

ContentWatch controls employees' Internet access

BY LINDA MUSTHALER

Day after day, your office workers show up for work and turn on their PCs. They fire up a browser and head to the Internet to...do what? Get into your employee portal? Check on competitors' pricing? Buy a few songs on iTunes? Check last night's sports scores on ESPN.com? Download a few sexually explicit videos? How can you be sure what employees do with that high speed Internet access you provide for their business use?

Employers want to believe the best of their employees - that workers would not abuse the resources provided to them at company expense. Most workers do deserve that trust and use their own good judgment in not spending company time or resources to visit Web sites that aren't truly job related.

However, there are people who allow themselves to be distracted from work by spending too much time on inappropriate Web sites. Not only is this a productivity buster; it can also be a liability for your company. And, browsing of untrusted Web sites is a prime way to allow malware into your corporate network. For example, just one click on a porn site - even for the briefest peek - is a likely way to pick up a keystroke logger on the PC.

The 2005 Electronic Monitoring & Surveillance Survey from American Management Association (AMA) and

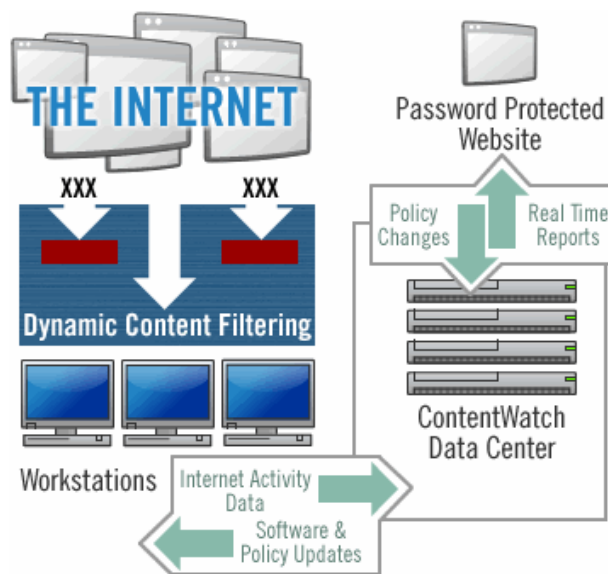
The ePolicy Institute shows that two-thirds of the 526 responding U.S. companies now use software to block access to inappropriate sites, and three-quarters of the companies monitor their workers' web usage. This is a growing trend; in 2001, just 27% of the companies blocked access to specific types of Web sites.

Managing what employees do on the Internet and which Web sites they visit is a prudent practice. It can reduce corporate liability and enhance network security. Employee Internet management should be a part of every company's policy on the use of electronic assets and communication tools.

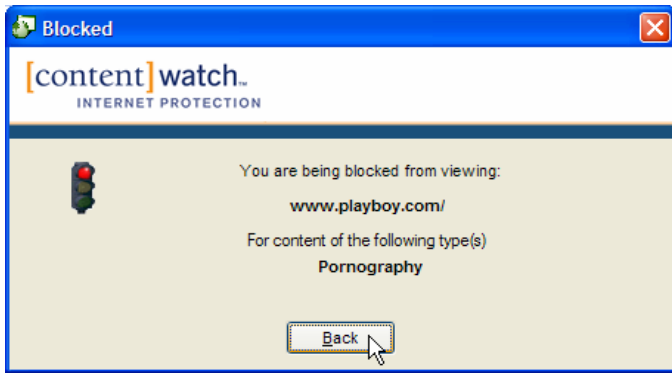
ContentWatch offers an interesting Internet management tool called [ContentProtect Professional](#). Unlike most Web filtering products that work by blacklisting specific URLs, ContentProtect uses a content analysis engine and your company ePolicy to analyze and categorize the content of a Web site requested by a user. If

the content of the Web site appears to be inappropriate - based on the user's profile in your policy guidelines - the user will not be given access to the site.

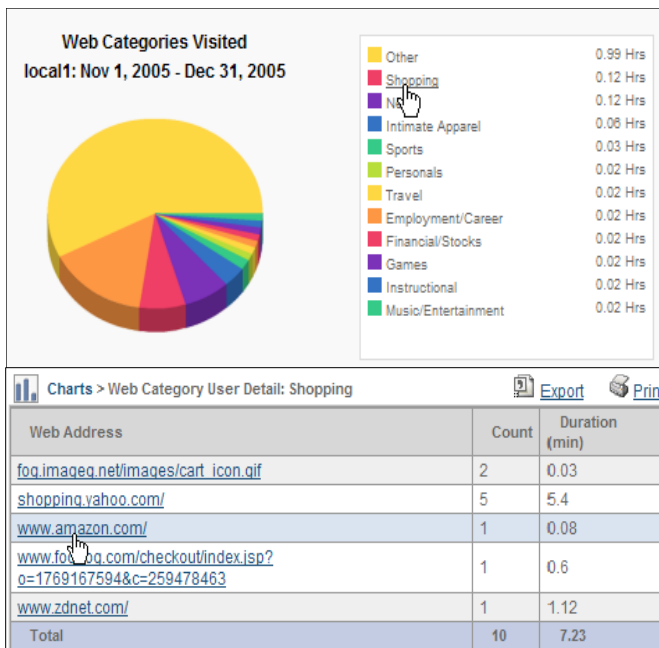
Profiles can differ from one employee to the next, giving the administrator the flexibility to determine access based on job function or position.



Content analysis is a far more effective filtering technique than URL blocking, since it's practically impossible to keep track of the ever-changing URLs belonging to objectionable sites. What's more, the analysis doesn't add any significant lag time to calling up a Web site. The end user probably won't even notice the scan happening in the background before he accesses his site.



The software also yields reports on what Web sites people are visiting, and for how long. It's useful to know if someone is popping into eBay for five minutes or spending hours a day there. The reports are an "early warning system" when there is a problem and an employee needs to be reminded of company policy.



ContentProtect is aimed at small to midsized businesses. Annual licenses are in the \$30 to \$40 per seat range, depending on the quantity of licenses purchased. Because it is client-based, there's no investment to make in a server or appliance. The software can be installed on laptops and on the PCs belonging to remote workers.

Lest you underestimate the value of a tool like ContentProtect, I'd like to tell you a very personal tale of woe. I wish my own company had had this product in place last summer. At the time, we had an employee who was falling behind in his work assignments, despite having ample time to complete them. An investigation of his e-mail, hard disk and Internet history files showed an extensive abuse of his Web browsing privileges. He visited many inappropriate sites and downloaded undesirable and illegal materials, putting the company at risk for viruses and malware as well as lawsuits. Because his actions were in complete conflict with company policy, he was let go.

ContentProtect could have prevented this entire situation. The company would not have lost valuable time and money to an ineffective employee and would not have been exposed to critical risks. And, had the employee been doing his job instead of horsing around, he might still be with us today. We could have seen what he was doing and nipped it in the bud before it became a real problem.

Unfortunately, this story isn't rare. The AMA/ePolicy Institute study revealed that a quarter of the firms in the survey have fired workers for misusing the Internet or e-mail.

Internet management does not have to be complicated or expensive. ContentProtect costs literally pennies a day to add assurance that your employees are using the Internet wisely.

Linda Musthaler is vice-president of Currid & Company. The firm researches information technology and how it can change the rules of business. Analysts focus on emerging technologies and methods by which organizations can obtain the best results from these innovations.



2369 West Orton Circle
 Salt Lake City, Utah 84119 USA
 Tel: (801) 977-7777 Fax: (801) 975-8144
www.contentwatch.com