Trend Micro™

DEEP SECURITY

La sécurité intégrale des serveurs physiques, virtualisés ou Cloud

La virtualisation a transformé le data center et les organisations migrent maintenant tout ou partie du traitement de leurs données vers le Cloud. Pour tirer parti des avantages de la virtualisation et du Cloud, vous devez déployer une sécurité qui protège tous vos serveurs physiques, virtualisés ou Cloud. Cette sécurité ne doit pas avoir d'impact sur les performances des serveurs hôtes, la densité des machines virtuelles, ou le retour sur investissement attendu de la virtualisation et du Cloud. C'est ce que propose Trend Micro™ Deep Security™ grâce à une sécurité intégrale conçue sur mesure pour les environnements virtualisés et Cloud.

Protection des données et haute disponibilité
Deep Security – disponible en tant que logiciel ou sous forme de service – protège les traitements réalisés dans votre data center virtualisé ou dans le Cloud contre les piratages et les indisponibilités. Deep Security permet également de respecter les contraintes réglementaires en réduisant efficacement les écarts avec les référentiels de sécurité dans les environnements virtualisés et Cloud.

Différentes fonctions de sécurité gérées à partir d'un tableau de bord unique
Deep Security intègre différents modules de sécurité (anti-malware, réputation Web, pare-feu, prévention d'intrusion, monitoring de l'intégrité et inspection des logs) pour garantir la sécurité des serveurs, applications et données dans les environnements, physiques, virtuels ou Cloud. Deep Security peut être déployé comme un agent unique et multifonction, et propose une interface unifiée d'administration qui simplifie les opérations de sécurité. Vous pouvez utiliser Trend Micro Control Manager comme tableau de bord, ou encore VMware vRealize, Splunk, HP ArcSight et IBM QRadar.

Intégration transparente et application des règles sur l'ensemble des Clouds
Deep Security s'intègre en toute transparence avec les plateformes Cloud et notamment Amazon Web Services (AWS), Microsoft Azure et VMware vCloud Air : les règles de sécurité de votre data center s'appliquent ainsi à vos processus Cloud. Compatible avec de nombreux environnements, Deep Security permet aux entreprises et fournisseurs de services d'offrir un environnement Cloud différencié et mutualisé (multi-tenant) à leurs utilisateurs et clients.

Problématiques métiers

Sécurité des postes de travail virtualisés (VDI)
Optimise les performances et le taux de consolidation grâce à une sécurité sans agent adaptée aux environnements VDI.

Virtual patching
Protège des vulnérabilités avant qu'elles ne puissent être exploitées, éliminant ainsi les contraintes liées à l'application des correctifs en urgence, à la fréquence des cycles de patchs et aux indisponibilités.

Conformité
Assure la conformité avec de nombreuses réglementations comme PCI DSS 3.0, HIPAA, HITECH, FISMA/NIST, NERC, SSAE 16, et davantage.

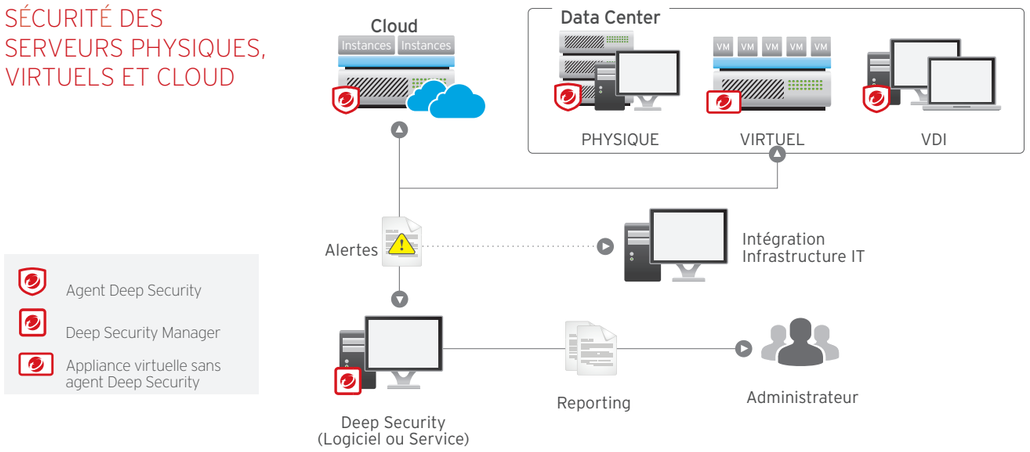
ACCÉLÉREZ LE ROI DES PROJETS CLOUD ET VIRTUALISATION, GRÂCE À UNE SECURITÉ ADAPTÉE AU DATA CENTER MODERNE

