Web Filtering *and* Monitoring *for* Small Business

A whitepaper by ContentWatch
— June 2005

Executive Summary

The issue of unwanted Internet content is reaching epidemic proportions. The liability risk, lost productivity, and cost of addressing these issues are especially problematic for small organizations.

The following report addresses the unique challenges small organizations face in addressing the issues of Internet filtering. This report will also discuss the various solutions that are emerging, with a specific eye towards the unique practicality and feasibility issues that small businesses, schools, libraries and government organizations must face.

The Problem

A recent FBI study reported by Computerworld said that 78 percent of surveyed companies are dealing with employee abuse of Internet privileges such as downloading pornography or pirated software.

The liability issue of inappropriate content is critical. If employees are subjected to racist or pornographic content, the business may be held liable for creating an unsafe work environment. For schools, libraries and publicly funded institutions, the liability issue is even more direct: the Children's Internet Protection Act (CIPA) mandates that schools are required to protect students from inappropriate Web content.

In addition to these direct abuses, the problem is even larger for workplaces when companies consider the time they lose to Internet browsing, shopping, and other non work-related Internet activities employees are engaging in during company time.

The cost of computer downtime related to viruses and malware that come into a business from unknown websites and downloads is an expensive proposition as well.

There are various ways of looking at the problem and addressing it. Industry analysts now categorize this broad category as Secure Content Management (SCM), which includes web filtering, anti-virus software and message security as three of the primary areas of risk.

As the problems grow, the realm of solutions to address them is growing as well. The SCM industry is expected to grow from $4.2 billion in 2004 to more than $10 billion by 2010.

The Unique SMB Challenge

As problematic as the issues of unwanted content are to families and large enterprises, the problem is particularly challenging for small organizations. While there are an assortment of options for homes and families, these solutions aren't suitable for the rotation of users and robustness issues a school, a library or a small business would face. Similarly, the solutions that typically protect large organizations are far too complex and expensive to serve as practical solutions for a small business to use. This vast and underserved market segment – the small to medium organization – is the area that is currently most vulnerable to liability and lost productivity costs.

While virtually all companies are aware of the dangers of unwanted content, it's small businesses that are most typically at risk. The firewalls, comprehensive management suites and patch management policies that protect large organizations are simply not viable or practical for smaller companies to employ.

The threat is even greater when you consider that in the small business sector, critical data is typically stored on site and access to the network is handled in a much more casual fashion.

Additionally, very few small organizations—particularly businesses of 15 fewer—have access to full or even part-time Information Technology (IT) employees.

As a security expert for Computer Associates recently noted, "These companies are realizing they don't have the resources or the expertise to put up the barriers that a big company does."

The SMB Opportunity

For all the benefits and recent advances in the SCM technology space, for the most part, small businesses (particularly organizations or workgroups of 5-25 people) are still left out in the cold.

Yet the Small to Medium Business (SMB) is a surprisingly vast market sector. Recent research from Inc. Magazine shows there are more than 7.8 million small and medium businesses in the U.S. as compared to only 8,500 large companies. For every one large U.S. business, there are more than 900 small and medium companies in existence today.

Interestingly, of these 7.73 million businesses, there are 4.2 million companies of 1-4 employees. There are 1.5 million organizations with 5-9 people. And another 1.6 million companies comprise groups of 10-49.

SCM Alternatives

Currently, the spectrum of available SCM alternatives includes firewalls, content filters, and a variety of SCM related point products and suites.

Fire Walls

For the SMB marketplace, firewalls and enterprise suites are clearly impractical.
First, let's consider the issue of firewalls.

While small business and personal firewalls are plentiful, these solutions are insufficient for reliably protecting a company from pornography and are entirely inadequate for monitoring employee Internet use.

As a protection from pornography, a firewall can be set to block site categories such as pornography, gambling, or hate groups. However, the most common methods of blocking involve matching page requests against a "black list" of known URLs. However, with new sites emerging daily and even hourly, and content coming in through pernicious back-door methods, most firewalls are insufficient for keeping small organizations secure.

To successfully block content, a solution must employ a dynamic filtering method to quickly identify and block inappropriate content on the fly.

