Trend Micro™

DEEP SECURITY

La sécurité intégrale de vos environnements virtualisés, Cloud et de conteneurs

La virtualisation a transformé le data center et les organisations migrent désormais leurs charges de travail vers le Cloud et les conteneurs. Le Cloud hybride, s'il présente de nombreux avantages, n'est cependant pas exempt de risques. Votre entreprise doit assurer sa conformité réglementaire et sécuriser l'ensemble de ses charges en environnement physique, virtualisé, Cloud et de conteneurs. Trend Micro™ Deep Security™ offre une sécurité intégrale des environnements virtualisés, Cloud et de conteneurs, ainsi qu'un riche panel d'API qui automatise la sécurité et simplifie la tâche de vos équipes.

ROBUSTESSE
Protège contre les vulnérabilités, malware et modifications non autorisées

SIMPLICITÉ
Une protection pertinente et une visibilité précise sur l'ensemble de votre Cloud hybride

AUTOMATISATION
Une sécurité interconnectée s'intègre en toute transparence avec vos processus de développement et opérationnel

SÉCURITÉ
Des fonctions intelligentes de sécurité vous permettent de tenir vos engagements de sécurité et de conformité dès les versions initiales de vos logiciels

DÉPLOIEMENT RAPIDE
Une sécurité automatisée et intégrée dans votre pipeline CI/CD

INTEROPÉRABILITÉ
Une sécurité optimisée pour les différentes plateformes accueillant vos applications

Défis métiers

Protection automatisée
Automatisez la sécurité à l'aide d'API RESTful et de modèles Cloud pour minimiser les processus manuels et maîtriser les coûts d'exploitation.

Sécurité unifiée
Déployez et configurez la sécurité pour vos environnements physiques, virtualisés, multi-Cloud et de conteneurs, avec un seul agent et une plateforme unique.

Sécurité dans le pipeline CI/CD
Des outils adaptés au développement logiciel et un panel d'API permettent d'intégrer les fonctions de sécurité au sein des processus DevOps.

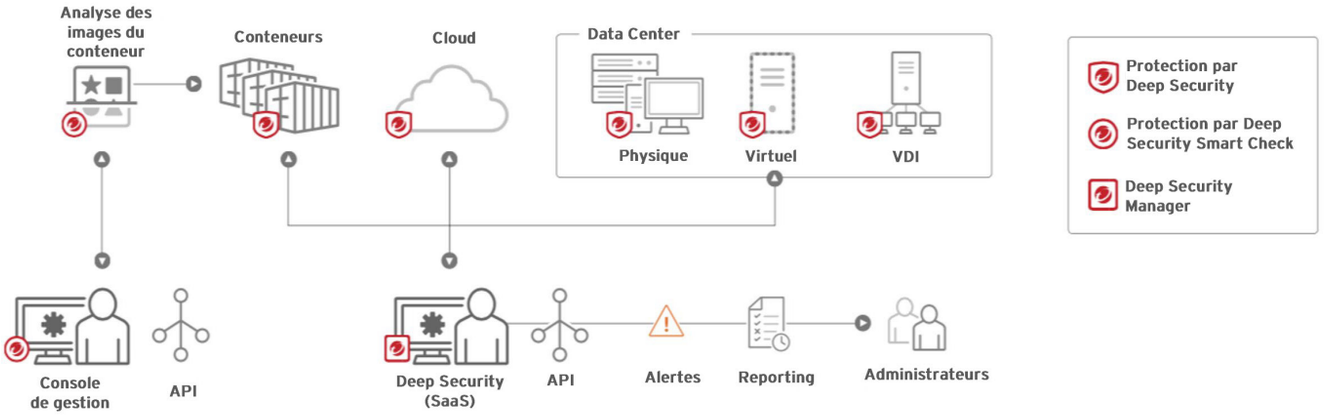
Accélérer la mise en conformité
Assurez votre conformité avec de nombreuses réglementations : RGPD, PCI DSS, HIPAA, NIST, FedRAMP, etc.

UNE SÉCURITÉ DE CONFIANCE POUR LE CLOUD HYBRIDE

Une sécurité sur l'ensemble du cycle de vie des conteneurs - Deep Security optimise la protection des conteneurs en environnement de production Une sécurité multi-couche vous protège des attaques sur l'hôte, la plateforme du conteneur (Docker®), l'outil d'orchestration (Kubernetes®), les conteneurs eux-mêmes et les applications en conteneur. Avec son riche panel d'API, Deep Security protège les conteneurs via des processus et fonctions de sécurité automatisés. La sécurité s'intègre dans le pipeline CI/CD de DevOps, pour que les bonnes pratiques de sécurité soient appliquées au sein d'infrastructures en évolution. En analysant les images des versions logicielles dans le pipeline, Deep Security déploie une protection intégrale à chaque étape du cycle de vie d'un conteneur.

