Trend Micro™

EMAIL SECURITY

Neutralisez le phishing, les ransomware et les attaques frauduleuses à l'aide d'un mix de techniques cross-générationnelles de lutte contre les menaces

Si l'email est un outil de communication essentiel, les menaces véhiculées par email, dont les ransomware et arnaques par usurpation d'identité, connaissent une croissance exponentielle, difficile à maîtriser. Même vos collaborateurs les plus avertis peuvent cliquer par erreur sur un lien malveillant et exposer votre organisation à des exactions criminelles.

Trend Micro™ Email Security neutralise les tentatives de phishing, de ransomware et d'usurpation d'identité par email. Optimisé par la sécurité XGen™, le service capitalise sur un mix de techniques cross-générationnelles contre les menaces, parmi lesquelles le Machine Learning, l'analyse en sandbox et la prévention des pertes de données, pour juguler toutes les menaces par email. La solution, simple à administrer, se connecte avec d'autres couches de sécurité de Trend Micro pour partager des informations de veille sur les menaces et offrir une visibilité centralisée sur l'ensemble de votre entreprise. La solution protège Microsoft® Exchange™, Microsoft® Office 365®, Gmail™ et autres plateformes email hébergées ou sur site.

FORRESTER®
WAVE LEADER 2019
Enterprise Email Security

FONCTIONNALITÉS CLÉS

- **Une protection en profondeur** : offre une protection intégrale contre le phishing, le spam et les emails malveillants à l'aide de multiples techniques : analyse des expéditeurs, des contenus et des images, Machine Learning et davantage.
- **Protection contre les emails frauduleux** : protège contre les arnaques par email grâce au Machine Learning, associé à des règles expertes, qui analyse l'entête et le contenu d'un email. La fonction Trend Micro™ Writing Style DNA est proposée pour analyser le style rédactionnel des emails et prévenir les usurpations d'identité. Une licence Trend Micro™ Cloud App Security est nécessaire pour Writing Style DNA.
- **Détection des exploits de documents** : détecte les malware et vulnérabilités de documents PDF, Microsoft® Office et autres, à l'aide de techniques statiques et heuristiques qui identifient les éléments suspects.
- **Protection avancée contre les menaces** : identifie les malware inconnus à l'aide de différentes techniques sans signature comme le Machine Learning appliqué aux fichiers suspects (avant leur exécution) et l'analyse en sandbox. La technologie de sandbox de Trend Micro™ Deep Discovery™ analyse en temps réel les fichiers joints et URLs suspectes au sein d'un environnement virtualisé et cloisonné.
- **Vérification des URLs cliquées** : neutralise les emails contenant des URL malveillantes avant leur livraison et re-vérifie la sécurité d'une URL si celle-ci est cliquée par un utilisateur.
- **Vérification et authentification de la source** : utilise Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM) et Domain-based Message Authentication, Reporting and Conformance (DMARC).
- **Veille sur les menaces** : tire parti de Trend Micro™ Smart Protection Network, une des bases de données les plus importantes en matière de veille sur les menaces, pour corréler des informations issues du Web, de l'email, de registres de noms de domaine et d'autres sources, afin d'identifier les infrastructures des assaillants en amont d'une éventuelle attaque.
- **Chiffrement des emails** : le chiffrement des emails basé sur des règles inclut un service de gestion des clés et permet aux destinataires de lire les emails déchiffrés à partir de l'équipement de leur choix et via un navigateur Web.
- **DLP** : intègre des modèles de DLP pour identifier, répertorier et protéger les informations sensibles et confidentielles.
- **Continuité de l'email** : propose un système email secondaire pour une continuité du service en cas de défaillance du serveur email.
- **Reporting flexible** : génère un reporting avec des contenus personnalisés.
- **Connected Threat Defense** : se synchronise avec Trend Micro Apex Central™ pour définir une liste d'objets suspects (URLs et fichiers).

