Trend Micro™

APEX ONE™

Une sécurité automatisée, pertinente et intégrale des Endpoints, proposée par un leader de confiance

La protection contre les menaces a longtemps été plutôt binaire et simple : il s'agissait de séparer le bon grain de l'ivraie. Il est, aujourd'hui, bien plus difficile de faire ce distinguo et les antivirus traditionnels, basés seulement sur des signatures, ne sont plus la panacée contre les menaces inconnues qui parviennent à s'immiscer au sein du réseau. Les technologies de nouvelle génération aident à contrer certaines menaces mais restent inefficaces face à d'autres, tandis qu'installer plusieurs anti-malware sur un Endpoint n'assure en rien qu'ils collaboreront entre eux. Pour rendre les choses plus complexes, vos utilisateurs sont toujours plus nombreux à accéder aux ressources corporate ou services Cloud, à partir de lieux et de dispositifs différents. Vous avez donc besoin d'une sécurité Endpoint qui soit intelligente, optimisée et interconnectée, proposée par un fournisseur de confiance.

Trend Micro™ Apex One™ capitalise sur un panel de techniques de protection évoluées pour pallier les carences de sécurité issues des activités des utilisateurs et sur les Endpoints. La solution apprend et s'adapte en permanence. Elle partage automatiquement des informations de veille sur les menaces sur l'ensemble du périmètre protégé.

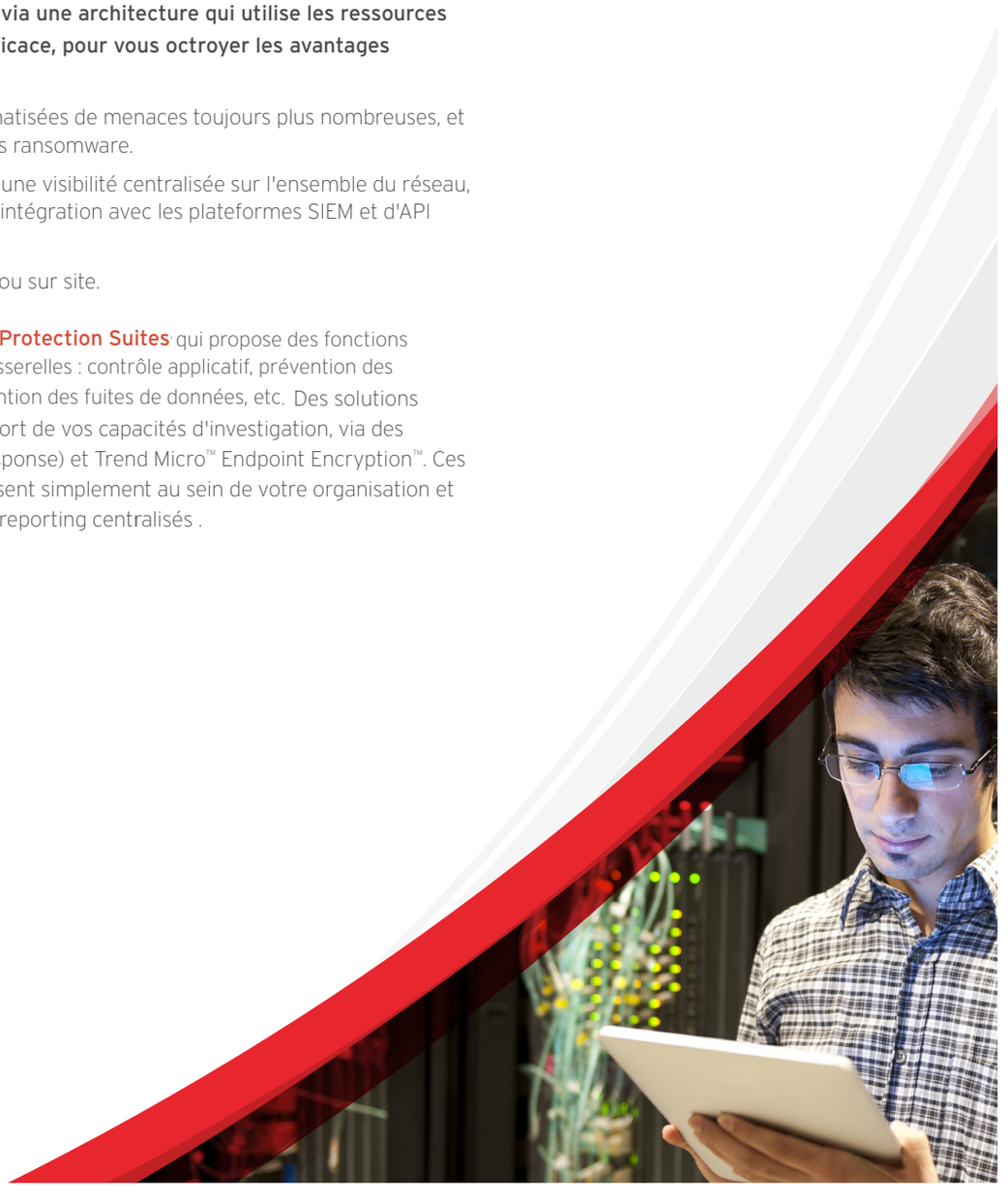
Ce panel de fonctions de sécurité est fourni via une architecture qui utilise les ressources CPU et réseau des Endpoints de manière efficace, pour vous octroyer les avantages suivants :

