

MarketScope for URL Filtering, 2006

Lawrence Orans, Arabella Hallawell

Many vendors now sell products for URL filtering that are good enough for most organizations. But this technology will increasingly be sold as part of integrated packages that guard against malicious code.

WHAT YOU NEED TO KNOW

Companies increasingly want anti-spyware, antivirus and instant messaging (IM) security protection for their Internet gateway malicious code protection. Uniform resource locator (URL) filtering decisions will become only one feature in a multifunction solution. However, despite growing demand from enterprises, few vendors today actually supply an integrated solution across all these areas. Shorter-duration URL filtering contracts provide the flexibility to more quickly align those vendors that offer the best Web-based malicious code management gateway solutions. Companies should sign one- or two-year contracts, and avoid the commonly proposed three-year solution (unless the premium for the additional year is 10 percent or less). Negotiate aggressively on pricing, as most URL filtering solutions are adequate for a typical enterprise.

MARKETSCOPE

In the early days of the Internet boom, organizations were driven to implement URL filtering solutions for three reasons: to protect themselves from legal liability, to safeguard bandwidth and to mitigate a loss of productivity from employees. In 2005, security jumped to the top of this list. Organizations increasingly use URL filtering as a first line of defense, by blocking access to Web sites that spread spyware and other forms of malware. This trend shows no sign of abating, and it is rapidly driving small and midsize businesses (SMBs) to adopt URL filtering as a must-have solution. Indeed, URL filtering is but one of a few perimeter-based security technologies for protecting against malicious Internet content. It is the most widely deployed and the most necessary, but antivirus and anti-spyware scanning of Web traffic is becoming increasingly important (see Note 1).

To date, technology and product innovation are not the first words used to characterize the URL filtering vendors. Indeed, the incumbent vendors have considerable gaps to fill in their strategy and product road maps before they can meet enterprise requirements for broader gateway malicious code protection across a variety of form factors. The URL filtering vendors are still predominantly software-based, and very few of them own all the "pieces" themselves (antivirus, anti-spyware and URL filtering) for gateway malicious code management. Websense and SurfControl have not integrated Web-based antivirus or anti-spyware signature scanning into their offerings. Secure Computing still has to manage its overlap with the CyberGuard Webwasher solution and Blue Coat is only beginning to seriously focus on its own URL filtering. Vendors that will be successful must focus, innovate and own key technology in antivirus, anti-spyware and URL filtering for the gateway (see Note 2). Thus, in addition to rating vendors strictly on their current URL filtering functionality, we also considered their ability to integrate these other security functions as part of an overall solution.

Management and reporting capabilities for URL filtering products have slowly improved across the board. But users still report that specific per-user activity reporting and searching through logs can be manually intensive with several solutions. As the URL filtering market has matured, so has the quality of most vendors' databases (see Note 3). Subsequently, price should be a heavily weighted criterion for any organization making a URL filtering decision, particularly as most of the vendors in this MarketScope provide solutions that are adequate for a typical organization. The most common URL filtering pricing model is based on per-seat, per-year charges — an approach that applies to many software and appliance-based solutions. SurfControl's perpetual software licensing model is the exception, although it also charges a per-user subscription for content. The appliance vendors charge separately for their devices, and prices vary widely depending on the scale of the appliance and its ability to support multiple functions. Gartner compared U.S. list prices for a 5,000-seat contract (single-year) for all the vendors in this report. Prices range from

approximately \$6.50 to over \$12.00 per seat, per year. Websense is nearly always the most expensive solution because of its additional charges for premium groups.

Architectural differences in current products dictate whether vendors are truly capable of delivering an integrated malicious code management gateway solution. URL filtering solutions can be classified into two models — an out-of-band and an in-band approach. With the out-of-band model, outbound traffic is "mirrored" to a filtering device that is not in the line of traffic. With this approach, the filtering function does not add latency to the outbound request, and the filtering device can be inexpensive because it does not require a high-performance processor. 8e6 Technologies and some implementations of SurfControl utilize this technique. The out-of-band model provides an effective URL blocking solution, but out-of-band solutions are unable to process in-bound content (for example, no Web-based antivirus or gateway anti-spyware protection) and are, therefore, architecturally limited from providing a complete multifunction solution. These out-of-band models will remain specialty URL filtering solutions and will ultimately lose market share to in-band methods that have integrated strong URL filtering, antivirus and anti-spyware components.

