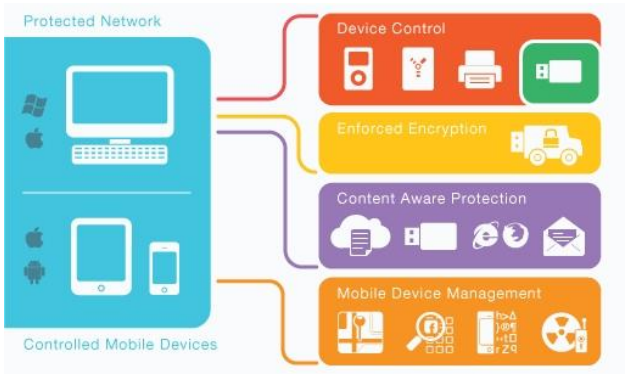
ENDPOINT PROTECTOR 4

Solución Data Loss Prevention, Control de Dispositivos y Mobile Device Management (MDM) de iOS & Android para PYMES y grandes cuentas

Solución fuera de la caja para proteger los datos contra amenazas de los dispositivos, gestionar la Prevención de Pérdida de Datos y MDM.

En un mundo donde los dispositivos portátiles y la nube transforman la manera en que vivimos y trabajamos, Endpoint Protector 4 está diseñado para proteger la información, mantener la productividad y hacer el trabajo más cómodo, seguro y agradable.
Endpoint Protector 4, disponible en formato de appliance virtual o hardware, puede ser instalado en unos minutos.



Ventajas claves

- El hardware y la maquina virtual pueden ser implementados en unos minutos
- Solución 3 en 1, Control de Dispositivos, DLP y MDM
- Interfaz basada en la web
- Protección para Windows, Mac, Linux, iOS y Android
- Protección proactiva contra el abuso de dispositivos y datos
- VMware ready

Seguridad de estaciones de trabajo, portátiles y Netbooks con Windows/Mac OS X y Linux

Protección contra amenazas planteadas por dispositivos portátiles extraíbles. Detiene la divulgación no autorizada de datos, el robo, la pérdida, o la infección con malware intencionados o imprevistos.

Controle los siguientes Dispositivos y Aplicaciones y muchos más:

- **Dispositivos USB***
- Unidades USB* (normales, U3)
- Tarjetas de Memoria* (SD, CF, etc.)
- CD/DVD-Burner (int., ext.)
- HDDs externos* (incl. sATA)
- Impresoras*
- Unidades Floppy
- Lectores de Tarjeta* (int., ext.)
- Cámaras web*
- Tarjetas de red WiFi
- Cámaras Digitales*
- iPhones / iPads / iPods*
- Smartphones/BlackBerry/PDAs
- Unidades FireWire*
- Reproductor MP3/Reproductores Media*
- Dispositivos Biométricos
- Dispositivos Bluetooth*
- Unidades ZIP
- Tarjetas Express (SSD)
- USB inalámbrico
- Puerto Serie
- Placa Teensy
- Dispositivos de almacenamiento PCMCIA
- Network Share
- Tunderbolt

- **Clientes de e-mail**
  - Outlook
  - Lotus Notes
  - Thunderbird, etc.
- **Navegadores Web**
  - Internet Explorer
  - Firefox
  - Chrome
  - Safari, etc.
- **Mensajería Instantánea**
  - Skype, ICQ, AIM.
  - Microsoft Communicator
  - Yahoo Messenger, etc.
- **Aplicaciones para compartir archivos**
  - Dropbox, iCloud
  - BitTorrent, SkyDrive
  - Kazaa, etc.
- **Otras Aplicaciones**
  - iTunes
  - Samsung Kies
  - Windows DVD Maker
  - Total Commander
  - FileZilla
  - Team Viewer
  - EasyLock, y muchos más

Gestión centralizada basada en Web / Panel de control

Gestiona de forma centralizada el uso de dispositivos portátiles extraíbles y la transferencia de datos confidenciales a través de aplicaciones online en tiempo real