Automatisation de la sécurité du Cloud - Deep Security sécurise en temps réel le Cloud, avec une découverte automatisée des charges des fournisseurs Cloud tels qu'AWS, Microsoft® Azure® et Google Cloud™. La console de gestion de Deep Security offre une visibilité unifiée sur l'ensemble de vos charges de travail et automatise la protection sur les environnements multi-Cloud, avec des règles pertinentes et contextuelles. Les API RESTful intègrent la sécurité avec vos outils de sécurité existants, dans une optique d'automatisation, pour gérer les règles de sécurité, évaluer les niveaux de sécurité et assurer un reporting de conformité.

Sécurité du data center virtualisé - Deep Security déploie une protection évoluée des serveurs physiques et virtualisés, favorisant ainsi un déploiement et une gestion simplifiée de la sécurité sur de multiples environnements, grâce à une gestion automatisée des règles et, pour VMware®, une sécurité sans agent intégrée à l'hyperviseur. Deep Security protège les postes de travail et serveurs virtualisés contre les malware Zero-Day, les ransomware, le cryptomining et les attaques réseau, tout en réduisant l'impact des ressources peu efficaces et du patching en urgence sur l'opérationnel.



AVANTAGES

Protection avancée contre les menaces

- Protège vos serveurs et applications à l'aide de fonctions évoluées : IPS, monitoring de l'intégrité, Machine Learning, contrôle applicatif, etc.
- Détecte et bloque les menaces en temps réel, avec un impact minimal sur les performances, ainsi que l'exécution de logiciels suspects (contrôle applicatif).
- Protège les vulnérabilités connues et inconnues dans le web, les applications d'entreprise et les systèmes d'exploitation, via un IPS.
- Détection avancée des menaces et remédiation des objets suspects et des activités malveillantes.
- Alerte et prévention lors de la détection d'une activité malveillante.
- Sécurise les systèmes en fin de support à l'aide de patchs virtuels fournis par un IPS : vos systèmes obsolètes restent ainsi protégés.
- Protège les utilisateurs contre les sites web infectés grâce au service de réputation des domaines de Trend Micro.
- Identifie et neutralise les botnets et les communications C&C (Command & Control) des attaques ciblées.
- Prévient les menaces les plus récentes grâce à la veille sur les menaces issue de Trend Micro™ Smart Protection Network™.

Une sécurité unifiée pour le Cloud hybride

- Les connecteurs Cloud et pour data center identifient automatiquement les charges de travail de votre environnement Cloud hybride pour offrir une visibilité intégrale sur votre environnement, ainsi qu'une gestion automatisée des règles.
- Évite de déployer plusieurs solutions autonomes et favorise une sécurité intégrée sur les environnements physiques, virtualisés et Cloud, grâce à un agent logiciel unique et léger et une seule console de gestion.
- Sécurise les différentes couches de vos environnements de conteneurs : l'hôte, la plateforme de conteneur (Docker), la plateforme d'orchestration (Kubernetes), les conteneurs eux-mêmes ainsi que les applications dans les conteneurs.
- Sécurise votre hôte de conteneur à l'aide des mêmes fonctions sophistiquées qui protègent vos charges de travail physiques, virtualisées et Cloud.
- Surveille les changements et attaques sur les objets Docker et Kubernetes grâce au monitoring d'intégrité et à l'inspection des logs.
- Protège les conteneurs en production en restaurant leurs vulnérabilités (via un IPS), en activant une protection antimalware en temps réel et en inspectant le trafic entrant et sortant des conteneurs.

Accompagner les équipes d'intervention post incident

- La prise en charge des incidents est assurée grâce à des fonctions EDR (Endpoint Detection and Response) : monitoring des indicateurs d'attaque et la neutralisation d'applications et de processus suspects.
- Intégrez Deep Security avec votre SIEM pour identifier les menaces sophistiquées et les indicateurs de compromission. Associez cette solution avec les outils d'orchestration, d'automatisation et de remédiation.
- En l'absence de ressources ou du temps nécessaires, optez pour le service MDR (Managed Detection & Response) de Trend Micro.

- Sécurise proactivement le pipeline : les analyses d'images et de registres qu'offre Deep Security Smart Check viennent en complément des fonctions de Deep Security, pour ainsi protéger les conteneurs à chaque étape de leur cycle de vie.
- Tire parti d'une intégration étroite de Trend Micro avec les principaux fournisseurs Cloud tels qu'AWS, Azure et Google Cloud, pour une protection de vos environnements multi-Cloud et une visibilité unifiée.
- Permet aux fournisseurs de service d'offrir à leur client un Cloud public sécurisé et mutualisé (multi-tenant).
- Apporte les avantages de la micro-segmentation dans le data center software defined et tire parti de l'intégration de Deep Security avec VMware pour appliquer automatiquement des règles contextuelles.

