



# Endpoint Protector Appliance™

Control de dispositivos / Prevención de pérdida de datos para PC y Mac



## Una solución rápida y fácil para tener puntos finales seguros frente a amenazas en los dispositivos

Endpoint Protector Appliance ofrece un enfoque basado en políticas para hacer cumplir las normas de uso de los dispositivos extraíbles en los puntos finales.

*Es la única solución que ofrece protección para PC y Mac.*

Los dispositivos portátiles están transformando nuestra vida y cómo trabajamos.

Su enfoque basado en "listas blancas" permite la utilización de dispositivos específicos para determinados usuarios/grupos de forma que sigan siendo productivos a la vez que mantienen un control sobre los dispositivos que se están utilizando y qué datos pueden transferir estos usuarios.

Endpoint Protector 2009 reduce drásticamente el riesgo que suponen las amenazas internas que podrían producir la pérdida, robo o deterioro de los datos o, en cualquier caso, comprometer la información.

### Tipos de dispositivos controlados:

- Unidades extraíbles USB (Unidades USB normales, U3, etc.)\*
- Tarjetas de memoria (SD, MMC, CF, etc.)\*
- Grabadoras y reproductores de CD/DVD (internos y externos)\*
- HDDs externos\*
- Unidades de disquete
- Lectores de tarjetas (internos y externos)\*
- Unidades ZIP
- Cámaras digitales\*
- Smartphones / BlackBerry / PDAs
- iPhones / iPads / iPods\*
- Dispositivos FireWire\*
- Dispositivos MP3 Player / Media Player\*
- Unidades biométricas
- Dispositivos Bluetooth\*
- Impresoras
- Tarjetas Expresscard (SSD)
- USB inalámbrico
- Puertos serie

**Endpoint Protector Appliance es el firewall entre el equipo y los dispositivos**

Endpoint Protector permite a las empresas aplicar políticas de utilización de dispositivos internos, normativas y estándares relativos a la seguridad de los datos, gestión de filtraciones de información y gobierno de TI.

### Appliance de seguridad de punto final para PC y Mac

Protección frente a las amenazas que afectan a los dispositivos portátiles extraíbles. Evita la filtración intencionada o accidental de los datos, el robo, pérdida o su infección por virus o malware.

### Gestión de dispositivo / Control de dispositivo\*

Define los permisos para dispositivos / usuarios o equipos en su red.

### Gestión centralizada basada en web / Panel de control

Gestiona de forma centralizada el uso de dispositivos portátiles extraíbles. La interfaz de administración e informes basada en web satisface las necesidades del personal de administración y seguridad de TI, brindando información en tiempo real sobre los dispositivos controlados en toda la empresa y la actividad de transferencias de datos.

### File Tracing / File Shadowing

File Tracing registra todos los datos que se copian a y desde los dispositivos previamente autorizados. File Shadowing guarda una copia de todos los archivos, incluso de aquellos que hayan sido borrados, que se usaron en los dispositivos controlados.

### Listas blancas de archivos

Sólo se pueden transferir los archivos autorizados a los dispositivos autorizados. El resto de archivos quedan bloqueados y se genera un informe de los intentos de transferencia.

### Registro de actividad del dispositivo – Auditoría

Se guardan los registros de actividad del dispositivo de todos los clientes y dispositivos conectados, creando un historial de dispositivos, PCs y usuarios para la realización de auditorías y análisis detallados.

### Informe y análisis

Potentes herramientas de informes, gráficos y análisis de datos para revisar fácilmente la actividad.

### Fácil cumplimiento de sus políticas de seguridad (Active Directory)

Las políticas de gestión de dispositivos simplificadas con plantillas personalizables para grupos de usuarios definidos (Active Directory GPO) permiten la sencilla aplicación y mantenimiento de políticas de seguridad en toda su red.

### Desbloqueo temporal de contraseñas / Modo de red "offline"

Los PC controlados que se encuentran desconectados de la red permanecen protegidos. Para mantener en marcha la productividad, los dispositivos pueden desbloquearse mediante la funcionalidad de Desbloqueo de contraseña offline.

### Autodefensa de cliente Endpoint Protector

Proporciona protección incluso en PCs donde los usuarios poseen permisos de administrador.

Haga cumplir las políticas de seguridad para puntos finales y tome el control de cómo y quién transfiere la información.