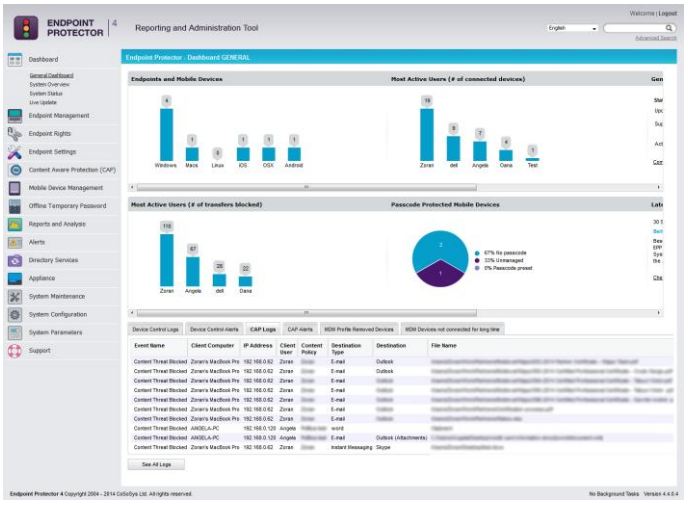
Beneficios claves:

- Endpoint Protector implica un TCO que es con 50% más bajo que la media del mercado
- La duración de implementación está reducida con 70% comparando con otras soluciones
- Costes más bajos con 45% en comparación con otras soluciones similares.

2014 Computing Security Awards WINNER DLP Solution of the Year

Info Security Products Guide 2015 GLOBAL EXCELLENCE GOLD

"He elegido Endpoint Protector Appliance por el coste, la facilidad de administración y control detallado. La solución es fácil de instalar, eficiente, fuerte y fácil de gestionar. Me encantan las características de registro, de shadowing y de desbloqueo temporal de contraseña en modo de red "offline" (muy práctico, por cierto)."
Marc Rossi, Infrastructure Director, NASS y WIND SAS France



Mobile Device Management (MDM) para OSX, iOS y Android

- Imponer Política de Contraseña y Seguridad
- Localizar Dispositivos / Bloquear / Borrar Dispositivos
- Desplegar ajustes E-mail, VPN, WiFi (dispositivos iOS)
- Geofencing - políticas a base de un perímetro seguro
- Solución BYOD, para más detalles, por favor lea MDM datasheet

Gestión de dispositivos / Control de dispositivos

Definir los permisos a nivel de dispositivos pero también de usuarios, equipos y grupos: bloquear, permitir, permitir el uso de solo lectura, permitir si es TrustedDevice.

Content Aware Protection / Filtrado de contenido

Escaneo de Documentos para la detección de contenido confidencial, registro e informes de los incidentes de contenido. Bloquear la salida de datos a través de dispositivos portátiles, aplicaciones y servicios online.

Filtrado según Tipo de Archivo/ Contenido / Expresiones Regulares

Los filtros según el tipo de archivo bloquean los tipos de archivos especificados. Se pueden crear filtros también a base de contenido predefinido, personalizado y de expresiones regulares.

Listas blancas de archivos / Dispositivos / URLs / Dominios

Solo los archivos autorizados se pueden transferir a los dispositivos, aplicaciones online y correos electrónicos autorizados. Los demás intentos de transferencias de archivos quedan bloqueados y se genera un informe.

Informes y Análisis / Panel de control y gráficos / Auditoría

Se guardan los registros de actividad de todos los dispositivos conectados y las transferencias de archivos, proporcionando un historial completo para auditorías y análisis.

Fácil cumplimiento de las Políticas de Seguridad (Active Directory)

La integración con Active Directory permite importar la estructura de grupos, equipos y usuarios. La funcionalidad de AD Sync sincroniza las nuevas entidades.

Desbloqueo Temporal de Contraseña / Modo de red "offline"

Los equipos controlados que se encuentran desconectados de la red permanecen protegidos. Para mantener en marcha la productividad, los dispositivos y las transferencias de archivos pueden ser permitidos temporalmente (desde 30 minutos a 30 días).

Gestión de departamentos
Los departamentos pueden ser organizados y separados por políticas dedicadas.

Autodefensa del Cliente Endpoint Protector
Proporciona protección incluso en equipos donde los usuarios tienen permisos de administrador.

Encriptación forzada- proteger los datos en tránsito con EasyLock
En combinación con nuestro software EasyLock, instalado en dispositivos removibles, los datos copiados a dispositivos son cifrados automáticamente. Con nuestra tecnología TrustedDevice se puede aplicar seguridad adicional utilizando dispositivos portátiles de almacenamiento encriptados para almacenar datos.

