

Trend Micro

Produits

Service et assistance





Pour contacter Trend Micro :

TREND MICRO France
85, avenue Albert 1er
92500 Rueil-Malmaison
France
Tél. : +33 (0) 1 76 68 65 00

www.trendmicro.com

**Trouvez un revendeur spécialisé via l'outil de recherche
de partenaires Trend Micro**
<https://partnerlocator.trendmicro.eu>



SOMMAIRE

01	L'ENTREPRISE	4
02	APERÇU DES PRODUITS.....	6
03	SUITES DE SÉCURITÉ.....	10
04	SÉCURITÉ DES TERMINAUX.....	14
05	SÉCURITÉ DE SERVEUR ET DE STOCKAGE.....	17
06	SÉCURITÉ D'ENVIRONNEMENTS DE COLLABORATION	19
07	SÉCURITÉ DE PASSERELLE	21
08	CHIFFREMENT	24
09	SÉCURITÉ DE RÉSEAU.....	26
10	SÉCURITÉ DU CLOUD	29
11	GESTION DE LA SÉCURITÉ/SÉCURITÉ HORS LIGNE	31
12	SERVICE ET ASSISTANCE.....	32
13	LIGNES DIRECTRICES SUR LA CONCESSION DE LICENCES.....	38
14	AUTRES.....	40

Notre vision

Un monde sans danger propice à l'échange d'informations numériques

Une sécurité fiable pour tous

L'utilisation d'Internet s'est banalisée dans notre société actuelle. Malheureusement, on ne peut pas en dire autant de la sécurité de cette société centrée sur Internet. Trend Micro dispose d'une longue expérience et de technologies avancées lui permettant de protéger les particuliers et les entreprises contre les menaces sur Internet liées au monde moderne.

Nous nous sommes donné pour tâche de combattre ces menaces ainsi que de continuer d'assurer la sécurité des réseaux et des connexions au niveau international.



Eva Chen
PDG et cofondatrice

Équipe dirigeante

Eva Chen

PDG et cofondatrice

Mahendra Negi

Directeur financier

Wael Mohamed

Directeur de l'exploitation

Steve Chang

Président et fondateur

Raimund Genes

Directeur de la technologie et associé
de Trend Micro Deutschland GmbH

Akihiko Omikawa

Vice-président exécutif, Directeur
général pour le Japon, Unité
commerciale des utilisateurs privés
internationaux, Unité commerciale
des services internationaux

Cotation en bourse

Bourse de Tokyo 4704

Notre mission

Grâce à des innovations de pointe, offrir la meilleure sécurité de contenu
s'intégrant facilement à l'infrastructure informatique existante

Des solutions optimales grâce à des innovations continues

En tant que leader du marché du domaine de la sécurité de contenu, Trend Micro propose des solutions pour garantir une société d'informations plus sûre. Telle est notre mission.

On assiste non seulement à des changements continus en matière de menaces, à des développements rapides dans le domaine du cloud computing et à l'utilisation croissante des dispositifs mobiles, mais aussi à des changements dans l'environnement réseau. Grâce au développement de produits et services innovants, nous œuvrons pour protéger les informations précieuses à tout moment et en tous lieux contre les menaces imprévisibles.

Le progrès nous permet de réagir vite face à cet environnement en constante mutation au moyen de solutions optimales.

L'innovation continue est notre mission.

TREND MICRO France

85, avenue Albert 1er
92500 Rueil-Malmaison
France
Tél. : +33 (0) 1 76 68 65 00

www.trendmicro.com

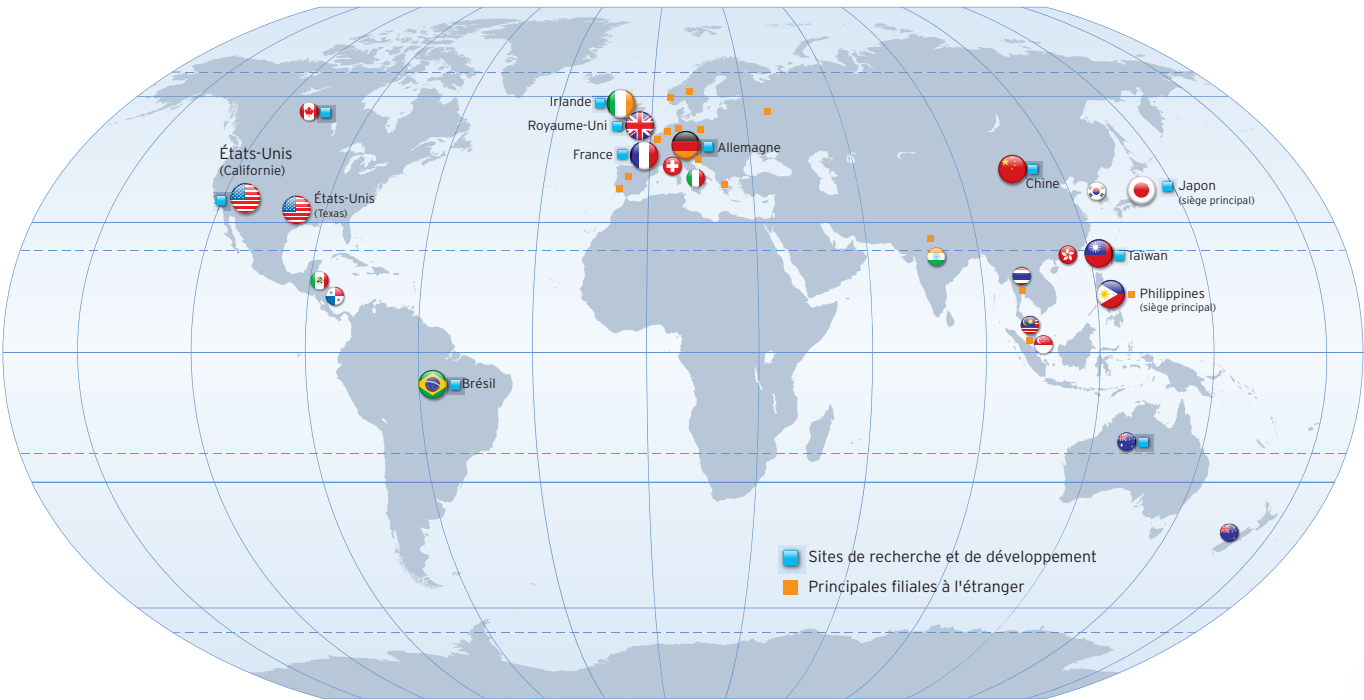
Pour une sécurité sans souci au-delà des frontières

Trend Micro réagit face aux menaces dans le monde entier à l'aide d'un réseau international dédié à l'analyse des menaces

Trend Micro est une multinationale japonaise ayant su dépasser les frontières pour devenir une entreprise transnationale.

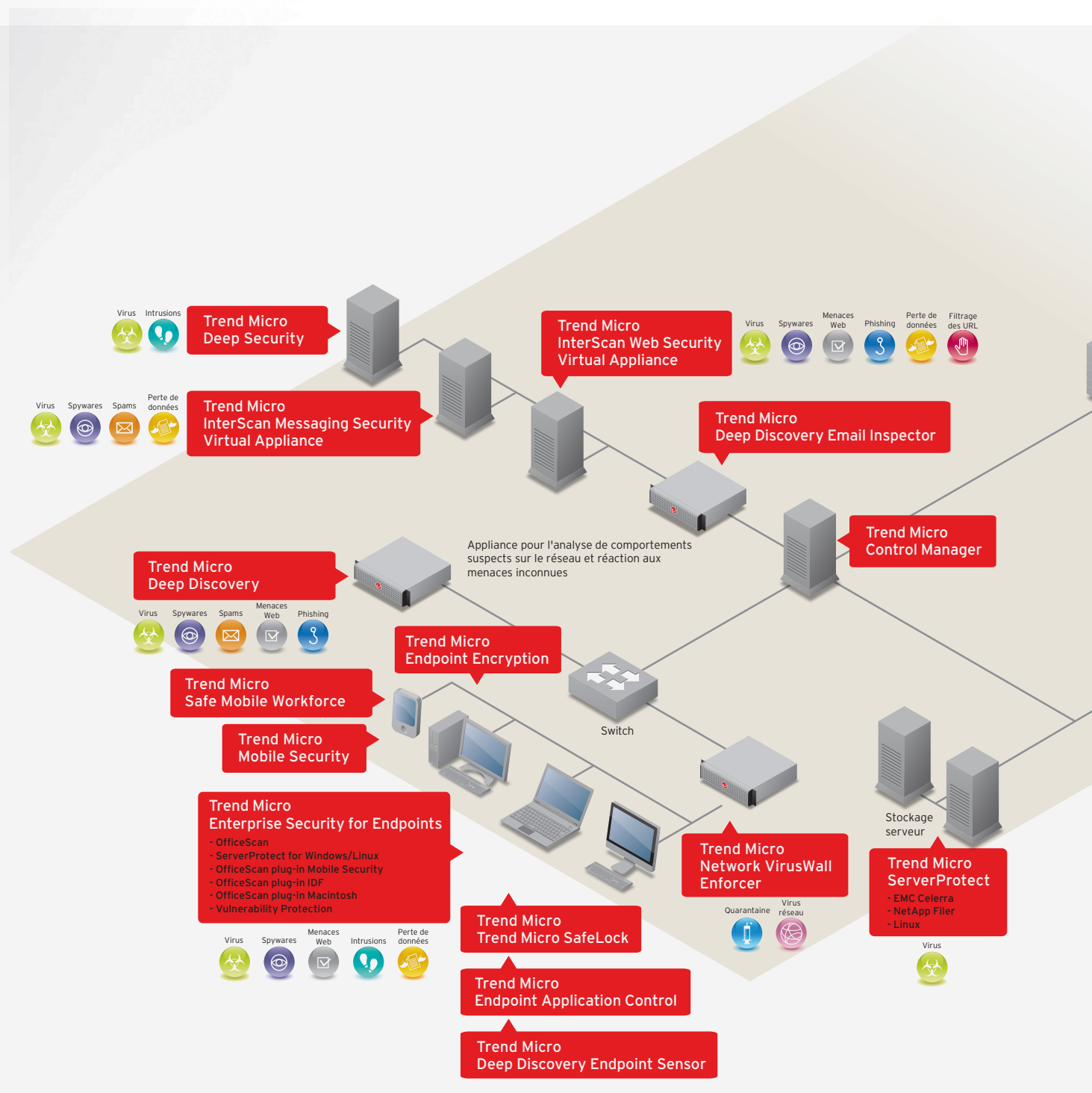
Créée en 1988 en Californie (États-Unis), l'entreprise s'est installée en 1989 au Japon. Depuis, cette multinationale dont le siège se situe à Tokyo ne cesse de se développer. Des sites présents dans le monde entier ont permis à Trend Micro de créer un réseau capable de surveiller en permanence les menaces à l'échelle internationale et régionale. Ainsi, l'entreprise met rapidement à la disposition de ses clients des solutions adaptées.

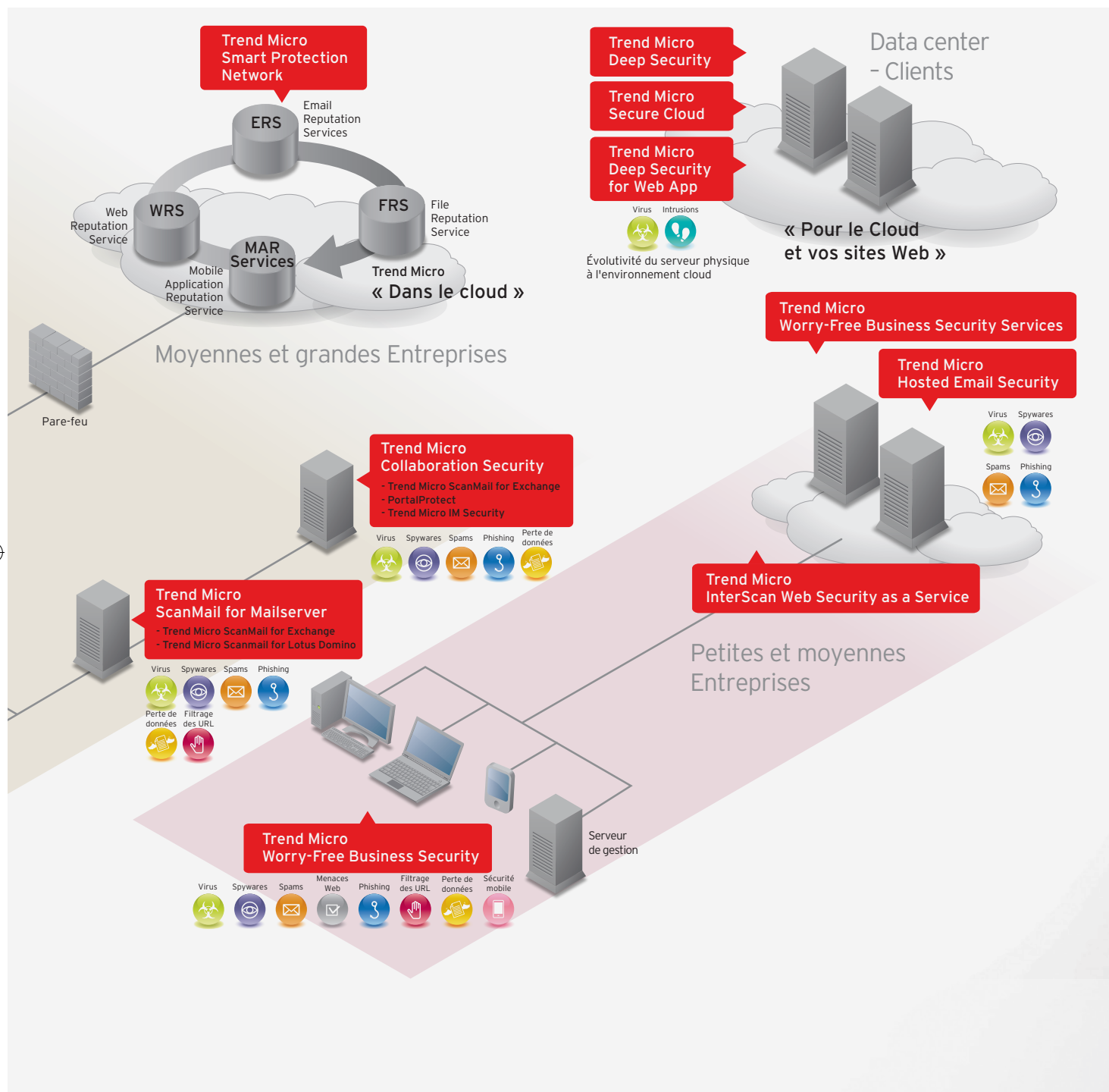
Le réseau Trend Micro dans le monde



Le TrendLabs Philippines est certifié ISO 20000-12005. Les informations sur les programmes malveillants ainsi que les services d'identification/nettoyage et l'assistance technique qu'il fournit répondent aux exigences de qualité fixées par cette norme.

Siège principal	Japon										
TrendLabs (régionaux)	Allemagne	Philippines (siège principal)	États-Unis	Japon	Taiwan	Irlande	Chine	France	Royaume-Uni	Brésil	
Sites de recherche et de développement	Japon	États-Unis	Canada	Allemagne	Royaume-Uni	Taiwan	Chine	Australie	Irlande	France	Brésil
Filiales	Allemagne	États-Unis	Irlande	Chine (Pékin)	Chine (Shanghai)	Taiwan	France				
	Suisse	Chine (Hongkong)	Inde	Corée du Sud	Italie	Royaume-Uni	Australie				
	Canada	Thaïlande	Mexique	Malaisie	Nouvelle-Zélande	Singapour	Brésil				





02

APERÇU DES PRODUITS

Performances des produits



Catégorie	Produits	Anti-virus	Réputation Web	Filtrage des URL	Anti-spam	Chiffrement	Gestion des dispositifs mobiles	Pare-feu	IDS/IPS	Surveillance de l'intégrité des fichiers	Vérification de protocoles	VDI	Contrôle des dispositifs	Protection intégrée contre la perte de données	Contrôle des applications
Sécurité des terminaux	Enterprise Security for Endpoints	●	●				●*	●	●			●	●*		
	Enterprise Security for Endpoints Light	●	●					●	●				●*		
	Smart Protection for Endpoints	●	●			●	●	●	●			●	●	●	●
	Worry-Free Business Security Advanced	●	●	●	●		●*	●					●*		
	Worry-Free Business Security Standard	●	●	●				●					●*		
	Worry-Free Business Security Services	●	●	●			●*	●					●*		
Sécurité de stockage serveur	Deep Security	●**	●**					●**	●**	●**	●	●			
	ServerProtect Windows/NetWare/Linux	●													
	ServerProtect NetApp/EMC Celerra	●													
Suites de sécurité	Enterprise Security for Endpoints and Mail Servers	●	●		●		●*	●	●			●	●*		
	Enterprise Security Suite	●	●	●	●		●*	●	●			●	●*		
	Suite Smart Protection Complete	●	●	●	●	●	●	●	●			●	●	●	●
Sécurité cloud	SecureCloud					●									
	Deep Security pour application Web	●	●						●						
Sécurité hors ligne	Portable Security	●													

* étendue de fonctions limitées

** sans agent dans les environnements VMware ESX

Catégorie	Produits	Vérification des valeurs de hachage/de certificats	Création de listes blanches/noires par catégorie	Applications spécifiques aux clients	Inventaire des applications disponibles	Mode d'évaluation	Verrouillage du système avec listes blanches	Intégration d'Active Directory
Contrôle des applications	Endpoint Application Control	●	●	●	●	●	●	●
	SafeLock		●	●	●	●	●	

Catégorie	Produits	Chiffrement de disque plein	Chiffrement de fichier/dossier	Authentification compatible réseau avant le démarrage	Gestion des clés transparente	Prise en charge de FileVault d'Apple	Prise en charge de BitLocker de Microsoft	Intégration d'Active Directory
Chiffrement	Endpoint Encryption	●	●	●	●	●	●	●