As a method of monitoring usage, firewalls are even less suitable. For human resource or technology managers to pour over Web logs to try to determine where people have been, what they were looking at, and how long they stick around is completely impractical. And for companies who share machines or employ floating IP addresses, the logs are entirely meaningless.

Security Management Suites

For large organizations, the adoption of a comprehensive desktop management suite can be a reasonable solution. The benefits of a centralized and remotely manageable single vendor solution (over the installation and management of potentially conflicting point products to address virus, spyware, and content filtering) are clear.

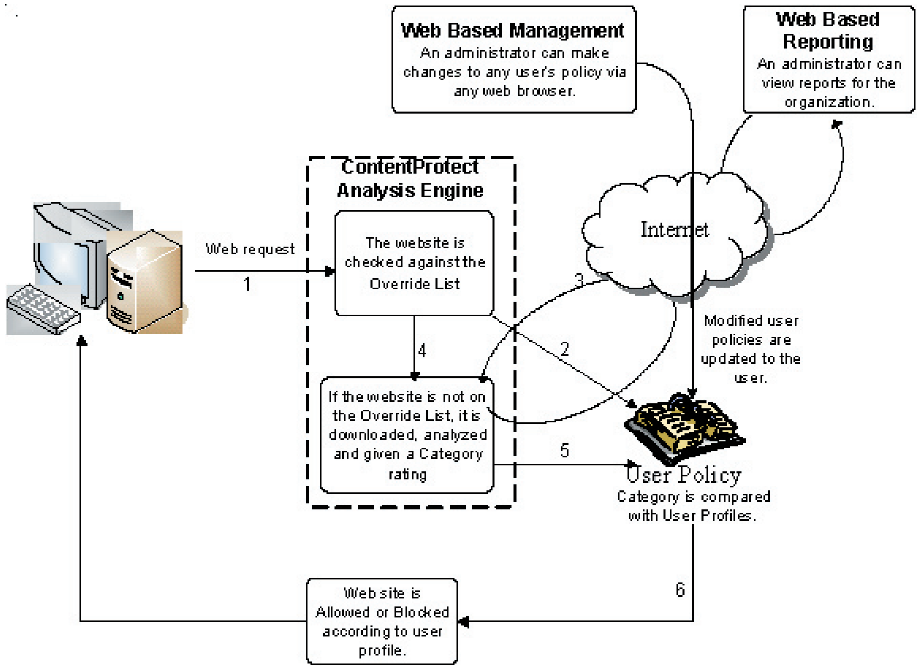
However, these product families can be complex to install and from a cost standpoint are completely impractical for an organization of fewer than at least 100 (if not 1,000) employees.

ContentProtect, from ContentWatch Inc.

For the SMB market, there is currently only one practical solution: ContentProtect, from ContentWatch. Available as a standalone-filtering product or with virus, e-mail, pop-up and audit/cleanup functionality in the comprehensive ContentWatch Protect Professional Suite, ContentProtect is able to offer small organizations a solution that is

- Easy to use
- Fast
- Extremely adaptable and scalable
- Ideal for mobile or notebook users
- Remotely manageable, and
- Inexpensive. Not only is the purchase price for ContentProtect surprisingly low; organizations report an immediate return on investment.

In a nutshell, the following diagram illustrates how the ContentProtect engine works: ContentWatch's powerful "content analysis engine," is the mechanism whereby the ContentProtect receives requests for Internet objects (a Web page, a chat session, etc.) and analyzes the object to determine the appropriate response. To illustrate, we will assume in the diagram below that the application is a Web browser and the requested object is a Web page. The content analysis engine process flow for this request looks something like this:


Web Based Management
An administrator can make changes to any user's policy via any web browser.
Web Based Reporting
An administrator can view reports for the organization.
ContentProtect Analysis Engine
Web request
1
The website is checked against the Override List
4
If the website is not on the Override List, it is downloaded, analyzed and given a Category rating
Internet
3
2
5
Modified user policies are updated to the user.
User Policy
Category is compared with User Profiles.
6
Web site is Allowed or Blocked according to user profile.

