CLOUDFLARE

PRÉSENTATION PRODUIT

Cloudflare Email Security

Une protection autonome et multicanale pour sécuriser la communication de l'espace de travail

Se protéger contre les attaques de phishing ciblées

Bloquez et isolez sans effort les menaces que les autres solutions ignorent

Le courrier électronique étant l'application professionnelle la plus utilisée et la plus exploitée, il est plus essentiel que jamais de protéger les utilisateurs contre les attaques de phishing qui cherchent à tirer profit de leur confiance. Alors que les entreprises continuent d'adopter les services de courrier électronique cloud via Microsoft 365 et Google Workspace afin de mieux prendre en charge les collaborateurs hybrides, les acteurs malveillants sont passés à des attaques plus ciblées et de faible volume, capables d'échapper aux passerelles e-mail sécurisées (SEG, pour Secure Email Gateway en anglais) traditionnelles, comme Proofpoint et Mimecast.

C'est pourquoi la solution de sécurité des e-mails cloud-native de Cloudflare a été spécialement conçue pour tirer parti de nos informations préventives sur les campagnes, de l'analyse de contenu basée sur l'apprentissage automatique (Machine Learning) et d'une plateforme Zero Trust unifiée afin de bloquer les menaces de phishing avant qu'elles n'atteignent vos collaborateurs.

91 %

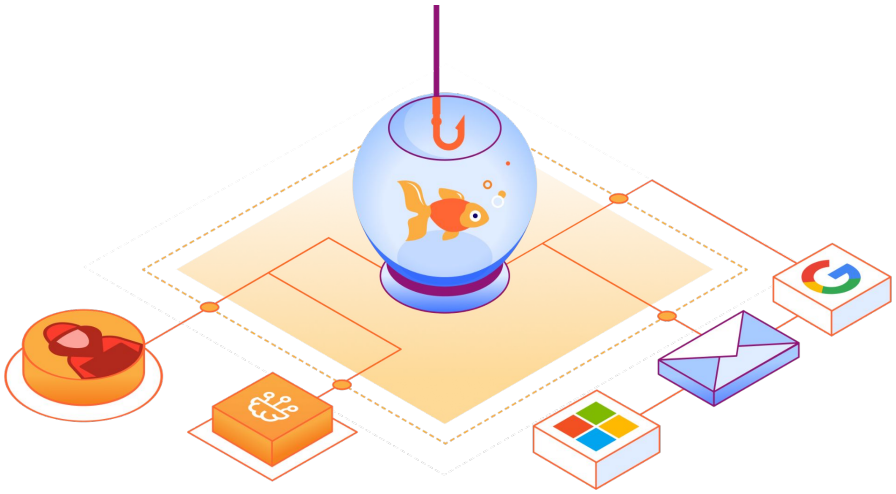
de l'ensemble des cyberattaques commencent par un e-mail de phishing[1]

50 milliards

de pertes dues aux attaques BEC sur les dix dernières années[2]

81 %

des entreprises ont subi une attaque multicanale au cours des 12 derniers mois[3]



Mettez un terme à la compromission du courrier électronique professionnel (BEC)

Détectez les comptes usurpés et compromis à l'aide de l'analyse contextuelle multicouche reposant sur l'apprentissage automatique.

Isolez les attaques différées et multicanales

Isolez les utilisateurs du contenu web malveillant véhiculé via des liens inconnus ou dissimulés.

Bloquez les rançongiciels et les pièces jointes malveillantes

Empêchez les tentatives d'extorsion et le code malveillant de compromettre votre entreprise.

Plus de protection et de simplicité

Mettez en œuvre une sécurité multicouches capable d'assurer une meilleure protection pour un coût bien moindre

Alors que les attaques de phishing continuent de proliférer, Microsoft et Google poursuivent leurs efforts visant à développer des fonctionnalités natives proposant des capacités essentielles de protection des données et du courrier électronique, comme l'authentification, l'archivage et le chiffrement côté client. Toutefois, les acteurs malveillants ont fait évoluer leurs tactiques afin de lancer des attaques plus ciblées et évasives, souvent capables de contourner les mesures de sécurité natives et bénéficiant d'un taux de réussite bien supérieur.

En superposant leur sécurité sur Cloudflare, les entreprises peuvent bloquer ou isoler automatiquement les attaques de phishing ciblées qui s'appuient sur des pièces jointes et des liens malveillants, mais aussi sur des comptes compromis, pour dérober des informations sensibles et commettre des actes frauduleux sur le plan financier.

