Trend Micro

CLOUD ONE™ – WORKLOAD SECURITY

La sécurité des serveurs physiques, virtuels, Cloud et des conteneurs en environnement de production

Les entreprises sont toujours plus nombreuses à migrer leurs serveurs vers le Cloud et à tirer parti des conteneurs et du serverless pour concevoir leurs applications Cloud-native. Le Cloud hybride, s'il présente de nombreux avantages, n'est néanmoins pas exempt de risques. Votre entreprise doit assurer sa conformité réglementaire et sécuriser tous ses serveurs physiques, virtualisés et Cloud, ainsi que ses conteneurs.

Trend Micro™ Cloud One™ – Workload Security est une solution unifiée pour une sécurité intégrale des environnements virtualisés, Cloud et des conteneurs. Workload Security sécurise tous les types d'environnements et offre un riche panel d'API qui automatise la sécurité et simplifie la tâche de vos équipes.

UNE SÉCURITÉ FIABLE POUR LE CLOUD HYBRIDE

Sécuriser l'ensemble du cycle de vie des conteneurs

Workload Security optimise la protection des conteneurs en production. La sécurité en profondeur vous protège contre les attaques ciblant l'hôte, la plateforme de conteneurs (Docker®), l'outil d'orchestration (Kubernetes®), les conteneurs eux-mêmes et les applications en conteneur. Avec son riche panel d'API, Workload Security protège les conteneurs via des processus et fonctions de sécurité automatisées.

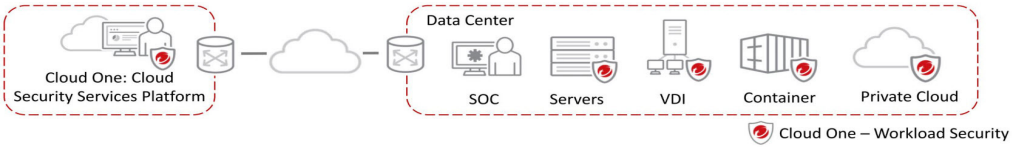
La sécurité s'intègre aux approches DevOps directement dans le pipeline CI/CD afin d'appliquer les bonnes pratiques au sein d'infrastructures en évolution. En complément de la sécurité des conteneurs, Trend Micro Cloud One™ – Container Image Security recherche et évalue les vulnérabilités, les malwares et la conformité au sein des images délivrées par vos développeurs.

Automatisation de la sécurité Cloud

Workload Security sécurise en temps réel le Cloud, avec une découverte automatisée des instances sur AWS, Microsoft® Azure® et Google Cloud™. La console de gestion de Workload Security offre une visibilité unifiée sur l'ensemble de vos serveurs et automatise la protection sur les environnements multi-Cloud, avec des règles pertinentes et contextuelles. Les scripts de déploiement et les API RESTful permettent d'intégrer la sécurité avec vos outils existants pour automatiser la protection, gérer les règles, évaluer les niveaux de sécurité, assurer un reporting de conformité, etc.

Sécurité du data center et de la virtualisation

Workload Security déploie une protection évoluée des serveurs physiques et virtualisés, pour un déploiement et une gestion simplifiés de la sécurité sur de multiples environnements, via une gestion automatique des règles. Workload Security protège les postes de travail et les serveurs virtualisés contre les malwares zero-day, les ransomwares, le cryptomining et les attaques réseau, tout en réduisant l'impact des ressources peu efficaces et du patching en urgence sur l'opérationnel.



Problématiques métiers

- **Protection automatisée**

Favorise les gains de temps et de ressources via des règles automatisées qui s'appliquent au sein des data centers et du Cloud, au fur et à mesure de la migration des nouveaux services.

- **Sécurité unifiée**

Déployez et configurez la sécurité sur vos environnements physiques, virtualisés, multi-Cloud et de conteneurs (un seul agent et une seule plateforme).

- **Sécurité du pipeline CI/CD**

Des outils adaptés au développement logiciel et des API intègrent les fonctions de sécurité dans les processus DevOps.

- **Accélérer la mise en conformité**

Assurez votre conformité réglementaire avec le RGPD, PCI DSS, HIPAA, NIST, FedRAMP, etc.

