

Next-Generation Secure Web Gateway

Trends And Requirements

*A commissioned study conducted by Forrester Consulting on behalf of
McAfee, Inc.*

December 2008



Headquarters

Forrester Research, Inc., 400 Technology Square, Cambridge, MA 02139 USA
Tel: +1 617.613.6000 • Fax: +1 617.613.5000 • www.forrester.com

Table Of Contents

Executive Summary	4
Introduction And Survey Methodology.....	5
Web 2.0 Is Prevalent And Here To Stay	7
Mobile Filtering Is Increasingly Important	9
Mobile Workforce Is Increasingly Common	9
Mobile Filtering Is Considered Important	10
Large Companies Prefer Mobile Filtering To Be Part Of The Gateway Solution	12
Security And Control Requirements For A Web Filtering Solution	13
Data Leaks Are A Top-Of-Mind Concern.....	13
Malware Continues To Be A Costly And Challenging Problem	14
Application Control Is An Important Item For Web Filtering	16
Anonymizing Proxy Detection And SSL Processing Are Considered Important.....	17
Strategy To Deal With The Unknown Is Primitive.....	19
Analysis: Current Web Filtering Solutions Do Not Adequately Reflect Requirements	20
The Changing (And Broadening) Role Of Web Filtering Solutions	22
Web Filtering Takes On SSO, Especially For Large Organizations	22
Quality Of Service Management Of Web Traffic Emerges As A New Requirement, Led By Large Organizations	24
Forward-Looking Trends	26
SaaS Is Not Universally Embraced: SMBs Prefer SaaS More Than Their Larger Counterparts .	26
Consolidation In Content Security Is Preferred By Many	28
Users' View Of Emerging Internet Threats	30
Conclusions	31
Web Filtering Is Not Just About Security; It Is A Business Initiative	31

DLP Is Important But Not Practiced Universally 31

Mobile Filtering Strategies Are Imminently Important..... 31

Users Should Look To Vendors With These Functionalities 31

Appendix A: Methodology 33

Appendix B: Endnotes 34

© 2008, Forrester Research, Inc. All rights reserved. Forrester, Forrester Wave, RoleView, Technographics, TechRadar, and Total Economic Impact are trademarks of Forrester Research, Inc. All other trademarks are the property of their respective companies. Forrester clients may make one attributed copy or slide of each figure contained herein. Additional reproduction is strictly prohibited. For additional reproduction rights and usage information, go to www.forrester.com. Information is based on best available resources. Opinions reflect judgment at the time and are subject to change.

Executive Summary

As part of an ongoing market research effort, Secure Computing commissioned Forrester Consulting in November 2008 to conduct a study of Web filtering requirements and trends across small and medium-size businesses (SMBs) and enterprises. Also in November 2008, McAfee acquired Secure Computing.¹ This study is an update of a similar commissioned study Forrester Consulting conducted on behalf of Secure Computing in October 2007. The purpose of this study is to understand how various factors and trends — including Web 2.0 usage, changing business requirements on the Web, and the prevalence of remote workers — impact users' views on and requirements of Web filtering technologies.

We surveyed 253 IT and security professionals who are primary IT decision-makers about Web security technologies. Their roles include director of IT, director of IT security, enterprise architect, information security officer, and network security architect. The organizations surveyed have at least 500 Internet users. Thirty-four percent of those we surveyed have more than 5,000 Internet users.

We found that Web 2.0 usage remains prevalent in organizations of all sizes, including those that have less than 1,000 Internet users. Many also anticipate their Web 2.0 usage to increase for the foreseeable future.

We also found that the role of Web filtering is changing from a security-centric function to more of a business function. More and more organizations are using Web filtering beyond defending against Web threats. Rather, they are incorporating functions such as productivity management, traffic quality of service (QoS) management, and even single sign-on (SSO). As organizations' worker populations becomes more mobile and distributed, many indicated that mobile filtering is an increasingly important new requirement for Web filtering solutions.

Given the rising complexity of Web communications and the nonrelenting Web threats, we recommend that organizations look to vendors with these future-looking capabilities: 1) Web malware detection; 2) a solid in-the-cloud infrastructure; 3) a strong consolidation and integration strategy; and 4) the ability to perform fine-grained controls for Web 2.0 applications.

Introduction And Survey Methodology

In November 2008, Secure Computing (prior to the acquisition by McAfee) commissioned Forrester Consulting to conduct a survey of 253 businesses across North America and Europe with 500 or more employees. The purpose of the survey is to understand market needs and requirements for next-generation Web filtering solutions. This is also an update survey from last year's study.²

To understand the challenges around security threats caused by Web 2.0 and live applications on the Web, Secure Computing commissioned Forrester Consulting to conduct an online survey with 253 respondents. Of these respondents:

- The companies were based in:
 - The US and Canada — 130 respondents.
 - Europe (including the UK, France, Germany, and Nordic countries) — 123 respondents.
- The respondents were IT decision-makers or influencers responsible for security issues.
- The companies had 500 or more Internet users.
- Forrester kept the names and the companies of interviewees confidential.
- Secure Computing was not identified as the sponsor.

Of the 253 survey respondents, we have a nearly 50/50 breakdown between North American companies and European companies. More specifically, there are 100 companies from the US, 30 from Canada, and the remaining 123 are from European countries.

The size of the companies we surveyed can be seen here (see Table 1).

Table 1: Size Breakdown Of Survey Respondents

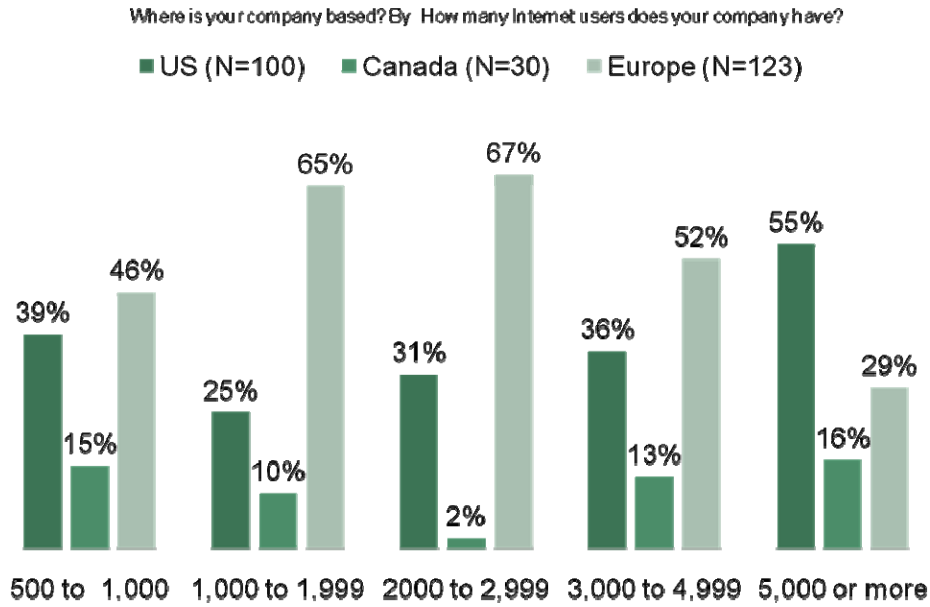
Internet user size	Number of respondents	Percentage
500 to 999	39	15%
1,000 to 1,999	49	19%
2,000 to 2,999	48	19%
3,000 to 4,999	31	12%
More than 5,000	86	34%

Base: 253 global IT decision-makers

Source: "Next Generation Secure Web Gateway," A commissioned study by Forrester Consulting on behalf of McAfee

A more detailed demographic of our survey correspondents is depicted here (see Figure 1).

Figure 1: Company Size And Geo-Location Of Survey Respondents



Base: 253 global IT decision-makers

Source: "Next Generation Secure Web Gateway," A commissioned study by Forrester Consulting on behalf of McAfee

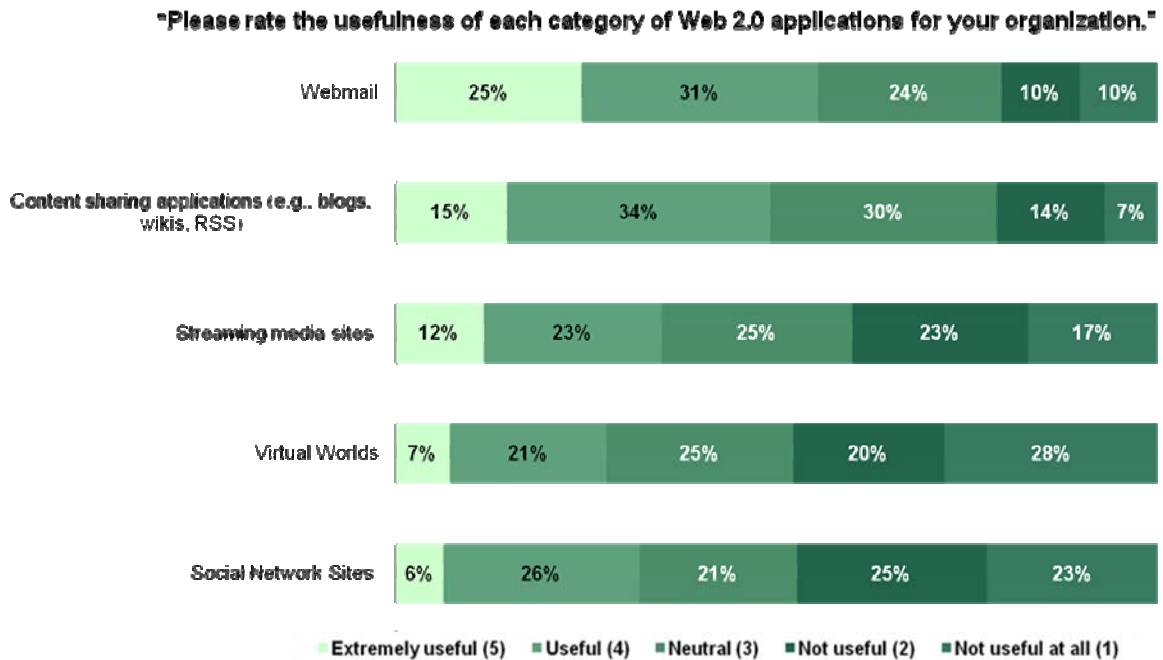
The roles of the actual respondents include IT decision-makers, network architects, network security personnel, and those who make purchase decisions for networking and security technologies.

