CARBONITE® + WEBROOT®
OpenText Security Solutions

FICHE DE DONNÉES

Advanced Email Encryption développé par Zix™

Spécialement conçu pour les MSP qui desservent les petites et moyennes entreprises (PME)

Défi

Le courrier électronique est l'aspect le plus vulnérable de votre entreprise. Il est assez facile pour les employés d'envoyer des informations sensibles par e-mail. Avec le télétravail, la nécessité pour vos clients et partenaires commerciaux de vous envoyer facilement des e-mails et des fichiers sensibles n'a jamais été aussi grande. Pour les MSP qui desservent les PME, la sécurisation des communications par e-mail est un défi en raison des menaces toujours croissantes par e-mail. En outre, les exigences réglementaires telles que HIPAA, Sarbanes Oxley et GBLA exigent que les données sensibles et confidentielles soient protégées, car si elles tombent entre de mauvaises mains, cela pourrait entraîner des dommages à la réputation ainsi que d'énormes pertes financières en raison d'amendes dont les PME pourraient ne jamais se remettre.

En plus de la protection des données, les PME doivent également garder un œil sur la prévention des pertes de données (DLP). L'augmentation du nombre de travailleurs à distance depuis la pandémie a également entraîné une augmentation des pertes de données par e-mail. Selon Tessian, enquête sur l'état du DLP 2020 (comprend les États-Unis et le Royaume-Uni), 84 % des responsables informatiques ont déclaré que le travail à distance rend le DLP plus difficile. En résumé, les MSP ont besoin d'une solution facile à utiliser, qui sécurise les communications par e-mail et empêche les fuites de données sensibles pour les PME.

Solution : Advanced Email Encryption (AEE) développé par Zix

L'AEE supprime les tracas liés au cryptage des e-mails et donne aux équipes la tranquillité d'esprit que les données sensibles envoyées par e-mail sont sécurisées. À l'aide de filtres de contenu avancés, les e-mails et les pièces jointes sont analysés automatiquement et tout message contenant des informations sensibles est crypté pour la livraison. L'AEE augmente votre défense contre les menaces et permet à chacun de communiquer en toute sécurité en dehors de votre réseau. Il crypte ou met en quarantaine automatiquement en fonction des politiques que vous définissez pour n'importe quel environnement de messagerie afin de sécuriser votre boîte aux lettres bien au-delà de ses capacités natives. Webroot AEE peut également fournir aux expéditeurs et aux gestionnaires un aperçu de la cause du cryptage d'un e-mail, contribuant ainsi à promouvoir la sensibilisation à vos politiques de conformité des e-mails. Et si un employé non autorisé envoie un e-mail avec un contenu sensible, Webroot peut mettre en quarantaine le message et la gestion des alertes pour examen.

Les filtres Webroot Data Loss Prevention (DLP) déclenchent des politiques de cryptage, d'acheminement, de blocage ou de mise en quarantaine des e-mails, sont prêts à l'emploi et hautement personnalisables.

- Les politiques spécifiques à l'industrie détectent les informations dans l'objet, le corps et les pièces jointes des e-mails
- Aider les clients à adopter les meilleures pratiques en matière de gouvernance, de risque et de conformité (GRC)
- Élaborateur de politiques pour sélectionner la bonne combinaison de filtres pour le secteur de vos clients

Différenciateurs

- Filtres contre la perte de données (DLP) de messagerie par défaut et personnalisables inclus sans frais supplémentaires
- Plusieurs options de livraison sécurisées pour répondre aux besoins de cryptage de votre PME
- Rapports graphiques pour la conformité, les méthodes de livraison et plus encore
- Cryptage à la demande et automatique pour l'expéditeur et le destinataire
- Renforcer la collaboration externe via le portail Secure Compose

Principaux avantages pour les MSP

- Statut amélioré dans l'espace de sécurité des e-mails en tant que conseiller de confiance
- Statut de fournisseur de sécurité amélioré dans les secteurs réglementés
- Console de gestion unique pour plusieurs produits de sécurité de messagerie
- Traiter avec un seul fournisseur de solutions de cyber-résilience pour les PME
- Aider potentiellement les PME à obtenir une cyber-assurance ou à réduire son coût

Secure Compose permet à tout partenaire commercial ou client extérieur à votre organisation de lancer un e-mail crypté dans votre organisation via un portail de messagerie sécurisée.

