

Une plateforme. Chaque destinataire. Sécurisé à chaque fois.

Votre guide des options de livraison Echoworx — et la méthode plus intelligente pour protéger chaque message qui quitte votre entreprise

Chaque jour, votre organisation envoie des informations sensibles à des clients, des partenaires, des régulateurs et des collègues qui travaillent chacun différemment et attendent une expérience différente. Echoworx se situe à la frontière de votre environnement, évalue chaque message sortant par rapport à votre politique et le route automatiquement via la bonne méthode de livraison. Les pages suivantes vous guident à travers chaque option à tour de rôle, afin que vous puissiez associer la bonne méthode au bon destinataire en toute confiance.

Encryption Options Delivered in 28 Languages

Pull				Push		Direct			
Portal User (default)		Portal Message Level		Full Message	Attachment (PDF, Office, ZIP)	TLS	PGP (with certificate harvesting)	S/MIME (with certificate harvesting)	
							DigiCert API		
							SwissSign API		
							AWS API		
Authentication Options									

Authentication Options

OAuth	OpenID	SSO	2FA (TOTP & Phone)	PassKey	Sender Set	Out Of Band	No Auth	Text & Call	Sender Set	User Managed	Sender Set	User Managed
-------	--------	-----	--------------------	---------	------------	-------------	---------	-------------	------------	--------------	------------	--------------

Portail Web

Lorsque des informations sensibles nécessitent un espace contrôlé et traçable, le Portail Web Sécurisé les livre sans la fatigue des mots de passe qui frustre les destinataires et inonde l'informatique de tickets de réinitialisation. Les destinataires s'authentifient à l'aide d'identifiants qu'ils connaissent déjà, les expéditeurs et les administrateurs conservent une visibilité totale sur chaque message, et la gouvernance accompagne chaque communication depuis la première livraison jusqu'à la réponse et le rappel.

Fonctionnalités clés

- **Connexion fédérée et OAuth 2.0** : Prise en charge complète d'OAuth 2.0 pour Microsoft 365, Gmail, Hotmail, Facebook, LinkedIn, Salesforce et d'autres fournisseurs. Les destinataires se connectent avec des identifiants qu'ils possèdent déjà — pas de nouveaux comptes, pas de nouveaux mots de passe.
- **OpenID Connect** : Les organisations prenant en charge OpenID pour l'authentification permettent aux destinataires de se connecter avec leurs identifiants actuels, en contournant entièrement la création de nouveaux comptes.
- **Intégration SSO** : L'intégration des services web permet la connexion automatique via un portail d'entreprise existant, intégrant de manière transparente l'accès aux messages sécurisés dans l'environnement familier du destinataire.
- **Mode sans authentification** : Pour les communications à faible risque, les destinataires accèdent aux messages via un lien direct sans connexion requise, tandis que l'activité des messages et le suivi des réponses entrantes sécurisées restent actifs.
- **Mot de passe défini par l'expéditeur** : Les expéditeurs définissent une phrase secrète partagée avec un indice facultatif via le complément M365 Outlook, communiquée au destinataire par un canal distinct. Les destinataires accèdent au message sans s'inscrire.
- **Vérification par message texte** : Les expéditeurs saisissent un numéro de téléphone du destinataire via le complément M365 Outlook et un code à usage unique est envoyé sur l'appareil du destinataire pour l'authentification au portail.
- **Vérification par appel vocal pour la vérification en 2 étapes** : Pour les destinataires qui ne peuvent pas recevoir de message texte — que ce soit en raison de leur emplacement, de leur connectivité ou de leurs besoins en matière d'accessibilité — la livraison par appel vocal constitue une alternative fiable, maintenant l'accès sans délais ni réclamations.
- **Clés d'accès (accès sans mot de passe)** : L'authentification biométrique via un lecteur d'empreintes digitales ou la biométrie de l'appareil permet un accès sécurisé en une seule étape au portail à l'aide d'un code PIN ou d'un remplissage automatique biométrique.
- **Contrôles Répondre à tous** : Limite le Répondre à tous du portail aux abonnés internes et supprime automatiquement les domaines non reconnus des brouillons, fermant un chemin courant vers l'exposition accidentelle de données et renforçant votre politique DLP.
- **Transfert sécurisé des messages** : Restreint les destinataires enregistrés au transfert de messages uniquement au sein des domaines autorisés, maintenant la collaboration dans un canal sécurisé et entièrement auditable.
- **Ajout de destinataires au portail** : Permet aux destinataires enregistrés d'ajouter des participants lors d'actions de réponse ou de transfert, dans le même environnement régi par les politiques, afin que le vrai travail d'équipe ne quitte jamais vos limites définies.
- **Contrôles de notification par destinataire** : Permet aux destinataires de se désabonner des notifications de rappel et finales, réduisant la friction dans la boîte de réception sans compromettre l'intégrité des échanges.
- **Accessibilité** : La conformité WCAG élargie sur l'ensemble du portail destinataire répond au niveau d'accessibilité désormais standard dans les appels d'offres d'entreprise et les audits de conformité.