Seguridad para:

Cliente(s) Endpoint Protegido(s)
- Windows 8 (32/64bit)
- Windows 7 (32/64bit)
- Windows Vista (32/64bit)
- Windows XP (SP2) (32/64bit)
- Windows 2003/2008/2012 (32/64bit)
- Mac OS X 10.5+
- Ubuntu 14.04
- Ubuntu 10.04
- openSUSE 11.4

Mobile Device Management (MDM) - Dispositivos Moviles soportados
- iPad, iPhone, iOS 4+
- Android 2.2+,
  Android 4+ requerido para algunas funcionalidades

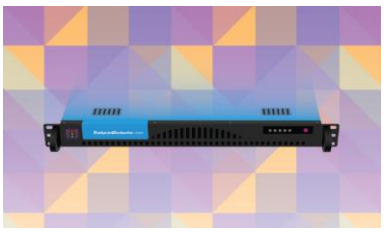
Directory Service (no requerido)
- Active Directory

Certificados:

Endpoint Protector Hardware Appliance
Endpoint Protector Hardware Appliances son disponibles en varias capacidades adecuadas para las necesidades de su negocio.

Modelos seleccionados (más disponibles)	Número End-points	Capacidad adicional	Carcasa (montable en Rack)	CPU	HDD	Fuente de alimentación
A20	20	4	Standalone	ULV Single Core	320 GB	60W
A50	50	10	1U	ULV Dual Core	320 GB	200W
A100	100	20	1U	ULV Dual Core	320 GB	200W
A250	250	50	1U	Pentium 2 Core	500 GB	260W
A500	500	100	1U	Pentium 2 Core	1TB	260W
A1000	1000	200	1U	Intel Xenon 4 Core	2x TB (Raid 1)	260W
A2000	2000	400	2U	2x Intel Xenon 4 Core	4x 1TB (Raid 5)	2x720W
A4000	4000	800	3U	2x Quad Core	6x 1TB (Raid 5)	2x800W
Garantía del hardware	1 año incluido. Garantía adicional y opciones de recambio disponibles					

Endpoint Protector Virtual Appliance
Endpoint Protector Virtual Appliance puede ser utilizado por compañías de cualquier tamaño. El Virtual Appliance está disponible en formato VMX, VHD o OVF para ser compatible con las plataformas de virtualización más populares.



Utilizando el Virtual Appliance puede protegerse contra el uso no autorizado de dispositivos y la pérdida de datos dentro de unos minutos.

Entornos Virtuales Soportados	Versión	.ovf	.vmx	.vhd	.xva	.pvm
VMware Workstation	7.1.4	-	*	-	-	-
VMware Workstation *	9.0.2	*	*	-	-	-
VMware Player *	6.0.0	*	*	-	-	-
VMware Fusion *	5.0.0	-	*	-	-	-
VMware vSphere (ESXi)	5.1.0	*	-	-	-	-
Oracle VirtualBox	4.2.18	*	-	-	-	-
Parallels Desktop for Mac	9.0.2	-	-	-	-	*
Microsoft Hyper-V Server	2008/2012	-	-	*	-	-
Citrix XenServer 64bit	6.2.0	-	-	-	*	-

Para los entornos marcados con *, por favor contacte nuestra línea de soporte.
Otros entornos de virtualización pueden estar disponibles.

Visite www.EndpointProtector.com para una prueba gratuita.

CoSoSys
Germany
E-Mail:
sales.de@cososys.com
Phone: +49-7541-978-2627-0
Fax: +49-7541-978-2627-9

CoSoSys
North America
sales.us@cososys.com
+1-888-271 9349

CoSoSys Ltd.
sales@cososys.com
+40-264-593110
+40-264-593113

Contacte su partner local para más información:

Creado en 12-Jun-2015

ENDPOINT PROTECTOR 4

Content Aware Protection para Windows
Una parte importante de su estrategia DLP a nivel de endpoint

Solución fuera de la caja para proteger los datos contra fuga y robo a través de aplicaciones online, servicios en la nube, dispositivos portátiles y otros puntos de salida.

Content Aware Protection es un modúlo del conjunto Endpoint Protector DLP (Data Loss Prevention) que cubre las necesidades de seguridad procedentes de los riesgos planteados por los numerosos puntos de salida de los datos confidenciales de la compañía.
En un mundo donde los dispositivos portátiles y la nube transforman la manera en que vivimos y trabajamos, Endpoint Protector 4 está diseñado para proteger la información, mantener la productividad y hacer el trabajo más cómodo, seguro y agradable.
Endpoint Protector 4, disponible en formato de appliance virtual o hardware, puede ser instalado en unos minutos. La solución permite reducir drásticamente los riesgos planteados por las amenazas internas que podrían llevar a brechas o robos de datos.