- Une détection et une prise en charge automatisées de menaces toujours plus nombreuses, et notamment des malware sans fichiers et des ransomware.
- Des fonctions d'investigation pertinentes et une visibilité centralisée sur l'ensemble du réseau, à l'aide d'outils EDR et MDR robustes, d'une intégration avec les plateformes SIEM et d'API ouvertes.
- Un seul agent qui se déploie en mode SaaS ou sur site.

Apex One™ est un des piliers de notre offre **Smart Protection Suites** qui propose des fonctions intégrées de protection des Endpoints et des passerelles : contrôle applicatif, prévention des intrusions (protection des vulnérabilités), prévention des fuites de données, etc. Des solutions Trend Micro supplémentaires viennent au renfort de vos capacités d'investigation, via des fonctionnalités EDR (Endpoint Detection & Response) et Trend Micro™ Endpoint Encryption™. Ces différentes technologies avant-gardistes s'utilisent simplement au sein de votre organisation et offrent une visibilité, une administration et un reporting centralisés .

Périmètre de protection

- Endpoints physiques
- Endpoints virtualisés (add-on)
- PC et serveurs sous Windows
- Équipements Mac
- Terminaux de point de vente et distributeurs bancaires



SAISISSEZ TOUS VOS AVANTAGES

- **Protection évoluée contre les malware et ransomware :** protège les Endpoints - sur et hors du réseau - contre les malware, les chevaux de Troie, les vers, les spyware et les ransomware : vous êtes protégés contre les nouvelles variantes inconnues de malware et les menaces évoluées (malware de chiffrement, malware sans fichier).
- **Détection et de remédiation :** Apex One™ intègre toutes les fonctions évoluées de détection et de remédiation nécessaires. Notre outil d'investigation Trend Micro Endpoint Sensor et notre service managé MDR (Managed Detection Response) sont proposés en option.
- **Un Virtual Patching particulièrement efficace :** Apex One™ Vulnerability Protection™ applique des patchs virtuels aux vulnérabilités connues et inconnues, vous protégeant ainsi en temps réel, même en l'absence de patch officiel.
- **Une ligne de défense interconnectée :** Apex One™ s'intègre avec d'autres produits de sécurité en local sur votre réseau et avec le service de veille mondiale sur les menaces de Trend Micro, pour mettre à jour rapidement les Endpoints dès la détection d'une nouvelle menace. La protection est active plus rapidement ce qui contre la propagation des malware.
- **Visibilité et contrôle centralisées :** lorsque déployé avec Trend Micro™ Apex Central™, de nombreuses fonctionnalités peuvent être gérées via une console unique pour offrir une visibilité et un contrôle centralisés sur l'ensemble des fonctions.
- **Intégration de la sécurité mobile :** intégrez Trend Micro™ Mobile Security™ et Apex One™ à l'aide d'Apex Central™ pour centraliser la gestion de la sécurité et le déploiement de règles sur l'ensemble des Endpoints. Mobile Security assure la protection des dispositifs mobiles contre les menaces, la gestion des applications mobiles, la gestion des flottes mobiles et la protection des données.
- **Disponible sur site ou sous forme de service :** Apex One™ se déploie sur site au sein de votre réseau ou est disponible en tant que service. Les fonctionnalités proposées sont strictement les mêmes dans les deux options.