Catégorie	Produits	Antivirus	Analyse Sandbox	Réputation Web	Filtrage des URL	Anti-phishing	Antispam	Chiffrement des e-mails	Protection contre la perte de données
Sécurité d'environnements de collaboration	ScanMail for Microsoft Exchange	●		●		●	●		●
	ScanMail for IBM® Domino	●		●	●	●	●		●
	PortalProtect for Microsoft SharePoint	●		●		●			●
	IM Security for MS Lync and Office Communications Server	●		●		●			●
Sécurité de passerelles (e-mail/Internet)	InterScan Messaging Security	●		●		●	●	●	●
	InterScan Web Security	●		●	●	●			●
	Enterprise Security for Gateways	●		●	●	●	●	●	●
	Hosted Email Security	●				●	●	●	
	Deep Discovery Email Inspector	●	●	●		●			

Catégorie	Produits	Analyse Sandbox	Menaces inconnues	Menaces connues	Recherche de cybercriminels	Rapport d'analyse	Isolement de sources infectées	Quarantaine	Surveillance des comportements
Sécurité de réseau/ Analyse des menaces	Deep Discovery	●	●	●	●	●			●
	Capteur de terminaux Deep Discovery		●	●	●	●			●
	Network VirusWall Enforcer			●			●	●	

Catégorie	Produits	Antivirus	Réputation Web	Filtrage des URL	Chiffrement	Commande d'accès au dispositif	Verrouillage à distance	Suppression des données à distance	Pare-feu
Sécurité mobile	Mobile Security	●	●	●	●	●	●	●	●

Catégorie	Produits	Bring Your Own Device	Aucune donnée d'entreprise sur les terminaux mobiles	Infrastructure mobile virtuelle	iOS/Android/Windows Phone/RT	Intégration à Microsoft Exchange	Systèmes de stockage externes	Intégration d'Active Directory
Sécurité mobile	Safe Mobile Workforce	●	●	●	●	●	●	●

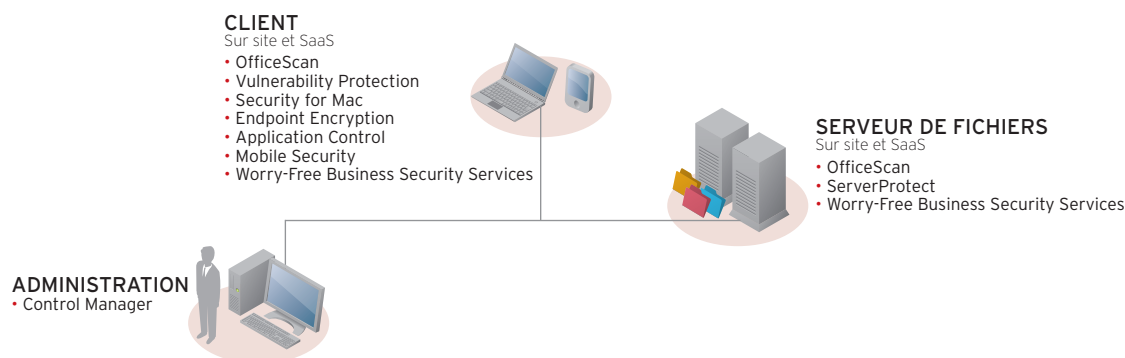
Catégorie	Produits	Lien avec mot de passe et limite de temps	Antivirus	Chiffrement	Protection contre la perte de données	Plugin Outlook	Dossier équipe	Application pour iOS/Android	Intégration d'Active Directory
Synchronisation et échange de données	SafeSync for Enterprise	●	●	●	●	●	●	●	●

Smart Protection for Endpoints

Trend Micro Smart Protection for Endpoints propose des technologies anti-programmes malveillants complètes protégeant les postes de travail virtuels et physiques contre les menaces dynamiques actuelles. Cette suite complète de sécurité des terminaux offre une protection multicouche des données contre les menaces afin de protéger vos utilisateurs et vos données d'entreprise indépendamment du type de dispositif ou de l'application. De plus, vous avez le choix entre une solution installée localement, une solution sur le cloud ou une combinaison de ces deux options. Mais le principal avantage est la possibilité d'administrer les actions des utilisateurs indépendamment du type de dispositif, du mode de transmission des menaces et du modèle d'installation, et ce, depuis un point central et transparent. Vous disposez ainsi d'un aperçu complet de la sécurité de votre environnement à tout moment.

Avantages

- **Protection complète des dispositifs mobiles, postes de travail et serveurs**
 - Cette solution rassemble le plus large éventail de technologies de sécurité des terminaux qui soit. Elle protège toutes les activités des utilisateurs et diminue ainsi le risque de perte de données confidentielles.
- **Administration centralisée et orientée utilisateurs via des solutions SaaS et sur site**
 - Grâce à la flexibilité optimale de cette suite en matière de modèles d'installation, les différentes combinaisons entre sécurité locale et sécurité basée sur le cloud, même si elles évoluent en permanence, sont prises en charge.
- **Assistance directe 24 h/24, 7 j/7**
 - Grâce à l'assistance 24 h/24, Trend Micro est en mesure d'apporter une solution immédiate à vos problèmes.



Protection complète des terminaux

PROTECTION MULTICOUCHE	PROTECTION DE LA PLATEFORME	AVANTAGE
Administration centralisée		
Control Manager	Logiciel : Windows	Gestion centrale de la sécurité
Sécurité des terminaux		
OfficeScan	Logiciels : Windows, Apple Macintosh	Protection des clients Windows et Mac physiques et virtuels
Worry-Free Business Security Services	Logiciel en tant que service (SaaS) basé sur le cloud	Protection des serveurs et postes de travail Windows, clients Mac, iOS et Android
Vulnerability Protection	Logiciel : Windows	Système de prévention d'intrusions sur l'hôte (HIPS) proactif et patching virtuel
Endpoint Application Control	Logiciel : Windows	Listes blanches et verrouillage du système
Endpoint Encryption	PC, ordinateurs portables, CD, DVD et USB	Contrôle des dispositifs, gestion des données et des clés
Server Protect	Logiciels : serveurs Windows et Linux	Protection des serveurs Windows et Linux physiques et virtuels
Sécurité mobile		
Mobile Security	iOS, Android, BlackBerry, Symbian et Windows Mobile	MDM, sécurité des données, sécurité mobile et gestion des applications
Sécurité des données intégrée		
Data Loss Prevention	Module intégré pour les terminaux, les e-mails, le travail en équipe et pour une meilleure sécurité des passerelles Internet	Application des stratégies de DLP à l'échelle de l'entreprise

Suite Smart Protection Complete

Trend Micro Smart Protection Complete est une suite composée de solutions de sécurité interconnectées et protégeant les utilisateurs en tout lieu, quelles que soient leurs activités. Cette solution de sécurité multicouche innovante offre une protection optimale des terminaux, applications et réseaux grâce à ses technologies anti-programmes malveillants complètes. En outre, vous avez la possibilité d'étendre votre protection à mesure que votre entreprise se développe en choisissant le modèle de déploiement local, basé sur le cloud ou hybride. Cette flexibilité garantit la sécurité de votre environnement informatique aujourd'hui comme demain.

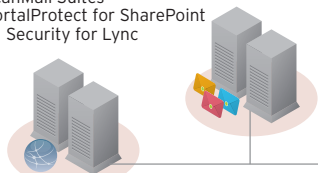
Enfin, vous pouvez administrer les utilisateurs depuis un point central et transparent, quel que soit le mode de transmission des menaces. Vous disposez ainsi d'un aperçu complet de la sécurité de votre environnement à tout moment.

Avantages

- Protection complète pour dispositifs mobiles, postes de travail, serveurs, serveurs de messagerie et de collaboration et passerelles Web et de messagerie
- Administration centralisée et orientée utilisateurs via des solutions SaaS et sur site
- Assistance directe 24 h/24, 7 j/7

SERVEUR DE MESSAGERIE ET COLLABORATION

- ScanMail Suites
- PortalProtect for SharePoint
- IM Security for Lync



CLIENT

Sur site et SaaS

- OfficeScan
- Vulnerability Protection
- Security for Mac
- Endpoint Encryption
- Application Control
- Mobile Security
- Worry-Free Business Security Services



SERVEUR DE FICHIERS

Sur site et SaaS

- OfficeScan
- ServerProtect
- Worry-Free Business Security Services



PASSERELLE

Sur site et SaaS

- InterScan Virtual Appliance
- InterScan Web Security as a Service
- Hosted Email Security



ADMINISTRATION

- Control Manager



Protection complète pour l'ensemble du réseau

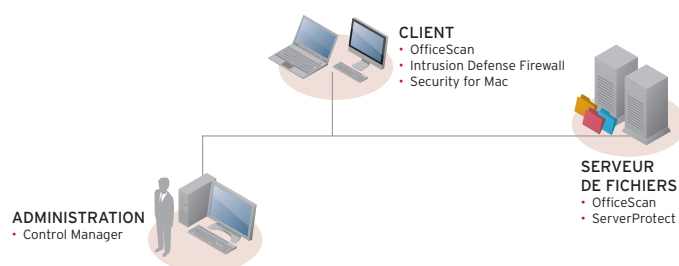
PROTECTION MULTICOUCHE	PROTECTION DE LA PLATEFORME	AVANTAGE
Administration centralisée		
Control Manager	Logiciel : Windows	Gestion centrale de la sécurité
Sécurité des terminaux		
OfficeScan	Logiciels : Windows, Apple Macintosh	Protection des clients Windows et Mac physiques et virtuels
Vulnerability Protection	Logiciel : Windows	Système de prévention d'intrusions sur l'hôte (HIPS) proactif et patching virtuel
Endpoint Application Control	Logiciel : Windows	Listes blanches et verrouillage du système
Endpoint Encryption	PC, ordinateurs portables, CD, DVD et USB	Contrôle des dispositifs, gestion des données et des clés
Server Protect	Logiciels : serveurs Windows et Linux	Protection des serveurs Windows et Linux physiques et virtuels
Worry-Free Business Security Services	Logiciel en tant que service (SaaS) basé sur le cloud	Protection des serveurs et postes de travail Windows, clients Mac, iOS et Android
Sécurité mobile		
Mobile Security	iOS, Android, BlackBerry, Symbian et Windows Mobile	MDM, sécurité des données, sécurité mobile et gestion des applications
Sécurité de messagerie et de collaboration		
InterScan Messaging Security	<ul style="list-style-type: none"> • Appliance logicielle virtuelle : VMware, Hyper-V, appliance virtuelle • Logiciels : Windows, Linux 	Protection de la passerelle de messagerie contre les spams et autres menaces par e-mail
ScanMail Suite for Microsoft Exchange	Logiciel : Windows	Blocage des spams, programmes malveillants et autres menaces par e-mail au niveau du serveur de messagerie
ScanMail Suite for Lotus Domino	<ul style="list-style-type: none"> • Logiciels : Windows, Linux pour x86, IBM AIX, IBM iS OS, Sun Solaris, Linux sur IBM® zSeries, IBM z/OS 	Blocage des spams, programmes malveillants et autres menaces par e-mail au niveau du serveur de messagerie
Hosted Email Security	SaaS basé sur le cloud	Protection actualisée en permanence contre les spams et virus avant qu'ils n'atteignent votre réseau
PortalProtect for Microsoft SharePoint	Logiciel : Windows	Protection de votre travail en équipe sur SharePoint
IM Security for Microsoft Lync	Logiciel : Windows	Protection de la messagerie instantanée
Meilleure sécurité de la passerelle Internet		
InterScan Web Security	<ul style="list-style-type: none"> • Appliance logicielle virtuelle : VMware, Hyper-V, appliance virtuelle • SaaS basé sur le cloud 	Protection de la passerelle Internet contre les menaces Internet / filtrage des URL
Sécurité des données intégrée		
Data Loss Prevention	Module intégré pour les terminaux, les e-mails, le travail en équipe et pour une meilleure sécurité des passerelles Internet	Application des stratégies de DLP à l'échelle de l'entreprise

Enterprise Security for Endpoints/Enterprise Security for Endpoints Light

Protégez vos postes de travail, ordinateurs portables, serveurs et smartphones aussi bien à l'intérieur qu'à l'extérieur du réseau grâce à l'association innovante d'anti-programmes malveillants et d'une protection basée sur le cloud de premier choix, via Trend Micro Smart Protection Network. L'évaluation de la réputation de fichiers soulage désormais les ressources des terminaux grâce à des fichiers de signatures basés sur le cloud. L'évaluation de la réputation Web, pour sa part, bloque l'accès aux sites Web malveillants.

Avantages

- Protection immédiate
- Réduction des risques commerciaux
- Sécurité complète
- Diminution des coûts informatiques
- Architecture évolutive



Aperçu

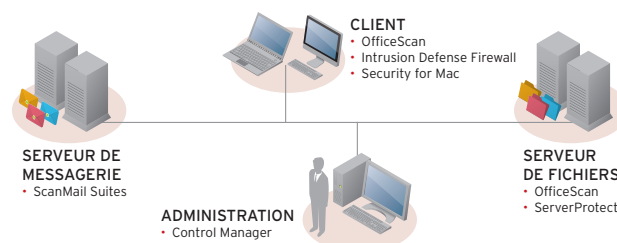
	OfficeScan	Intrusion Defense Firewall	Security for Mac	VDI	Mobile Security	ServerProtect for Windows, NetWare, Linux	Trend Micro Control Manager
Enterprise Security for Endpoints Light	●					●	Standard
Enterprise Security for Endpoints	●	●	●	●	●	●	Advanced

Enterprise Security for Endpoints and Mail Servers

Protection maximale et complexité minimale pour serveurs de messagerie et de fichiers, clients et terminaux mobiles. Protégez vos serveurs de messagerie et de fichiers, vos postes de travail et ordinateurs portables contre les virus, les spywares, les spams, le phishing, les contenus indésirables et les menaces complexes, grâce à une solution intégrée unique.

Avantages

- Optimise la protection
- Réduit les coûts
- Réduit la complexité

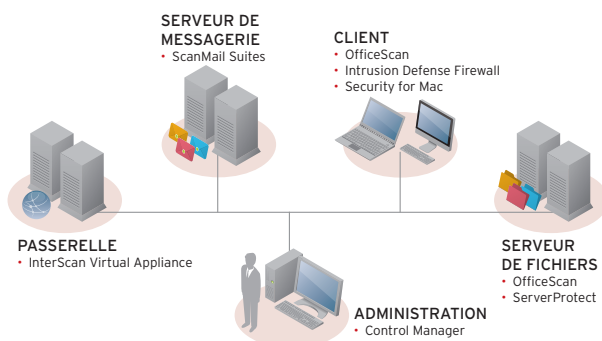


Protection maximale des terminaux et serveurs de messagerie

Protection multicouche	Protection de la plateforme	Avantage
SERVEUR DE MESSAGERIE		
ScanMail Suite for Microsoft Exchange	Windows	Bloque les spams et les spywares sur le serveur de messagerie
ScanMail Suite for IBM® Domino	Windows, Linux	Bloque les spams et les spywares sur le serveur de messagerie
SERVEUR DE FICHIERS		
OfficeScan	Windows	Protège les serveurs Windows
ServerProtect for Windows/Novell NetWare	Windows, NetWare	Protège les serveurs de fichiers Windows et NetWare
ServerProtect for Linux	Linux	Protège les serveurs de fichiers Linux
CLIENT/TERMINAL MOBILE		
OfficeScan	Windows	Protège les clients Windows
Intrusion Defense Firewall	Windows	Système de prévention d'intrusions sur l'hôte (HIPS) proactif et protection contre les failles
Security for Mac	Apple Macintosh	Protège les clients Mac contre les programmes malveillants et bloque les sites Web malveillants
VDI	-	Protège l'environnement des postes de travail virtuels
Mobile Security	Android, iOS, Windows Phone et autres	Protège les terminaux mobiles tels que les smartphones et les tablettes
ADMINISTRATION		
Control Manager Advanced	Windows	Gestion centrale de la sécurité

Enterprise Security Suite

Protégez votre passerelle Internet ainsi que vos serveurs de messagerie et de fichiers, vos postes de travail, vos ordinateurs portables et vos terminaux mobiles à l'aide de cette solution de sécurité entièrement intégrée, à gestion centralisée. Celle-ci offre une protection multicouche optimale contre les virus, les spywares, les spams et les menaces complexes, notamment les menaces Web. Grâce à sa protection complète et à des fonctionnalités telles que la prise en charge de la virtualisation, des options de configuration flexibles, une évolutivité élevée et une large prise en charge de plateformes, Enterprise Security Suite permet de réduire la complexité et de diminuer les coûts.