We asked the respondents a series of 31 questions, spanning Web filtering technologies, threats, Web usage trends, and corporate requirements. The remainder of this document summarizes our findings from this survey.

Web 2.0 Is Prevalent And Here To Stay

In our survey, we found that Web 2.0 applications continue to enjoy heavy usage in both enterprises and small to medium sized businesses (SMBs). We asked the respondents to rate the usefulness of Web 2.0 applications, including Web mail, streaming media sites, and social networks. Many respondents indicated that they consider these Web 2.0 applications useful for business purposes. Of the 253 respondents, 56% believe Web mail is useful; 49% rated content-sharing applications. More than 30% rated streaming media and social networking useful, while 28% consider virtual worlds a useful business tool (see Figure 2).

Figure 2: Web Mail Is Ranked The Most Useful Web 2.0 Application



Base: 253 global IT decision makers

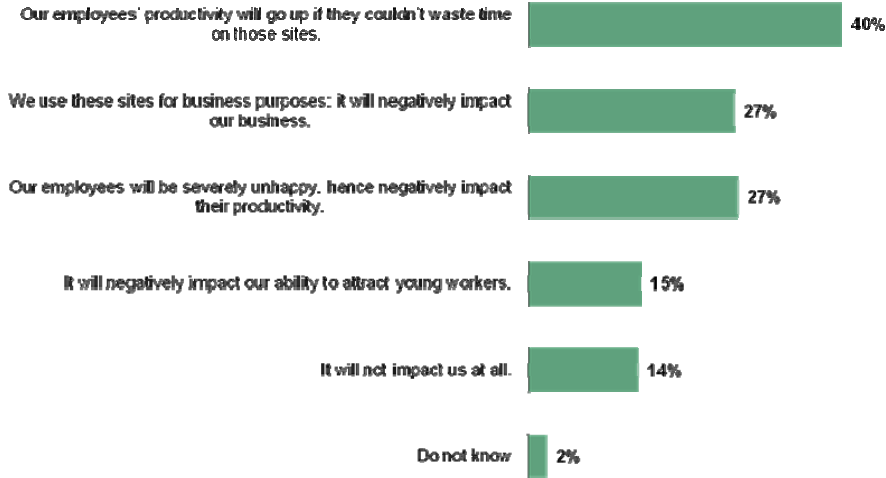
Source: "Next Generation Secure Web Gateway," A commissioned study by Forrester Consulting on behalf of McAfee

Social networking and streaming media see increased business usage. More companies this year are considering social networking and streaming media useful business tools than last year. In last year's study, 24% indicated that social networking sites were useful, and this year, this number rose to 32%. Last year, only 22% said streaming media was useful for business; this year, 35% said so (see Figure 3). Though slightly decreased from last year's numbers, approximately 50% of all companies we surveyed indicated that both Web mail and content-sharing applications were useful for business purposes.

When we asked about social networking sites in particular, a nontrivial percentage (27%) indicated that they use social networking sites specifically for business purposes. If access to these sites is blocked, it will negatively impact their business. Another 15% indicated that blocking access to these sites would impact their ability to attract young workers (see Figure 3).

Figure 3: Access To Social Networking Sites Is Important To Business

"If access to social networking sites, such as MySpace and Facebook, is blocked, how would this impact your organization?"



Base: 253 global IT decision makers

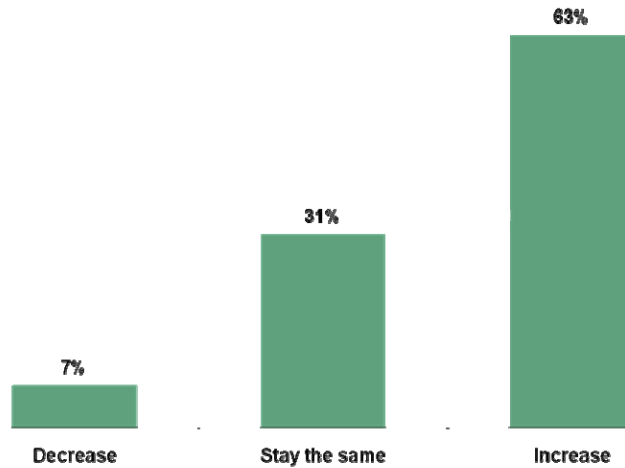
Source: "Next Generation Secure Web Gateway," A commissioned study by Forrester Consulting on behalf of McAfee

Many believe usage of Web 2.0 will continue to increase. In this year's study, we saw an increasing percentage of companies (19%) for which Web 2.0 usage takes more than 50% of their bandwidth. Last year, only 14% of the respondents fell into this category.

In addition, many respondents — 63% of those we surveyed — believe the use of Web 2.0 applications would increase in their organization in the next 12 months (see Figure 4). These answers were universal across enterprises, those with 2,000 or more Web users, and SMBs, whose user populations are less than 2,000. In addition, the answers from the US and the European respondents were remarkably similar, signifying a universal acceptance and the trend of increasing Web 2.0 usage across the US and Europe.

Figure 4: Increase In Web 2.0 Application Usage Is Expected

"How do you anticipate your organizations use of Web 2.0 applications to change in the next 12 months?"



Base: 253 global IT decision makers

Source: "Next Generation Secure Web Gateway," A commissioned study by Forrester Consulting on behalf of McAfee

Mobile Filtering Is Increasingly Important

Many organizations today have some form of a mobile workforce, including home workers, travelers, and partners. These personnel work on corporate-sensitive tasks and yet often lie beyond the physical corporate boundaries.

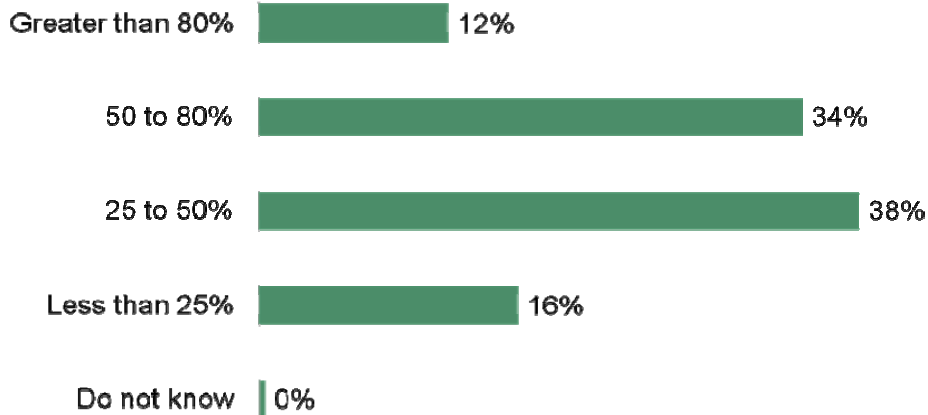
Mobile Workforce Is Increasingly Common

Our survey data showed 84% of the companies have at least a quarter of their employee population "mobile," and they often access the Web beyond the corporate network for business purposes (see Figure 5).

In the study we conducted last year, 44% of respondents said they had less than 25% mobile population. This year, this number has dwindled to 16%. In this global economy, traditional business models are fast disappearing; more and more companies are employing mobile workforces. We expect this trend to continue for the foreseeable future.

Figure 5: Many Organizations Have Significant Mobile Populations

“What percentage of your user population is mobile and accesses the web using their computers or smart phones outside the office?”



Base: 253 global IT decision makers

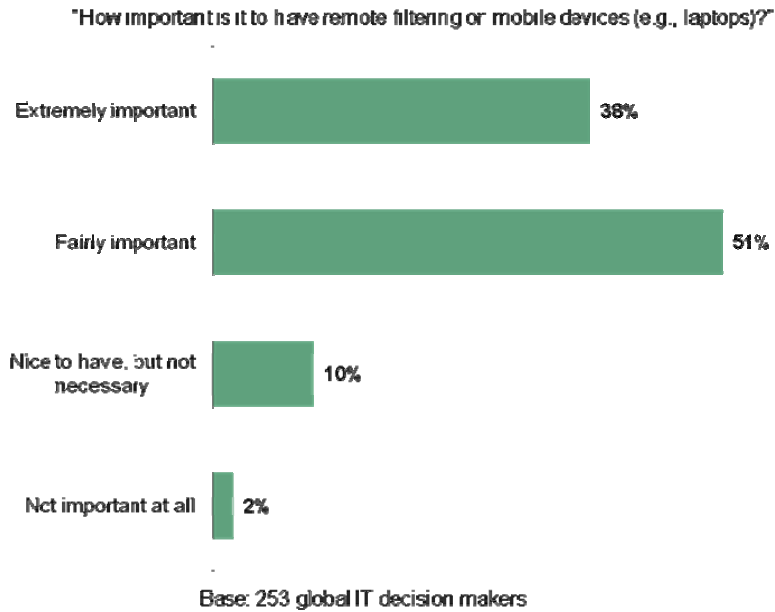
Source: “Next Generation Secure Web Gateway,” A commissioned study by Forrester Consulting on behalf of McAfee

Mobile Filtering Is Considered Important

A mobile workforce presents a challenge to traditional on-premise filtering approaches, as the browsing traffic from the mobile endpoints do not go through any corporate filtering points. Therefore, a special filtering treatment is needed to accommodate mobile workers. Because of this complexity, many organizations today simply do not perform Web filtering on mobile endpoints. All kinds of security problems could ensue due to this practice, including infected mobile laptops bringing malware into the corporate network.

