CLOUDFLARE

SOLUTION BRIEF

Everywhere Security™

Une sécurité unifiée à tous les niveaux d'Internet pour vos collaborateurs et vos réseaux, afin de réduire la complexité et d'accélérer votre activité.

Problème : environnement IT complexe et découplé

Le chaos en matière de sécurité informatique crée des opportunités pour les acteurs malveillants

La plupart des architectures informatiques sont trop compliquées ou obsolètes pour appliquer la sécurité partout où elle devrait l'être. Les équipes de sécurité sont contraintes d'assembler manuellement plusieurs outils cloisonnés disposant d'une visibilité limitée et de mesures de contrôle imprécises sur les environnements. Or, cette situation ralentit votre activité.

Cette complexité entraîne une surcharge de travail pour les équipes, qui conduit elle-même à un accroissement des vulnérabilités, à des attaques plus dévastatrices, ainsi qu'à un niveau de ressources impossible à maintenir, uniquement pour rester à jour vis-à-vis des menaces d'hier.

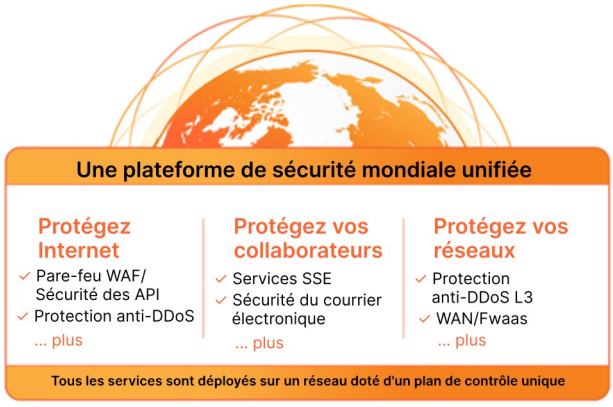
Solution : Everywhere Security

Simplifiez votre approche à l'aide d'une plateforme unique et unifiée

Reprenez le contrôle, abaissez les coûts et réduisez les risques en faisant converger votre sécurité sur la plateforme intelligente de Cloudflare, composée de services programmables et cloud-native.

Protégez votre entreprise sur tous les fronts...

- sur l'ensemble des environnements informatiques ;
- tout au long du cycle de vie des attaques ;
- et partout dans le monde.



Les risques connaissent une escalade...

Les surfaces d'attaque sont en expansion

75 %

des entreprises classées au Fortune 100 fonctionnent sur le principe du travail hybride. Les nouvelles normes de ce type, sans compter le processus de développement moderne d'applications orientées API, créent de nouveaux points d'entrée pour les acteurs malveillants.[1]

Les équipes de sécurité éprouvent des difficultés

40 %

des équipes chargées de l'informatique et de la sécurité expliquent qu'elles sont en train de perdre le contrôle de leurs environnements, tout en devant jongler avec des charges de travail de plus grande ampleur et des responsabilités de plus en plus intimidantes.[2]

L'innovation surpasse la sécurité

89 %

des RSSI déclarent que la transformation numérique, qui inclut l'expérimentation avec l'IA et le développement de nouvelles applications, introduit de nouveaux risques pour les données.[3]

Cycle de vie d'une cyberattaque

La sécurité traditionnelle basée sur des solutions dédiées et une architecture réseau plane facilite le travail aux cyberattaques cherchant à cibler votre environnement informatique pour progresser dans leur cycle de vie.

① Identification de la surface d'attaque

Les acteurs malveillants commencent par identifier une vulnérabilité dans votre surface d'attaque en pleine expansion.