Fonctionnalités supplémentaires

- Livraison indépendante des appareils sur toutes les principales plateformes et facteurs de forme, où que travaillent vos destinataires.
- Contrôles de marque étendus pour les pages destinées aux clients, les messages chiffrés et les notifications, afin que les destinataires reconnaissent toujours la source.
- Prise en charge de la localisation en 28 langues.
- Tous les messages stockés chiffrés au repos dans le cloud Echoworx, avec des périodes de conservation standard de 30, 60 ou 90 jours et des durées prolongées disponibles sur demande.
- Exportation locale des messages aux formats Outlook et PDF chiffré pour la conservation à long terme par le destinataire.
- Gestion des mots de passe disponible pour les expéditeurs et les destinataires.
- Fonctionnalité de réponse sécurisée et d'accusé de réception pour des échanges continus et auditaibles.
- Capacités complètes d'audit et de rappel des messages pour les expéditeurs et les administrateurs.
- Accessibilité : La conformité WCAG élargie sur l'ensemble du portail destinataire répond au niveau d'accessibilité désormais standard dans les appels d'offres d'entreprise et les audits de conformité.

Note technique

Les messages sont accessibles en ligne via le portail et ne sont pas stockés de façon permanente sur l'appareil local du destinataire. Les destinataires qui ont besoin de conserver une copie à long terme doivent sauvegarder ou exporter les messages à leur réception.

Ce que cela signifie pour vous : Vos destinataires se connectent avec des identifiants en lesquels ils ont déjà confiance et accèdent à leurs messages en quelques secondes — sur n'importe quel appareil, dans n'importe quelle langue, sans créer de nouveaux comptes. Vos expéditeurs gardent un contrôle total sur qui lit, répond et transfère chaque message. Et votre organisation répond aux normes de gouvernance, d'accessibilité et de conformité que les régulateurs et les équipes d'achat considèrent désormais comme standard.

PDF chiffré

Parfois, la façon la plus rapide de protéger des informations sensibles est de les envoyer sous forme de document verrouillé, et non d'un lien vers un portail. La livraison par PDF chiffré sécurise à la fois le corps du message et ses pièces jointes en utilisant les technologies fiables Secure PDF, Office 365 et ZIP. Les destinataires reçoivent un fichier familier qu'ils peuvent ouvrir, enregistrer et conserver, tandis que votre organisation maintient le contenu protégé dès l'instant où il quitte votre passerelle.

Fonctionnalités clés

- **Accès par code de vérification :** Imaginez l'envoi d'un document sécurisé à un destinataire non technique dans un délai serré. L'inscription devient un goulot d'étranglement. Cette méthode de chiffrement de document le supprime entièrement. L'expéditeur partage un code généré à la volée via un canal séparé, comme un rapide appel téléphonique, et le destinataire l'utilise pour ouvrir immédiatement le PDF chiffré ou les pièces jointes. Pas d'inscription, pas de mots de passe, pas de délais — juste une sécurité qui avance au rythme de la conversation.
- **Auto-inscription :** Les destinataires définissent leur propre mot de passe via une seule invite unique, ce qui simplifie le premier accès.
- **Gestion des mots de passe :** Les destinataires récupèrent ou mettent à jour leur mot de passe via un lien en libre-service, sans appeler votre service d'assistance.
- **Mots de passe définis par l'expéditeur :** Les expéditeurs créent une phrase de passe partagée et la transmettent au destinataire hors bande, offrant aux deux parties un contrôle sur l'accès.
- **Visualisation transparente :** Les PDF chiffrés et les documents Office s'ouvrent directement dans Gmail ou Outlook pour le Web, sans rien de nouveau à télécharger ou à installer.

Fonctionnalités supplémentaires

- Livraison flexible sur n'importe quel appareil, où que travaillent vos destinataires.
- Image de marque personnalisable pour les messages et les notifications, afin que les destinataires reconnaissent toujours la source.
- Prise en charge de 28 langues.
- Accès hors ligne avec chiffrement au repos, permettant aux destinataires de conserver des copies sécurisées aussi longtemps qu'ils en ont besoin.
- Réponses sécurisées avec copies pour les destinataires, maintenant la conversation protégée dans les deux sens.

