Trend Micro™

SCANMAIL™ SUITE FOR MICROSOFT® EXCHANGE™

Protection optimale. Administration simplifiée.

Le saviez-vous ? Plus de **90%** des attaques ciblées sont initiées via un email de spear phishing, ce qui rend la sécurité de votre serveur email d'autant plus essentielle. Malheureusement, la majorité des outils de sécurité, et notamment celui intégré à Exchange 2013, se contente de mises à jour de signatures virales qui ne détectent que les logiciels malveillants classiques. Aucune protection spécifique n'est proposée pour détecter les URL malveillantes et autres vulnérabilités de logiciel utilisées par les attaques ciblées et les menaces de types APT (Advanced Persistent Threats).

ScanMail™ Suite for Microsoft® Exchange™ neutralise les attaques ciblées par email et le spear phishing grâce à l'identification des vulnérabilités, à un service optimal de réputation Web et à un environnement de sandboxing. Ces fonctionnalités érigent une ligne de défense contre les menaces APT. ScanMail est la seule solution du marché à neutraliser les malware à l'aide des technologies de réputation (email, fichier et Web) et à effectuer une veille mondiale contre les menaces proposée par l'infrastructure de sécurité Trend Micro™ Smart Protection Network™ basée dans le cloud.

ScanMail offre une administration optimisée, tant en temps qu'en coût, grâce à une administration centralisée, une prévention des fuites de données (DLP - Data Leak Prevention) à base de templates, et une gestion des accès fondée sur les rôles. La solution offre le coût total de possession (TCO) le plus bas du marché selon un benchmark réalisé par le cabinet Osterman Research et portant sur 5 outils concurrents. ScanMail offre enfin des performances optimales grâce à une compatibilité en natif avec le 64-bit.

Logiciel

Périmètre de protection

- Serveur de messagerie
- Inspection en interne
- Données entrantes et sortantes

Protection des données et contre les menaces

- Antivirus
- Protection contre les menaces Web
- Antispam
- Antiphishing
- Filtrage de contenus
- Prévention des fuites de données
- Menaces ciblées et APT

AVANTAGES

Protection contre les menaces APT et les attaques ciblées

- Maîtrise l'impact des attaques ciblées grâce à de nombreux outils de protection.
- Exécute les fichiers suspects en environnement sandbox protégé et offre une veille personnalisée sur les menaces grâce à une intégration avec Deep Discovery Advisor.
- Offre des mises à jour de sécurité pour notifier les autres couches de sécurité et empêcher toute nouvelle attaque menée via un malware déjà identifié.

Une technologie de réputation qui neutralise davantage de malware, de phishing et de spam

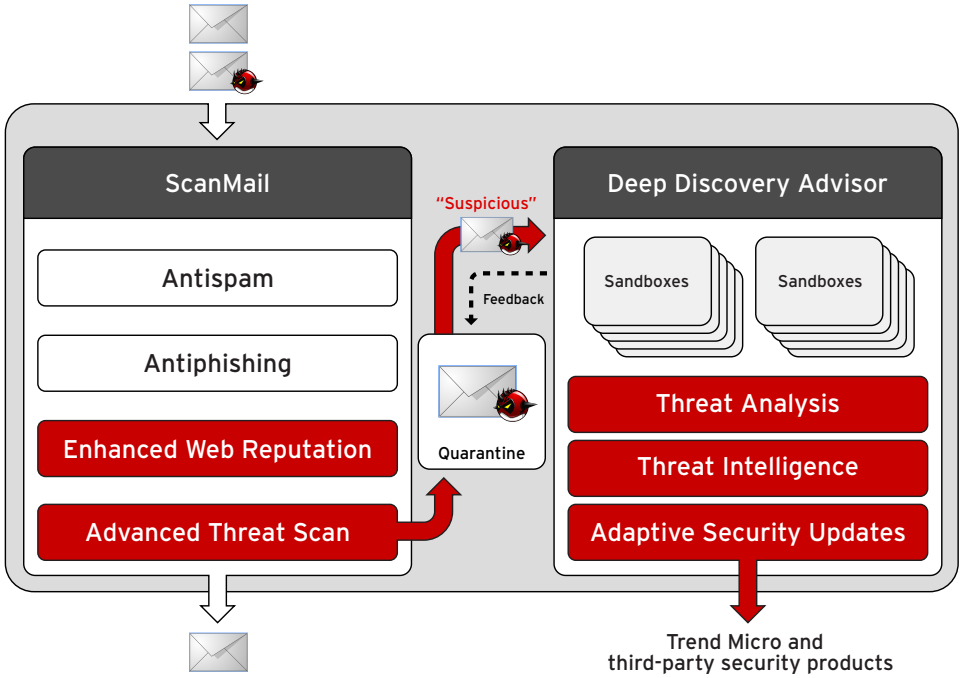
- Détecte les fichiers joints suspects et les liens Web malveillants, et neutralise les téléchargements malveillants.
- Le seul outil de sécurité email qui corrèle des services de réputation email, fichiers et Web pour juguler davantage de menaces véhiculées par email.
- Le meilleur taux de neutralisation du spam sur le marché selon un benchmark réalisé par Opus One.