Avantages

- **Optimise la protection**
 - Réduit les risques contre les nombreuses menaces grâce à une vaste protection multicouche
 - Offre une protection immédiate grâce à des données sur les menaces basées sur le Web
 - Augmente la productivité par le biais d'antispam et de filtres Web à la pointe du secteur
- **Réduit les coûts**
 - Baisse les taux d'infection des terminaux de 62 %
 - Réduit les coûts de gestion pour la sécurité informatique de 40 %
- **Réduit la complexité**
 - Réduit le temps d'acquisition, d'installation et de gestion grâce à une solution intégrée
 - Facilite l'administration via une gestion centrale basée sur le Web

Protection maximale et complexité minimale pour tous les points et plateformes protégés

Protection multicouche	Protection de la plateforme	Avantage
PASSERELLE		
InterScan Messaging Security Virtual Appliance	VMware ou appliance logicielle	La sécurité de passerelle de messagerie virtualisée bloque les spams et les menaces de messagerie
InterScan Web Security Virtual Appliance	VMware, Hyper-V ou appliance logicielle	La sécurité de passerelle Internet virtualisée bloque les menaces Web et filtre les URL
SERVEUR DE MESSAGERIE		
ScanMail Suite for Microsoft Exchange	Windows	Bloque les spams et les spywares sur le serveur de messagerie
ScanMail Suite for IBM® Domino	Windows, Linux	Bloque les spams et les spywares sur le serveur de messagerie
SERVEUR DE FICHIERS		
OfficeScan	Windows	Protège les serveurs Windows
ServerProtect for Windows/Novell NetWare	Windows, NetWare	Protège les serveurs de fichiers Windows et NetWare
ServerProtect for Linux	Linux	Protège les serveurs de fichiers Linux
CLIENT/TERMINAL MOBILE		
OfficeScan	Windows	Protège les clients Windows
Intrusion Defense Firewall	Windows	Système de prévention d'intrusions sur l'hôte (HIPS) proactif et protection contre les failles
Security for Mac	Apple Macintosh	Protège les clients Mac contre les programmes malveillants et bloque les sites Web malveillants
VDI	-	Protège l'environnement des postes de travail virtuels
Sécurité mobile	Android, iOS, Windows Phone et autres	Protège les terminaux mobiles tels que les smartphones et les tablettes
ADMINISTRATION		
Control Manager Advanced	Windows	Gestion centrale de la sécurité

OfficeScan - Infrastructure de poste de travail virtuel

Trend Micro Virtual Desktop Security est conçu spécialement pour les environnements dotés de postes de travail virtuels. Cette solution optimise la protection d'un grand nombre de scénarios d'utilisation des postes de travail virtuels.

Avantages

- Agents optimisés pour la VDI
- Préviend les conflits de ressources
- Nettoie et scanne la mémoire vive et surveille les comportements
- Reconnaît automatiquement tout agent présent sur un terminal physique ou virtuel
- Réduit le temps de scan des postes de travail virtuels en établissant une liste blanche des images de base et des contenus précédemment scannés

Sécurité mobile

Trend Micro Mobile Security permet aux entreprises d'élargir la protection éprouvée des PC aux terminaux et aux données mobiles. Ainsi, les plateformes des smartphones et des tablettes, de plus en plus appréciées par les employés, peuvent être intégrées sans problème. Grâce à un aperçu et à un contrôle centraux de la gestion et de la protection des terminaux, les entreprises peuvent réduire leurs coûts. Cette solution fait prévaloir l'utilisation de mots de passe, chiffre les données et supprime à distance les données de terminaux perdus ou volés. Les données sont donc protégées de manière fiable et les pertes de données sont limitées.

Avantages

- Protection contre les menaces
 - Programmes malveillants
 - Spywares
 - Menaces Web
- Réduction des coûts d'exploitation
- Baisse des pertes de données
- Diminution des risques liés à la sécurité

Intrusion Defense Firewall/ Vulnerability Protection

En tant que plug-in pour OfficeScan intégré à Trend Micro Enterprise Security for Endpoints, Intrusion Defense Firewall complète la sécurité OfficeScan déjà très efficace à l'échelle du client, grâce à un système de prévention d'intrusions sur l'hôte (HIPS) à l'échelle du réseau.

Vulnerability Protection est une solution IDS/IPS d'OfficeScan indépendante, destinée à la protection des terminaux contre l'exploitation de failles de sécurité.

Avantages

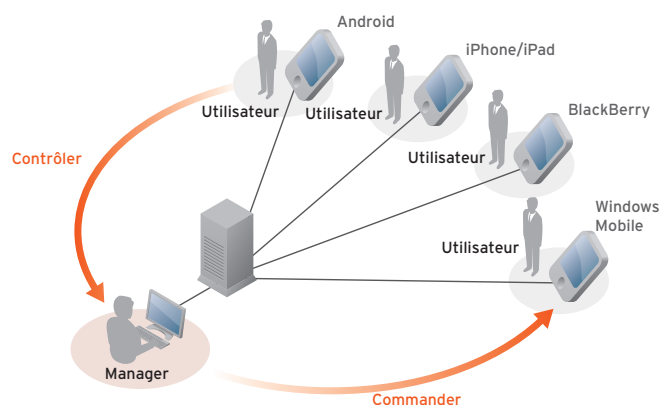
- Protège les terminaux en cas d'atteinte minimale au trafic réseau, aux performances du système et à la productivité des utilisateurs
- Bloque les attaques avant qu'elles ne puissent atteindre les applications au niveau des terminaux ou qu'elles ne puissent les exécuter
- Offre une protection avant la mise à disposition de patches

Sécurité pour dispositifs Mac

En tant que plug-in pour OfficeScan, Trend Micro Security for Mac utilise efficacement Smart Protection Network™ afin de limiter activement le risque de danger dû aux menaces. La technologie d'évaluation de la réputation des sites Web empêche en temps réel les utilisateurs et applications d'accéder à des contenus Web malveillants.

Avantages

- Bloque les attaques issues de programmes malveillants envahissant les systèmes, y compris Mac OS et Windows



Safe Mobile Workforce

Les dispositifs mobiles, notamment les smartphones et tablettes des employés, font actuellement partie intégrante du quotidien d'une entreprise moderne. Pour rester compétitif, il est indispensable de garantir l'accès des employés aux données et applications de l'entreprise, où qu'ils soient et quel que soit leur dispositif. Ce phénomène s'accompagne toutefois d'importants risques pour la sécurité.

Avec Trend Micro Safe Mobile Workforce, les données confidentielles ne sont pas sauvegardées sur le dispositif mobile, car elles seraient alors soumises à des mesures de sécurité qui risqueraient de restreindre considérablement l'accès aux données et les performances du dispositif. Il suffit d'ouvrir une application iOS ou Android pour accéder, via une infrastructure mobile virtuelle (VMI), aux ressources de l'entreprise. Toutes les données et applications sont conservées en toute sécurité sur les serveurs de l'entreprise, tandis qu'un système d'exploitation Android hébergé propose un environnement de travail virtuel familier et intuitif.

Avantages

- Optimise la sécurité grâce à une nette distinction entre les données personnelles et professionnelles sans ralentir la navigation
- Renforce la satisfaction des utilisateurs et leur productivité
- Garantit l'application des stratégies de conformité
- Permet l'utilisation d'applications familières et répandues dans le monde entier
- Élimine tout risque en cas de vol, car les données et applications ne sont pas sauvegardées sur le dispositif
- Réduit les coûts



Endpoint Application Control

Chaque jour, des centaines de milliers de nouvelles applications logicielles malveillantes sont mises en circulation. Il devient donc difficile de maîtriser tous les vecteurs d'attaque potentiels. Toute action indésirable de l'utilisateur risque alors d'entraîner la perte de données d'entreprises confidentielles stockées sur son ordinateur, c'est pourquoi il est désormais capital de protéger les données et les ordinateurs de comportements inadéquats et des accès non autorisés. Les antivirus traditionnels n'en sont malheureusement pas capables. Il vous faut donc une solution de sécurité multicouche qui bloque les menaces de façon proactive avant même qu'elles n'atteignent votre terminal. Par ailleurs, il est également important d'opposer une réponse rapide aux programmes malveillants déjà présents sur le terminal.

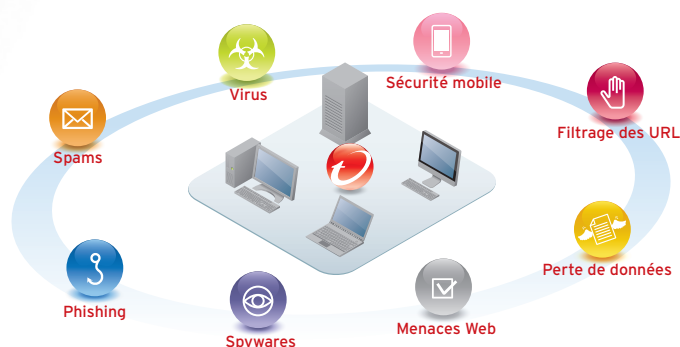
Avec Trend Micro Endpoint Application Control, élargissez votre protection face aux programmes malveillants et aux attaques ciblées en empêchant l'installation et l'exécution d'applications inconnues et indésirables sur les terminaux d'entreprise. Grâce à la combinaison de stratégies souples et simples à gérer, de fonctions de listes blanches et de listes noires et d'une base de données d'applications mondiale basée sur le cloud, cette solution simple à gérer réduit considérablement la vulnérabilité des terminaux face aux attaques. Endpoint Application Control s'intègre aux solutions Trend Micro Complete User Protection pour proposer une protection avancée face aux attaques et à la perte de données.

Avantages

- Empêche l'exécution de logiciels indésirables par les utilisateurs ou les machines
- Répartit simplement les agents, notamment avec OfficeScan
- Propose des fonctions étendues pour appliquer les stratégies d'entreprise
- Exploite des données corrélées de menaces à partir de milliards de données enregistrées chaque jour
- Aide au respect des exigences de conformité

Worry-Free Business Security Advanced Worry-Free Business Security Standard Worry-Free Business Security Services

Offre une protection rapide, efficace et simple contre les virus informatiques, les cybercriminels et la perte de données. Ainsi, vous pouvez vous concentrer sur vos affaires sans avoir à vous inquiéter pour votre sécurité Internet. Des tests indépendants ont révélé que Worry-Free était la solution numéro 1 en matière de protection contre les menaces Web, AVANT que celles-ci n'atteignent les PC, les clients Mac, les serveurs de fichiers et de messagerie. Cette solution propose donc une protection améliorée sans ralentir votre ordinateur.



Avantages

- Protection complète de tous les terminaux
- Protection contre les menaces Web
- Recherche intelligente
 - Accélération de la recherche automatique et des mises à jour
- Protection contre la perte de données
- Antispam complet
- Commande d'accès au dispositif
- Aucune dépense obligatoire pour les mises à jour (cela s'applique seulement à la version Services)

	Worry-Free Business Security Services	Worry-Free Business Security Standard	Worry-Free Business Security Advanced
AVANTAGES UNIQUES DE WORRY-FREE			
Protection contre les menaces Web, blocage des virus et autres menaces Web avant qu'elles n'atteignent votre entreprise	●	●	●
Protection d'Intuit QuickBooks		●	●
Accélération de la reconnaissance et de la réaction face aux nouvelles menaces via Smart Feedback	●	●	●
Outil intégré de suppression de faux programmes antivirus		●	●
Prise en charge d'IPv6		●	●
PLATEFORMES			
PC, ordinateurs portables, serveurs Windows	●	●	●
Clients et serveurs Mac (iMac et MacBooks)	●	●	●
NOUVEAU : fonctions de gestion des dispositifs mobiles par Microsoft Exchange ActiveSync pour iOS, Android, BlackBerry, Windows Phone			●
Antivirus pour les dispositifs Android™ (chaque licence permet de protéger 2 dispositifs Android)	●		
PROTECTION CONTRE LES VIRUS ET SÉCURITÉ INTERNET			
Bloque les virus, les spywares, les zombies et les rootkits	●	●	●
Le filtrage avancé des URL bloque l'accès aux sites Web présentant des contenus inappropriés	●	●	●
ADMINISTRATION CENTRALISÉE			
Console Web intuitive	●	●	●
Site du serveur de gestion	Hébergé	Local	Local
SÉCURITÉ DES DONNÉES			
Commande du dispositif : contrôle l'accès aux lecteurs USB et aux autres dispositifs connectés pour empêcher la perte des données et bloquer les menaces	●	●	●
La protection contre la perte de données empêche l'envoi, volontaire ou non, de données critiques dans les e-mails professionnels			●
SÉCURITÉ DE MESSAGERIE ET ANTISPAM			
Scanne les e-mails et empêche que les spams atteignent la boîte POP3	●	●	●
Bloque les spams et les virus véhiculés par e-mail avant qu'ils n'atteignent votre serveur de messagerie	Disponible séparément		●
Protection intégrée contre les menaces et antispam multicouche pour Microsoft Exchange Server			●

Deep Security

Trend Micro Deep Security offre une plateforme de sécurité complète pour les data centers virtualisés, permettant de les protéger contre le vol de données et les interruptions d'activités. Elle garantit également le respect des exigences de conformité en vigueur. Cette solution sans agent basée sur VMware vSphere facilite la gestion d'activités importantes pour la sécurité et accélère la rentabilité des projets de virtualisation et de cloud.

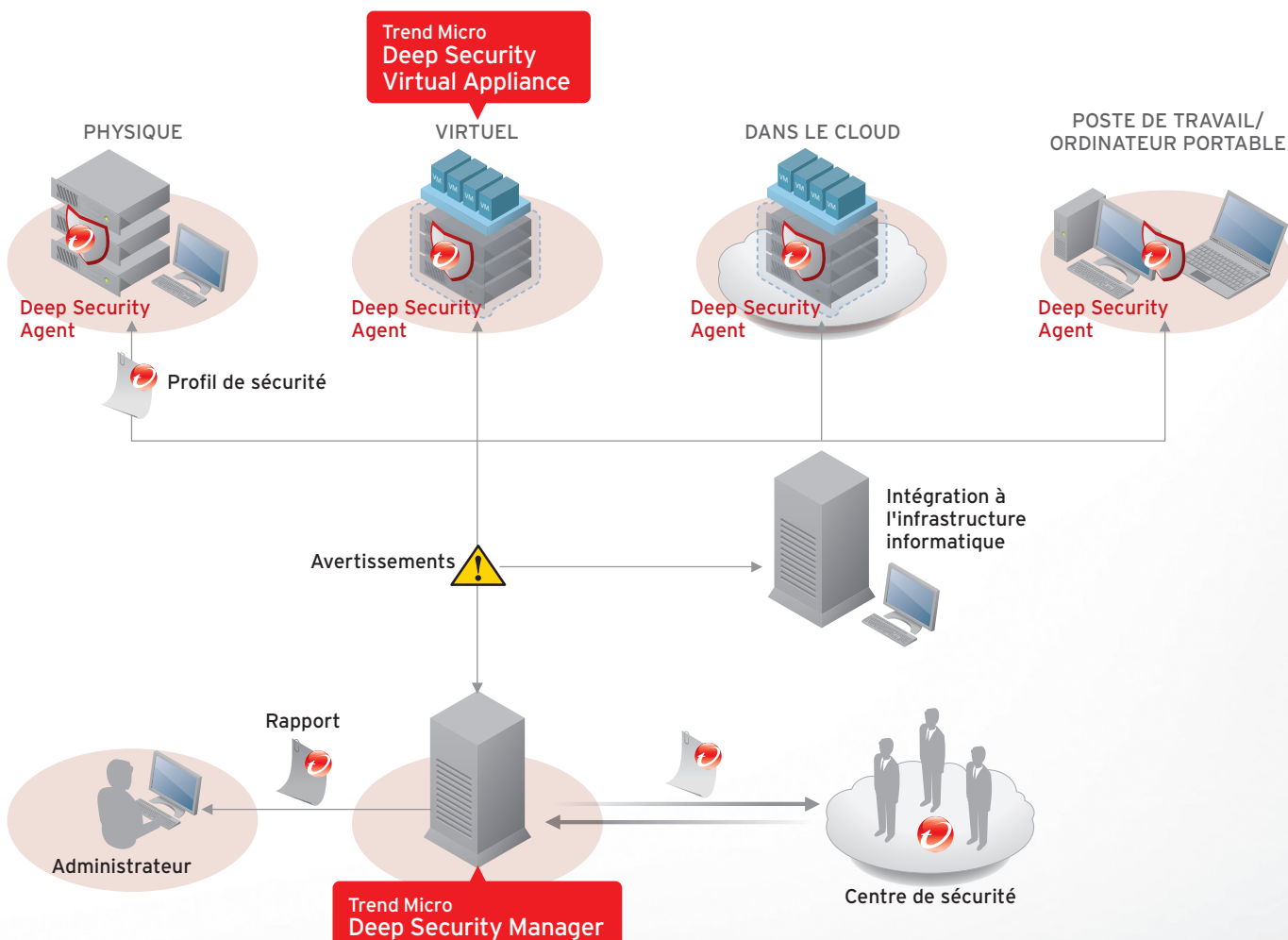
Des modules compatibles peuvent être intégrés à la plateforme afin d'assurer la sécurité des serveurs, des applications et des données sur les systèmes physiques, virtuels et basés sur le cloud ainsi que sur les postes de travail virtuels. Ainsi, vous profitez de solutions de sécurité parfaitement adaptées à vos exigences en associant à votre guise des éléments de protection avec ou sans agent : anti-programmes malveillants, évaluation de la réputation Web, pare-feu, défense contre les intrusions, contrôle de l'intégrité et vérification de protocole. Résultat : une plateforme de sécurité modulable et efficace pour serveur qui protège les applications et les données importantes des entreprises contre les attaques et les interruptions d'activités et élimine même le problème des patches d'urgence coûteux.

Fonctionnalités

- Anti-programmes malveillants
- Contrôle de l'intégrité
- Réputation Web
- Reconnaissance et défense contre les intrusions
- Pare-feu avec état bidirectionnel
- Vérification de protocoles
- Multi-tenant
- Contrôle de l'intégrité/de l'hyperviseur
- Intégration d'AWS et vCloud
- Certifié IPv6 Ready
- **NOUVEAU** Prise en charge de VMware NSX
- **NOUVEAU** Agent anti-programmes malveillants Realtime Linux

Avantages

- Accélère la rentabilité en cas de virtualisation, VDI et de cloud computing
 - Offre une méthode de gestion plus légère et plus simple pour protéger les VM
- Réduit considérablement les coûts d'exploitation
- Empêche la perte de données et les interruptions d'activités
 - Reconnaît et supprime les programmes malveillants en temps réel en cas d'atteinte minimale aux performances
- Met en œuvre des stratégies rentables
 - Répond aux exigences de conformité principales, notamment des normes PCI DSS 2.0, HIPAA, etc.