PROBLÉMATIQUES MÉTIERS

* Les malware et ransomware sont trop nombreux à s'immiscer et les menaces avancées contournent les techniques sensées les détecter en phase de pré-éxécution
* Une solution s'impose pour se protéger des menaces connues et inconnues sur les PC et Mac
* Des difficultés à corréler et prioritiser toutes les alertes reçues
* Les utilisateurs demandent plus de visibilité et une approche automatisée pour contrer les menaces potentielles
* Les outils de sécurité Endpoint qui ne collaborent pas entre eux ralentissent les fonctions de sécurité et les rendent plus complexes à gérer
* Les risques liés aux télétravailleurs et au partage d'informations dans le Cloud
* Le patching rapide et complet des Endpoints est complexe, ce qui expose à des vulnérabilités

Périmètre de protection

- Endpoints physiques
- Endpoints virtualisés (add-on)
- PC et serveurs sous Windows
- Équipements Mac
- Terminaux de point de vente et distributeurs bancaires

Fonctions de détection des menaces

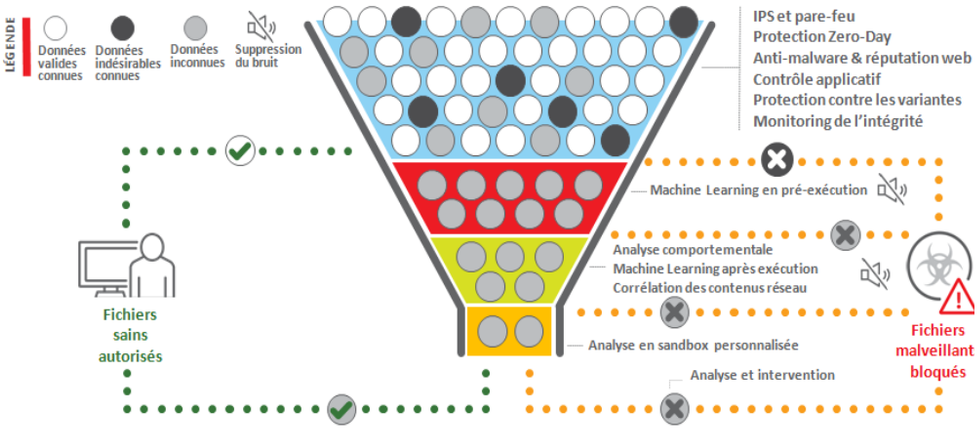
- Machine Learning de fiabilité optimale (avant et après exécution des fichiers analysés)
- Analyse comportementale (attaques par script, injection de code, ransomware, piratage des ressources mémoire, exploits du navigateur)
- Réputation de fichiers
- Protection contre les variantes
- Prévalence
- Réputation Web
- Prévention des exploits (pare-feu hôte, protection contre les exploits)
- Neutralisation des communications C&C
- Prévention des pertes de données
- Monitoring/contrôle des dispositifs
- Validation des fichiers sains
- Intégration avec une sandbox et la détection des intrusions
- Fonctions de détection et de remédiation :
- Chiffrement des Endpoints (agent distinct)
- Protection contre les vulnérabilités

Découvrez-nous en action

https://www.trendmicro.com/en_us/business/technologies/competitive-benchmarks.html

Sécurité XGen™ maximale

- Intègre un Machine Learning fiable aux autres techniques de détection, pour une protection la plus large contre les ransomware et attaques évoluées.