Améliorez vos mesures de sécurité des e-mails existantes

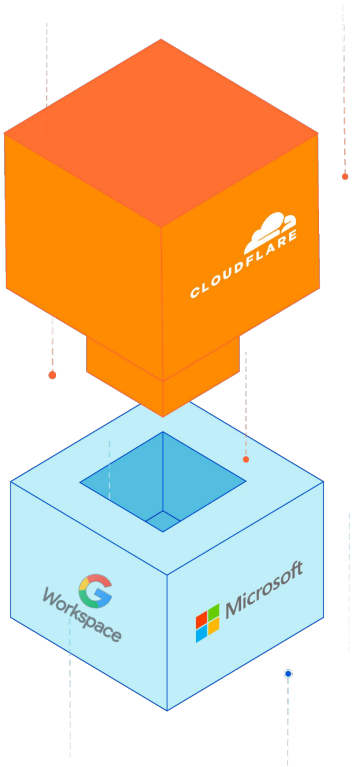
La solution de sécurité des e-mails cloud-native de Cloudflare peut être déployée en quelques minutes afin de renforcer les déploiements SEG existants ou de compléter les fonctionnalités intégrées aux e-mails proposées par Microsoft et Google. Les entreprises peuvent bénéficier d'une meilleure protection contre le phishing en ne consacrant que peu de temps et d'efforts à la gestion continue de la solution, et encore moins à ajuster finement cette dernière.

« Depuis la mise en œuvre de Cloudflare [par-dessus M365], nous avons constaté une réduction de 50 % du nombre d'e-mails malveillants ou suspects reçus chaque jour par nos utilisateurs. Cette diminution libère de nombreuses heures que nous pouvons réinvestir dans d'autres objectifs. »

Werner Enterprises
(Fortune 1000)

Email Security : protection contre le phishing ciblé et les attaques BEC

Fournisseur de courrier électronique : fonctionnalités essentielles de protection des données et des e-mails



Réinvestissez les heures économisées grâce à l'accroissement de l'automatisation

La solution légère et automatisée de Cloudflare offre une intégration parfaite aux processus Microsoft et Google, tout en proposant une interface utilisateur unique et intuitive pour les activités d'analyse.

Parvenez à 99,997 % d'efficacité de détection

L'alliance des capacités natives de votre fournisseur de courrier électronique à la protection contre le phishing et les attaques BEC de Cloudflare permet aux entreprises de disposer d'une couverture complète afin de réduire les risques au minimum.

Réalisez une plus grande valeur ajoutée

Le remplacement des déploiements obsolètes, coûteux et complexes par la solution à faible interaction de Cloudflare peut réduire les surcoûts opérationnels, les fonctionnalités redondantes et l'excès de réglages.

Bloquer les attaques BEC sophistiquées

Déjà 50 milliards de dollars de pertes signalées, un chiffre en croissance permanente

Les attaques BEC étant responsables d'un montant impressionnant de pertes ces dix dernières années, il est donc surprenant que certaines entreprises n'aient toujours pas accordé la priorité à la lutte contre une telle forme de fraude financière. Si les attaques BEC ne représentent qu'un très faible pourcentage des menaces de phishing, elles ne sont bien souvent pas détectées par les SEG et les fournisseurs de courrier électronique cloud, avec pour résultat de plus grandes pertes financières encore. Ces attaques ciblées sont difficiles à identifier, car elles tirent parti de comptes usurpés ou compromis et de contexte issu de discussions pour se faire passer pour un collaborateur ou un fournisseur de confiance.

Étendre les principes Zero Trust aux e-mails

Lorsqu'ils tirent parti du compte e-mail compromis d'un collaborateur ou d'un fournisseur, les acteurs malveillants peuvent échapper aux mesures de sécurité traditionnelles, qui tentent uniquement de confirmer la légitimité du compte de l'expéditeur. Cloudflare va plus loin en analysant un vaste ensemble d'attributs comportementaux, de schémas d'écriture, d'indicateurs de sentiment et d'historiques de conversations afin de déterminer l'authenticité de l'expéditeur. En plus des informations extensives sur le réseau, les modèles de menaces de Cloudflare, soutenus par l'apprentissage automatique (Machine Learning), proposent l'arme la plus efficace contre les comptes compromis utilisés pour extraire des paiements frauduleux.