Atouts majeurs

- **Automatisation**

Security as Code permet aux équipes DevOps d'intégrer la sécurité dans le pipeline de conception et d'assurer la sortie fréquente de nouvelles versions. Avec une automatisation intégrée (découverte et déploiement notamment), des modèles prêts à l'emploi et notre Automation Center, vous sécurisez votre environnement et assurez votre conformité.

- **Flexibilité**

La sécurité porte sur votre Cloud hybride, le multi-Cloud, vos environnements multi-services, ainsi que la fourniture applicative.

- **Tout-en-un**

Une seule plateforme propose la richesse fonctionnelle et l'innovation nécessaires pour répondre à vos besoins de sécurité Cloud, aujourd'hui comme demain.

UNE SÉCURITÉ CONCUE POUR LE CLOUD

Une sécurité unifiée pour le Cloud hybride

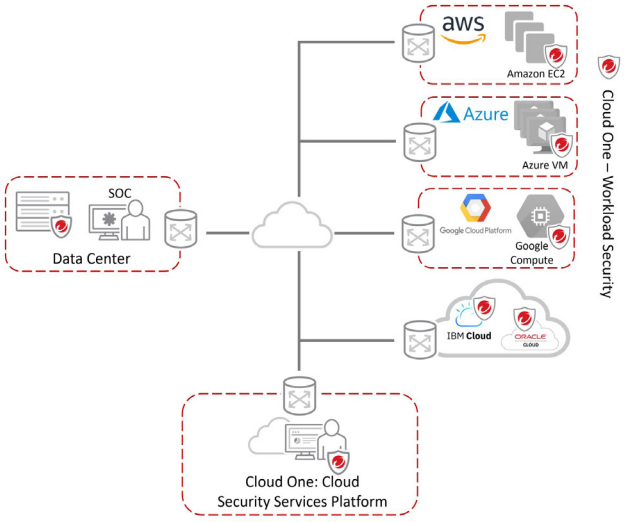
- Les connecteurs pour le Cloud et les data centers identifient les serveurs/instances de votre environnement de Cloud hybride, offrent une visibilité sur votre environnement et automatisent la gestion des règles.
- Élimine le coût lié au déploiement de plusieurs outils autonomes et favorise une sécurité intégrée sur les environnements physiques, virtualisés et Cloud (un agent logiciel, une console de gestion).
- Sécurise les différentes couches de vos environnements de conteneurs : l'hôte, la plateforme de conteneurs (Docker), la plateforme d'orchestration (Kubernetes), les conteneurs eux-mêmes ainsi que les applications hébergées en conteneur.
    - Sécurise l'hôte des conteneurs à l'aide des mêmes fonctions sophistiquées qui protègent les serveurs physiques, virtualisés et Cloud.
    - Surveille les modifications et attaques sur les plateformes Docker et Kubernetes grâce à un 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 et en inspectant le trafic entrant et sortant des conteneurs.
- Sécurise proactivement le pipeline avec l'analyse d'images (à l'étape « build » ou au sein du référentiel) qu'offre Container Image Security. Ce module complémentaire de Workload Security protège les conteneurs à chaque étape de leur cycle de vie.

Une sécurité automatisée et simplifiée

- Automatise le déploiement de la sécurité, la gestion des règles et le reporting de conformité grâce aux API REST de Workload Security.
- Réduit les coûts de gestion en automatisant les tâches de sécurité répétitives, en réduisant le nombre de faux-positifs d'alertes et via un workflow de prise en charge des incidents de sécurité.
- Simplifie le monitoring d'intégrité des fichiers grâce à une liste blanche d'événements de confiance.
- Adapte la sécurité à vos besoins, pour restreindre le nombre de personnes affectées à des tâches de sécurité spécifiques.
- Simplifie l'administration en centralisant la gestion de l'ensemble des produits Trend Micro. Un reporting centralisé sur plusieurs fonctions de sécurité est plus simple que de créer un reporting pour chacune d'entre elles.
- Connectez la sécurité avec les outils DevOps déjà en place et avec l'environnement existant, grâce à une intégration avec les principaux outils de SIEM, de gestion de la sécurité, d'orchestration, de monitoring, de pipeline et de gestion des services IT.

