



Comment Article

SNIA – Content Security in the Age of Mass Storage – Feb 2009

By Bob Tarzey, Service Director, Quocirca Ltd

To outsiders, the world of IT storage can sound a bit dull. However, if they stopped to consider the innovations that have occurred in storage during the last decade they should not fail to be impressed. Certainly those with the power to reward achievement have been so: in 2007 the Nobel committee saw fit to award its Physics Prize to Peter Gruenberg and Albert Fert for their discovery of giant magneto resistance (GMR) in the late 1980s.

GMR is perhaps the most important phenomenon behind the storage revolution. Commercial use of GMR has led to huge increases in the density of information that can be stored and to the miniaturisation of storage devices, which in itself has underpinned the boom in consumer products such as iPods and HDD recorders. It has also led to a huge decrease in the cost of storage for businesses and an equally big increase in storage capacity at all levels. For businesses, the biggest headache around storage has become not a lack of space but a surfeit of it, making it difficult to know what is stored and where and to ensure the security of their data.

Finding stuff is aided by increasingly powerful enterprise search tools. Stored content is indexed and later searched for and retrieved based on various search criteria. Search tools are powerful, but do not address the whole problem. There are so many places that content can end up, often beyond the reach of such tools. Without controls around content creation and use, sensitive information can end up almost anywhere and unwanted content can appear seemingly from nowhere; search does not prevent unwanted content getting stored in the first place.

So, it is not surprising that in the last decade an overriding concern for IT departments has become content security, which has seen a convergence of the storage and security disciplines in IT. One of the aims of this is to enable better monitoring of content in use and in

so doing restrict where it is copied to and stored. This helps prevent confidential material ending up on non-secure devices and making sure unwanted content does not enter the corporate domain in the first place. In short, if the ability to create content and move it around networks is not controlled, then, in effect, IT departments have no idea whatsoever what some of its stored content is and where any of its content might end up. From a compliance point of view that is a nightmare.

There is no silver bullet for ensuring content security; it needs to be addressed in three main areas:

1. End point security. For many users storage on laptops today seems almost limitless and content can be copied to memory sticks, mobile phones and other devices with their own huge storage capacity. When an end point comes back on to the network what has the user loaded on to it whilst out in the "wild"? End point security tools can limit and monitor activity on user devices and check they are clean when they come back on to a network. Alternatively, virtualisation can allow an isolated and controlled working environment to be created on PCs, or desktop management can be centralised, in effect turning PCs into thin clients. Whatever methods are used, end point security techniques need to cover both PCs and handheld devices.
2. Internal use of data. What is being copied, printed and emailed where, by whom and should they be allowed to do it? Enforcement of policies around the use of content requires knowledge of the user and their permissions, the content and what it contains, and the policy that links the two. The tools for doing this are now grouped together in a discipline that spans security and storage called data loss prevention (DLP) which embraces search, authentication and e-policy. DLP has

now gone mainstream and most of the major security and storage vendors have acquired or developed products in this area now.

3. At the network edge. In one respect, this is an extension of DLP and relates back to the long established discipline of outbound email security. But network edge security needs to be much broader than just outbound email; it must cover other channels such as HTTP (the web), FTP and instant messaging. And it is not just about what goes out but also what comes in—checking for malware, pornography, illegal music downloads and so on and making sure they never get stored in the first place. Some established email security vendors have developed their technology and repositioned themselves as DLP vendors.

Total content security is a utopian vision that can never be guaranteed, but a lot can be done to get close. Making sure we at least know what has been stored by whom, and where, is a starting point for controlling the tsunami of content unleashed by Gruenberg and Fert, which is in danger of overwhelming any business.

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>