Figure 1 : analyse de message

Détectez les attaques BEC grâce à l'analyse contextuelle soutenue par l'apprentissage automatique

L'identification précise des attaques BEC nécessite plus que la simple analyse structurelle d'un message. Une détection réussie implique également une compréhension détaillée des variations d'une conversation en termes de style et d'intention. La télémétrie réseau extensive de Cloudflare (plus de 3 000 milliards de requêtes DNS par jour) et l'évolution des modèles d'apprentissage automatique nourrissent le moteur d'analyse à petits modèles qui décompose chaque aspect d'un e-mail afin d'évaluer les schémas d'écriture, les sentiments, le contexte historique et une vaste gamme d'autres variables permettant d'aider à identifier l'authenticité de l'expéditeur.

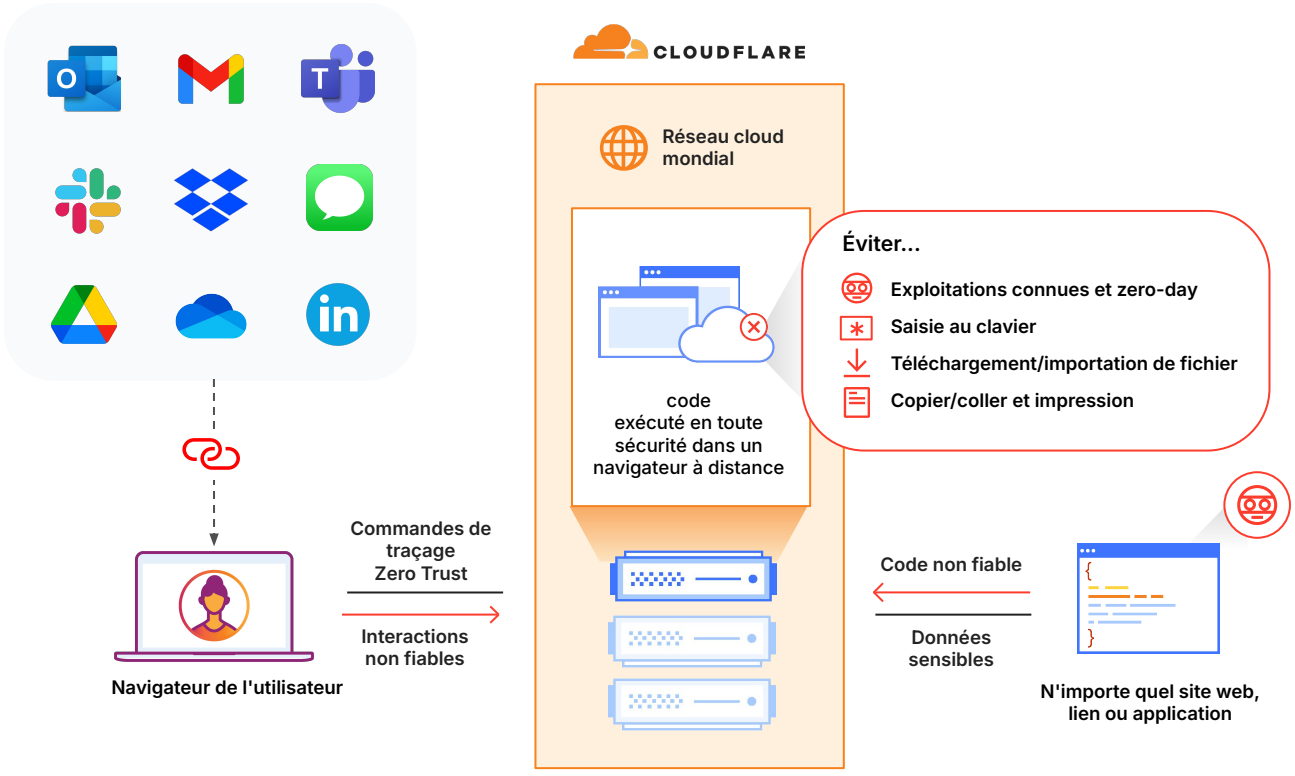
Isoler les attaques reposant sur des liens

Les attaques reposant sur les liens sont devenues la méthode de choix pour dérober des identifiants, charger des logiciels malveillants/rançongiciels et extraire des informations sensibles. Le recours à une combinaison d'e-mail, de chat, de SMS, de réseaux sociaux et autres applications pour transmettre ces liens complique davantage la garantie de protection tant pour les employés que pour les données contre les attaques par phishing.

