Trend Micro™

OFFICESCAN™

Trend Micro™ XGen™ : la sécurité des endpoints proposée par un leader de confiance

La protection contre les menaces a longtemps consisté en une approche visant à reconnaître simplement les éléments connus pour être malveillants. Il est aujourd'hui bien plus difficile de faire ce distinguo et les organisations se focalisent plus que jamais sur la sécurité de leurs endpoints, en sachant que les antivirus traditionnels, basés sur les seules signatures, ne représentent plus la solution adaptée contre les menaces inconnues qui parviennent à s'immiscer au sein du réseau. Les technologies de nouvelle génération permettent d'identifier uniquement certains types spécifiques de menaces, tandis que l'installation de plusieurs outils antimalware n'assure en rien qu'ils puissent collaborer efficacement 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 différents. Votre sécurité endpoint doit fournir une protection à dimensions multiples pour se maîtriser toutes les formes de menaces, une protection offerte par un partenaire de confiance.

Trend Micro™ OfficeScan™ avec la sécurité pour endpoints XGen™ ajoute au panel des fonctions de protection contre les menaces des technologies d'apprentissage automatique (Machine Learning) afin de détecter et d'éliminer les menaces encore inconnues. La solution apprend et s'adapte en permanence tout en partageant automatiquement des informations de veille concernant les menaces sur l'ensemble du périmètre protégé. Ce panel de fonctions de sécurité est fourni via une architecture qui utilise les ressources des endpoints et du réseau de manière efficace.

OfficeScan est une composante essentielle de notre offre **Smart Protection Suites**, qui propose davantage de fonctions de protection des endpoints et des passerelles : contrôle applicatif, prévention des intrusions (protection contre les vulnérabilités), chiffrement des endpoints, prévention des fuites de données, etc. D'autres solutions Trend Micro renforcent votre protection contre les attaques évoluées, grâce à l'analyse des endpoints et des analyses post-incident. De plus, la fonction de sandbox proposée par **Deep Discovery** se veut rapide (mise à jour des signatures en temps réel), dès qu'une menace est détectée sur un endpoint, ce qui accélère la prise en charge et la neutralisation des malware. Ces différentes technologies avant-gardistes s'utilisent simplement au sein de votre organisation et offrent une visibilité, une administration et un reporting centralisés.

TOUS LES AVANTAGES À VOTRE DISPOSITION

- **Protection évoluée contre les malware et les ransomware :** protège les endpoints, à l'intérieur et en dehors du réseau corporate, contre les malware, chevaux de Troie, spyware, vers et ransomware. La protection s'adapte aux nouvelles variantes qui émergent.
- **Défense interconnectée contre les menaces :** OfficeScan s'intègre avec d'autres produits de sécurité 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 et stoppe la propagation des malware.
- **Visibilité et contrôle centralisées :** lorsque déployés avec Trend Micro™ Control Manager™, plusieurs serveurs OfficeScan peuvent être gérés via une seule console pour offrir une visibilité totale à ses utilisateurs.
- **Sécurité mobile :** Trend Micro™ Mobile Security s'intègre avec OfficeScan via Control Manager pour centraliser la gestion de la sécurité et le déploiement des règles de sécurité 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.

Périmètre de protection

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

Protection contre les menaces

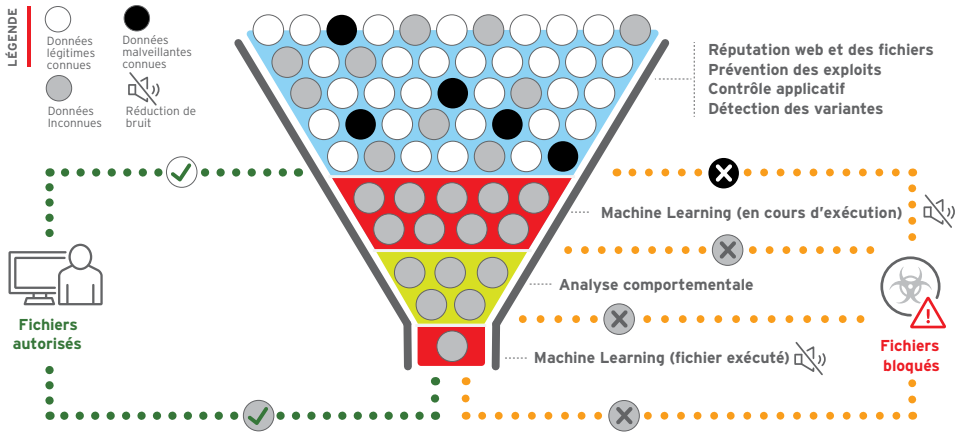
- Machine Learning de fiabilité optimale (avant et pendant l'exécution des fichiers analysés)
- Analyse comportementale (attaques par script, injection, ransomware, des ressources mémoire, du navigateur)
- Réputation de fichiers
- Protection contre les variantes
- Prévalence
- Réputation Web
- Prévention des exploits (pare-feu HIPS, protection contre les exploits)
- Neutralisation des communications C&C
- Prévention des pertes de données (module DLP)
- Monitoring/contrôle des dispositifs
- Validation des fichiers légitimes
- Sandbox et détection des intrusions

