



## Comment Article

### Policy everywhere, with little to link it – July 2009

By Bob Tarzey, Analyst and Director, Quocirca Ltd

As Quocirca discusses in its freely available report "Content Security for the next decade", policies that define the way data must be handled are fundamental to good e-security practice, but where do you store the associated e-security policies? A written set of policies for handling data should be the starting point and such a document should be readily available to all employees and, where relevant, external data users for a given organisation. But policy can be enforced through a range of security tools in various parts of the IT infrastructure and this can lead to policy needing to be defined in several places.

For example, a policy may say that those in the financial department can share their spreadsheets with others in the same department but no one else. To enforce such a policy means that data in transit needs to be checked to see who is sending spreadsheets to whom, that on their PCs accountants must be prevented from copying spreadsheets to USB memory sticks and sending them to printers, and that such spreadsheets should only be stored in encrypted format—this requires one simple policy that can be enforced through technology, but probably only be defining it in three places.

Organisations can identify their users by getting them to authenticate against directories. User directories are generally accessed via a standard called LDAP (lightweight directory access protocol), and most security tools link to such directories to understand who users are and what groups they belong to. A well organised IT department may have just one user directory. But when it comes to policy, it usually needs to be defined time and again as there are no real standards and few generic repositories for policy that can be shared by multiple security tools.

IBM's initiatives this year around data security underline the problem. IBM can enforce

encryption by defining policies in Tivoli Storage Manager, but to boost its offerings it has formed two new partnerships: Verdasys for the management of end points and Fidelis Security Systems for monitoring data in use. The problem is that both the new partners' products have policy engines too—so three in total; plenty of scope for duplication and inconsistency.

IBM is not alone. Other security vendors have addressed data security through multiple product lines developed in-house, acquired or via partnership. For example Symantec bought Sygate for end point security (now Symantec End Point Protection or SEP V11) and Vontu for data leak prevention or DLP (now Symantec DLP V9), both of which had their own policy engines.

CA, EMC/RSA, Trend Micro and Websense have all made acquisitions in the DLP and end point areas and face similar problems with co-ordinating policy. McAfee has one of the most centralised approaches. Its ePolicy Orchestrator (ePO) was developed in-house and is core to its security suite. All its acquired technology is integrated with ePO as well as with 50-plus partner products, all done using McAfee's own proprietary software development kit—so still not standards based. Meanwhile Microsoft has made some moves in this direction with the beta release of its new security management tools code named "Stirling".

Well defined and managed policy is essential to achieving and being seen to achieve good security practice. The industry needs a more co-ordinated approach on how policy is defined and shared across multiple products; it is possible for the management of people's identities through the use of directories and there are standards for access to these—what is needed now is to make it easier to find out what they are allowed to do.

## 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>