Cloudflare apporte une solution contre les attaques de phishing grâce à un rendu de tout le code web à distance sur notre réseau cloud mondial et non sur l'appareil local de l'utilisateur. Cela permet d'atténuer les logiciels malveillants et les attaques de navigateur zero-day, tout en fournissant un contrôle granulaire sur les actions de l'utilisateur (par exemple désactivation de la saisie au clavier) permettant de prévenir les collectes d'informations d'identifications et les fuites de données.

Éliminer le risque de phishing sans ralentir vos équipes

En intégrant des fonctionnalités d'isolement de navigateur de dernière génération développées avec notre technologie unique de rendu réseau vectoriel (NVR pour Network Vector Rendering), Cloudflare est en mesure d'apporter une solution fluide, sécurisée et évolutive permettant d'isoler les liens potentiellement malveillants. À la différence des techniques gourmandes en bande passante, NVR diffuse des commandes de traçage sécurisé vers l'appareil. Cela permet d'éliminer le risque de contenu web malveillant sans nuire à l'expérience utilisateur. Grâce à NVR et au réseau à faible latence de Cloudflare, les organisations peuvent isoler des menaces multicanales tout en garantissant une productivité sans interruption pour leurs collaborateurs.



Investigations et résolutions rapides

Une gestion de la sécurité intuitive et à faible interaction

Grâce à une plus grande automatisation et à une quantité minimale de configuration nécessaire pour atteindre des résultats optimaux, Cloudflare réduit considérablement le temps et les efforts requis pour gérer la sécurité du courrier électronique en continu. Les équipes de sécurité peuvent immédiatement profiter d'une visibilité complète sur l'ensemble des tendances et des indicateurs principaux au sein du tableau de bord, tout en bénéficiant de la possibilité de cliquer sur les messages marqués pour faire apparaître davantage de détails. L'exploration en profondeur des tendances permet d'identifier rapidement les types d'attaques fréquents, les collaborateurs ciblés, les attaques différées atténuées et d'autres points de données essentiels.

Vous retrouverez l'ensemble des analyses, de la télémétrie, des données observables sur les menaces et des indicateurs de compromission (IoC, Indicators of Compromise) via une API extensive afin de faciliter l'intégration à vos outils existants en matière d'analyse et d'orchestration.

« J'explique souvent à mes collaborateurs à quel point Cloudflare (en tant que solution SaaS basée sur le cloud) se révèle à la fois simple et facile à utiliser, tout en ne manquant pas d'exprimer ma pleine satisfaction devant son haut degré de précision. »

Japan Airlines

Gestion de la détection et des réponses (PhishGuard)

PhishGuard, le service de sécurité des e-mails géré de Cloudflare, complète votre équipe SOC existante afin de libérer des cycles d'investigations de sécurité et de proposer de précieuses informations sur les menaces. Le service PhishGuard peut vous aider à enrayer les campagnes de phishing en contribuant aux investigations, aux évaluations de menaces internes, à la neutralisation des fraudes actives et aux besoins complexes en matière de mesures correctives. PhishGuard étend les ressources et l'expertise en matière de sécurité afin de vous informer de manière active sur les potentielles fraudes et menaces internes, tout en débusquant également les menaces basées sur le courrier électronique.

Fonctionnalités et avantages de PhishGuard :

- Signalements des tentatives de phishing et réponses aux incidents gérées pour une résolution plus rapide.
- Notifications proactives en matière d'attaques BEC et de fraudes, afin de permettre aux entreprises de réagir rapidement, dès le début du cycle de vie de l'attaque.
- Ressources dédiées pour le suivi en temps réel, l'examen périodique des comptes et l'évaluation des menaces en continu.
- Signatures de blocage personnalisées basées sur l'analyse des menaces au sein de l'environnement géré.

Plus de 1 100

heures économisées chaque année grâce à l'automatisation du triage manuel

La solution automatisée de Cloudflare élimine les tâches manuelles et chronophages, afin d'améliorer les temps de réponse et de dégager des cycles supplémentaires.

50 %

de réduction du nombre d'e-mails malveillants ou suspects transmis (en plus de M365)

La superposition de Cloudflare à Microsoft 365 permet aux entreprises de détecter les attaques ciblées et de réduire le nombre total d'e-mails malveillants.

40

heures au total passées sur la configuration de la sécurité des e-mails sur une période de sept ans

La solution de sécurité des e-mails à faible interaction proposée par Cloudflare ne demande que peu de configuration préalable et peu de réglages en continu. Elle offre immédiatement un degré élevé d'efficacité en matière de détection.