Sécurité des environnements virtualisés
Deep Security protège les postes de travail et serveurs virtualisés contre les vulnérabilités zero-day et les attaques réseau, et réduit l'impact lié à l'indisponibilité de ressources et au déploiement de correctifs en urgence.

Sécurité du Cloud
Avec Deep Security, les fournisseurs de services et managers de data centers offrent un Cloud multi-tenant, sécurisé par des règles contextuelles, cohérentes et centralisées, applicables aux processus Cloud.

Sécurité des serveurs
Deep Security consolide toutes les fonctions de sécurité au sein d'une plateforme intégrée et flexible qui optimise la protection des serveurs physiques, virtualisés et Cloud.

SÉCURITÉ DES SERVEURS PHYSIQUES, VIRTUELS ET CLOUD



AVANTAGES CLÉS

Efficacité et productivité

- Meilleure utilisation des ressources et densité plus importante des VM par rapport aux outils de sécurité traditionnels.
- Flexibilité et défense en profondeur grâce à un agent de sécurité multifonction simple à gérer.
- Des performances optimales grâce à une déduplication des analyses au niveau de l'hyperviseur.
- Intégration avec les plateformes Cloud AWS, Microsoft Azure et vCloud Air de VMware, permettant aux organisations de gérer leurs serveurs physiques, virtuels et Cloud, à l'aide de règles de sécurité contextuelles et cohérentes.
- Les fournisseurs de services peuvent offrir un Cloud public sécurisé avec cloisonnement des différents environnements clients grâce à une architecture multi-tenant.
- Offre des fonctions d'auto-scaling, de facturation à l'utilisation et un mode self-service adaptés aux organisations agiles opérant des SDDC (Software Defined Data Center).
- Intégration étroite Deep Security - VMware : détection automatique des nouvelles VM et application de règles contextuelles garantissant une sécurité cohérente sur l'ensemble du data center et du Cloud
- Intégration avec VMware vSphere 6 et NSX™. Deep Security étend les avantages de la micro-segmentation au sein des SDDC, grâce à des règles et fonctions de sécurité qui s'appliquent aux VM, même lorsqu'elles sont migrées.

Prévient les piratages de données et les indisponibilités

- Détecte et neutralise les malware sur les serveurs virtuels en temps réel, avec un impact minimal sur les performances.
- Neutralise les malware qui tentent de ne pas se faire détecter en désinstallant ou neutralisant les programmes de sécurité.
- Protège des vulnérabilités connues et inconnues au sein des applications Web et d'entreprise, et des systèmes d'exploitation.
- Envoie des alertes et active une prévention proactive dès la détection d'une activité suspecte ou malveillante.
- Assure un suivi du niveau de confiance des sites Web et protège les utilisateurs contre les sites infectés, grâce à un service de réputation fourni par la base de données de réputation mondiale de Trend Micro.
- Identifie et neutralise les botnets, attaques ciblées et communications Command & Control, grâce à une veille sur les menaces fournie par la base de données de réputation des domaines de Trend Micro.