Ventajas claves

- El hardware y la maquina virtual pueden ser implementados en cuestión de minutos
- Interfaz basada en la web
- Gestión intuitiva de políticas y endpoints
- Protección para Windows y Mac OS X
- Protección proactiva contra el abuso de dispositivos y datos
- VMware ready

Content-Aware Data Loss Prevention
Protección frente a las amenazas planteadas por la transferencia de datos a dispositivos portátiles y aplicaciones y servicios online. Detiene la fuga intencional o accidental de datos, el robo y la pérdida de datos.

Compatible con Windows y Mac OS X
Monitoreo y bloqueo del flujo de datos en las plataformas más populares y más fuertes para proteger los datos de su compañía.

Controle el flujo de datos a las siguientes y más Aplicaciones y Dispositivos:

- **Clientes de E-Mail**
  - Outlook
  - Lotus Notes
  - Thunderbird, etc.
- **Navegadores Web**
  - Internet Explorer
  - Firefox
  - Chrome, etc.
- **Mensajería Instantánea**
  - Skype, etc.
  - Microsoft Communicator
  - Yahoo Messenger, etc.
- **Aplicaciones de compartir archivos**
  - Dropbox
  - BitTorrent
  - Kazaa, etc.
- **Otras Aplicaciones**
  - iTunes
  - Samsung Kies
  - Windows DVD Maker
  - Total Commander
  - FileZilla
  - Team Viewer
  - EasyLock, y muchos más

- **Dispositivos / Puertos**
- Dispositivos USB*
- Unidades USB*
- Tarjetas de Memoria* (SD, CF, etc.)
- CD/DVD-Burner (int., ext.)
- HDDs externos* (incl. sATA)
- Impresoras*
- Unidades Floppy
- Lectores de Tarjeta* (int., ext.)
- Cámaras web*
- Tarjetas de red WiFi
- Cámaras Digitales*
- iPhones / iPads / iPods*
- Unidades FireWire
- Smartphones/BlackBerry/ PDA
- Dispositivos FireWare
- Network Share
- Thunderbolt
- MP3/Reproductores Media*
- Dispositivos Biométricos
- Dispositivos Bluetooth*
- Unidades ZIP
- Tarjetas Express (SSD)
- USB inalámbrico
- etc.

Gestión centralizada basada en Web / Panel de control
Gestione y monitorice de forma centralizada las transferencias de datos fuera de las redes corporativas. La interfaz de administración e informes basada en web satisface las necesidades del personal de administración y seguridad de TI y ofrece información en tiempo real sobre los dispositivos controlados en toda la empresa y la actividad de transferencia de datos.

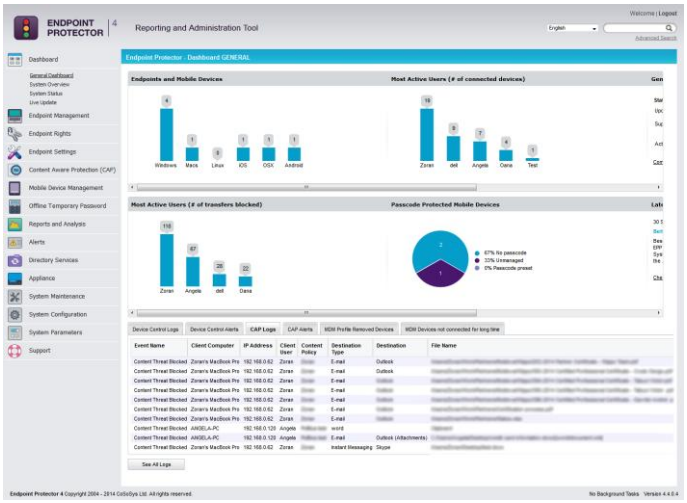
Desbloqueo temporal de contraseña / Modo de red "offline"*
Los equipos controlados que se encuentran desconectados de la red permanecen protegidos. Para mantener en marcha la productividad, los dispositivos y las transferencias de archivos pueden ser permitidos temporalmente (desde 30 minutos a 30 días).

Beneficios claves

- Endpoint Protector implica un TCO que es con 50% más bajo que la media del mercado
- La duración de implementación está reducida con 70% comparando con otras soluciones
- Costes más bajos con 45% en comparación con otras soluciones similares.