## REQUISITOS DEL SISTEMA

### Cliente(s)

- Windows 7 (32/64bit)
- Windows Vista (32/64bit)
- Windows XP (SP2) (32/64bit)
- Windows 2003/2008 (32/64bit)
- Mac OS X 10.4+
- .Net 2.0 Framework
- mín. 32 MB de espacio en disco

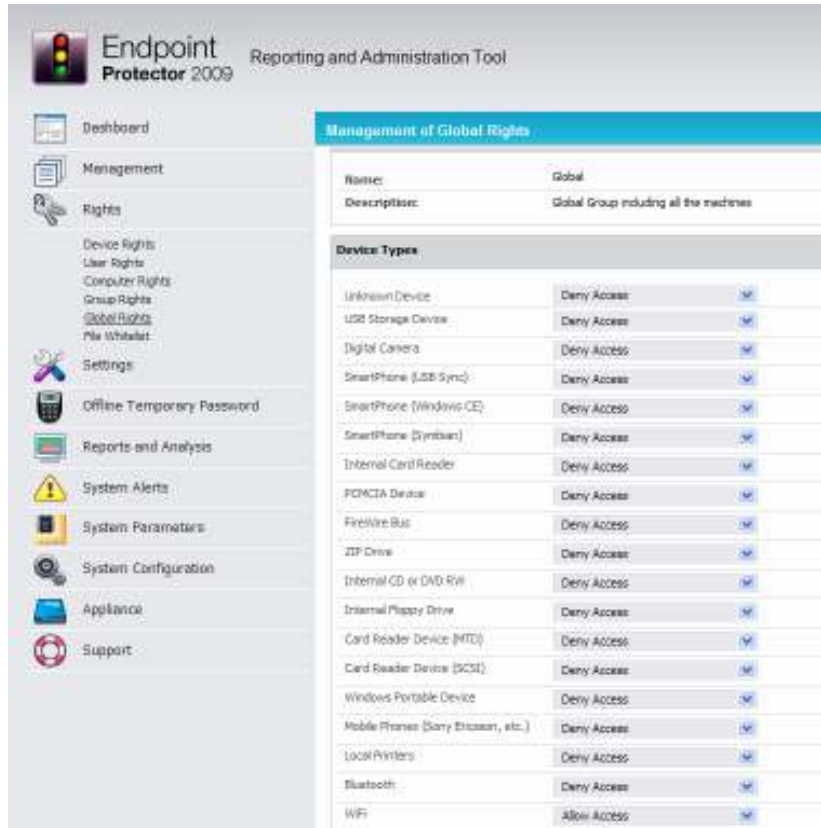
### Servicio de directorio

- Directorio Activo

Instalación sencilla mediante mecanismos MSI configurados automáticamente.

Endpoint Protector Appliance incluye todo el hardware de servidor necesario. Sólo tiene que sacarlo de la caja y conectarlo a su red, distribuir el software cliente a los PCs y Macs y en cuestión de minutos todos los puertos estarán protegidos ante el uso de dispositivos no controlados.

Su intuitiva interfaz basada en web permite una administración eficiente.



Interfaz basada en web de Endpoint Protector Appliance y herramienta de administración e informes

Modelos	A50	A100	A250	A1000	A4000
Protección para equipos (PC/Mac)	50	100	250	1000	4000
Capacidad adicional	25	50	125	500	2000
Carcasa (Montable en rack)	1U	1U	1U	1U	3U

## Encriptación garantizada – transferencia protegida de datos sensibles con EasyLock

La tecnología TrustedDevice con el software EasyLock opcional ha sido diseñada para garantizar que en el entorno protegido todos los dispositivos portátiles no solo están autorizados y controlados por medio de políticas de seguridad, sino que también garantizan la protección de la información sensible y confidencial que se transfiere. Esto asegura que, en caso de robo o pérdida de un dispositivo, toda la información almacenada en él se encuentra cifrada e inaccesible para otras personas.

Visite [www.EndpointProtector.com](http://www.EndpointProtector.com) para obtener más información y una licencia de evaluación gratuita



**CoSoSys Ltd.**  
 E-Mail: [sales@cososys.com](mailto:sales@cososys.com)  
 Tel: +40-264-593110  
 Fax: +40-264-593113

**CoSoSys Norteamérica**  
[sales.us@cososys.com](mailto:sales.us@cososys.com)  
 +1-208-850 7563

**CoSoSys Alemania**  
[sales.de@cososys.com](mailto:sales.de@cososys.com)  
 +49-7541-978-2627-0  
 +49-7541-978-2627-9



© Copyright 2004-2010 CoSoSys Ltd. Todos los derechos reservados. Lock it Easy, Surf it Easy, Carry it Easy, Carry it Easy +Plus, Carry it Easy +Plus Bio, Secure it Easy, TrustedDevices, TrustedLogin My Endpoint Protector y Endpoint Protector son marcas comerciales de CoSoSys Ltd. El resto de nombres comerciales mencionados aquí aparecen únicamente a título informativo y son marcas de sus respectivos propietarios.

\* Las características marcadas con \* están disponibles para Mac OS X.