We asked our respondents how important it is to enforce Web filtering on mobile endpoints; nearly 90% said it was important, including 38% who indicated “Extremely important” and 51% who said it was “Fairly important” (see Figure 6).

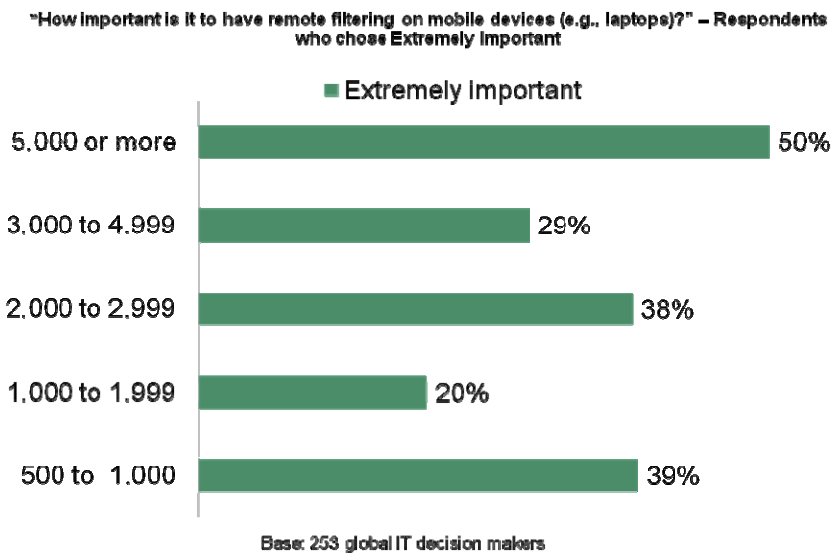
Figure 6: Remote Filtering On Mobile Devices Is Important



Source: "Next Generation Secure Web Gateway," A commissioned study by Forrester Consulting on behalf of McAfee

Another look into the answers revealed that large organizations, those with 5,000 employees or more, are more likely to find mobile filtering extremely important (see Figure 7).

Figure 7: Remote Mobile Filtering Is An Important Functionality



Source: "Next Generation Secure Web Gateway," A commissioned study by Forrester Consulting on behalf of McAfee

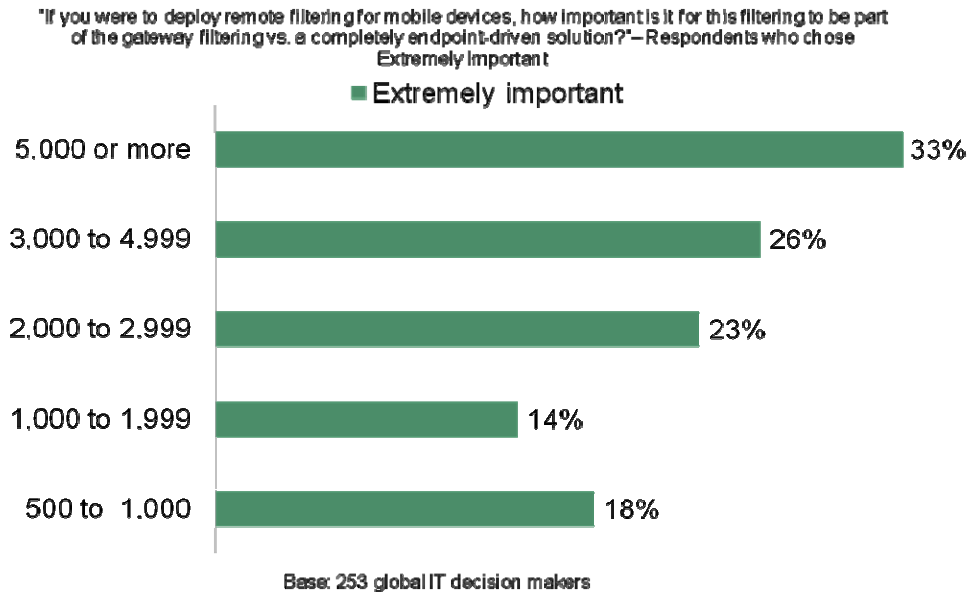
Large Companies Prefer Mobile Filtering To Be Part Of The Gateway Solution

A number of different approaches exist for mobile filtering. Companies that have a virtual private network (VPN) can filter the Web traffic at a central location (e.g., at a filtering gateway) when the remote worker is logged on via the VPN connection. Other approaches also exist to enforce backhauling of Web traffic through a corporate filtering point. An alternative is to enforce mobile filtering using a client-based approach; an agent (tamper-resistant agent preferred) installed on the mobile endpoint can enforce the corporate usage policies or enforce a cloud-based proxy that performs policy-based filtering.

We asked our respondents how important it is for mobile filtering to be part of a gateway strategy (i.e., backhauling endpoint traffic to the gateway) as opposed to other delivery models, such as a complete endpoint-driven approach. We found that large organizations prefer the gateway solution; 33% of companies with 5,000 or more employees responded with an “Extremely important” answer, while less than 20% of those with less than 2,000 employees gave the same answer (see Figure 8).

It is perhaps not surprising why large organizations may prefer mobile filtering to take place as part of a corporate gateway solution, as they typically would have a gateway-based filtering system already, and folding remote filtering into that strategy would render centralized policy management and reporting, which is a fairly attractive proposition.

Figure 8: Large Organizations Favor Gateway Filtering



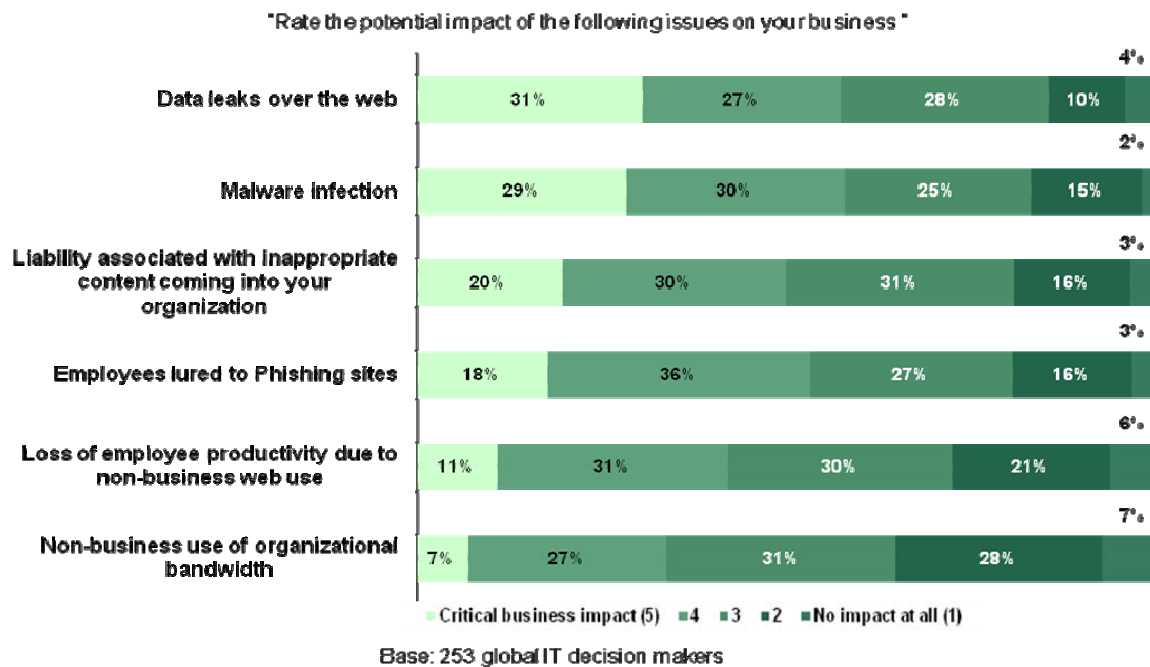
Source: “Next Generation Secure Web Gateway,” A commissioned study by Forrester Consulting on behalf of McAfee

Security And Control Requirements For A Web Filtering Solution

Data Leaks Are A Top-Of-Mind Concern

Data leaks remain one of the top concerns for organizations. We asked our respondents to rate the business impact of several Web-related risks, including data leaks, malware, loss of productivity, nonbusiness use of bandwidth, and liability for inappropriate content. The answers we received put data leaks on the Web the No. 1 issue — 31% said it had a critical business impact, and 27% said it had an impact (see Figure 9).