Sécurité automatisée et simplifiée

- Automatise le déploiement de la sécurité, la gestion des règles et le reporting de conformité grâce aux API REST de Deep Security.
- Réduit les coûts de gestion en automatisant les tâches de sécurité répétitives, en réduisant le nombre de faux-positifs d'alertes et en proposant un workflow de prise en charge des incidents de sécurité.
- Simplifie le monitoring d'intégrité des fichiers grâce à une liste blanche d'événements Cloud et de confiance.
- Adapte la sécurité à vos besoins, pour restreindre le nombre de personnes nécessaires à des tâches de sécurité spécifiques.
- Simplifie l'administration grâce à une gestion centralisée de l'ensemble des produits Trend Micro. Le reporting centralisé sur de multiples fonctions de sécurité est une alternative plus simple à la création d'un reporting pour chaque produit.
- Connectez la sécurité avec les outils de sécurité et DevOps déjà en place, grâce à une intégration avec les principaux outils de SIEM, de gestion de la sécurité, d'orchestration, de monitoring, du pipeline et de gestion des services IT.

Une conformité à moindre coût

- Facilite la conformité aux exigences du RGPD, de PCI DSS, de HIPAA et autres.
- Offre un reporting détaillé qui documente les attaques neutralisées et le niveau de respect des règles de sécurité.
- Accélère les délais de préparation et allège les efforts nécessaires aux audits.
- Favorise les initiatives internes de conformité pour renforcer la visibilité sur l'activité du réseau interne.
- Permet de consolider les outils de conformité réglementaire grâce à des fonctions optimales de monitoring de l'intégrité des fichiers.
- Capitalise sur des technologies certifiées Common Criteria EAL 2 et FIPS 140-2.
- Favorise la conformité dans le pipeline de développement grâce aux analyses de Deep Security Smart Check portant sur les images et les registres.

FONCTIONNALITÉS DE DÉTECTION ET DE PROTECTION DE DEEP SECURITY

Les outils de sécurité réseau détectent et neutralisent les attaques et protègent les applications et serveurs vulnérables

- ***Prévention des intrusions basée sur l'hôte :***
  Détecte et neutralise l'exploitation de vulnérabilités connues au sein d'applications et de systèmes d'exploitation populaires, à l'aide de règles IPS.
- ***Réputation web :***
  Neutralise l'accès aux URL et sites web malveillants.
- ***Pare-feu :***
  Un pare-feu sur l'hôte protège les Endpoints sur le réseau à l'aide d'une inspection dynamique.
- ***Analyse des vulnérabilités :***
  Identifie les vulnérabilités réseau connues des systèmes d'exploitation et applications.

Des outils de sécurité système verrouillent les systèmes et détectent les activités suspectes

- ***Contrôle applicatif :***
  Neutralise l'installation d'exécutables et scripts non identifiés comme sains.
- ***Inspection des logs :***
  Identifie et alerte sur les changements non planifiés, les intrusions ou les attaques sophistiquées par malware (ransomware notamment) sur vos systèmes.
- ***Monitoring de l'intégrité des fichiers :***
  Surveille toute modification apportée aux fichiers, aux bibliothèques et aux services. Pour valider la sécurité des configurations, une image de base est créée pour représenter ce qu'est une configuration sécurisée. Lorsqu'un écart par rapport à de cet état cible est identifié, les détails sont mis en log et des alertes peuvent être émises vers les personnes concernées.

La prévention des malware neutralise les malware et les attaques ciblées

- ***Anti-Malware :***
  i. Réputation de fichiers : neutralise les fichiers malveillants à l'aide de nos signatures antimalware.
  ii. Protection contre les variantes : recherche les variantes furtives ou polymorphes de malware en utilisant des fragments de malware déjà identifiés et des algorithmes de détection.
- ***Analyse comportementale :***
  Examine les éléments inconnus et recherche les comportements suspects dans le système d'exploitation, les applications et les scripts.
- ***Machine Learning :***
  Analyse les fichiers inconnus et les menaces Zero-Day à l'aide d'algorithmes de Machine Learning pour déterminer si le fichier est malveillant.
- ***Analyse en sandbox :***
  Les objets suspects peuvent être soumis à la sandbox de Trend Micro™ Deep Discovery™ à des fins d'analyses poussées. Une réponse rapide est alors fournie à Deep Security..

