CLOUDFLARE
AREA 1 SECURITY

DOSSIER DE SOLUTION

Améliorez les défenses de la messagerie Microsoft 365 avec Cloudflare Area 1

Étendez l'architecture Zero Trust à votre outil de communication n° 1 – la messagerie cloud

Préservez les boîtes de réception Microsoft des menaces grâce à une solution de sécurité des e-mails préventive et cloud-native

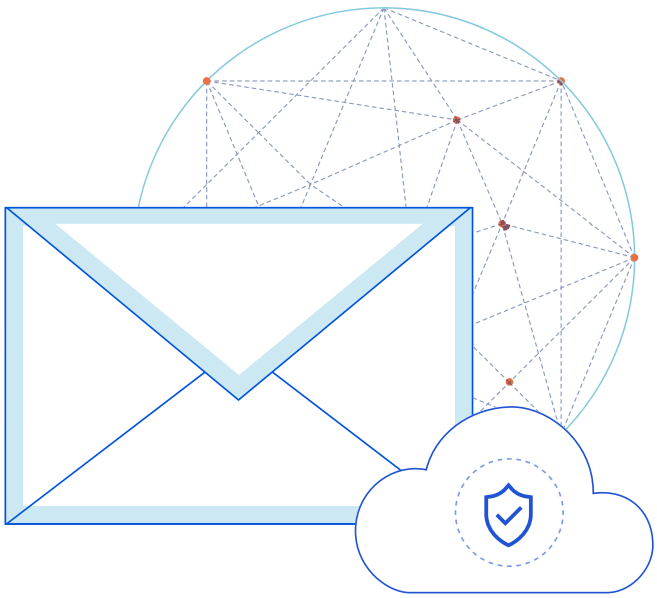
Microsoft 365 offre une excellente protection contre les menaces à fort volume, telles que le spam et les virus, et fournit une protection supplémentaire aux clients utilisateurs de Microsoft Advanced Threat Protection (ATP).

Néanmoins, Gartner® remarque[1] : « Si les fonctionnalités de sécurité intégrée ... ont progressé, les auteurs de menaces gagnent également en sophistication, ciblant souvent [les utilisateurs] avec de fausses pages de connexion afin de collecter des informations d'identification. Les menaces sophistiquées transmises par e-mail incluent des sites web compromis et des documents infectés, utilisés pour déployer des logiciels malveillants. De nombreux groupes fournissant des rançongiciels en tant que service utilisent les e-mails comme point d'entrée initial. Au-delà des logiciels malveillants, les menaces liées à la compromission d'adresses e-mail professionnelles (Business Email Compromise, BEC) et la prise de contrôle de comptes continuent d'augmenter, entraînant des pertes financières importantes. »

Les menaces sophistiquées à faible volume, telles que celles mentionnées ci-dessus, sont d'abord construites avec une infrastructure et des techniques d'attaque que Cloudflare Area 1 permet, grâce à une capacité unique, d'identifier « dans la nature ». En identifiant et en bloquant automatiquement les campagnes dès les premières phases du cycle de vie de l'attaque (en moyenne 24 jours avant le lancement), Area 1 préserve les boîtes de réception des menaces.

Intégré à la plateforme Cloudflare Zero Trust, le service de sécurité des e-mails Area 1 offre également les avantages suivants :

- **Révélation des fraudes financières sans logiciels malveillants**, souvent mises en œuvre au cours de plusieurs conversations par e-mail avec des fournisseurs « de confiance »
- **Blocage en temps réel d'attaques jamais encore observées**, sans nécessiter d'ajuster la configuration d'une passerelle de messagerie sécurisée ou d'attendre des mises à jour de signatures/politiques
- **Identification des comptes et domaines compromis**, ainsi que des domaines nouveaux, semblables et proches, utilisés par les acteurs malveillants pour contourner DMARC/SPF/DKIM
- **Isole et bloque les attaques multicanaux et différées** grâce à l'intégration dans Cloudflare Browser Isolation (bêta)



Aperçu de la solution

Dans un monde orienté cloud, les passerelles de messagerie sécurisées (Secure Email Gateway, SEG) sont inflexibles et inefficaces contre des menaces continuellement changeantes, telles que la compromission des adresses e-mail professionnelles, l'usurpation d'identité et les rançongiciels.

