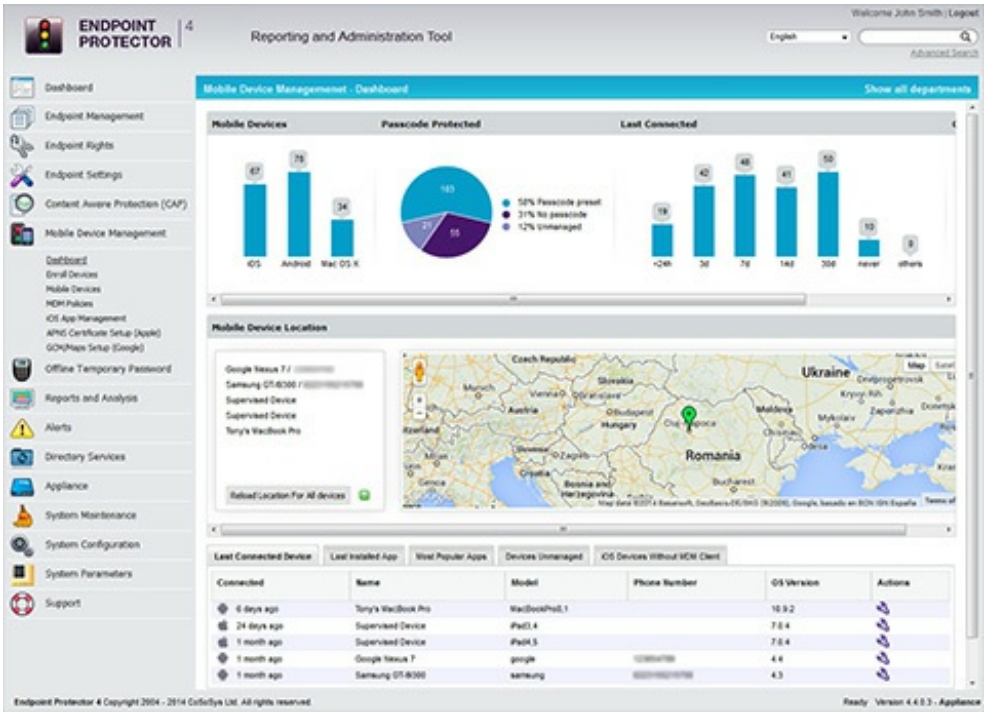
Connecting cloud storage services and cloud-based data loss prevention

Posted on 04 July 2014.

CoSoSys released a new version of My Endpoint Protector, a cloud-based Data Loss Prevention (DLP) and Mobile Device Management (MDM) solution for both Macs and PCs. The new features provide corporate IT departments with increased data loss and data theft prevention services to keep pace with the growing worldwide demand for cloud adoption and storage solutions.



According to internal research, CoSoSys discovered that the number of enterprise customers that opted for the SaaS version of their DLP and MDM solution has registered an increase of 140% since the beginning of 2014. The areas where SaaS DLP is mostly implemented include the United States and Western Europe, particularly in the United Kingdom, Germany and Switzerland.

“Our customers were keen to take advantage of Endpoint Protector’s functionalities straight from the cloud. For a significant percentage of companies, a cloud-based version is easier to test, it requires less resources and it represents a more agile way of securing information,” said Roman Foeckl, CEO of CoSoSys.

“Globalization has forced companies to allow the use of cloud storage services like Dropbox, Google Drive, iCloud, OneDrive, and many others, in order to support collaboration from different parts of the country or the world. The same reasoning is applied for cloud-based DLP and MDM solutions in the enterprise.”

In this context, data privacy while storing data in the cloud is a major point of concern for businesses of all sizes across all industries. Any and all corporate information, especially anything related to a company’s Intellectual Property, should be filtered before it ends up in a less controllable environment. Different levels of authorization for data transfers should also be put in place to make sure productivity is not affected.

The new version of My Endpoint Protector brings updates that support both IT administrators and organizations by enhancing protection against data loss and theft.

On the Content Aware Protection (DLP) section, the additions to My Endpoint Protector increase users' productivity and network performance by eliminating unneeded restrictions. Specifically, URL and Domain Whitelists allow data transfers to trusted web addresses and e-mail addresses.

For advanced custom content filters, Regular Expressions have been added, so IT Administrators can easily create their own data algorithms to be scanned in documents, which are consequently blocked and reported. Additionally, enhancements to the Offline Temporary Password features help mobile workforces obtain access to removable devices and enable users to send / upload files that normally are not authorized. The new version also provides a Custom Classes option, which can be used in scenarios like authorizing a specific brand of devices that are given by the management to employees.