ServerProtect for Microsoft Windows/ Novell NetWare

Empêche la propagation de virus sur le réseau en les bloquant avant qu'ils n'atteignent l'utilisateur. Trend Micro ServerProtect for Microsoft Windows/Novell NetWare scanne, reconnaît et supprime les virus présents dans les fichiers et les fichiers compressés en temps réel. ServerProtect offre une assistance 24 h/24 et une protection contre les virus à l'aide de mises à jour automatiques et incrémentielles sur les virus. La gestion du serveur centralisée par une console à interface Web facilite la protection du réseau.

Avantages

- Prend en charge Microsoft Windows Server 2000, 2003, 2008 et 2008 R2 pour des performances, une fiabilité, une sécurité, une évolutivité et une disponibilité élevées
- Permet une recherche des virus en temps réel performante en cas d'atteinte minimale aux serveurs

ServerProtect for Linux

Trend Micro ServerProtect for Linux empêche que votre serveur de fichiers Linux n'héberge des virus, des chevaux de Troie, des zombies et une multitude d'autres programmes malveillants à votre insu. Cette solution offre une protection en temps réel ainsi qu'une défense efficace en cas d'atteinte minimale aux performances du processeur. Elle prend aussi en charge toutes les fonctions courantes de Linux. ServerProtect for Linux élargit la stratégie de conformité et de sécurité de votre entreprise pour y ajouter une solution performante.

Avantages

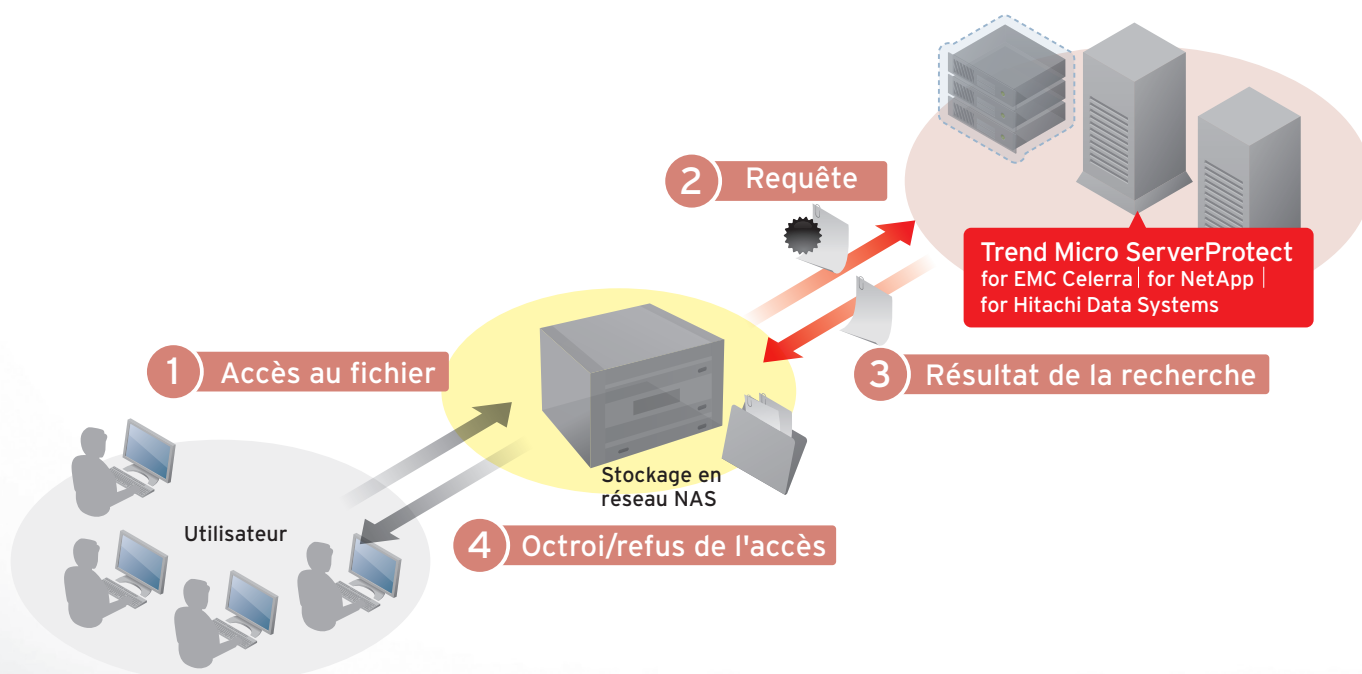
- Empêche que les menaces des serveurs Linux ne soient transmises à d'autres serveurs ou PC
- Optimise les performances et réduit l'atteinte aux performances du processeur grâce à une recherche à noyau multifilière

ServerProtect for EMC ServerProtect for NetApp

Trend Micro ServerProtect pour le stockage représente la solution de sécurité la plus fiable et la plus performante du secteur pour les plateformes de stockage. Elle protège les systèmes de stockage des fichiers grâce à la reconnaissance et à la suppression des virus et des spywares en temps réel.

Avantages

- Intégration étroite à EMC Celerra, NetApp Filer ou Hitachi NAS
- Recherche performante des virus en temps réel en cas d'atteinte minimale aux serveurs, et sans conséquence pour l'utilisateur final

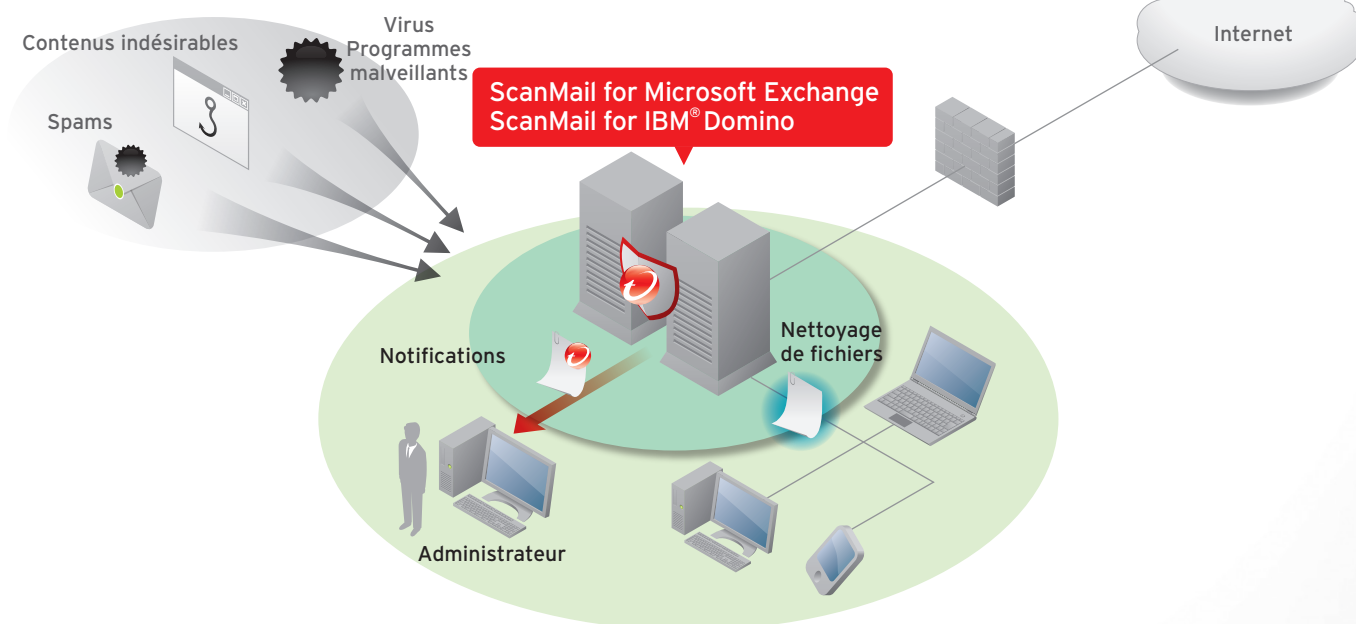


ScanMail for Microsoft Exchange

ScanMail Suite for Microsoft Exchange offre une sécurité de contenu basée sur la signature à la pointe du secteur, ainsi que des technologies d'évaluation de la réputation Web et de messagerie innovantes pour se protéger contre le vol de données et les pertes accidentelles. ScanMail for Microsoft Exchange identifie les attaques ciblées au moyen de la reconnaissance d'exploits et du sandboxing et fait partie de Custom Defense, la solution Trend Micro pour une protection flexible contre les menaces individuelles.

Avantages

- Intégration et adaptation à l'environnement de serveur Microsoft Exchange
- Protection contre les spams, programmes malveillants et attaques de type « zero-day »
- Filtrage de contenu flexible
- Évaluation unique de la réputation Web
- Évaluation de la réputation des e-mails (facultative)
- Protection intégrée contre la perte de données pour préserver les données confidentielles



ScanMail for IBM® Domino

Bloque les virus, les spywares, les spams, le phishing et les contenus inappropriés présents sur le serveur de messagerie, soit le point de sécurité central pour la vérification de messages internes et entrants, avec Trend Micro ScanMail Suite for IBM® Domino. Si cette solution est intégrée à Trend Micro Deep Discovery Advisor, elle fait partie de Custom Defense, la solution Trend Micro pour une protection flexible contre les menaces individuelles, et bloque donc les attaques de messagerie ciblées.

Avantages

- Protection de premier plan contre les virus, spywares, spams, phishing et attaques de type « zero-day »
- Technologie d'évaluation de la réputation Web innovante
- Filtrage de contenu flexible

PortalProtect for Microsoft SharePoint

Grâce à sa couche de protection spécialisée, Trend Micro PortalProtect protège votre système de collaboration contre les programmes malveillants, les liens et les sites Web malveillants et les autres menaces que la plupart des administrateurs SharePoint ne connaissent pas.

La technologie d'évaluation de la réputation des sites Web protège votre portail Web contre les liens vers des sites Web malveillants, tandis que le filtrage de contenu performant ainsi que les composants de SharePoint contenus dans des fichiers ou basés sur le Web se chargent de la surveillance.

Avantages

- Protection des utilisateurs et données SharePoint
- Blocage de nombreux fichiers et URL malveillants
- Filtrage de contenus inappropriés issus des composants sociaux de SharePoint
- Vérification des données confidentielles au vu de l'application des stratégies et de la gestion des risques
- Réduction des efforts de gestion
- Évolutivité à tout type d'environnement
- Protection intégrée contre la perte de données pour préserver les données confidentielles

IM Security for Microsoft Lync and Office Communications Server

Protégez votre communication de messagerie instantanée en temps réel à l'aide du blocage des attaques frénétiques développées pour propager les programmes malveillants, entraîner les internautes vers des sites Web malveillants et voler les données. Prise en charge par Trend Micro Smart Protection Network et l'architecture client sur le cloud unique, la solution IM Security bloque les liens vers les sites Web malveillants avant que ces derniers ne soient envoyés. Des technologies de sécurité indépendantes des signatures contre les attaques de type « zero-day », des antivirus et de nouveaux antispyswares de premier plan préviennent tous dégâts éventuellement causés par des programmes malveillants. De plus, le filtrage de contenu flexible empêche l'utilisation inappropriée de services de messagerie instantanée et protège contre le vol de données.

Fonctions et avantages

- **UNIQUE !** Bloque les liens vers des sites Web malveillants avant leur envoi grâce à l'évaluation de la réputation Web
- Reconnaît et bloque les attaques de type « zero-day » via la technologie propriétaire IntelliTrap
- Stoppe davantage de spywares avant qu'ils n'infiltrerent les PC à l'aide d'une surveillance spécialisée
- Filtre les contenus contre la perte de données et l'utilisation de langage injurieux
- Réduit les efforts de gestion grâce à une intégration étroite à la plateforme et à une commande stable et centralisée

Enterprise Security for Communication and Collaboration

Trend Micro Communication & Collaboration Security protège les systèmes de messagerie, de collaboration et de messagerie instantanée Microsoft en bloquant les menaces en temps réel avant qu'elles ne les affectent. L'architecture client sur le cloud unique de Trend Micro Smart Protection Network

offre plusieurs fonctions de sécurité (par ex. l'évaluation de la réputation Web et de messagerie) pour se protéger contre les menaces en temps réel. L'association de ces fonctions avec les technologies de sécurité de contenu conventionnelles de premier plan vous permet de communiquer en toute sécurité.

Communication & Collaboration Security



Administration centralisée
Trend Micro Control Manager



Serveur de collaboration
Trend Micro PortalProtect for Microsoft SharePoint



Serveur de messagerie
Trend Micro ScanMail Suite for Microsoft Exchange



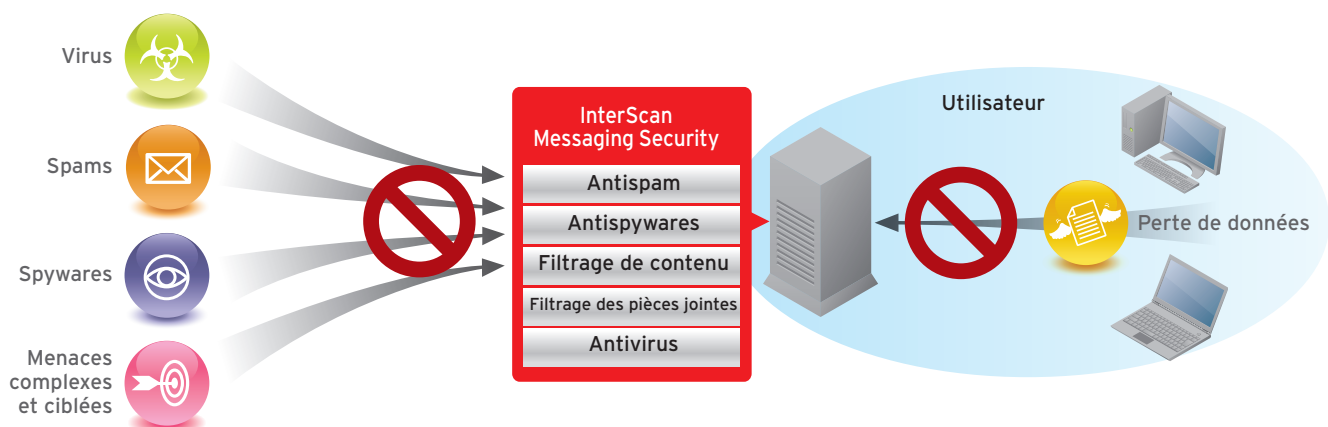
Serveur de messagerie instantanée
Trend Micro IM Security for Microsoft Office Communications Server

InterScan Messaging Security Virtual Appliance

Trend Micro InterScan Messaging Security stoppe les menaces traditionnelles sur le cloud à l'aide de données internationales sur les menaces, protège les données confidentielles au moyen de fonctions contre la perte de données et le chiffrement et reconnaît les attaques ciblées, en tant que partie intégrante d'un système de défense contre les menaces avancées persistantes (APT). Cette installation SaaS hybride rassemble la protection des données et le contrôle d'une appliance virtuelle locale avec la protection proactive de services de préfiltres basés sur le cloud.

Avantages

- Reconnaît et bloque les menaces complexes et ciblées (menaces avancées persistantes, APT)
- Déjoue les programmes malveillants complexes et les attaques de phishing ciblées
- Facilite la sécurité des données et le chiffrement
- Stoppe davantage de spams : solution numéro un selon des tests indépendants

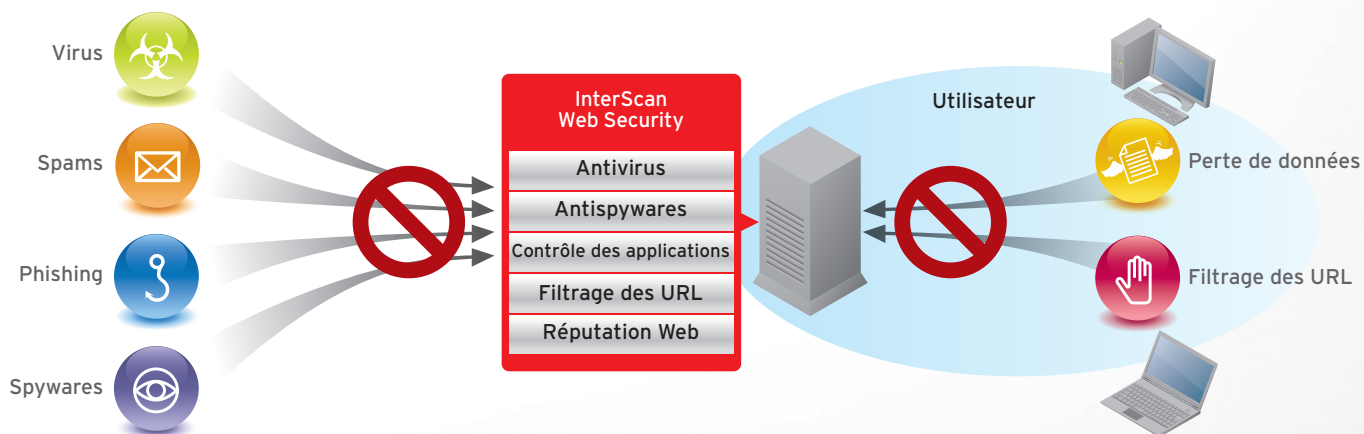


InterScan Web Security Virtual Appliance

InterScan Web Security Virtual Appliance est une appliance logicielle virtuelle combinant le contrôle grâce à l'utilisation d'applications basées sur le Web avec la recherche de programmes malveillants, l'évaluation de la réputation Web innovantes en temps réel et le filtrage flexible d'URL. Elle offre ainsi une protection de premier plan contre les menaces Web.

