CLOUDFLARE

DOSSIER DE SOLUTION

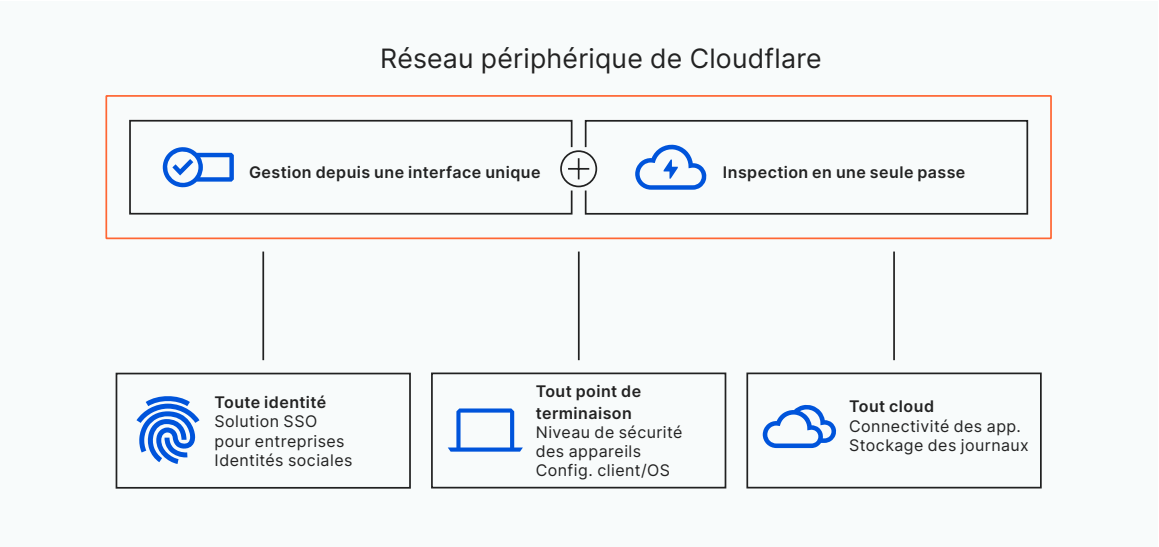
Les intégrations de la plateforme Zero Trust de Cloudflare

Tirez parti des fournisseurs d'identités, de points de terminaison et de cloud que vous utilisez déjà

Devoir jongler avec différents fournisseurs d'identités, de points de terminaison et de cloud au sein d'une organisation est une situation inévitable, mais pas nécessairement fastidieuse. Cloudflare se donne pour objectif de doter votre organisation d'une sécurité extrêmement robuste, offrant une simplicité d'utilisation inégalée. Contrairement à d'autres fournisseurs, nous n'avons aucun intérêt direct dans votre choix de fournisseurs spécifiques dans ces catégories, aujourd'hui comme à l'avenir.

Nous sommes agnostiques. C'est pourquoi notre stratégie est, de longue date, de concevoir la plateforme Cloudflare Zero Trust afin qu'elle s'intègre à autant d'autres solutions que possible.

Par le biais des intégrations, Cloudflare agrège les signaux provenant de plusieurs fournisseurs et propose une interface de contrôle unique, permettant d'appliquer des politiques granulaires et fortement contextualisées à l'ensemble de son réseau mondial. Par ailleurs, ces intégrations ne nécessitent pas d'étudier une documentation technique dense ; elles sont préconstruites sous forme de flux de travail pour offrir une gestion plus fluide, depuis une interface unique.



Ici, nous soulignons trois principes que nous suivons pour rencontrer les clients là où ils se trouvent :

- **Agnosticisme vis-à-vis de l'identité :** authentifiez les utilisateurs à l'aide de plusieurs types de fournisseurs d'identités, afin de garantir un accès fluide à tous les utilisateurs, sans difficultés liées à la configuration.
- **Agnosticisme vis-à-vis des points de terminaison :** enrichissez vos contrôles du niveau de sécurité des appareils de manière plus granulaire et adaptative, avec des signaux provenant à la fois de vos fournisseurs préférés de points de terminaison et de notre client sur appareil.
- **Agnosticisme vis-à-vis du cloud :** sécurisez les applications dans n'importe quel cloud public ou privé (sur site), afin d'éviter l'enfermement propriétaire à long terme.

