



Press Release

Endpoint Protector 2009 for Mac Introduces File Tracing for Portable Devices

New File Tracing and Temporary Offline Password features available for Mac OS X, offering complete control over online and offline use of portable devices

Boise, ID, Bucharest, Romania, October 13, 2010. The only device control, endpoint security and data loss prevention solution for Mac / Apple computers in the world, Endpoint Protector 2009, has just released a new version of its Mac application. The newly introduced features are designed to increase protection for business confidential data and to offer road warriors a way to stay active and productive when a permanent Internet connection is unavailable. Moreover, the carried data is kept safe from the common threats posted by improper usage of portable storage devices that often leads to severe security breaches.

Endpoint Protector 2009 now features the File Tracing functionality, which provides companies and their IT departments with enhanced control over data transfers and activity within their network. When enabled, the File Tracing feature logs all data and file related activity and stores it for later auditing. Each time an employee edits, deletes or renames a certain file originating from or subsequently copied to a portable device, his actions are recorded, along with his user credentials and the device specifications.

The second main feature of the new Endpoint Protector release for Mac OS X device control allows authorized company representatives to issue temporary offline passwords for staffers who are traveling. When on a business trip, employees might be unable to connect to the Internet and need to authorize a new portable device, a memory stick to save a presentation for an event etc. To help them save time and complete their tasks, a temporary offline password can be provided to them by phone and subsequently they can authorize devices for a period ranging from 30 minutes to one week.

“The new Mac version of Endpoint Protector focuses on two important aspects of device control and data loss prevention - keeping a close eye on data activity within the company to prevent possible leaks or theft (and File Tracing enables the needed close watch and audit) and making sure productivity and mobility are not impaired by security policies, while at the same time providing a safe way to work with portable devices,” explains Roman Foeckl, CoSoSys CEO.

Endpoint Protector 2009 is designed to minimize internal threats, reduce data leakage risks and control devices connected at Windows and Macintosh endpoints. It allows IT departments to proactively take control of the devices' internal use, while tracking all data transferred in or out of the protected network and enforcing encryption of data in transit on portable devices. It is available at <http://www.EndpointProtector.com>.

To request a 30 day free evaluation version of Endpoint Protector please visit:
http://www.endpointprotector.com/en/index.php/products/device_management_for_Mac_OS_X



About CoSoSys

CoSoSys is specialized in network endpoint security for Windows and Mac and development of software for portable storage device enhancement. The application portfolio includes functions from password security, data synchronization and network security. CoSoSys distributes its products globally through the world's leading hardware manufacturers, software Distributors, Resellers and directly to users at <http://www.CoSoSys.com> and <http://www.EndpointProtector.com>. CoSoSys enjoys a continuously growing installation base of users worldwide. The company has offices in Germany, the United States and Romania.

Images and additional materials:

<http://www.cososys.com/images.html>
http://www.cososys.com/press_room.html

Press Contacts:

Mirror Communications

Alina Popescu
Phone: +40 741 073753
E-mail: alina@mirror-communications.com

CoSoSys Ltd.

Anca Goron
Phone: +40 264 593 110 Ext. 113
E-mail: anca.goron@cososys.com