UNE SÉCURITÉ CONÇUE POUR LE CLOUD

Deep Security est conçu pour les infrastructures des principaux fournisseurs de services Cloud et est compatible avec les systèmes d'exploitation les plus courants :

Linux | Windows | SUSE
redhat | CentOS | ubuntu

Compatibilité avec configuration, événement et outils d'orchestration :

CHEF | puppet labs | OpsWorks | SALTSTACK
sumologic | ANSIBLE | |
SWIMLANE | now | DEMISTO | splunk>

ARCHITECTURE

Agent Deep Security

Applique les règles de sécurité en vigueur (contrôle applicatif, anti-malware, IPS, pare-feu, monitoring d'intégrité et inspection des logs) via un composant logiciel léger déployé sur le serveur ou la VM (peut être déployé automatiquement avec des outils de gestion opérationnelle comme Chef, Puppet®, Ansible et AWS OpsWorks).

Deep Security Manager

Une console de gestion centralisée et puissante : une administration fondée sur le rôle et l'application des règles sur de multiples niveaux favorisent un contrôle granulaire. Les fonctions d'automatisation des tâches, comme les analyses de recommandation et les tâches basées sur des évènements simplifient l'administration de la sécurité. L'architecture multi-tenant permet d'isoler des règles pour un client final et de déléguer la gestion de la sécurité aux administrateurs de ce client.

Appliance virtuelle Deep Security

Applique les règles de sécurité aux VM de Mware vSphere®. Pour les environnements VMware NSX®, ceci permet plusieurs fonctions : anti-malware sans agent, réputation web, monitoring d'intégrité et protection par pare-feu. Un mode « combiné » peut être utilisé dans lequel l'appliance virtuelle est utilisée au format sans agent pour le monitoring d'intégrité et l'anti-malware en tant qu'agent pour l'IPS, le contrôle applicatif, le pare-feu, la réputation web et l'inspection des logs.

Une veille mondiale sur les menaces

Deep Security s'intègre avec le Smart Protection Network pour offrir une protection en temps réel contre les menaces émergentes. Cette protection évalue et corrèle des informations sur les menaces et de réputation pour les sites web, l'email et les fichiers.

SPÉCIFICATIONS SYSTÈMES (Software as a Service (SaaS), Manager, appliance virtuelle et agents)

- Deep Security est disponible en tant que service et tous les composants de gestion sont hébergés et maintenus par Trend Micro.
- Deep Security est également disponible en tant que logiciel ou appliance virtuelle qui se déploie dans votre data center ou votre Cloud. Les spécifications systèmes sont disponibles sur : **https://help.deepsecurity.trendmicro.com/11_3/on-premise/Get-Started/Install/system-requirements.html**

PLATEFORMES COMPATIBLES (pour l'agent)

- Trend Micro se rend compatible à de nouveaux systèmes d'exploitation et versions. Merci de consulter l'URL suivante pour connaître les plateformes compatibles, dont Microsoft® Windows®, Linux®, Solaris, AIX et les conteneurs Docker : **https://help.deepsecurity.trendmicro.com/11_3/on-premise/Manage-Components/Software-Updates/compatibility.html**

DEEP SECURITY AS A SERVICE (DSaaS)

DSaaS vous apporte la protection éprouvée de Deep Security mais sous une forme de service prêt à l'emploi. Nous nous occupons du déploiement et du provisioning du service. Nous gérons les mises à jour du kernel et du produit, nous installons la base de données de sécurité et en assurons la maintenance, et nous administrons le gestionnaire de Deep Security. Nos offres de sécurité fournies à partir du Cloud favorisent une installation rapide et simplifient les opérations de sécurité des instances Cloud.

Avantages clés

- **Rapidité** : sécurisez vos charges en quelques minutes
- **Maîtrise des coûts** : une tarification à l'utilisation à partir de €0,01 / heure
- **Simplicité** : de multiples fonctions de sécurité à partir d'un seul produit
- **Gain de temps** : nous gérons et mettons à jour le service à votre place
- **Sécurité éprouvée** : des milliers des clients & des millions de serveurs protégés
- **Flexibilité** : disponible via les marketplaces d'AWS et d'Azure pour protéger les environnements multi-Cloud

Deep Security Scanner est un module qui protège les systèmes SAP en s'intégrant avec l'interface de scan antiviral de SAP NetWeaver®.

SAP Partner

CERTIFICATION FOR CLOUD SERVICE PROVIDERS (CSPs)

Le programme mondial pour les partenaires CSP de Trend Micro vise à valider l'interopérabilité des fournisseurs de services Cloud avec les solutions de sécurité Cloud de Trend Micro.

"Avec un partenaire comme Trend Micro, qui tire parti de technologies modernes pour neutraliser les menaces sophistiquée en temps réel, nos charges de travail sont protégées en permanence, même lorsque les architectures évoluent."

Jason Cradit
Senior Director of Technology, TRC

TREND MICRO™

Securing Your Connected World