Trend Micro™

OFFICESCAN™

La sécurité des endpoints assurée par le leader du marché

Le paysage des menaces était autrefois binaire, et il suffisait d'empêcher l'accès des éléments malveillants et d'autoriser celui des éléments fiables. Toutefois, la situation a changé, et il est plus difficile de faire ce distinguo. Les approches antivirus traditionnelles, basées sur la signature des programmes, ne parviennent plus à assurer une défense face aux ransomwares et menaces inconnues qui parviennent souvent à s'immiscer. Les technologies de nouvelle génération permettent d'identifier uniquement certains types bien spécifiques de menaces, et l'installation de plusieurs outils anti-malware en un seul endpoint entraîne une surcharge de produits non compatibles. Pour rendre les choses encore plus complexes, vos utilisateurs sont toujours plus nombreux à accéder à des ressources professionnelles ou services Cloud depuis une multitude d'emplacements et d'appareils. Vous avez ainsi besoin d'une protection des endpoints intelligente, optimisée et connectée, conçue par un partenaire dont la réputation n'est plus à faire.

La technologie OfficeScan™ de Trend Micro™ intègre l'apprentissage automatique de haute fidélité dans une combinaison de techniques de protection contre les menaces afin de combler les failles de sécurité à travers l'intégralité des endpoints et activités de vos utilisateurs. Celle-ci ne cesse d'apprendre, de s'adapter et partage automatiquement les renseignements sur les menaces dans votre environnement. Cette combinaison de protection contre les menaces est assurée via une architecture qui utilise les ressources des endpoints plus efficacement, pour devancer la concurrence en termes de charge du réseau et de processeur.

OfficeScan est un composant essentiel de notre **suite Smart Protection**, assurant une protection des endpoints et passerelles de connexion, à travers le contrôle des applications, la prévention des intrusions (protection des vulnérabilités), le cryptage des endpoints, la prévention de la perte de données (DLP) et bien plus encore, le tout dans une seule solution tout-en-un. Les solutions Trend Micro additionnelles renforcent votre protection face aux attaques avancées, grâce au système d'analyse et d'intervention des endpoints (EDR). D'autre part, la fonction de sandboxing réseau de Deep Discovery assure une intervention rapide sur les endpoints dès qu'une nouvelle menace est détectée localement. Avec la mise à jour en temps réel de la signature des programmes, vous bénéficiez d'une réactivité accrue et d'un contrôle des menaces à la source. Cette technologie de pointe est accessible à votre entreprise en toute simplicité, grâce à une visibilité, une gestion et une génération de rapports centralisées.

UNE SOLUTION GLOBALE

- **Protection avancée contre les ransomwares et malwares –** Protège les endpoints à l'intérieur et en dehors du réseau professionnel, contre les malwares, chevaux de Troie, vers, spywares et ransomwares, tout en s'adaptant aux nouvelles variantes qui émergent.
- **Défense connectée contre les menaces –** OfficeScan s'intègre localement avec d'autres produits de sécurité sur votre réseau et avec le service de veille mondiale sur les menaces de Trend Micro, assurant une mise à jour rapide du sandbox réseau vers les endpoints dès la détection d'une nouvelle menace. Vous bénéficiez ainsi d'une réactivité accrue et d'un contrôle des menaces à la source.
- **Administration et visibilité centralisées –** Déployés avec Trend Micro™ Control Manager™, plusieurs serveurs OfficeScan peuvent être gérés via une seule console pour offrir une visibilité à 360° des utilisateurs.
- **Intégration de Mobile Security –** Trend Micro™ Mobile Security s'intègre à OfficeScan via Control Manager pour centraliser la gestion de la sécurité et le déploiement des politiques de sécurité sur l'ensemble des endpoints. Mobile Security assure la protection des appareils mobiles contre les menaces, la gestion des applications mobiles, la gestion des appareils mobiles (MDM) et la protection des données.
- **Disponible sur site ou en tant que service –** OfficeScan peut être déployé sur site dans votre réseau, mais est également disponible en tant que service (SaaS).