Maîtrise des coûts d'exploitation

- Supprime les coûts associés au déploiement de plusieurs logiciels, grâce à un agent logiciel (ou appliance virtuelle) unique, polyvalent et géré de manière centralisée.
- S'intègre étroitement avec les consoles d'administration de Trend Micro ou VMware, et les plateformes telles que VMware vRealize, Splunk, HP ArcSight et IBM QRadar.
- Protège contre les vulnérabilités connues et inconnues au sein des applications Web et d'entreprise, et des systèmes d'exploitation.
- Allège les coûts d'administration : automatisation des tâches de sécurité répétitives et mobilisant des ressources importantes, réduction du nombre de faux-positifs lors des alertes de sécurité et workflow de prise en charge des incidents de sécurité.
- Simplifie le contrôle d'intégrité des fichiers, grâce à une liste blanche d'événements basée dans le Cloud.
- Identifie les logiciels et correctifs installés via une analyse de recommandation, détecte les vulnérabilités et déploie automatiquement les protections adaptées.
- Favorise la productivité opérationnelle, grâce à un agent intelligent et temps-réel qui facilite le déploiement et optimise l'attribution des ressources au sein du data center et du Cloud
- Adapte la sécurité à vos besoins, en attribuant le niveau de ressources requis pour les fonctions de sécurité spécifiques.
- Centralise l'administration de tous les produits Trend Micro. Le reporting centralisé sur toutes les fonctions de sécurité évite de créer un rapport pour chaque produit de sécurité.

Une conformité réglementaire économique

- Une solution unique, intégrée et économique qui assure la conformité avec PCI DSS 3.0, HIPAA, HITECH, NIST et SAS 70.
- Des rapports d'audit détaillés répertorient les attaques bloquées et le statut de conformité aux règles de sécurité.
- Accélère et simplifie la préparation des audits.
- Accompagne les initiatives internes de mise en conformité pour améliorer la visibilité sur l'activité du réseau interne.
- Utilise des technologies certifiées Common Criteria EAL 4+.

LES MODULES DE DEEP SECURITY

Anti-malware avec réputation Web

- Intégration avec les API de VMware vShield Endpoint pour protéger les machines virtuelles VMware, sans impact sur l'hôte.
- Agent anti-malware pour protéger les serveurs physiques, virtualisés et dans le Cloud, au sein des environnements AWS, Microsoft et VMware notamment.
- Améliore les performances grâce aux fonctions de mise en cache et de déduplication au niveau de VMware ESX.
- Evite d'exécuter des opérations en simultané, dont les charges sont susceptibles de peser sur les performances lors des analyses antivirales et la mise à jour de signatures.
- Protège contre les attaques sophistiquées ciblant les environnements virtuels, en isolant tout malware des modules critiques du système d'exploitation et de sécurité.
- S'adosse à l'infrastructure Trend Micro™ Smart Protection Network™ et bénéficie de services de réputation renforçant la protection des serveurs et des postes de travail virtuels.

Prévention des intrusions

- Analyse le trafic entrant et sortant. Détecte les anomalies protocolaires, les violations des règles de sécurité et les contenus caractéristiques des attaques.
- Protège automatiquement contre les vulnérabilités non corrigées, grâce à un mécanisme de patch virtuel qui interdit l'exploitation de la vulnérabilité : cette protection est mise à disposition de milliers de serveurs en quelques minutes et sans redémarrage du système.
- Favorise la conformité réglementaire avec l'exigence 6.6 de PCI DSS et protège les applications et les données qu'elles traitent.
- Protège contre les vulnérabilités des applications Web (injection SQL, cross-site scripting…)
- Propose une protection prête à l'emploi contre les vulnérabilités des principaux systèmes d'exploitation et de plus de 100 applications (bases de données, applications web, email, serveur FTP, etc.)
- Offre d'avantage de visibilité et de contrôle sur les applications accédant au réseau.

Pare-feu hôte bidirectionnel

- Restreint la surface d'attaque des serveurs physiques, virtuels et Cloud grâce à un filtrage granulaire, des règles par réseau et la géolocalisation, pour tous les protocoles IP et les types de trames.
- Gestion centralisée des règles du pare-feu des serveurs, avec notamment des modèles pour les types de serveurs courants.
- Empêche les attaques de déni de service et détecte les scans de reconnaissance.
- Logue les événements du pare-feu, facilitant ainsi le reporting de conformité et d'audit, essentiel pour les Clouds publics.