We recommend companies use price as a significant selection criterion when they only require URL filtering. Ease of reporting and policy management are other factors to consider. Companies should also consider their broader gateway malicious code protection needs and evaluate antivirus, anti-spyware and IM filtering capabilities of solutions when renewing or considering switching vendors.

Market/Market Segment Description

The market is defined by vendors with products or services for managing employee access to the Internet via URL filtering. The market consists of appliance-based and software-based solutions that run on common server platforms. "In the cloud" URL filtering services offered via network service providers, or as a managed service, is an emerging segment, although it represents less than 5 percent of the overall market. URL filtering vendors own a categorized database of URLs, or they have algorithms for dynamically classifying uncategorized entries, or they are capable of providing both techniques. The market is driven by partnerships between the URL filtering vendors and network gateway vendors (mainly proxy caches and firewalls), many of which are original equipment manufacturers (OEMs) or resell solutions from the URL filtering providers.

All indications point to the fact that URL filtering is a maturing market. Vendor consolidation has been widespread and prolonged, as shown by Secure Computing's acquisition of CyberGuard (and its Webwasher solution in January 2006), Blue Coat's acquisition of Cerberian (2004) and from Secure Computing's acquisition of N2H2 (2003). Microsoft has entered the market by acquiring a URL filtering product from FutureSoft (February 2006). It has yet to declare its plans, but Microsoft will likely price its URL filtering offering as an inexpensive add-on to its ISA Server solution.

We estimate the enterprise market was worth approximately \$350 million in 2005. The segmentation of the market is yet another indication of its maturity, as vendors have emerged that target primarily SMBs (like St. Bernard), or have introduced SMB-focused appliances (like 8e6 Technologies and SurfControl).

Inclusion and Exclusion Criteria

The following criteria must be met to be included in this MarketScope:

- The vendor must own, manage and maintain a database of URL entries, or it must own algorithms for dynamically classifying URLs. Vendors that license these solutions from URL providers are excluded from this analysis.

- The vendor's overall annual revenue (from all product classes) must exceed \$10 million.
- The vendor's URL database must have a worldwide focus. Vendors that have a regional focus or a non-English language focus have been excluded. For example, Optenet's Web Filter (European focus) and Digital Arts Japan's iFILTER have been excluded from this MarketScope.
- Vendors that bundle (for example, do not charge separately) URL filtering as part of a broader gateway solution have been excluded (see Note 4). Internet Security Systems, Fortinet and Symantec fall into this category — they have not productized URL filtering. They do not have the same focus on reporting, accuracy and product innovation as vendors that charge separately for URL filtering, and these solutions do not meet the URL filtering needs of most enterprises.
- Vendors that focus primarily on the consumer market have been excluded from this analysis.

Rating for Overall Market/Market Segment

Overall Market Rating: Promising

The demand for vendor-provided URL filtering solutions is healthy and will remain so for at least the next five years. Self-maintained "blacklists and whitelists" have proven to be ineffective and too labor intensive for most organizations. The challenge for vendors in this market is that organizations also need to do much more than block outbound access to inappropriate and unsafe Web sites. Organizations will ultimately turn to integrated antivirus, anti-spyware and URL filtering gateway solutions to protect against Internet threats, thereby diminishing the significance of vendors that specialize only in URL filtering solutions.

Evaluation Criteria

Table 1. Evaluation Criteria

Evaluation Criteria	Comment	Weighting
Market Understanding	Ability of the vendor to understand buyers' needs and translate these needs into products and services for the URL filtering market. The ability to anticipate market trends and to quickly adapt via partnerships and/or acquisitions.	high
Marketing Strategy	A clear, differentiated set of messages consistently communicated throughout the organization and externalized through the Web site, advertising, customer programs and positioning statements.	standard
Business Model	The vendor's ability to build a business model around its target market.	standard