Périmètre de protection

- Endpoints physiques
- Endpoints virtuels (extension)
- PC et serveurs Windows
- Ordinateurs Mac
- Terminaux de points de vente et distributeurs de billets

Protection contre les menaces

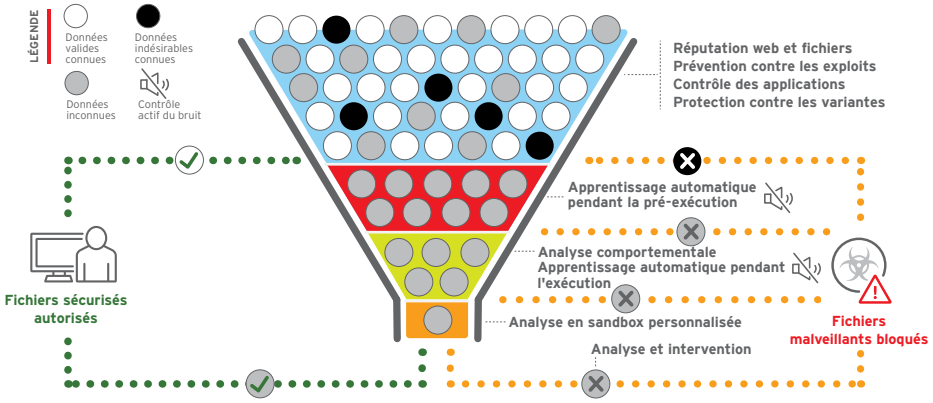
- Apprentissage automatique (avant et pendant l'exécution)
- Analyse comportementale (attaques par script, injection, ransomware, mémoire et navigateur)
- Réputation des fichiers
- Protection contre les variantes
- Vérification des recensements
- Réputation web
- Prévention des exploits (pare-feu hôte, protection contre les exploits)
- Blocage des communications C&C (Command & Control)
- Prévention de la perte de données (module DLP)
- Contrôle des appareils
- Validation des fichiers sains
- Sandbox et détection des intrusions

Découvrez nos résultats de test

AVANTAGES

Technologie de sécurité XGen™ pour une protection maximale

Intègre une technologie d'apprentissage automatique aux autres techniques de détection pour une protection plus large contre les ransomwares et attaques avancées.



- Filtre les menaces à l'aide de la technique la plus efficace pour une détection optimale sans faux positifs.
- Associe des techniques sans signature (apprentissage automatique de haute fidélité, analyse comportementale, protection contre les variantes, contrôle des recensements, prévention des exploits et validation des fichiers sains) avec des techniques de réputation des fichiers, de réputation web et de blocage des communications C&C.
- Trend Micro est le premier acteur à introduire la technologie d'apprentissage automatique de haute fidélité, qui analyse les fichiers en amont mais également au cours de leur exécution pour une détection plus efficace.
- Des techniques de réduction du bruit (recensement, listes blanches, etc.) au niveau de chaque couche permettent de minimiser le taux de faux positifs.
- Partage des informations relatives à des activités réseau et fichiers suspects avec d'autres couches de sécurité pour empêcher toute attaque ultérieure.
- Une protection avancée contre les ransomwares surveille les activités de chiffrement suspicieuses des points de terminaison, met un terme à toute activité malveillante, et assure même la restauration des fichiers perdus si nécessaire.

Impact minimal

Réduit l'impact sur les utilisateurs et les frais de gestion.

- OfficeScan en tant que service (uniquement disponible dans le cadre de la suite Smart Protection) vous permet de déployer et de gérer OfficeScan depuis notre service basé sur le Cloud, tout en offrant les mêmes fonctionnalités que l'option sur site.
- Cette solution de sécurité légère et optimisée utilise la technique de détection la plus appropriée au bon moment, pour minimiser l'impact sur les appareils et réseaux.
- Une vue d'ensemble complète de l'état des postes de travail vous permet d'avoir rapidement une visibilité sur les risques de sécurité.
- Le partage automatique des données de veille sur les menaces avec l'ensemble des couches de sécurité protège contre les menaces émergentes à travers toute l'entreprise.
- La sécurité et la mise en conformité sont assurées hors site via un serveur relais Edge, qui fait le lien entre les collaborateurs hors du réseau d'entreprise et OfficeScan sans VPN.
- Des tableaux de bord personnalisables répondent à l'ensemble des besoins d'administration.
- Une assistance 24 h/24 et 7 j/7 permet à Trend Micro d'intervenir dès qu'un problème est détecté.

