

Straight Talking – Tighten content security

By Bob Tarzey, Service Director, Quocirca Ltd, May 2008

Spam has been with us, in name at least, for some 15 years. According to the watchdog Spamhaus, 90 per cent of all email now sent is spam. Fortunately that does not mean 90 per cent of our inboxes are filled with the stuff.

The problem has been contained through the widespread deployment of anti-spam products and services in the highly competitive market of the past decade.

Before spam became a big problem, there were still specialist email security vendors like Clearswift and Marshal Software that checked outgoing email to ensure it complied with internal rules on content distribution and decency.

But that was the mid-1990s, when sending email externally was a relatively new concept and volumes were low. The vendors' software was installed on email servers themselves - at the heart of the IT department, which was the last place spam with its sometimes viral payloads was welcome.

Then came a rapid evolution of products that kept spam at arm's length - either appliances at the network edge or in-the-cloud services that ensured an almost clean incoming email stream. These specialist solutions identified and eliminated spam but also targeted its sources and cut them off.

Many of the biggest names to have emerged in email security have now been acquired by the big IT infrastructure vendors. We now have such pairings as Google and Postini, Microsoft and FrontBridge, and Cisco and IronPort. Others have become, or remain part of, some of the major IT security companies, such as Trend Micro, Symantec, Websense and Secure Computing. A few, like MessageLabs and Mimecast, still retain their independence.

The interesting thing is that the market has now come full circle. With most business users having spam controls in place, the email security vendors have found new business harder to acquire and have been limited to attracting

competitors' customers rather than finding green-field opportunities.

This difficulty has meant they have started to target broader content security issues, such as content accessed and uploaded via web browsers and email archiving.

The aim is to expand the range of products and services sold to existing customers and to be more attractive to those of competitors who may be tempted to jump ship.

This broadening of focus has also allowed a number of small vendors that might otherwise have died to diversify and stay in the market. Both Marshal and Clearswift now see themselves as content policy engines.

Regardless of the content's origin or destination, they aim to ensure people only distribute content they are authorised to. Others like Tumbleweed and Proofpoint, having failed to establish a strong presence in Europe first time around, reckon they can make more of a mark with a renewed focus.

The choice can seem mind-boggling if you take all these vendors and review them alongside other content security specialists such as ScanSafe, which specialises in managed services for web security; Bloxx with appliances for web security; and anti-spyware vendor Webroot, which recently acquired spam-filtering firm Email Systems.

The whole market has converged on content security for a good reason - and one that is sometimes lost sight of. One of the main functions of IT is to allow the secure sharing of content, within organisations and externally.

For this to occur within employers' and regulators' guidelines requires policies to be in place and implemented. This has led to much talk about data leak prevention (DLP), a term that has come into general use in the past few years.

DLP is all about stopping the wrong stuff going to the wrong people. Most vendors will have the term somewhere on their marketing materials.

But there is no silver bullet for DLP. For any organisation this is a broad discipline that requires integrating multiple products from different vendors.

First there are people - who they are, what groups they belong to. For most organisations this information is already defined in existing directories, generally Microsoft's Active Directory or an LDAP-based product. Any content-filtering products need to integrate with this and build on it, and not require redefinition.

Then there is content. Nearly all the products from content-filtering companies deal with data moving across networks - apart from some email archiving services.

But content spends most of its life at rest sitting quietly on a disk somewhere until someone disturbs it. Content security must start here,

ensuring that such data is secure, whether on a storage array in a data centre, on an employee's desktop or on some mobile device out in the field. Content filtering companies do not address this.

Only when content is on the move - or when it has been created on the fly, as are many emails - can policy engines really decide what content is and if the person doing something with it should be authorised to do so.

Before investing in a new product from a content-filtering vendor, perhaps based on some lively marketing relating to the hazards of data leaks, IT departments should take a good look at what is already in place and what gaps need filling.

They may well find they have many of the components already. Where they do not, existing suppliers may already have evolved their offerings to plug those gaps.

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, Dell, T-Mobile, Vodafone, 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>