

# OpenText Core Advanced Email Threat Protection

Solution spécialement conçue pour sécuriser les communications professionnelles par message électronique

## Facteurs de différenciation

- Taux de détection de 99,9 % avec extrêmement peu de faux positifs grâce à l'intelligence artificielle, à l'analyse automatisée du trafic et au machine learning
- Équipe d'analystes surveillant en direct les menaces 24 h/24, 7 j/7, 365 jours/an qui identifie les nouvelles menaces, met à jour le système et émet des avertissements en permanence
- Fonction Protection d'identité/Prévention de l'usurpation d'identité incluse dans l'offre de base
- Réécriture des liens vers des versions sécurisées et réalisation d'une analyse du temps de clic au niveau de l'adresse de destination
- Désactivation et/ou réalisation d'une analyse approfondie des pièces jointes dans un environnement sandbox sécurisé basé sur le cloud

## Principaux avantages

- Sécurité renforcée pour les communications stratégiques
- Console de gestion unique pour plusieurs produits de sécurité des messages électroniques
- Sécurité renforcée dans les secteurs d'activité réglementés
- Fournisseur unique pour tous vos besoins en matière de cybersécurité

## Défi

Les messages électroniques sont l'un des moyens de communication les plus efficaces et les plus économiques à l'échelle mondiale. Les entreprises en sont dépendantes alors qu'ils constituent l'un des aspects les plus vulnérables de leur activité. Les cybercriminels ciblent les messages électroniques en raison de leur usage généralisé et des vulnérabilités particulières qu'ils présentent.

Les attaques croissantes de phishing, les virus et le courrier indésirable ne représentent qu'une petite fraction des menaces de sécurité existantes transmises par les messages électroniques qui peuvent entraîner une perte financière ou nuire à la réputation d'une entreprise. Avec l'augmentation des attaques via l'ingénierie sociale, par ransomware, par compromission de messages électroniques professionnels (BEC), par usurpation d'identité ainsi que des attaques ciblées, les cybercriminels exploitent les messages électroniques pour voler des informations confidentielles.

Selon notre dernier rapport de renseignements sur les menaces Webroot/BrightCloud, une augmentation de 1 122 % des attaques de phishing a été constatée d'une année sur l'autre. Dans la plupart des cas, les entreprises ne détectent pas la violation, ne savent pas comment en évaluer l'impact ou ne disposent pas d'outils appropriés pour traiter le problème. De nombreuses entreprises étant soumises à des exigences réglementaires, elles doivent se prémunir contre les menaces liées aux messages électroniques si elles veulent rester en conformité.

## Solution : OpenText Core Advanced Email Threat Protection

OpenText™ Core Advanced Email Threat Protection offre un filtrage multicouche pour les messages entrants, sortants et désormais internes. La solution autorise les messages électroniques légitimes et bloque automatiquement les menaces malveillantes telles que les tentatives de phishing, les ransomware, l'usurpation d'identité, les attaques BEC et les courriers indésirables.

