

Plateforme de chiffrement des courriels

Plateforme de chiffrement des courriels Echoworx

Il s'agit d'un service haute performance de protection des données de messagerie, fondé sur une approche périmétrique, conçu pour protéger durablement vos informations sensibles. Il regroupe l'envoi des courriels et la distribution de documents au sein d'un système unifié.

Chiffrement des courriels Echoworx : méthode de diffusion unique

Offre aux organisations la possibilité de sélectionner une seule méthode de diffusion sécurisée à partir de notre plateforme de protection des données de messagerie.

Chiffrement des courriels Echoworx : documents à grand volume

Conçue pour les besoins intensifs et la diffusion de masse, cette option permet aux organisations d'envoyer des volumes pratiquement illimités de documents chiffrés et de relevés sécurisés.

Principaux différenciateurs et avantages

- **Nombreuses méthodes de diffusion (Push/Pull)**

Nous prenons en charge le portail Web, TLS (avec repli), le chiffrement intégral des messages, le chiffrement des pièces jointes uniquement (PDF, ZIP, Office XML), S/MIME et PGP. Cela facilite l'utilisation pour les expéditeurs comme pour les destinataires. La solution est optimisée pour les appareils mobiles. Les utilisateurs peuvent choisir leur méthode de diffusion sécurisée préférée, y compris des options ne nécessitant aucune inscription.

- **Gestion des certificats S/MIME**

Simplifiez votre gestion de S/MIME à l'échelle de chaque tenant. Récupérez automatiquement les certificats des destinataires, générez de nouvelles clés et intégrez des autorités de certification de confiance comme DigiCert et SwissSign. Vous pouvez générer des identifiants auto-signés ou permettre aux destinataires de téléverser leurs propres certificats x509. Notre système prend en charge les messages S/MIME signés en mode opaque et en mode clair pour la vérification des signatures entrantes.

- **Gestion des clés PGP**

Tirez parti d'une solution PGP entièrement gérée et hébergée dans le cloud pour la génération automatisée des clés, le stockage sécurisé et la migration fluide des clés. Nous prenons en charge la récupération des clés basée sur LDAP ainsi que le téléversement de clés publiques par les destinataires.

- **Contrôle adossé au matériel**

Nous proposons des capacités MYOK (*Manage Your Own Key*) ainsi qu'une prise en charge complète des modules matériels de sécurité (HSM), alimentés par AWS KMS, avec validation FIPS 140-3 niveau 3.

- **Contrôles d'authentification et d'accès**

L'authentification peut être définie par politique, par l'expéditeur ou par le destinataire. Les options incluent : l'auto-inscription, la phrase secrète définie par l'expéditeur, les connecteurs sociaux (OAuth), OpenID et l'authentification unique (SSO), les codes de

vérification générés par le système et l'authentification à deux facteurs (2FA). Nous prenons également en charge les biométries comme les passkeys et les lecteurs d'empreintes digitales, pour offrir une simplicité de niveau grand public à une sécurité de niveau entreprise.

- **Protection de marque étendue**

Préservez l'intégrité de votre marque grâce à des fonctionnalités telles que les domaines vanity, les indicateurs de marque pour l'identification des messages (BIMI) et les modèles personnalisables. Appliquez les éléments de marque à l'ensemble des notifications afin de renforcer votre identité et de consolider votre réputation. Nous prenons en charge le multimarque via des politiques de profil et de modèles, et assurons un routage conforme au DMARC pour tous les messages sortants.

- **Conception inclusive**

Notre protection de marque et la conformité de notre interface répondent aux exigences strictes des normes WCAG 2.2 niveau AA.

- **Localisation sur mesure**

Choisissez parmi 28 options linguistiques, y compris la prise en charge des caractères double octet pour des langues comme le chinois et le japonais. Des avertissements de message intégrés et personnalisables peuvent être insérés de manière fluide dans l'en-tête comme dans le pied de page.

- **Rapports et visibilité pilotés par API**

Echoworx simplifie l'accès aux fichiers journaux pour les équipes informatiques. Vous pouvez extraire en toute sécurité les données d'audit à l'aide de clés API. Chaque action administrateur et chaque journal de traitement des messages alimentent directement votre SIEM pour un reporting d'activité précis et fiable ainsi qu'une journalisation simple des événements, tels que l'ouverture, le transfert et le rappel des courriels.

Réalisez des gains concrets grâce à des investissements plus judicieux

Avec un taux de renouvellement annuel supérieur à 98 %, nous sommes fiers d’offrir l’alliance idéale entre la protection des données de messagerie et la simplicité d’utilisation.

Efficacité des coûts et des ressources

Nous sommes entièrement consacrés à la protection des données que vous transmettez par courriel. Notre feuille de route, guidée par les besoins de nos clients, apporte des améliorations concrètes — rationalisation des flux de travail, renforcement de la sécurité et réduction des frictions — pour vous aider à répondre aux exigences d’aujourd’hui tout en anticipant les défis de demain.

Gardez le contrôle sur vos informations

Echoworx dispose de centres de données aux États-Unis, au Royaume-Uni, en Allemagne, en Irlande et au Canada. Répondre aux exigences modernes comme KRITIS-DachG, NIS 2 et DORA nécessite des capacités de chiffrement de nouvelle génération. Nous veillons à ce que vos données restent étroitement contrôlées et géographiquement proches, tout en respectant ces exigences réglementaires strictes et évolutives.

Développez votre activité numérique

Notre plateforme de chiffrement des données de messagerie regroupe l’envoi des courriels et la distribution de documents au sein d’une seule plateforme, conçue pour répondre à vos besoins intensifs — et non les freiner. Elle vous aide ainsi à atteindre une véritable efficacité économique.

Améliorez l’efficacité opérationnelle

Echoworx s’intègre de manière transparente à votre écosystème de sécurité existant, notamment Gmail, Outlook, Proofpoint et Mimecast, tout en s’harmonisant avec des règles DLP complexes. Que votre environnement soit sur site, dans le cloud ou hybride, notre plateforme garantit un chiffrement invisible au sein de vos flux de travail.

Assurance de sécurité validée

Nous soumettons nos pratiques de sécurité à des audits rigoureux couvrant tous les aspects de notre activité. Nos certifications incluent l’audit SOC2, la certification PCI DSS niveau 1, FSQS (*Financial Services Qualification System*), la qualification AWS et la certification OpenID Connect RP.