Agrégez plusieurs identités dans Cloudflare

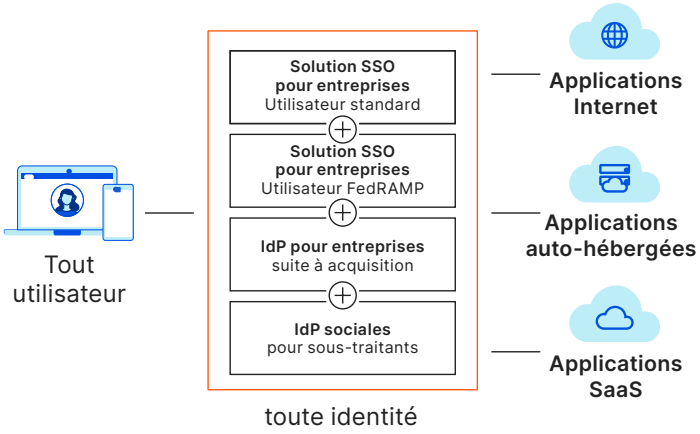
Multi-fournisseurs SSO

Cloudflare a développé l'une des premières solutions d'accès Zero Trust permettant la prise en charge simultanée de plusieurs fournisseurs d'identités (IdP). Aujourd'hui, nous permettons l'intégration d'éminents fournisseurs d'identités pour entreprises (comme Okta ou Azure AD), ainsi que d'identités sociales (comme LinkedIn ou Github) et de normes open source (comme SAML ou OIDC). En outre, nous prenons en charge plusieurs instances du même fournisseur d'identités (par exemple, des utilisations FedRAMP et non-FedRamp d'Okta).

Fédérer plusieurs identités à la fois

Notre capacité à fédérer les identités fournies par plusieurs fournisseurs peut accélérer le processus de conception de politiques sensibles à l'identité. Les organisations n'ont plus besoin de développer des intégrations personnalisées entre leurs fournisseurs d'identité.

Pour les organisations en phase de croissance dotées d'une équipe de sécurité informatique limitée, la fédération peut être un outil particulièrement puissant, permettant d'étendre une stratégie Zero Trust sans nécessiter la consolidation d'un répertoire centralisé unique.



Fonctionnalités principales

- Cloudflare permet l'intégration simultanée de plusieurs fournisseurs d'identités, tous de référence
- Fédérez plusieurs fournisseurs d'identité et plusieurs instances de chaque fournisseur
- Intégration plus rapide d'utilisateurs tiers et de partenaires de fusion et acquisition

Scénario d'utilisation :

Donner aux utilisateurs tiers l'impression d'être des citoyens de première classe

L'approche agnostique des identités de Cloudflare s'avère particulièrement pratique lorsque vous collaborez avec des tiers extérieurs à votre organisation, tels que des sous-traitants, des entreprises acquises ou des partenaires. Des règles d'accès selon le moindre privilège peuvent être mises en place en quelques minutes seulement, sur la base des identités dont ces utilisateurs disposent déjà.

Cette flexibilité sans complexité permet d'éviter les inefficacités et les risques de sécurité liés au provisionnement de licences SSO, au déploiement de VPN ou à la création d'autorisations à usage unique.

