Mobile Device Management for iOS and Android devices

Posted on 06 November 2012.

CoSoSys released Mobile Device Management (MDM) for iOS and Android as a new module within Endpoint Protector 4.3 including support for iOS 6.

With Mobile Device Management capabilities fully integrated in Endpoint Protector 4 Hardware and Virtual Appliances, IT departments can deal easily with the Bring-Your-Own-Device trend they are facing from iOS and Android users. The MDM features enable IT administrators now to monitor and manage mobile devices, while the Device Control features ensures a complete control over where these devices connect to in the network, offering overall to IT departments a powerful tool to secure data and audit the use of devices, said Roman Foeckl, CEO of CoSoSys.

The presence of smartphones and tablets in today´s corporate environments is extending the boundaries of business processes other times confided within a companys four walls. While there are significant benefits in adopting mobile devices as a way to increase work efficiency, there are also significant concerns for IT departments about how to keep sensitive corporate data secure wherever and on whatever device the employee accesses and stores it.

Mobile Device Management by Endpoint Protector allows businesses to embrace portability and mobility without compromising the security of their own business critical data and without burdening IT. The new module can be easily integrated in companies existing IT infrastructures, allowing for a secure and fast self or over-the-air enrollment and provision process, via E-Mail, SMS, web portal or QR code of both corporate and privately-owned devices.

Using a one-time-code enrollment mechanism, it prevents any unauthorized access and stops untrusted devices connecting to the company network.

As a complementary solution to the existing endpoint Device Control module for Desktops and Laptops, Mobile Device Management ensures a proactive protection over mobile endpoints, allowing IT administrators to efficiently manage mobile devices in a transparent manner from one intuitive web based reporting and administration interface. The new module addresses the major challenges faced by IT departments:

- Mobile data security, to protect against the latest data loss, leakage and theft threats with key features like strong security policies enforcement, advanced password rules, device encryption, remote device lock and data wipe
- Tracking and precise locating, offering complete reporting of where company critical business data is on devices and was at any time and for any managed device
- Mobile apps monitoring and management, allowing a close control over the large number of unwanted apps that can easily make their way on employees mobile devices.