Press Release

Thunderbolt and USB 3.0 ports: two more reasons for companies to use Device Control and DLP solutions for Mac OS X to prevent data loss

Support for Thunderbolt and USB 3.0 ports against data theft and data leakage through portable storage devices is essential to protect company data is now available with Endpoint Protector 4 for Mac OS X

Cluj-Napoca, Romania, January 24th, 2013. While the number of companies incorporating more and more Macs into their networks is increasing, the need for protecting these computers against data leakage and data theft is rising. Especially since all new Macs come standard with Thunderbolt and USB 3.0 ports for even faster data transfer rates. Endpoint Protector offers now to companies the possibility to prevent data breaches that can occur by carrying data transferred on devices which are compatible with Thunderbolt and USB 3.0.

Thunderbolt and USB 3.0 ports are offering incredibly fast transfer rates which makes moving Gigabytes of data in seconds easy, but also dangerously fast for data thieves and accidental data losses. In order to secure Macs in business environments it is essential that companies address these risks. They can do that by pro-actively controlling the use of these ports which means either blocking or locking them down completely, or monitoring what data is being copied back and forth. Furthermore, it is possible to selectively allow only company owned devices (e.g. a company approved backup HDD), while preventing the use of personally owned USB Flash Drives.

Along the new support for Thunderbolt storage devices and USB 3.0, Endpoint Protector 4 is already controlling the use of CD/DVD, FireWire, card readers, USB and many other ports and device types that could lead to companies losing valuable data. In a time where everybody carries personal devices to work (hence Bring-Your-Own-Device) it is vital to take measures and to be certain that only trusted and approved devices actually can transfer data.

“Companies need to monitor what is happening to their data on Macs just like they do on their Windows PCs. In order to be safe, IT administrators should not allow the employees to use unapproved and unsecure devices that could cause data loss or make data theft easy. Locking down USB and Thunderbolt is simple and can be done centrally with Endpoint Protector to make sure data stays where it should” said Roman Foeckl, CoSoSys CEO.
About CoSoSys

CoSoSys is specialized in network device control, endpoint security and data loss prevention (DLP) for Windows/Mac and development of applications for portable storage device enhancement. The application portfolio includes functions from device control, file tracing and shadowing, password security, data synchronization and network security. CoSoSys distributes its products globally through Distributors, Resellers and directly to users at http://www.EndpointProtector.com. CoSoSys is an independent software developer since a management buyout from Astaro in July 2011. CoSoSys enjoys a continuously growing installation base of users worldwide and was recognized in 2011 as one of the fastest growing technology companies being a winner of the 2011 Deloitte Technology FAST 50 ranking for Central Europe. The company has offices in Germany, the United States and Romania.

Images and additional materials:
http://www.endpointprotector.com/company/press_room

Press Contacts:

CoSoSys Ltd.
Angela Lepadatu
Phone: +40 264 593 110 Ext. 116
E-mail: angela.lepadatu@cososys.com