Bitdefender GravityZone Email Security

Sécurité multi-couches, basée dans le cloud, de l'ensemble des e-mails de votre entreprise. Fournit une prévention contre les menaces à tous vos déploiements Office 365

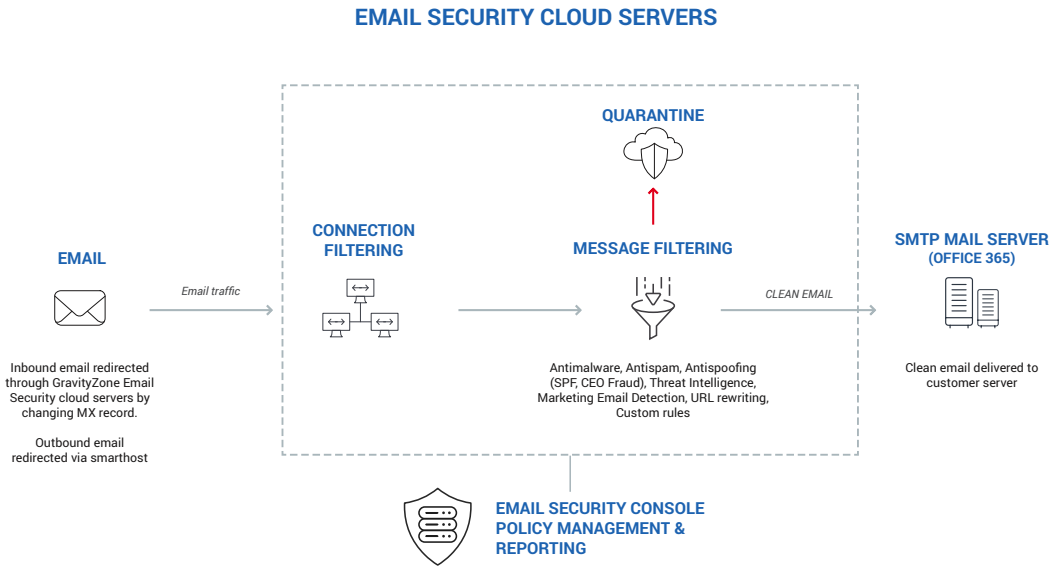
Bitdefender GravityZone Email Security est une solution complète de protection des e-mails. Elle fournit une protection complète des e-mails de votre entreprise, au-delà des malwares et autres menaces traditionnelles comme le spam, les attaques de phishing à grande échelle et les URL malveillantes. En effet, elle bloque également les menaces modernes, ciblées et sophistiquées qui transitent via les e-mails, telles que les menaces liées à l'usurpation d'identité en entreprise (BEC ou Business Email Compromise) et les fraudes au président.

Protection inégalée contre les menaces	Protection contre les attaques par fraude au président	Moteurs d'analyse multiples
Une pile technique complète pour assurer une protection précise contre les menaces connues, inconnues et émergentes qui se diffusent via e-mail	Détection des menaces qui ne se basent pas sur des malwares, telles que le phishing et les e-mails frauduleux	Les moteurs traditionnels basés sur les signatures sont associés à des moteurs antimalwares analysant les comportements afin d'automatiquement fournir une protection contre les nouvelles techniques utilisées par les malwares

Fonctionnement de la solution

- Les méthodes d'analyse traditionnelles par comparaison des modèles, des attributs et des caractéristiques sont complétées **par l'analyse algorithmique, permettant une détection beaucoup plus précise des menaces**.
- **De multiples moteurs antimalwares basés sur des signatures et de l'analyse comportementale** assurent une protection contre tous les types de malwares, y compris les variantes Zero-day.
- **L'analyse comportementale** intègre plus de 10 000 algorithmes analysant plus de 130 variables extraites de chaque e-mail.
- **Le moteur basé sur des politiques** permet à l'administrateur de personnaliser précisément les flux d'e-mails entrant et sortant de l'entreprise. Le moteur peut inspecter tous les aspects des e-mails, notamment la taille, le contenu, les pièces jointes, les en-têtes, l'émetteur et les destinataires, puis prendre les mesures adaptées : par exemple le distribuer, le mettre en quarantaine, le mettre en quarantaine d'entreprise, le rerouter, afficher une notification ou le rejeter.
- **GravityZone Email Security est à la fois une solution de sécurité avancée pour les e-mails et un moteur de routage d'e-mails basé dans le cloud,** intégrant un système de mise en quarantaine au niveau de l'entreprise ou des utilisateurs. Système de catégorisation avancée : distingue par exemple les e-mails marketing professionnels des campagnes d'e-mailing suspectes de masse. Cela permet de définir des politiques flexibles qui détaillent précisément comment différents types de messages sont traités et tagués.
- **Le suivi détaillé des messages** est un outil clé pour les administrateurs, permettant de visualiser rapidement et précisément pourquoi un e-mail a été distribué ou rejeté, y compris les en-têtes et la conversation complète avec le serveur de messagerie distant.