Découvrez nos résultats de test

AVANTAGES

XGen™, la sécurité optimale des endpoints

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



- Filtre les menaces, à l'aide de la technique la plus efficace : détection optimale et sans faux positifs.
- Associe des techniques sans signatures (Machine Learning fiable, 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 une technologie de Machine Learning qui analyse les fichiers en amont de leur exécution mais aussi au cours de leur exécution (détection plus efficace).
- Des techniques de réduction de bruit (prévalence, listes blanches) permettent de minimiser le taux de faux positifs.
- Le partage des informations relatives à des activités et fichiers suspects avec d'autres couches de sécurité met en échec toute ré-exécution d'une attaque déjà identifiée.
- Une protection évoluée contre les ransomware surveille les activités de chiffrement sur les endpoints, interrompt toute activité malveillante et assure la restauration des fichiers perdus si nécessaire.

Impact minimal

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

- La sécurité, légère et optimale, utilise la technique de détection la plus appropriée, au bon moment, 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 permet de se protéger contre les menaces émergentes sur l'ensemble du périmètre organisationnel.
- La sécurité et la mise en conformité sont assurées hors site, via un relais en périphérie (Edge relay) qui fait le lien entre les collaborateurs hors du réseau corporate et OfficeScan (sans VPN).
- Des tableaux de bord personnalisables répondent à tous les besoins d'administration.
- Un support 24 h/24 et 7j/7 permet à Trend Micro de traiter et résoudre 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.

- Plus de 25 années d'innovation dans la sécurité.
- Plus de 155 millions de endpoints protégés.
- 45 des 50 plus grandes entreprises mondiales sont clientes de Trend Micro.
- Depuis 14 ans, Trend Micro est référencé parmi les leaders des solutions de sécurité pour les endpoints dans le Gartner Magic Quadrant for Endpoint Protection Platforms.

Problématiques métiers

- Les malware et ransomware sont trop nombreux à s'introduire au sein du réseau
- Une solution s'impose pour se protéger des menaces connues et inconnues sur les postes PC, MAC et virtualisés
- Des outils de sécurité endpoint qui ne collaborent pas entre eux ralentissent les fonctions de sécurité et rendent leur gestion plus complexe.
- Risques liés aux télétravailleurs et au partage d'informations dans le Cloud
- Baisse de la productivité lorsque les outils de protection des données et contre les menaces évoluées ne sont pas intégrés.

> “Mon premier objectif ? Ne plus subir la lourde charge sur nos systèmes liée à notre outil de sécurité endpoint précédent. Objectif tenu avec OfficeScan ! Mon second objectif était de déployer une sécurité réellement efficace. Depuis que nous avons remplacé notre précédente solution, nous constatons que Trend Micro a su neutraliser les infections.”

Bruce Jamieson,
Responsable réseau & systèmes
A&W Food Services of Canada

PERSONNALISEZ VOTRE SÉCURITÉ ENDPOINT

Renforcez la sécurité endpoint de Trend Micro à l'aide de modules de sécurité supplémentaire :

Data Loss Prevention (DLP)

Evite les pertes/fuites de vos données sensibles et optimise la visibilité et le contrôle.