Contrôle d'intégrité

- Surveille les fichiers critiques du système d'exploitation et des applications (répertoires, clés de registre et valeurs) pour détecter et consigner en temps réel les modifications non programmées et/ou malveillantes.
- Utilise la technologie Intel TPM/TXT pour contrôler l'intégrité de l'hyperviseur face aux changements non autorisés, étendant ainsi la couverture des fonctions de sécurité et de conformité au niveau de l'hyperviseur.
- Réduit les charges d'exploitation avec la définition d'événements de confiance, qui entraînent une exécution automatique d'actions prédéfinies sur l'ensemble du data center.
- Propose un système de liste blanche automatique d'événements de confiance, basé dans le Cloud et géré par Trend Micro.

Inspection des logs

- Recueille et analyse les logs applicatifs et du système d'exploitation dans plus de 100 formats de logs, pour identifier les comportements suspects, ainsi que les événements de sécurité et d'administration sur l'ensemble du data center.
- Favorise le respect de l'exigence 10.6 de PCI DSS pour identifier des événements de sécurité importants mais peu visibles.
- Re-route les événements vers des systèmes SIEM à des fins de corrélation, de reporting et d'archivage.

Certification pour les CSP

Trend Ready for Cloud Service Providers est un programme mondial de certification à l'intention des CSP (Cloud Services Provider ou fournisseurs de services Cloud) pour assurer l'interopérabilité avec les solutions de sécurité Cloud de Trend Micro.

Certification et Alliances

- Partenaire Amazon Advanced Technology
- Certifié Red Hat Ready
- Validation Cisco UCS
- Common Criteria EAL 4+
- Validation EMC VSPEX
- Partenaire HP Business
- Microsoft Application Protection Program
- Microsoft Certified Partnership
- Validation NetApp FlexPod
- Oracle Partnership
- Tests de conformité à PCI pour le HIPS (NSS Labs)
- SAP Certified (NW-VSI 2.0 et HANA)
- Validation VCE Vblock
- Virtualization par VMware

awsmarketplace

vmware

Microsoft Azure

TREND MICRO READY

Deep Security for SAP est un module de protection intégré avec les systèmes SAP.

SAP Partner

DÉPLOIEMENT ET INTÉGRATION

Déploiement rapide : capitaliser sur les investissements existants

- Intégration avec vShield via les librairies epsec pour une protection anti-malware des machines virtuelles vSphere au sein des environnements non-NSX.
- Deep Security en Combined Mode optimise la protection des machines virtuelles. Une appliance virtuelle peut être utilisée pour déployer un anti-malware et un contrôle d'intégrité sans agent. Elle peut être associée à l'agent Deep Security pour la prévention d'intrusions, le firewalling et la réputation Web, et garantir ainsi une protection optimale des environnements non-NSX.
- L'intégration avec NSX Manager permet un déploiement rapide sur les serveurs ESX en tant qu'appliance virtuelle pour protéger les VM vSphere de manière immédiate et transparente.
- Les événements liés à la sécurité serveur peuvent être intégrés aux systèmes SIEM HP ArcSight, Intellitactics, IBM QRadar, NetIQ, RSA Envision, Q1Labs, Loglogic, etc.
- Intégration avec les annuaires d'entreprise tels qu'Active Directory de Microsoft.
- Des agents logiciels peuvent être déployés simplement via les mécanismes d'outils tels que Chef, Puppet, AWS OpsWorks, Microsoft System Center Configuration Manager (SCCM), Novell ZENworks et Symantec Deployment Solution.

ARCHITECTURE DE LA PLATEFORME

Appliance virtuelle Deep Security. Applique de manière transparente les règles de sécurité sur les machines virtuelles VMware vSphere NSX, et déploie en mode sans-agent les fonctions d'anti-malware, de réputation Web, de prévention des intrusions, de monitoring de l'intégrité et de pare-feu. Pour les environnements autres que NSX, l'appliance virtuelle sans agent peut être utilisée pour l'anti-malware et le contrôle de l'intégrité, tandis qu'un agent assurera les fonctions de pare-feu, de réputation web et d'inspection des logs.