Maîtrise des coûts informatique, meilleures performances

- Simplifie les opérations de sécurité email, grâce à la possibilité de configurer et de gérer des roupes, et des logs/reporting centralisés.
- Simplifie les initiatives de mise en conformité et de confidentialité, via une fonction de prévention des fuites de données gérée de manière centralisée et basée sur des templates.
- Allège les coûts d'administration et optimise le TCO, surclassant ainsi 4 autres outils concurrents selon Osterman Research.

LES ATTAQUES CIBLÉES IMPLIQUENT UNE DÉFENSE PERSONALISÉE

Les solutions de sécurité email de Trend Micro neutralisent les attaques ciblées grâce à un service optimisé de réputation Web, un nouveau moteur de détection et une analyse détaillée en sandbox. Ces fonctionnalités permettent de déployer une ligne de défense personnalisée pour détecter, analyser et prendre en charge les attaques ciblées.



La suite ScanMail

ScanMail a été enrichi de nombreuses fonctionnalités de protection contre les attaques ciblées :

Enhanced Web Reputation neutralise les URL malveillantes présentes dans le corps des messages ou en fichiers joint. Cette fonction est adossée à Trend Micro™ Smart Protection Network™ qui assure la corrélation des informations grâce à un traitement analytique et une technologie prédictive orientés big data.

Advanced Threat Scan Engine est un moteur qui détecte les malware présents furtivement dans des documents PDF, MS Office et autres formats, grâce à des sondes statiques ou comportementales qui détectent les vulnérabilités zero-day ou connues. La base email d'Exchange est également analysée pour identifier des menaces qui se seraient immiscées avant que l'outil de sécurité ne soit actif.

Lorsqu'intégré avec Trend Micro™ Deep Discovery Advisor, ScanMail met en quarantaine les fichiers suspects qui seront exécutés au sein d'une sandbox, et sans ralentir l'acheminement des autres messages.

Deep Discovery Advisor (en option)

Deep Discovery Advisor est une appliance matérielle qui offre le sandboxing, la détection des menaces, ainsi que des mises à jour de sécurité en local, au sein d'une plateforme de veille unifiée qui se veut la clé de voûte de l'offre Trend Micro Custom Defense.

Custom Threat Analysis assure une analyse détaillée et automatique des fichiers joints suspects au sein d'une sandbox, et notamment des exécutables et des documents MS Office. La solution permet aux clients de créer et d'analyser plusieurs images cibles personnalisées qui correspondent précisément à leurs environnements hôtes.

Custom Threat Intelligence corrèle les informations liées à des attaques qui ciblent votre environnement avec les données de veille de Trend Micro, pour offrir une visibilité précise qui permet d'évaluer, de maîtriser et de restaurer les incidents de sécurité.

Adaptive Security Updates propose des mises à jour de sécurité personnalisées avec, par exemple, la localisation des nouveaux serveurs C&C et Web malveillants identifiés lors des analyses sandbox : la protection et les restaurations gagnent ainsi en flexibilité avec ScanMail, et s'intègre avec les autres produits de sécurité de Trend Micro pour passerelles et postes clients, ainsi qu'avec les autres couches de sécurité existantes.

FONCTIONNALITÉS

Protection contre le Spear Phishing et les attaques ciblées

Contrairement aux autres outils de sécurité email, ScanMail offre un service de réputation web optimisé, la détection des vulnérabilités au sein de documents, une analyse en sandbox et une veille personnalisée sur les menaces. Ces fonctionnalités sécurisent totalement les emails contre le spear phishing associé aux menaces APT et aux attaques ciblées. Cette protection :

- Détecte les vulnérabilités connues ou nouvelles dans les documents PDF, MS Office et autres.
- Exécute les malware à des fins d'analyse, génère une veille personnalisée, et offre des mises à jour de sécurité via le module Deep Discovery Advisor proposé en option.
- Neutralise les menaces en amont de votre environnement avec une protection immédiate qui capitalise sur une veille mondiale sur les menaces.

Module de prévention des fuites de données

Renforce la sécurité existante pour assurer la conformité et prévenir les fuites de données. La protection DLP apporte une visibilité au cœur des données en transit ou stockées.

- Identifie les données sensibles au sein de votre outil email ou dans la base d'emails.
- Installation rapide et meilleure précision grâce à plus de 100 templates préinstallés.
- Déploiement simplifié grâce à un add-on qui active immédiatement la prévention des fuites de données et ne requiert aucun autre logiciel, ni matériel, pour appliquer des règles basées sur Active Directory.
- La console Control Manager™ permet aux équipes en charge de la conformité de gérer les règles de DLP de manière centralisée et de réagir à toute transgression identifiée sur les autres produits de sécurité pour postes clients et passerelles.

Optimisé pour Microsoft® Exchange

ScanMail s'intègre étroitement avec votre environnement Microsoft pour protéger efficacement l'email et avec un niveau de charges minimal.