- Sécurise les données privées sur et hors du réseau, avec notamment le chiffrement de fichiers avant leur sortie du réseau.
- Empêche les fuites de données vers un espace de stockage cloud, une clé USB, des dispositifs mobiles, des connexions Bluethooth et autres médias.
- Compatible avec un large panel d'équipements, d'applications et de types de fichiers.
- Encourage la conformité grâce à une visibilité plus large et l'application des règles de sécurité.

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.

- Une exposition moindre aux menaces Web, et notamment à la prolifération des malware ciblant les Mac.
- Conforme à l'univers graphique et convivial de Mac OS X.
- Des gains de temps et de productivité grâce à une administration centralisée de tous les endpoints, et notamment des clients Mac.

Virtual Desktop Infrastructure (VDI)

Une solution unifiée pour une sécurité endpoint consolidée qui s'applique aux postes physiques et virtualisés.

- Identifie si un agent est sur un endpoint physique ou virtuel et adapte la protection et les performances à cet environnement spécifique.
- Mise en série des analyses et des mises à jour, et mise en liste blanche des images et contenus déjà analysés, pour réduire la consommation de ressources.

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 dérobés ou égarés. Trend Micro™ Endpoint Encryption offre le niveau nécessaire à la sécurité de vos données, grâce au chiffrement complet des disques, répertoires, fichiers et supports amovibles.

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

Vulnerability Protection

Neutralise les menaces zero-day sur vos postes de travail physiques et virtuels présents sur ou hors du réseau. À l'aide d'un système de prévention des intrusions sur les hôtes (HIPS), Trend Micro™ Vulnerability Protection protège contre les vulnérabilités connues et inconnues, avant même la disponibilité ou le déploiement d'un correctif (patch). Protège également les plateformes critiques utilisant des OS obsolètes comme Windows XP.

- Supprime l'exposition aux attaques grâce au Virtual Patching.
- Réduit les indisponibilités dues aux opérations de restauration et de patching réalisées dans l'urgence.
- Permet de mener votre patching à votre propre rythme.
- Identifie les vulnérabilités de sécurité avec un reporting basé sur CVE, MS-ID et le niveau de gravité.

Endpoint Application Control

Renforce vos défenses contre les malware et attaques ciblées, en bloquant l'exécution d'applications indésirables et inconnues sur les endpoints d'entreprise.

- Protège contre l'exécution de logiciels malveillants par les machines ou les utilisateurs.
- Des règles dynamiques allègent l'administration et offrent plus de flexibilité en termes d'environnements pour les utilisateurs.
- Verrouille les systèmes et ne permet d'installer que les applications autorisées.
- Corrèle des données sur les menaces à partir de milliards de fichiers pour créer et maintenir une base de données à jour d'applications validées et légitimes.

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 système, pour permettre aux analystes d'évaluer la nature et l'étendue d'une attaque. Les fonctions de détection, de veille et de contrôle de Deep Discovery vous permettent de :

- Détecter et analyser vos assaillants.
- D'adapter immédiatement la protection contre les attaques.
- De réagir rapidement avant toute perte de données sensibles.

Trend Micro™ Control Manager™

Cette console centralisée assure une gestion cohérente de la sécurité, ainsi qu'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 environnements protégés : 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. Control Manager offre également un accès à des données de veille décisionnelles proposées par Trend Micro Smart Protection Network: cette veille en temps réel permet de neutraliser les menaces de manière proactive.

SPÉCIFICATIONS SYSTÈMES - OFFICESCAN

CONFIGURATION REQUISE POUR LE SERVEUR

Systèmes d'exploitation du serveur OfficeScan :

- Windows Server 2008 (SP2) et 2008 R2 (SP2) (x64)
- Windows Storage Server 2008 (x86/x64), Storage Server 2008 R2 (SP1) (x64)
- Windows HPC Server 2008 et HPC Server 2008 R2 (x64)
- Windows MultiPoint Server 2010 (x64) et 2012 (x64)
- Windows Server 2012 et 2012 R2 (x64)
- Windows MultiPoint Server 2012 (x64)
- Windows Storage Server 2012 (x64)
- Windows Storage Server 2016 (x64)

Spécifications du serveur OfficeScan :

Processeur : 1,86 GHz Intel Core 2 Duo (2 cœurs) ou plus

Mémoire : 1 Go minimum (2 Go recommandés) avec 500 Mo minimum alloués exclusivement à OfficeScan (sur Windows 2008)

