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.

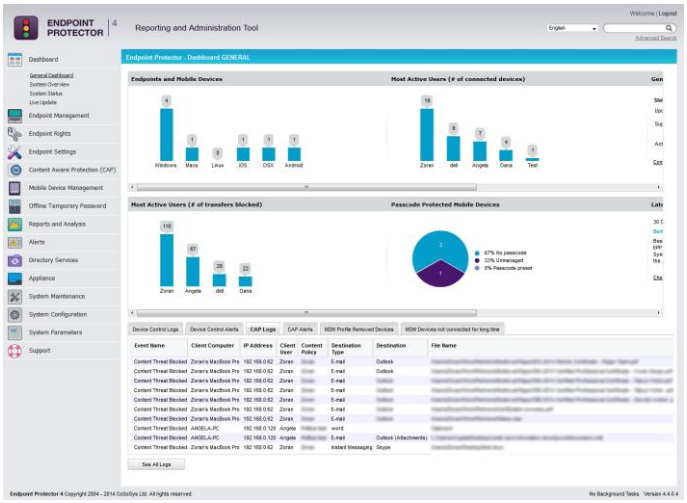
Desbloqueo temporal de contraseña / Modo de red "offline"*
Los equipos controlados que se encuentran desconectados de la red permanecen protegidos. Para mantener en marcha la productividad, los dispositivos y las transferencias de archivos pueden ser permitidos temporalmente (desde 30 minutos a 30 días).

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