

## Quocirca's Changing Channels: Of Microsoft Forefront security

By Bob Tarzey, Service Director, Quocirca Ltd, July 2<sup>nd</sup> 2007

With the launch of its Forefront security product range this week, Microsoft has deployed its tanks on the lawns of Symantec, McAfee and many other IT security vendors. So is it time for resellers to entrust Microsoft with all their customers' IT security needs and kiss goodbye to their current security partners?

Not quite.

In fact Microsoft's offensive started six months ago with the launch of its Windows Live OneCare service aimed at consumers. OneCare provides consumers' PCs with continuously updated signature-based protection against viruses, worms, spyware and so on. It also includes backup and restore capabilities.

Both OneCare and Forefront share a common desktop anti-virus engine based on technology Microsoft acquired four years ago. Other than this Forefront is very different to OneCare. Its broad range of client and server based protection for business is mostly based on various acquisitions Microsoft has made over the last few years which it has eventually pulled together in to a coherent suite, at least from a marketing view point.

The Forefront product range includes:

- Forefront Client Security
- Forefront Security for Exchange
- Forefront Security for SharePoint
- Internet Security and Acceleration Server (ISA) 2006
- Intelligent Gateway 2007

On the surface this looks like a fairly comprehensive security suite, but there are a number of good reasons why resellers should maintain their existing relationships with security vendors while taking a look at the new Microsoft offerings. The most obvious of which is that Forefront anti-malware components only secure Microsoft platforms. This might be OK for some smaller business, but larger business need

something more comprehensive to secure their heterogeneous infrastructure.

On the desktop Forefront alone does not provide a range of end point security functions such as controlling the use of USB devices and making sure corporate policies around online activities are adhered to. This can be done but only if used in conjunction with Microsoft's Active Directory, which is not part of Forefront.

Furthermore, ISA server currently only provides comprehensive URL filtering capabilities if a third party product like Websense is separately purchased. A large part of accelerating network traffic is cutting out unnecessary user activities like surfing YouTube, downloading music and listening to the test match. Microsoft has actually acquired technology to do this but is yet to deploy it as part of Forefront.

Microsoft itself admits that the Forefront products for Exchange and SharePoint are not the most comprehensive form of protection in their own right. Microsoft has some very impressive figures for spotting known threats but these all relied on using five different virus scanning products including its own. Kaspersky, CA, Sophos and Norman were highlighted amongst a total of seven currently supported. This simply recognises real world practice where IT departments go for the belt and braces approach of multiple anti-virus engines for server protection.

Another problematic area is management. For its devotees Microsoft is also launching a Server Security Management Console. But this will only manage Microsoft Security products, in this initial release at least. And therein lies Microsoft's biggest problem. Security is nothing new, businesses have been investing in it for years and have lots of existing products deployed that they are familiar with and are not likely to ditch in a hurry. Those existing products will protect a range of Microsoft and non-

Microsoft platforms and in many cases management tools will be in place.

Microsoft could attempt something underhand like embedding security in its operating systems. There are honourable reasons to do this over and above winning market share; Microsoft has a genuine interest in seeing that its customers use of its products is safe and secure. The majority of internet access is carried out using Microsoft Internet Explorer running on Microsoft Windows operating system – so Microsoft has a massive brand protection issue. But such a move would almost certainly be deemed anti-competitive and Microsoft has stated categorically that the Forefront products will be sold and shipped separately.

Of course, behind the scenes all sorts could go on. Who knows what will go into Microsoft's Select Agreements for its customers' comprehensive use of its products. Who knows how its agreements with PC manufacturers will change, they all work with Microsoft already to embed Windows. But resellers will be the key to how quickly Microsoft is able to penetrate the

market for IT security. Resellers are charged with protecting their customers' IT and data assets and should be cautious about relying on Microsoft's products alone for the reasons outlined above.

There is a danger of panic. If Symantec, McAfee and others seek to defend themselves with a price war it could play into Microsoft's hands; suppose one of them were to offer desktop anti-virus for free in order to maintain or grow market share. Microsoft would then see little danger in doing the same thing as it would no longer be anti-competitive, it would then be free to leverage the power of its desktop and server Windows installed base.

Microsoft's security competitors need to carry on with what they have been doing for last few years in the build up to the Forefront release. Continue to build comprehensive, leading edge security suites which provide for all the security requirements of their customers. Microsoft tanks aren't going to be withdrawn but they still only have limited fire power.

## 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's primary research involves the surveying of many thousands of technical and business end users each quarter, analyzing their perceptions of the possible impact of emerging, evolving and maturing technologies on their businesses.