BYOD 2.0: Moving beyond MDM

Joakim Sundberg, 2013-19-02

While it seems like the industry has been talking about it for years, a recent report by Forrester warned that BYOD uptake has only just begun.

It's true the concept started to be discussed by corporates back in 2007 when business executives began demanding access to corporate resources on their shiny new iPhones. But Forrester's right in that it's only now that large numbers of organisations are starting to implement BYOD initiatives. And this increase is largely driven by the rise of cloud apps we can access on our mobile devices, and the influence they're having on the way we work.

The appeal of BYOD is obvious. Allowing employees to access their data on personal devices, from any location at any time provides a number of benefits; they are likely to work more flexibly and efficiently, as well as gleaning more satisfaction from their jobs. On the flipside – and the concern that's held many businesses back – is the numerous security issues it raises as employees are demand access to sensitive corporate data on unmanaged and potentially unsecured devices.

At F5 we'd suggest the first phase of the flexible working revolution, BYOD 1.0 if you will, was the period from 2009 – 2012. This was the industry's first attempt at solving BYOD security issues in the workplace and this was done by managing employees devices as a whole (MDM: Mobile Device Management). But MDM is not without its drawbacks. Employees don't like giving their companies control over their devices as they contain personal applications and information. When an employee leaves a company, wiping their mobile may mean losing all their enterprise data along with photos of their family. IT departments don't like this scenario either; having to manage an employee's entire device means their personal traffic becomes an IT problem.

But as we enter BYOD 2.0, which Forrester indicates is the true beginning of the mobile working revolution, these issues are being addressed. MDM is over and Mobile Application Management (MAM) is set to take its place. By managing applications rather than entire devices, employees can feel safe in the knowledge that their personal data is kept private and that they have control over their own devices. IT departments are happy because they now only need to concern themselves with the control, management and security of enterprise data and applications, rather than personal content.

Today we've announced our Mobile App Manager [F5 Mobile App Manager] which securely extends the enterprise to personal mobile devices. This builds on the BYOD 1.0 foundation, but the emphasis has now moved from management of the device to management of the application. Business applications are the future of BYOD, offering employees more control, more flexibility and the opportunity to work within a safe, secured infrastructure.

Executives have been quick to embrace the BYOD trend and now that their concerns over enterprise management of their personal data should be a thing of the past, it'll be interesting to see just how far the trend goes.

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