Cloudflare Area 1 offre une sécurité des e-mails préventive et cloud-native pour arrêter complètement ces attaques de phishing ciblées et d'autres.

Les organisations qui superposent Microsoft 365 à Cloudflare Area 1 bénéficient des avantages suivants :

- **Une protection exhaustive contre le phishing** couvrant les e-mails internes et externes, le trafic web et le trafic réseau
- **Une complexité informatique réduite** et une réponse plus rapide aux incidents de phishing
- **Un déploiement simple en quelques minutes**, avec une approche orientée API
- **Des investigations prioritaires du SOC**, avec la rétraction de messages après distribution et des intégrations aux solutions SIEM/SOAR

Comment pouvez-vous bloquer plus de menaces grâce à la sécurité des e-mails dans le cloud d'Area 1 ?

Microsoft 365 offre une excellente sécurité contre les menaces à grand volume transmises par e-mail ; cependant, les attaques par phishing à faible volume, extrêmement ciblées, qui sont à l'origine de plus de 90 % des violations de cybersécurité, peuvent encore se glisser à travers les mailles du filet.

Comment les organisations qui utilisent Microsoft 365 et doivent encore faire face à des tentatives de phishing manquées doivent-elles gérer les menaces modernes ?

C'est là qu'interviennent les solutions de **sécurité intégrée des e-mails dans le cloud** (Integrated Cloud Email Security, ICES). Selon Gartner®, « Les solutions qui s'intègrent directement à la messagerie cloud via une API, plutôt que sous forme de passerelle, facilitent l'évaluation et le déploiement et améliorent la précision de la détection, tout en tirant parti de l'intégration de l'essentiel de la protection contre le phishing avec la plateforme centrale ».[2]

« D'ici 2023, au moins 40 % des organisations utiliseront les fonctionnalités de protection intégrées des fournisseurs de messagerie cloud, plutôt qu'une passerelle de messagerie sécurisée, contre 27 % en 2020. »

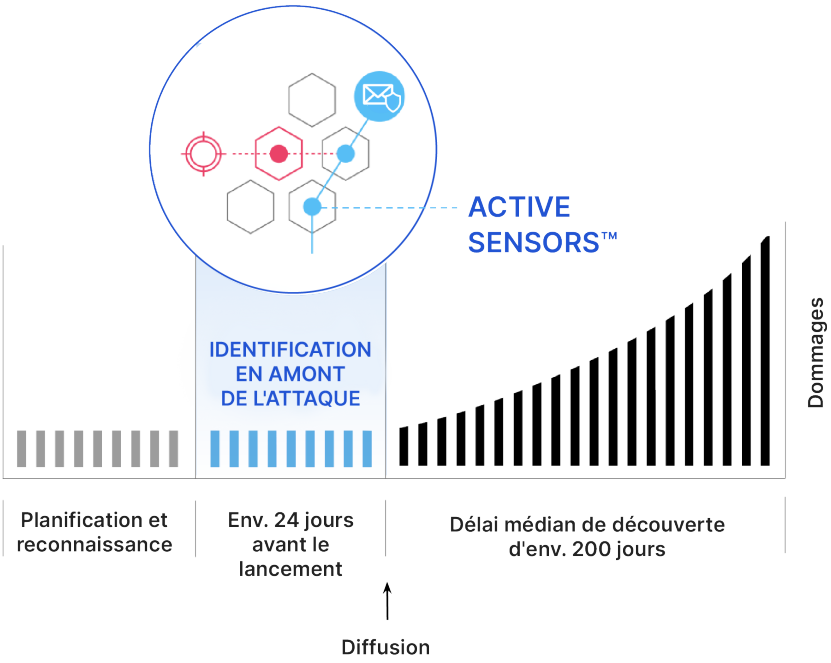
« D'ici 2025, 20 % des solutions anti-phishing seront mises en œuvre via l'intégration d'API avec la plateforme de messagerie, contre moins de 5 % aujourd'hui. »

