



## FILTERS FIND A HOME IN SECURITY

---

With so many attacks finding their way past normal security mechanisms in the guise of 'content', it's probably no surprise that content-scanning companies have seen a role for their products in the security market.

Companies like WebSense, which has just released a broad suite of products designed to add security to its traditional home ground of employees Internet management; and WebSpy, which has won a contract to integrate into Microsoft's Internet Security Accelerator environment, are working to premise that a content-based attack is best dealer with in the world of content management.

WebSense regional sales manager Graham Person said that from a starting point of preventing inappropriate use of resources", it's a fairly straightforward progression. Spyware is a good example: in a corporate environment, software which returns user activity is tantamount to stealing processing time from the company that actually owns the PCs, the LAN, and the Internet bandwidth.

And, Pearson pointed out, many of the blended threats look and act very much like spyware: they execute as applications on the target machine, and they return information (like unsecured user accounts, logged keystrokes and son on) to external addresses.

WebSense also identifies applications which tunnel through Port 80 as creating high risk. So in its Enterprise V5 product, it allows administrators to manage access not just to sites, but also to protocols – so (for example) instant messaging, media streaming and P2P applications can be managed according to the application that invokes the protocol, and whether a user has the rights to use that application.

There's also a feature called AppCatcher, which may attract the attention of security managers: if an 'unknown' application to access the corporate Internet connection, it is blocked and the administrator notified.

WebSpy has also noticed the opportunity to apply its technology to the security market. CEO Jack Andrys says an industry built on watching application traffic has the chance to make itself more valuable to customers if it can help secure their networks rather than just blocking pornography.

"The person who runs the system and looks at server logs may not be into the presentation layer – but we are."

The simplistic stance taken by filter companies had become outdated, Andrys said, because too much emphasis on employee behavior is immature. "Management has to get beyond running around asking 'what are people doing wrong?'"

In applying access management and filtering software to the security problem, Andrys said, the same principles apply as for any other security environment. "You have to work out what you need to protect, what you need to lock down, and where that system is.

"You have to families yourself with the risks, and with your resources," he said. "If you don't understand these things, you won't know where to start."

In both security and Internet misuse, Andrys lays the blame at the feet of a company's executive in the first instance. "People have embraced the revolution without understanding what they need to protect," he said.

Managing and securing networks is part of managing business, he said: "The executive has to be able to understand the resource. Otherwise, how will they understand the impact of not managing it correctly, whether it's a network breach or inappropriate use?"

***Comms World, May 2003***