Architecture de GravityZone Email Security



Principales fonctionnalités de GravityZone Email Security

PROTECTION

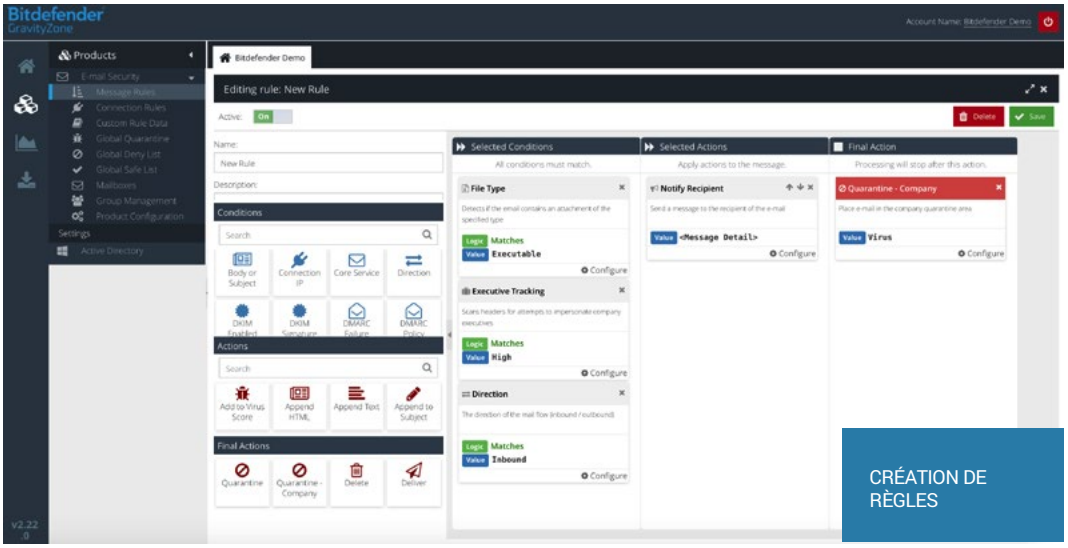
- Antispam : les moteurs utilisent une combinaison de nombreuses technologies pour détecter le spam ainsi que le phishing ciblé et sophistiqué, et les attaques par usurpation d'identité.
- Antimalware : les multiples moteurs antivirus se basent sur des signatures et de l'analyse comportementale pour détecter les malwares.
- Protection de type "Time-of-click" : réécrit les URL dans les e-mails et assure une protection au moment du clic en utilisant plusieurs services de réputation.
  - Options pour rediriger automatiquement, cliquer pour continuer, bloquer les menaces et afficher/masquer l'URL cible.
  - Option pour analyser les liens au moment de la distribution du message ou au moment du clic.
- Listes personnalisables : créez des listes sûres et de refus, pour toute l'entreprise ou par utilisateur.
- TLS / Opportunistic TLS :
  - Force le chiffrement TLS et restreint la communication avec les autres serveurs de messagerie non compatible avec le protocole TLS.
  - Option d'activation "Opportunistic TLS" convertissant le message en texte brut si le TLS n'est pas pris en charge par le serveur de messagerie du destinataire.
- Authentification des e-mails : prise en charge de SPF, DKIM et DMARC.
- Liste de suivi des dirigeants de l'entreprise : utilisez les informations synchronisées avec Active Directory pour détecter automatiquement les vrais noms dans les en-têtes et adresses, afin de protéger l'entreprise contre les attaques par usurpation d'identité et fraude au président.
- Domaines proches (cousins) :
  - Compare le domaine de l'émetteur à des noms de domaine légitimes pour identifier les domaines proches (dont le nom n'est différent que d'un ou de deux caractères par rapport au nom de domaine réel).
  - Protège des attaques par usurpation d'identité / fraude au président.
- Taggage du sujet et en-têtes :
  - Ajoute de tags comme [EXTERNE] ou [MARKETING] aux sujets des messages.
  - Ajoute des en-têtes HTML ou du texte aux messages entrants pour alerter les utilisateurs de potentiels risques.
- Pièces jointes :
  - Contrôle de type MIME des pièces jointes et peut bloquer les types de fichiers dangereux.
  - Détecte les archives protégées par mot de passe.
- Listes de mots-clés : crée une quantité illimitée de listes de mots-clés. Utilise des règles pour analyser les messages et prendre des mesures sur la base de l'aspect confidentiel ou sensible du contenu.
- File d'attente d'e-mails : les e-mails sont automatiquement mis en liste d'attente pendant 7 jours en cas de panne du service/serveur de messagerie principal.
- Surveillance des limites d'envoi : protection automatique contre les tentatives d'envois de grandes quantités de messages pour éviter la mise en liste noire du domaine.
- Prévention contre les attaques d'annuaire (DHA) : annule les e-mails destinés à des adresses e-mail fausses ou invalides.

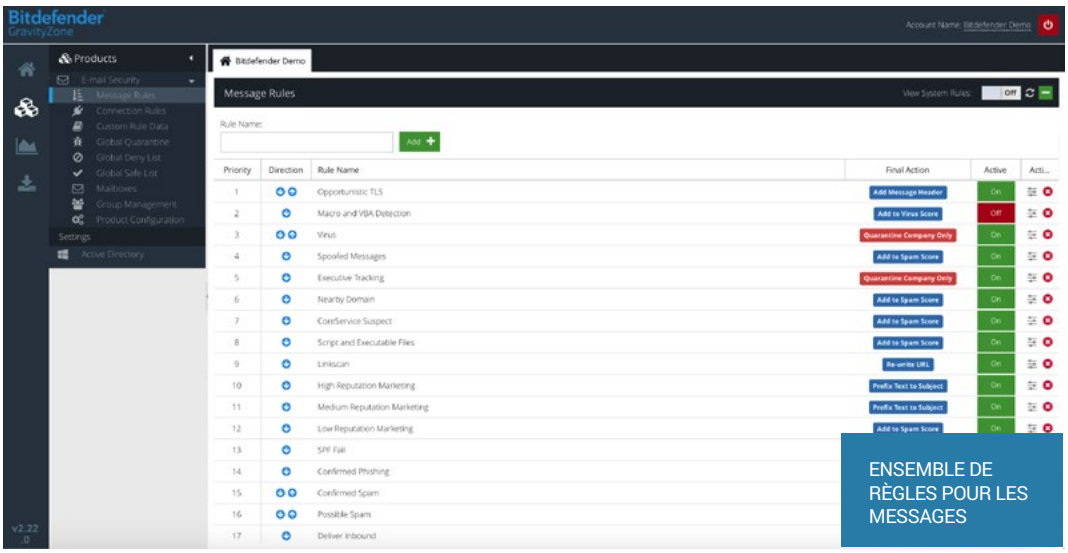
ADMINISTRATION

- Moteur basé sur des politiques : plus de 20 déclencheurs conditionnels permettent de contrôler la distribution des e-mails et filtrer les messages en fonction de leur taille, de mots-clés, du score de spam, de l'heure, de la source, de la destination, de la taille des pièces jointes, des en-têtes, des attributs AD, etc.
- Synchronisation des utilisateurs : le service de synchronisation Active Directory assure que tous les changements sont répliqués. Applique des règles basées sur les groupes AD, si besoin.
- Interface Web entièrement accessible et administrée via la console GravityZone Email Security.
- Administration déléguée : permet la création de multiples administrateurs avec différents niveaux d'accès.
- Quarantaine : option de déplacement des messages dans la quarantaine de l'utilisateur ou de l'entreprise.
- Synthèse des messages en quarantaine : liste tous les messages de la quarantaine de l'utilisateur et permet de les prévisualiser, de les "libérer" ou de les bloquer. En interagissant avec le récapitulatif, l'utilisateur peut gérer ses listes sûres et de refus. Les utilisateurs peuvent régler la fréquence à laquelle les e-mails récapitulatifs sont envoyés.
- Avertissement : ajoute un avertissement HTML ou en texte brut à tous les e-mails sortants. Il est possible de régler différents avertissements pour différents domaines.