- Filtre les menaces, à l'aide de la technique la plus efficace, pour une détection maximale et sans faux-positifs.
- Associe des techniques sans signatures (Machine Learning haute-fidélité, analyse comportementale, protection contre les variantes, prévalence, prévention des exploits et validation des fichiers sains) avec des techniques de réputation de fichiers, de réputation web et de neutralisation des communications C&C.
- Trend Micro est le premier acteur à miser sur un Machine Learning qui analyse les fichiers en amont de leur exécution mais aussi une fois exécutés (détection plus précise).
- Des techniques de réduction de bruit (prévalence, listes blanches) permettent d'optimiser le taux de faux-positifs.
- Partage des informations relatives à des activités et fichiers suspects avec d'autres couches de sécurité pour éviter le rejeu d'une attaque déjà identifiée.
- Une protection évoluée contre les ransomware surveille les chiffrements sur les Endpoints, stoppe les activités malveillantes et assure la restauration des fichiers perdus si nécessaire.

Impact minimal

Impact réduit sur l'utilisateur et maîtrise des coûts d'administration :

- Apex One™ as a Service (proposé uniquement dans le cadre des suites Smart Protection) vous permet de déployer et de gérer Apex One™ à partir du Cloud et d'offrir les exactes mêmes fonctionnalités que celles d'une version sur site.
- L'agent logiciel, léger et optimal, active la technique de détection la plus appropriée, au moment le plus opportun, pour minimiser l'impact sur les équipements et réseaux.
- Une visibilité centralisée et totale sur le statut des Endpoints permet d'identifier les risques de sécurité.
- Le partage automatique des données de veille sur les menaces avec l'ensemble des couches de sécurité neutralise les menaces émergentes sur l'ensemble de l'entreprise.
- Assure la sécurité et la conformité hors site, grâce à un relais en périphérie (Edge relay) qui fait le lien entre les collaborateurs hors du réseau et Apex One™, et ce, sans VPN.
- Des tableaux de bord personnalisables répondent à différents besoins d'administration
- Un support en 24/7 permet à Trend Micro de traiter tout incident dès son apparition.

Un partenaire et expert de la sécurité

Trend Micro est connu et reconnu pour son innovation et l'efficacité de ses technologies de sécurité. Notre ambition est de continuer à concevoir les technologies nécessaires pour lutter contre les menaces actuelles et à venir.

- 30 années d'innovation dans la sécurité.
- Plus de 155 millions d'Endpoints protégés.
- 45 des 50 plus grandes entreprises mondiales sont clientes de Trend Micro.
- Trend Micro compte parmi les trois Leaders du Magic Quadrant for Endpoint Protection Platforms 2018 de Gartner, sur un panel de 21 constructeurs évalués.

POWERED BY XGen™ SECURITY

La solution Trend Micro User Protection est optimisé par XGen™, une approche intelligente, optimisée et interconnectée à la sécurité

> “Avec un réseau comme le nôtre qui couvre l'ensemble du pays, la possibilité de sécuriser les dispositifs mobiles et fixes à partir d'une seule plateforme simplifie la sécurité de notre réseau et améliore la productivité de notre équipe.”

Greg Bell,
IT director, DCI Donor Services

PERSONNALISEZ LA SÉCURITÉ DE VOS ENDPOINTS

Avec Apex One™, vous bénéficiez de fonctions de sécurité et d'investigation supplémentaires afin de renforcer la sécurité de vos Endpoints. Choisissez parmi les fonctions avancées ci-après pour répondre à vos besoins spécifiques.

VULNERABILITY PROTECTION

Adossée à des travaux de recherche sur les vulnérabilités, la fonction de Virtual Patching d'Apex One™ déploie une protection actualisée contre les vulnérabilités pour sécuriser les Endpoints, et notamment les équipements des points de vente, les objets connectés et les systèmes d'exploitation en fin de support.

Neutralisez les menaces Zero-Day sur vos Endpoints présents sur ou hors du réseau.

Trend Micro™ Vulnerability Protection, associé aux multiples fonctions de protection pour Endpoints de Trend Micro étend la protection aux plateformes critiques, et notamment celles en fin de support.

Défense contre les menaces sophistiquées

- Restaure les vulnérabilités connues et inconnues, même avant de déployer les patchs officiels.
- Protège les systèmes d'exploitation hérités et en fin de support, qui ne bénéficient plus de patchs.
- Analyse puis recommande automatiquement les patchs virtuels à déployer sur votre environnement spécifique.
- Module automatiquement les paramètres de sécurité selon la localisation d'un Endpoint.
- Protège les Endpoints avec un minimum d'impact sur les performances réseau et la productivité des utilisateurs.
- Neutralise le trafic réseau indésirable vers les postes clients.
- Protège les systèmes hébergeant les données sensibles pour encourager la conformité réglementaire.