Une conformité à moindre coût

- Facilite la conformité aux exigences du RGPD, de PCI DSS et autres.
- Offre un reporting détaillé qui documente les attaques neutralisées et le 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 grâce à un monitoring de l'intégrité des fichiers.
- Favorise la conformité au sein du pipeline de développement grâce aux analyses des versions et du registre qu'offre Container Image Security.



Avantages clés

- **Rapidité :** sécurisez vos serveurs en quelques minutes
- **Maîtrise des coûts :** abonnement annuel et tarification à l'utilisation à partir de €0,01 / heure
- **Simplicité :** de multiples fonctions de sécurité proposées par un seul produit
- **Gain de temps :** nous gérons et mettons à jour le service à votre place
- **Sécurité éprouvée :** des milliers de clients et des millions de serveurs protégés dans le monde
- **Flexibilité :** achat & déploiement à partir des marketplaces AWS et Azure

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

Linux · Windows · SUSE · redhat · CentOS · ubuntu

La solution est compatible avec les outils de configuration, de gestion des événements et d'orchestration suivants :

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

FONCTIONS DE DÉTECTION ET DE PROTECTION

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

- ***Prévention des intrusions***

  Via des règles IPS, toute exploitation de vulnérabilités connues au sein d'applications et de systèmes d'exploitation populaires est détectée et neutralisée.

- ***Réputation web***

  Neutralise l'accès aux URL et sites web malveillants.

- ***Pare-feu***

  Un pare-feu hôte assure l'inspection stateful du trafic des serveurs.

- ***Analyse des vulnérabilités***

  Les vulnérabilités connues des systèmes d'exploitation et applications sont identifiées.

Des outils de sécurité pour verrouiller les systèmes et détecter les activités suspectes

- ***Contrôle applicatif***

  Neutralise l'installation d'exécutables et de scripts non identifiés comme sains.

- ***Inspection des logs***

  Identifie et alerte sur les changements non planifiés, les intrusions ou les attaques sophistiquées par malwares (ransomwares 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 en tant que référence de ce qu'est une configuration sécurisée. Lorsqu'un écart par rapport à cette référence est identifié, les détails sont mis en log et les personnes concernées alertées.

Prévention des malwares et des attaques ciblées

- ***Anti-Malware***

  a. File Reputation – Neutralise les fichiers malveillants à l'aide de nos signatures antimalware.

  b. Variant Protection – Recherche les variantes furtives ou polymorphes de malwares en utilisant des fragments de malwares déjà identifiés et des algorithmes de détection.

- ***Analyse comportementale***

  Examine les objets inconnus lors de leur chargement 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 qui déterminent si le fichier est malveillant.

- ***Analyse en sandbox***

  Les objets suspects peuvent être soumis pour analyse à la sandbox Trend Micro™ Deep Discovery™. Une réponse rapide est fournie à Workload Security.

AVANTAGES

Protection avancée contre les menaces

- Protège vos serveurs et applications critiques à l'aide de fonctionnalités 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.
- Détecte et neutralise l'exécution de logiciels prohibés grâce au contrôle applicatif.
- Protège les vulnérabilités connues et inconnues dans le Web, les applications d'entreprise et les systèmes d'exploitation, via un IPS.
- Détecte les menaces avancées et restaure des objets suspects et activités malveillantes, grâce à l'analyse en sandbox.
- Déclenche des alertes et une prévention proactive lorsqu'une activité malveillante est détectée.
- Sécurise les systèmes en fin de support à l'aide de patchs virtuels fournis par un IPS : vos systèmes obsolètes restent protégés.
- Protège les utilisateurs contre les sites Web infectés grâce à une veille sur les menaces issue de la base de données de réputation 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 l'infrastructure de veille sur les menaces Trend Micro™ Smart Protection Network™.

Accompagner les équipes d'intervention post incident

- Assure la prise en charge des incidents grâce à des fonctions EDR (Endpoint Detection and Response), un monitoring des indicateurs d'attaque et la neutralisation d'applications et de processus suspects.
- Workload Security s'intègre avec votre plateforme SIEM pour rechercher les menaces sophistiquées et identifier les indicateurs de compromission. Cette solution s'associe également avec des outils SOAR (orchestration, automatisation et remédiation).
- Si vous ne disposez pas du temps et des ressources nécessaires pour analyser et neutraliser les menaces, le service Managed XDR de Trend Micro vous fournit de nombreux services de sécurité sous forme managée.

