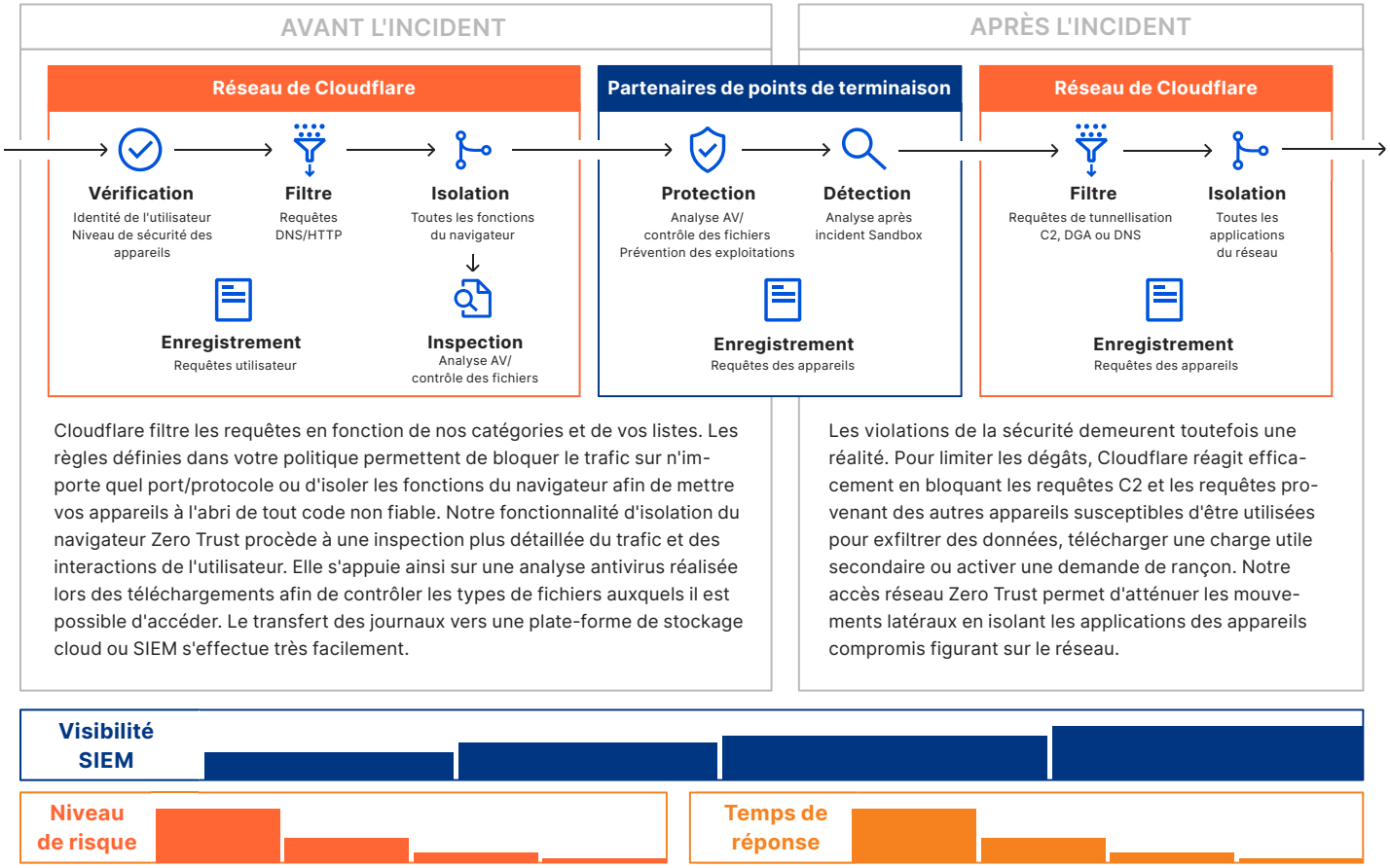
Une défense contre les menaces plus simple et plus efficace

Vous ne pourrez totalement échapper aux logiciels malveillants, à l'hameçonnage, au minage de cryptomonnaie et aux autres attaques, mais vous pouvez en atténuer les effets.