– 2021 Gartner® Market Guide for Email Security

Area 1 Horizon (désormais appelé service de sécurité des e-mails Cloudflare Area 1) est nommée « Representative Vendor » dans la catégorie « Integrated Cloud Email Security (ICES) » du rapport Gartner Market Guide.

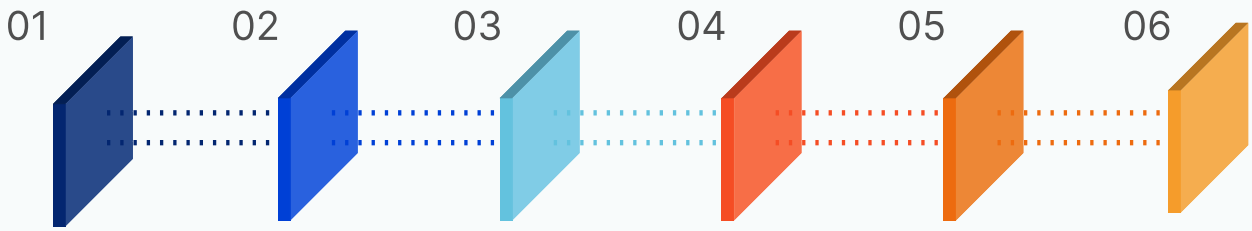
Contrairement à d'autres solutions, Area 1 **indexe continuellement et de manière proactive le web** afin d'identifier les nouvelles campagnes de phishing et les infrastructures d'acteurs malveillants « dans la nature ». En moyenne, Area 1 détecte préventivement les sites et les contenus malveillants 24 jours avant le lancement d'attaques.

Figure 1 : bloquez préventivement les attaques par phishing, avant qu'elles n'atteignent votre boîte de réception, avec Cloudflare Area 1



Area 1 emploie également une sélection de **techniques de détection plus avancées**, notamment NLU, NLP, l'analyse de graphiques de confiance (modèles de communication par e-mail) et la reconnaissance d'images afin de détecter et d'arrêter les attaques les plus sophistiquées, notamment les toutes nouvelles menaces ciblant avec précision un utilisateur, plutôt qu'une multitude d'utilisateurs.

Figure 2 : analysez le contenu, le contexte et les graphiques de confiance des communications par e-mail afin de bloquer les menaces modernes, telles que la compromission des adresses e-mail professionnelles



Analyse structurelle
En-têtes
Corps, images, interprétation de données visuelles
Liens, contenu

Modélisation NLU (Natural Language Understanding)
Modèles d'écriture
Catégories
Expressions

Analyse des sentiments
Intention, ton, relation, Hiérarchie

Analyse des fils
Conversations
Variations
Durée

Modélisation du secteur
Verticales
Lingua franca
Processus commerciaux

Confiance Graphiques
Graphiques de confiance des partenaires, historique d'envoi, recherche des usurpations de compte
Usurpation d'identité de partenaires

Un déploiement simple, en quelques minutes

Grâce à une approche orientée API, offrant une intégration fluide à Microsoft 365, le déploiement d'Area 1 ne demande que quelques minutes. Détectez et bloquez les attaques par phishing de manière plus précise et efficace, sans la complexité informatique qu'entraîne l'ajustement continu de la configuration d'une passerelle de messagerie sécurisée traditionnelle et inefficace.

