

Trend Micro™

Deep Security 6

Protection des serveurs et des applications pour les centres de données dynamiques

Les entreprises sont de plus en plus actives en lignes et dépendantes des données. Et quelle que soit la fonction des applications - connexion des partenaires, du personnel, des fournisseurs ou des clients - celles-ci sont de plus en plus visées par les cyberattaques. Ces attaques ciblées n'ont jamais été aussi puissantes et sophistiquées qu'aujourd'hui et les exigences de conformité de la sécurité des données sont de plus en plus strictes. Votre société a besoin d'une sécurité sans compromis vous permettant de moderniser votre centre de données grâce à la virtualisation et au « cloud computing » (informatique en ligne) sans réduction des performances : des produits et services simples et intégrés, et des solutions économiques protégeant les données sensibles et minimisant les risques. Trend Micro a les solutions qui satisferont les besoins de votre centre de données.

Deep Security est un logiciel complet de protection des serveurs et applications permettant aux serveurs physiques et virtuels, ainsi qu'aux environnements virtuels, de s'autodéfendre. Cette solution permet la conformité à six exigences majeures de la norme PCI, notamment les exigences de pare-feu de couche application Web, la détection et la prévention des intrusions, la surveillance de l'intégrité des fichiers et la segmentation du réseau, ainsi qu'un large éventail d'autres exigences de conformité.

ARCHITECTURE

- **Deep Security Agent.** Ce petit composant logiciel déployé sur le serveur ou la machine virtuelle protégée assure la mise en œuvre des stratégies de sécurité du centre de données (IDS/IPS, protection des applications Web, contrôle des applications, pare-feu, surveillance de l'intégrité et inspection des journaux).
- **Deep Security Manager.** La puissante gestion centralisée permet aux administrateurs de créer des profils de sécurité et de les appliquer aux serveurs, de surveiller les alertes, de prendre des mesures préventives contre les menaces, de distribuer les mises à jour de sécurité aux serveurs et de générer des rapports.
- **Centre de sécurité.** Notre équipe d'experts de la sécurité vous aide à garder une longueur d'avance sur les dernières menaces en développant et en proposant rapidement des mises à jour de sécurité corrigeant les dernières failles de sécurité détectées. Un portail clients permet l'accès aux mises à jour de sécurité envoyées à Deep Security Manager pour être déployées.

INTÉGRATION ET DÉPLOIEMENT

Déploiement rapide pour tirer pleinement parti des investissements informatiques et de sécurité

- L'intégration de VMware, avec VMware vCenter et VMware ESX Server, permet l'importation d'informations organisationnelles et opérationnelles des nœuds vCenter et ESX vers Deep Security Manager et l'application de la sécurité détaillée sur l'infrastructure VMware de l'entreprise.
- Les événements de sécurité détaillés de niveau serveur sont fournis à un système de gestion des informations et des événements de sécurité (SIEM), tel qu'ArcSight™, Intellitectics, NetIQ, RSA Envision, Q1Labs, Loglogic et d'autres systèmes grâce à de nombreuses options d'intégration
- Intégration des annuaires avec les annuaires de l'entreprise, notamment Microsoft Active Directory
- La communication de la gestion configurable minimise, voire élimine, les changements de pare-feu généralement nécessaires aux systèmes à gestion centralisée en permettant soit à Manager soit à l'agent de lancer la communication
- Le logiciel agent peut être déployé facilement grâce à des mécanismes de distribution standard tels que Microsoft® SMS, Novel Zenworks et Altiris

PRINCIPAUX AVANTAGES

Empêche les fuites de données et les interruptions d'activité

- Offre une ligne de défense au niveau du serveur, qu'il soit physique, virtuel ou en ligne
- Empêche l'exploitation des failles de sécurité connues et inconnues dans les applications et systèmes d'exploitation
- Bloque les attaques sur les systèmes d'entreprise
- Identifie les activités et les comportements suspects en permettant des mesures proactives et préventives

Contribue à la conformité avec la norme PCI ainsi qu'avec d'autres réglementations et normes

- Permet la conformité avec six exigences majeures de la norme PCI, ainsi qu'avec de nombreuses autres exigences de conformité
- Fournit des rapports détaillés et adaptés aux audits, répertoriant les attaques bloquées et l'état de conformité aux stratégies
- Réduit le temps et les efforts nécessaires à la préparation des audits

Permet la réduction des coûts d'exploitation

- Permet aux entreprises de profiter pleinement de la réduction des coûts propre à la virtualisation ou au cloud computing
- Assure la protection contre les failles en vue d'accélérer la reprogrammation des codes de sécurité et la mise à disposition économique des correctifs de sécurité non prévus
- Assure une protection complète grâce à un seul agent logiciel à gestion centralisée, éliminant ainsi les coûts liés au déploiement de clients logiciels multiples

MODULES DE DEEP SECURITY

Inspection approfondie des paquets

- Examine l'ensemble du trafic entrant et sortant pour détecter tout détournement de protocole, ainsi que tout contenu présentant les caractéristiques d'une attaque ou d'une violation des stratégies
- Fonctionne en mode détection ou en mode prévention pour protéger les systèmes d'opération et corriger les failles de sécurité des applications d'entreprise
- Assure la protection contre les attaques de couche application et les attaques de type SQL injection ou cross-site scripting
- Fournit de précieuses informations sur l'heure et la date de l'attaque, son auteur, ainsi que la cible visée par l'exploit
- Notifie automatiquement les administrateurs lorsqu'un incident survient