La superposition des défenses constitue la meilleure pratique à adopter pour suivre le rythme des menaces en constante évolution. Toutefois, si la multiplication excessive des différents outils d'amélioration de la sécurité se révèle non seulement coûteuse et complexe, elle peut également nuire aux performances. Les petites organisations recherchent la simplicité en matière de réduction des risques, les organisations de taille moyenne souhaitent des réponses plus efficaces et les grandes ont besoin de visibilité en un seul endroit.

Cloudflare réunit un grand nombre de services de sécurité autrefois distincts (jusqu'au déplacement de l'ensemble des opérations des points de terminaison effectuées dans les navigateurs) au sein d'une plate-forme Zero Trust exécutée sur un réseau périphérique Anycast de grande envergure. Une défense contre les menaces plus efficace commence par l'approche Zero Trust : c'est-à-dire vérifier que les appareils sont bien sécurisés avant de leur permettre de se connecter aux ressources de l'entreprise.

La solution : un système de défense contre les menaces intégré à l'ensemble des mesures de sécurité du réseau et des points de terminaison

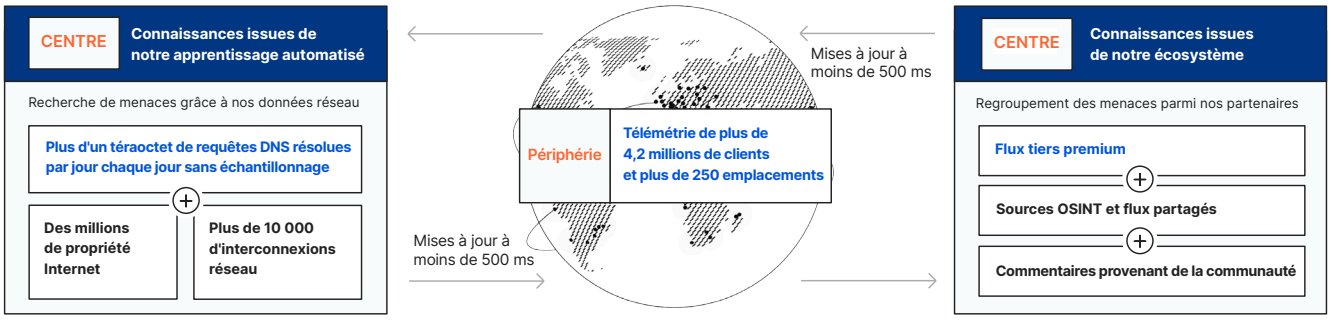


Cloudflare filtre les requêtes en fonction de nos catégories et de vos listes. Les règles définies dans votre politique permettent de bloquer le trafic sur n'importe quel port/protocole ou d'isoler les fonctions du navigateur afin de mettre vos appareils à l'abri de tout code non fiable. Notre fonctionnalité d'isolation du navigateur Zero Trust procède à une inspection plus détaillée du trafic et des interactions de l'utilisateur. Elle s'appuie ainsi sur une analyse antivirus réalisée lors des téléchargements afin de contrôler les types de fichiers auxquels il est possible d'accéder. Le transfert des journaux vers une plate-forme de stockage cloud ou SIEM s'effectue très facilement.

Les violations de la sécurité demeurent toutefois une réalité. Pour limiter les dégâts, Cloudflare réagit efficacement en bloquant les requêtes C2 et les requêtes provenant des autres appareils susceptibles d'être utilisées pour exfiltrer des données, télécharger une charge utile secondaire ou activer une demande de rançon. Notre accès réseau Zero Trust permet d'atténuer les mouvements latéraux en isolant les applications des appareils compromis figurant sur le réseau.