- Compatible avec Exchange 2013, 2010 et 2007, et notamment avec les environnements hétérogènes lors des périodes de mise à niveau.
- Hautes performances – Jusqu'à 57% plus rapide que les autres outils.
- Evite de dupliquer les inspections grâce à des analyses antivirales multithread et au CPU throttling.
- Analyses efficaces et compatibilité aux environnements 64-bit.
- Intégration avec Microsoft® System Center Operations Manager et le filtre Junk E-mail d'Outlook®.
- Prévention des modifications de règles prohibées et contrôle d'accès fondé sur le rôle.

Fonction innovante Search & Destroy

Contrairement aux outils de sécurité proposés en matif par Exchange, ScanMail Search and Destroy identifie les emails de manière évoluée et précise.

- Mène des recherches ciblées par mot clé ou expression régulière au sein d'Exchange.
- Permet aux administrateurs de répondre rapidement aux demandes urgentes émanant des directions juridiques ou RH pour identifier, suivre et supprimer de manière permanente certaines adresses email.

Technologie évoluée de réputation
contre le spam, le phishing et les malware
Un traitement analytique orienté big data et une technologie prédictive sont utilisés pour corréler, dans le cloud, les données de réputation au niveau fichiers, web et email, et ainsi déployer une protection immédiate contre les menaces émergentes, avant que ces dernières n'atteignent les utilisateurs qui accèdent à leur messagerie, notamment via leurs équipements mobiles.

- Identification des liens malveillants dans le corps des emails et en fichier joint pour déjouer les attaques par phishing, grâce à une réputation Web performante.
- Une réduction du volume des emails entrants allant jusqu'à 85%, grâce au service de réputation qui valide les expéditeurs d'email.
- Neutralise davantage de spam que toute autre solution de sécurité email selon des tests indépendants.

Avantages

- Protège les utilisateurs contre les attaques ciblées, menées par spear phishing notamment.
- Offre une sécurité du Cloud de premier rang pour neutraliser les menaces à l'échelle du serveur d'emails et en amont des utilisateurs.
- Visibilité et contrôle sur les données pour prévenir les fuites de données et assurer la conformité.
- Débit accéléré grâce à une prise en charge en natif des plateformes 64-bit.
- Performances jusqu'à 57% plus rapides que celles de MS Forefront.
- Maîtrise des coûts d'administration et du TCO, grâce à une gestion centralisée.

SPÉCIFICATIONS SYSTÈMES

Mémoire	Espace DD	Navigateur	Serveur Web
• 1Go RAM • 2Go RAM recommandé (Exclusivement pour ScanMail)	• 2Go d'espace DD	• Microsoft Internet Explorer 6.0, 7.0, 8.0, et 9.0 • Mozilla Firefox 3.0 ou ultérieur • MSXML • MSXML 4.0 SP2 ou ultérieur	• Microsoft Internet Information Services (IIS) 7.5 ou 7.0

SPÉCIFICATIONS SYSTÈMES POUR MICROSOFT EXCHANGE

	Processeur	Système d'exploitation	Serveur Email
Microsoft Exchange 2013	• Matériel x64 avec processeur Intel compatible avec l'architecture Intel 64 (ex- Intel EM64T) • AMD processor that supports the AMD64 platform	• Windows Server 2012 Standard ou Datacenter • Windows Server 2008 R2 Standard avec SP1 • Windows Server 2008 R2 Enterprise avec SP1 • Windows Server 2008 R2 Datacenter RTM ou ultérieur	• Microsoft Exchange Server 2013
Microsoft Exchange 2010	• Matériel x64 avec processeur Intel compatible avec l'architecture Intel 64 (ex- Intel EM64T) • Processeur AMD compatible avec plateforme AMD64	• Windows Server 2012 Standard or Datacenter • Microsoft Windows Server 2008 avec Service Pack 2 (64-bit) • Microsoft Windows Server 2008 R2 avec Service Pack 1 (64-bit) • Microsoft Windows Server 2008 R2 (64-bit) • Microsoft Small Business Server (SBS) 2011	• Microsoft Exchange Server 2010 avec Service Pack 1, 2 ou 3 • Microsoft Exchange Server 2010
Microsoft Exchange 2007	• Matériel x64 avec processeur Intel compatible avec l'architecture Intel 64 (ex- Intel EM64T) • Processeur AMD compatible avec plateforme AMD64	• Microsoft Windows Server 2008 with Service Pack 2 (64-bit) • Microsoft Windows Server 2008 R2 with Service Pack 1 (64 bit) • Microsoft Windows Server 2008 R2 (64 bit) • Microsoft Windows Small Business Server 2008 (64 bit) • Microsoft Windows Server 2003 R2 avec Service Pack 2 (64-bit) • Microsoft Windows Server 2003 avec Service Pack 2 (64-bit)	• Microsoft Exchange Server 2007 avec Service Pack 1, 2 ou 3

TREND MICRO™

Securing Your Journey to the Cloud

Trend Micro SA
85, avenue Albert 1er
92500 Rueil Malmaison
http://www.trendmicro.fr
http://blog.trendmicro.fr

Tél : +33 (0) 1 76 68 65 00
email : sales@trendmicro.fr