EMAIL SECURITY : QUELS SONT VOS AVANTAGES ?

Neutralise le phishing et le spam

- Valide l'authenticité et la réputation de l'expéditeur de l'email pour éliminer les sources malveillantes
- Analyse le contenu des emails à l'aide de différentes techniques, pour éliminer le spam et le phishing
- Protège contre les URLs malveillantes, lors de la remise de l'email et lorsqu'une URL est cliquée (réécrit et analyse les URLs lorsque celles-ci sont cliquées, et neutralise tout accès à ces URLs si malveillantes)

Détecte et neutralise les menaces évoluées

- Détecte et neutralise les ransomware et les autres types de malware Zero-Day, grâce à un Machine Learning en pré-éxécution, des analyses globales, une détection des exploits et une analyse en temps réel des fichiers et des URLs en sandbox
- Le Machine Learning (pré-exécution) neutralise les malware inconnus en amont de l'analyse en sandbox, pour une protection optimale et efficace contre les menaces
- Partage des informations sur les menaces avec d'autres couches de sécurité pour déjouer les attaques persistantes et ciblées

Protection contre les usurpations d'identité par email

- Analyse les attributs comportementaux de l'email (fournisseur d'email non-sécurisé, domaine frauduleux ou réponse à un email associé à un service gratuit), l'intention (demande d'ordre financière, demande urgente, incitation à une action), ainsi que le style rédactionnel de l'auteur de l'email
- Vous permet de définir vos utilisateurs dont l'identité est susceptible d'être usurpée par email

Soyez serein

- Bénéficie d'un support technique en 24/7
- Les emails sur la zone EMEA (Europe, Moyen-Orient et Afrique) sont routés vers des data centers en Europe de l'Ouest. Les emails sur la zone Australie et Nouvelle-Zélande sont routés vers des data centers en Australie. Les emails des clients issus du reste du monde sont redirigés vers nos data centers aux États-Unis
- Le service principal est hébergé sur AWS. La sandbox Cloud est hébergée au sein de data centers Trend Micro certifiés ISO 27001. Les data centers des différentes régions opèrent de manière indépendante et ne sont pas interconnectés, pour des raisons de confidentialité et de souveraineté de données

COMPARATIF : TREND MICRO EMAIL SECURITY

FONCTION	STANDARD	ADVANCED
Analyse et authentification de l'expéditeur de l'email par SPF, DKIM et DMARC	Oui	Oui
Protection : menaces connues (spam, malware, URLs malveillantes et graymail)	Oui	Oui
Protection : détection des malware inconnus	Détection des exploits, Machine Learning prédictif	Détection des exploits, Machine Learning prédictif, analyse des fichiers en sandbox
Protection : protection contre les URLs inconnues	Vérification des URLs cliquées	Vérification des URLs cliquées, analyse des URLs en sandbox
Protection : détection par IA des emails frauduleux et vérification de l'entête et des contenus de l'email	Oui	Oui
Protection : détection par IA des emails frauduleux et vérification de la parternité des emails	-	Oui*
Conformité : DLP et chiffrement de l'email	Oui	Oui
Reporting : reporting personnalisé et programmé	Oui	Oui
Syslog pour l'export de logs	Oui	Oui
Connected Threat Defense : listes d'objets suspects (fichiers, URL) à partir d'Apex Central	Oui	Oui
Mise en quarantaine des utilisateurs	Oui	Oui
Continuité de l'email : pérennise le service en cas de défaillance du serveur email	-	Oui
Délai de recherche et de suivi des emails	30 jours	60 jours

* Licence Trend Micro Cloud App Security nécessaire

CONFIGURATION REQUISE

Trend Micro Email Security

Pour toute information sur les données personnelles que nous recueillons et les raisons pour lesquelles nous les recueillons, merci de consulter notre politique de confidentialité sur :
https://www.trendmicro.com/fr_fr/about/legal.html

TREND MICRO™

Securing Your Connected World