettant de traiter les données à proximité de la source pour une analyse et une réponse rapides en temps réel, tout en respectant les exigences en matière de confidentialité et de sécurité » (source). En optant pour des solutions fondées sur les architectures de demain, vous pouvez donner à vos équipes l'avantage stratégique de meilleures performances réseau sans sacrifier les éléments essentiels de la confidentialité et de la sécurité.

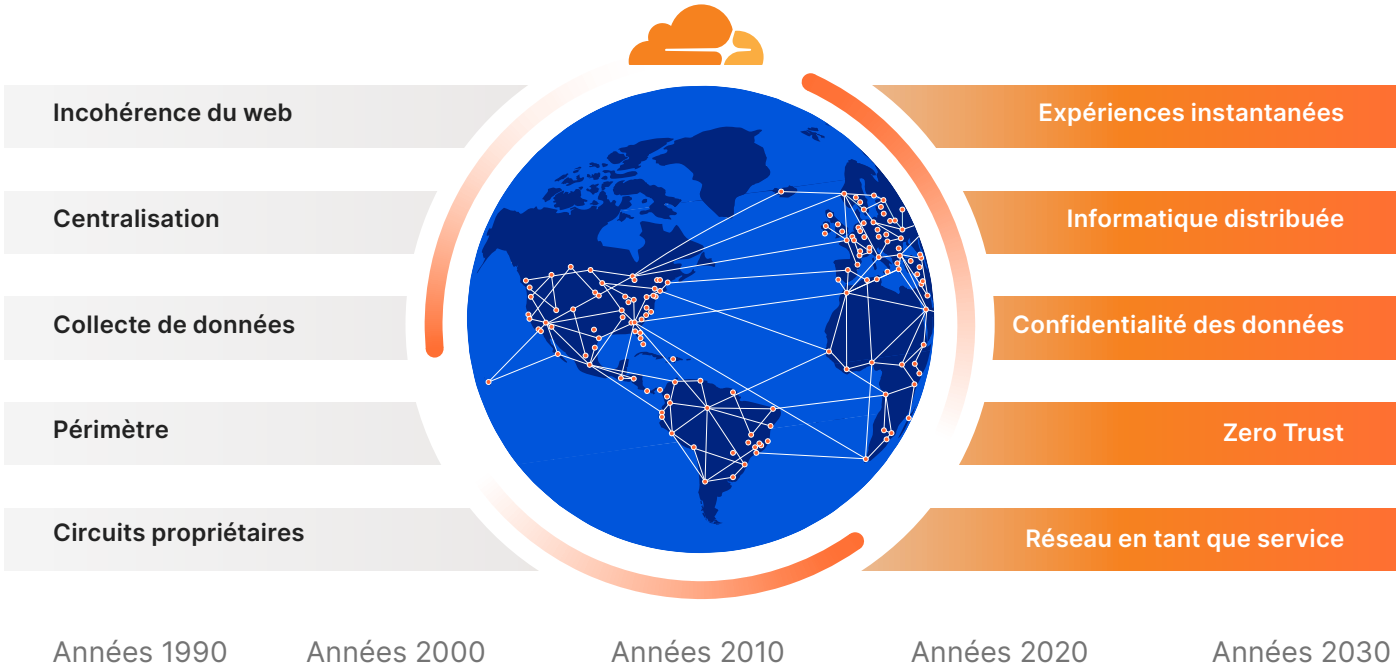
En résumé, pour améliorer le niveau de cybersécurité en période d'incertitude, vous pouvez prendre les mesures suivantes :