Détection et prévention des intrusions

- Protège contre les attaques connues ou de type « zero-day » en couvrant les failles de sécurité connues contre les exploits illimités
- Couvre automatiquement les failles récemment découvertes en quelques heures, en assurant la distribution de la protection vers des milliers de serveurs en quelques minutes sans nécessiter de réinitialisation du système
- Comprend une protection contre les failles prête à l'emploi pour plus de 100 applications (bases de données, Web, messagerie, serveurs FTP).
- Des règles intelligentes permettent une protection « zero-day » contre les exploits inconnus visant une faille inconnue, en détectant les données de protocole inhabituelles contenant du code malicieux

Surveillance de l'intégrité

- Surveille les fichiers critiques du système d'exploitation et des applications, tels que les répertoires, les clés de registre et les valeurs en vue de détecter les modifications inattendues et malveillantes
- Permet la détection à la demande ou programmée, vérifie les propriétés des fichiers (PCI 10.5.5) et surveille des répertoires spécifiques
- Assure une surveillance flexible et pratique grâce aux inclusions/exclusions et permet la génération de rapports adaptés aux audits

Protection des applications Web

- Contribue à la conformité (PCI 6.6) afin de protéger les applications Web et les données qu'elles traitent
- Protège contre les attaques de type SQL injection, cross-site scripting et d'autres failles d'applications Web
- Couvre les failles jusqu'à ce que la reprogrammation du code soit achevée

Contrôle des applications

- Permet une meilleure visibilité ou un meilleur contrôle des applications accédant au réseau
- Utilise des règles de contrôle des applications pour identifier les logiciels malveillants accédant au réseau
- Réduit l'exposition des serveurs aux failles

Pare-feu dynamique bidirectionnel

- Réduit la surface d'attaque des serveurs physiques, virtuels et en ligne
- Permet la gestion centralisée de la stratégie de pare-feu des serveurs et comprend notamment des modèles de serveurs courants
- Comprend des fonctions de filtrage fin (adresses, ports IP et MAC), de stratégies de conception par interface réseau et de prise en compte du lieu d'utilisation
- Empêche les attaques de refus de service et détecte les scans de reconnaissance
- Couvre tous les protocoles IP (TCP, UDP, ICMP, etc.) et tous les types de trames (IP, ARP, etc.)

Inspection des journaux

- Collecte et analyse les journaux du système d'exploitation et des applications pour les événements liés à la sécurité
- Optimise l'identification d'événements de sécurité essentiels enfouis dans de multiples entrées de journaux
- Envoie les informations relatives aux événements au système SIEM ou au serveur de journalisation centralisé pour la corrélation, la génération de rapports et l'archivage
- Détecte les comportements suspects, collecte les informations des événements de sécurité et les mesures administratives sur l'ensemble de votre centre de données et crée des règles avancées à l'aide de la syntaxe OSSEC

PLATES-FORMES PROTÉGÉES

Microsoft® Windows®

- 2000 (32 bits)
- XP (32 bits/64 bits)
- XP Embedded
- Windows 7
- Windows Vista (32 bits/64 bits)
- Windows Server 2003 (32 bits/64 bits)
- Windows Server 2008 (32 bits/64 bits)

Solaris™

- Système d'exploitation : 8, 9, 10 (SPARC 64 bits, x86)

Linux

- Red Hat® Enterprise 3.0 (32 bits), 4.0, 5.0 (32 bits/64 bits)
- SUSE® Enterprise 9, 10 (32 bits)

UNIX®*

- AIX 5.3
- HP-UX® 10, 11i v2, 11i v3

* Seules la surveillance de l'intégrité et l'inspection des journaux sont disponibles

VIRTUALISATION

- VMware® : VMware ESX Server (système d'exploitation invité)
- Citrix® : XenServer Guest VM
- Microsoft® : HyperV Guest VM
- Sun : partitions de système d'exploitation Solaris 10

CERTIFICATIONS CLÉS ET ALLIANCES

- Common Criteria EAL 3+
- Test de « PCI Suitability » pour HIPS (NSS Labs)
- Virtualisation par VMware
- Programme de protection des applications Microsoft
- Partenariat Microsoft certifié
- Novell
- Partenariat Oracle
- Partenariat HP Business
- Certification de conformité Red Hat

MODULES DE DEEP SECURITY						
Obligations pour les centres de données	Inspection approfondie des paquets			Pare-feu	Surveillance de l'intégrité	Inspection des journaux
	IDS/IPS	Protection des applications Web	Contrôle des applications			
Protection serveur	●			●	●	○
Protection des applications Web	●	●			○	●
Sécurité de la virtualisation	●	○		●	●	
Détection des comportements suspects	○		●	●	●	●
Sécurité du cloud computing	●	○		●	●	●
Rapports de conformité	○	●	○	○	●	●

● Essentiel ○ Avantageux



© 2009 par Trend Micro Incorporated. Tous droits réservés. Trend Micro, le logo t-ball de Trend Micro, OfficeScan et Trend Micro Control Manager sont des marques commerciales ou des marques déposées de Trend Micro, Incorporated. Tous les autres noms de sociétés et/ou de produits peuvent être des marques commerciales ou déposées de leurs propriétaires respectifs. Les informations contenues dans ce document peuvent être modifiées sans préavis. [DS01DeepSecurity6_090811FR]

www.trendmicro.com