



Comment Article

Securing remote users

Commissioned by Ingram Micro – Dec 2010

By Bob Tarzey, Analyst and Director, Quocirca Ltd

More and more of us are working remotely, for at least some of the time, enabled by an increasingly diverse range of mobile devices. For businesses this has many benefits whether it is making field based employees more responsive, improving workflow or enabling flexible working practices. But many studies show that the biggest perceived down side is security; for resellers this is an opportunity.

Remote devices themselves, be they smartphones, netbooks, tablets or laptops, provide only small margins for resellers, as do the network connectivity services that link them to back office applications. But mobile device management (MDM), software and services to manage and secure these growing fleets of devices, are more attractive.

Controlling what employees can get up to and ensuring that their use of IT is safe is far easier when they are constrained behind a firewall than when they are 'at large' with mobile devices. There are three basic problems to solve: protecting the device from malware, protecting the data generated and stored on the device and securing and authenticating the connection.

With the larger form factor devices (laptop, netbooks and some tablets – mobile PCs from hereon) it is possible to protect the device and the user by forcing access back via the corporate network. They are then subject to internal security controls. There are three basic ways of doing this:

1. Enforce the use of virtual private networks – a controlled work space can be created on the mobile PC with access to a given set of backend applications, user productivity applications (word processors etc.) are still usually installed locally

2. Use virtual desktops infrastructure (VDI) – this means all applications are run inside the firewall including user productivity applications
3. Force all network traffic back via a firewall – user productivity applications are run locally, but everything going to or from the PC is subject to internal controls

Securing the use of smartphones has thrown up some new challenges and, as yet, it is not really possible to take a unified approach to managing all mobile devices. For a start it is harder to force smartphone users back on to the corporate network, due to the convenience of making direct internet connections via mobile network operators (MNO), second VDI is hard to adapt to their smaller screens, third there are different device based security products for the different types of devices and finally, the range of operating systems for smartphones is much more diverse.

There is one measure that can be taken centrally to protect all remote users; email filtering. Most organisations today will have this in place to catch spam and email-born malware and also to check what is being sent via corporate email. However, the target of many malware writers and an increasing source of data leaks is web traffic. It is possible to use proxies to force web access for mobile PC users via a central web traffic filter, but, for the reasons outlined above, this is less easy to enforce for smartphone users.

So, as smartphones increasingly become target for data theft and they are, by their very nature, easier to lose, it is necessary to make sure the device itself is secure. This also applies to any mobile PC for which internet access is allowed independent of the corporate network and, unless device based security blocks the use of low cost of 3G dongles, this is almost inevitable.

A few years ago, given the range of mobile operating systems, it seemed obvious to select a corporate standard smartphone and impose it. But the increasing overlap between work and personal lives means most employees prefer to use the device of their choice. This consumerisation of IT may look like a headache for IT managers, but it has one big advantage; if the device an employee uses for work is also their favourite toy – they will take more care of it – step one to mobile security – user love of their device!

But that is not enough; there are a number of other steps that need to be taken:

Password protection – basic but obvious – making sure the device cannot easily be used when it falls in to the wrong hands.

- Malware protection – now offered by many of the security vendors for mobile PCs and smartphones. Smartphones are now a target as they are being used more and more to access sensitive data.
- Device firewall – these are now becoming available for mobile devices, allowing the customised filtering of web traffic on the device itself
- Encryption – if any amount of sensitive information or intellectual property is to be stored on a device then that data, or probably all data, should be encrypted. Recent rulings by regulators make this clear. Remember, contact list with telephone number and note may constitute sensitive data.
- Remote disablement and wipe, should a device be compromised making sure the services available to it are discontinued and that data is wiped (less of a concern if the data is encrypted).
- Advanced security features including SIM recognition and geolocation using GPS

Ensuring all this protection is in place and remains so, that device software and security is up to date, and that action can be taken when a problem arises requires MDM tools. Such tools can also enable the auditing of device ownership and use, for example logging phone calls made, SMS content and photos.

For many businesses, especially mid-market and smaller ones, these will be new and unprecedented challenges. The number of threats and the range of options for mitigating them will seem daunting and the in-house skills will not be available. Resellers that provide tools and services for managing mobile device security and safe remote IT access will be relieving their customers of a headache and enabling their businesses for the future.

About Quocirca

Quocirca is a primary research and analysis company specialising in the business impact of information technology and communications (ITC). With world-wide, native language reach, Quocirca provides in-depth insights into the views of buyers and influencers in large, mid-sized and small organisations. Its analyst team is made up of real-world practitioners with first hand experience of ITC delivery who continuously research and track the industry and its real usage in the markets.

Through researching perceptions, Quocirca uncovers the real hurdles to technology adoption – the personal and political aspects of an organisation's environment and the pressures of the need for demonstrable business value in any implementation. This capability to uncover and report back on the end-user perceptions in the market enables Quocirca to advise on the realities of technology adoption, not the promises.

Quocirca research is always pragmatic, business orientated and conducted in the context of the bigger picture. ITC has the ability to transform businesses and the processes that drive them, but often fails to do so. Quocirca's mission is to help organisations improve their success rate in process enablement through better levels of understanding and the adoption of the correct technologies at the correct time.

Quocirca has a pro-active primary research programme, regularly surveying users, purchasers and resellers of ITC products and services on emerging, evolving and maturing technologies. Over time, Quocirca has built a picture of long term investment trends, providing invaluable information for the whole of the ITC community.

Quocirca works with global and local providers of ITC products and services to help them deliver on the promise that ITC holds for business. Quocirca's clients include Oracle, Microsoft, IBM, O2, T-Mobile, HP, Xerox, EMC, Symantec and Cisco, along with other large and medium sized vendors, service providers and more specialist firms.

Details of Quocirca's work and the services it offers can be found at

<http://www.quocirca.com>