

GravityZone Security for Email

Sécurité multicouche de l'ensemble de vos boîtes de messagerie cloud

GravityZone Security for Email fournit aux entreprises une sécurité complète des e-mails contre les menaces connues comme émergentes, y compris les attaques par usurpation, la compromission des e-mails professionnels (BEC), l'arnaque au président, le phishing, les ransomwares, etc. La threat intelligence avancée associe les méthodes d'analyse traditionnelles par comparaison des modèles, des attributs et des caractéristiques des messages à l'analyse algorithmique pour permettre une détection optimale des menaces et protéger les réseaux contre les attaques ciblées par e-mail - avec un taux presque nul de faux positifs.

GravityZone Security for Email 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.

Principales capacités

- De multiples moteurs antivirus basés sur le comportement et les signatures protègent contre toutes les formes de malwares, y compris les variantes Zero-day
- Le suivi détaillé des messages est un outil clé pour les administrateurs, en donnant une vue rapide permettant de déterminer pourquoi un e-mail a été distribué ou rejeté, y compris les en-têtes et la conversation complète avec le serveur de messagerie distant
- Protection multicouche contre les menaces : les multiples moteurs de sécurité utilisent une combinaison de nombreuses technologies pour détecter le spam ainsi que le phishing ciblé et sophistiqué, et les attaques par usurpation d'identité
- 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
- Contrôle complet sur les flux d'e-mails avec un puissant moteur de politiques permettant de contrôler la distribution des e-mails et le filtrage des messages sur la base de critères tels que la taille, la source, la destination, les mots clés, etc.
- Protection en temps réel de l'utilisateur - Une protection au moment du clic réécrit les liens dans les messages et protège les employés en temps réel en bloquant les liens vers des pages Internet malveillantes et en avertissant les utilisateurs.
- Le filtrage des messages sortants permet d'en contrôler les contenus pour éviter l'inscription en liste noire de l'IP.
- Analyse et inspection approfondies - Une analyse détaillée via plusieurs moteurs inspecte chaque e-mail sous toutes ses facettes, y compris sa taille, son contenu, ses pièces jointes, les en-têtes, l'expéditeur, les destinataires et les liens, puis prend automatiquement les mesures appropriées. Par exemple le transmettre, le mettre en quarantaine, le rerouter, envoyer une notification ou le rejeter.

En bref

Notre solution de sécurité des e-mails est basée à 100 % dans le cloud et est facile à déployer. Notre moteur de politiques utilise de multiples moteurs AV, notamment par mise en sandbox statique des pièces jointes, et offre une analyse complète des e-mails entrants et sortants utilisant une liste de mots-clés illimitée. Il protège également tous les fournisseurs de messagerie et supporte les environnements hybrides qui utilisent Exchange on-premise, Microsoft 365, Exchange Online ou Gmail.

Avantages clés

- Analyse comportementale avancée basée sur un système avancé qui regroupe plus de 10 000 algorithmes pour analyser plus de 130 variables extraites de chaque e-mail et garantir une détection et une prévention de pointe.
- Gestion et contrôle - Grâce au contrôle total dont ils bénéficient, les administrateurs informatiques peuvent personnaliser les flux d'e-mails entrants et sortants de l'organisation, créer des listes illimitées de mots clés, utiliser des règles pour analyser les messages et agir sur la base d'informations confidentielles ou sensibles.
- Sécurité renforcée de la messagerie - Les multiples moteurs et technologies d'analyse assurent une détection des menaces de pointe, simple à déployer et à administrer pour les entreprises de toutes les tailles.

« J'accorde une grande importance à rationaliser, simplifier et harmoniser les processus. Bitdefender a été une occasion parfaite de consolider et de gérer la sécurité des endpoints et des e-mails sur nos environnements physique et cloud, dans Azure, et ce depuis une seule console. »

Andrew Black, DSI
A-Core Concrete Specialists

- Blocage des fraudes - Détecte les attaques autres que celles de malwares comme le phishing, les attaques BEC, les arnaques au président, etc.
- Contrôle complet - Fournit un contrôle détaillé sur les flux d'e-mails, prend en charge un grand nombre de fournisseurs de messagerie et s'intègre de manière transparente à Microsoft 365

Le moteur basé sur des politiques permet à l'administrateur de personnaliser précisément les flux d'e-mails entrants et sortants de l'entreprise. Le moteur inspecte 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.

Analyse multicouche

De multiples moteurs antivirus et antispam traditionnels basés sur les signatures et les comportements détectent toutes les formes de malwares et de spams, y compris les variantes de type Zero day. GravityZone Security for Email affiche un taux de détection des spams de 99,999 % - ce avec quasiment aucun faux positif et une protection à 100 % contre les virus.