CERTIFICATION POUR LES CLOUD SERVICE PROVIDERS (CSPs)

Le programme partenaires CSP de Trend Micro est un programme mondial qui valide l'interopérabilité des fournisseurs de services Cloud avec les solutions de sécurité Cloud de Trend Micro.

ARCHITECTURE ET PLATEFORMES COMPATIBLES

Workload Security est une plateforme SaaS hébergée et pilotée par Trend Micro. Nous gérons les mises à jour du kernel et du produit, nous installons la base de données de sécurité et nous en assurons la maintenance. Nous administrons la plateforme de gestion. Nos offres de sécurité fournies à partir du Cloud accélèrent et simplifient les opérations de sécurité des instances Cloud.

Agent Workload 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 des opérations comme Chef, Puppet®, Ansible, Microsoft SCCM et AWS OpsWorks).

- Trend Micro se rend compatible à de nouveaux systèmes d'exploitation et versions. Merci de consulter l'URL suivante pour connaître toutes les plateformes compatibles, dont Microsoft® Windows®, Linux®, Solaris™, AIX et les conteneurs Docker :

https://help.deepsecurity.trendmicro.com/Manage-Components/Software-Updates/compatibility.html

NOTE : pour l'installation logicielle, merci de vous référer au logiciel Trend Micro™ Deep Security™ qui propose des fonctionnalités similaires et qu'il est possible d'installer et de gérer dans votre propre data center ou environnement Cloud.

Une tarification flexible et adaptée à vos besoins

Tarification SaaS à l'utilisation :

TYPE D'INSTANCE EC2 D'AWS	MACHINE VIRTUELLE MICROSOFT AZURE	TARIF HORAIRE
Micro, small, medium	1 cœur : A0, A1, D1	€ 0,01
Large	2 cœurs : A2, D2, D11, G1	€ 0,03
XLarge et au-delà	4 cœurs et plus : A3-A11, D3-D4, D12-D14, G2-G5, D3, D4, D12-D14, G2-G5	€ 0,06

Workload Security fait partie de Trend Micro Cloud One™, une plateforme proposant également les services suivants :

- **Trend Micro Cloud One™ – Container Image Security :**
  Scan des images au sein de votre pipeline
- **Trend Micro Cloud One™ – File Storage Security :**
  Sécurité de vos fichiers Cloud et de vos services de stockage d'objets
- **Trend Micro Cloud One™ – Application Security :**
  Sécurité des fonctions serverless, des API et des applications
- **Trend Micro Cloud One™ – Network Security :**
  Sécurité et IPS des réseaux Cloud
- **Trend Micro Cloud One™ – Conformity :**
  Gestion du niveau de conformité et de sécurité du Cloud

ZERO DAY INITIATIVE

Trend Micro ZDI a détecté 1449 vulnérabilités en 2018, pour une disponibilité ultra-rapide des patchs virtuels.

Une sécurité optimisée par la recherche

Nos 15 centres de recherche mondiaux et nos 450 chercheurs collaborent ensemble pour offrir une visibilité sur l'ensemble de la surface d'attaque. Grâce à nos équipes dédiées aux applications Cloud et Cloud-native, nous renforçons nos produits et maîtrisons les menaces actuelles et à venir.

Périmètre

Nous analysons et identifions en permanence de nouveaux malwares, ransomwares, URL malveillantes, serveurs C&C (Command & Control) et domaines susceptibles d'être utilisés lors d'attaques.

Grâce au projet Zero Day initiative™, le tout premier programme mondial de récompense à l'identification de bugs, nous divulguons de nouvelles vulnérabilités affectant de très nombreuses plateformes.

Certifications, conformité et alliances

- AWS Advanced Technology Partner
- AWS Container Competency Partner
- ISO 27001
- PCI DSS
- RGPD
- HP Business Partnership
- Microsoft Application Development Gold Partner
- Microsoft Certified Partnership
- Virtualization by VMware
- VMware Cloud on AWS Partner
- VMware Global Partner of the Year

TREND MICRO™

Securing Your Connected World