Get Mobile Now — Security And Application Support Solutions For BYOD

What role will you play in helping your customers address the security and application challenges that come with the BYOD (bring your own device) to work trend?

By Paul Andersen, marketing manager, Array Networks

The consumerization of IT is underway. In its report *Tablets Will Rule the Future Personal Computing Landscape*, Forrester predicts sales of 375 million tablets in 2016 with over 750 million tablets in use. Because tablets are productivity enhancing, portable, and trendy, employees are bringing them to work in droves. Like cloud computing, mobility is causing businesses to reevaluate their approach to information technology.

Referred to as *The Consumerization of IT* or *BYOD*, the trend is here to stay. As a consequence, IT is faced with solving two major challenges. The first is security. Every mobile device connected to the corporate network is a threat and every personal tablet and smartphone introduces the potential for data leakage. The second challenge is a lack of native enterprise apps. While this will change over time, there exists a gap between the volume of applications used in the enterprise and those that are available as native mobile apps.

Security concerns arise when traditional VPNs are used to connect mobile devices to the corporate network. VPNs create a tunnel through which data may escape or attacks may be introduced. In addition, it is impossible to lock down personal devices the way one would a managed device. Mobile devices are also greater in number, more prone to becoming lost or stolen and exposed more frequently to the risks of personal use. Mobile device management (MDM) provides control over mobile devices connected to the corporate network and simplifies provisioning of apps, but does not address the above concerns.

Although many more native enterprise apps will be developed over time, the challenge is in enabling mobility and BYOD today. At present, the vast majority of enterprise applications remain tied to Windows and traditional desktop environments. As a result, solutions aimed at mobility and BYOD must address not just security, but also provide a means by which to bridge the gap between mobility and the applications employees use every day to be productive and complete their work.

Paul Andersen

Array Networks

Paul Andersen is the marketing manager at Array Networks, a provider of networking solutions that allows companies to give access to any user, anywhere, on any device to applications, desktops, and services running in either the cloud or the enterprise data center.

In response, solution providers and value added resellers are leveraging a clever approach to help customers get mobile today — one that takes advantage of remote desktop access and secure access gateways to extend applications on physical or virtual desktops or terminal services to mobile devices.

Unlike using VPNs, with this method, mobile devices never connect to the corporate network. Because data never leaves the corporate network, data leakage is fully eliminated, and because devices are kept off the network, the risk of attack is eliminated as well.

Any application on a physical desktop or in a virtual environment can be immediately "mobilized" to provide full access to enterprise applications from personal tablets and smartphones. While the experience is less polished than a native enterprise app, it is counterbalanced by the ability to cost-effectively and securely help customers mobilize any enterprise application, right now.

When the balance between traditional applications and mobile apps shifts, mobile VPN on the secure access gateway, in conjunction with MDM solutions, may be enabled to support native enterprise apps. Adding secure access gateway solutions to their portfolio, solution providers and value added resellers gain a platform capable of generating revenue and helping customers get mobile now and in the future. ●

Web Exclusive