Note technique

Le chiffrement par push livre chaque message directement au destinataire pour un accès immédiat. Étant donné que le document arrive directement dans leur boîte de réception, les messages envoyés de cette façon ne peuvent pas être rappelés.

Ce que cela signifie pour vous : Vos destinataires reçoivent un document simple et familier qu'ils peuvent ouvrir sur n'importe quel appareil, votre équipe peut atteindre même les contacts non techniques en quelques secondes grâce aux codes de vérification, et votre contenu sensible reste protégé de l'envoi à l'ouverture.

Pièce jointe chiffrée

Lorsque des informations sensibles doivent circuler rapidement, le chemin le plus sûr est parfois le plus simple : une pièce jointe verrouillée qui arrive directement dans la boîte de réception du destinataire. La livraison par pièce jointe chiffrée protège vos documents tout en laissant le corps du message en texte clair, de sorte que les destinataires reçoivent un e-mail familier avec un fichier sécurisé qu'ils peuvent ouvrir, enregistrer et conserver. C'est la solution idéale pour les travaux à volume élevé axés sur les documents, comme le traitement de relevés électroniques en masse, où la rapidité et la sécurité doivent aller de pair.

Fonctionnalités clés

- **Accès par code de vérification** : Imaginez envoyer un document sécurisé à un destinataire non technique dans un délai serré. L'étape d'inscription traditionnelle devient un goulot d'étranglement. Cette méthode par code de vérification la supprime entièrement. L'expéditeur partage un code généré à la volée via un canal séparé, comme un rapide appel téléphonique, et le destinataire l'utilise pour ouvrir immédiatement la pièce jointe chiffrée. Pas d'inscription, pas de mot de passe, pas de délai. Une sécurité qui suit le rythme d'une conversation, et non d'une file d'attente administrative.
- **Vérification par appel vocal pour la vérification en 2 étapes** : Lorsqu'un destinataire ne peut pas recevoir de message texte — en raison de son lieu de résidence, d'un besoin d'accessibilité ou simplement d'un problème de signal — la vérification par appel vocal pour la vérification en 2 étapes lui offre une alternative fiable. L'accès reste ouvert, les délais d'authentification diminuent, et les réclamations des destinataires aussi.
- **Chiffrement natif pour PDF, Microsoft Office et ZIP** : Les pièces jointes sont chiffrées nativement, en préservant le nom d'origine et les propriétés de chaque fichier, afin que les destinataires reconnaissent exactement ce qu'ils ouvrent.
- **Visualisation transparente** : Les PDF et documents Office chiffrés s'ouvrent directement dans Outlook pour le Web et le client Gmail, sans rien de nouveau à télécharger ou à installer.
- **Prise en charge étendue des fichiers** : Les autres types de pièces jointes sont regroupés dans un PDF ou un format ZIP chiffré, de sorte qu'aucun document ne reste non protégé.
- **Auto-inscription** : Les destinataires définissent leur propre mot de passe via une seule invite unique, ce qui simplifie le premier accès.
- **Phrase de passe partagée définie par l'expéditeur** : Les expéditeurs créent une phrase de passe partagée et la communiquent au destinataire hors bande, donnant aux deux parties le contrôle de l'accès.
- **Corps du message personnalisé et à l'image de la marque** : Les en-têtes et pieds de page peuvent contenir un lien de gestion des mots de passe ou un indice discret pour la phrase de passe partagée, afin que les destinataires sachent toujours qu'ils sont au bon endroit.

Fonctionnalités supplémentaires

- Lisez des documents sécurisés n'importe où, sur n'importe quel appareil, où que travaillent vos destinataires.
- Conservez le corps du message en texte clair tandis que seules les pièces jointes sont chiffrées, de sorte que le contexte habituel reste lisible.
- Envoyez plusieurs pièces jointes chiffrées dans leurs formats d'origine au sein d'un seul e-mail.
- Atteignez un public mondial grâce à la prise en charge multilingue en 28 langues.
- Livrez directement dans la boîte de réception du destinataire, sans visite de portail requise.
- Protégez les pièces jointes chiffrées au repos, de sorte que les fichiers restent sécurisés longtemps après leur réception.
- Choisissez des options de mot de passe flexibles définies par les expéditeurs ou les destinataires, y compris la vérification par téléphone et les clés d'accès.
- Ouvrez des documents sécurisés hors ligne, à tout moment et n'importe où pour les destinataires.