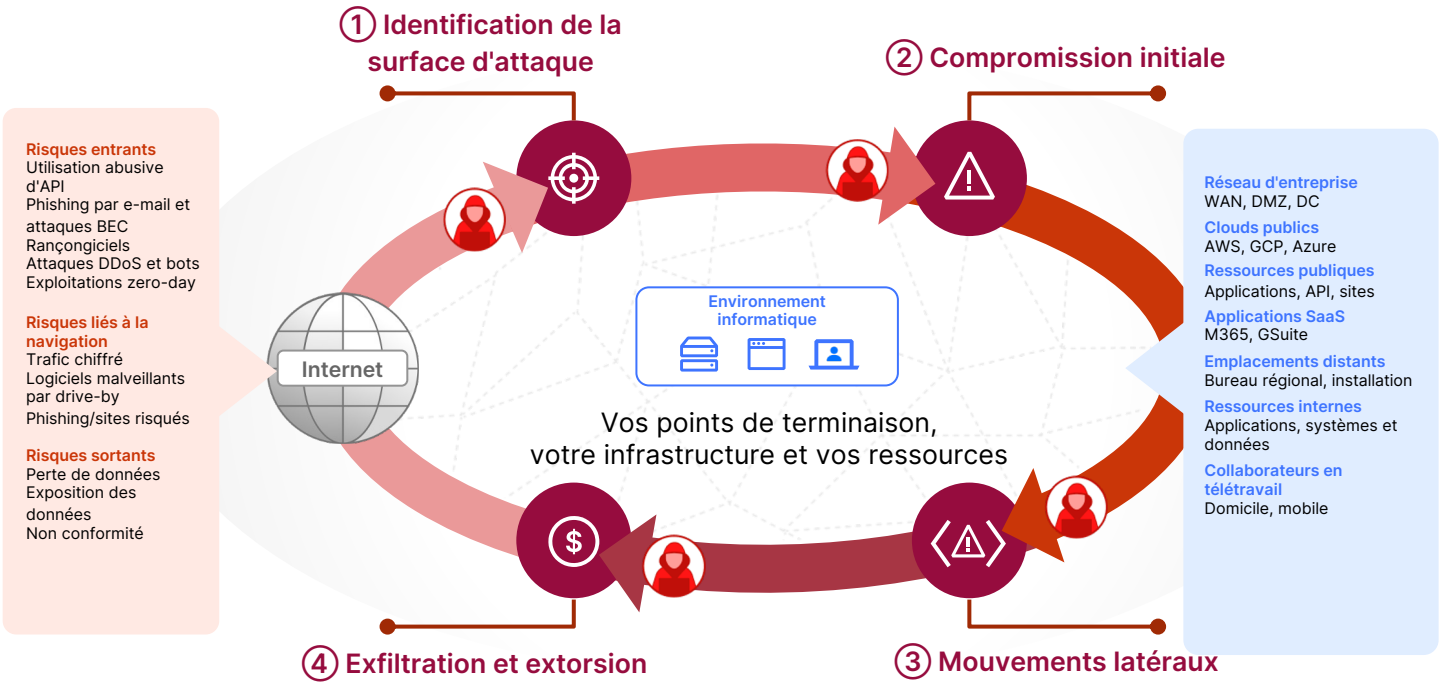
Plus les environnements informatiques s'étendent, plus ces points d'entrée se multiplient, notamment les adresses IP et les ressources informatiques exposées présentant un défaut de configuration ou les vulnérabilités au sein d'un pare-feu/VPN, d'une application/API auto-hébergée, d'une application SaaS ou d'un navigateur web.

② Compromission initiale

Les acteurs malveillants exploitent ensuite ce point d'entrée pour prendre pied au sein de votre environnement informatique.

Les tactiques utilisées comprennent le phishing d'identifiants auprès des utilisateurs ou l'exploitation d'applications par abus d'API ou bourrage d'identifiants (Credential Stuffing).

Les outils obsolètes laissent généralement davantage de vulnérabilités et de failles de sécurité pour les opérations de compromission.



④ Exfiltration et extorsion

En règle générale, les acteurs malveillants terminent leur campagne en dérobant des ressources financières ou des données, voire en laissant votre entreprise désorganisée dans le cadre d'un sabotage.

Ils peuvent également communiquer avec des serveurs de Command-and-Control situés à l'extérieur du réseau de l'entreprise afin de lancer des attaques supplémentaires.

③ Mouvements latéraux

Une fois à l'intérieur, les acteurs malveillants effectuent bien souvent des mouvements latéraux et élèvent leurs privilèges au sein de votre environnement afin d'atteindre la cible désirée.

Les architectures planes et non segmentées autorisant par défaut l'accès aux ressources facilitent cette phase.