- E-mail sécurisé et bidirectionnel
- Authentification de l'utilisateur pour les e-mails entrants
- Liste déroulante personnalisée des adresses e-mail, noms ou services de l'entreprise

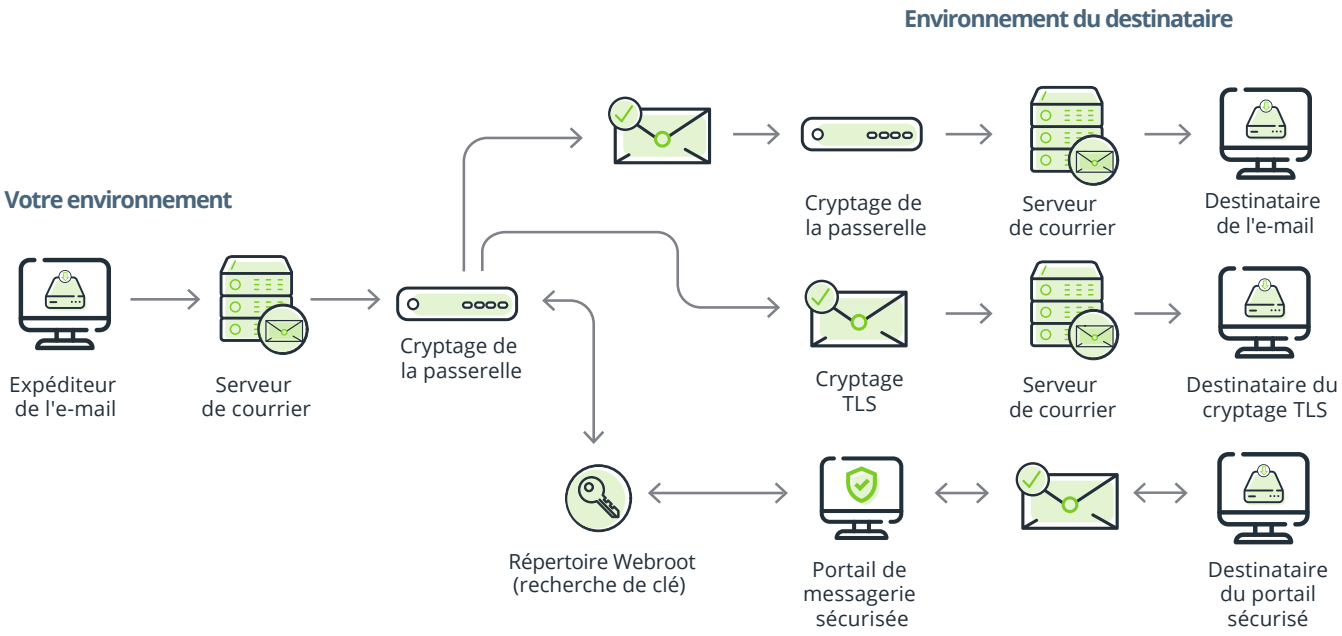
Comment ça marche : Meilleure méthode de livraison (BMOD)

Le moteur de filtrage multicouche offre un niveau de précision extraordinaire qui réduit à la fois les faux négatifs (les mauvais e-mails entrants) et les faux positifs (les bons e-mails sont exclus). Cela réduit le temps que vous passez à gérer le système et réduit les frictions pour les utilisateurs.

Spécialement conçu pour améliorer votre résilience contre les cyberattaques

OpenText Security Solutions rassemble les meilleures solutions pour aider votre entreprise à atteindre la cyber-résilience en vous permettant de poursuivre vos opérations commerciales même en cas d'attaque. Ensemble, Carbonite et Webroot peuvent vous aider à prévenir et à vous protéger des violations en premier lieu, à minimiser l'impact en détectant et en répondant rapidement à une violation, puis en récupérant rapidement les données pour réduire l'impact et vous aider à vous adapter et à vous conformer aux exigences réglementaires changeantes.

L'AEE fait partie intégrante de nos solutions de cyber-résilience et améliore votre posture de sécurité et fournit la première ligne de défense en protégeant et en prévenant le vol et la fuite de données sensibles.



Option de livraison 1

- Livraison bidirectionnelle, transparente et sécurisée entre les clients Zix
- Cryptage au niveau des messages (S/MIME)

Option de livraison 2

- Livraison TLS (Transport Layer Security) basée sur des politiques

Option de livraison 3

- Portail de messagerie sécurisée
- Livraison sécurisée sur n'importe quel appareil, n'importe où, n'importe quand

À propos de Carbonite et Webroot

Les sociétés Carbonite, Webroot et OpenText exploitent le cloud et l'intelligence artificielle pour fournir des solutions complètes de cyber-résilience aux entreprises, aux particuliers et aux fournisseurs de services gérés. La cyber-résilience signifie être capable de rester opérationnel, même face aux cyberattaques et à la perte de données. C'est pourquoi nous avons uni nos forces pour fournir des solutions de protection des postes et des réseaux, de sensibilisation à la sécurité et de sauvegarde des données et de reprise après sinistre, ainsi que des services de renseignement sur les menaces utilisés par les principaux fournisseurs de technologies du marché dans le monde entier. Nous exploitons la puissance de l'apprentissage automatique pour protéger des millions d'entreprises et de particuliers, et sécuriser le monde connecté. Webroot et Carbonite sont implantés en Amérique du Nord, en Europe, en Australie et en Asie. Découvrez la cyber résilience sur carbonite.com et webroot.com.

En savoir plus sur webroot.com

CARBONITE® + WEBROOT®
OpenText Security Solutions