Avantages

- Transparence et contrôle immédiats
- Blocage des menaces Web avant qu'elles ne pénètrent dans le réseau de l'entreprise
- Réduction de vos coûts totaux
- Protection intégrée contre la perte de données pour préserver les données confidentielles



Enterprise Security for Gateways

Protégez vos données confidentielles ainsi que vos employés lors du traitement de contenus Internet multiples. Trend Micro Enterprise Security for Gateways intègre une sécurité virtualisée pour les passerelles Internet et de messagerie. Cette solution optimise sensiblement la protection et réduit les efforts ainsi que les coûts totaux jusqu'à 40 %.* L'évaluation de la réputation Web et de messagerie basée sur le cloud, combinée à un antispam et un antivirus leaders du secteur ainsi qu'un filtrage d'URL, offre une défense multicouche bloquant les programmes malveillants, les liens vers les sites

Web malveillants et les contenus inappropriés, avant que ces derniers ne puissent pénétrer dans le réseau. Grâce à des rapports en temps réel, vous recevez un aperçu unique des activités actuelles sur Internet afin de mettre tout de suite un terme aux comportements imprudents. Un filtrage du contenu sortant ainsi qu'un chiffrement d'e-mails** protège les données confidentielles et garantit le respect des exigences de conformité en vigueur pour une sécurité de passerelle complète.

* Osterman Research, Pourquoi la virtualisation mérite votre attention, février 2009.

** Trend Micro Encryption for Gateway est un add-on facultatif.

Protection maximale et efforts minimaux sur la passerelle

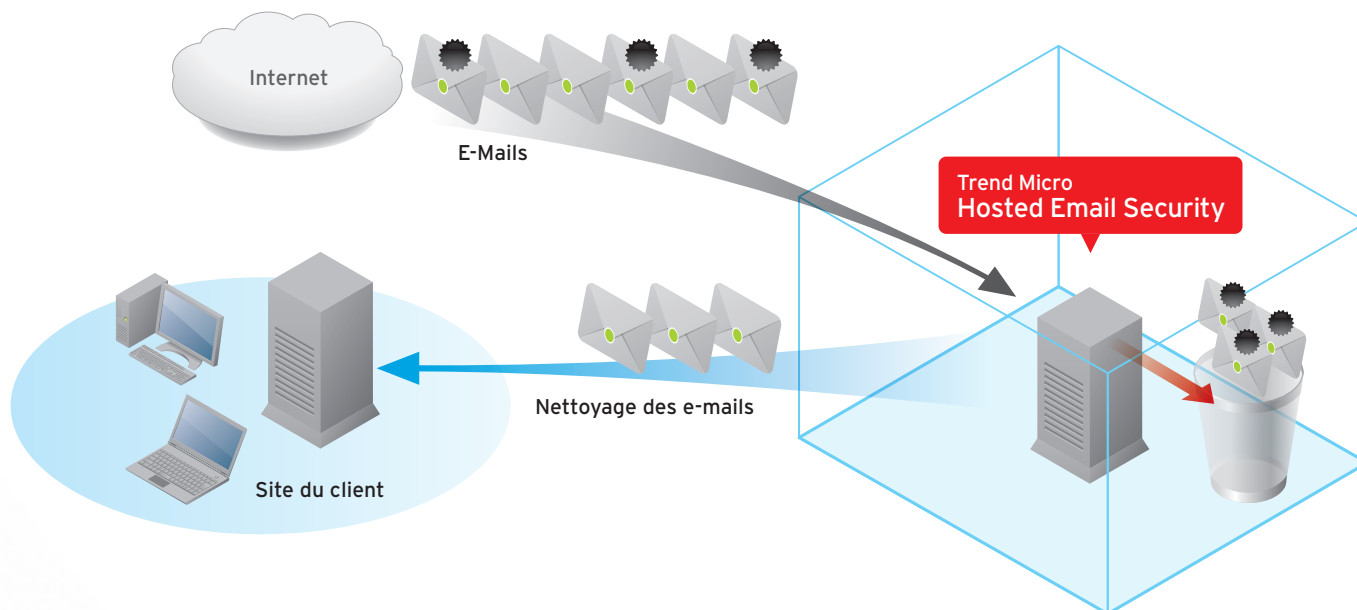
Protection multicouche	Avantage
PASSERELLE	
InterScan Messaging Security Virtual Appliance	La sécurité de passerelle de messagerie virtualisée bloque les spams et les menaces de phishing et de messagerie
InterScan Web Security Virtual Appliance	La sécurité de passerelle Internet virtualisée bloque les menaces Web et filtre les URL
Trend Micro Encryption for Email Gateway	La sécurité de passerelle de messagerie virtualisée chiffre les contenus d'emails et les pièces jointes

Hosted Email Security

Trend Micro Hosted Email Security est une solution sans entretien, offrant une protection actualisée en permanence et bloquant les spams et les virus avant qu'ils n'atteignent le réseau.

Avantages

- Soulage la bande passante et augmente la productivité
- Libère votre temps pour implémenter les initiatives professionnelles essentielles

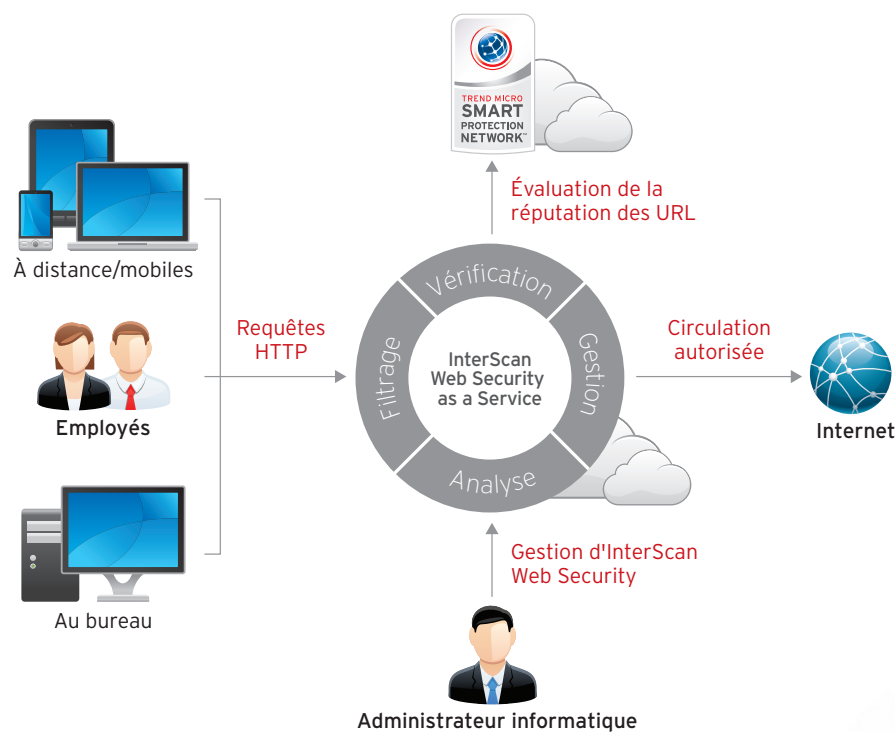


InterScan Web Security as a Service

Trend Micro InterScan Web Security as a Service (IWSaaS) offre une protection dynamique contre les cyberattaques dans le cloud, avant même qu'elles n'atteignent vos utilisateurs ou votre réseau et vous garantit la transparence et le contrôle de l'utilisation d'Internet par vos employés en temps réel. En tant que solution basée sur le cloud, IWSaaS protège tous les utilisateurs, partout, sur tous les dispositifs, en s'appuyant sur une directive unique, indépendamment du lieu où se trouvent les utilisateurs. Finis les retours coûteux du trafic des données ou la gestion de plusieurs passerelles Internet protégées à des emplacements différents. En outre, vous pouvez adapter la solution à la croissance de votre entreprise, sans devoir investir dans l'acquisition, la gestion ou la maintenance de logiciels ou de matériel. Si vous optez pour une installation hybride, l'appliance locale « InterScan Web Security Virtual Appliance » peut facilement s'intégrer aux fonctions générales de gestion, de rapports et de stratégies d'InterScan Web Security en tant que service.

Avantages

- La meilleure protection, partout et sur tous les dispositifs
- Offre aux utilisateurs plus de liberté tout en garantissant transparence et contrôle
- Gestion et rapports simples mais performants
- Optimisation des avantages du cloud : rentabilité et flexibilité



Sécurité de passerelle

08 CHIFFREMENT

Endpoint Encryption

Endpoint Encryption chiffre les données sur de nombreux systèmes tels que les ordinateurs portables, les postes de travail, les tablettes, les CD, les DVD, les lecteurs USB et autres supports amovibles. Cette solution intègre le chiffrement, à l'échelle de l'entreprise, du disque dur, des fichiers, des dossiers et des supports amovibles, combiné à une commande d'accès ciblée aux terminaux et aux ports afin d'empêcher l'accès non autorisé à des données confidentielles et leur emploi par des utilisateurs non autorisés. Une console de gestion unique vous permet de gérer le chiffrement de matériel et de logiciel à l'échelle de l'entreprise pour les disques durs, les données définies, les dossiers, les supports amovibles et les dispositifs de stockage.

Fonctionnalités

- **Rapports et audits approfondis**
 - Application automatique des exigences de conformité en vigueur au moyen d'un chiffrement basé sur des règles
 - Audits et rapports détaillés selon l'utilisateur, l'unité d'entreprise et le système
- **Authentification à facteurs multiples avant le démarrage**
 - Authentification flexible, incluant des mots de passe, CAC, PIV, Pin et ColorCode® définis
 - Fonction de verrouillage en cas d'authentification erronée
- **Outils de gestion et intégration d'Active Directory**
 - Utilisation d'Active Directory et de l'infrastructure informatique existante pour l'installation et la gestion
 - Allègement de la charge de l'équipe informatique, car les utilisateurs peuvent modifier eux-mêmes leurs mots de passe et leurs comptes et les réinitialiser

Avantages

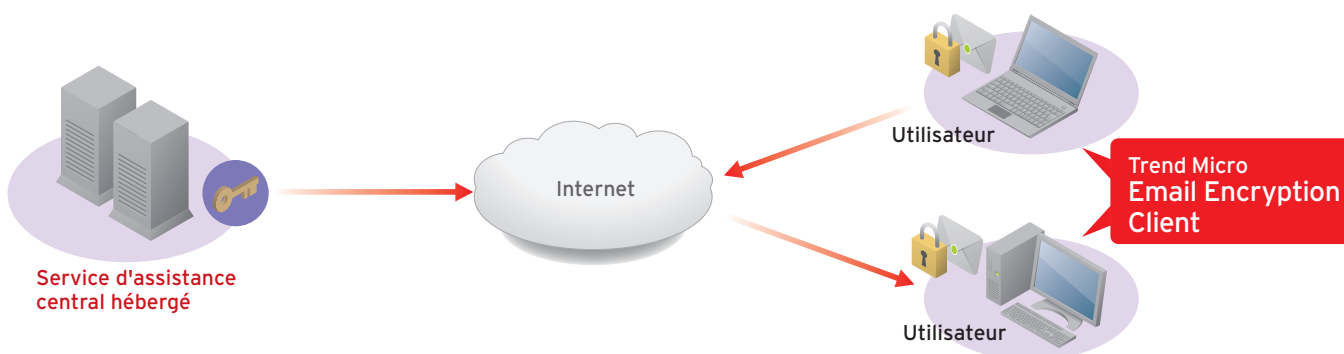
- **Optimisation de la protection de la plateforme pour le chiffrement de données et de systèmes**
 - Chiffrement de données confidentielles au moyen de fonctions de chiffrement entièrement intégrées pour disques durs, fichiers, dossiers, lecteurs USB et supports amovibles
- **Réduction des coûts totaux d'entreprise à l'aide d'une gestion des clés et des stratégies centralisée**
 - Fonctionnement simplifié grâce au stockage des données unifié au moyen d'un serveur de gestion centralisé et d'une console de gestion
- **Simplification de la gestion des terminaux à distance**
 - Respect des réglementations et protection des données en cas de perte d'un terminal ou d'oubli de mots de passe, sans inquiéter l'utilisateur
 - Gestion des stratégies et protection des données présentes sur les PC, ordinateurs portables, tablettes, lecteurs USB, CD et DVD

Fonctions principales	Trend Micro	
	Endpoint Encryption	Chiffrement des fichiers
Gestion centralisée des clés et des stratégies	●	●
Certification de chiffrement FIPS 140-2	Niveau de sécurité 2	Niveau de sécurité 2
Chiffrement AES 256 bits	●	●
Chiffrement de fichiers et de dossiers	●	●
Chiffrement de supports amovibles (CD/DVD/USB)	●	●
Commande à distance ciblée de ports et de dispositifs	●	●
Disques durs de gestion à chiffrement automatique	●	
Chiffrement de disques durs	●	
Authentification compatible réseau avant le démarrage		

Email Encryption Client

Trend Micro Email Encryption protège chacun des e-mails envoyés depuis une messagerie électronique. Le chiffrement basé sur le client permet à l'utilisateur de choisir d'un simple clic sur l'interface de son bureau les e-mails qu'il souhaite chiffrer. La possibilité de chiffrer des e-mails spécifiques contenant des données particulières optimise le chiffrement basé sur les stratégies, qui permet de chiffrer

automatiquement tout type de contenu. Ces composants constituent ainsi une solution complète de chiffrement des e-mails. Trend Micro Email Encryption Client est un plug-in de logiciel pour les clients de messagerie les plus courants pouvant être déployé sans modification des processus de l'entreprise existants et intégré sans problème dans l'infrastructure de messagerie.



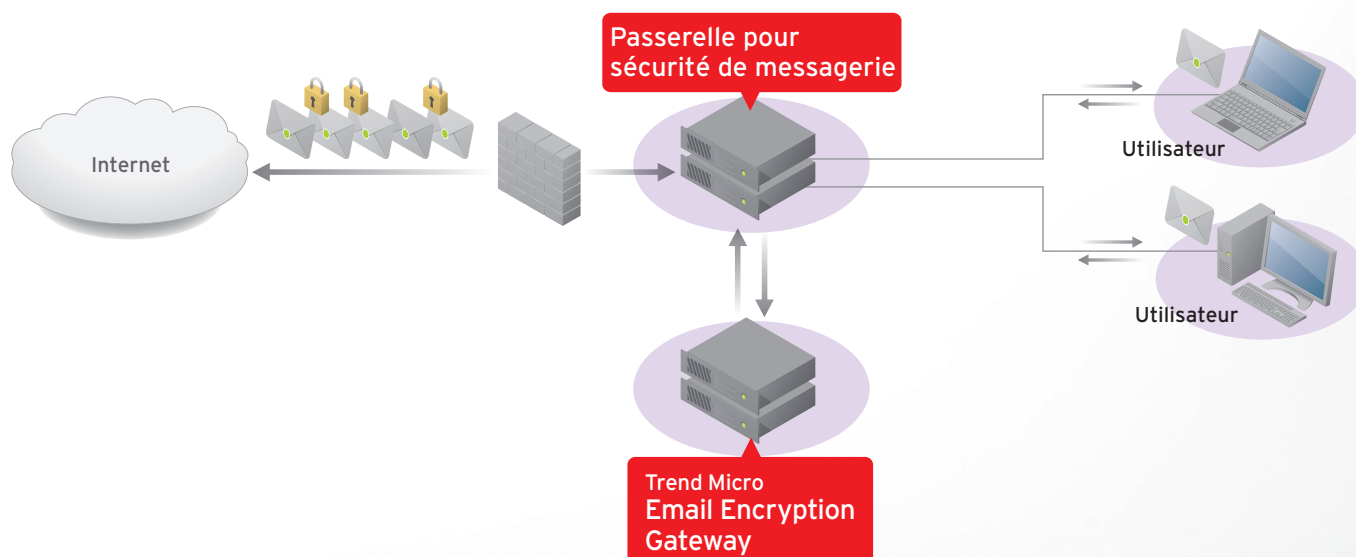
Encryption for Email Gateway

Le chiffrement pour les passerelles d'entreprises augmente la sécurité de messagerie à l'aide du déploiement d'un chiffrement basé sur des stratégies et d'une intégration à l'infrastructure de sécurité de messagerie. Cette solution offre une implémentation et une administration simples, ne nécessitant aucune modification des processus de l'entreprise existants. Grâce à l'association à la sécurité de contenu, les entreprises peuvent chiffrer automatiquement les e-mails et les pièces jointes, sans que la présence des utilisateurs soit nécessaire pour la protection de données confidentielles.

Plug-ins Hosted Email Encryption pour Hosted Email Security

Ce service de chiffrement basé sur des stratégies peut être intégré sans problème à la fonction de filtrage de contenu de Hosted Email Security. Ainsi, des types de contenus définis sont reconnus et des e-mails sont chiffrés dès que les règles sont mises en place.

* Uniquement en association avec Hosted Email Security avec un filtre pour contenus de messagerie sortants. Aucun matériel ou logiciel supplémentaire requis.



Chiffrement

Solution Deep Discovery

Trend Micro Deep Discovery offre exactement la transparence et le contrôle à l'échelle du réseau nécessaires aux entreprises et aux autorités pour réduire le risque de menaces complexes prolongées et d'attaques ciblées. Deep Discovery reconnaît et identifie les menaces camouflées de manière individuelle et en temps réel. Ensuite, une analyse complète et des informations importantes sont transmises afin de stopper les attaques visant les données d'entreprises, de les découvrir et de les limiter.