Des partenaires d'exception pour la protection des points de terminaison

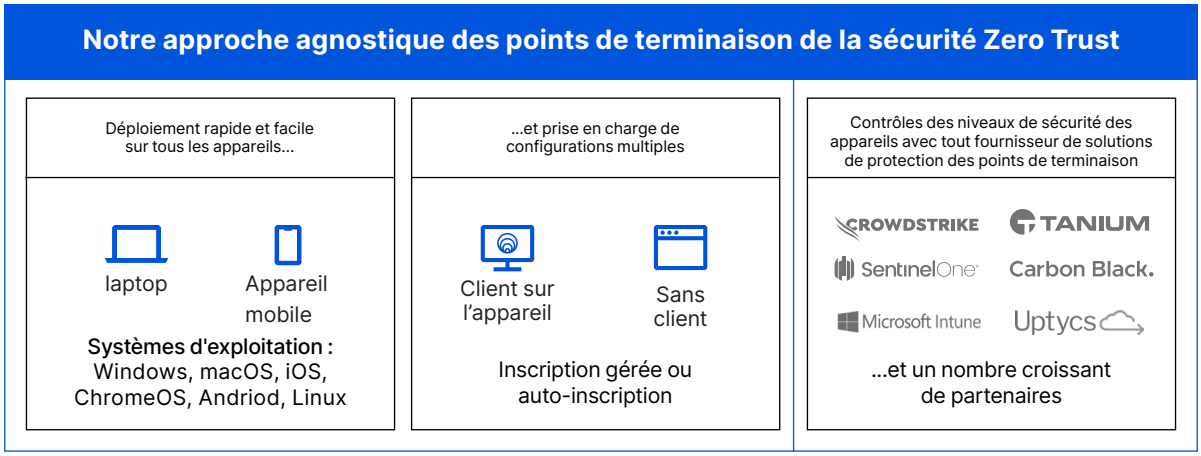
Partenariats

Cloudflare travaille en partenariat avec CrowdStrike, SentinelOne, VMware Carbon Black, Tanium, Uptycs et Microsoft Intune.

Les clients peuvent intégrer plusieurs fournisseurs de protection des points de terminaison à la fois et tirer parti des signaux de sécurité et des capacités d'évaluation des risques de ces solutions.

Configuration

La configuration de l'un de ces fournisseurs se déroule en quelques clics seulement depuis le tableau de bord de Cloudflare, avec les flux de travail prédéfinis. Une fois la configuration terminée, Cloudflare peut vérifier que les appareils exécutent votre logiciel pour points de terminaison préféré, afin d'assurer une surveillance continue des logiciels malveillants et des autres menaces avant d'autoriser ou de refuser l'accès à une application protégée.



Intégrations améliorées par notre client sur appareil (WARP)

Le renforcement de la sécurité nécessite souvent un client sur appareil capable d'enrichir les contrôles du niveau de sécurité de l'appareil avec des attributs supplémentaires. Nous avons délibérément optimisé le nôtre dans l'optique d'offrir une adoption flexible et aisée.

Déploiement sur la plupart des systèmes d'exploitation

- Notre client pour entreprises (WARP) s'exécute sur un nombre croissant de systèmes d'exploitation populaires (par ex. Windows, macOS, Linux, iOS, ChromeOS et Android).
- Notre architecture moderne WireGuard nécessite uniquement des modifications mineures du code spécifique au système d'exploitation.
- Notre client pour entreprises est disponible dans une version grand public, utilisée chaque jour par des millions de personnes dans le monde. Grâce aux tests effectués par autant d'utilisateurs individuels, WARP est plus « apte au déploiement » que la plupart des clients utilisés pour la sécurité Zero Trust.

Options d'inscription gérée ou d'auto-inscription

- Pour les appareils gérés, nous documentons les déploiements effectués avec toute méthode à base de scripts dans les logiciels de gestion d'appareils mobiles (MDM, « Mobile Device Management ») les plus courants.
- L'auto-inscription à WARP peut être utile pour les utilisateurs tiers et ne demande que quelques minutes pour tout ordinateur de bureau ou téléphone mobile.

Éviter l'enfermement prioritaire auprès des fournisseurs de cloud

Problème

Certains fournisseurs « monolithiques » cherchent avant tout à augmenter votre consommation de leurs services de cloud, notamment au niveau des couches de stockage et de calcul.

Sans surprise, l'intégration de leurs solutions de sécurité complémentaires avec les autres fournisseurs de services cloud n'est pas aussi simple qu'elle devrait l'être. Les petits désagréments s'accumulent, à l'image d'une documentation insuffisante et de la présence de bugs. L'enfermement propriétaire dans cette pile technologique complique la vie de votre personnel de sécurité informatique.

