Are more businesses turning their back on BYOD?

Joakim Sundberg, 2013-29-04

BYOD and working flexibly are vital tenets of many modern businesses, but there's no denying that both are still viewed with a certain scepticism in some quarters. You only need to look as far as Yahoo's decision to ban working from home earlier this year for very public evidence of this, not to mention recent calls for businesses to ban the Facebook 'Home' launcher for Android devices for fear of security breaches.

These fears are understandable, there are very real security threats that can be introduced by flexible working policies and unrestrained BYOD (we'll leave the productivity issues for another time!). However, these are not threats that are insurmountable and there are benefits to be enjoyed by businesses that can contain the risks.

To deal with the threats inherent in remote and flexible working, it is vital to have a network which is contextually aware. By this I mean a network which can identify the source of traffic geographically, by type of device and by authentication and then make intelligent decisions based on this information. Say your CEO is trying to access files from the server on their personal laptop; if the correct security software installed and network access is secure then that would be fine, but if there was a question over the security of the connection or the device, the network could intelligently deliver a read-only access to the files that they need. Preventing any unwanted intrusion attempts while simultaneously allowing the CEO to make use of the IT resources they expect to be available. It's a win-win. The network is secure and the CEO can work unimpeded.

BYOD is a slightly different matter. A contextually aware network will help to deliver appropriate content types to a mobile device (for example, delivering lower resolution images to improve load times on mobile web apps) but the security implications of having personal and corporate information housed on the same device are still there. I know very few people who are happy to have their personal communications and files monitored by their company, but this is frequently the approach taken in the current generation of mobile device management tools. Far better, is to have a separation of the business apps and files from the personal – as explained by my colleague Thorsten Freitag. This can be achieved by management at the application, rather than device, level – or as we call it: BYOD 2.0.

Mobile application management adds a layer of control to only those applications used for business purposes, encrypting data and making sure that only secure connections are used to transmit it. This means that corporate oversight is kept only to the corporate functions of the device, granting users the freedom to use their devices for both personal and business purposes with peace of mind, and giving businesses the control that they require.

F5 Networks, Inc. | 401 Elliot Avenue West, Seattle, WA 98119 | 888-882-4447 | f5.com

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
apacinfo@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com