
BlueFinch ESB
Zero Trust
File Transfer

Les challenges

Pour de nombreuses organisations, les méthodes de sécurité telles que le chiffrement PGP ne suffisent plus, car une fois les fichiers téléchargés et non chiffrés, ces fichiers peuvent toujours être partagés avec des destinataires non autorisés. Ils ont encore besoin d'un moyen d'appliquer la méthode Zero Trust à leurs transferts de fichiers.

Une autre limitation est l'impossibilité d'envoyer des fichiers volumineux de manière sécurisée avec des parties externes. Une situation critique lorsque l'on tente de partager des fichiers de fabrication, des productions médias, etc.

De plus, avec l'augmentation des politiques réglementaires, étatiques et gouvernementales en matière de protection des fichiers, les entreprises doivent également s'assurer que les données sont protégées conformément aux exigences de conformité.

La solution

La sécurisation des documents transitent et au repos grâce aux transfertx de fichiers sécuriséx est une étape importante pour protéger les données de votre entreprise, des partenaires et des clients. Dans un cadre de sécurité Zero Trust, aucune personne ni aucun système qui tentant d'accéder aux données n'est automatiquement approuvé.

Comment ça marche ?

Ce pack combine la puissance des solutions suivantes :

- Les transferts de fichiers sécurisés
- ICAP Gateway
- Les outils collaboratifs sécurisés et le contrôle des accès

Votre équipe a besoin de collaborer avec l'externe mais des données sensibles sont impliquées.

Partagez des données sensibles via un navigateur ou un courrier électronique chiffrer avec une solution de transferts de fichiers.

Zero Trust signifie que les fichiers peuvent rester protégés même hors ligne, en contrôlant qui a accès et où ils peuvent être partagés.

L'accès aux documents protégés peut être révoqué à tout moment, même si l'utilisateur est hors ligne.

Vos données restent protégées tout au long de leur parcours collaboratif.

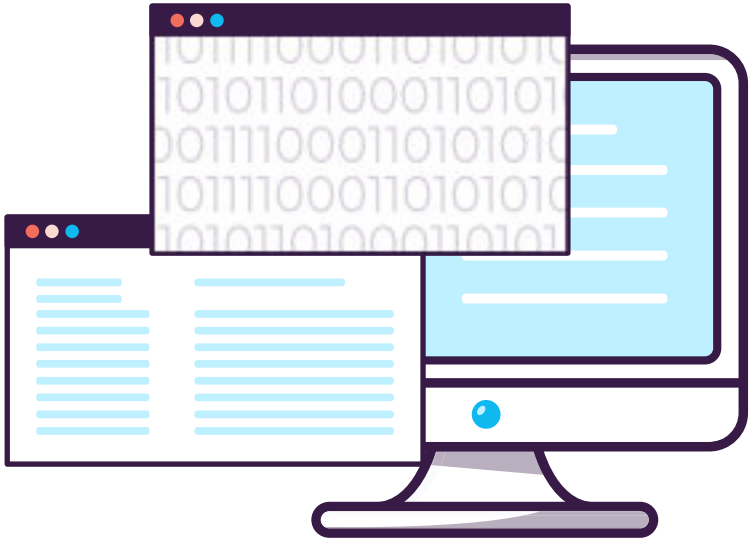
Cas d'étude

- **Envoyez ou recevez des fichiers volumineux par courrier électronique en les chiffrant.** Le chiffrement reste associé au fichier, même après son téléchargement et l'accès peut être révoqué à tout moment.

- **Ajouter des fichiers protégés à des dossiers partagés.** Protégez-les afin que seuls les utilisateurs autorisés puissent ouvrir et télécharger les fichiers en fonction des politiques internes. Une fois ces fichiers téléchargés, gardez en le contrôle.

- **Téléchargez en toute sécurité des fichiers via des formulaires web.** Permettez à GoAnywhere d'appliquer une collaboration sécurisée à chaque pièce jointe, en envoyant un lien de téléchargement protégé par Vera aux destinataires et en n'autorisant l'accès qu'aux personnes habilitées.

- **Inspecter les fichiers à la recherche de menaces et d'informations sensibles.** Avant d'envoyer ou de recevoir des fichiers, vérifiez qu'ils ne contiennent pas de virus ou de logiciels malveillants. Supprimez les métadonnées indésirables ou les informations sensibles avant de continuer à partager le fichier.



Informations complémentaires GoAnywhere

La solution Vera renforce le chiffrement des fichiers de GoAnywhere MFT. Les clients GoAnywhere doivent posséder les modules Advanced Workflows et Secure Forms, pour pouvoir étendre cette optimisation.

A propos

BlueFinch-ESBD est partenaire platinium et privilégié de Fortra. Nous collaborons ensemble depuis plus de 10 ans et avons mené de nombreux projets. Fortra est une société de cybersécurité qui développe un portefeuille de solutions complètes et évolutives.

www.bluefinch-esbd.com