2014 Computing Security Awards WINNER DLP Solution of the Year

Info Security Products Guide 2015 GLOBAL EXCELLENCE GOLD



Crear políticas de seguridad para entidades específicas
Las políticas de Content Aware Protection ofrecen control flexible de escaneo de documentos, permitiendo la selección de usuarios, equipos o grupos a monitorizar.

Filtrar por Contenido Predefinido o palabras claves relevantes
Filtrar los datos que salen de los terminales protegidos a base de un formato de contenido predefinido que incluye: detalles de Tarjeta de Crédito, Números de Seguro Social (formatos distintos por país), Información de Cuentas Bancarias, etc.

Filtrar por Diccionario/ Contenido personalizado y Expresiones Regulares
El módulo de Content Aware Protection busca palabras clave e impide que los datos / archivos que los contienen se filtren o se roben a través de los puntos de salida protegidos. Se pueden crear varios diccionarios igual que políticas avanzadas a base de RegEx.

Filtrar por Tipo de Archivo
Endpoint Protector bloquea los documentos que salen de la empresa en función del tipo de archivo. Soporta los tipos de archivos actualmente en uso como archivos de MS Office y gráficos, ejecutables, y muchos otros.

Threshold para Filtros
Define hasta qué número de incidentes se permite una transferencia de archivos. Se aplica a cada tipo de contenido confidencial y no se refiere a la suma de todos los incidentes.

Monitorizar Portapapeles para evitar Copiar & Pegar datos
Monitorizando el Portapapeles podrá detener los usuarios que copien & peguen información confidencial de la compañía en Outlook, applicaciones de webmail u otros canales a través de los cuales la información se puede perder.

Desactivar Imprimir Pantalla
Desactivando la opción de impresión de pantalla en su política evitará que los usuarios realicen capturas de pantalla y llevarlos fuera de la empresa como imágenes. Esto fortalece aún más su política DLP.

Prevenir fuga de datos a través de Outlook y Thunderbird
Como archivo adjunto o incluso si los datos confidenciales se encuentran en el cuerpo de texto del correo, se impide el envío y el incidente se reporta.

Filtrar datos saliendo por navegadores web
Firefox, Google Chrome y muchos otros navegadores representan un gran riesgo por la seguridad de los datos ya que los usuarios pueden cargar cualquier archivo si lo pueden acceder. Es vital de controlar todos los accesos a documentos que tengan los navegadores web antes de que los archivos lleguen a internet.

Filtrar la transferencia de datos a través de distintas aplicaciones antes de salir del terminal protegido
Endpoint Protector escanea los documentos y el texto copiado en aplicaciones como Skype, Yahoo Messenger, Dropbox, Outlook, etc. y bloquea la transferencia si procede.

Autodefensa del Cliente Endpoint Protector
Proporciona protección incluso en equipos donde los usuarios poseen permisos de administrador.

Cliente(s) Endpoint Protegido(s)
- Windows 8 (32/64bit)
- Windows 7 (32/64bit)
- Windows Vista (32/64bit)
- Windows XP (SP2) (32/64bit)
- Windows 2003/2008/2012 (32/64bit)
- Mac OS X 10.5+

Servicio de Directorio (no requerido)
- Active Directory

Módulo Endpoint Protector Device Control (requerido)

Endpoint Protector 4 es la única solución en su categoría disponible como appliance virtual o hardware. Protegiendo su red con Endpoint Protector ahorra mucho tiempo comparando con otras soluciones.

Endpoint Protector Hardware Appliance
Endpoint Protector Hardware Appliances son disponibles en varias capacidades adecuadas para las necesidades de su negocio.

Common Criteria

Modelos seleccionados (más disponibles)	Número End-points	Capacidad adicional	Carcasa (montable en Rack)	CPU	HDD	Fuente de alimentación
A20	20	4	Standalone	ULV Single Core	320 GB	60W
A50	50	10	1U	ULV Dual Core	320 GB	200W
A100	100	20	1U	ULV Dual Core	320 GB	200W
A250	250	50	1U	Pentium 2 Core	500 GB	260W
A500	500	100	1U	Pentium 2 Core	1TB	260W
A1000	1000	200	1U	Intel Xenon 4 Core	2x TB (Raid 1)	260W
A2000	2000	400	2U	2x Intel Xenon 4 Core	4x 1TB (Raid 5)	2x720W
A4000	4000	800	3U	2x Quad Core	6x 1TB (Raid 5)	2x800W

Garantía del hardware: 1 año incluido. Garantía adicional y opciones de recambio disponibles

Device Control para Endpoints (Sobremesas, Portátiles, etc.)
Con el Control de Dispositivos, los administradores de TI reciben informes detallados y registros que indican la ruta de un archivo transferido y también pueden guardar una copia de los archivos, a través de File Tracing & File Shadowing.