Partenaire reconnu en matière de sécurité

Trend Micro est en perpétuelle recherche d'innovation, ce qui lui permet de proposer les technologies de sécurité les plus efficaces et productives du marché. Nous cherchons toujours à développer la technologie nécessaire pour lutter contre les menaces évolutives de demain.

- Plus de 25 ans d'innovation en matière de sécurité.
- Protège plus de 155 millions de points de terminaison.
- 45 des 50 plus grandes entreprises mondiales font confiance à Trend Micro.
- Trend Micro figure parmi les leaders du rapport Magic Quadrant 2017 de Gartner consacré aux plateformes de protection des points de terminaison pour sa capacité d'exécution et l'exhaustivité de sa vision.

Problématiques clés

- Trop de malwares et ransomwares parviennent à s'introduire au sein du réseau
- Une solution est nécessaire pour se protéger contre toutes les menaces connues et inconnues sur les points de terminaison PC, MAC et virtuels
- Des solutions de sécurité de points de terminaison ne communiquent pas entre elles, ralentissent le délai de protection et alourdissent la gestion
- Risques liés aux utilisateurs travaillant à distance et aux nouvelles méthodes de partage des informations via le Cloud, etc.
- Baisse de la productivité lorsque les outils de protection des données et des menaces avancées ne s'intègrent pas

« Mon premier objectif ? Alléger la charge de traitement sur nos systèmes par rapport à notre ancienne solution de sécurité des points de terminaison. Pari tenu avec OfficeScan. Mon deuxième objectif était de déployer une solution de sécurité réellement efficace. Depuis que nous avons changé de système, on constate que Trend Micro a su stopper toutes les infections. »

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

PERSONNALISEZ LA SÉCURITÉ DE VOS ENDPOINTS

Renforcez la sécurité de vos endpoints assurée par Trend Micro à l'aide de modules de sécurité supplémentaire :

Module de prévention de perte des données (DLP)

Protège vos données sensibles pour une visibilité maximale et un contrôle optimal.

- Sécurise les données privées sur le réseau ou en dehors, avec notamment le chiffrement des fichiers avant qu'ils ne quittent votre réseau
- Protège contre les fuites de données via le stockage Cloud, les clés USB ou les appareils mobiles connectés, les connexions Bluetooth et autres supports
- Couvre une large gamme d'appareils, d'applications et de types de fichiers
- Assure la conformité grâce à une visibilité plus large et l'application de règles de sécurité

Module Security for Mac

Protège spécifiquement les clients Mac sur votre réseau, et prévient l'accès aux sites malveillants et la prolifération des malwares, même si ces derniers ne ciblent pas spécifiquement les systèmes d'exploitation Mac.

- Réduit l'exposition aux menaces web, y compris aux programmes malveillants à propagation rapide ciblant les Mac
- Reprend l'interface graphique de macOS pour une expérience utilisateur intuitive
- Assure des gains de temps et de productivité grâce à la gestion centralisée de tous les endpoints, y compris les Mac

Module Virtual Desktop Infrastructure (VDI)

Permet de consolider la sécurité de vos endpoints en une seule solution pour les postes physiques et virtuels.

- Identifie si un agent est sur un endpoint physique ou virtuel, et adapte la protection et les performances à cet environnement spécifique
- Met en série les analyses et mises à jour, et crée des listes blanches des images et contenus déjà analysés pour réduire l'utilisation de ressources

Option Endpoint Encryption

Assure la confidentialité des données grâce au chiffrement des informations stockées sur vos endpoints (PC, Mac, DVD, clés USB), ces derniers pouvant facilement être volés ou perdus. L'option Endpoint Encryption de Trend Micro™ offre le niveau nécessaire à la sécurité de vos données, grâce au chiffrement intégral des disques, répertoires, fichiers et supports amovibles.

- Protège les données stockées grâce à un logiciel de chiffrement complet du disque
- Automatise la gestion des données grâce à des disques durs à chiffrement automatique
- Chiffre les données de fichiers, dossiers partagés et supports amovibles spécifiques
- Définit des règles dédiées au contrôle des appareils et à la gestion des données
- Prend en charge Microsoft Bitlocker et FileVault d'Apple

Option Vulnerability Protection

Neutralise les menaces zero-day sur vos postes de travail physiques et virtuels, sur ou en dehors du réseau. À l'aide d'un système de prévention des intrusions sur les hôtes (HIPS), l'option Vulnerability Protection de Trend Micro™ protège contre les vulnérabilités connues et inconnues avant même le déploiement d'un correctif. Cette option permet d'étendre la protection aux plateformes critiques, y compris les anciens systèmes d'exploitation tels que Windows XP.