Evaluation Criteria	Comment	Weighting
Geographic Strategy	The vendors' ability to provide accurate and comprehensive URL filtering solutions in multiple geographies and languages.	low
Product/Service	The vendor's ability to provide URL filtering solutions and related reporting capabilities. The ability to supplement core URL filtering functionality with complementary solutions, such as HTTP-based AV scanning, instant messaging blocking and filtering, mitigating spyware threats.	high
Overall Viability (Business Unit, Financial, Strategy, Organization)	Viability includes an assessment of the vendor's overall financial health, the financial and practical success of the business unit and the likelihood of the individual business unit to continue to invest in the product.	standard
Sales Execution/Pricing	The vendors' capabilities in all pre-sales activities and the structure that supports them. This includes pricing and negotiation, pre-sales support and the overall effectiveness of the sales channel.	high

Source: Gartner (March 2006)

Figure 1. MarketScope for URL Filtering, 2006

	RATING				
	Strong Negative	Caution	Promising	Positive	Strong Positive
8e6 Technologies		x			
Blue Coat			x		
Secure Computing			x		
St. Bernard		x			
SurfControl			x		
Trend Micro		x			
Websense			x		

As of 14 March 2006

Source: Gartner (March 2006)

Vendor Product/Service Analysis

8e6 Technologies

8e6 Technologies is an appliance-based vendor that targets the education market and large enterprises. Its R3000 filtering appliances are positioned out-of-band and monitor outbound Internet requests, so they do not require integration with proxy caches or firewalls. Blocking is achieved by sending a TCP Reset message to break a connection. Ease of implementation and scalability are strengths of 8e6's solution. 8e6 also offers a separate appliance for reporting, an approach that enhances filtering scalability by offloading log scanning and report generation. 8e6 also resells networked attached storage (NAS) and storage attached network (SAN) solutions — options that appeal to large customers that store log data for extended periods of time. In February 2006, 8e6 added a remote user agent to its product family.

Because of the R3000's out-of-band positioning, its appliance is unable to provide antivirus scans (and cannot handoff antivirus scanning to a separate appliance). Nor can it provide anti-spyware signature scanning or function as a proxy for enhancing IM security. Thus, 8e6's R3000 appliances will be limited to specializing in URL filtering.

8e6 has, at times, exhibited an unfocused strategy. In 2004, it briefly entered the bandwidth management market with a dedicated appliance. It was unsuccessful in competing against established quality-of-service vendors and WAN-link compression vendors, and it quickly exited the market. 8e6 now has a more focused message as a security company that is dedicated to Internet filtering and reporting. But it faces challenges from other vendors, especially Blue Coat in the large enterprise market, that are now selling appliance-based URL filtering solutions. Nonetheless, 8e6 has an impressive installed base of large enterprises and it continues to fulfill at a moderate price level the requirements of those organizations that emphasize reporting and archiving.

Rating: Caution

Blue Coat

Blue Coat has long offered URL filtering functionality by reselling many of the software-based solutions, including Secure Computing, SurfControl and Websense (Europe only). In November 2004, Blue Coat acquired Cerberian, a small software-based URL filtering vendor. It now offers this solution, which it labels WebFilter, as an alternative to its partners' offerings. The Cerberian acquisition was bold, because it threatens to disrupt the trust between Blue Coat and its partners, but Gartner believes that Blue Coat has made the right move. URL filtering has become a secondary decision to the network gateway decision. To capitalize on this trend, Blue Coat will continue to lead with its flagship proxy appliances, and will position URL filtering as an important feature of the proxy.

WebFilter provides an optional dynamic URL classification feature for those URLs which are not in its database — Blue Coat calls this Dynamic Real Time Rating (DRTR). There is no additional charge for this feature. Early feedback from Blue Coat customers reports that it is accurate, and that it results in fewer unclassified results than vendors without a dynamic classification capability. DRTR requires that an organization send back to Blue Coat all of its uncategorized URL requests. Some organizations may be concerned that DRTR will make the Web surfing habits of its employees available to Blue Coat, although Blue Coat states that it does not capture specific user or company identity.

Blue Coat's WebFilter has a long way to go before it threatens the market leaders. For 3Q06, Blue Coat reported that WebFilter generated revenue of nearly \$3 million. The company got off to a slow start in promoting WebFilter, but in mid-2005 it took on more aggressive marketing tactics.