La solution Everywhere Security neutralise le cycle de vie des attaques

Grâce à sa plateforme unique, Cloudflare neutralise les cyberattaques à tous les niveaux, à chaque étape de leur cycle de vie, et ce pour chaque point de terminaison, infrastructure ou ressource.

① Minimiser la surface d'attaque

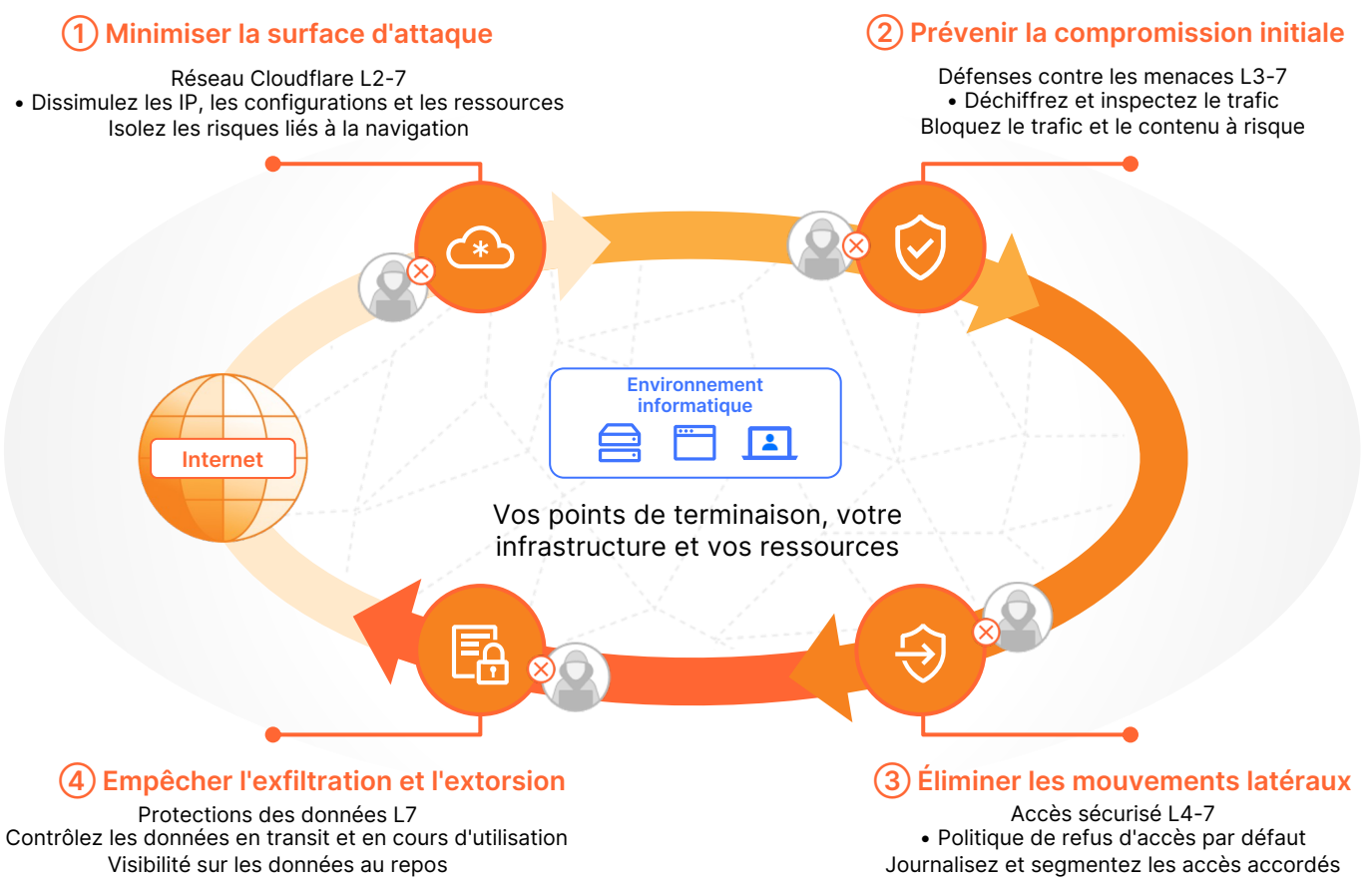
Lorsque vous connectez des réseaux et des applications à Cloudflare, vous minimisez votre surface d'attaque en dissimulant les adresses IP, les configurations et les ressources informatiques.