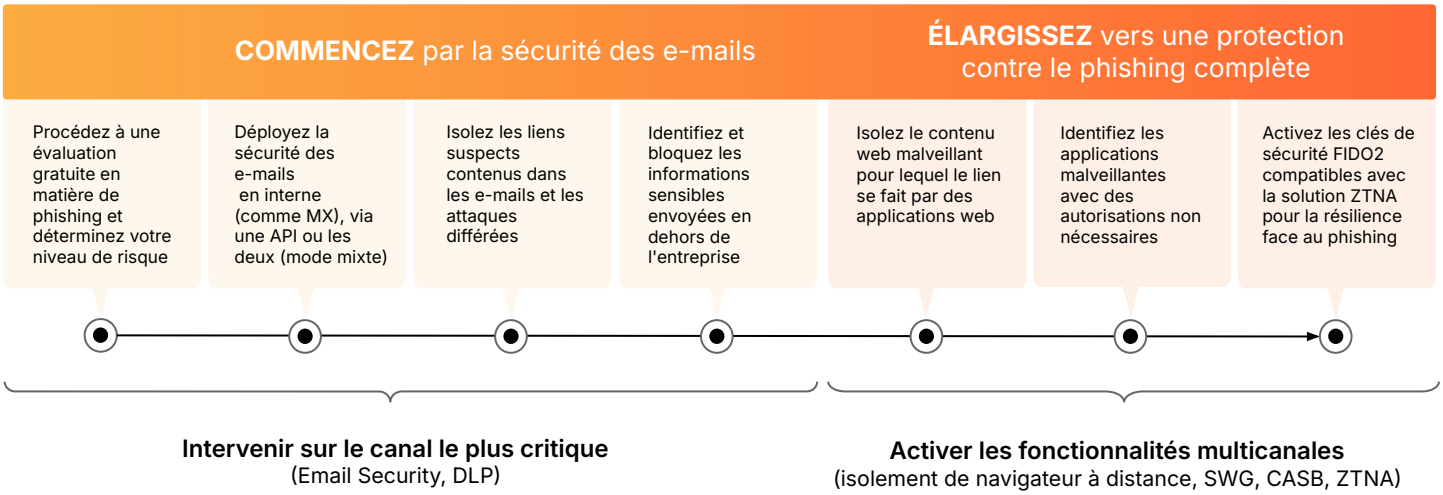
AVANTAGES

Protection multicanale complète

Une campagne de phishing se répand très vite au-delà des e-mails, il est devenu plus urgent que jamais pour les entreprises de mettre en œuvre une solution pour le phishing conduisant rapidement et simplement à une protection multicanale complète.

Avec la plateforme de sécurité unifiée de Cloudflare, les entreprises peuvent commencer par déployer une solution de sécurité des e-mails à la pointe du marché pour intervenir sur le canal de phishing le plus critique ; avant d'activer facilement des services Zero Trust afin d'élargir la protection à tous les canaux et bloquer efficacement les menaces de phishing connues ou émergentes.

- **Une protection à faible interaction et à haute efficacité :** Réduisez les risques de phishing avec une solution de détection la plus efficace du secteur exigeant très peu de réglage.
- **Une plus grande consolidation pour un coût moindre :** Diminuez les dépenses avec une plateforme unique et entièrement intégrée qui permet de résoudre tous les scénarios de phishing.
- **Rapidité de déploiement, facilité de gestion :** Garantissez une protection immédiate tout en réduisant le temps et les efforts nécessaires à la gestion sur le long terme.



Évaluer et comparer

Procédez à un examen de votre situation actuelle en matière de défense des e-mails et déterminez les menaces qui vous échappent

Effectuez une analyse rétroactive (Retro scan) gratuite de quelques minutes pour observer les menaces de phishing à côté desquelles vous êtes passé au cours des 14 derniers jours ou demandez une évaluation du risque de phishing pour vérifier la présence de phishing dans vos boîtes de réception. Comparez les résultats à ceux d'autres fournisseurs de services immédiatement fonctionnels afin de découvrir quelle solution de sécurité des e-mails propose la protection la plus rapide et la plus simple.

Exécuter une analyse rétroactive | Demander une PRA

1. Recherches Deloitte 2020: source
2. FBI IC3 PSA 2023 : source
3. Forrester Opportunity Snapshot 2023 : source