Deep Discovery comprend :

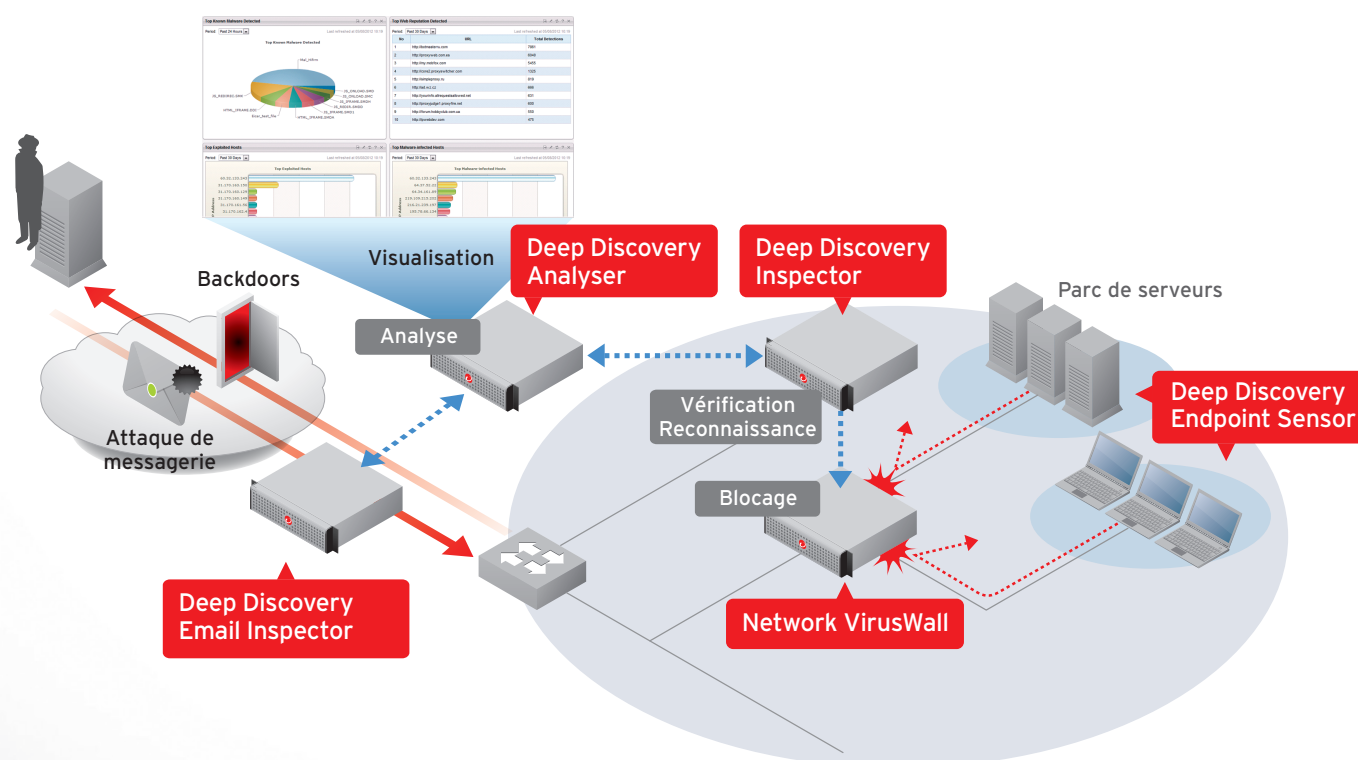
- Deep Discovery Inspector
- Deep Discovery Analyser
- Deep Discovery Endpoint Sensor
- Deep Discovery Email Inspector

Avantages

- **Reconnaissance d'attaques complexes et ciblées (APT)**
 - Réduit le risque de dégâts et de pertes de données causés par les menaces complexes et ciblées
- **Transparence à l'échelle du réseau**
 - Clarifie votre profil de sécurité réel
- **Analyses et aperçus complets**
 - Livre des informations en temps réel sur la classification et l'élimination des menaces
- **Possibilité d'intégration**
 - Fournit des mises à jour de sécurité en fonction des résultats et les transmet à d'autres solutions de sécurité. Celles-ci améliorent la reconnaissance et le blocage des menaces à l'échelle de l'entreprise.

Fonctionnement de Deep Discovery

	Reconnaissance des attaques	Méthodes de reconnaissance
Contenus malveillants	<ul style="list-style-type: none"> • E-mails comprenant des exploits intégrés aux documents • Attaques par téléchargements intempestifs • Attaques de type « zero-day » et menaces connues 	<ul style="list-style-type: none"> • Décodage et décompression de fichiers intégrés • Simulation sandbox de fichiers suspects • Reconnaissance de kits d'exploits dans les navigateurs • Recherche de programmes malveillants (signature et heuristique)
Communication suspecte	<ul style="list-style-type: none"> • Communication C&C pour tous types de programmes malveillants : zombies, téléchargeurs, vers, programmes malveillants de vol de données et menaces complexes • Activités de backdoor du pirate 	<ul style="list-style-type: none"> • Analyse des objectifs (URL, IP, domaine, e-mail, canal IRC etc.) au moyen de listes noires et de listes blanches dynamiques • Évaluation de la réputation des URL grâce à Smart Protection Network • Règles sur les critères de communication
Comportements d'attaque	<ul style="list-style-type: none"> • Activités des programmes malveillants : propagation des spams et des programmes malveillants, téléchargements, etc. • Activités des cybercriminels : recherche automatique, force brute, exploitation de services, etc. • Extorsion de données 	<ul style="list-style-type: none"> • Analyse heuristique basée sur des règles • Identification et analyse de l'utilisation de centaines de protocoles et d'applications, y compris les applications HTTP



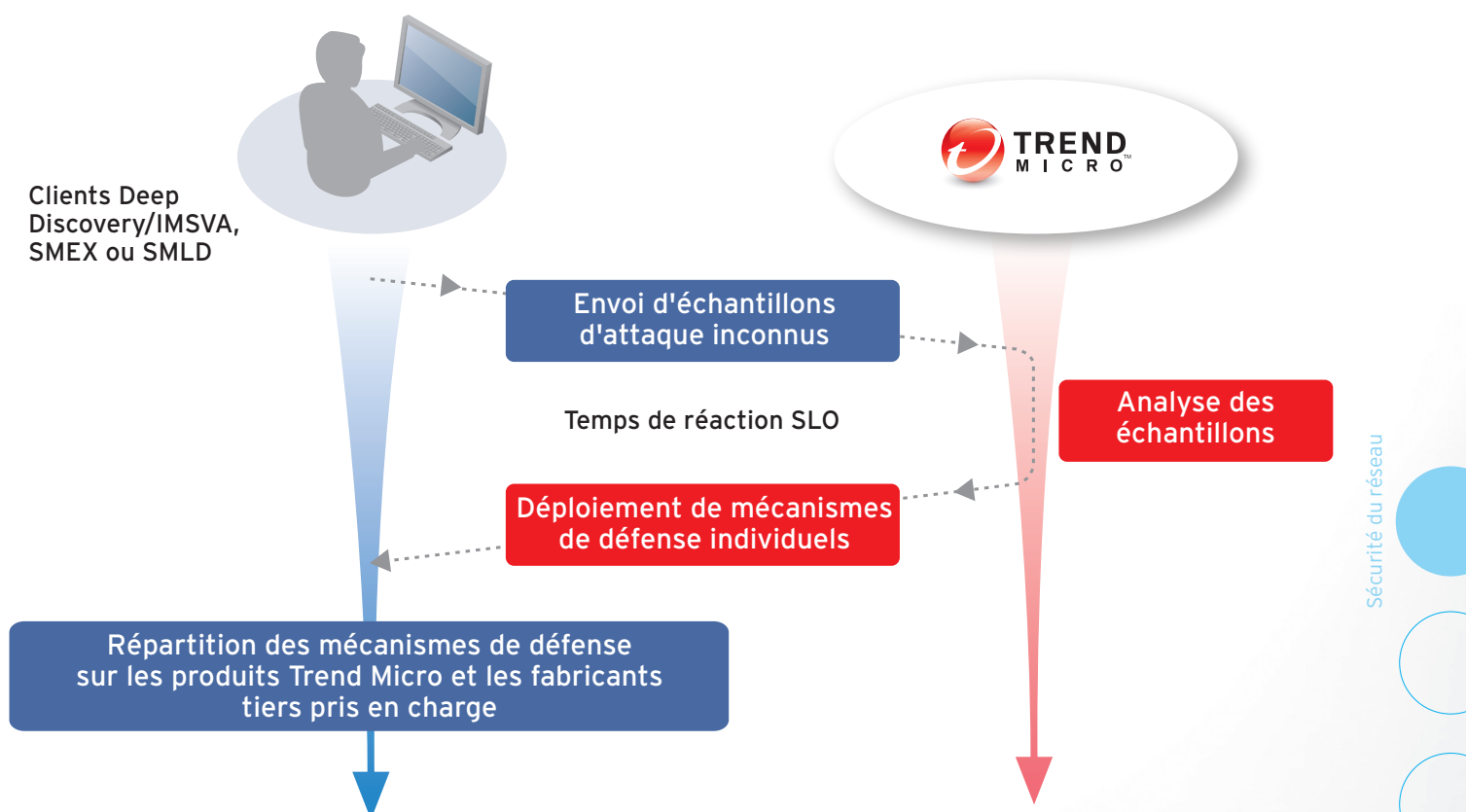
Custom Defense - Solution Trend Micro pour une protection flexible contre les menaces inconnues

Les menaces complexes et ciblées (APT) visent des entreprises bien définies. Ces entreprises doivent relever des défis ambitieux, à savoir être capables de reconnaître ces nouvelles menaces et mettre en place des contre-mesures appropriées.

La solution Custom Defense de Trend Micro identifie et analyse les menaces inconnues. Elle génère des informations pour la défense et les communique aux systèmes connectés pour établir une protection individuelle.

Avantages

- Déploiement de mécanismes de défense individuels grâce à Custom Defense
- Objectifs de niveau de services (Service Level Objectives, SLO) compris dans une période de réaction prédéfinie
- Utilisation efficace de la technologie sandbox de Deep Discovery

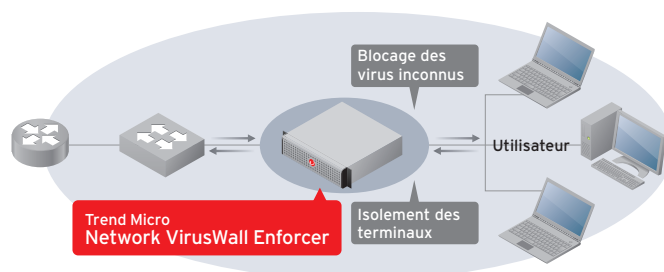


Network VirusWall Enforcer

Trend Micro Network VirusWall Enforcer protège le réseau de l'entreprise, en garantissant que tous les terminaux respectent les directives de sécurité de l'entreprise avant d'accéder au réseau. Cette solution NAC sans agent scanne chaque terminal, géré ou non, local ou à distance, pour obtenir l'état de sécurité actuel et identifier les patchs critiques de Microsoft. Les terminaux qui ne respectent pas les directives sont automatiquement mis en quarantaine et redirigés vers un processus d'élimination de défauts. Si un terminal remplit les conditions préalables de sécurité, l'accès au réseau lui est autorisé. De plus, Network VirusWall Enforcer filtre le trafic réseau pour reconnaître et bloquer les vers de réseau, sans fausse alarme. L'appliance simple à gérer isole les domaines infectés du reste du réseau, empêchant ainsi la propagation des menaces.

Avantages

- Réduit les risques de sécurité
- Contrôle chaque terminal
- Protège le trafic réseau
- Minimise les dégâts
- Facilite la gestion



Integrated Data Loss Prevention

Trend Micro Integrated Data Loss Prevention (iDLP) simplifie grâce à la gestion centralisée des stratégies la sécurité des données sur plusieurs niveaux de l'infrastructure de sécurité informatique existante. Il simplifie l'administration et assure une application homogène, renforçant ainsi la sécurité des données et le respect des exigences de conformité tout en minimisant les efforts et les coûts.

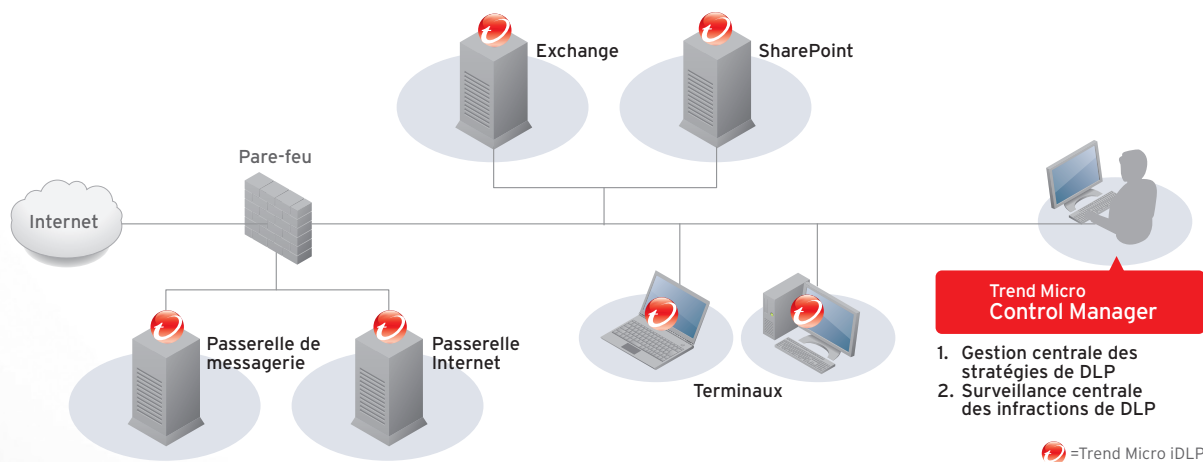
Avantages

• Integrated Data Loss Prevention

- Les fonctions de sécurité des données intégrées dans les solutions de sécurité traditionnelles (des solutions pour terminaux aux solutions pour réseaux en passant par les solutions pour messagerie) simplifient l'implémentation et réduisent les coûts pour l'infrastructure tout en vous offrant l'assurance que les données sont protégées.

Avantages (suite)

- Gestion des stratégies de DLP centralisée
 - La configuration et l'application centrales de modèles de stratégies prédéfinis au niveau de chaque couche de protection réduisent les efforts de gestion à court et long terme et assurent une application homogène des stratégies dans toute l'entreprise.
- Affichages et rapports consolidés personnalisables
 - Des journaux, rapports et affichages de tableau de bord récapitulatifs offrent un aperçu de toute l'entreprise en temps réel et permettent de contrôler les fuites de données et les infractions en matière de protection des données.



10 SÉCURITÉ CLOUD

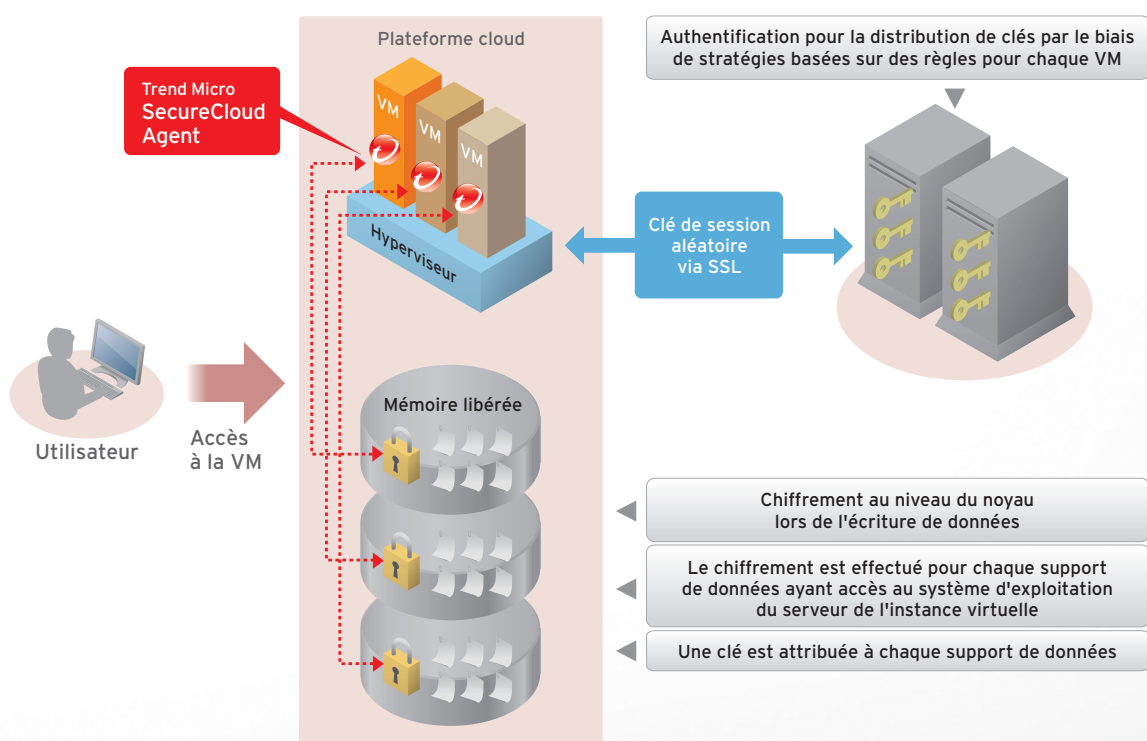
SecureCloud

De plus en plus d'entreprises adoptent le cloud computing et la virtualisation pour réaliser des économies de coûts et profiter d'une disponibilité et d'une flexibilité accrues. Mais ces avantages s'accompagnent d'une augmentation des risques pesant sur la protection des données et la sécurité. Les entreprises ne savent pas toujours où se trouvent leurs données et qui y a accès.

Trend Micro SecureCloud assure une protection particulière des données dans les environnements virtuels et basés sur le cloud grâce au chiffrement avec gestion des clés basée sur des stratégies et à une fonction de validation de serveur unique. Il est ainsi possible de protéger de manière sûre et simple les données confidentielles enregistrées sur les serveurs des principaux fournisseurs de services cloud, tels qu'Amazon EC2, DELL, Eucalyptus ou encore VMware vCloud ou tout autre environnement virtuel. SecureCloud protège les informations confidentielles dans les environnements virtuels et basés sur le cloud face au vol, à l'accès non autorisé ou aux migrations géographiques non autorisées vers d'autres data centers. Cette protection facilite la gestion des activités et assure la conformité aux exigences de Sarbanes-Oxley, PCI DSS, HIPAA, HITECH et GLB, entre autres. En outre, SecureCloud est certifié conforme à la norme FIPS 140-2. Il répond ainsi aux besoins des autorités et des entreprises soumises à des normes de sécurité contraignantes.

