Data loss threats on Macs

Roman Foeckl, CEO of CoSoSys, looks at how Macs became part of enterprise networks, and considers how to deal with the challenges this can bring.

In the last few years, an interesting phenomenon regarding people's consumer behaviour has emerged. No matter what they buy, their preference reflects their personality - the more customised, the better. This behaviour extends also to their workplace. You see on their desks personalised mugs, family photos and their personal gadgets, used for both work and leisure.

Apple long ago sensed this - and created MacBooks, iMacs and other iconic products, with a special design and user-friendly operating systems, for a certain category of people to use at home and the office. Eventually, more and more people identified with the values promoted by Apple. Users' demand for Macs is also driven by their fondness for iPhones, and thus searching for a similar user experience.

Employers have noticed that and use it to leverage productivity. They invest in Macs and use them as workstations or allow people to bring their own Mac to work, calling it the BYOD model. Therefore, Macs have become more popular in companies, and that homogeneous environment that existed with 100% Windows computers no longer represents the current state of play.

Biotech, graphic design and other industries have embraced Macs for a long time and now Macs are increasingly making inroads in all industries. The truth is that the current landscape of endpoints is a mix of Windows PCs, Macs and even Linux distributions, such as Ubuntu.

The impact of Macs being more popular in companies involves IT administrators on the one hand, as they are required to manage more platforms, and on the other employees, who benefit from the advantage of working with a high-end Mac. Inevitably, this takes us to a third and important component that sets a common ground between IT administrators and employees - DATA.

IN THE BALANCE If Mac OS X has a reputation for being more secure compared to Windows when it comes malware, then the scales are balanced when it comes to data losses. The chances of data breaches occurring are similar for both platforms, since Macs come with super-fast thunderbolt and USB ports to transfer gigabytes in seconds. Yet the bigger threat is represented by uncontrolled data transfers to the cloud, with services like Dropbox and iCloud or webmailers, like Gmail. With an alarming number of leaks, intentional or unintentional, caused by insiders, the need for a device control and content-aware data loss prevention solution for Macs is bigger than ever before.

There are very few solutions to cover the most obvious methods used by employees to take their work home or in business travels. With Endpoint Protector from CoSoSys, IT admins can go a step further to secure data on Macs and prevent data losses. They have the option to control data transfers to removable devices made from Macs and vice versa, in terms of just monitoring or also blocking. At the same time, they can create flexible policies for users concerning transfers by email or to the cloud, while also having detailed reports for audits and for specific measures, should policy violations occur.

In summary, IT admins shouldn't overlook Macs when it comes to insider threats, as they exist independently of the operating system.

For more information about Mac OS X DLP solutions, visit www.endpointprotector.com