Exfiltre les données indésirables du trafic critique

- Applique des filtres de contrôle pour neutraliser des types spécifiques de trafic (messagerie instantanée, streaming média...).
- Utilise une inspection de type DPI pour identifier les contenus pouvant porter préjudice à la couche applicative.
- Filtre le trafic prohibé et autorise le trafic légitime grâce à une inspection stateful.

Offre une protection proactive

- Assure une protection en amont du déploiement de patch, et souvent avant même leur disponibilité.
- Protège les systèmes d'exploitation et les applications communes contre les attaques connues et inconnues.
- Détecte le trafic malveillant qui se rend furtif en utilisant des protocoles légitimes, sur des ports non standards.
- Neutralise le trafic susceptible d'endommager les composants à risque grâce à une inspection des vulnérabilités sur le réseau.
- Neutralise les backdoors sur les réseaux corporate.
- Neutralise les exploits connus grâce à des signatures permettant la prévention des intrusions.
- Protège les applications personnalisées et existantes, à l'aide de filtres spécifiques et paramétrables par l'utilisateur.

Déploiement et administration dans le cadre de votre infrastructure existante

- Facilite la mise en place d'un contrôle granulaire grâce à un tableau de bord simplifié et à une visibilité orientée utilisateur, à partir de la console de gestion.
- Exécute les analyses de vulnérabilité sur la base des identifiants des bulletins de sécurité de Microsoft, des identifiants CVE et d'autres informations importantes.
- Assure une intégration avec les principales plateformes SIEM.
- Simplifie le déploiement et l'administration en utilisant l'agent unique Apex One™, avec visibilité et contrôle centralisés.

Logiciel

Périmètre de protection

- Endpoints

Protection contre les menaces

- Exploitation des vulnérabilités
- Attaque de déni de service
- Trafic réseau prohibé
- Menaces web

Fonctions et avantages

- Maîtrise les conséquences d'une absence de patch
- Rallonge la durée d'exploitation des systèmes d'exploitation en fin de support
- Accélère les restaurations grâce à une protection par incrément contre les attaques Zero-Day
- Permet de mener votre patching à votre propre rythme
- Maîtrise les risques réglementaires en améliorant la conformité en matière de sécurité des données
- Améliore la protection par pare-feu des postes clients distants et mobiles

ENDPOINT APPLICATION CONTROL

Trend Micro Apex One™ Application Control™ renforce vos défenses contre les malware et les attaques ciblées, en bloquant l'exécution d'applications indésirables et inconnues sur les Endpoints de votre entreprise. Des règles, listes blanches et listes noires souples et faciles à gérer s'associent à une base de données d'applications pour offrir une solution conviviale qui maîtrise l'exposition de vos Endpoints aux attaques. Pour davantage de visibilité sur les menaces, la visibilité et la gestion des règles centralisées sont proposées par Apex Central™. Apex Central™ étend la visibilité et le contrôle sur l'ensemble des environnements : sur site, Cloud et hybride. Accédez à une veille décisionnelle sur les menaces grâce à une sandbox en local ou depuis Trend Micro Smart Protection Network qui offre cette veille en temps réel, à partir du Cloud, pour neutraliser les menaces de manière protacive.

FONCTIONS ET AVANTAGES

Une protection renforcée contre les malware, les attaques ciblées et les menaces Zero-Day.

- Prévient les dommages potentiels d'applications indésirables (exécutables, dll, applications de la boutique Windows Apps, pilotes de périphérique, panneaux de configuration et autres fichiers exécutables PE).
- Fournit des données de veille en temps réel sur la réputation de fichiers, ces données étant corrélées à l'échelle mondiale.
- Interagit avec des couches de sécurité supplémentaires pour une meilleure corrélation des données sur les menaces, ce qui permet de bloquer les attaques en plus grand nombre et de manière récurrente.
- Tire parti de données applicatives analysées et corrélées, issues de plus de d'un milliard d'enregistrements de fichiers sains (Trend Micro Smart Protection Network).
- Vient au renfort d'outils de sécurité tels que les antivirus, les systèmes hôtes de prévention d'intrusion, les outils de prévention des pertes de données et les outils de protection mobile.