Fonctions et avantages

- **Techniques de sécurité avancées**
 - Offre la certification FIPS 140-2 et un chiffrement AES conforme aux FIPS
 - Assure le chiffrement et le déchiffrement en temps réel des informations de telle sorte que les données enregistrées sont constamment protégées
 - Permet le chiffrement de supports de données complets et protège ainsi toutes les données, métadonnées et structures associées sans affecter la fonctionnalité des applications
- **Contrôles d'accès et d'authentification**
 - Différencie clairement les tâches à l'aide de la gestion à base de rôles
 - Automatise la validation des clés et l'autorisation des machines virtuelles afin d'accélérer le déroulement des activités ou exige l'autorisation manuelle afin d'augmenter la sécurité
 - Permet le changement des droits d'accès pour les fournisseurs de cloud
- **Gestion des clés basée sur des stratégies**
 - Exploite l'application des stratégies basée sur l'identité et l'intégrité pour assurer que seules les machines virtuelles autorisées puissent obtenir des clés ou accéder à des supports de données sécurisés
 - Permet l'utilisation de stratégies pour déterminer quand et où des accès aux informations ont lieu
- **Audits, rapports et mises en garde complets**
 - Journalise les activités dans la console de gestion à des fins de contrôle
 - Offre des fonctions complètes de génération de rapports et d'avertissements avec notifications basées sur les événements et les intervalles



DEEP SECURITY for WEB APPS

Les entreprises adoptent de plus en plus d'applications Web pour offrir leurs services à leurs employés, partenaires et clients. Cette pratique contribue à renforcer le paysage des menaces et entraîne des défis de sécurité de plus en plus complexes, aggravés par l'accès facilité aux applications Web dans le cloud ou le data center par un grand nombre de nouveaux dispositifs mobiles.

La recherche de failles se limite traditionnellement à la reconnaissance d'attaques de réseau à faible niveau alors que les menaces actuelles sont sophistiquées et diversifiées. Les tests au niveau de l'application ne sont que rarement voire jamais effectués, ce qui augmente le nombre de failles et les risques.

En effet, la plupart des entreprises sont exposées à des menaces difficiles à reconnaître et contre lesquelles elles ont du mal à se protéger. En outre, la gestion des fausses alertes et la lutte permanente contre les menaces sont coûteuses et chronophages.

La solution Deep Security for Web Apps a été spécialement conçue pour faire face à la complexité du paysage actuel de menaces et propose des options de sécurité intégrées en une solution complète afin de reconnaître les menaces et les failles et de protéger les applications Web.

Avantages

- **Scan des applications pour repérer les failles**
 - Reconnaît les failles des applications Web sans fausse alerte parasite.
- **Tests de logique de gestion effectués par des experts**
 - Couvre les failles de la logique des applications avec l'aide des experts en sécurité de Trend Micro et établit des preuves exhaustives des failles exploitées.
- **Scan de plateforme**
 - Reconnaît les failles de sécurité importantes au niveau de la plateforme et effectue des recherches dans le système d'exploitation et sur les serveurs Web et d'applications.
- **Protection automatique**
 - Couvre les failles avant qu'elles ne puissent être exploitées et évite le patching d'urgence, les problèmes de mise à jour des applications et les interruptions coûteuses du système.
- **Sécurité SSL rentable**
 - Certificats SSL illimités, comprenant les certificats Extended Validation, pour la protection des transactions et pour votre sérénité.
- **Conformité**
 - Scanne en permanence les applications et assure le respect des exigences des directives PCI, DSS, HIPAA parmi d'autres.

DEEP SECURITY for WEB APPS



Trend Micro Control Manager

Simplifiez la gestion des solutions de sécurité Trend Micro avec la dernière version de Control Manager. Cette console de gestion à interface Web surveille la sécurité, signale les incidents de programmes malveillants et les infractions aux stratégies, et automatise les tâches de routine. Les nouvelles fonctions comprennent un tableau de bord personnalisable et offrent un aperçu rapide des statistiques sur les menaces grâce à Trend Micro Smart Protection Network, l'infrastructure de sécurité en ligne de Trend Micro.

Avantages

- **Diminution des risques**
 - Transparence et contrôle de la sécurité
- **Baisse des coûts**
 - Simplifie la gestion de la sécurité
- **Réduction de la complexité**
 - Constitue un système de sécurité intégré à gestion centralisée avec fonctions de défense uniques

Control Manager est disponible en deux versions : Standard et Advanced

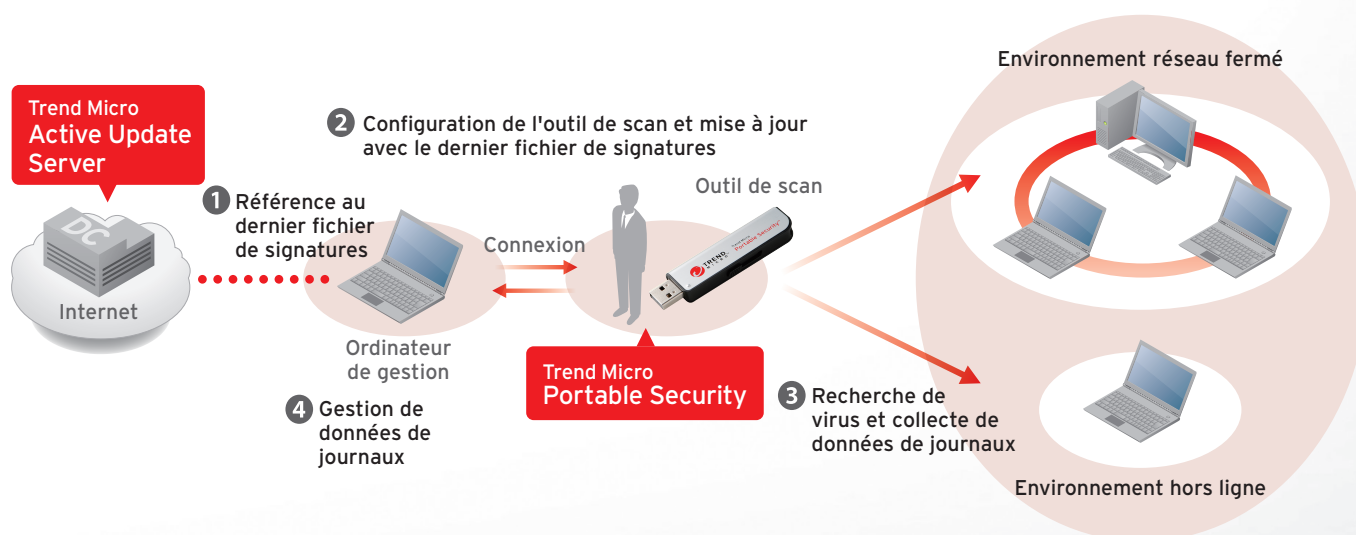
Trend Micro Control Manager	Standard	Advanced
Gestion de la sécurité centralisée à interface Web	●	●
Tableau de bord personnalisable, requête adaptée aux besoins, mises en garde	●	●
Statistiques sur les menaces par Smart Protection Network	●	●
Transparence des clients		●
Gestion multicouche		●
Génération de rapports personnalisable		●
Gestion des licences		●

Portable Security

Trend Micro Portable Security est un nouveau concept de produit antivirus prévu pour les environnements où l'installation d'un antivirus peut s'avérer difficile : environnements de fabrication, cabinets médicaux, institutions publiques ou écoles. Portable Security permet aux responsables informatiques de rechercher et d'éliminer les virus grâce à une clé USB, même en l'absence de connexion Internet.

Avantages

- Utilisable rapidement et évolutif dans le temps ; aucune installation nécessaire
- Exécution sur une clé USB ; aucune installation nécessaire
- Recherche et élimine les virus à l'aide des derniers fichiers de signatures
- Journalise les activités de recherche ; inclut la gestion des données natives de journaux
- Mises à jour effectuées depuis un ordinateur de gestion centralisée



Services

Grâce à son système mondial de service et d'assistance, Trend Micro est le mieux placé pour aider ses clients nationaux et internationaux à répondre aux exigences croissantes de la sécurité informatique. Nos services s'appuient sur des méthodes éprouvées et vous permettent de profiter pleinement des produits et solutions Trend Micro tout en protégeant vos investissements à long terme. Nos prestations de services couvrent le cycle de vie complet de nos solutions et s'étendent du conseil (PLANIFIER) à l'exploitation (EXÉCUTER) en passant par l'assistance lors de l'installation (ÉLABORER) et aux services, dont l'objectif est l'optimisation de nos solutions, le renforcement de la sécurité et la réduction des frais administratifs (OPTIMISER).

Le réseau de service et assistance Trend Micro est présent dans le monde entier : sur chaque continent sur trouvent des spécialistes de Trend Micro pour tous les produits et services. Trois centres d'assistance mondiaux sont à l'origine de nos prestations de services. Soumis au principe du « suivi du soleil » (follow the sun), ils assurent une assistance de qualité 24 h/24 pour vos environnements critiques. Outre les spécialistes de Trend Micro, faites confiance aux partenaires de services certifiés pour la prestation de services de conseil et de déploiement.



Services de conseil

Dans un contexte de cycles d'innovation courts des technologies et de paysage des menaces en évolution permanente, l'offre de solutions de sécurité informatique s'est diversifiée. Ce marché très compétitif impose de préparer, d'arrêter et de réaliser les choix d'investissement sur des périodes de plus en plus courtes. Grâce à nos services de conseil, profitez des connaissances et de l'expérience de nos experts techniques pour atteindre vos objectifs.

Nos consultants travaillent en étroite collaboration avec votre équipe informatique pour planifier et concevoir votre infrastructure de sécurité :

- Après un bilan détaillé, des experts vous assistent pour les étapes techniques difficiles et développent des solutions d'avenir qui répondent à vos exigences ainsi qu'une architecture parfaitement adaptée à vos besoins pour maximiser l'efficacité des solutions Trend Micro.
- Dans le cadre de nos démonstrations de faisabilité et de technologies, nous vous prouvons les avantages des solutions Trend Micro dans un environnement de test. Nos experts vous montrent et vous expliquent chaque fonction selon vos exigences individuelles. Vous observez ainsi des résultats concrets avant même de passer par une implémentation complète.

Services de déploiement de technologies

Nos services de déploiement sont conçus pour vous aider à implémenter de nouveaux produits en toute simplicité ou à mettre à niveau les solutions déjà présentes dans votre infrastructure informatique. Objectif ? Garantir un retour sur investissement maximal. Notre équipe analyse les exigences de performances de votre environnement système et réseau, ainsi que vos stratégies de sécurité. À partir de procédures éprouvées, nos consultants élaborent avec vous un projet de mise en œuvre. Pour les projets de grande envergure, la mise en œuvre est supervisée par un gestionnaire de projet expérimenté, qui coordonne les ressources nécessaires et surveille en permanence l'avancée du projet. Une fois le projet de mise en œuvre autorisé, la solution est alors implémentée conformément à vos exigences de gestion des changements. L'implémentation prend généralement fin avec l'exécution d'un test d'acceptation pour évaluer le bon fonctionnement des composants de la solution au sein de votre environnement.

Formations

Notre programme complet de formations vous aide à découvrir et maîtriser l'installation, la configuration et l'administration de vos solutions Trend Micro. Nos cours sont dispensés par des professionnels qualifiés dans des centres de formation chez Trend Micro ou nos partenaires de formation. Ils englobent des savoirs théoriques ainsi que des exercices de laboratoire permettant de mettre en pratique les connaissances acquises. Notre offre de cours couvre l'ensemble de notre portefeuille de produits, depuis les formations sur les terminaux et sur la sécurité mobile jusqu'aux solutions de protection contre les attaques ciblées en passant par la sécurité de virtualisation et du cloud. Nos formations vous aident à réduire les tâches administratives, à améliorer la gestion des failles au sein de l'entreprise, à minimiser les risques et à renforcer la protection générale de votre entreprise.

Services d'assistance

Trend Micro vous propose un large choix de prestations d'assistance, fournies soit directement, soit par l'intermédiaire d'une entreprise mandatée par Trend Micro.

Assistance Foundation Support

L'assistance Foundation Support est une assistance gratuite directe de niveau 1 destinée aux clients de produits Trend Micro pour un maximum de 250 utilisateurs par produit.

Assistance Select/Select+ Support

Si vous êtes une entreprise moyenne comptant entre 250 et 2 500 utilisateurs, vous pouvez profiter de prestations de services directes supplémentaires avec Select et Select+ Support. Vous aurez alors directement accès à nos techniciens d'assistance de niveau 2. Vous pourrez ouvrir des dossiers d'assistance par téléphone ou via l'outil de gestion en ligne des cas, accéder à la messagerie instantanée d'assistance ou au besoin bénéficier de l'aide d'un technicien à distance. Avec le service Select+ Support, ces possibilités sont même disponibles 24 h/24, 7 j/7.

Les services Trend Micro Select/Select+ Support sont disponibles pour Worry-Free Business Security et les solutions pour grandes entreprises. Les versions suivantes sont disponibles :

- **Select/Select+ pour Worry-Free**
- **Select/Select+ pour les produits pour grandes entreprises**

- **Select+ pour le module anti-programmes malveillants de Deep Security**
- **Select+ pour tous les autres modules Deep Security**

Trend Micro Select Support EMEA

Assistance technique	Foundation	Select	Select+
Numéro de téléphone local	✓		
Appel gratuit		✓	✓
Temps d'attente	60 sec.	30 sec.	30 sec.
Disponibilité	9:00 - 18:00	9:00 - 17:30	24 h/24, 7 j/7
Niveau d'assistance	Niveau 1	Niveau 2	Niveau 2
Délai de réponse pour un dossier en ligne	1,5 jour	4 heures de travail	4 heures
Messagerie instantanée		✓	✓
Accès à distance		✓	✓
Assistance par e-mail contre les programmes malveillants*	✓	✓	✓
Assistance téléphonique contre les programmes malveillants		✓	✓
Accès au service client		✓	✓
Accès à l'historique des événements		✓	✓

Foundation correspond à l'assistance directe pour PME de niveau 1
 * Disponible uniquement en anglais avec l'assistance Foundation

Les services Select/Select + Support sont vendus à un prix unitaire en fonction du nombre d'utilisateurs, quel que soit le nombre de solutions que vous utilisez. C'est également le cas pour les produits achetés ultérieurement (sauf pour Deep Security, Deep Discovery et les produits pour particuliers). Les services Select/Select + Support peuvent être achetés à tout moment. Toutefois, nous recommandons de coupler leur achat à celui des licences afin que les dates d'expiration coïncident.

Premium Support

Évaluer et gérer les menaces avancées persistantes et autres attaques dans les environnements mobiles et cloud est un combat de tous les instants. Maximisez la valeur de votre solution de sécurité Trend Micro avec Trend Micro Premium Support. Vous aurez un accès direct au savoir des experts du service mondial d'assistance Trend Micro, 7 j/7, 24 h/24, basé sur des accords de niveau de service (SLA) et des services d'informations proactifs supplémentaires grâce à notre programme Premium Support (PSP).

Gestion de comptes technique

Avec les services de gestion technique de comptes par Trend Micro, vous êtes sûr que votre infrastructure informatique est prise en charge et protégée. Vous bénéficiez d'un accompagnement personnalisé par un chargé de clientèle technique (TAM) dans le cadre du programme Premium Support. Le TAM est votre interlocuteur pour tous vos besoins d'assistance. Son rôle est de représenter vos intérêts au sein de l'organisation Trend Micro et de garantir que les composants essentiels du programme Premium Support sont bien mis en œuvre conformément à vos besoins et que leur efficacité vous satisfait.

Nos experts en sécurité bénéficient d'une formation complète pour vous aider à réagir face aux menaces et à planifier, préparer et optimiser les solutions de sécurité de manière ciblée.

Le chargé de clientèle technique s'appuie sur votre environnement informatique, sur vos processus d'entreprise et sur l'état de votre sécurité pour vous garantir un retour sur investissement optimal en fonction de nos solutions de sécurité. Il vous aide à identifier et régler rapidement les problèmes afin d'optimiser la disponibilité et le fonctionnement de votre solution de sécurité. Le chargé de clientèle technique peut faire appel à des spécialistes internes pour trouver une solution ciblée aux problèmes critiques et complexes. Plus de 1 500 ingénieurs et experts en sécurité TrendLabs sont à votre disposition dans le monde.

Les performances du chargé de clientèle technique peuvent se résumer ainsi :

- Compréhension approfondie de votre architecture informatique, de vos processus d'entreprise et de vos objectifs afin d'optimiser les performances de la solution Trend Micro mise en place et de maximiser la durée de vie de la protection
- Évaluations de sécurité, recommandations et informations proactives sur les menaces critiques
- Assistance lors de la consolidation de l'architecture de sécurité et conseils qualifiés pour faciliter l'identification précoce et le traitement des problèmes
- Observation et réglage rapides des problèmes éventuels d'assistance par la mobilisation de ressources adéquates

Le prix de Premium Support dépend du niveau de service ainsi que du nombre de régions et de contacts pris en charge. Le nombre de solutions et de licences que vous possédez n'est pas pris en compte. Vous pouvez acquérir les services Premium à tout moment. Toutefois, nous vous recommandons de coupler leur achat à celui des licences afin que les dates d'expiration coïncident. Vous trouverez un tableau récapitulatif des performances de Premium Support à la page suivante.

Services d'optimisation

Les services d'optimisation contribuent d'une part au bon déroulement de l'installation et du fonctionnement des produits Trend Micro. D'autre part, ils permettent une évaluation et une amélioration permanente de votre architecture de sécurité en fonction de vos stratégies informatiques actuelles. Dans le cadre des services d'évaluation, vous êtes informé de l'état actuel de la sécurité de votre réseau et de vos données via l'étude des infections potentielles, l'identification des pertes de données et l'évaluation des zones à risque. Après l'analyse et l'évaluation des résultats, nous vous fournissons des conseils concrets et réalisables pour traiter les problèmes observés et améliorer votre niveau de sécurité.