Note technique

Echoworx recommande un logiciel ZIP capable d'ouvrir des fichiers AES 256 bits, notamment WinZip, Secure ZIP, WinRAR et notre préféré, 7-Zip. Gardez à l'esprit que le chiffrement push livre chaque e-mail immédiatement au destinataire ; ainsi, les messages envoyés de cette manière ne peuvent pas être rappelés par Echoworx.

Ce que cela signifie pour vous : Vos destinataires reçoivent un e-mail familier avec un fichier sécurisé qu'ils peuvent ouvrir sur n'importe quel appareil, votre équipe peut contacter même des contacts non techniques en quelques secondes grâce aux codes de vérification et à la vérification par appel vocal inclusive, et vos documents sensibles restent protégés de l'envoi à l'ouverture.

Chiffrement TLS avec Basculement

Certains messages doivent circuler discrètement et instantanément, sans mots de passe, sans portails, et sans étapes supplémentaires pour quiconque. Le chiffrement TLS avec basculement fait exactement cela : il chiffre vos messages et pièces jointes en transit et les achemine directement au destinataire. Lorsque le domaine d'un destinataire ne prend pas en charge TLS, la plateforme ne laisse jamais un message exposé. Elle bascule automatiquement vers un autre canal sécurisé, de sorte que la protection reste constante et la livraison reste sans effort.

Fonctionnalités Clés

- **Validation TLS à la volée** : La plateforme vérifie la validité de chaque connexion TLS en temps réel, de sorte que chaque message est contrôlé pour un chemin véritablement sécurisé avant d'être envoyé.
- **Contrôle par liste d'autorisation** : Configurez une liste d'autorisation pour envoyer des messages uniquement aux domaines TLS de confiance, vous donnant un contrôle strict sur les destinations vers lesquelles le courrier sécurisé peut voyager.
- **Contrôle par liste de blocage** : Créez une liste de blocage pour exclure des domaines TLS spécifiques, fermant toute voie que vous ne souhaitez pas utiliser.
- **Basculement sécurisé automatique** : Lorsqu'un domaine n'est pas éligible à la livraison TLS, Echoworx bascule de manière transparente vers une méthode sécurisée alternative, telle que le Portail Web ou le PDF sécurisé, afin que la protection ne soit jamais interrompue.
- **Conformité sans effort** : Ce basculement transparent applique votre politique de sécurité sans intervention manuelle, prenant en charge les contrôles résilients attendus dans le cadre de réglementations telles que DORA et NIS2.

Fonctionnalités Supplémentaires

- Les expéditeurs envoient simplement leurs messages, tandis que la plateforme de chiffrement décide quand utiliser TLS et quand basculer vers une autre méthode.
- Les destinataires ne changent rien, car la livraison transparente maintient une expérience familière de bout en bout.
- De nombreuses options de personnalisation de la marque vous permettent de personnaliser les en-têtes et les pieds de page afin que chaque message soit incontestablement le vôtre.
- Idéal pour les environnements B2B où les deux parties s'appuient déjà sur TLS pour les échanges sécurisés.

Note Technique

Une fois qu'un message est livré via TLS, il n'est pas chiffré au repos dans la boîte de messagerie du destinataire. Les réponses sécurisées voyagent en dehors de la plateforme Echoworx et s'appuient sur la propre connexion TLS du destinataire pour la protection en transit.

Ce que cela signifie pour vous : Vos expéditeurs continuent d'envoyer sans y penser à deux fois, vos destinataires reçoivent des courriers sécurisés sans rien de nouveau à apprendre, et votre organisation maintient sa politique de sécurité appliquée automatiquement, jusqu'aux contrôles de conformité que les régulateurs attendent.

Chiffrement par certificat

Lorsque vos destinataires possèdent déjà un certificat S/MIME ou PGP de confiance, le chiffrement par certificat le met automatiquement à contribution. Les messages et les pièces jointes sont chiffrés de bout en bout, signés pour authenticité, et livrés sans demander à quiconque de modifier sa façon de travailler.