Une gestion simplifiée pour une protection plus rapide

- Facilite la mise en place d'un contrôle granulaire grâce à un tableau de bord et une console de gestion personnalisés.
- Capitalise sur des règles dynamiques et intelligentes, qui permettent aux utilisateurs d'installer des applications dont l'innocuité est validée sur la base d'indicateurs de réputation : prévalence, niveau d'utilisation à l'échelle régionale et maturité de l'application.
- Offre davantage de visibilité sur les infections en cours grâce à une visibilité orientée utilisateur, une gestion des règles et une agrégation des logs. Assure un reporting sur les différentes couches de sécurité des solutions de Trend Micro via Apex Central™.
- Catégorise les applications et offre des mises à jour régulières pour simplifier l'administration grâce à Certified Safe Software Service de Trend Micro.

Les listes blanches et noires neutralisent les applications inconnues et indésirables

- Utilise le nom, le chemin, une expression régulière ou le certificat d'une application pour sa mise en liste noire ou blanche.
- Propose des catégories d'applications et permet de sélectionner ces applications à partir du catalogue des applications de Trend Micro, régulièrement mis à jour.
- S'assure d'installer des patchs et mises à jour pour les applications en liste blanche, et permet à vos programmes de mise à jour d'installer des patchs et mises à jour légitimes.
- Autorise la création de vos propres listes blanches et noires en interne.
- Propose de nombreuses données sur la réputation des applications et des fichiers.

La conformité aux règles IT internes limite les risques juridiques et financiers.

- Restreint l'utilisation d'applications à une liste spécifique d'applications prises en charge par les produits de prévention des pertes de données (DLP) pour des utilisateurs ou Endpoints spécifiques.
- Identifie et limite l'utilisation des applications selon les clauses des contrats de licence.
- Offre un verrouillage permettant de sécuriser les systèmes des utilisateurs en évitant l'exécution de nouvelles applications.

> “Mon premier objectif ? Ne plus subir la lourde charge sur nos systèmes liée à notre outil de sécurité Endpoint précédent. Et mon second objectif est de disposer d'une sécurité qui fonctionne réellement. Depuis que nous avons remplacé notre précédente solution, nous constatons que Trend Micro a su neutraliser les infections.”

Bruce Jamieson,
Network Systems Manager
A&W Food Services of Canada

DATA LOSS PREVENTION (DLP)

Trend Micro™ Apex One™ Data Loss Prevention™ (DLP) offre une sécurité des données qui intègre directement la fonction DLP dans votre solution existante de sécurité des Endpoints. Bénéficiez d'une visibilité et d'un contrôle sur vos données sensibles et surveillez les possibles vecteurs de fuite de données : clé USB, email, applications SaaS, Web, dispositifs mobiles ou stockage dans le Cloud. Tirez parti de modèles en langue locale pour simplifier les déploiements et vous conformer aux recommandations et réglementations locales. Apex One™ DLP™ vous permet de déployer une sécurité des données à un tarif bien plus économique que les outils traditionnels de DLP.

FONCTIONS ET AVANTAGES

Renforce la protection et le contrôle sur les données

- Permet aux équipes IT d'encadrer l'utilisation des clés USB, des dispositifs nomades connectés via USB, des lecteurs de CD/DVD, du stockage dans le Cloud et d'autres dispositifs amovibles, avec un contrôle granulaire sur les équipements et des règles de DLP.
- Favorise un stockage dans le Cloud avec une application des règles de DLP pour le chiffrement des fichiers, et pour les applications SaaS (Microsoft® Office 365®).
- Détecte une utilisation suspecte de données, sur la base de mots clés, d'expressions régulières et d'attributs de fichiers.
- Sensibilise les collaborateurs aux règles d'utilisation des données au travers d'alertes, d'un reporting ou de prévention de certaines activités à risque.

