CRN www.channelweb.co.uk

Click here to print

DLP systems: worth buying, worth selling

Confidential data leakage is one of the biggest challenges for modern business, according to Olga Gorshkova

Olga Gorshkova, CRN 18 Feb 2009

Research at InfoWatch reported 249 incidents of unauthorised use of confidential information over the first nine months of 2008. This concerned the interests of more than 100 million people all over the world.

The world financial crisis, accompanied by mass job losses, only makes the problem worse because information becomes more valuable. Data leakage prevention software can help, because during a time of crisis the role of business reputation increases.

The mechanism of such systems is simple: a smart set of monitors is installed in all possible channels of sending or copying data. The monitors may block suspicious data, or let such data leave the company and notify those responsible.

DLP systems have been on the market for only a few years. Their benefits include relative ease of installation as it requires practically no changes to corporate processes.

InfoWatch believes DLP solutions can prevent about 70 per cent of all data leakages. Content filtration can be set up to discern specific terminology used and act accordingly.

DLP systems guarantee compliance with the current IT security legislation, including the European Code of Corporate Governance, Basel II for banks, and so on. They are not to be used as a substitute for other IT security systems; rather, they should be seen as complementary.

The DLP systems market grew 50 per cent in 2008 and more than 100 percent growth is expected in the future, according to market research group IDC. One of the benefits of using such DLP systems is that they can control several data transfer channels at once. This is mostly because control of email content and data transferred over the internet is no longer enough.

Also, the protection system provides several functional capabilities. For example, it controls data copied to removable media or the print-out of such data.

Centralised setup, management and reporting tools are another feature of DLP systems. You can often control data classification and analysis, and manage security policies and tools that help prevent incidents connected with confidential data leakage.

Such a solution should block and encrypt data, place suspicious data in quarantine with a notification to the responsible person, and also place copies of such data in the archive for further investigation.

Some have real-time content filtration of email correspondence, web traffic and database access using a linguistic analysis module. This can prevent unauthorised actions, including copying of information to mobile media or print-out on workstations. Copies of all data that have left the corporate network through email, web, flash cards, removable media, mobile devices and printers are stored.

They can be self-learning systems, which means the system is able to improve the quality of data recognition in the process of exploitation. It is relatively easy to deploy such systems, and they can be integrated with a data encryption system easily.

DLP solutions can also help with subsequent analysis of different incidents and the submission of evidence to, for instance, the courts, if required. DLP products can attract partners as consultants, integrators or suppliers of additional services. DLP vendors support partners with supplementary services.

Knowledge and experience of such systems also offers competitive advantage to the partner who plays in the IT security space, and solutions are integrated easily with other security software, such as document flow systems or data protection solutions.

Olga Gorshkova is PR manager at InfoWatch