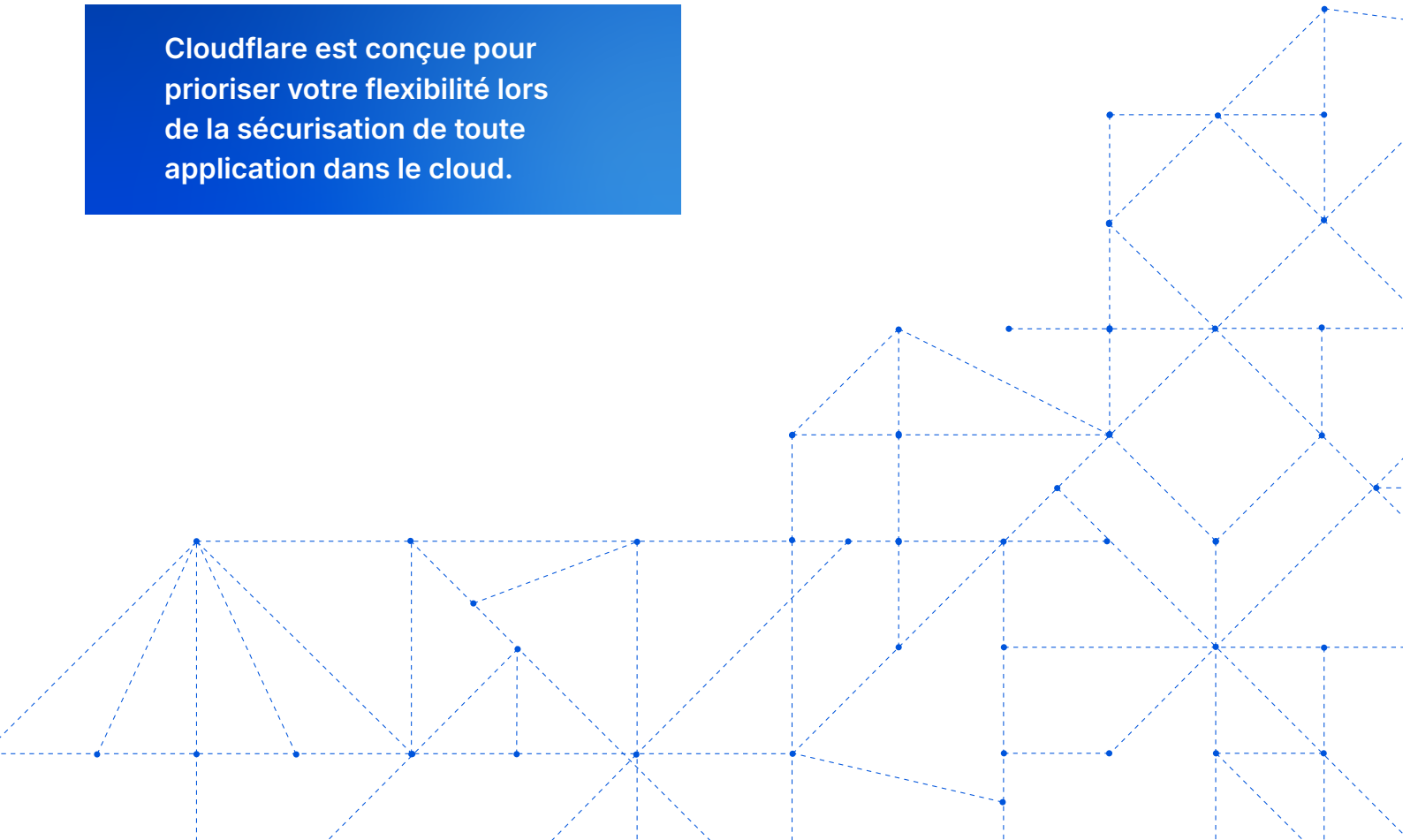
Solution

À l'inverse, notre objectif stratégique est votre sécurité, et non votre consommation de services de cloud. Cloudflare est agnostique vis-à-vis du cloud : nous sécurisons l'accès à toute ressource dans tout environnement de cloud public, privé ou SaaS.

Cloudflare est conçue pour prioriser votre flexibilité lors de la sécurisation de toute application dans le cloud.

