Endpoint Protection Plus

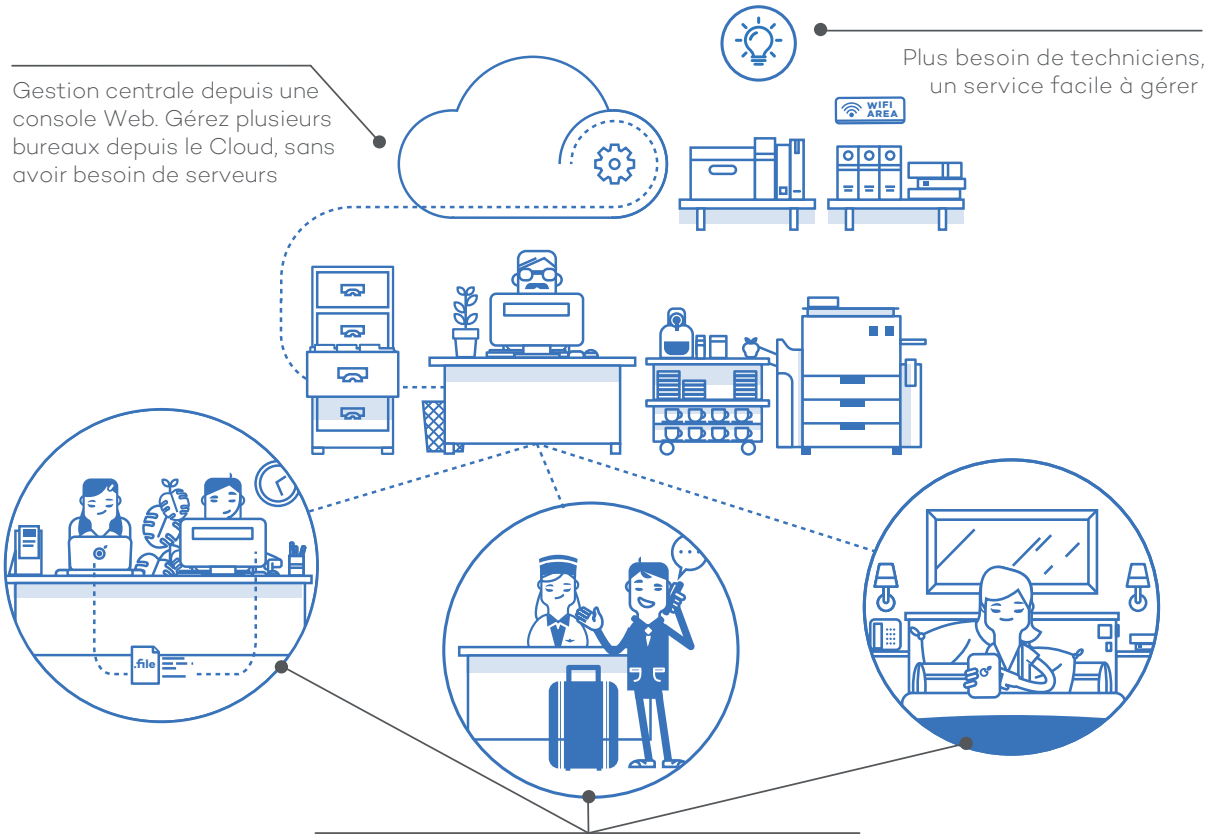
Solution de sécurité et de productivité simple et légère pour les terminaux

GÉREZ LA SÉCURITÉ DE TOUS LES ORDINATEURS DE VOTRE RÉSEAU ET CONTRÔLEZ LA PRODUCTIVITÉ DES UTILISATEURS AVEC UN COÛT DE POSSESSION RÉDUIT

Panda Security présente sa solution de sécurité et de productivité simple et légère: **Endpoint Protection Plus.** Le logiciel offre une protection centralisée et permanente pour tous vos postes de travail (Windows, Mac et Linux), y compris les ordinateurs portables et les serveurs ainsi que les plateformes de virtualisation les plus répandues.

La technologie **d'Intelligence Collective de Panda Security** protège en temps réel les postes de travail et les serveurs contre les cybermenaces et les exploitation frauduleuses des failles de sécurité logicielles non corrigées (0-day) sans nécessiter de serveurs supplémentaires ni d'infrastructure IT. En outre, la solution surveille et filtre le trafic Internet et le spam : la société peut ainsi se concentrer exclusivement sur son coeur de métier, sans avoir à se soucier du manque de productivité de ses employés.

Grâce à **Endpoint Protection,** la protection peut être gérée aisément depuis une console Web unique. La gestion centralisée est autorisée à tout moment et n'importe où, sans nécessiter de connaissances techniques.