1. A user tries to access a Web site.
2. The Web site the user tried to access exists in the Override list. It is checked with the user's profile.
    - The Web site is either allowed or block according to user's profile

    Or
    - The Web site the user tried to access does not exist in the Override list. It is downloaded from the internet
3. Then sent to the dynamic analysis engine for analysis.
4. The dynamic analysis engine obtains the requested Web site
5. The dynamic analysis engine analyzes the content of returned Web site and categorized it.
6. The category of the requested Web site is compared with the user's profile
7. Again, the Web site is either allowed or blocked according to the user's profile.

Recent Examples

Repeatedly, small organizations are discovering that ContentProtect is the practical alternative that is easy to use, affordable, and produces an immediate return on investment. The following examples show how a small restaurant chain, a construction company, and a regional car dealership have all benefited from protecting their companies with ContentProtect.

Biaggi's Ristorante Italiano, Bloomington, Ill.

*I*n 7 years, Biaggi's restaurant has expanded to 18 locations in the Eastern and Midwest states. With so many remote locations, typical methods of managing a directly connected network are impossible. Biaggi's network administrator, Zed Al-Safar, searched extensively for a workable solution. He found 20 prospective alternatives—however, with the exception of ContentProtect, all of the other products were designed for full corporate environments.

The product was easy to install and put an immediate stop to inappropriate web surfing. In the six months since its implementation, employee productivity has seen a dramatic increase.

Flaherty Construction, Mokena, Ill.

*F*laherty Construction is a 35-year-old company with 80 employees. Of this sizeable employee base, however, only 15 users require PCs. Flaherty had known for some time it would need to find a web filtering solution. But in February 2005, when one of the offsite computers developed trouble as the result of an inappropriate download, the situation became dire.

Flaherty's accountant, who also fills the company's computer technology role, began searching on Yahoo. He found a number of alternatives—but all but three were beyond the budget and scope of a smaller company. Of the three alternatives he looked at, he quickly settled on ContentProtect.

"We've been thrilled with this solution," he said. "Not only did it give us the protection we needed, but it also effectively eliminated unproductive Web surfing time. We recouped the cost of the 10 software licenses we purchased during the two week trial period alone."

Weber BMW, Fresno, Calif.

*A*bout 18 months ago, Weber BMW became concerned about the risk of virus, spyware and questionable content coming in on the dealership's 53 PCs. Not only was the company concerned about productivity, they were worried about professionalism as well—many of these computers are also visible to the company's customers.

Without internal IT capability, Weber depended on an outside consultant for a recommendation. Jon Johnson, of Central California Internet Services (CCIS) recommended ContentWatch's ContentProtect.

"The flexibility ContentWatch gives me—coupled with the interface and the surprisingly low price—made this product not only an easy recommendation, but essentially the only really good recommendation for a company of this size."

Weber BMW's controller reports that the cost of the ContentWatch product was quickly recouped on simply the increased productivity in the use of company time.

Channel Considerations

As unwanted content becomes a growing problem for small business owners, resellers, ISPs and integrators who serve small organizations play an increasingly critical role.

If resellers and ISPs don't have good solutions to these problems, they risk losing customers.

Conversely, providers who can offer practical and cost effective solutions are able to act as increasingly effective partners.

For these providers, education is crucial. Resellers can take the opportunity to make small businesses aware of the risks and the alternatives at a fundamental and non-technical level.

Resellers can also assist their SMB customers in setting up security-related rules that are meaningful, and most importantly, that are enforced.

Conclusion

To effectively answer the unique needs of the SMB marketplace, an SCM solution needs to have very specific characteristics. For small organizations, the solutions they choose must be particularly fast, and must be easy to install and to use. They need to be remotely manageable, since many small businesses are geographically dispersed—yet they need to be cost effective and practical for non-technical people to use. And most importantly, they need to provide an immediate return on investment.

In this category, there is one product and company that stands alone in meeting this unique set of needs: ContentProtect from ContentWatch Inc.

For more information about ContentWatch, to find regional ContentWatch providers, and for additional resources, readers can visit www.contentwatch.com.