Mobile Device Management (MDM) para iOS y Android
Características como Remote Nuke (Wipe), Remote Block, Tracking & Localización, así como Mobile Application Management y Push Network Settings están disponibles. Para más detalles, ver la hoja de datos de MDM.

Endpoint Protector Virtual Appliance
Endpoint Protector Virtual Appliance puede ser utilizado por compañías de cualquier tamaño. El Virtual Appliance está disponible en formato VMX, VHD o OVF para ser compatible con las plataformas de virtualización más populares.

Utilizando el Virtual Appliance puede protegerse contra el uso no autorizado de dispositivos y la pérdida de datos dentro de unos minutos.

VMWARE CERTIFIED VIRTUAL APPLIANCE

vmware READY

Entornos Virtuales Soportados	Versión	.ovf	.vmx	.vhd	.xva	.pvm
VMware Workstation	7.1.4	-	*	-	-	-
VMware Workstation *	9.0.2	*	*	-	-	-
VMware Player *	6.0.0	*	*	-	-	-
VMware Fusion *	5.0.0	-	*	-	-	-
VMware vSphere (ESXi)	5.1.0	*	-	-	-	-
Oracle VirtualBox	4.2.18	*	-	-	-	-
Parallels Desktop for Mac	9.0.2	-	-	-	-	*
Microsoft Hyper-V Server	2008/2012	-	-	*	-	-
Citrix XenServer 64bit	6.2.0	-	-	-	*	-

Para los entornos marcados con *, por favor contacte nuestra línea de soporte. Otros entornos de virtualización pueden estar disponibles.

Visite www.EndpointProtector.com para una prueba gratuita.

CoSoSys Germany
E-Mail: sales.de@cososys.com
Phone: +49-7541-978-2627-0
Fax: +49-7541-978-2627-9

CoSoSys North America
sales.us@cososys.com
+1-888-271-9349

CoSoSys Ltd.
sales@cososys.com
+40-264-593110
+40-264-593113

Contacte su partner local para más información:

COSOSYS

Creado en 12-Jun-2015

ENDPOINT PROTECTOR 4

Mobile Device Management (MDM) para iOS y Android

Mobile Device Management es un módulo de Endpoint Protector 4 cubriendo especialmente las necesidades de seguridad surgidos por el uso aumentado de dispositivos móviles personales (BYOD) o perteneciendo a la compañía.
Endpoint Protector es una solución todo en uno que hace posible que los Administradores de TI implementen y gestionen una Solución Data Loss Prevention en su red cubriendo ordenadores (Windows, Mac OS x, Linux) y dispositivos móviles (iOS y Android) de una manera eficiente y económica.
En un mundo donde los dispositivos portátiles y de estilo de vida transforman la manera en que vivimos y trabajamos, Endpoint Protector 4 está diseñado para mantener la productividad y hacer el trabajo más cómodo, seguro y agradable.

Ventajas claves

- Protección para iOS y Android
- El hardware y la maquina virtual implementados en unos minutos
- Interfaz basada en la Web
- Gestión intuitiva de Endpoints
- Protección proactiva contra el robo de datos
- VMware ready

Seguridad de Endpoint Móvil

Políticas fuertes de seguridad aplicadas en los smartphones y las tabletas de la compañía garantizarán una protección proactiva de los datos críticos del negocio donde quiera y en cualquier dispositivo móvil desde que se acceden.

Soporta Dispositivos Móviles iOS y Android

Controlar y gestionar las dos más famosas y poderosas plataformas móviles en crecimiento para proteger los datos de su compañía.

Aplicación de Contraseña

Forzar cambio periódico de contraseña directamente Over-The-Air o bien con la participación del usuario.

Seguimiento y Localización

Seguir de cerca la flota de dispositivos móviles de la compañía y saber siempre donde se encuentran los datos confidenciales de su empresa. Para iOS la aplicación EPP MDM tiene que ser instalada en el dispositivo.