As the market leader in proxy cache appliances, Blue Coat has a large installed base to sell into. Today, many of these appliances provide URL filtering via Secure Computing, SurfControl, Websense and others. As these contracts expire, Blue Coat is in an excellent position to convert them to WebFilter customers — particularly since the WebFilter solution is inexpensive in relation to the competition. Conversely, Blue Coat's potential is limited, as WebFilter requires a Blue Coat proxy appliance. Those organizations that have implemented Network Appliance, Microsoft, or Cisco Systems' proxy caches are unlikely to switch proxy solutions just to run Blue Coat's WebFilter.

Rating: Promising

Secure Computing

In January 2006, Secure Computing completed its acquisition of CyberGuard. The CyberGuard acquisition includes the Webwasher product line, complete with its URL filtering solution. The acquisition gives Secure Computing access to the Webwasher URL filtering installed base and a steady revenue stream, which Gartner estimates to be in the range of \$25 million annually. Webwasher offers a broader gateway malicious code protection, which includes partnerships with antivirus vendors and Akonix, an IM security vendor. The Webwasher product family supports Internet Content Adaptation Protocol (ICAP), which gives Secure Computing a better chance to sell into the installed base of Blue Coat and Network Appliance proxy caches and other ICAP-enabled gateways. Previously, Secure Computing's lack of ICAP support limited SmartFilter's off-box deployment. The acquisition presents branding and product integration challenges for Secure Computing, since it now has three product families for URL filtering: SmartFilter (for commercial enterprises), SmartFilter Bess (a cost-effective solution targeted at the K-12 environment) and the Webwasher product family. Secure Computing also needs to resolve its pricing strategies, since the Webwasher solution was priced inexpensively, whereas SmartFilter is priced at a moderate level. Secure Computing needs to quickly address these issues and articulate its post-acquisition road map.

As URL filtering increasingly becomes a feature of multifunction gateway devices, Secure Computing's on-box strategy will serve it well. The company already leads its competitors with more on-box integrations for proxy caches and firewalls than any other URL filtering vendor. Additionally, it offers URL filtering as an option with its own Sidewinder firewall appliance. Secure Computing's on-box strategy has enabled it to build a loyal distribution channel via its network gateway partners, because the on-box strategy enables the gateway vendor to own the customer relationship. Now that Secure Computing has the off-box Webwasher solution, it needs to manage these partnerships even more carefully.

Rating: Promising

St. Bernard

St. Bernard sells an appliance-based URL filtering solution targeted at SMBs. It is the only vendor in this MarketScope that is focused solely on the SMB market. Its iPrism appliance is a good URL filtering-only solution for organizations with 1,000 end users or less. The appliance form factor and the aggressive pricing, combined with a marketing message focused on security, reflect that St. Bernard understands the needs of the SMB market. St. Bernard also offers separate appliances for e-mail security and for patch management, but Gartner estimates that URL filtering generates approximately 75 percent of its overall revenue.

The St. Bernard iPrism is commonly deployed as an in-band (in-line) solution, although its default configuration is to analyze outbound traffic only. It has limited ability to analyze inbound traffic and it lacks antivirus and anti-spyware signature scanning capabilities. Also, it lacks the ability to strip off inbound IM attachments. In its current form, iPrism is limited to specializing in URL filtering.

St. Bernard is merging with the Sand Hill IT Security Acquisition Corporation, a publicly traded corporation that has raised capital to invest in IT security companies (technically, St. Bernard is acquiring Sand Hill). The transaction is expected to close in the first half of 2006. Sand Hill provides St. Bernard with a cash infusion, although there are many unanswered questions about how the deal will affect the company's overall strategic direction. St. Bernard has struggled with visibility and is focused mainly on the North American market. It will likely use its new resources to diversify internationally and to raise its overall visibility.

Rating: Caution

SurfControl

SurfControl is an established vendor in the URL market, with over two-thirds of its approximately \$100 million revenue in 2005 coming from its URL filtering business. Unlike Websense, SurfControl has also entered the e-mail security market, and now offers a bundled solution, offering e-mail and URL solutions for a competitive price. Like Websense, SurfControl does a good job at maintaining its URL and application lists, and has released an agent for remote users. Yet it has not managed to gain the best-of-breed status in e-mail security, as it has in URL filtering. The e-mail security market is an extremely competitive one, where best-of-breed players aggressively try to out match each other with frequent product changes as the e-mail security threats quickly shift. SurfControl has found it tough to keep up.