Figure 9: Data Leaks Have Significant Business Impact



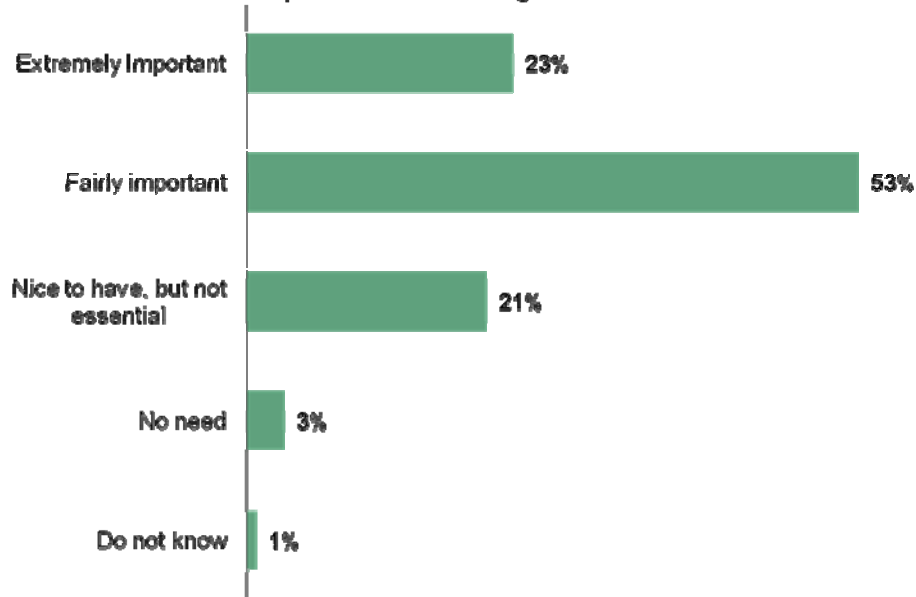
Source: "Next Generation Secure Web Gateway," A commissioned study by Forrester Consulting on behalf of McAfee

We also found that users look to Web filtering solutions to perform data leak prevention (DLP). When asked about the importance of outbound content inspection for DLP purposes, 76% replied it was important (see Figure 10). Among those who answered "Extremely important," 27% come from organizations with 5,000 or more employees, while 15% are from companies with 1,000 or less employees. As such, large organizations appear to be more concerned about the risk of data leaks over the Web.

Although 86% consider data leaks an important threat, when asked what policy they have to govern internal employees contributing content to external blogs and wikis, only 68% said they impose some form of restriction (either complete block or selective block), while 31% said they do not have any restriction for employees to access these third-party sites.

Figure 10: DLP As Part Of Web Filtering Is Considered Important

"How important is the capability of outbound content inspection for data leak prevention (DLP) purposes, as part of the Web filtering solution?"



Base: 253 global IT decision makers

Source: "Next Generation Secure Web Gateway," A commissioned study by Forrester Consulting on behalf of McAfee

Malware Continues To Be A Costly And Challenging Problem

Malware, traditionally distributed via email, is now using the Web as a primary distribution channel. Web malware, especially those that are scripts-based, can effectively evade signature-based anti-virus scanning.

We asked our respondents how much they spent in the past 12 months for malware cleanup. Forty percent of all organizations spent more than \$50,000 last year on malware cleanup alone, and nearly 20% spent more than \$100,000 (see Figure 11).

Figure 11: Costs Of Malware Cleanup Remains High



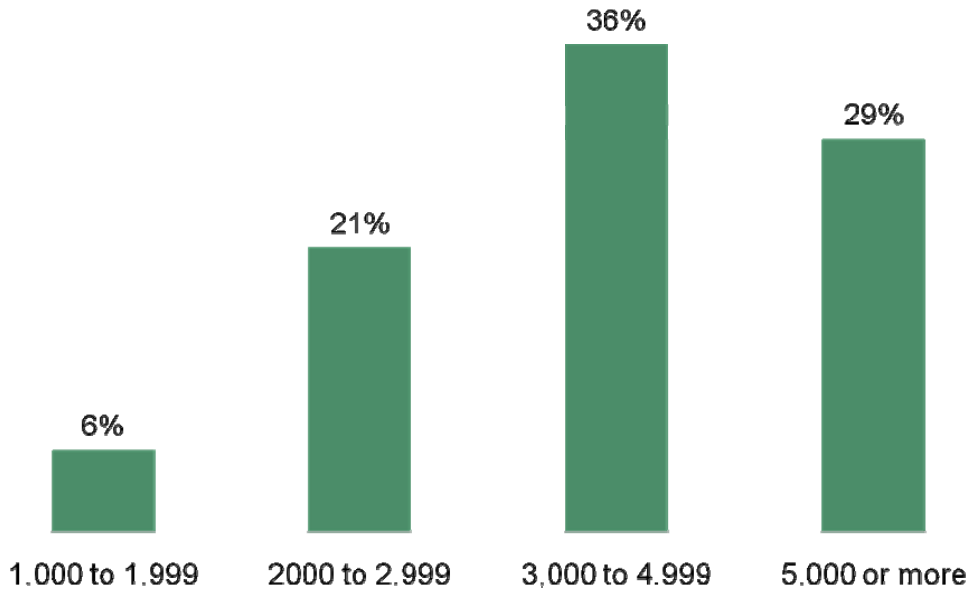
Source: "Next Generation Secure Web Gateway," A commissioned study by Forrester Consulting on behalf of McAfee

Year after year, despite the proliferation of anti-virus software, these cost figures do not let up. The reality is that Web-based malware is a whole new class of threats, different from traditional computer viruses. It requires different analysis and detection methods, which are still nascent for many Web filtering solutions.

The cost figures are clearly dependent on the size of the organization--large companies tend to spend more on malware cleanup. In our study, we found that companies with 3,000 or more employees are more likely to spend more than \$100,000 per year on malware cleanup, while none of the sub-1,000 organizations spent more than \$100,000 (see Figure 12).

Figure 12: Companies That Spent More Than \$100,000 On Malware Cleanup, By Size

"In the past fiscal year, how much did your organization spend on malware cleanup?" – Greater than \$100,000



Base: 253 global IT decision-makers

Source: "Next Generation Secure Web Gateway," A commissioned study by Forrester Consulting on behalf of McAfee

We also found that European companies spent more on malware cleanup than the US and Canadian companies. More specifically, 24% of the European respondents (UK, France, Germany, and Nordic countries) reported that they spent more than \$100,000 last year on malware cleanup, while only 10% of Canadian companies and 16% of US companies fall in the same category.

When asked how concerned they are about the increase of malware from legitimate Web sites, nearly 50% of all respondents replied they are definitely concerned and are actively doing something about it. When we look closer at the data, we found that only 30% of the sub-1,000 companies fell in this category, while more than 50% of companies with 2,000 or more employees are actively protecting against this threat. Small organizations appear to be lagging behind in this particular functionality.

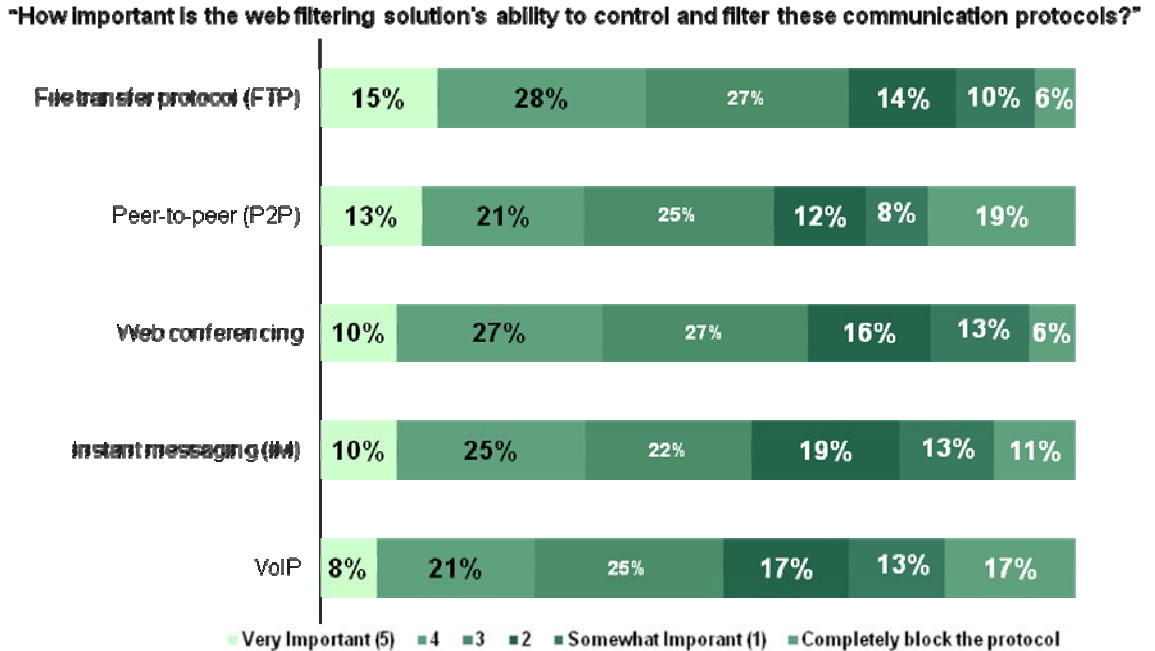
Application Control Is An Important Item For Web Filtering

Detection and control of other communication protocols, such as FTP and P2P, have been part of the Web filtering functionality family for some time now. In this survey, we asked our respondents to rate the importance of the Web filtering solution's ability to control and filter a set of different communication protocols.

