Endpoint Protector 4.1 Adds Content Aware Protection

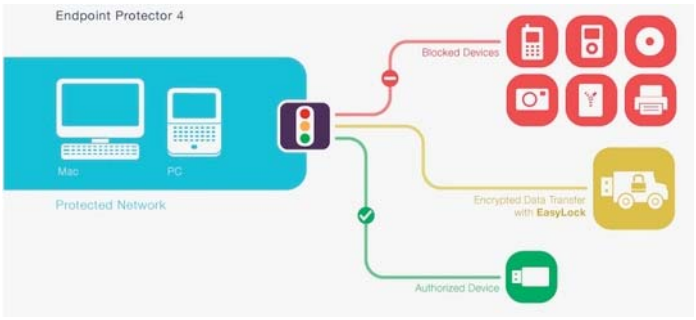
This is a Press Release edited by StorageNewsletter.com on Wed, May 30th, 2012

To prevent data leaks to cloud

Company data security is under threat more than ever with cloud services such as Google Drive, Dropbox and iCloud finding their way on company PCs.

Endpoints such as USB ports, CD/DVD drives, printers etc. are no longer the only concern when it comes to stopping leaks of sensitive data. The Internet and the cloud poses an even greater security threat by allowing an easy transfer of data through file upload services, e-mail, instant messaging applications and other types of applications. On top of these are the currently expanding cloud services, which bring new security risks for companies worldwide.

To prevent data loss for businesses via the cloud and at the endpoint, CoSoSys Ltd. announces the availability of Endpoint Protector 4.1 version as a customer preview with an Content Aware Protection feature available for its Windows Endpoint Protector Client.



The new version offers IT departments security features to minimize all risks of losing files to the cloud or of exposing them to data theft or data leaks. Having the ability to inspect in depth data on the Client PC endpoint before it leaves the network, it lets IT departments know at all times where, how and who in their network is trying to copy or move sensible information outside the company and take action by enforcing policies to either stop data before leaving the network or to monitor all data in motion, all this offering an insight to employee and insider intentions.

"*The increased use of cloud services to help share valuable business data without limits, has not only improved efficiency, but at the same time led to hard to detect data leakage threats, making data sharing over the cloud today's IT security matter*," says CoSoSys CEO Roman Foeckl. "*Taking action at the endpoint is the most effective way to a full data loss prevention strategy. Trying to stop data on the gateway is usually already a step to late since data has been encrypted by the specific application or service that accesses it and cannot be inspected anymore at this point for sensible content violations. Therefore DLP has to happen at the endpoint.*"

As more and more cloud services are adding additional security risks to company data, the Content Aware Protection feature allows data to be flagged as sensible based on each company's own defined policies that can be enforced for regulated data such as credit card numbers or personal identifiable information like social security numbers or on keywords and even for certain file types. It monitors all data use and identifies users trying to move data away from their laptop or workstation out of the network via:

- Cloud services (Google Drive, Dropbox, iCloud, SugarSync, etc.),
- Applications such as e-mail clients (Outlook, Thunderbird, etc.), Instant Messaging (Skype, Yahoo Messenger, etc.), Web browsers (Internet Explorer, Firefox, etc.) or
- Removable devices like USB flash drives or external hard drives

Endpoint Protector 4.1 with Content Aware Protection module is **available as hardware or virtual (€24) appliance**. The data and device security solution ensures a proactive protection against both inside and outside threats for organizations with integration and easy administration through its web-based interface.