Multiplateforme et mobilité

Protection complète qui couvre tous les vecteurs d'infection : protection du réseau (pare-feu), protection des emails, protection de la navigation Web, protection des terminaux mobiles

Sécurité simple et centralisée pour tous les appareils

Gestion centralisée de la sécurité et des mises à jour produit via un simple navigateur Web pour tous les serveurs et postes de travail du réseau. Gérez votre protection Windows, Linux, Exchange Server ou Mac OS X depuis une console d'administration unique.

Mesures correctives

Lancez à distance l'application Cleaner Monitor pour réparer les postes de travail infectés par des codes malveillants non conventionnels, ou inconnus.

Redémarrez les serveurs et les postes de travail à distance pour vous assurer qu'ils disposent bien des dernières mises à jour de produits.

Surveillance et rapport en temps réel

Surveillance détaillée de votre infrastructure IT en temps réel, grâce aux tableaux de bord complets et intuitifs.

Les rapports peuvent être générés et envoyés automatiquement, avec le détail du statut de la protection, les détections et l'utilisation inappropriée de ressources.

Protection basée sur le profil d'utilisateur

Appliquez des politiques de protection basées sur le profil afin que chaque groupe d'utilisateurs soit soumis aux mesures de protection les plus adaptées à sa spécificité.

Surveillance et filtrage du Web

Augmentez la productivité de vos utilisateurs pendant les heures de travail en empêchant et/ou surveillant l'accès aux contenus considérés comme dangereux ou improductifs, quel que soit le type de navigateur employé.

Dites adieu aux boîtes mail saturées

Réduisez le risque d'attaques sur vos serveurs Exchange avec la fonctionnalité de filtrage de contenu. Améliorez la productivité et la protection des utilisateurs finaux en filtrant les messages indésirables et malveillants avec les systèmes antimalware et antispam intégrés.

Malware Freezer

Ne soyez plus victime des faux positifs. La fonction Malware Freezer procède à une mise en quarantaine pendant 7 jours des codes malveillants détectés, juste au cas où il s'agirait d'un faux positif. Si cela est le cas, le fichier en quarantaine est automatiquement restauré dans le système.

Conforme aux normes ISO 27001 et SAS 70. Disponibilité 24/7 garantie

La solution est stockée sur Microsoft Azure et garantit une protection complète des données. Nos centres de données sont certifiés ISO 27001 et SAS 70.

CONFIGURATION MINIMALE REQUISE

Console Web

- Connexion Internet.
- Internet Explorer 10 / Microsoft Edge.
- Firefox (dernière version).
- Google Chrome (dernière version).

Pour les postes de travail et les serveurs de fichiers

- L'un d'entre eux au moins doit posséder une connexion Internet.
- Systèmes d'exploitation (postes de travail) : Windows XP SP2 (32 et 64-bits) et versions ultérieures, Vista, Windows 7 , Windows 8/8.1 (32 et 64 bits).Windows 10 (32 et 64 bits)..
- Systèmes d'exploitation (serveurs) : Windows 2003 (32, 64 bits et R2) SP1 et versions ultérieures, Windows 2008 (32 et 64 bits), Windows 2008 R2 (64 bits), Windows Small Business Server 2011, Windows Server 2012 (64 bits et R2) Windows Server 2016.

Serveur de messagerie

- Microsoft Exchange Server 2003, 2007, 2010, 2013 et 2016

Pour les postes de travail et les serveurs de fichiers Mc

- Mac OS X 10.6 Snow leopard
- Mac OS X 10.7 Lion
- Mac OS X 10.8 Mountain Lion
- Mac OS X 10.9 Mavericks
- Mac OS X 10.10 Yosemite
- Mac OS X 10.11 El Capitan
- Mac OS Sierra

Pour les postes de travail et les serveurs de fichiers Linux

- Ubuntu 12 (32/64 bits) et versions ultérieures
- Red Hat Enterprise Linux 6.0 (64 bits) et versions ultérieures
- CentOS 6.0 (64 bits) et versions ultérieures
- Debian 6.9 Squeeze et versions ultérieures
- OpenSuse 12 (32/64 bits) et versions ultérieures
- Suse Enterprise Server 11SP2 (64 bits) et versions ultérieures

Pour les appareils mobiles

- Android (version 4.0 ou ultérieur)

Moteurs de virtualisation compatibles :

- VMWare ESX 3.x,4.x, 5,x
- VMWare Workstation 6.0, 6.5, 7.x, 8.x et 9.x
- Virtual PC 6.x
- Microsoft Hyper-V Server 2008 R2 et 2012 3.0
- Citrix XenDesktop 5.x, XenClient 4.x, XenServer et XenApp 5.x, 6.x

Compatible avec :

Certifications :