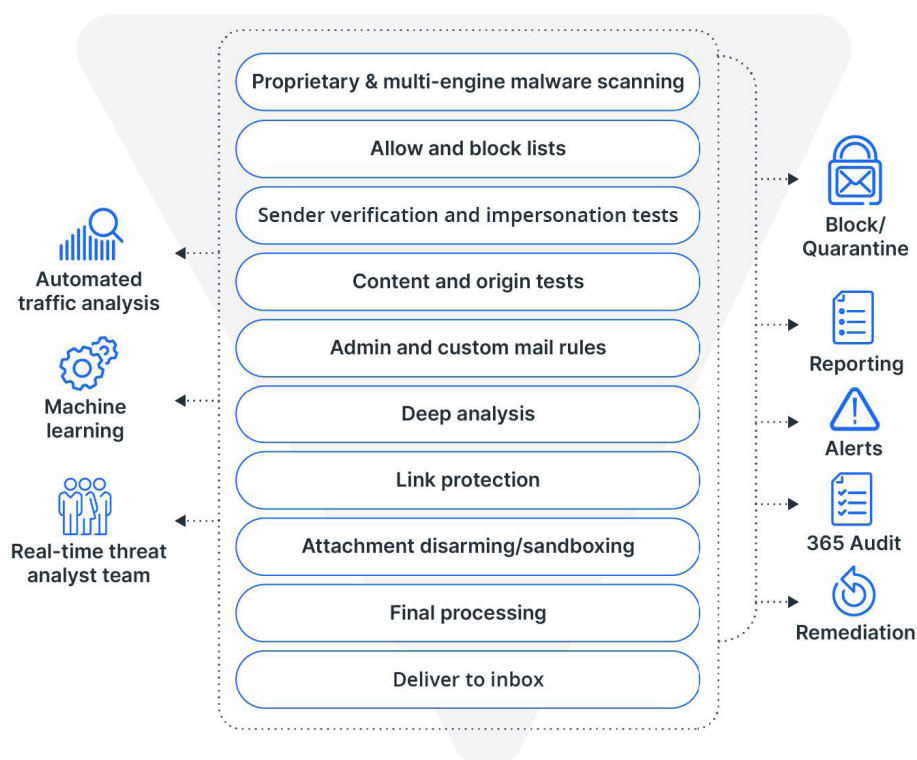
- La fonction **Protection des liens** réécrit les liens et effectue une analyse du temps de clic au niveau de l'adresse de destination. Selon les résultats des tests, les utilisateurs sont redirigés automatiquement vers un site sécurisé, avertis en cas de site suspect, voire bloqués lorsqu'un site est potentiellement malveillant.
- La fonction **Mise en quarantaine des pièces jointes** effectue une analyse approfondie des pièces jointes dans un environnement sandbox sécurisé basé sur le cloud. Elle peut également fournir instantanément une version désactivée des fichiers en supprimant les macros ou en convertissant les fichiers au format PDF.
- La fonction **Retrait des messages (pour Microsoft 365)** améliore la réponse aux incidents en permettant le retrait des messages malveillants déjà envoyés dans la boîte de réception des utilisateurs. Cela permet de réduire les risques en empêchant les utilisateurs d'accéder aux messages électroniques malveillants, accélérant ainsi le traitement du problème. Le système fournit également un suivi d'audit détaillé.
- La fonction **Filtrage des messages électroniques internes (pour Microsoft 365)** étend la protection contre les attaques BEC en sécurisant les communications internes (d'un utilisateur à l'autre). Cela freine considérablement la capacité des cybercriminels à exploiter la « confiance » des collaborateurs et à se déplacer latéralement au sein d'une organisation.

## Principales fonctionnalités

- Mise en oeuvre simple et rapide
- Portail facile à utiliser
- Tableaux de bord permettant une gestion intuitive
- Filtrage personnalisable
- Fonctionnalités complètes de consignation et de création de rapports
- Accès mobile

## Fonctionnement

Le moteur de filtrage multicouche offre un remarquable niveau de précision qui limite à la fois le nombre de faux négatifs (messages électroniques malveillants non détectés) et de faux positifs (messages électroniques légitimes bloqués à tort). Cela diminue le temps consacré à la gestion du système ainsi que les frictions pour les utilisateurs, tout en permettant à chacun de rester productif.



## Solution spécialement conçue pour améliorer votre résilience contre les cyberattaques

OpenText Cybersecurity réunit les meilleures solutions de leur catégorie pour aider votre entreprise à devenir cyberrésiliente, en vous permettant de poursuivre vos opérations commerciales même en cas d'attaque. OpenText peut vous aider à prévenir les violations et à vous en protéger immédiatement, en limitant leur impact grâce à une détection et une réponse rapides, puis en récupérant les données rapidement. Cela réduit les conséquences et vous permet de vous adapter et de respecter des exigences réglementaires en constante évolution.

OpenText Core Advanced Email Threat Protection fait partie intégrante de nos solutions de cyberrésilience et améliore la sécurité en fournissant la première ligne de défense via une sécurité multicouche contre les menaces transmises par message électronique telles que le phishing, les ransomware, l'usurpation d'identité et les attaques BEC.

OpenText Cybersecurity fournit des solutions de sécurité complètes pour les entreprises et les partenaires de toutes tailles. De la prévention à la détection, en passant par la réponse, la récupération, l'enquête et la conformité, notre plateforme unifiée de bout en bout aide les clients à développer leur cyberrésilience via un portefeuille de sécurité global. Grâce à des informations exploitables issues de nos renseignements en temps réel et contextuels sur les menaces, les clients d'OpenText Cybersecurity bénéficient de produits hautement efficaces, d'une expérience conforme et d'une sécurité simplifiée pour les aider à gérer les risques métiers. DS\_010523