1. **Réalisez un audit des outils de sécurité existants pour identifier les chevauchements de fonctionnalités**
   - Consolidez les outils qui se chevauchent
   - Transférez les investissements des dépenses en capital vers les dépenses d'exploitation
2. **Concentrez-vous sur les données, et pas seulement sur les outils**
   - L'interopérabilité des outils procure des ensembles de données améliorés et plus précis
   - Des ensembles de données et des rapports plus précis offrent de meilleures informations, qui sont cruciales pour atteindre les objectifs opérationnels
3. **Envisagez l'adoption de modèles « en tant que service » dans le cloud pour une innovation maximale et une complexité minimale**
   - Si la cybersécurité n'est pas votre secteur d'activité, vous avez tout intérêt à déléguer la gestion des correctifs, de la maintenance et des mises à jour et à opter pour des offres « en tant que service »
   - Les modèles cloud et « en tant que service » offrent la flexibilité indispensable pour préserver votre agilité dans un environnement économique fluctuant
4. **Transformez l'expérience de vos collaborateurs**
   - Un trop grand nombre d'outils disséminés dans un trop grand nombre d'emplacements peut créer des lacunes en termes de sécurité et susciter de la frustration chez les collaborateurs. La consolidation et la simplification favorisent l'optimisation de leur expérience
   - Optimiser la facilité d'utilisation des solutions pour les collaborateurs permet de fidéliser ces derniers et de les dissuader de se tourner vers l'informatique fantôme (Shadow IT) pour effectuer leur travail
5. **Identifiez les coûts dissimulés et les possibilités d'amélioration des performances dans votre pile de cybersécurité actuelle**
   - Réalisez un audit des outils existants afin d'identifier les possibilités d'améliorer les performances ; toutefois, n'oubliez pas que vous ne pouvez pas optimiser une architecture insatisfaisante
   - L'adoption d'outils de portée mondiale établis au plus près de la localisation prévue de vos clients permet à votre entreprise de proposer une expérience client optimale et sécurisée

Ce que Cloudflare peut vous apporter

Cloudflare a été fondée en 2010, au lendemain de la crise économique de 2008, avec la volonté d'être un leader de la transition des infrastructures sur site vers le cloud. Nous avons conçu la plateforme de Cloudflare autour d'un objectif audacieux : contribuer à bâtir un Internet meilleur. La suite de produits proposée par Cloudflare protège et accélère toutes les applications connectées à Internet, sans nécessiter d'ajout de matériel, d'installation de logiciels ou de modification de lignes de code.

Cloudflare redirige et achemine l'ensemble du trafic web des propriétés Internet qu'elle héberge sur son réseau mondial intelligent, qui apprend de chaque requête. Nous aidons nos clients à travailler plus intelligemment, à construire plus solidement, à opérer plus rapidement et à se développer en toute sécurité. Aujourd'hui, Cloudflare protège et accélère des millions de propriétés Internet.



Contrôle

Bénéficiez de la puissance d'un réseau mondial intégré offrant une connectivité, une sécurité et une puissance de calcul exhaustives, tout en vous laissant le contrôle de vos politiques.