Fonctionnalités principales

- Accès à la solution Zero Trust dans les environnements de cloud public, privé et SaaS
- Pas d'enfermement propriétaire sur les destinations de traitement ou de stockage dans le cloud
- Des connecteurs d'applications, des partenaires d'accès réseau direct et des intégrations de stockage qui facilitent l'interaction avec les applications dans tous les clouds



Forces de Cloudflare

Connexions étendues aux applications dans tous les clouds

Notre connecteur d'applications léger est compatible avec tous les clouds

- Exécution de l'outil de ligne de commande en tant que service sous Linux et d'autres systèmes d'exploitation
- Mise en œuvre dans un package, sous forme de conteneur Docker
- Prise en charge des répliques pour les environnements Kubernetes modernes
- Configuration et surveillance du tunnel via l'IU

Interconnexions étendues avec les fournisseurs de cloud

- Connexions rapides pour les utilisateurs assurées par 11 000 interconnexions entre notre réseau et d'autres fournisseurs de cloud, dont 50 interconnexions privées avec les datacenters de Microsoft, Amazon et Google

Divers partenaires d'accès réseau direct (« on-ramp ») non spécifiques au cloud

- Connectez facilement tout environnement de cloud public et privé à notre réseau avec votre méthode de routage SD-WAN existante (par ex., VMware) ou établissez une interconnexion privée sur plus de 1 600 sites de fournisseurs de services de colocation (par ex., Equinix)

Transfert des données de journaux vers n'importe quel cloud

Stockage des données de journaux dans le cloud ou envoi direct aux fournisseurs de services de données analytiques

- Prise en charge intégrée d'une ou plusieurs destinations de stockage simultanées, notamment AWS, Azure, Google Cloud et n'importe quelle API compatible S3 (par ex. Digital Ocean Spaces)
- Intégrations prédéfinies aux outils de données analytiques et SIEM, tels que Sumo Logic, Splunk et Datadog

Sécurité dans tous les clouds publics et privés

Liste de partenaires d'intégration Zero Trust

Au fil du temps, Cloudflare agrégera les signaux provenant d'une liste encore plus vaste de fournisseurs préférés, avec le soutien des connaissances de notre plateforme Zero Trust et de notre réseau mondial.

Fournisseurs d'identité

SSO pour entreprises

- Centrify
- Citrix ADC
- Google Workspace
- Jumpcloud
- Microsoft Azure Active Directory (AD)
- Okta
- OneLogin
- Ping Identity

Identités sociales

- Facebook
- GitHub
- Google
- LinkedIn
- Yandex

Open Source

- OIDC
- SAML 2.0

Fournisseurs de points de terminaison

Fournisseurs de protection des points de terminaison

(pour le niveau de sécurité des appareils)

- Crowdstrike
- Microsoft Endpoint Manager
- SentinelOne
- Tanium
- Uptycs
- VMWare Carbon Black

Fournisseurs de gestion des points de terminaison

(pour les déploiements de clients)

- Hexnode
- Ivanti
- Jamf
- Jumpcloud
- Kandji
- Microsoft Intune

Partenaires d'accès réseau direct (« on-ramp »)

Partenaires d'interconnexion physique

- 365 Data Centers
- BBIX
- CoreSite
- Cyxtera
- Databank
- Digital Realty
- EdgeConneX
- Equinix
- Netrality Data Centers
- Teraco
- Zayo

Partenaires d'interconnexion de l'infrastructure

- Console Connect/ PCCW
- CoreSite
- Epsilon Infiny
- Equinix Fabric
- Megaport
- PacketFabric

SD-WAN

- Aruba (Silverpeak)
- Cisco
- VMWare (Velocloud)

Fournisseurs de cloud

Destinations de stockage dans le cloud

- AWS S3
- Stockage Google Cloud
- Microsoft Azure Blob Storage
- Autres fournisseurs disposant d'une API compatible S3

Partenaires de services de données analytiques cloud et SIEM

- Azure Sentinel
- Datadog
- Elastic
- Google Cloud
- Graylog
- IBM QRadar
- Looker
- New Relic
- Splunk
- Sumo Logic

Pour en savoir plus sur Cloudflare Zero Trust et demander une démonstration ou une démonstration de faisabilité à un représentant commercial, veuillez consulter : https://www.cloudflare.com/fr-fr/products/zero-trust/.

CLOUDFLARE

© 2022 Cloudflare Inc. Tous droits réservés. Le logo Cloudflare est une marque commerciale de Cloudflare. Tous les autres noms de produits et d'entreprises peuvent être des marques des sociétés respectives auxquelles ils sont associés.

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

RÉV. : BDES-3795.2022SEP26