



Endpoint Protection Plus

Solución de seguridad fácil y ligera

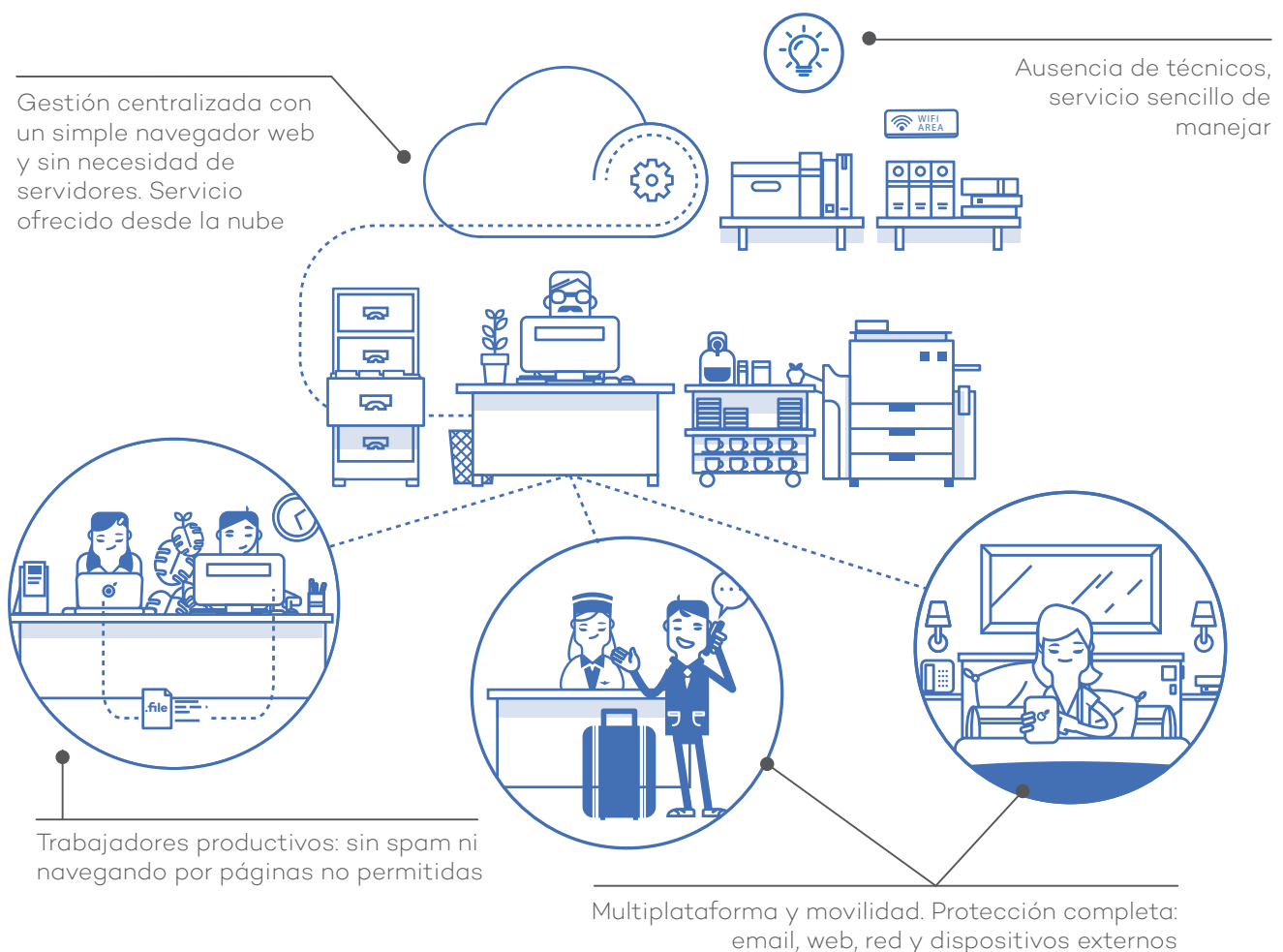


GESTIONA LA SEGURIDAD DE TODOS LOS EQUIPOS DE TU RED Y CONTROLA LA PRODUCTIVIDAD DE LOS USUARIOS AL MENOR COSTE DE PROPIEDAD POSIBLE

Panda Security te presenta su solución de seguridad y productividad fácil y ligera para el endpoint. **Endpoint Protection Plus** protege de forma centralizada e ininterrumpida todas tus estaciones de trabajo Windows, Mac y Linux, incluyendo equipos portátiles y servidores así como los principales sistemas de virtualización y dispositivos Android.