Isolez la navigation web en périphérie de notre réseau afin d'écarter les utilisateurs et les appareils des menaces ou des risques envers les données.

② Prévenir la compromission initiale

Protégez le réseau d'entreprise dans son ensemble et tout ce que vous connectez à Internet à l'aide de services L3-L7 (couches 3 à 7) afin d'atténuer les risques entrants.

Inspectez l'ensemble du trafic chiffré, c'est-à-dire celui où la plupart des menaces rôdent, même en cas d'utilisation des derniers outils de cryptographie.



④ Empêcher l'exfiltration et l'extorsion

Regagnez visibilité et contrôle sur vos données afin d'empêcher l'exfiltration ou la fraude et d'atténuer le risque d'exposition.

Adaptez-vous aux risques avec agilité en étendant les principes du Zero Trust à l'aide de fonctionnalités composables sur l'ensemble des environnements applicatifs : web, privés et SaaS.

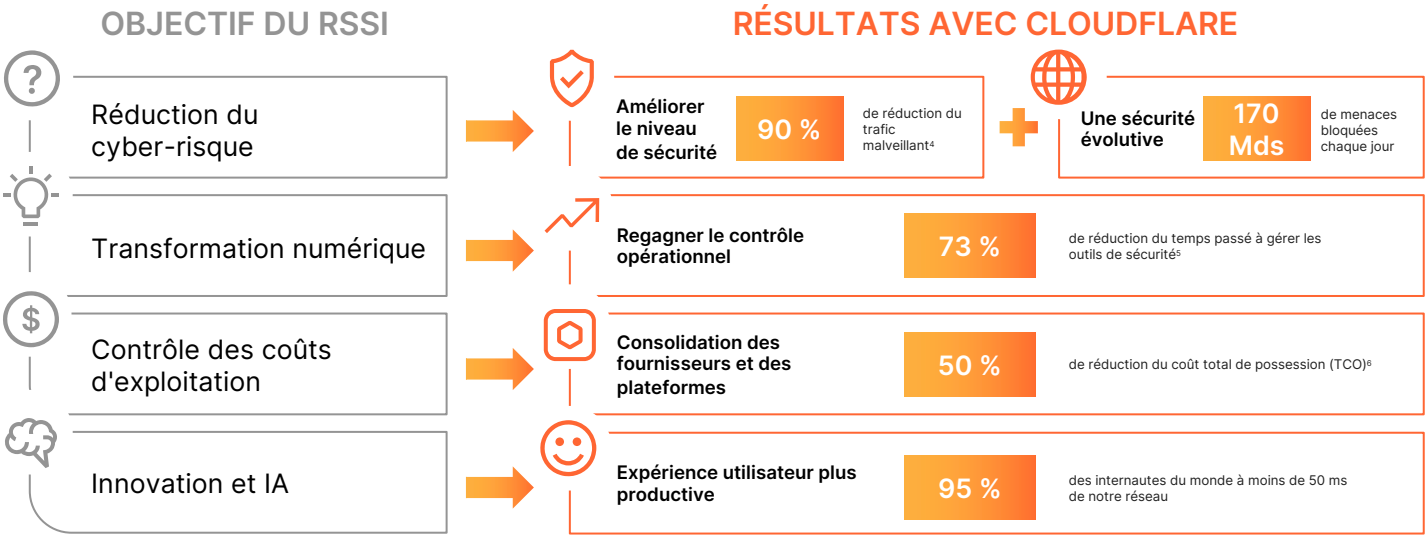
③ Éliminer les mouvements latéraux

Éliminez les mouvements latéraux grâce aux bonnes pratiques Zero Trust que sont le refus d'accès par défaut et le principe du moindre privilège.

Adoptez progressivement les mesures de contrôle basées sur l'identité et le contexte pour sécuriser l'accès sur l'ensemble des environnements.

Avantages

En réduisant la complexité et en proposant la sécurité sur tous les fronts, Cloudflare aide les RSSI à accélérer leurs priorités stratégiques et à moderniser leur entreprise, avec des résultats concrets à la clé.



La différence Cloudflare

Plateforme unifiée et composable

Faites converger la protection des API et des applications web (WAAP), les services de sécurité en périphérie (Security Service Edge, SSE), la sécurité du courrier électronique et d'autres secteurs de la sécurité sur une plateforme et un plan de contrôle uniques.

Bénéficiez d'une interopérabilité illimitée entre tous les services et d'intégrations flexibles aux outils tiers, afin que les mesures de sécurité puissent s'adapter rapidement aux nouveaux risques.

Informations sur les menaces à grande échelle

Les informations sur les menaces de Cloudflare sont basées sur le volume élevé et la grande variété du trafic mondial, avec notamment :

- **20 %** d'Internet
- **2 To** de requêtes DNS/jour
- **Plus de 8 Mds** de pages indexées toutes les deux semaines

Cette visibilité unique et en temps réel alimente les modèles soutenus par IA/ML conçus pour vous défendre contre les menaces émergentes et zero-day.

Réseau à l'échelle réelle

Proposez des capacités locales à l'échelle mondiale :

- **Plus de 310** emplacements réseau
- **Plus de 120** pays
- **228 Tb/s** de capacité
- **Plus de 13 000** interconnexions

Chaque client peut exécuter chaque service de sécurité dans chaque emplacement, afin que l'inspection en une seule passe et l'application de politiques soit toujours rapide, cohérente et résiliente.

Témoignages de clients

Comment Cloudflare aide les entreprises à **protéger leur surface d'attaque**

Homeland Security

100+
En savoir plus

agences civiles américaines disposent de bureaux sécurisés à l'aide du filtrage DNS de Cloudflare.

GPC

450 M
En savoir plus

de menaces bloquées par an sur plus de 900 propriétés web.

Comment Cloudflare permet de **bloquer les menaces zero-day**

Zero-day HTTP/2 Rapid Reset

En août 2023, Cloudflare a contribué à l'identification de la vulnérabilité CVE-2023-44487 et a atténué les attaques DDoS les plus volumineuses que nous ayons jamais observées.

201 M
En savoir plus

de requêtes par seconde en pic
3 fois plus que le record précédent.

Zero-day Ivanti Connect Secure

Le pare-feu WAF assisté par IA de Cloudflare protège de manière proactive contre les attaques visant deux vulnérabilités zero-day récemment découvertes et affectant les produits Ivanti.

<24
En savoir plus

heures après la publication des CVE, de nouvelles règles WAF étaient disponibles.

Comment Cloudflare aide les entreprises à **adopter le Zero Trust**

FORTUNE 500

En savoir plus

100K+

collaborateurs en travail hybride protégés.

Une entreprise de télécoms classée au Fortune 500 a sécurisé son accès à Internet et aux applications grâce au Zero Trust, puis a remplacé Cisco.

bouvet

Cabinet de conseil en informatique scandinave

« Nous dépendons de Cloudflare pour réduire notre surface d'attaque en sécurisant nos ports, en filtrant les menaces et en nettoyant notre trafic. »

— Victor Persson, Security Operations Lead
En savoir plus

Le catalogue des produits de cybersécurité Cloudflare

Unifiez votre approche de sécurité grâce à la protection des API et des applications web (WAAP), aux services de sécurité en périphérie (Security Service Edge, SSE), à la sécurité du courrier électronique et à bien d'autres fonctionnalités. Adoptez les nouvelles capacités à votre rythme.

Simplifiez la sécurité.
Consolidez vos fournisseurs pour réduire la complexité et les risques pesant sur l'entreprise.

Une meilleure visibilité, pour mieux vous protéger.
Tirez parti des données issues de notre gigantesque réseau mondial, qui vous informent en temps réel sur les menaces.

Évoluez sur tous les fronts.
Bénéficiez de protections résilientes dans tous les emplacements, partout dans le monde.

Modernisez votre approche de la cybersécurité

Demander un atelier

CLOUDFLARE

1. BuildRemote.com
2. Forrester Consulting
3. Salt, State of the CISO 2023
4. Chiffre moyen basé sur quatre études de cas
5. Chiffre basé sur les données collectées au cours d'une étude client menée par TechValidate (juin-août 2023)
6. Étude TechValidate