Flexibilité

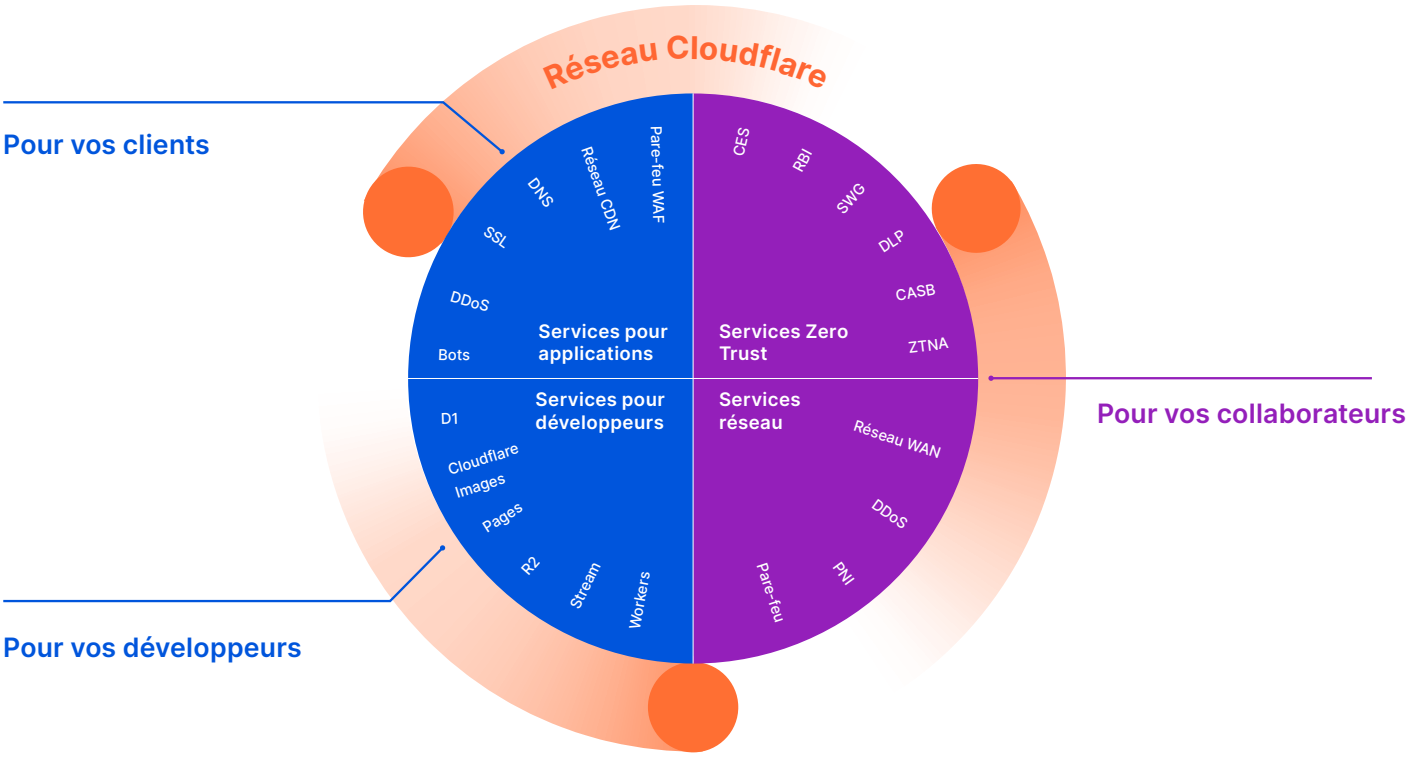
Grâce aux services cloud-native, aucune dépense d'investissement n'est nécessaire. Vous pouvez facilement augmenter ou diminuer l'utilisation en fonction des fluctuations de votre activité.

Prévisibilité

Une facturation prévisible, sans coûts inattendus tels que des frais de trafic sortant déplafonnés. Vous évitez ainsi de réaliser des dépenses d'investissement maintenant pour acheter des équipements qui ne seront livrés que l'année prochaine.

Grâce au réseau mondial de Cloudflare, tous les équipements connectés à Internet sont sécurisés, privés, rapides et fiables.

- **Sécurisez** vos sites web, vos API et vos applications Internet.
- **Protégez** vos réseaux d'entreprise, vos employés et vos équipements.
- **Créez** et **déployez** du code exécuté à la périphérie du réseau.