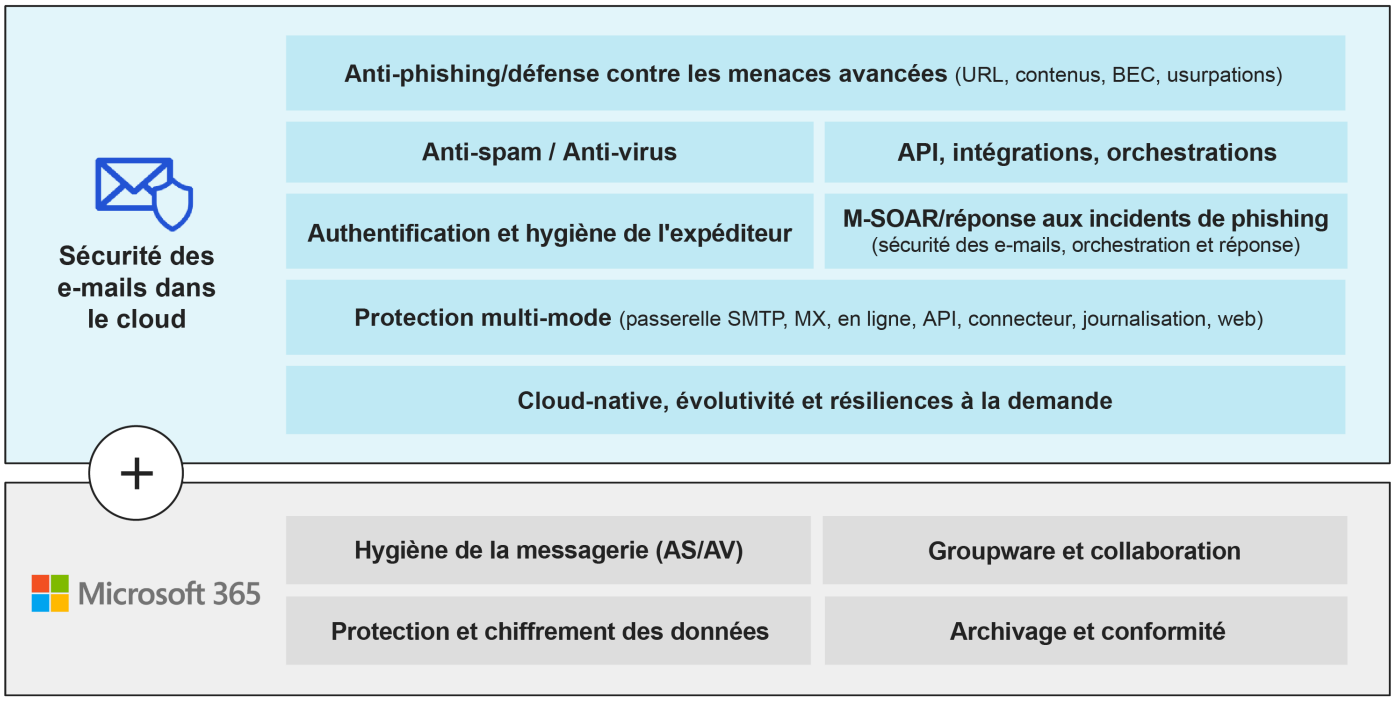
Figure 3 : exemple d'option de déploiement du service de sécurité des e-mails Area 1

Area 1 :

- Peut être déployée en moins de cinq minutes, sans nécessiter d'installation et sans affecter votre infrastructure existante ;
- Offre des options de déploiement plus flexibles (notamment MX/en ligne, connecteur et API) que d'autres solutions ;
- S'intègre avec fluidité aux autres fonctionnalités de sécurité des e-mails de Microsoft 365, telles que la protection anti-spam, la prévention des pertes de données, le chiffrement et l'archivage ;
- Peut facilement supprimer tout message malveillant directement dans les boîtes de réception de Microsoft 365, grâce aux fonctionnalités intégrées de correction et de rétraction de messages ; et
- Offre une expérience parfaitement transparente à vos utilisateurs finaux, tout en offrant des fonctionnalités exhaustives de détection et de protection contre le phishing.