La tecnología “**Inteligencia Colectiva**” desarrollada por **Panda Security** protege en tiempo real todos los equipos de la red contra amenazas y exploits que aprovechan vulnerabilidades desconocidas (**zero-day**) sin necesidad de instalar servidores ni infraestructura de IT adicionales. Además monitoriza y filtra el tráfico web y el spam de forma que la empresa podrá centrarse en su negocio y olvidarse de los comportamientos improductivos de los trabajadores.

Con **Endpoint Protection Plus** la protección se gestiona cómoda y fácilmente desde una única consola Web, permitiendo una administración centralizada en cualquier momento y desde cualquier lugar y sin requerir de conocimientos técnicos.



Seguridad sencilla y centralizada para todos los dispositivos

Gestión centralizada de la seguridad y de las actualizaciones del producto con un simple navegador web para todos los puestos y servidores de la red. Controla la protección de equipos Windows, Linux, servidores Exchange, Mac OS X o Android desde una misma consola de administración.

Acciones de remediación

Ejecuta de forma remota Cleaner Monitor y repara los puestos de trabajo infectados por malware avanzado o no convencional.

Reinicia remotamente estaciones y servidores para garantizar la actualización a la última versión del producto.

Monitorización en tiempo real e informes

Monitorización detallada de la seguridad del parque informático en tiempo real a través de completos dashboards y gráficas de rápida interpretación.

Generación y envío automático de informes sobre el estado de la protección, las detecciones, y el uso inadecuado de dispositivos.

Configuración por perfiles

Asigna distintas políticas de protección a los usuarios mediante perfiles, asegurando la aplicación de la política más apropiada cada grupo de equipos.

Control centralizado de dispositivos

Evita la entrada de malware y las fugas de información bloqueando categorías de dispositivos completas (llaves y modems USB, webcams, DVD/CD etc), estableciendo excepciones con listas blancas de dispositivos o simplemente denegando determinadas acciones peligrosas.

Monitorización y filtrado de sitios Web

Incrementa la productividad de la empresa impidiendo y/o monitorizando la navegación de aquellas categorías web consideradas peligrosas o improductivas en horario de trabajo, sin preocuparse de la versión del navegador utilizado por los usuarios.

No más buzones saturados

El filtrado de contenidos disminuye la superficie de ataque en los servidores Exchange y el motor antimalware y antispam aumenta la seguridad y la productividad de los usuarios, evitando el correo basura y los mensajes maliciosos.

Malware Freezer

No te quemes con los falsos positivos. Malware Freezer congela el malware detectado durante siete días y, en caso de falso positivo, restaura el archivo en el sistema de forma automática.

Certificación ISO27001 y SAS 70 con disponibilidad 24x7

Solución alojada en la plataforma Microsoft Azure con garantía absoluta de la protección de información. Centros de datos certificados (ISO 27001 y SAS 70).

REQUISITOS TÉCNICOS

Consola web

- Conexión a Internet
- Internet Explorer 10
- Microsoft Edge
- Firefox (última versión)
- Google Chrome (última versión)

Para estaciones de trabajo y servidores de ficheros

- Uno de ellos al menos con conexión a Internet
- Sistemas Operativos (estaciones): XP SP2 y superiores, Windows Vista, Windows 7, Windows 8 (32 y 64-bit), Windows 8.1 (32 y 64-bit) y Windows 10 (32 y 64-bit).
- Sistemas Operativos (servidores): Windows 2003 (32, 64-bit and R2) SP1 y superiores, Windows 2008 (32 y 64-bit), Windows 2008 R2, Windows Small Business Server 2011, Windows Server 2012, Windows Server 2012 R2 y Windows Server 2016.

Para servidores exchange server

- Microsoft Exchange Server 2003, 2007, 2010, 2013 y 2016.

Para estaciones de trabajo y servidores de ficheros Mac

- 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
- macOS Sierra

Para estaciones de trabajo y servidores de ficheros Linux

- Ubuntu 12 32/64 bits y superiores
- Red Hat Enterprise Linux 6.0 64 bits y superiores
- Debian 6.0 Squeeze y superiores
- OpenSuse 12 32/64 bits y superiores
- Suse Enterprise Server 11SP2 64 bits y superiores

Para dispositivos Android

- Android (desde 4.0)

Certificado en los entornos de virtualización

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

Compatible with:

