CLOUDFLARE
AREA 1 SECURITY

DOSSIER DE SOLUTION

Cloudflare Area 1 et Google Cloud :

Sécurité intégrée des e-mails dans le cloud et sécurité préventive anti-phishing

Défis de l'industrie :

Les attaques par phishing sophistiquées actuelles, telles que la compromission des adresses e-mail professionnelles (BEC, Business Email Compromise) sans logiciel malveillant, la fraude par prise de contrôle de comptes et les menaces internes sont difficilement détectables par les passerelles de messagerie sécurisées traditionnelles ou les solutions d'authentification des e-mails.

La solution :

Le service Cloudflare Area 1 Email Security indexe proactivement le web afin de découvrir les campagnes de phishing. Il utilise ensuite ces informations précocement obtenues et des techniques d'analyse contextuelle des e-mails pour protéger vos boîtes de réception contre les attaques par phishing avant qu'elles ne puissent causer des dommages.

Conçue sur la plateforme Google Cloud, la solution Area 1 peut être déployée en quelques minutes seulement, et offre une couche incomparable de sécurité anti-phishing en profondeur.

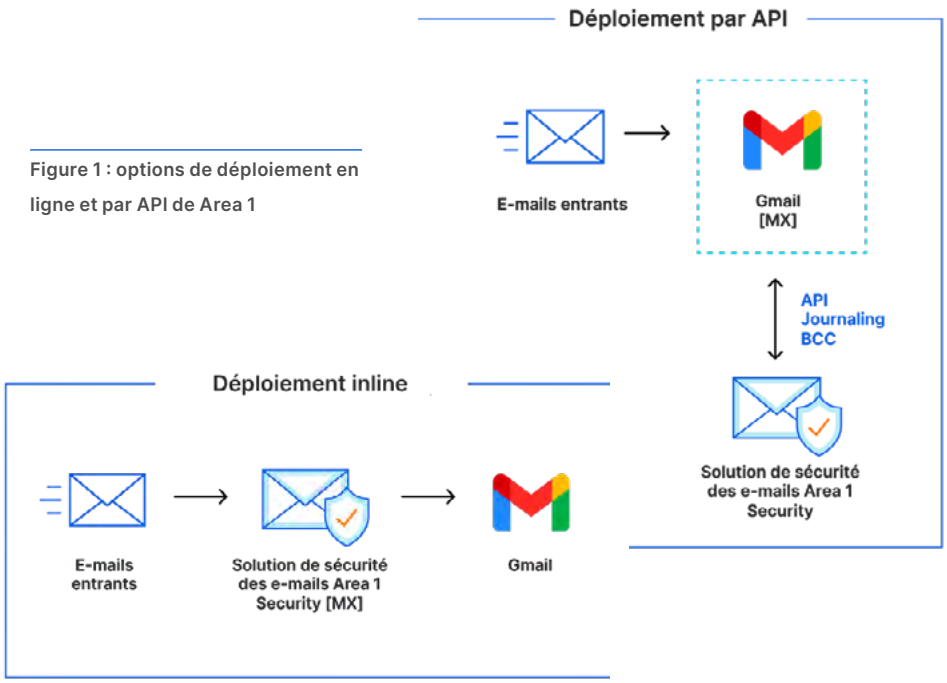

Figure 1 : options de déploiement en ligne et par API de Area 1

Défendez votre organisation contre les attaques modernes ciblant votre application cloud n° 1 : les e-mails

Arrêtez de manière préventive les attaques par phishing, la compromission des adresses e-mail professionnelles (BEC), la fraude par e-mail et d'autres menaces avancées.

Isolez et prévenez les menaces multicanaux grâce à l'intégration de Cloudflare Area 1 et de la solution d'isolation de navigateur à distance de Cloudflare.

Découvrez les comptes et les domaines compromis, ainsi que les domaines nouveaux, semblables et proches utilisés par les acteurs malveillants pour contourner les standards SPF/DKIM/DMARC.

Pourquoi opter pour Cloudflare Area 1 :

Sécurité préventive

Identifiez à l'avance l'infrastructure et les mécanismes de diffusion employés par les auteurs d'attaques afin d'arrêter les attaques par phishing dès les premières étapes de leur cycle.

Une protection complète

La solution couvre l'intégralité des types d'attaques reposant sur les e-mails (URL, contenus malveillants, compromission des adresses e-mail professionnelles), des vecteurs (e-mail, web, réseau, multicanal) et des canaux d'attaque (externe, interne, partenaires de confiance).

Analyse contextuelle

Tirez profit de techniques de détection avancées (analyse du langage, vision artificielle, analyse graphique sociale et bien d'autres) pour intercepter les tentatives de compromission des adresses e-mail professionnelles et d'utilisation frauduleuse des adresses e-mail de fournisseurs, ainsi que les autres menaces avancées.

Protection continue

Déployez une défense approfondie avec des couches de protection contre les menaces placées avant, pendant et après la réception d'un e-mail.

Pourquoi opter pour Cloudflare Area 1 et Google Cloud :

- **Améliorer l'efficacité opérationnelle –** Réduisez la complexité en remplaçant les passerelles de messagerie sécurisées traditionnelles par une architecture moderne, orientée cloud.
- **Déploiement fluide et flexible –** Déployez le service élastique Area 1 en moins de 5 minutes et bénéficiez de l'intégration transparente avec les fonctionnalités natives de Google Cloud, telles que la protection anti-spam, la prévention des pertes de données, le chiffrement et l'archivage.
- **Sécurité SaaS simplifiée –** En plus de la sécurité intégrée des plateformes de messagerie cloud Area 1, la plateforme Cloudflare Zero Trust fournit des fonctionnalités d'agent de sécurité des accès au cloud (CASB, Cloud Access Security Broker) pour Google. Prévenez facilement les fuites de données et les violations de conformité et bénéficiez d'une solution exhaustive et unique pour mettre un terme aux pertes de données, au phishing, aux rançongiciels, au Shadow IT et aux mouvements latéraux dans l'ensemble de votre organisation.

Étude de cas : une entreprise leader des biens de consommation courante cotée à l'indice S&P 100 protège sa direction et les utilisateurs contre les menaces liées à sa solution de messagerie cloud.

Défis du client	Résultats avec Cloudflare Area 1
• Menaces échappant à Google Workspace et à l'infrastructure de sécurité existante • Attaques par compromission des adresses e-mail professionnelles ciblant la direction et les membres du conseil d'administration • L'équipe informatique consacre du temps et des ressources à la configuration continue des règles de sécurité des e-mails et des listes de blocage	• Plus de 8 millions d'attaques ciblées bloquées en un an • L'équipe informatique est désormais en mesure de fournir de meilleurs indicateurs et rapports d'information sur la sécurité des e-mails lors des réunions du conseil d'administration • Amélioration de la productivité et réduction considérable du risque de cybersécurité

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