Favorise la mise en conformité

- Simplifie la conformité réglementaire grâce à des modèles de conformité prêts à l'emploi.
- Accélère les audits grâce au recueil de données post-incident et à un reporting en temps réel.
- Offre des modèles pour assurer la conformité à des réglementations et pour aider les clients à respecter les exigences que leur impose le RGPD, PCI/DSS, HIPAA, GLBA, SB-1386 et US PII.

Administration simplifiée, coûts maîtrisés

- Renforce la visibilité et le contrôle, grâce à une solution intégrée et gérée de manière centralisée.
- Réduit les besoins en ressources et l'impact sur les performances : un seul agent consolidé assure la sécurité des Endpoints, le contrôle des dispositifs et la prévention des fuites de données.

Visibilité et contrôle centralisés

- Trend Micro™ Apex Central™ s'accompagne d'une console de gestion centralisée et pratique, qui consolide les règles, les événements et le reporting sur de multiples solutions de DLP.

Protégez vos données stockées, utilisées ou en transit

- Protection des données stockées : reconnaît et traite plus de 300 types de fichiers associés à des applications email et de bureautique, langages de programmation, images, fichiers d'ingénierie et fichiers compressés et archivés. Les Endpoints, les serveurs de fichiers, les archives d'email, le référentiel Microsoft© SharePoint© Portal Server, les applications SaaS et les espaces Cloud de stockage, sont analysés pour identifier les données confidentielles.
- Protection des données en transit : offre visibilité et contrôle sur vos données en transit (email, webmail, message instantané, applications SaaS, etc.) sur la majorité des protocoles réseau tels que FTP, HTTP/HTTPS et SMTP.
- Protection des données utilisées : offre visibilité et contrôle sur les données utilisées au niveau des ports USB, des CD, des DVD, des ports COM et LPT, des disques durs amovibles, des équipements d'imagerie et à infrarouge, des bus PCMCIA et des modems. La solution peut également surveiller les opérations de copier-coller et de copie d'écran.

Visibilité précise sur les données à l'aide d'identifiants

- En complément des modèles, Apex One™ DLP™ propose une liste précise d'identifiants internationaux pour repérer des données spécifiques selon leur structure, des formules ou leur position, etc. Ces identifiants peuvent également être créés individuellement.

Avantages d'Apex One™ DLP™

Périmètre de protection

- Protège vos données, dès aujourd'hui
- Déployez une fonction DLP et obtenez visibilité et contrôle sur vos données

Maîtrisez vos coûts de DLP

- Allégez votre facture de déploiement et de maintenance par rapport aux outils traditionnels de DLP

Protégez votre confidentialité

- Identifiez, surveillez et prévenez les pertes de données, sur et hors de votre réseau
- Assurez votre conformité réglementaire
- Mettez en œuvre des fonctions de protection, de visibilité et d'application des règles de sécurité

Sensibilisez vos utilisateurs

- Alertez les collaborateurs présentant un comportement à risque et appliquez un contrôle sur les utilisateurs si nécessaire.

ENDPOINT SENSOR

Propose des fonctions d'expertise et de reporting post-incident sur les Endpoints, grâce à l'enregistrement et au reporting sur les activités systèmes, pour permettre aux analystes d'évaluer la nature et l'étendue d'une attaque. Les fonctions personnalisées de détection, de veille et de contrôle de Deep Discovery vous permettent de :

- Enregistrer les activités système de manière détaillée
- Réaliser une recherche à des niveaux multiples sur l'ensemble des Endpoints à l'aide de différents critères de recherche : OpenIOC, Yara et objets suspects.
- Détecter et analyser des indicateurs évolués sur les menaces, comme les attaques basées sur des malware sans fichiers.
- Réagir rapidement avant toute perte de données sensibles.

ENDPOINT ENCRYPTION

Assure la confidentialité des données grâce au chiffrement des données stockées sur vos Endpoints (PC, Mac, DVD, clé USB), ces derniers pouvant être détournés ou égarés. Trend Micro™ Endpoint Encryption, disponible en tant qu'agent distinct, offre le niveau de sécurité requis pour vos données, grâce au chiffrement complet des disques, répertoires, fichiers et médias amovibles.