- Élimine l'exposition aux risques liés aux failles de sécurité grâce au patching virtuel
- Réduit les indisponibilités dues aux opérations de restauration et au développement de correctifs d'urgence
- Permet l'application de correctifs selon vos propres conditions et échéances
- Identifie les vulnérabilités de sécurité avec un reporting basé sur CVE, MS-ID et le niveau de sévérité

Option Endpoint Application Control

Renforce vos défenses contre les programmes malveillants et les attaques ciblées en empêchant l'exécution d'applications indésirables et inconnues sur vos points de terminaison d'entreprise.

- Protège contre l'exécution de logiciels malveillants par les machines ou les utilisateurs
- Des règles dynamiques allègent l'impact de gestion, et offrent plus de flexibilité en termes d'environnements pour les utilisateurs
- Verrouille les systèmes pour autoriser uniquement les applications approuvées par votre entreprise
- Corrèle des données sur les menaces provenant de milliards de fichiers pour créer et maintenir une base de données à jour d'applications validées et légitimes

Option Endpoint Sensor

Assure une analyse et intervention (EDR) des endpoints adaptés au contexte, qui enregistre et rapporte les activités détaillées au niveau du système pour permettre aux spécialistes des menaces d'évaluer rapidement la nature et l'étendue d'une attaque. Les fonctions de détection, de renseignements et de contrôle vous permettent de :

- Enregistrer les activités détaillées au niveau du système
- Effectuer des recherches de plusieurs niveaux à travers différents points de terminaison, à l'aide de critères de recherche enrichis tels qu'OpenIOC, Yara et objets suspicieux
- Détecter et analyser les indicateurs de menaces avancées, tels que les attaques sans fichiers
- Intervenir rapidement face à la perte imminente de données sensibles

Module Control Manager™ de Trend Micro™

Cette console centralisée assure une gestion globale de la sécurité, ainsi qu'une visibilité et un reporting complets sur les différentes couches de la sécurité interconnectée de Trend Micro. Elle étend également la visibilité et le contrôle sur les modèles de déploiement sur site, Cloud et hybrides. La gestion centralisée combinée à une visibilité personnalisée améliore la protection, réduit la complexité et élimine les tâches redondantes et répétitives de l'administration de la sécurité. Control Manager offre également un accès à des données de veille décisionnelles proposées par Trend Micro™ Smart Protection Network™, qui s'appuie sur des données de renseignements mondiales sur les menaces afin d'assurer une sécurité en temps réel depuis le Cloud, bloquant les menaces de manière proactive.

OFFICESCAN – CONFIGURATION MINIMALE REQUISE

CONFIGURATION MINIMALE DU SERVEUR RECOMMANDÉE

Systèmes d'exploitation de serveur OfficeScan :
- Windows HPC Server 2008 et HPC Server 2008 R2 (x64)
- Windows MultiPoint Server 2010 (x64) et 2012 (x64)
- Éditions Windows Server 2012 et 2012 R2 (x64)
- Éditions Windows MultiPoint Server 2012 (x64)
- Éditions Windows Storage Server 2012 (x64)
- Éditions Windows Server 2016 (x64)

Plateforme de serveur OfficeScan :
Processeur : Processeur Intel Core 2 Duo 1,86 GHz (2 cœurs) ou supérieur
Mémoire : 1 Go minimum (2 Go recommandés) avec au minimum 500 Mo alloués exclusivement à OfficeScan (sur la gamme Windows 2008)
- 2 Go minimum avec au moins 500 Mo exclusivement alloués à OfficeScan (sur la gamme Windows 2010/2011/2012/2016)

Espace disque : 6,5 Go minimum, 7 Go minimum (en utilisant l'installation à distance)