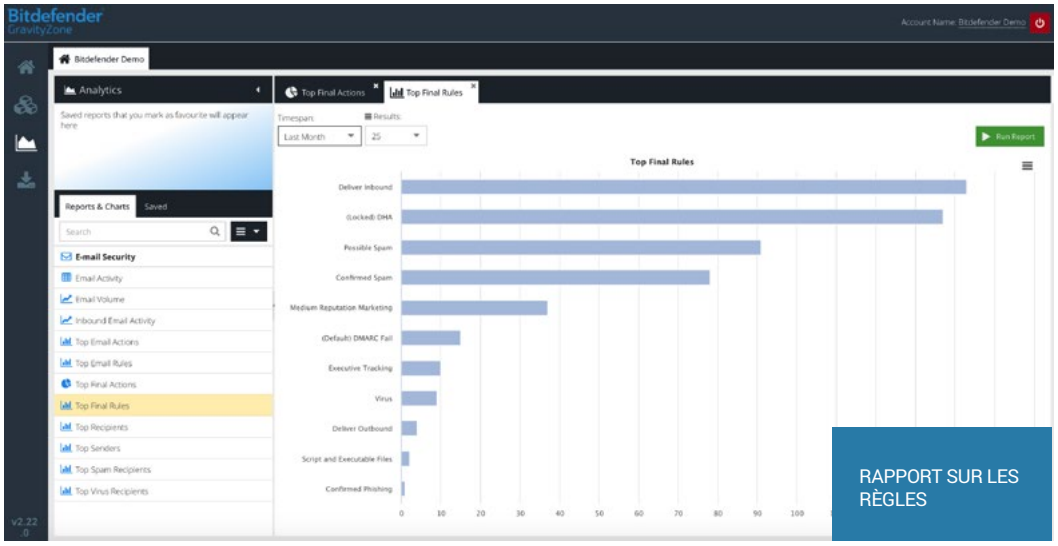
REPORTING

- Visibilité en temps réel : des graphiques fournissent une visibilité détaillée sur les flux d'e-mails entrants et sortants, ainsi que sur les règles déclenchées et les mesures prises. Intègre aussi la possibilité de générer des rapports détaillés.
- Créateur de rapports : les administrateurs peuvent paramétrer leurs propres rapports en fonction des noms de champs et critères disponibles. Les rapports peuvent être enregistrés puis exportés. Il est possible de rechercher des rapports d'audits selon des critères comme l'heure, l'utilisateur, l'adresse de l'émetteur, le sujet, l'IP de l'émetteur, le destinataire, la direction, l'action finale, le nom de la règle. En marquant des rapports en tant que "Favoris", ils apparaissent dans une zone d'accès rapide.
- Planification et alertes : relie des rapports à des calendriers et, en option, permet de ne recevoir un rapport que si un contenu existe (mode alerte). Alertes sur les règles, actions, contenus, etc.
- Rapports sur les principales tendances : sélection de rapports sur les tendances au sein de graphiques et de tableaux. Les rapports de tendance peuvent être exportés en PDF et envoyé par e-mail.
- Visualisation multiple : analyses et rapports selon des critères comme l'heure, l'utilisateur, l'adresse de l'émetteur, le sujet, l'IP de l'émetteur, le destinataire, la direction, l'action finale, le nom de la règle.
- Audit détaillé (suivi de message) : visualisation de l'analyse de chaque message indiquant la raison exacte de sa distribution ou non. Intègre les en-têtes et la conversation complète avec le serveur de messagerie distant.
- Rétention des journaux et archivage automatique : les journaux de GravityZone Email Security sont automatiquement archivés après 90 jours et sont disponibles au téléchargement depuis la console pendant une période supplémentaire de 12 mois.





ENSEMBLE DE RÈGLES POUR LES MESSAGES



RAPPORT SUR LES RÈGLES

DÉPLOIEMENT

- Déploiement simple et rapide : redirige les enregistrements de domaine MX vers le cloud GravityZone Email Security.
- Compatibilité avec tous les prestataires de services de messagerie. Distribue les e-mails à différents destinataires en fonction de l'appartenance de l'utilisateur à un groupe AD - prend en charge les environnements hybrides sous Exchange sur site avec O365 Exchange Online ou Gmail.
- Modifie les enregistrements MX afin de rerouter les e-mails entrants et en les faisant transiter par les serveurs cloud de GravityZone Email Security.
- Configure des hôtes intelligents afin de rerouter les e-mails sortants en les faisant passer par les serveurs cloud de GravityZone EMail Security.

Pour en apprendre plus, rendez-vous sur : https://www.bitdefender.com/business/gravityzone-addons/email-security.html

Ou contactez votre partenaire local Bitdefender.

Bitdefender est une entreprise mondiale de sécurité qui développe des solutions de cybersécurité de pointe et qui protège plus de 500 millions de systèmes dans plus de 150 pays. Depuis 2001, Bitdefender développe des technologies régulièrement récompensées, pour les marchés des entreprises et des particuliers, et est un fournisseur recommandé pour sécuriser les infrastructures hybrides et protéger les endpoints. Grâce à ses équipes R&D, ses alliances et partenariats, Bitdefender est reconnu pour être un éditeur innovant, proposant des solutions de sécurité fiables et efficaces, sur lesquelles vous pouvez compter. Plus d'informations sur www.bitdefender.fr

BD-NGZ-Nov20.2019-TKit-new2.ist
Bitdefender-NGZ-EmailSecurity-Datasheet-CREA174014-A4-FR