

# Mobile Device Management de Endpoint Protector está ahora disponible para proteger Dispositivos Móviles iOS y Android

## Endpoint Protector añade Funciones Mobile Device Management (MDM) y Enterprise Mobility Management (EMM) para iOS y Android

Cluj-Napoca, 7 Noviembre, 2012. Hoy anunciamos el lanzamiento de Mobile Device Management (MDM) para iOS y Android como un nuevo módulo integrado en Endpoint Protector 4.3, incluyendo soporte para iOS 6.

“Como desarrolladores con experiencia de Soluciones de Prevención de Pérdida de Datos (DLP), Control de Dispositivos, Seguridad de la Red para Windows, Mac OS X y Linux, era simplemente una decisión natural para nosotros de seguir la gran demanda que nuestros clientes han expresado enfrentando todos los iPads y iPhones invadir el espacio de trabajo y las redes de la empresa. Con funciones de Mobile Device Management totalmente integradas en Virtual y Hardware Appliance de Endpoint Protector, los departamentos TI pueden tratar fácilmente con la tendencia Traiga-Su-Propio-Dispositivo-Móvil que están enfrentando con los usuarios de iOS y Android. Las características MDM permite ahora a los administradores TI monitorizar y gestionar dispositivos móviles, mientras que las características de Control de Dispositivos aseguran un control total sobre donde se conectan estos dispositivos a la red, ofreciendo, en general, a los departamentos TI una herramienta poderosa para proteger los datos y auditar el uso de dispositivos”, dijo Roman Foeckl, CEO de CoSoSys.

La presencia de los teléfonos inteligentes y de las tabletas en entornos corporativos actuales está ampliando las fronteras de los procesos de negocio otras veces confiados dentro de las cuatro paredes de la empresa. Mientras que hay beneficios significativos en la adopción de dispositivos móviles como una forma de aumentar la eficiencia en el trabajo, también existen preocupaciones significativas para los departamentos de TI sobre cómo mantener seguros los datos corporativos confidenciales en cualquier lugar y en cualquier dispositivo que el empleado utiliza para almacenarlos. Mobile Device Management de Endpoint Protector permite a las compañías adoptar la portabilidad y la movilidad sin comprometer la seguridad de los datos críticos de negocio y sin sobrecargar el departamento de TI. El nuevo módulo se puede integrar fácilmente en las infraestructuras de TI existentes, permitiendo un proceso de inscripción y provisión seguro y rápido, tanto de dispositivos corporativos como privados, que puede ser de sí mismo o a distancia a través de correo electrónico, SMS, portal web o código QR. Usando un mecanismo de inscripción con un one-time-code, se impide cualquier acceso no autorizado y detiene la conexión de dispositivos no fiables a la red de la empresa.

Como solución complementaria al módulo ya existente de Control de Dispositivos en puntos finales para equipos Desktop y Portátiles, Mobile Device Management asegura una protección proactiva para los puntos finales móviles, permitiendo a los administradores TI gestionar de forma eficaz y transparente los dispositivos móviles desde una interfaz intuitiva basada en la web, de informes y

administración. El nuevo modulo se dirige a los principales desafíos que enfrentan los departamentos TI:

- Seguridad de los datos móviles, para proteger contra las últimas amenazas de pérdida, fuga y robo de datos con características clave como la aplicación de políticas fuertes de seguridad, reglas avanzadas de contraseña, cifrado de dispositivo, bloqueo remoto de dispositivo y borrado remoto de datos
- Seguimiento y localización precisa, ofreciendo en cualquier momento y para cualquier dispositivo gestionado informes completos sobre la ubicación de la información crítica de la compañía
- Monitoreo y gestión de aplicaciones móviles, permitiendo un control riguroso sobre el gran número de aplicaciones no deseadas que pueden llegar fácilmente en los dispositivos móviles de los empleados

Mobile Device Management está disponible con Endpoint Protector Versión 4.3 como Appliance Hardware y Virtual. La solución de seguridad de dispositivos y de datos garantiza una protección completa y proactiva contra amenazas tanto dentro como fuera de las organizaciones de una manera sencilla, pero altamente eficiente, con una integración perfecta y sin restricciones del sistema operativo. Para más detalles, por favor visite: [http://www.endpointprotector.com/products/mobile\\_device\\_management](http://www.endpointprotector.com/products/mobile_device_management)

#### Acerca de CoSoSys

CoSoSys está especializada en el control de dispositivos de la red, la seguridad de punto final, la prevención de pérdida de datos (DLP) para Windows / Mac, Mobile Device Management para iOS y Android y el desarrollo de aplicaciones para el cifrado y la mejora de dispositivos portátiles de almacenamiento. La cartera de aplicaciones incluye funciones de control del dispositivo, File Tracing y File Shadowing, seguridad por contraseñas, sincronización de datos y seguridad de la red. CoSoSys distribuye sus productos globalmente a través de Distribuidores, Revendedores y directamente a los usuarios en <http://www.EndpointProtector.com>. CoSoSys es un desarrollador de software independiente, desde la compra de gestión de Astaro en julio de 2011. CoSoSys goza de una base de instalación cada vez mayor de usuarios en todo el mundo y fue reconocida en 2011 como una de las compañías de tecnología de más rápido crecimiento, siendo un ganador de la clasificación de 2011 Deloitte Technology Fast 50 para Europa Central. La compañía cuenta con oficinas en Alemania, Estados Unidos y Rumanía.

#### Imágenes y materiales adicionales:

[http://www.endpointprotector.com/company/press\\_room](http://www.endpointprotector.com/company/press_room)

#### Contacto de Prensa:

CoSoSys Ltd.

Angela Lepadatu

Tel.: +40 264 593 110 Ext. 116

E-mail: [angela.lepadatu@cososys.com](mailto:angela.lepadatu@cososys.com)

**Datos de contacto:**

Angela Lepadatu

Nota de prensa publicada en: [400040, Cluj-Napoca, Rumania](#)

Categorías: [Ciberseguridad](#)

---

**NotasdePrensa**

<https://www.notasdeprensa.es>