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

La plate-forme d'informations Cloudflare One



Catégories de risques pour la sécurité à bloquer, isoler ou placer en logpush vers SIEM en fonction des règles de vos politiques

Logiciels malveillants	Domaines récemment observés	Domaines DGA	Logiciels espions
Hameçonnage (phishing)	Nouveaux domaines	Tunnelling DNS	Spam
Minage de cryptomonnaie	Domaines inaccessibles	C2 et botnet	Service d'anonymisation

Les informations de Cloudflare permettent de bloquer efficacement les menaces connues et émergentes grâce aux données provenant de notre réseau et à notre écosystème. Pourtant, peu importent...

- le nombre de dispositifs de détection de menaces ou de flux d'informations sur les menaces dont dispose un fournisseur,
- la quantité de données ou d'apprentissage automatique utilisée, ou
- la fréquence de mise à jour et la rapidité d'application des informations

... le filtrage et l'inspection ne parviennent pas à bloquer 100 % des menaces.

Vos équipes de sécurité ne peuvent pas bloquer tous les sites qui présentent un risque pour votre organisation sans perturber le travail de vos employés, soit un constat potentiellement plus onéreux en termes de perte de productivité et de traitement des tickets informatiques que les dommages résultant d'une attaque.

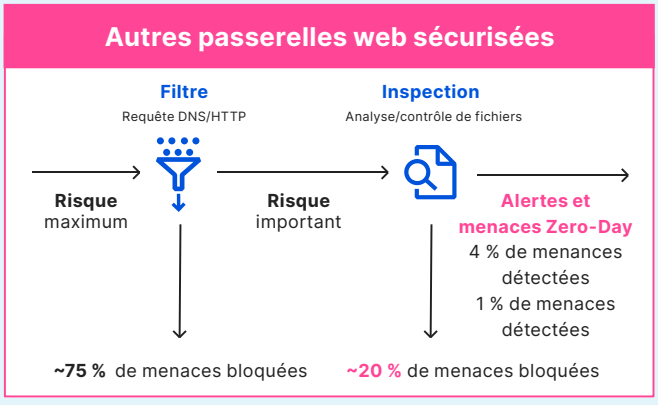
Voilà pourquoi vous devez adopter une solution Zero Trust pour la navigation sur Internet. La solution d'isolation de navigateur Cloudflare Browser Isolation...

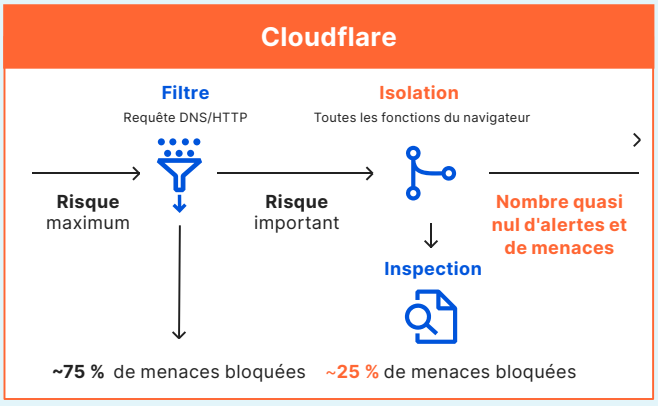
- **offre une expérience utilisateur irréprochable, rapide comme l'éclair**
- **et s'avère particulièrement rentable à utiliser pour l'ensemble des sites non bloqués appartenant aux catégories suivantes :**

Sans catégorie	À risque	À faible risque

Prochainement, vous pourrez :

- Inspecter et contrôler les données en cours d'utilisation et pas uniquement les données en transit.
- Préciser l'emplacement de stockage des fichiers téléchargés.
- Empêcher la saisie des identifiants dans les formulaires.





Contactez-nous dès aujourd'hui pour demander l'accès à un compte Cloudflare Zero Trust dans le cadre d'une offre Entreprise.