Plateforme du serveur relais Edge d'OfficeScan :
Processeur : Processeur Intel Core 2 Duo 2 GHz (2 cœurs) ou supérieur
Mémoire : 4 Go minimum
Espace disque : 50 Go minimum
Système d'exploitation : Windows Server 2012 R2
Carte réseau :
1. 2 cartes réseau connectées
   - Une pour la connexion intranet au serveur OfficeScan
   - L'autre pour la connexion externe aux agents hors site d'OfficeScan
2. 1 configuration de carte réseau afin d'utiliser différents ports pour les connexions intranet et Internet

Base de données :
1. SQL Server 2008 R2 Express (ou supérieur)
2. SQL Server 2008 R2 (ou supérieur)

CONFIGURATION MINIMALE DE L'AGENT RECOMMANDÉE

Système d'exploitation de l'agent
- Éditions Windows XP (SP3) (x86)
- Windows XP (SP2) (x64) (Professionnel)
- Éditions Windows 7 (avec ou sans SP1) (x86/x64)
- Éditions Windows 8 et 8.1 (x86/x64)
- Windows 10 (32 bits et 64 bits)
- Windows 10 IoT Embedded
- Éditions Windows Server 2003 (SP2) et 2003 R2 (x86/x64)
- Windows Computer Cluster Server 2003 (actif/passif)
- Éditions Windows Storage Server 2003 (SP2) et Storage Server 2003 R2 (SP2) (x86/x64)
- Éditions Windows Server 2008 (SP2) (x86/x64) et 2008 R2 (SP1) (x64)
- Éditions Windows Storage Server 2008 (SP2) (x86/x64) et Storage Server 2008 R2 (x64)
- Éditions Windows HPC Server 2008 et HPC Server 2008 R2 (x86/x64)
- Windows Server 2008/2008 R2 Failover Clusters (actif/passif)
- Windows MultiPoint Server 2010 et 2011 (x64)
- Éditions Windows Server 2012 et 2012 R2 (x64)
- Éditions Windows Storage Server 2012 et 2012 R2 (x64)
- Éditions Windows MultiPoint Server 2012 (x64)
- Windows Server 2012 Failover Clusters (x64)
- Éditions Windows 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)
- Éditions Windows 8 et 8.1 Embedded (x86/x64)

Plateforme de l'agent
Processeur : Intel Pentium 300 MHz ou équivalent (gamme Windows XP, 2003, 7, 8, 8.1, 10)
- 1,0 GHz minimum (2,0 GHz recommandés) Intel Pentium ou équivalent (gamme Windows Vista, Windows Embedded POS, Windows 2008 (x86))
- 1,4 GHz minimum (2,0 GHz recommandés) Intel Pentium ou équivalent (gamme Windows 2008 (x64), Windows 2016)

Mémoire : 256 Mo minimum (512 Mo recommandés) avec au minimum 100 Mo exclusivement alloués à OfficeScan (gamme Windows XP, 2003, Windows Embedded POSready 2009)
- 512 Mo minimum (2,0 Go recommandés) avec au minimum 100 Mo exclusivement pour OfficeScan (gamme Windows 2008, 2010, 2011, 2012)
- 1,0 Go minimum (1,5 Go recommandé) avec au minimum 100 Mo exclusivement pour OfficeScan (gamme Windows Vista)
- 1,0 Go minimum (2,0 GB recommandés) avec au minimum 100 Mo exclusivement pour OfficeScan (Windows 7 (x86), 8 (x86), 8.1 (x86), gamme Windows Embedded POSReady 7)
- 1,5 Go minimum (2,0 Go recommandés) avec au moins 100 Mo alloués exclusivement à OfficeScan (gamme Windows 7 (x64), 8 (x64), 8.1 (x64))
- Espace disque : 650 Mo minimum

Espace disque : 650 Mo minimum

Configurations requises détaillées disponibles en ligne sur **docs.trendmicro.com**.

> « Avec un réseau comme le nôtre qui couvre l'ensemble du pays, la possibilité de sécuriser les appareils mobiles et fixes depuis une seule plateforme simplifie la sécurité de notre réseau et améliore la productivité de notre équipe. »
>
> **Greg Bell,**
> Directeur Informatique DCI
> Donor Services

La solution Trend Micro User Protection utilise XGen™, une sécurité intelligente, optimisée et connectée.

POWERED BY XGen™ SECURITY

TREND MICRO™

Securing Your Journey to the Cloud