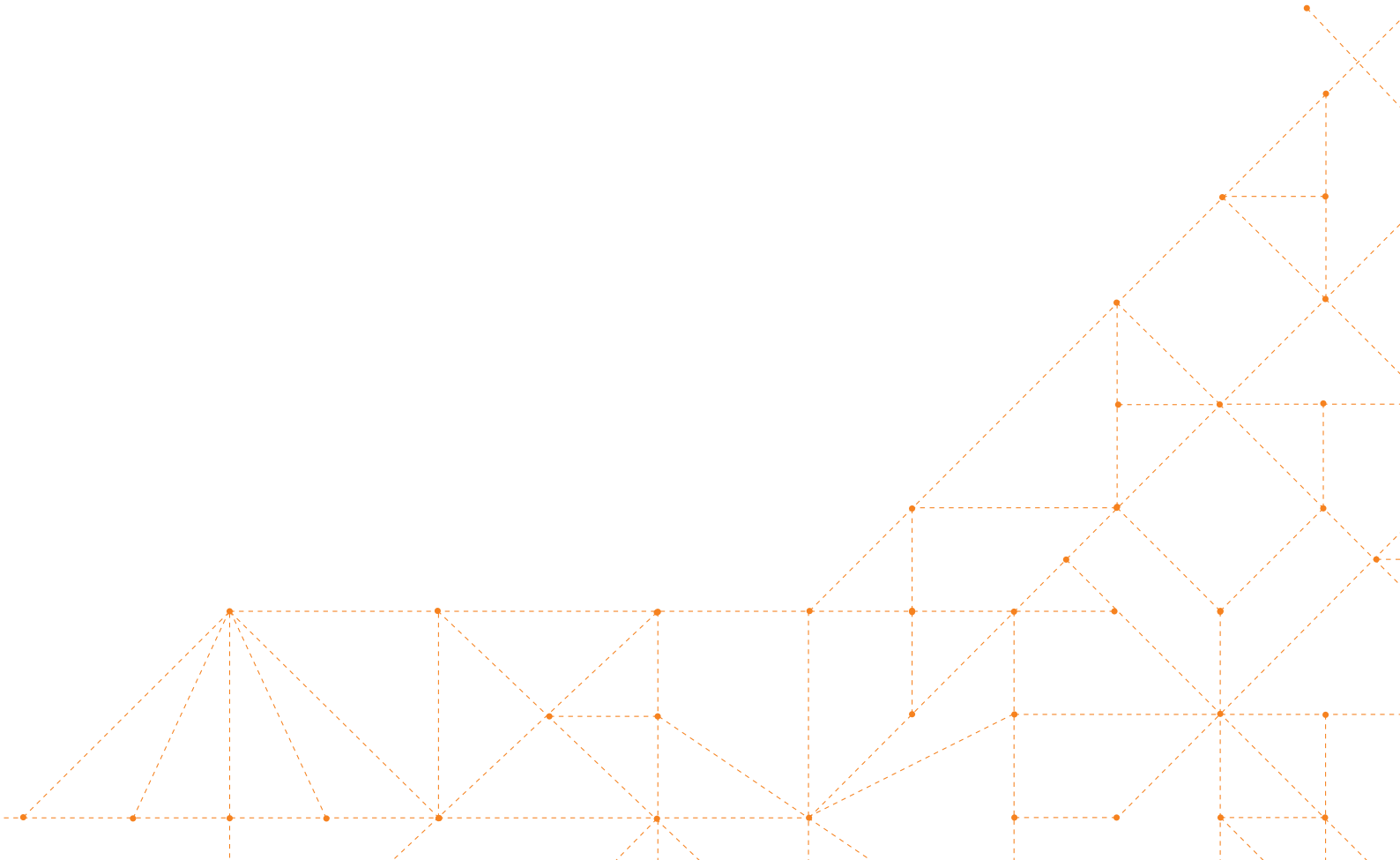
Notre plateforme

À propos de Cloudflare

Cloudflare a été lancée en 2010 pour mener la transformation des infrastructures sur site vers le cloud. Nous avons intégralement construit la plateforme de Cloudflare autour d'une compréhension exhaustive de notre audacieux projet : contribuer à bâtir un Internet meilleur. Les produits composant la suite proposée par Cloudflare protègent et accélèrent toutes les applications Internet en ligne, sans nécessiter d'ajout de matériel, d'installation de logiciels ou de modification de lignes de code.

Cloudflare redirige et achemine l'ensemble du trafic web des propriétés Internet qu'elle protège par son réseau mondial intelligent, qui apprend de chaque requête. Nous aidons nos clients à travailler plus intelligemment, à construire plus solidement, à opérer plus rapidement et à se développer en toute sécurité. Aujourd'hui, Cloudflare protège et accélère des millions de propriétés Internet.

Pour en savoir plus, consultez www.cloudflare.com/fr-fr/.



CLOUDFLARE

+33 7 57 90 52 73 | enterprise@cloudflare.com | www.cloudflare.com/fr-fr/

RÉV. : BDES-4327.2023MAR10