- Automatise la gestion des données grâce à des disques durs à chiffrement autonome.
- Chiffre les données présentes dans des fichiers spécifiques, répertoires partagés et médias amovibles.
- Définit des règles dédiées à la gestion des données et des équipements.
- Gère Microsoft Bitlocker et FileVault

TREND MICRO APEX CENTRAL

Cette console centralisée assure une gestion cohérente de la sécurité, et offre une visibilité et un reporting complets sur les différentes couches de la sécurité interconnectée de Trend Micro. La visibilité et le contrôle portent sur tous les modèles de déploiement : sur site, Cloud et hybride. L'administration centralisée bénéficie d'une visibilité basée sur l'utilisateur pour améliorer la protection, simplifier l'infrastructure et éliminer les tâches administratives redondantes et répétitives. Apex Central™ offre également un accès à des données de veille décisionnelles proposées par Trend Micro Smart Protection Network, qui utilise cette veille temps-réel pour offrir une sécurité à partir du Cloud, capable de neutraliser les menaces en amont.

SECURITY FOR MAC

- Protège spécifiquement les clients Mac sur votre réseau, et prévient l'accès aux sites malveillants et la prolifération des malware - même si ces malware ne ciblent pas Mac OS X.
- Réduit l'exposition aux menaces Web, et notamment à la prolifération des malware ciblant les clients Mac.
- Reprend l'univers graphique et convivial de Mac OS X.
- Assure des gains en temps et de productivité grâce à une administration centralisée de tous les Endpoints, et notamment des clients Mac.

Périmètre de protection

- Endpoints
- Serveurs
- Équipements de point de vente et embarqués

Protection contre les menaces

- Exploitation des vulnérabilités
- Applications malveillantes (exécutables, fichiers dll, pilotes de périphérique, applications Windows® et autres)
- Identifiez, surveillez et prévenez les pertes de données, sur et hors de votre réseau
- Assurez votre conformité réglementaire
- Mettez en œuvre des fonctions de protection, de visibilité et d'application des règles de sécurité

Sensibilisez vos utilisateurs

- Alertez les collaborateurs présentant un comportement à risque et appliquez un contrôle sur les utilisateurs si nécessaire

CONFIGURATION REQUISE POUR L'AGENT

SYSTÈMES D'EXPLOITATION DE L'AGENT :

- Windows 7 (6.1)
- Windows 8/8.1 (6.2/6.3)
- Windows 10 (10.0)
- Windows Server 2008 R2 (6.1)
- Windows Server 2012 (6.2)
- Windows Server 2012 R2 (6.3)
- Windows Server 2016 R2 (10)
- Windows Server 2019
- macOS® Mojave 10.14
- macOS High Sierra 10.13
- macOS Sierra 10.12
- OS X® El Capitan 10.11
- OS X Yosemite 10.10 ou ultérieur
- OS X Mavericks 10.9 ou ultérieur

SPÉCIFICATIONS MATÉRIELLES POUR L'AGENT :

- Processeur : 300 MHz Intel® Pentium® ou équivalent (Windows 7, 8.1, 10) et processeur Intel® Core™ pour Mac
- 1.0 GHz minimum (2.0 GHz recommandé) Intel Pentium ou équivalent (Windows Embedded POSReady7)
- 1.4 GHz minimum (2.0 GHz recommandé) Intel Pentium ou équivalent (Windows 2008 R2, Windows 2016, Windows 2019)

Mémoire :

- 512 Mo minimum (2.0 Go recommandé) avec 100 Mo minimum alloués exclusivement à Apex One (Windows 2008/2010/2011/2012)
- 1 Go minimum (2 Go recommandé) avec 100 Mo minimum alloué exclusivement à Apex One (Windows 7 (x86), 8.1 (x86), Windows Embedded POSReady 7, 10 (x64))
- 2 Go minimum (4 Go recommandé) avec 100 Mo minimum alloués exclusivement à Apex One (Windows 7 (x64), 8,1 (x64), 10 (x64))
- 512 Mo minimum pour Apex One™ on Mac

Espace disque dur :

- 1,5 Go minimum (3 Go recommandé pour tous les produits) pour Windows, 300 Mo minimum pour Mac
- Endpoint Sensor exige 2 Go minimum pour Windows, 300 Mo for Mac

Le détail des configurations est disponible sur le site docs.trendmicro.com

TREND MICRO™

Securing Your Connected World