The answers we received put FTP and WebEx at the top, followed closely by P2P and IM. Popular communication protocol Skype is ranked at the bottom (see Figure 13). No visible patterns based

on company sizes emerged in the answers. This indicates that SMBs and large organizations alike have the need for application control across these various communication protocols.

Figure 13: FTP And WebEx Top The List Of Controlled Applications



Source: A commissioned study by Forrester Research on behalf of Secure Computing

Source: "Next Generation Secure Web Gateway," A commissioned study by Forrester Consulting on behalf of McAfee

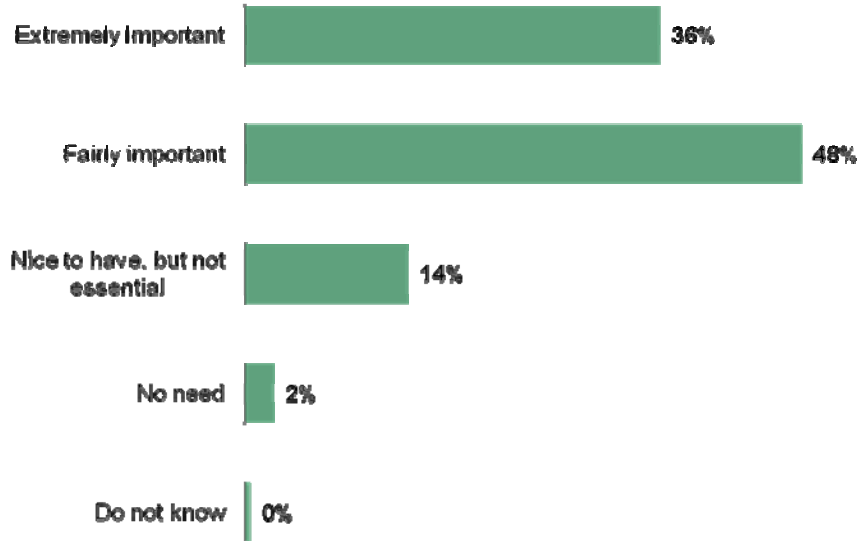
Anonymizing Proxy Detection And SSL Processing Are Considered Important

Anonymizing proxies on the Internet, acting as an intermediary between the destination Web site and the user, presents a problem for Web filtering solutions because they are often able to obscure the true browsing destination of the user, and as a result, foil any corporate policies regarding Web usage. Recently, Web filtering solutions are starting to include the ability to detect (and hence prevent) the use of anonymizing proxies. Detection mechanisms may vary, ranging from simple URL filtering (prevents users from going to well-known proxy sites) to traffic signature recognition.

We asked our respondents how they felt about the ability to detect and prevent the use of anonymizing proxies. The response is overwhelmingly positive; 84% of the 253 respondents consider the detection of anonymizing proxy sites an important function (see Figure 14). These statistics are evenly distributed across large organizations and small companies, which shows anonymizing proxies are an equal plight to large and small companies.

Figure 14: Organizations Consider Anonymizer And Proxy Sites Detection And Prevention An Important Function

How important is the ability to detect and prevent the use of anonymizer and proxy sites? (Anonymizer and proxy sites act as an intermediary proxy to obscure the true destination of a user's browsing the Internet)

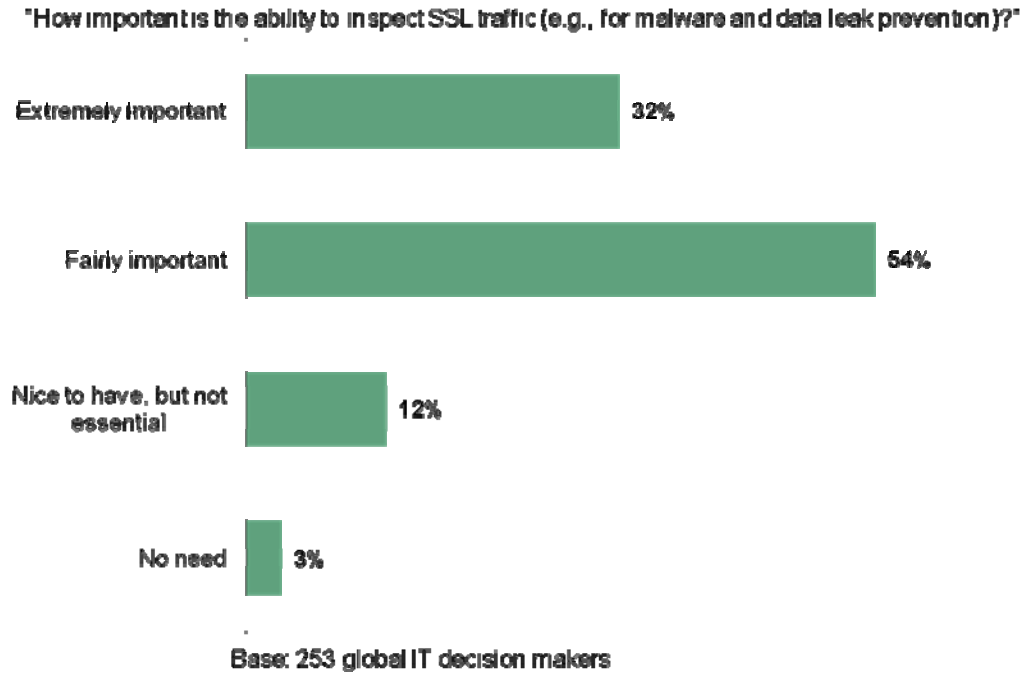


Base: 253 global IT decision makers

Source: "Next Generation Secure Web Gateway," A commissioned study by Forrester Consulting on behalf of McAfee

Being able to analyze SSL traffic, including looking inside the encrypted traffic and performing content filtering, is often another important requirement for Web filtering. When asked how important is the ability to inspect SSL traffic (e.g., for malware and DLP), 86% of the respondents indicated that it was important (see Figure 15). The answer to this question is again evenly distributed across large and small organizations.

Figure 15: It Is Important To Inspect SSL Traffic



Source: "Next Generation Secure Web Gateway," A commissioned study by Forrester Consulting on behalf of McAfee

Strategy To Deal With The Unknown Is Primitive

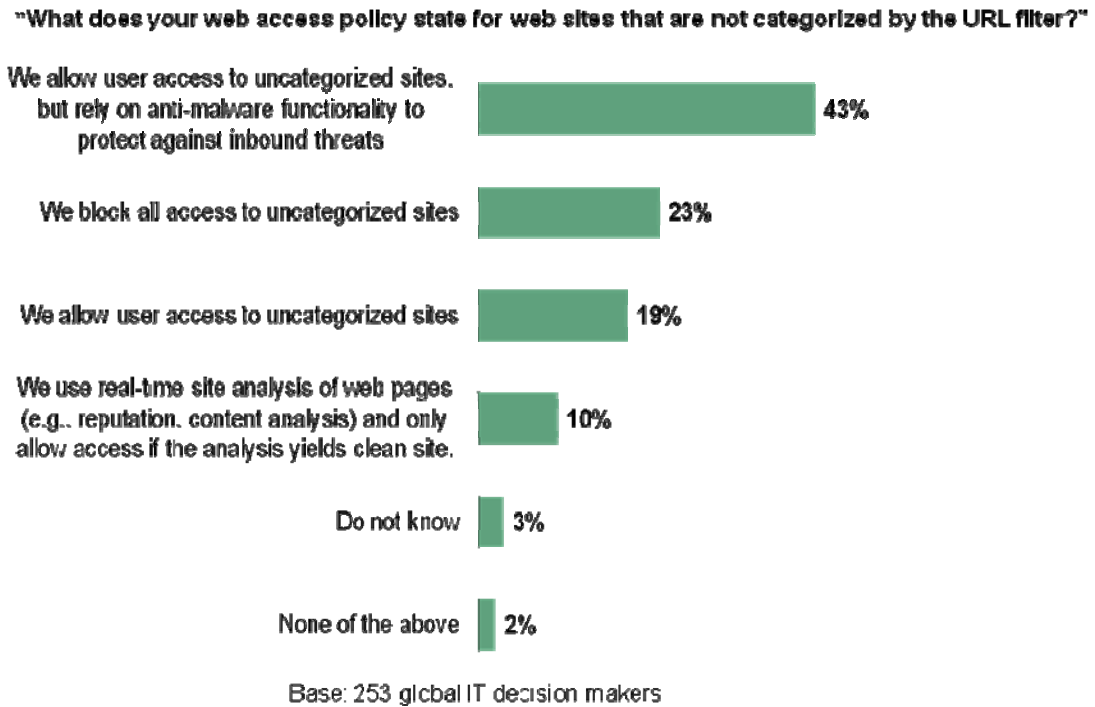
As URL filtering is widely deployed, and many organizations have policies governing users' browsing for well-understood Web content categories, we asked our respondents to describe their policies dealing with uncategorized Web sites (see Figure 16).

The results are interesting: Many organizations are taking a black-and-white approach — either block all access to unknown sites or allow them unequivocally (barring anti-malware scanning). A small percentage of respondents indicated that they utilize any kind of real-time site analysis technologies to classify content in real time and apply control policies.