La protection de vos environnements de messagerie Microsoft 365 avec Cloudflare Area 1 offre les avantages suivants :		
Une sécurité inégalée des e-mails dans le cloud	**Des flux de travail fluides**	**Une meilleure efficacité opérationnelle**
• Renforce les défenses natives de Microsoft pour offrir une protection complète contre les menaces modernes telles que la compromission des adresses e-mail professionnelles, les attaques par e-mail contre la chaîne logistique, les comptes de fournisseurs compromis, les menaces internes et bien d'autres. • Une visibilité plus étendue des menaces et les analyses médico-légales facilitent les investigations et améliorent les temps de réponse.	• Intégration en profondeur aux environnements, API et flux de travail Microsoft. • Intégration à ADFS, envoi d'alertes à Teams et transmission des journaux à Azure Sentinel. • Les utilisateurs finaux conservent les tableaux de bord natifs de Microsoft, garantissant une productivité continue et exempte de distractions.	• Service fondé sur une infrastructure dynamique et évolutive, afin de gérer les pics de trafic dans le cloud. • Remplace les passerelles de messagerie sécurisée traditionnelles, pour une sécurité et une efficacité opérationnelle améliorées. • Détection, triage et réponse avancés sur une plateforme unique, pour une défense en profondeur.

Préservez vos boîtes de réception contre les menaces avec une solution de sécurité intégrée et exhaustive de la messagerie cloud :



Microsoft + Cloudflare : pour un cloud plus sécurisé et plus privé

Cloudflare a construit des intégrations en profondeur avec Microsoft pour aider les organisations à franchir la prochaine étape de leur parcours Zero Trust. Ces intégrations permettent aux organisations d'améliorer l'efficacité opérationnelle des déploiements clients, tout en proposant une expérience utilisateur fluide et une évolutivité à la mesure de l'activité.

En plus d'Area 1, les intégrations de services Zero Trust de Cloudflare incluent :