SurfControl blocks IM sites, rather than filters IM traffic. We see the latter becoming a more important feature of these solutions, as companies decide to allow some use of IM. SurfControl has not invested in partnerships for antivirus scanning, and its HTTP gateway anti-spyware capability is rudimentary. In 2005, SurfControl acquired a desktop-focused anti-spyware company, Apreo. However, the technology is not integrated into the gateway and is only available as a desktop product. As Web-based antivirus and anti-spyware scanning become increasingly important drivers for buyers, SurfControl must deliver value here or its market share will be quickly eroded. SurfControl has partnerships with several proxy and appliance vendors, and, in 2005, it released a Windows-based appliance targeted at the SMB market. Offering companies a choice of form factors (software, appliance or managed service) will increasingly be necessary in this market.

Rating: Promising

Trend Micro

URL filtering is a very small business for Trend Micro (we estimate \$5 million to \$10 million of its \$621.9 million 2005 revenue). As we described above, we believe this market is heading toward a converged gateway offering of URL filtering, antivirus and anti-spyware protection. Trend Micro is, in theory, well positioned to capitalize on this trend. However, the reality is more disappointing. Trend's product offering is InterScan Web Security Suite (IWSS), which is primarily a Web-based antivirus scanning solution. URL filtering and active content scanning are both available for an extra charge. Price appears to be a significant motivating factor for customers choosing Trend Micro. Users tend to be existing customers that want an inexpensive add-on URL filtering solution. While Trend does have its own URL filtering capability (the list was acquired from a third party and maintained by Trend), it is not considered best of breed. For example, the list is not purged as frequently, nor are high-risk sites updated as quickly as some of the vendors, but investment appears to be increasing. Trend also does not offer URL filtering for its remote enterprise users, despite its desktop antivirus presence, where a compelling integration story can be made. While Trend has a strong reputation for its Web-based antivirus capabilities, Trend's anti-spyware is still rudimentary. The InterMute technology the company acquired last year is still not bundled into IWSS, and anti-spyware based on URL blocking has not been a focus. Users

report that the management and reporting has some challenges, and evaluating logs can be manually intensive. Trend has been solely software-focused to date, although it introduced an appliance that integrates its IWSS software in February 2006.

Rating: Caution

Websense

Websense continues to maintain its dominance as the market share leader in the enterprise URL filtering market, with revenue of just under \$150 million in 2005. It has adeptly focused its marketing and products on increased security concerns, a strategy which has helped it control approximately 40 percent of the overall market share for URL filtering. Although Websense remains the apple of Wall Street's eye, we continue to see longer-term enterprise IT trends shifting away from Websense.

Websense is the premium-priced URL filtering vendor. It is the only vendor that requires its customers to pay extra for blocking URLs deemed to be a security risk. These URLs are included in Websense's Security Premium Group. Websense also offers two other premium groups — a Bandwidth Group and a Productivity Group. Based on U.S. list prices, a Websense base subscription plus all three premium groups is priced at more than double the cost of many of its competitors. Websense has introduced new platinum coverage for dedicated support for an additional 25 percent of the license price.

We believe that Websense's current strategy is problematic and is missing the important macro shifts in the market. Websense is betting on growing its desktop presence with its Client Policy Manager, which includes its newly introduced remote user agent. Moving to the desktop market is extremely challenging, as this is a different buyer from the traditional network-focused Websense buyer, and the barriers to owning any piece of the enterprise desktop security market are very high. Rather, Websense's remote agent and application filtering capabilities are good OEM opportunities for desktop antivirus and personal firewalls (which are now fast converging).

The recent shift of Gene Hodges from McAfee (where he was President) to Websense (where he is now President and CEO), may signify the company will make the desktop a further focus. It is also likely that the company will start to make acquisitions, although they are likely to be outside the malicious code arena. Websense does not have either its own, or partners, for antivirus scanning or signature-based anti-spyware. Websense is still wholly software-focused, and relies on partners like Cisco Systems, Blue Coat and Network Appliance, which resell their lists as part of their offerings. As we illustrate above, network gateway vendors will want to carve out more of the security market for themselves. Also, Websense is ignoring the potential "in the cloud" services opportunity for HTTP-based antivirus and URL filtering. We anticipate the SMB market will slowly embrace this as an alternative to expensive upfront capital investments in hardware.

