

# OpenText Core Email Encryption

Spécialement conçu pour aider les entreprises à gagner en cyberrésilience

## Avantages

- Sécurité renforcée pour les communications stratégiques
- Sécurité renforcée dans les secteurs d'activité réglementés
- Console de gestion unique pour produits de sécurité des e-mails multiples
- Fournisseur unique de solutions de cyberrésilience
- Option Secure Compose qui permet à tout partenaire commercial ou client extérieur à votre entreprise d'envoyer un e-mail chiffré à votre organisation via un portail de messagerie sécurisée
- Messagerie électronique bidirectionnelle sécurisée
- Authentification de l'utilisateur pour les e-mails entrants
- Liste déroulante personnalisée des adresses e-mail, noms ou services de l'entreprise

## Défi

L'e-mail est la plus grande vulnérabilité de votre entreprise, et le moyen le plus simple pour vos employés d'envoyer des informations sensibles. Avec l'essor du travail à distance, il est plus que jamais nécessaire de sécuriser les échanges par e-mail. La sécurisation des e-mails est un défi pour les entreprises de toutes tailles en raison des menaces croissantes et d'exigences réglementaires toujours plus rigoureuses. La prévention de la perte de données (DLP) est également cruciale, car l'augmentation du nombre de travailleurs à distance a également entraîné une augmentation de la perte de données par e-mail. Les entreprises ont besoin d'une solution clé en main leur permettant de sécuriser les communications par e-mail et d'éviter les fuites de données.

**84 % des responsables IT ont déclaré que le travail à distance complexifiait la prévention de la perte de données**

## Solution : OpenText™ Core Email Encryption

Le chiffrement avancé des e-mails (AEE) élimine les difficultés liées au chiffrement des e-mails et permet aux équipes d'avoir l'esprit tranquille quant à la sécurisation des données sensibles envoyées par e-mail. L'utilisation de filtres de contenu avancés automatise l'analyse des e-mails et des pièces jointes et tout message contenant des informations sensibles est chiffré en vue de sa diffusion. L'AEE renforce votre défense contre les menaces et permet à chacun de communiquer en toute sécurité en dehors de votre réseau. Il chiffre ou met automatiquement en quarantaine les données en fonction des stratégies que vous avez définies pour vos environnements de messagerie afin de protéger votre boîte de réception bien au-delà de ses capacités natives.

Le chiffrement avancé des e-mails peut également aider les expéditeurs et les gestionnaires à comprendre ce qui a déclenché le chiffrement d'un e-mail, et contribue ainsi à sensibiliser les employés à vos stratégies de conformité des e-mails. Et si un employé non autorisé envoie du contenu sensible dans un e-mail, OpenText Core Email Encryption peut mettre en quarantaine le message et en informer la direction pour qu'il soit examiné dans les plus brefs délais.

- Les filtres de prévention de la perte de données (DLP) sont prêts à l'emploi et hautement personnalisables, et déclenchent des stratégies de chiffrement, de routage, de blocage ou de mise en quarantaine des e-mails.
- La définition de stratégies par secteur d'activité permet la détection d'informations contenues dans l'objet, le corps et les pièces jointes de l'e-mail
- Aidez vos clients à appliquer les meilleures pratiques en matière de gouvernance, de risque et de conformité (GRC)
- Générateur de stratégies permettant la sélection d'une combinaison de filtres adaptée au secteur d'activité de vos clients

## Facteurs de différenciation

- Plusieurs options de diffusion sécurisée pour répondre à vos besoins en matière de chiffrement
- Création de rapports graphiques pour la conformité, les méthodes de livraison et plus encore
- Chiffrement à la demande et automatique pour l'expéditeur et le destinataire
- Filtres de prévention de la perte de données par défaut et personnalisables inclus, sans frais supplémentaires
- Favorisez la collaboration externe via le portail Secure Compose

« Face au taux alarmant d'usurpations d'identité aux États-Unis, le chiffrement des e-mails était essentiel pour la protection des informations de nos membres. »

Rifat Ikram,  
Vice-président de Justice  
FCU, Electronic Delivery and  
Support Services, Justice  
Federal Credit Union

