BYOD Building Blocks

See Kay Leong **(4 mins)**

We cannot use point solutions to implement BYOD, we needs to take an architectural approach by building layers to support all the devices. What are the building blocks that will support a successful BYOD implementation?

The BYOD Smart Solution by Cisco is designed as a flexible set of building blocks that can be used to deliver different levels of BYOD business policies. These building blocks can be used or removed, depending on the customer's needs and the use case that they plan to build on. This gives IT, and all the people that are involved in the BYOD solution the flexibility to grow, and expand the network.

- Starting with the core infrastructure that comprises the network components such as the switches, routers. This infrastructure must be ready to support BYOD and to enable effective workspace delivery. The infrastructure is analogous to the road that supports the different vehicles. If you do not have good road, no matter how powerful your vehicle is, or how good a driver is, or even if you install the best tyres that you can get in the market your ride will be hindered by the condition of the road, and you will have an inefficient and rough ride.

- The next important block is Security (secure mobility), enabling seamless access anywhere. In BYOD, most devices access the network via wireless, (where data) is transmitted over the air. Data transmitted needs to be secured, and when users move from one network to another network, roaming from one technology to another, the security level need to be ensured.

- Policy management. How do you provide users and their devices with access to the right information when they need it. Take the scenario of a student and a lecturer. The student attends a lecture using his personal tablet to access the school network. The student should only have ‘student access’ that allows him to access the Internet, student lecture notes, tutorials or any reference materials. He should not have access to the lecturer’s guide, or exam papers especially, that are not scheduled for release, or school business applications. Hence, such policies have to be enabled, and defined, and be managed.

- Workspace management- providing IT with a solution for managing and securing the devices, as well as allowing end-to-end visibility across the network by applications, services, and users. For example, if a device is reported lost, how do we ensure that the lost device does not result in the compromise of data confidentiality when it falls into the wrong hands? This is where Mobile Device Management (MDM) comes into play.

- Last, but not least, the 'Applications' box which schools, corporate world allow BYOD devices to access the applications and ideally, it's seamless as if they are on the wired network.

The BYOD Smart Solution - In Cisco terminology we call it the Core Infrastructure Enterprise Networking where we have the wireless, the routers and the mobility management tool like 'Prime Infrastructure', that are built under the core infrastructure.

Under the 'Policy Management Infrastructure, what we have is the Identity Services Engine (ISE), which will determine, and enforce policy- how, when, what, where. When the users can access, what devices to access at what time, and what application. This enforcement of policies are done by the Identity Services Engine (ISE).

And of course, with our 'Secure Mobility', we're tie-in together with Cisco firewall, which is what you can see over here, is an ASA - Adaptive Security Appliance, working hand-in-hand with VPN client, which is known as AnyConnect.

Last, but not least, the Workspace Management. Mobile Device Management (MDM). If the device is lost, employee left the company, not in his job role, you don't want the user to access things that he is not allow to access to. This is where the MDM will come into play.

This will allow us to have a good, secure, seamless BYOD solution.