Agent logiciel Deep Security. Ce composant logiciel léger, déployé sur le serveur ou la machine virtuelle à protéger, applique les règles et fonctions de sécurité du data center (anti-malware, réputation Web, IDS/IPS, pare-feu, contrôle d'intégrité et inspection des logs). Le déploiement peut être automatisé via des outils de gestion opérationnelle tels que Chef, Puppet et AWS OpsWorks.

Deep Security Manager. Cette console d'administration puissante et centralisée propose une administration basée sur les rôles et permet de concevoir des règles de sécurité granulaires, hiérarchisées par des fonctions d'héritage. Les fonctions d'automatisation des tâches (analyse de recommandation et tagging d'événements) simplifient la gestion de sécurité au jour le jour. L'architecture multi-tenant permet de définir des règles applicables à des environnements spécifiques et de déléguer l'administration aux administrateurs de ces environnements.

Veille technologique globale. Deep Security s'intègre avec l'infrastructure Trend Micro Smart Protection Network pour une protection en temps réel contre les menaces émergentes, grâce à une évaluation et à une corrélation permanente des services de veille sur les menaces et de réputation pour les sites Web, les emails et les fichiers.

SPÉCIFICATIONS
Microsoft® Windows®
• Windows XP, Vista, 7, 8, 8.1 (32/64-bit) | Windows Server 2003 (32-bit/64-bit) | Windows Server 2008 (32-bit/64-bit), 2008 R2, 2012, 2012 R2, 2012 Server Core (64-bit) | XP Embedded (32/64-bit)[1]
Linux[2]
• Red Hat® Enterprise 5, 6, 7 (32/64-bit)[3] | SUSE® Enterprise 10, 11, 12 (32/64-bit)[3] | CentOS 5, 6 (32/64-bit)[5] | Ubuntu 10, 12, 14 (64-bit, LTS seulement)[4, 5] | Oracle Linux 5, 6, 7 (32/64-bit)[4, 5] | Cloud Linux 5, 6 (32/64-bit)[4] |Cloud Linux 7 (32/64-bit)[2] |Amazon Linux[4, 5] | Debian 6, 7 (64-bit)[4]
Oracle Solaris™ [6, 7]
• OS: 9, 10, 11 (64-bit SPARC), 10, 11 (64-bit x86)[7, 8] | Oracle Exadata Database Machine, Oracle Exalogic Elastic Cloud et SPARC Super Cluster via les systèmes d'exploitation Solaris compatibles
UNIX[6]
• AIX 5.3, 6.1, 7.1 sur IBM Power Systems[7, 8] | HP-UX 11i v3 (11.31)[7, 9]
VIRTUEL
• VMware® vSphere: 5.0/5.1/5.5/6.0, vCloud Networking and Security 5.1/5.5[10], View 4.5/5.0/5.1, ESX 5.5, NSX 6.1.X | Citrix®: XenServer[11] | Microsoft®: HyperV[11]

[1] Compte tenu de la personnalisation possible avec Windows XP Embedded, les clients doivent tester la solution dans leur environnement pour s'assurer que les ports réseaux et services nécessaires à l'exécution de Deep Security ont été activés | [2] Voir la documentation pour les kernels compatibles | [3] Support SAP seulement du côté agent de Red Hat 6 (64-bit) et SUSE 11 (64-bit). Pour que la sécurité SAP fonctionne correctement, le module anti-malware doit être activé du côté agent | [4] Anti-malware pour les analyses à la demande seulement | [5] Consultez les notes les plus récentes pour les versions compatibles | [6] Anti-malware et réputation Web non disponibles | [7] Pris en charge par les agents de la version 9.0 | [8] Anti-malware non disponible | [9] Inspection des logs et monitoring de l'intégrité seulement | [10] vCloud Networking and Security permet un monitoring et un anti-malware sans agent | [11] Protection via l'agent Deep Security Agent seulement.

TREND MICRO™

Securing Your Journey to the Cloud

http://www.trendmicro.com