Fonctionnalités clés

- **Découverte flexible des certificats** : Les certificats des destinataires sont localisés automatiquement via des recherches externes dans les annuaires LDAP, de sorte que l'échange de confiance démarre sans effort manuel.
- **Recherches dynamiques de clés des destinataires** : Echoworx découvre les clés PGP sur un serveur de clés LDAP à l'aide d'un URI standard dans le domaine du destinataire, simplifiant la livraison sécurisée dans l'ensemble de votre écosystème partenaire.
- **Téléversements en libre-service par les destinataires** : Les destinataires téléversent leur propre certificat x509 ou clé publique PGP directement via le portail web, ou génèrent un certificat S/MIME auto-signé lorsqu'ils n'en possèdent aucun.
- **Racines de confiance à la demande** : L'intégration transparente avec DigiCert et SwissSign récupère et génère des identifiants S/MIME de confiance pour vos employés au moment où une clé est nécessaire.
- **Génération de clés PGP en temps réel** : Echoworx crée des paires de clés publiques/privées PGP pour les expéditeurs à la volée, et le destinataire du message chiffré reçoit la clé publique de l'expéditeur en pièce jointe, rendant chaque échange autonome.
- **Signature pilotée par politique avec repli** : Les messages sortants sont signés numériquement à l'aide d'une clé liée à l'adresse e-mail de l'expéditeur, qu'elle soit téléversée ou générée. Si aucune n'est disponible, une clé de niveau entreprise, couvrant l'ensemble du domaine, intervient afin que les messages soient toujours signés.
- **Signature PGP « Expéditeur uniquement »** : Tout message que la passerelle ne peut pas signer valablement est renvoyé avec une réponse de non-livraison, étendant la même protection éprouvée, déjà reconnue pour S/MIME, aux communications signées PGP.
- **Tailles de clés configurables** : Définissez les tailles des clés S/MIME et PGP générées automatiquement au niveau du profil — RSA 2048, 3072 ou 4096 bits — la valeur par défaut étant désormais relevée à 3072 bits pour maintenir la robustesse cryptographique en conformité avec les normes modernes.
- **Déchiffrement entrant** : Les messages entrants chiffrés par S/MIME et PGP sont déchiffrés à l'aide de clés privées stockées de façon sécurisée sur la plateforme Echoworx, puis livrés avec des en-têtes et pieds de page de marque appliqués.
- **Déchiffrement PGP en libre-service** : Acheminez les messages chiffrés au niveau des points de terminaison existants vers la passerelle pour déchiffrement, maintenant les archives historiques accessibles, auditable et intactes.

Fonctionnalités supplémentaires

- **Renouvellement automatique des clés S/MIME arrivant à expiration** : Pour les clients DigiCert et SwissSign, les certificats des employés sont régénérés automatiquement avant leur expiration, faisant passer la sécurité d'une approche réactive à une approche proactive et évitant les interruptions de service de dernière minute.
- **Aperçu de la vérification des signatures** : Lorsque Echoworx vérifie un message signé entrant, le système injecte des en-têtes MIME supplémentaires pour signaler les problèmes de vérification et remet un rapport détaillé sous forme de signature_verification_results.html pour un flux de travail administratif plus clair.
- **Contrôle granulaire des serveurs LDAP** : Les administrateurs d'entreprise peuvent activer ou désactiver des annuaires LDAP spécifiques au sein de leurs profils, offrant un contrôle précis sur les serveurs interrogés.
- **Recherches LDAP S/MIME et PGP séparées** : Activez les recherches sur des serveurs de clés externes indépendamment pour S/MIME, PGP, ou les deux, afin que la découverte des clés suive vos règles et non un paramètre fixe par défaut.
- **API d'export de clés privées PGP** : Exportez les clés privées PGP de manière programmatique via un point de terminaison REST, prenant en charge la portabilité, la continuité et la souveraineté des clés attendue par les régulateurs.
- **Migration simplifiée et portée mondiale** : Importez l'ensemble des certificats et paires de clés de vos employés en une seule fois, générez automatiquement de nouvelles clés si nécessaire, et livrez de manière sécurisée à n'importe quelle adresse e-mail dans le monde — le tout sur une plateforme consolidée pour PGP et S/MIME.

Note technique

Pour déchiffrer les messages entrants et extraire les certificats des communications entrantes, configurez des règles supplémentaires dans votre passerelle pour acheminer ces messages vers Echoworx. Une fois ce routage en place, la découverte, le déchiffrement et la vérification des signatures s'exécutent automatiquement.

Ce que cela signifie pour vous : Vos destinataires continuent de travailler exactement comme aujourd'hui, vos expéditeurs atteignent toujours des partenaires de confiance avec la bonne clé, et vos administrateurs bénéficient d'un renouvellement proactif, d'un contrôle précis des annuaires et d'une visibilité claire sur la vérification — le tout sur une seule plateforme conçue pour maintenir la sécurité des communications basées sur les certificats, de l'envoi à l'ouverture.