BYOD User Challenges

See Kay Leong **(4 mins)**

Now, BYOD does pose some challenges. Let's look at what the users want. As much as the BYOD trend has brought many benefits, it poses quite a number of challenges. Let's look at it from a user perspective, like yourself and me. These are some of the challenges that we need to address.

First, how to keep it simple and consistent?

BYOD solutions and technologies are quickly evolving. One of the largest challenges is how to make it simple for people to get connected to and use company resources and applications to do their day to day work. The different types of mobile devices, the range of connection types and locations, and the lack of widely adopted approaches can cause difficulties for users.

Each device brand and form factor may require slightly different steps to be on-boarded and connected. Security precautions may vary depending upon how and where the user is trying to connect. For example, the corporate WiFi may require only credentials, whereas connecting through a public WiFi hotspot may require more than just the credentials. It require a virtual private network (VPN), keying in your token in order to get connected. This is some examples of security being built for users that are connecting remotely.

Ultimately any BYOD solution tends to be as simple as possible for users. If possible, provide a common experience no matter where and when they are connecting, and be as similar as possible across devices.

Second, Separation of work and personal data

Let's look at seamless transition between devices. BYOD brings a mix of personal and work tasks on the same device. Example, like contact lists, email, your data in your personal devices; the applications, Internet access can also pose a challenge. Ideally, users want to separate their personal data and activities from their work. Things like personal photos, text messages, phone calls, and Internet browsing done during their personal time, need to be subjected to personal privacy, while documents, files, applications using corporate data, and Internet browsing done during the company time need to be in compliance with corporate policies.

Some companies do allow their employees to use their personal devices only after the employee sign an agreement so the company can monitor compliance acceptable use policies, and otherwise, and to protect corporate data. In some cases this may include remote wiping of all data on the device- potentially including personal data- can be a source of contention between IT and users if not properly managed.

Third, Getting the Productivity and Experience Needed

One of the major drivers of BYOD is employees who want to take advantage of productivity tools they use as a consumer in the workplace. Companies want to embrace and benefit from that productivity, but also need to apply the appropriate security and policies to protect corporate data. If such security measures are too intrusive, it may erase any productivity gains.

Let's take an example, a common complaint in a company that lock down access to business applications and data through the deployment of Virtual Desktop Interface clients on a tablet device degrade the user experience or impact the speed such that the employee does not get a good experience. Now, that defeats that consistent experience of multiple devices and seamless transition between devices that users want. Thus defeats having BYOD in the first place.