

## Quocirca's Changing Channels – End Point Security Attracts New Vendors

By Bob Tarzey, Service Director, Quocirca Ltd

End point security is a fast maturing market and is becoming big business. Many of the major vendors have products, or at least future plans. But it is still worth resellers looking at some of smaller vendors who have interesting new products and ideas.

End points include everything from desktop PCs, printers, wireless access points through to some of the most vulnerable; mobile devices such as laptops, PDAs and smart-phones.

On any network the key is making sure devices that are supposed to be there are, that they are safe, and remain safe, and are used by users authorised to do so. Obviously, mobile devices are the most vulnerable - they regularly reattach to networks having been who knows where. But it is not just mobile devices: printers with their own operating system and storage capacity can be added to networks on an ad-hoc basis and, if not secured, can be compromised. A wireless access point can be added to a network with ease and who knows who might be accessing it. Once you get down to the level of USB devices the nightmare of monitoring activity on a large network becomes clear.

Giving employees the benefit of the doubt (for the time being), let's assume their threat to the network is benign. If this is the case, all we need to do is to make sure that their devices, especially mobile ones, start off and remain secure. This requires having a personal firewall, anti-virus and other content security software installed on each device. But just as important is ensuring this remains up to date. To do this the device needs checking each time it reattaches to the network. This is the driver behind Cisco's Network Admission Control initiative (NAC).

NAC validates a device when it attaches to the network, whether from a local or remote location, making sure security software is up to date – it can also check the patch level of the operating system. While this is a Cisco initiative, it has attracted a high level of interest - 22 other vendors are already shipping compliant versions of their products and many more are in development. This means your anti-virus or patching software, if NAC enabled, will be able to interface to the Cisco Trust Agent when it attaches to the network and any required updates can be automatically applied. If the Trust Agent identifies something it is unable to fix, the device can be quarantined. NAC is not the only show in town; Microsoft is working on something similar called Network Access Protection (NAP) to be supported in

the next versions of its desktop and server operating systems. Microsoft and Cisco have been mumbling about co-operation.

For NAC to work there needs to be software on the end point that can communicate with the Cisco Trust Agent, although it can be enabled third party software. But, what about all those less intelligent end points and other activity that might go on? Let's put less trust in the employee and assume they may be up to no good. What if they try to use mass storage USB devices to steal company information or send confidential attachments via an instant messenger? What if a printer is installed with an already compromised operating system? This requires constant end-point monitoring.

Symantec recognised this and, in October 2005, bought one of the early leaders in this market – Sygate. The Sygate product can monitor all end points - from PCs to printers and photocopiers. It knows what is authorised to be on the network, when something new appears, and what sort of state it is in. Similar products are available from other vendors, like McAfee's Policy Enforcer, SecureWave's Sanctuary and StillSecure's Safe Access.

With all this activity in a fast maturing market it would be brave to be a start-up. But that is just what an Israeli company Promisec is doing. Having launched its Spectator Professional product just a year ago, it is now going to try and crack Europe.

Promisec has some advantages - it has learnt from what has gone before and has produced a completely clientless product. This means it can be used to monitor any device on the network and report on its behaviour. Currently, it can only fix Windows devices, uninstalling applications, reversing registry changes, killing processes etc. Working with white-lists and black-lists, Spectator can be used to define what behaviour is and isn't allowed on a network. Use of instant messaging can be banned or controlled, the use of certain USB devices can be prevented or reported on. However, perhaps one of the most interesting initiatives from Promisec is one that could really help resellers with their day to day work.

The trouble with all IT security is convincing the customers it is something they need to invest in, especially cash strapped small businesses. Resellers and vendors alike can (perhaps unfairly) be accused of scaremongering. Promisec will licence its product to

resellers to sell as an auditing service. For a fixed fee a reseller can use it to audit a customer's network for a period of time and show them just what is going on. Of course, Promisec hopes this will lead to a sale in the longer term, but once a business gets a better view of exactly what is happening on its network, it may decide it has more urgent investments to make first – still an opportunity for the reseller though.

## About Quocirca

Quocirca is one of Europe's leading independent industry analyst firms. One of its biggest assets is the core team of highly experienced analysts drawn from both the corporate and the vendor communities. This team prides itself on maintaining a bigger picture view of what's going on in the IT and communications marketplaces. This allows all of Quocirca's activities to be carried out in the context of the real world and avoids distractions with fads, fashions and the nuts and bolts of specific technologies. Quocirca's focus has always been the point of intersection at which IT meets "the business".

## Quocirca Services

The insight and experience that comes from working as an industry analyst as well as a practitioner allows the Quocirca team to contribute significantly to IT Vendors, Service Providers and Corporate clients. To this end, it provides a range of consulting and advisory services. Details of these, along with some of Quocirca's latest analysis, may be obtained by visiting <http://www.quocirca.com>

Quocirca also provides bespoke primary research services through its daughter company QNB Intelligence. This involves interviewing thousands of senior decision makers on a quarterly basis.