F5 Forum London 2013: Joakim Sundberg on enabling the mobile workforce

Nick B, 2013-06-03

Joakim is a security solution architect for F5 in EMEA focusing on mobile access. He was the final speaker at F5's UK customer forum at Chelsea FC's West Stand conference centre.

Access policy is a pretty important topic in application delivery for mobile workers. Access itself is a given. No access = no mobile workforce. Context-based application of security policy is the thing that can make an access policy work for the organisation AND the the employee trying to access critical apps…or neither of them.

It's one thing to allow access to a specific user via a VPN, it's another to help the organisation understand who, where and from what device an access request is coming from.

The latter case is where context is applied, and in a BYOD, Web 2.0 world, where devices are often outside of corporate enforcement and control, applying effective policy is an essential part of supporting brand reputation, data integrity and making sure your apps are secure.

Beyond corporate necessities, user experience is something that is often overlooked when putting security policies in place. Consider how long you stay on a web page when it doesn't load – a matter of seconds, perhaps less, before you give up.

If your mobile workforce has to use business apps that are slow or unresponsive, they are about as likely to continue to use them as you would be to continue to use a retail shop's web page that takes 10 seconds to refresh the page.

So, security policy and the provision of an excellent user experience go hand in hand for application provision to mobile workers.

F5's Mobile Access Manager means you can segregate personal devices into 'corporate' and 'personal'. This means that – without affecting the 'personal' area of an employee's iPhone - enterprises can take steps to controlling the profile of an employee's personal device. It securely connects only corporate applications to the enterprise network, and manages only the enterprise content and applications on a device, as opposed to the entire device.

Why is this good news for IT teams as well as employees? For the enterprise, Mobile Access Manager allows the application and management of security policy. For the employee, control is retained over their device. Because F5 not only secures apps but speeds them up to, user experience is also improved.

BYOD 2.0 starts here.

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