This black-and-white approach is clearly insufficient in today's dynamic Internet environment. There are approximately 185 million Web sites on the Internet today.³ The largest URL filtering database today probably contains 30 million Web sites. That means many Web sites will be uncategorized, and many uncategorized Web sites may contain malware or content that violates the company's acceptable use policies. An approach that completely allows or disallows the entire uncategorized Web site population does not permit fine-grained access policies and will engender false positives and negatives.

In addition, it is increasingly common today that legitimate Web sites are used in malware distribution, which means straightforward category-based URL filtering is increasingly less effective. It is therefore imperative that real-time Web content analysis is used in addition to URL filtering. Real-time analysis includes reputation, malware analysis, content analysis, and real-time categorization.

Figure 16: Organizations View Access To Uncategorized Sites A Black-And-White Answer



Source: “Next Generation Secure Web Gateway,” A commissioned study by Forrester Consulting on behalf of McAfee

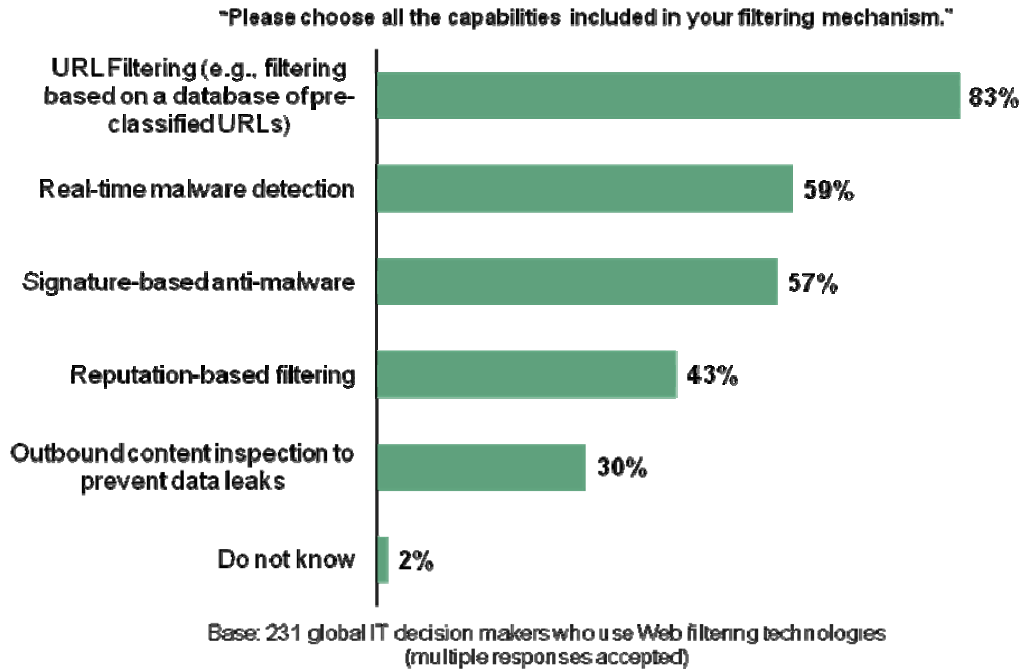
Analysis: Current Web Filtering Solutions Do Not Adequately Reflect Requirements

Many companies we surveyed use some form of Web filtering capability. We asked them to describe all the functions in their Web filtering solutions (see Figure 17). As shown, 83% of respondents have URL filtering, which is consistent with our belief that URL filtering is widely adopted across the industry. In contrast, only 74% of last year’s respondents reported the use of URL filtering.

Thirty percent of those we surveyed reported that they use some form of outbound content filtering for Web traffic. Given that data leaks are rated the No. 1 issue with business impact (see Figure 9), organizations are not doing nearly enough today to prevent data leaks over HTTP.

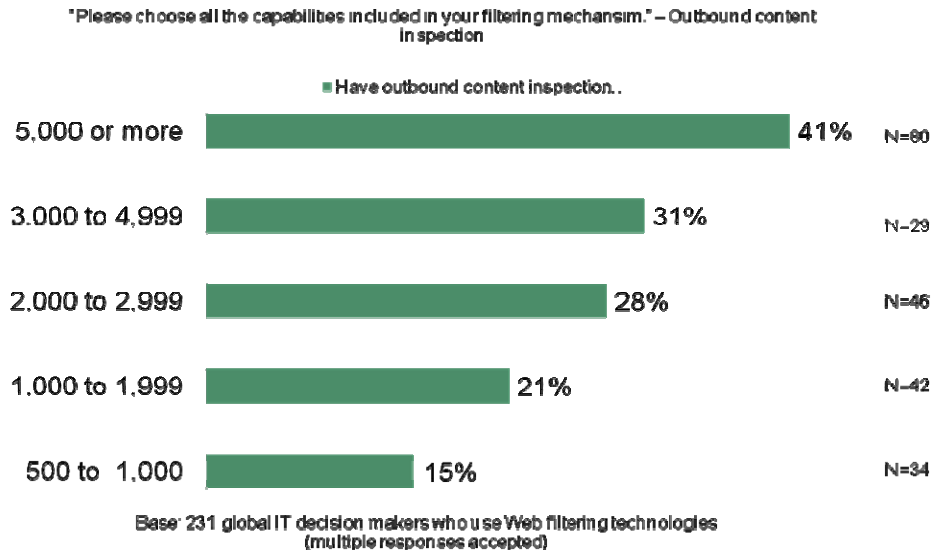
Another look at the data reveals that DLP is even less practiced at SMBs than enterprises--forty-one percent of companies with 5,000 or more employees have outbound content protection, while only 15% of those sub-1,000 companies use the same functionality. (see Figure 18)

Figure 17: Technical Components Of Current Web Filtering Solutions



Source: "Next Generation Secure Web Gateway," A commissioned study by Forrester Consulting on behalf of McAfee

Figure 18: Outbound Content Inspection Capabilities Are More Prevalent In Larger Organizations



Source: "Next Generation Secure Web Gateway," A commissioned study by Forrester Consulting on behalf of McAfee

Fifty-nine percent of the respondents indicated that they have real-time malware detection capabilities (see Figure 17). This is somewhat surprising, given that real-time analysis of Web

pages is a rare practice (see Figure 16). We believe the number of organizations that actually deploy real-time malware detection, such as heuristics and behavior-based techniques, is much smaller and that the respondents may not have understood fundamentally the difference between real-time and signature-based malware detection.

Another interesting statistic is that, although 43% of companies indicate that they have reputation-based filtering (see Figure 17), only 10% are actually using reputation information to filter uncategorized Web pages (see Figure 16). The reality is that many companies may have some form of reputation information in their Web filtering solution, but few are actually taking full advantage of this information for policy controls.

The Changing (And Broadening) Role Of Web Filtering Solutions

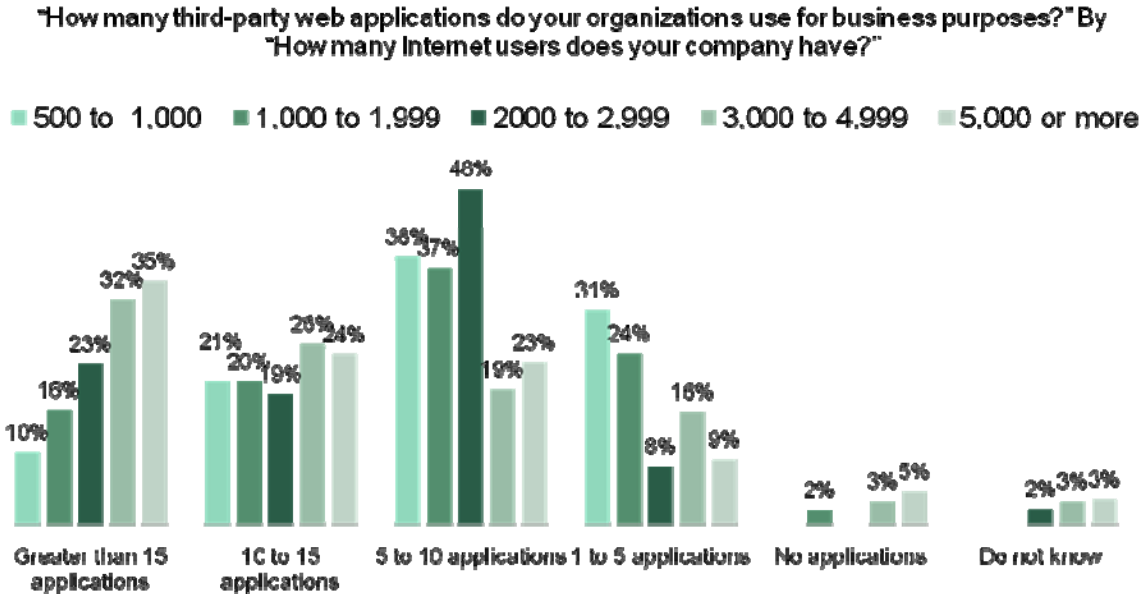
Traditionally, Web filtering is all about URL filtering — it's about making a decision, based on the category of the Web page, whether an internal user should be permitted to visit that page. The decision is sometimes about acceptable usage policies — whether users should waste bandwidth on non-business-related Web sites, for instance. Sometimes, it's a security-centric one — whether the destination Web site contains malware or potentially harmful programs.

Recently, however, Web filtering is taking on functionality outside of security or usage policies. For example, Web filtering solution is sometimes used to perform WAN acceleration, or rather WAN acceleration boxes sometimes take on Web filtering functions. Organizations are realizing that the Web filtering solution maybe the right place for other related traffic management functions.