## Fonctionnement

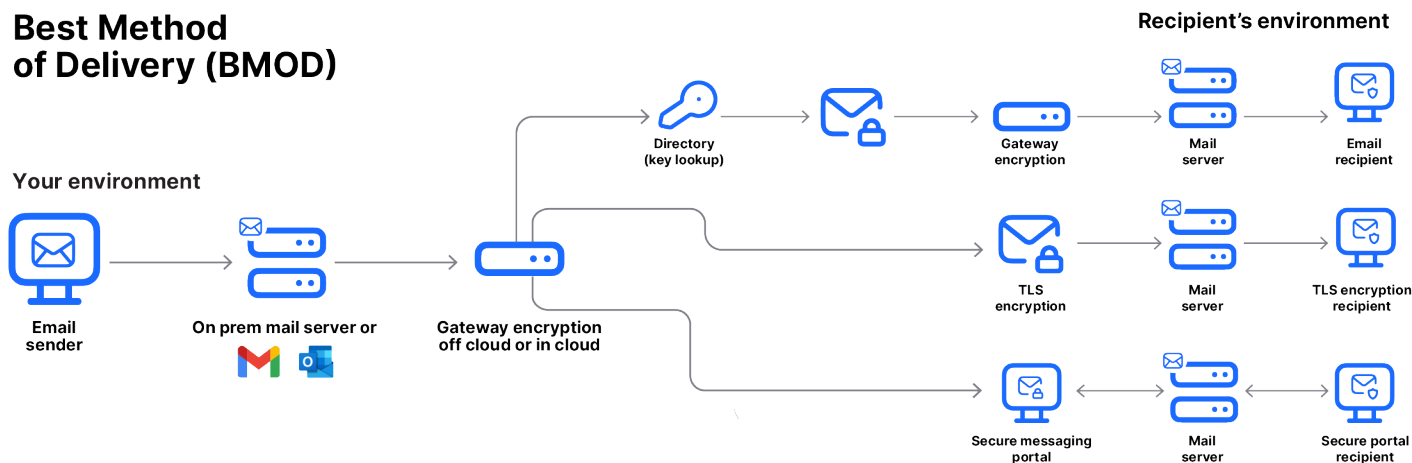
### Best Method of Delivery (BMOD)

La fonctionnalité BMOD (Best Method of Delivery) d'OpenText Core Email Encryption analyse automatiquement les e-mails sortants, en appliquant un chiffrement basé sur des stratégies personnalisables. Cette approche proactive limite les erreurs introduites par les utilisateurs, renforce la sécurité et encourage la conformité en mettant en quarantaine les messages non autorisés et en alertant la direction pour qu'ils soient examinés. Les employés ont la possibilité de communiquer en toute sécurité en dehors de votre réseau, sans perturber les workflows.

Le chiffrement fluide et en toute transparence offre une protection bidirectionnelle avec des options de livraison comme le chiffrement au niveau du message (S/MIME), le protocole TLS basé sur des stratégies, et un portail de messagerie sécurisée à utiliser sur n'importe quel appareil.

Depuis plus de 20 ans, la technologie de chiffrement des e-mails d'OpenText a su gagner la confiance des secteurs de la santé, de la finance et des administrations, dont 100 % des régulateurs de la FFIEC, la Securities and Exchange Commission des États-Unis et 7 divisions du département du Trésor des États-Unis. Ses stratégies personnalisables et ses portails conviviaux permettent aux entreprises de protéger efficacement leurs communications tout en simplifiant la gestion de la sécurité des e-mails.

### Best Method of Delivery (BMOD)



#### Option de livraison 1

- Transmission bidirectionnelle, transparente et sécurisée entre les clients
- Chiffrement au niveau des messages (S/MIME)

#### Option de livraison 2

- Livraison par protocole TLS (Transport Layer Security) basé sur des stratégies

#### Option de livraison 3

- Portail de messagerie sécurisé
- Livraison sécurisée vers n'importe quel appareil, n'importe où et à tout moment

## Spécialement conçu pour améliorer votre résilience contre les cyberattaques

OpenText Cybersecurity permet aux entreprises de gagner en cyberrésilience en permettant la continuité des opérations pendant les attaques. Nos solutions aident à prévenir les violations, à minimiser leur impact grâce à une détection et une réponse rapides, et à garantir une restauration rapide des données pour une conformité assurée vis-à-vis de réglementations en constante évolution. L'AE renforce cette résilience en protégeant les données sensibles contre le vol et les fuites, offrant ainsi une première ligne de défense robuste.