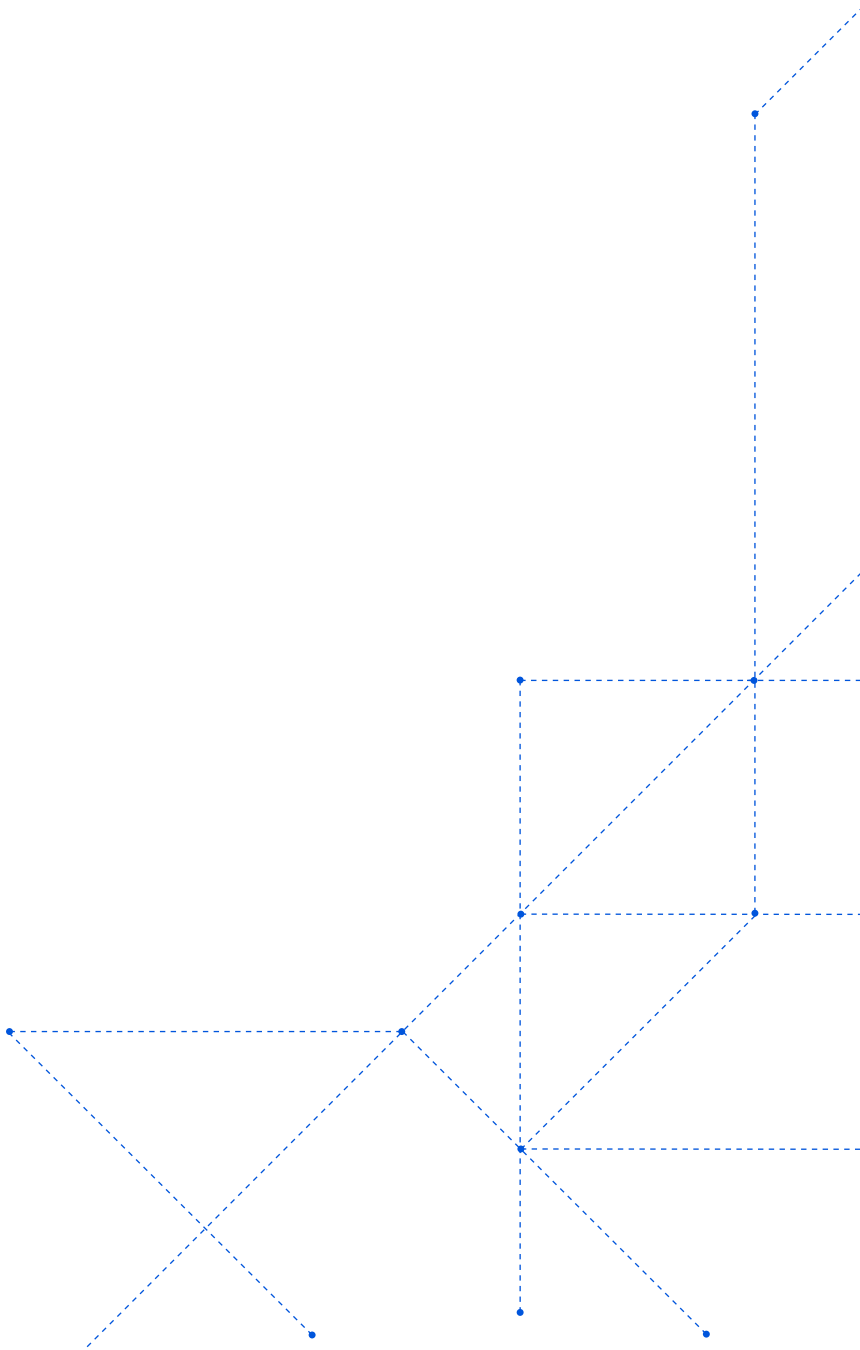
- **Azure Active Directory (AD)** – Tirez parti de puissants outils d'authentification tels que l'authentification multifacteur (MFA), les politiques d'accès conditionnel et les contrôles basés sur le risque.
- **Microsoft Cloud App Security (MCAS)** – Lancez l'intégration de M365 pour rechercher et présenter aux clients les nouveaux problèmes de sécurité concernant les utilisateurs, les données et les services intégrés aux applications de M365.
- **Zero Trust for Azure Apps** – Déployez un accès sécurisé aux applications sur site ou aux applications hébergées sur Azure, sans VPN.
- **Microsoft Endpoint Manager** – Évaluez le niveau de sécurité du client lors de la connexion via Microsoft Intune ; ceci permet à Cloudflare d'autoriser ou de refuser l'accès en fonction des signaux de sécurité ou de niveau de sécurité de l'appareil.
- **Microsoft 365** – Proposez une expérience utilisateur plus rapide et plus sécurisée en optimisant la connectivité des utilisateurs à Microsoft 365 via Cloudflare et le programme de partenariat réseau de Microsoft.

Pour en savoir plus sur les intégrations de partenaires de Cloudflare avec Microsoft, contactez-nous.

Pour découvrir comment Cloudflare Area 1 peut améliorer vos défenses contre le phishing dans Microsoft 365, demandez une évaluation personnalisée du risque ici.

Références

1 et 2 Gartner, « Market Guide for Email Security », 7 octobre 2021, Mark Harris, Peter Firstbrook, Ravisha Chugh, Mario de Boer



CLOUDFLARE
AREA 1 SECURITY

+33 75 7 90 52 73 | enterprise@cloudflare.com | www.cloudflare.com/fr-fr/

RÉV. : BDES-3778/2022SEPT07