Borrado Remoto (Nuke) / Bloqueo remoto – Protección contra el robo

Evitar que datos confidenciales lleguen a manos equivocados por tener control Over-The-Air y aplicar Nuke Remoto del Dispositivo (borrado remoto de datos) o bloquear el dispositivo en caso de pérdida o robo.

Restricciones para iOS

Desactivar funciones tales como iCloud, FaceTime, YouTube, AppStore, Compras In-App, iTunes, Siri, Cámara si no cumplen con la política de la empresa.

Gestionar Configuración de Correo, WiFi y VPN en dispositivos iOS

Gestionar Over-The-Air la configuración del E-mail, WiFi y VPN.

Borrar Configuración de E-mail y WiFi en dispositivos iOS

Borrar de forma remota el contenido y la configuración del E-mail corporativo y la configuración del WiFi. El contenido del E-mail corporativo se puede eliminar mientras que las cuentas personales de E-mail y contenido permanecen intactas.

Localizar dispositivo por sonido (Solo Android)

Fácil detección de cualquier dispositivo móvil perdido reproduciendo una canción el tiempo justo para localizar su smartphone / tableta.

Soporte para el Modelo Bring-Your-Own-Device

Tener control total sobre los datos confidenciales de la empresa sin importar si están almacenados en dispositivos personales o de la compañía y enfocar en hacer los empleados trabajar más eficiente.

Políticas basadas en localización/ Geofencing

Definir un perímetro virtual en un área geográfica utilizando un servicio basado en la localización. Esto proporciona una mejor gestión de las políticas de MDM que se aplican sólo en un área específica.

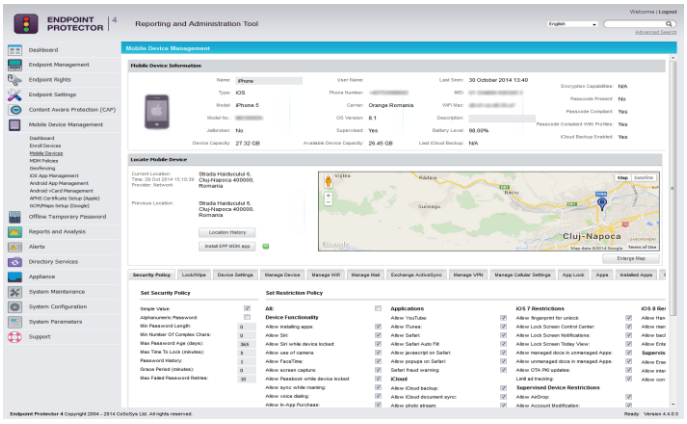
¡Las compañías tienen que definir y aplicar claramente políticas de Mobile Device Management para que se protejan!

Beneficios claves

- Imponer la política de uso de dispositivos móviles
- Proteger los datos de la compañía
- Control inmediato sobre el uso de dispositivos móviles
- Implementación Over-the-Air
- Impacto y esfuerzo mínimos para usuarios y administradores
- Cumplimiento
- Solución de seguridad BYOD

Gestión centralizada basada en Web / Panel de control

Gestione de forma centralizada el uso de dispositivos móviles. La interfaz de Administración e Informes basada en web satisface las necesidades del personal de administración y seguridad de TI y ofrece información en tiempo real sobre los dispositivos controlados en toda la empresa.



Gestión de inventario de Dispositivos Móviles

Permite el control y el inventario sobre los dispositivos móviles personales o de la compañía con registro e informes detallados de la actividad de dispositivos para auditoria posterior.

Encriptación de Dispositivo

Los iPhones y iPads vienen con encriptación hardware 256bit AES incorporada que es siempre activa y aplicada al establecer una contraseña al dispositivo.

Inscripción y Aprovisionamiento Over-The-Air

El proceso de inscripción garantizara una implementación fácil y segura de la plataforma MDM en cualquier infraestructura de TI.

Dispositivos Móviles Soportados

- iPad, iPhone, iOS 4.0, iOS 5.0, iOS 6.0, iOS 7.0, iOS 8
- Android 2.2+

Requerimientos para MDM

- Para MDM iOS se requiere una cuenta gratuita (hecha con un ID Apple) de Apple Push Notification Service (APNS)
- Para MDM Android se requiere una cuenta gratuita (hecha con una cuenta de Google) de Google Cloud Messaging para Android

Vista General de Características y Comparación para iOS y Android

Nuestro listado de características para iOS y Android se está extendiendo y sigue creciendo para cubrir siempre requerimientos de seguridad nuevos y emergentes.

