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.

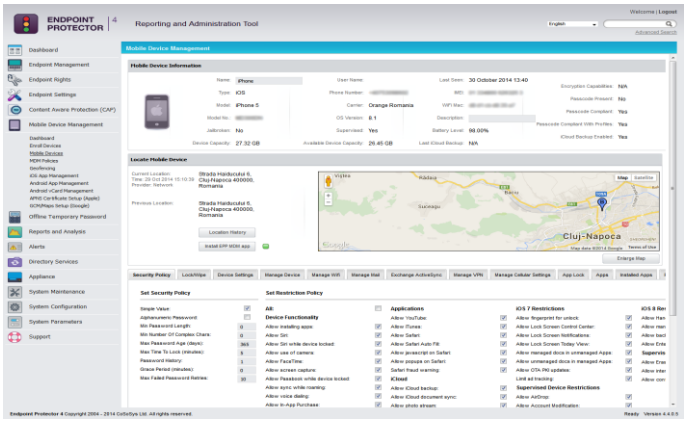
¡Las compañías tienen que definir y aplicar claramente políticas de Mobile Device Management para que se protejan!

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