Lastly, Websense has ignored the fast-growing e-mail security boundary market over the past three years, where we anticipate more product convergence with HTTP security. However, Websense has done a good job of extending beyond URL filtering for HR/acceptable use purposes, to well-maintained spyware, unwanted applications filtering and malicious code URL blocking. Websense has also improved its management and reporting, including offering delegated reporting and administration. The URL filtering market, even as it evolves to broader malicious code protection, will remain content-driven, and Websense has focused on maintaining its content. Yet, given the longer-term shifts in the market and Websense's current strategy, the company may increasingly become only an OEM to other solutions, rather than a purveyor of product directly to customers.

Rating: Promising

RECOMMENDED READING

"MarketScope for Instant Messaging Hygiene, 2006"

"Magic Quadrant for E-Mail Security Boundary, 1H05"

"Enterprise Antivirus Market in Disarray: Leaders Needed"

Note 1

The e-mail and HTTP security markets are slowly converging

The e-mail security boundary market is starting to slowly converge with the HTTP malicious code and URL filtering market. There are multiple drivers; the threats (such as phishing and spyware) are becoming more intersected, with messaging and HTTP traffic and technologies like instant messaging requiring coordination among all vectors. E-mail security vendors are looking at opportunities to grow, and the underpenetrated Web antivirus and anti-spyware gateway market offers good growth opportunities. The leading e-mail security vendors have been very innovative in the e-mail security market. Applying similar focus to HTTP security will be a wake-up call for the incumbent URL filtering vendors. Many of the leading e-mail security appliance and managed services vendors have released, or are likely to release, new offerings in this area.

Note 2

URL filtering evolves into gateway malicious code protection

Currently, we estimate fewer than 10 percent to 15 percent of enterprises have deployed Web-based antivirus scanning. This represents new opportunities for antivirus vendors as their desktop market becomes more challenging, and for e-mail security vendors eyeing adjacent markets. We see the market quickly shifting toward Internet gateway malicious code management solutions that integrate "best of breed" antivirus, anti-spyware and URL filtering. Also, as demands for performance-intensive functions like antivirus scanning of Web traffic grow, so too do the demands for high-performance appliances. Indeed, proxy servers, such as Network Appliance and Blue Coat, are playing an increasingly important role, as these in-line devices handoff Internet traffic to these other functions for content inspection. Gartner clients indicate they are looking at proxy servers and appliances as part of their Web-based antivirus scanning solution.

Note 3

URL database methods

Many vendors use similar approaches to developing and maintaining their databases. For example, many vendors use one or both of the following techniques as their main approach(es) to finding new URLs: automated "crawlers" that search for new and unclassified Web sites, and automatic collection of uncatalogued entries from customer log files. Categorizing the new sites is performed via a variety of techniques, with most vendors relying heavily on automated lexical analysis and manual classification via multilingual "surfmasters." Some vendors offer dynamic classification of uncatalogued URLs — a valuable feature, given the rapid growth of new Web sites. The absence of non-commissioned independent testing makes it difficult to rank the quality and to validate the size and accuracy of vendors' databases. Vendors do not make the contents of their databases public, so organizations are forced to rely on marketing claims to distinguish between the size of URL databases. The vendors in this report claim database sizes of approximately 6 million to 15 million URL entries that are classified into over 55 categories (Internet Security Systems and Fortinet are exceptions — they claim a database size of over 25 million). Accurate categorizations and timely additions of malicious code sites are more important criteria than having the largest database. Indeed, as the market shifts toward a focus on

malicious code, identifying and blocking high-risk sites as quickly as possible will become more important. Effective dynamic categorization of new sites and programs remains a work in progress, and one area where the vendors in this market must further innovate.

Note 4

Other vendors not included in the formal MarketScope analysis

Several vendors that offer solutions in this area have not been included in the formal analysis because they do not fit the inclusion criteria.

Vendors such as Fortinet, Internet Security Systems and Symantec offer multifunction security appliances and have their own URL lists. However, they do not focus on URL filtering. Fortinet offers an ASIC-based appliance and has its own antivirus engine and URL list. Unlike Internet Security Systems and Symantec, it offers a separate URL filtering service, but the company prefers to focus instead on its bundled offering which includes antivirus, URL and e-mail content filtering as part of its overall perimeter security suite. Fortinet also offers a remote user agent, which delivers URL filtering protection for mobile workers that are disconnected from their organization's network.