- 2Go minimum avec 500 Mo minimum alloués exclusivement à OfficeScan (sur Windows 2010/2011/2012/2016 famille)

Espace disque dur : 6,5 Go minimum, 7 Go minimum (pour une installation à distance)

Plateforme pour serveur OfficeScan Edge Relay :

Processeur : 2 GHz Intel Core 2 Duo (2 cœurs) ou plus

Mémoire : 4 Go minimum

Espace disque dur : 50 Go minimum

Système d'exploitation : Windows Server 2012 R2

Carte réseau :

1. 2 cartes réseau
   - Une pour connecter l'intranet au serveur OfficeScan
   - Une pour la connexion externe vers les agents OfficeScan distants
2. 1 carte réseau pour utiliser différents ports pour les connexions Intranet et Internet.

Base de données :

1. SQL Server 2008 R2 Express (ou ultérieur)
2. SQL Server 2008 R2 (ou ultérieur)

CONFIGURATION REQUISE POUR L'AGENT

Systèmes d'exploitation pour l'agent :

- Windows XP (SP3) (x86)
- Windows XP (SP2) (x64) (Professional Edition)
- Windows Vista (SP1/SP2) (x86/x64)
- Windows 7 (avec/sans SP1) (x86/x64)
- Windows 8 et 8.1 (x86/x64)
- Windows 10 (32-bit et 64-bit)
- Windows 10 IoT Embedded
- Windows Server 2003 (SP2) et 2003 R2 (x86/x64)
- Windows Compute Cluster Server 2003 (Actif/Passif)
- Windows Storage Server 2003 (SP2), Storage Server 2003 R2 (SP2) (x86/x64)
- Windows Server 2008 (SP2) (x86/x64) et 2008 R2 (SP1) (x64)
- Windows Storage Server 2008 (SP2) (x86/x64) et Storage Server 2008 R2 (x64)
- Windows HPC Server 2008 et HPC Server 2008 R2 (x86/x64)
- Windows Server 2008/2008 R2 (cluster de failover en actif/passif)
- Windows MultiPoint Server 2010 et 2011 (x64)
- Windows Server 2012 et 2012 R2 (x64)
- Windows Server 2012 et 2012 R2 (x64)
- Windows MultiPoint Server 2012 (x64)
- Windows Server 2012 - Clusters de failover (x64)
- Windows Storage Server 2016 (x64)
- Windows XP Embedded Standard (SP1/SP2/SP3) (x86)
- Windows Embedded Standard 2009 (x86)
- Windows Embedded POSReady 2009 (x86), Embedded POSReady 7 (x86/x64)
- Windows 7 Embedded (x86/x64) (SP1)
- Windows 8 et 8.1 Embedded (x86/x64)

Spécifications matérielles pour l'agent :

Processeur : 300 MHz Intel Pentium ou équivalent (Windows XP, 2003, 7, 8, 8.1, 10)

- 1,0 GHz minimum (2,0 GHz recommandé) Intel Pentium ou équivalent (Windows Vista, Windows Embedded POS, Windows 2008 (x86))
- 1,4 GHz minimum (2,0 GHz recommandé) Intel Pentium ou équivalent (Windows 2008 (x64), Windows 2016)

Mémoire : 256 Mo minimum (512 Go recommandé) avec 100 Mo minimum alloués exclusivement à OfficeScan (Windows XP, 2003, Windows Embedded POSready 2009)

- 512 Mo minimum (2,0 Go recommandés) avec 100 Mo minimum alloués exclusivement à OfficeScan (Windows 2008/2010/2011/2012)
- 1,0 Go minimum (1,5 Go recommandés) avec 100 Mo minimum alloués exclusivement à OfficeScan (Windows Vista)
- 1,0 Go minimum (2,0 Go recommandés) avec 100 Mo minimum alloués exclusivement à OfficeScan (Windows 7 (x86), 8 (x86), 8.1 (x86), Windows Embedded POSReady 7)
- 512 Mo minimum (2,0 Go recommandés) avec 100 Mo minimum alloués exclusivement à OfficeScan (Windows 7/8/8.1/2012)

Espace disque dur : 650 Mo minimum

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

> “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**,
> Directeur Informatique
> DCI Donor Services

TREND MICRO™

Securing Your Journey to the Cloud