Web Filtering Takes On SSO, Especially For Large Organizations

In our survey, we asked our respondents how many third-party Web applications they use for business purposes. The answers we received clearly delineated large organizations from small ones. In the sub-1,000 company category, only 10% of respondents said they use more than 15 in-the-cloud applications, while greater than 30% of the 5,000 or-more user companies indicated that they use more than 15 in-the-cloud applications (see Figure 19).

Figure 19: The Number Of Third-Party Web Applications Used By Organizations



Base: 253 global IT decision-makers

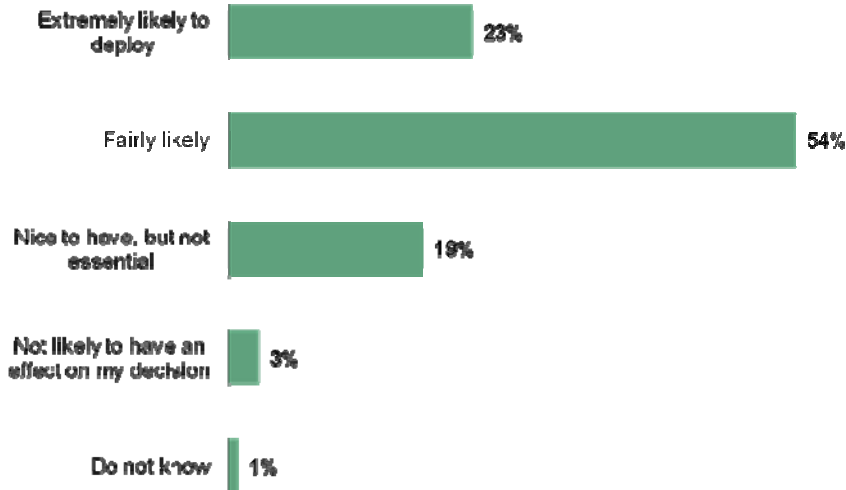
Source: "Next Generation Secure Web Gateway," A commissioned study by Forrester Consulting on behalf of McAfee

Overall, 96% of the companies we surveyed use third-party applications in the cloud. These applications include HR, travel portal, and payroll. As a result, many companies are experiencing some level of complexity in terms of identity management — each in-the-cloud application typically demands its own authentication credentials that are separate from corporate user directories. This ultimately becomes unwieldy and difficult to manage for enterprises, especially those that use a large number of in-the-cloud applications.

When we asked our survey respondents if they are more likely to employ a Web filtering solution if it included SSO for external Web applications, 79% responded "Extremely likely" and "Fairly likely" (see Figure 20). If we break this answer down based on company size, we find that 35% of companies with 5,000 or more employees replied "Extremely likely," while only 15% of those with 500 to 1,000 employees replied with the same level of enthusiasm.

Figure 20: Organizations Welcome Single Sign On As Part Of Web Filtering Solutions

"If the web filtering gateway includes single sign on capabilities to allow your users to use external web applications in a seamless way, are you more likely to employ such a filtering solution?"



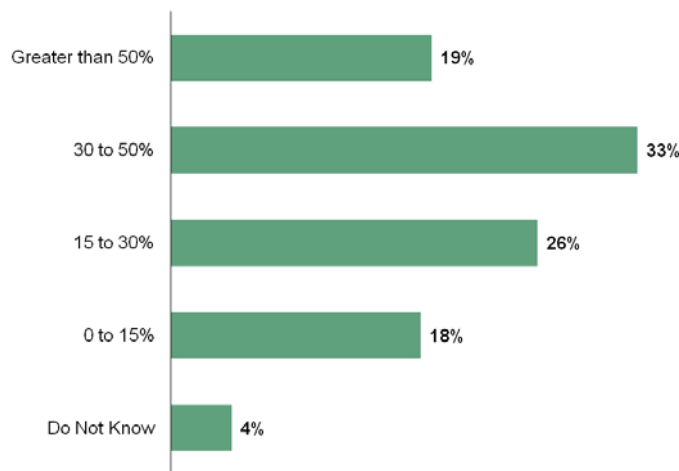
Base: 253 global IT decision makers

Source: "Next Generation Secure Web Gateway," A commissioned study by Forrester Consulting on behalf of McAfee

Quality Of Service Management Of Web Traffic Emerges As A New Requirement, Led By Large Organizations

Web usage is ubiquitous. Many organizations today have both business and non-business Web traffic. In our survey, we found that it is now commonplace for organizations to have more than 30% of their bandwidth taken up by Web 2.0 applications (see Figure 21).

Figure 21: Percentage Of Company's Bandwidth Consumed By Web 2.0 Apps



Base: 253 global IT decision-makers

Source: "Next Generation Secure Web Gateway," A commissioned study by Forrester Consulting on behalf of McAfee

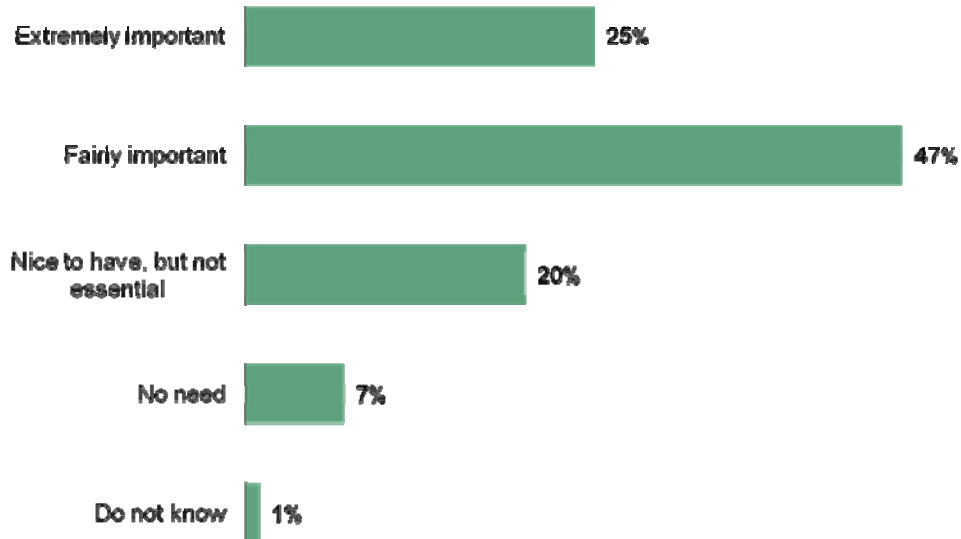
In daily interactions with user organizations, Forrester understands that many companies have difficulty regulating their Web traffic. Some, for fear of bandwidth loss and inappropriate content, take a strict stand and prohibit access to social networking sites and rich media sites. Others that allow access to these sites are doing so with very little control over the various types of traffic.

Given the choice, many organizations would prefer to have more flexibility and control dealing with nonbusiness traffic. For instance, a company may wish to limit access to YouTube whenever the volume of legitimate business traffic is high. Or it may want to enforce application-specific and user-specific policies regarding particular Web 2.0 applications. These requirements cannot be easily met with a simple quota system that works on hours of the day or bandwidth consumption by individual users. What you need is a quality-of-service treatment to Web traffic that allows the organization to allocate specific bandwidth usage for individual applications, based on a flexible set of parameters.

We asked our respondents how important is the ability to control individual Web applications; 72% of our survey respondents told us it was an important requirement for their organization (see Figure 22).

Figure 22: Many Believe The Ability To Allocate Bandwidth Usage For Individual Web Applications Is Important

"How important is it to your organization to be able to allocate bandwidth usage for individual web applications?"



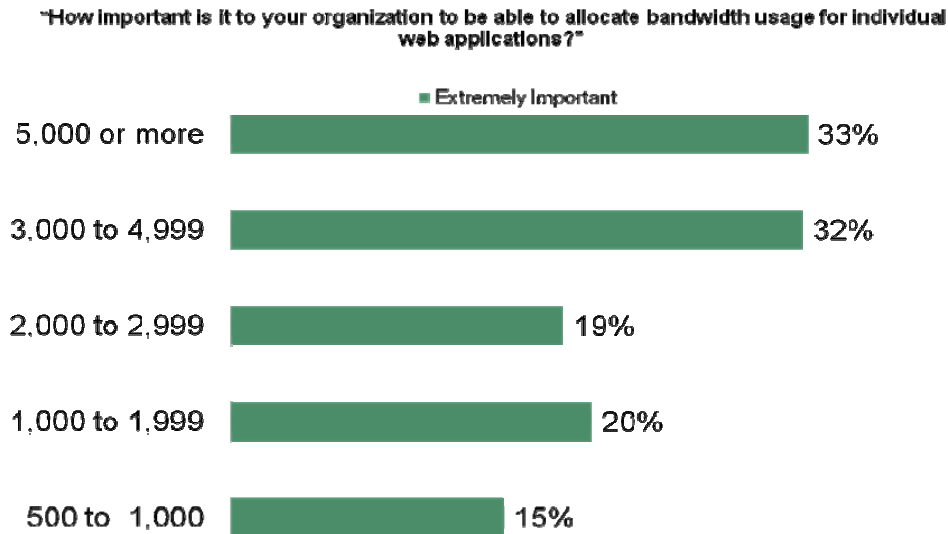
Base: 253 global IT decision makers

Source: "Next Generation Secure Web Gateway," A commissioned study by Forrester Consulting on behalf of McAfee

This requirement again seems to differ from large organizations to small ones. Figure 10 depicts the percentage of organizations that reported an "Extremely important" answer. As shown on the large end of the spectrum — those with 3,000 or more employees — more than 30% considered

individual control of Web applications extremely important. On the other hand, only 15% to 20% of SMBs consider this to be “Extremely important” (see Figure 23).