Symantec uses the URL list the company acquired from URL labs. Symantec's lack of a focused gateway solution for malicious code management is a significant hole in its portfolio, and we anticipate it will make investments in this area in 2006 and 2007.

Internet Security Systems bought Cobion in 2004, a well-regarded German content filtering company. However, Internet Security Systems has focused on multifunction security appliances that bundle in the URL filtering at no additional charge. These appliances tend not to be specialized enough for most large, or even midtier, enterprises. Internet Security Systems also OEMs the Cobion URL list to Aladdin and Blue Coat and we expect its OEM business to continue. Internet Security Systems licenses Sophos antivirus within its appliance, but its specialized anti-spyware is rudimentary. We believe Internet Security Systems could take advantage of the security-focused landscape and further invest in Cobion and anti-spyware capabilities, to release a more focused malicious code management gateway appliance.

McAfee has recently released an appliance for Web-based antivirus and spyware scanning, and has licensed the Secure Computing URL list.

Finjan and Aladdin also offer gateway solutions in this space using a combination of their own and others' technology. Finjan partners with URL vendors and antivirus partners like McAfee, and combines them with its active content scanning. Aladdin uses its own antivirus and licenses a URL list from Internet Security Systems.

We also anticipate the SMBs that are reluctant to make the capital investments in hardware may look to managed services for HTTP-based security threats. E-mail managed security services vendors have already partnered in this area. For example, MessageLabs resells the ScanSafe service and BlackSpider has licensed Secure Computing's SmartFilter URL filtering.

Gartner MarketScope Defined

Gartner's MarketScope provides specific guidance for users who are deploying, or have deployed, products or services. A Gartner MarketScope rating does not imply that the vendor meets all, few or none of the evaluation criteria. The Gartner MarketScope evaluation is based on a weighted evaluation of a vendor's products in comparison with the evaluation criteria. Consider

Gartner's criteria as they apply to your specific requirements. Contact Gartner to discuss how this evaluation may affect your specific needs.

In the below table, the various ratings are defined:

MarketScope Rating Framework

Strong Positive

Is a solid provider of strategic products, services or solutions.

- *Customers:* Continue investments.
- *Potential customers:* Consider this vendor a strong strategic choice.

Positive

Demonstrates strength in specific areas, but is largely opportunistic.

- *Customers:* Continue incremental investments.
- *Potential customers:* Put this vendor on a shortlist of tactical alternatives.

Promising

Shows potential in specific areas; however, initiative or vendor has not fully evolved or matured.

- *Customers:* Watch for a change in status and consider scenarios for short- and long-term impact.
- *Potential customers:* Plan for and be aware of issues and opportunities related to the evolution and maturity of this initiative or vendor.

Caution

Faces challenges in one or more areas.

- *Customers:* Understand challenges in relevant areas; assess short- and long-term benefit/risk to determine if contingency plans are needed.
- *Potential customers:* Note the vendor's challenges as part of due diligence.

Strong Negative

Has difficulty responding to problems in multiple areas.

- *Customers:* Exit immediately.
- *Potential customers:* Consider this vendor only if there are no alternatives.

REGIONAL HEADQUARTERS

Corporate Headquarters

56 Top Gallant Road
Stamford, CT 06902-7700
U.S.A.
+1 203 964 0096

European Headquarters

Tamesis
The Glanty
Egham
Surrey, TW20 9AW
UNITED KINGDOM
+44 1784 431611

Asia/Pacific Headquarters

Gartner Australasia Pty. Ltd.
Level 9, 141 Walker Street
North Sydney
New South Wales 2060
AUSTRALIA
+61 2 9459 4600

Japan Headquarters

Gartner Japan Ltd.
Aobadai Hills, 6F
7-7, Aobadai, 4-chome
Meguro-ku, Tokyo 153-0042
JAPAN
+81 3 3481 3670

Latin America Headquarters

Gartner do Brazil
Av. das Nações Unidas, 12551
9º andar—World Trade Center
04578-903—São Paulo SP
BRAZIL
+55 11 3443 1509