

# Get the system that suits your company

By Dermot Corrigan

**E**ach company which looks to monitor its staff's web and e-mail usage will require a system which suits its own particular business requirements and peculiarities. However, most organisations will want a system which offers full protection of their IT systems, does not allow staff near inappropriate or dangerous web pages, gives managers or administrators the flexibility to meet the needs of the business, and, importantly, allows staff who require significant internet access to be as productive as possible.

Smaller companies might choose to use the web-monitoring functionality of their existing IT security applications, according to Damien Foley, chief executive of CMGI.

"Most firewalls now come with an option for content filtering based on certain categories," said Foley. "They are quite cheap solutions, between €100 and €200 per year. They would update at regular intervals, but new sites may not be added for a while. They are quite weak, in that it is tied to each particular PC. They would only really suit small businesses."

More complex systems allow managers to monitor and manage all aspects of each individual's internet usage, said Michael Conway, director at Renaissance Contingency Services.

"There is no point in putting in place a total restriction, when it is impractical," said Conway. "Thomas might be entitled to look at the web any time he likes as it is important for his job, Ricardo might be entitled to look only at relevant business sites, and Harold might only have access to the web during his lunch time."

Foley said groups could be established with different permissions to simplify management of the systems.

"The enterprise level systems are very configurable, based on objects and user groups," he said. "For example, in your finance department you might have two groups – finance managers and finance staff – and restrict access to your online



Damien Foley, chief executive of CMGI: 'Most firewalls now come with an option for content filtering'

banking website to just the managers."

E-mail monitoring is also an integral element of an internet-use management product. The danger of data leakage is generally the most pressing concern for companies monitoring their staff's e-mail usage, according to Mourino Balsa, security product manager at DataSolutions.

"When it comes to tackling inappropriate use of e-mail, such as sending confidential information, a data leakage protection approach is the most convenient," said Balsa.

"DLP solutions not only tackle purposely planned attacks, but also mistakes which account for the vast majority of cases. It outlines the content of the data – not only attachments but also images or text in the e-mail's body – and informs the IT manager."

Neil Stone-Wigg, chief technology office of Trilogy Technologies, said that the latest monitoring systems could inform management about how their staff were spending their time online, what percentage was work-related or which individuals might

need to be spoken to regarding their web-use.

"The reporting aspects of these systems are excellent," said Stone-Wigg. "A whole set of reports can be produced to show managers what is going on. This information can be presented to the employee if an issue arises. We recommend that organisations inform the end users before they start to do this though."

Cloud-based monitoring technologies are becoming more popular, as they can provide monitoring capability while helping cut IT costs, according to Paul Ryan, senior security consultant of Integrity Solutions.

"Many vendors offer 'security as a service'-style hosted solutions since the economic downturn and reduction in IT budgets and staff numbers," said Ryan. "Vendors are also now offering unified, single management applications and appliances for web, e-mail, and data loss prevention and anti-malware, which helps to lower the total cost of ownership of content filtering and management."