Características MDM	iOS	Android
Políticas solidas de Seguridad	✔	✔
Longitud de contraseña	✔	✔
Reintentos de contraseña	✔	✔
Calidad de contraseña	✔	✔
Tiempo de bloqueo de pantalla	✔	✔
Aplicación de contraseña	✔	✔
Encriptación Forzada del	✔	✔
Seguimiento y Localización	✔(app)	✔
Localizar dispositivo perdido (sonido)		✔
Bloqueo Remoto	✔	✔
Nuke Remoto (Borrado Remoto)	✔	✔
Borrar dispositivo	✔	✔
Borrar contenido/ajustes de E- mail	✔	
Borrar Tarjeta SD		✔
Geofencing	✔	✔
Mobile Application Management	✔	✔
Restriccionar uso de cámara	✔	✔
Inscripción/Aprovisionamiento Over-The-Air	✔	✔
Inscripción por E-mail o por URL	✔	✔
Inscripción por SMS	✔	✔
Código-QR	✔	✔
Configuración de E-mail	✔	
Restringir uso de		
iTunes, iCloud, AppStore, Compras In-App, Siri, Cámara, FaceTime, Forzar copia de seguridad cifrada de iTunes, Safari, YouTube, etc.	✔ ✔ ✔ ✔ ✔ ✔	
Muchas más funciones disponibles	...	...
Versiones Soportadas	Apple iOS 4, 5, 6, 7, 8	Android 2.2+

Ciertas características de seguridad de dispositivos y de gestión no son soportados en versiones de SO antiguos y / o dispositivos.

Control de dispositivos para Windows, Mac OS X y Linux

Es otra de las características disponibles para la Prevención de Pérdida de Datos. Endpoint Protector ofrece características DLP adicionales para el control de dispositivos portátiles de almacenamiento y puertos en Windows, Mac OS X y Linux.

Protección de contenido para Endpoints (portátiles, etc.)

Protección de contenido para Windows y Mac OS X. Ofrece la posibilidad de controlar los datos sensibles que salen de la red corporativa. A través de inspección de contenido, las transferencias de documentos confidenciales de la empresa se registrarán y serán bloqueadas. Esta función evitará la fuga de datos a través de todos los posibles puntos de salida, desde dispositivos USB a aplicaciones como Microsoft Outlook, Skype, Navegadores Web, Dropbox, etc.

Endpoint Protector Hardware Appliance

Endpoint Protector Hardware Appliances son disponibles en diferentes capacidades para adaptarse a las necesidades de su negocio.

2013 MobileVillage Mobile Star Awards RISING STAR

2014 Computing Security Awards WINNER DLP Solution of the Year

Endpoint Protector Virtual Appliance

Endpoint Protector Virtual Appliance puede ser utilizada de negocios de cualquier tamaño. Está disponible en formatos OVF, VMX, OVF, VHD, XV bis y PVM para ser compatible con las plataformas de virtualización más populares.

Utilizando el Appliance Virtual puede protegerse contra el uso no autorizado de dispositivos y pérdida de datos en su red en unos minutos.

VMWARE CERTIFIED VIRTUAL APPLIANCE

vmware READY

Entornos Virtuales Soportados	Versión	.ovf	.vmx	.vhd	.xva	.pvm
VMware Workstation	7.1.4	-	*	-	-	-
VMware Workstation *	9.0.2	*	*	-	-	-
VMware Player *	6.0.0	*	*	-	-	-
VMware Fusion *	5.0.0	-	*	-	-	-
VMware vSphere (ESXi)	5.1.0	*	-	-	-	-
Oracle VirtualBox	4.2.18	*	-	-	-	-
Parallels Desktop for Mac	9.0.2	-	-	-	-	*
Microsoft Hyper-V Server	2008/2012	-	-	*	-	-
Citrix XenServer 64bit	6.2.0	-	-	-	*	-

Para los entornos marcados con *, por favor contacte nuestra línea de soporte. Otros entornos de virtualización pueden estar disponibles.

Visite www.EndpointProtector.com para una prueba gratuita.

CoSoSys Germany
E-Mail: sales.de@cososys.com
Phone: +49-7541-978-2627-0
Fax: +49-7541-978-2627-9

CoSoSys North America
sales.us@cososys.com
+1-888-271-9349

CoSoSys Ltd.
sales@cososys.com
+40-264-593110
+40-264-593113

Contacte su socio local para más información:

COSOSYS

Creado en 12-Jun-2015