• Évaluation de sécurité face aux menaces avancées persistantes (APT)

- Les attaques complexes et ciblées, ou menaces avancées persistantes (APT), agissent souvent en plusieurs phases, chacune se déroulant généralement en arrière-plan à votre insu. Les tendances du monde du travail moderne, comme la consommation (ou BYOD pour « Bring your own device ») et l'utilisation de dispositifs mobiles par les employés au sein de réseaux extérieurs, accroissent le risque d'exposition aux menaces. La grande complexité des attaques empêche souvent les utilisateurs de se rendre compte qu'ils en sont victimes. La plupart du temps, ils n'en comprennent les conséquences que trop tard. Nos experts analysent votre environnement informatique et déterminent dans quelle mesure votre entreprise est menacée ou infectée.

• Bilans de santé

- Les bilans de santé visent à vérifier et à optimiser les solutions Trend Micro sur les systèmes ou dans les environnements virtuels afin d'identifier et de résoudre les problèmes de sécurité, de performances ou de disponibilité avant qu'ils n'affectent vos activités.

Programme Premium Services

Contact direct avec l'assistance Trend Micro

Contact dédié direct ou TAM (chargé de clientèle technique)

TAM local en Allemagne/Autriche/Suisse

Accès en ligne 24 h/24, 7 j/7, 365 jours/an

Soutien via la messagerie instantanée, le Web et Remote Desktop

Assistance, notamment téléphonique, dans la langue locale (angl./all./fr.) lors des heures de bureau (9:00 - 17:00)

Assistance, notamment téléphonique, dans la langue locale (angl./all./fr.) en dehors des heures de bureau (24 h/24, 7 j/7, 365 jours/an)

Contact téléphonique au cas par cas

Nombre de contacts/interlocuteurs du côté du client

Conseils de sécurité et assistance proactifs et spécifiques aux clients

Notifications proactives concernant les menaces

Création d'un profil client spécifique

Gestion proactive du cycle de vie (patch/disponibilité de SP)

Soutien lors de la planification et de l'utilisation de produits Trend Micro

Conseils lors de la mise en œuvre de procédures éprouvées

Assistance d'urgence sur place

Visites sur place (techniques, examen de cas, etc.)

Conférences téléphoniques (avec TAM)

Cas gérés en priorité et de manière accélérée

Équipes d'assistance primaire EMEA/DACH (Allemagne, Autriche, Suisse)

Gestion des cas de virus via la console Premium Support (PSC) (envoi prioritaire des fichiers suspects via le portail)

Délais internes plus courts pour les cas de produits

Contrat de niveau de service de réaction au virus : fichier de signatures de virus renvoyé dans les 2 heures

Accès élargi direct aux informations actualisées et connaissances techniques d'experts

Ressources en ligne élargies (en cours d'activation)

Outil de gestion des cas (PSC)

Base de connaissances Premium

Guides de meilleures pratiques

Documentation de niveau 3

Participation aux PSP Tech Days

Participation aux ateliers de migration

Early Trend Adaptor Programme (programme des adeptes de la première heure)/ETAP

Régions géographiques couvertes

Nombre de régions contractuellement couvertes

Contrat extensible au TAM dans une autre région

Prise de contact avec TAM dans une autre région

TAM global en tant que coordinateur central



BRONZE	ARGENT	OR	PLATINE	DIAMANT
Équipe de TAM	TAM personnel	TAM personnel	TAM personnel	TAM exclusif
✗/Europe	✓	✓	✓	✓
✓	✓	✓	✓	✓
✓	✓	✓	✓	✓
✓	✓	✓	✓	✓
✗	✗	✓	✓	✓
✓	✓	✓	✓	✓
2	4	6	8	10
✓/voie électronique	✓/TAM	✓/TAM	✓/TAM	✓/TAM
✗	✓	✓	✓	✓
✗	✓	✓	✓	✓
✗	✓	✓	✓	✓
✗	✓	✓	✓	✓
✗	✗	✓/2 x par an	✓/2 x par an	✓/4 x par an
✗	✓/1 x par an	✓/2 x par an	✓/4 x par an	✓/TAM sur place
✗	✓/3 x par an	✓/6 x par an	✓/12 x par an	✓/TAM sur place
✓	✓	✓	✓	✓
✓	✓	✓	✓	✓
✗	✗	✓/selon le SLO interne	✓/selon le SLO interne	✓/selon le SLO interne
✗	✗	✓	✓	✓
✓	✓	✓	✓	✓
✓	✓	✓	✓	✓
✓	✓	✓	✓	✓
✓	✓	✓	✓	✓
✗	✗	✓	✓	✓
✗	✗	✓	✓	✓
✗	✗	✓	✓	✓
✗	✗	✗	✓	✓
1/Europe	1	1	3	1
✗	✗	✓/1 région suppl. Région	✓	✓
✗	✗	✗	✓	✓
✗	✗	✓	✓	✓

PALIER DE LICENCE

Les licences sont concédées par paliers :

5 - 250 utilisateurs :	par paliers de 5
251 - 1 000 utilisateurs :	par paliers de 10
1 000 utilisateurs et plus :	par paliers de 25

Exemple : Pour 573 comptes de messagerie, on arrondit à la dizaine d'utilisateurs supérieure (en l'occurrence 580). Veuillez noter que l'échelonnement commence à 26 utilisateurs pour les produits pour grandes entreprises.

CONCESSION DE LICENCES DE PRODUITS POUR PME

Les produits Trend Micro pour PME sont disponibles pour 5 utilisateurs minimum.

Exceptions : Worry-Free Business Security Services est disponible à partir de 2 utilisateurs et ses licences peuvent être achetées par paliers d'1 utilisateur. SafeSync for Business est disponible à partir de 3 utilisateurs et ses licences peuvent être achetées par paliers d'1 utilisateur.

Produits Trend Micro Worry-Free : Le nombre de licences correspond au total clients + serveurs. Chaque machine virtuelle sur laquelle Worry-Free Business Security est installé est également prise en compte. La concession de licences est possible pour 5 à 250 utilisateurs.

Exemple : La société Modèle SARL souhaite utiliser Worry-Free Business Security Advanced pour protéger son réseau. La société compte 5 serveurs, 40 postes de travail et 30 employés. 45 utilisateurs recevront une licence.

Trend Micro SafeSync for Business : Le nombre de licences correspond au nombre d'utilisateurs. Pour chaque utilisateur, le volume de stockage sous licence est augmenté de 50 Go. La concession de licences est possible pour 3 à 100 utilisateurs.

CONCESSION DE LICENCES DE PRODUITS POUR GRANDES ENTREPRISES

Les produits Trend Micro pour grandes entreprises sont disponibles pour 26 utilisateurs minimum. Il n'y a pas de nombre maximal.

Une licence est concédée à chaque utilisateur ayant accès à un ordinateur connecté directement ou indirectement au serveur de réseau sur lequel le logiciel Trend Micro est installé. Cela s'applique également lorsqu'un ordinateur est utilisé par plusieurs utilisateurs à différents horaires. On peut déterminer le nombre de licences nécessaires en prenant par exemple le nombre de comptes individuels de messagerie. Le nombre de serveurs sur lesquels le produit est installé n'est pas pris en compte.

Premier exemple : La société Modèle SARL achète une solution de sécurité pour le serveur de messagerie Microsoft Exchange comptant 400 comptes individuels de messagerie. Elle acquiert donc ScanMail for Exchange avec une licence pour 400 utilisateurs (les comptes groupés tels que info@modele.com, vente@modele.com, etc. ne sont pas des comptes individuels).

Deuxième exemple : La société Modèle SARL acquiert la solution de sécurité Trend Micro Enterprise Security for Endpoints pour ses clients réseau. C'est le nombre d'utilisateurs à protéger qui est déterminant et non pas le nombre d'ordinateurs portables, de stations de travail ou de serveurs. Il y a 100 utilisateurs à protéger, pour 120 postes de travail ou ordinateurs portables. 100 utilisateurs se voient concéder une licence.

Concession de licences Deep Security : La concession de licences est fonction du nombre de postes de travail/serveurs virtuels. Sur demande, les licences peuvent aussi être concédées en fonction du nombre de processeurs.

Exemple : La société Modèle SARL souhaite protéger ses 4 serveurs ESX comptant chacun 2 processeurs avec Deep Security. Sur chaque serveur, 5 machines virtuelles sont installées. 20 machines virtuelles se voient concéder une licence.

AUTRES PRODUITS ET SERVICES

SecureCloud : Somme des unités chiffrées avec une clé autonome.

Select Support : En fonction du nombre d'agents. Selon l'utilisation, lors de l'acquisition, de la charge par le serveur (nombre de machines virtuelles) ou les postes de travail (nombre de machines virtuelles) fonctionnant en tant qu'hôtes sur l'hyperviseur.

PREMIER ACHAT

Un premier achat correspond à la première acquisition par un client d'une licence Trend Micro ou d'un certain produit. La date d'achat correspond à la date de début de la licence. La durée d'une licence est toujours d'1 an. Si un contrat de licence pluriannuel est conclu, la première année est considérée comme celle du premier achat. Les années suivantes sont considérées comme une reconduction du contrat.

EXTENSION DE LICENCE

Une extension de licence désigne l'acquisition d'« utilisateurs » supplémentaires par un client disposant déjà d'une licence valide pour le produit concerné. La durée d'une extension de licence est de 12 mois à compter de la date de livraison.

Lors d'une extension de licence, le client peut éventuellement atteindre un palier supérieur du nombre d'utilisateurs ; il se voit alors offrir un prix unitaire réduit. La facturation de l'extension de licence s'effectue toujours en deux étapes :

- 1^{ère} étape :** Le nombre de nouveaux utilisateurs est ajouté au nombre d'utilisateurs existants.
- 2^{ème} étape :** Pour l'augmentation du nombre de licences, c'est le prix unitaire du volume total qui sert de base.
- 3^{ème} étape :** Pour obtenir une date d'expiration uniforme des anciennes et des nouvelles licences, la durée des licences existantes doit être prolongée de manière correspondante (calcul à hauteur de 2,5 % du prix répertorié pour chaque mois débuté (30 % par an) sur la base du prix unitaire du volume total).

RENOUVELLEMENT DE MAINTENANCE

Pour conserver les droits d'utilisation d'un produit Trend Micro, il est nécessaire de procéder au renouvellement annuel de maintenance avant l'expiration de la licence. Lors de la première année suivant l'installation (le premier achat), une maintenance de 12 mois est comprise dans le prix d'achat. La maintenance comprend les mises à niveau logicielles et les mises à jour du moteur de scan et des fichiers de signatures. Par la suite, les frais de maintenance sur 12 mois s'élèvent à 30 % (ou 35 % pour les solutions Worry-Free Business Security) du prix répertorié actuel concerné (exception : voir « Renouvellement de maintenance de services »).

La période d'une licence renouvelée débute le jour suivant la date d'expiration de la licence précédente. Cela s'applique également lorsque le client renouvelle sa licence après la date d'expiration de la licence précédente.

Exemple : La licence expire le 7 juillet :

- La période de la nouvelle licence débute le 8 juillet
- Si le client n'effectue le renouvellement de sa licence qu'en août, la période de la nouvelle licence aura tout de même débuté le 8 juillet.

RENOUVELLEMENT DE MAINTENANCE DE SERVICES

Les services Trend Micro reposent sur des frais annuels correspondant à 100 % du prix répertorié actuel. Ainsi, il n'y a pas de renouvellement de maintenance dans le sens classique du terme. C'est par exemple le cas pour les produits achetés dans le cadre du modèle xSP.

MISES À NIVEAU CROSS-UPGRADE

Une mise à niveau cross-upgrade a lieu lorsqu'un client passe d'un produit (ou d'une suite) Trend Micro à un(e) autre. Les produits Trend Micro déjà utilisés ou en cours de maintenance peuvent être facturés avec leur volume de licence. La maintenance du produit existant expire et débute à nouveau pour une durée de 12 mois à l'achat du pack de produits.

MISES À NIVEAU CROSS-GRADE

Une mise à niveau cross-grade a lieu lorsqu'un client passe d'une plateforme à une autre, par exemple de Trend Micro ScanMail for Exchange à Trend Micro ScanMail for IBM Domino. Dans un tel cas, les dates de début et d'expiration de la licence initiale restent inchangées. Des frais de changement à hauteur de 30 % du prix répertorié peuvent s'appliquer.

RÉDUCTIONS

Réduction pour les administrations (« e-government » ou administration en ligne) : Disponible pour les autorités nationales et locales, les municipalités, les bureaux, les administrations, les hôpitaux publics et les organisations appartenant à hauteur de 50 % au moins auxdites institutions, ainsi que les collectivités de droit public.

Réduction pour le secteur éducatif (organismes non gouvernementaux ou à but non lucratif) : Disponible pour tous les organismes non gouvernementaux ou à but non lucratif, les écoles et universités générales ou professionnelles, publiques ou reconnues par l'État, les instituts de formation pour adultes, publics ou reconnus par l'État, et autres institutions non commerciales (les églises et communautés religieuses, ainsi que les associations pouvant justifier leur caractère non commercial, comme par exemple la Croix-Rouge, les fédérations sportives, le CIO, l'Unicef).

Réduction pour migration concurrentielle : En cas de remplacement d'un ou plusieurs produits payants comparables d'un concurrent, Trend Micro concède une réduction de prix. Une preuve de licence du produit concurrent doit être fournie au plus tard lors de la commande.

ÉVALUATION DES LICENCES

Chaque licence peut faire l'objet d'une évaluation gratuite de 30 jours. Au besoin, une clé d'évaluation peut être fournie pour une période plus longue. Pour toute question, veuillez vous adresser à sales@trendmicro.fr en précisant les informations suivantes :

- | | | | |
|------------------------|--------------------------|-----------------------|------------------------|
| • Nom de revendeur | • Système d'exploitation | • Nom de client final | • Langue |
| • Période d'évaluation | • Version du produit | • Nom du produit | • Taille de la licence |

FUSION DE LICENCES AU SEIN D'UN GROUPE D'ENTREPRISES

Les licences de deux entreprises d'un groupe peuvent être regroupées ou modifiées au cours d'une période d'alignement de maintenance (produits correspondants avec une même date d'expiration). Dans ce cas, l'accord d'un employé de Trend Micro est nécessaire.

L'entreprise du groupe cédant ses licences au groupe doit fournir son accord par écrit.

DIVERS

Le contrat de licence de l'utilisateur final ou EULA (End User License Agreement) forme la base de la politique de concession de licences de Trend Micro <http://www.trendmicro.fr/apropos/politique-juridique/contrats-licences-utilisateurs/index.html>

Pour les grandes entreprises clientes, une adaptation des conditions peut être envisagée. Août 2014, sous réserve de modifications.

14 AUTRES

Enregistrement en ligne (OLR)

Trend Micro fournit avec les licences de produits des clés d'enregistrement (RK) destinées à la création de comptes et à l'enregistrement de produits. Après l'enregistrement, les utilisateurs doivent activer le logiciel avec un code d'activation (AC). Celui-ci leur permet d'accéder au serveur ActiveUpdate et de télécharger le dernier fichier de signatures.

L'enregistrement de produit Trend Micro doit être effectué par vous-même ou par un revendeur spécialisé à votre demande.

L'enregistrement en ligne permet l'activation d'un produit nouvellement acheté, le renouvellement d'un produit existant et la fusion de produits vendus en boîte. Cliquez sur ce lien pour accéder au site germanophone d'enregistrement en ligne :

<https://tm.login.trendmicro.com>

Webinaire et événements

Trend Micro organise régulièrement des webinaires et événements relatifs aux thèmes et produits d'actualité.

Pour en savoir plus : <http://www.trendmicro.fr/newsroom/events/index.html>

Versions d'essai – Programme bêta – Centre de mise à jour

Vous pouvez à tout moment tester les dernières solutions logicielles Trend Micro.

Pour ce faire, participez aux programmes et tests bêta.

Pour en savoir plus : <http://beta.trendmicro.com>

De plus, vous pouvez utiliser le Centre de mise à jour Trend Micro pour télécharger des versions de test ou de démonstration sur le site Web de Trend Micro. Vous avez généralement 30 jours pour tester le logiciel de votre choix. À l'issue de la période d'essai gratuite, vous pouvez acquérir une licence ou terminer l'évaluation. Pour toute demande de version d'essai, adressez-vous à votre revendeur spécialisé.

Pour en savoir plus : <http://downloadcenter.trendmicro.com>

Coordonnées Trend Micro

Équipe d'assistance technique : vous trouverez des informations générales sur l'assistance, par exemple le Centre de téléchargement ou la base de données d'assistance, à l'adresse www.trendmicro.com >>> « Assistance », dans le menu principal. Pour ouvrir un dossier d'assistance : <http://esupport.trendmicro.com/srf/SRFMain.aspx>

Trouvez un revendeur spécialisé via l'outil de recherche de partenaires Trend Micro

<https://partnerlocator.trendmicro.eu>



NOTES

Notes section with horizontal dotted lines for writing.





NOTES

20 horizontal dotted lines for taking notes.





Blank page with horizontal dotted lines for writing.





Trend Micro France

85, avenue Albert 1er
92500 Rueil-Malmaison
France
Tél. : +33 (0) 1 76 68 65 00
www.trendmicro.com



Copyright © 2014 Trend Micro Incorporated. Tous droits réservés. Trend Micro, le logo Trend Micro et le logo t-ball de Trend Micro sont des marques commerciales ou des marques déposées de Trend Micro Incorporated. Tous les autres noms de sociétés et/ou de produits peuvent être des dénominations sociales ou des marques déposées de leurs propriétaires respectifs. Les informations contenues dans ce document peuvent être modifiées sans préavis. Trend Micro, le logo Trend Micro et le logo t-ball portent le symbole de marque déposée des États-Unis.