Figure 23: Percentage Of Companies That Responded “Extremely Important” To Individual Control Of Web Applications



Base: 253 global IT decision makers

Source: “Next Generation Secure Web Gateway,” A commissioned study by Forrester Consulting on behalf of McAfee

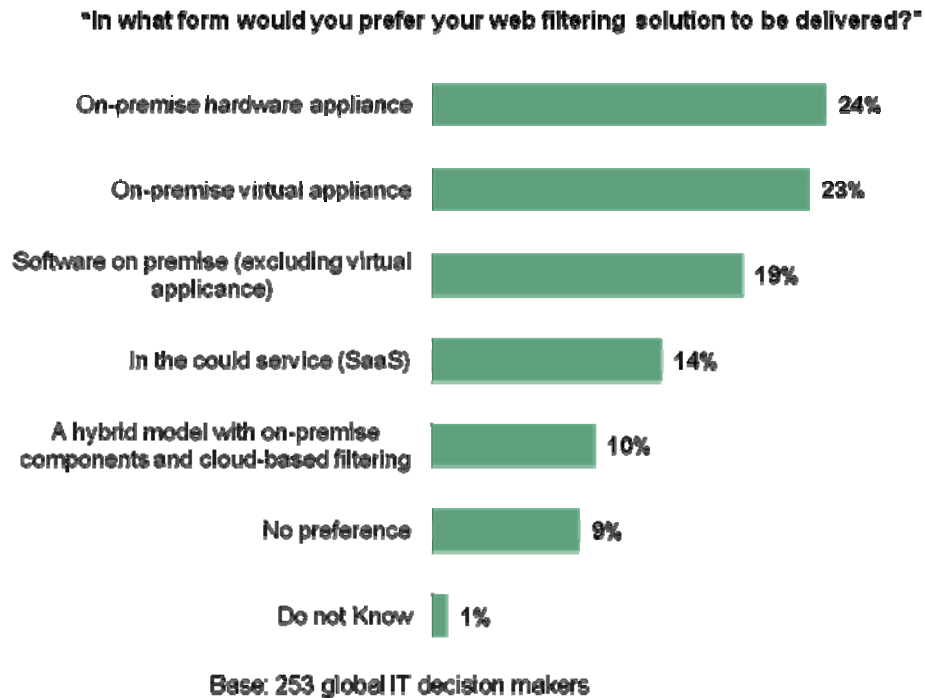
Forward-Looking Trends

In this survey, we included a number of questions designed to extract interesting usage trends. Among others, we focused on delivery models, including software-as-a-service (SaaS) and hybrid, consolidation, and threat trends.

SaaS Is Not Universally Embraced: SMBs Prefer SaaS More Than Their Larger Counterparts

In an effort to understand how organizations perceive various capability delivery models — SaaS versus on-premise, software versus appliance, and others — we asked our respondents how they would like their Web filtering solution to be delivered. The answers we received revealed a somewhat strong preference for on-premise solutions versus SaaS — only 14% responded with a preference for SaaS. The top choice remains the on-premise appliance form factor, both physical and virtual (see Figure 24).

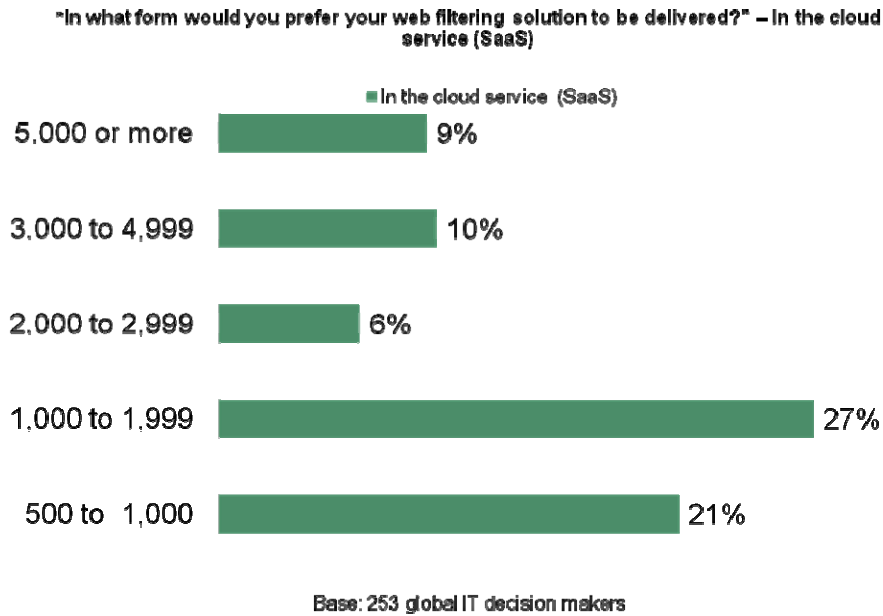
Figure 24: On-Premise Delivery Still Dominates Requirements



Source: "Next Generation Secure Web Gateway," A commissioned study by Forrester Consulting on behalf of McAfee

However, when we looked into the answers in detail, we found that more small companies prefer SaaS delivery than those on the larger side. Twenty-one percent of companies with less than 1,000 employees chose SaaS as the preferred delivery model, while 26% of the 1,000 to 2,000 employee category chose SaaS. In contrast, on the larger end of companies, only 9% of companies with 5,000 or more employees preferred SaaS, and 10% in the 3,000 to 5,000 employee category chose SaaS (see Figure 25).

Figure 25: Companies That Prefer SaaS-Based Web Filtering



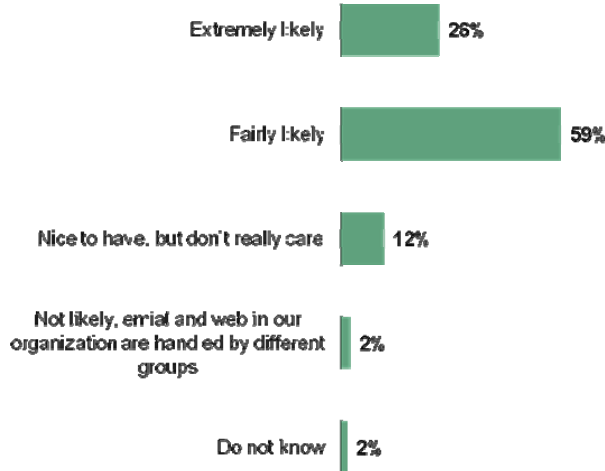
Source: "Next Generation Secure Web Gateway," A commissioned study by Forrester Consulting on behalf of McAfee

Consolidation In Content Security Is Preferred By Many

The content security industry, including email and Web filtering, is beginning to exhibit the trend of consolidation. For instance, instead of deploying individual point solutions for email and Web, many user organizations are now considering integrated or consolidated solutions, which offer integrated policy management, centralized reporting, and integrated threat analysis. Our survey respondents confirmed this trend — 85% of all respondents indicated that they would be more likely to employ an integrated content filtering solution that provides centralized policy management, configuration, and integrated DLP (see Figure 26).

Figure 26: Companies Prefer Consolidated Solutions

"How likely are you to employ a content filtering solution if it provides centralized policy management, configuration, and data leak protection (DLP) across email and web?"



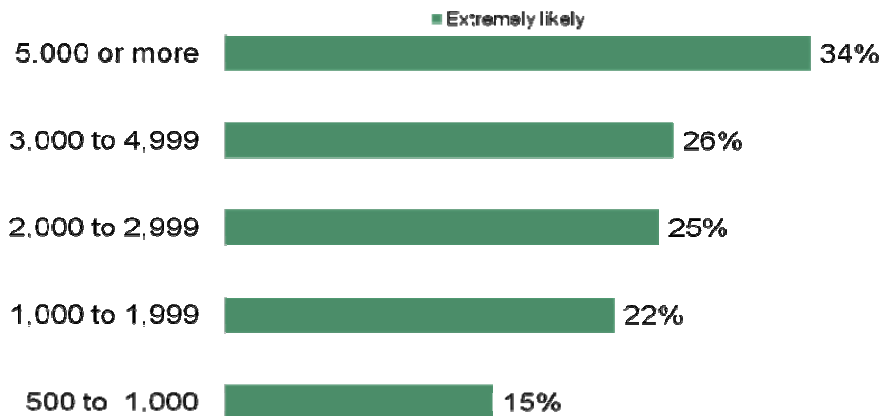
Base: 253 global IT decision makers

Source: "Next Generation Secure Web Gateway," A commissioned study by Forrester Consulting on behalf of McAfee

A more detailed analysis of the answers reveals that larger organizations are more likely to appreciate the benefits of a consolidated solution, including centralized policy management and integration with DLP (see Figure 27). Large organizations tend to have more mature policies and more sophisticated management needs; a consolidated platform would give the company the opportunity to enforce universal policies across different communication protocols, ease the job of reporting and trending by supplying a uniform report portal, and more importantly, the capability for cross-channel analysis and quicker identification of content-borne threats.

Figure 27: Companies That Replied "Extremely Likely" To The Consolidation Question

"How likely are you to employ a content filtering solution if it provides centralized policy management, configuration, and data leak protection (DLP) across email and web?" - Extremely likely



Base: 253 global IT decision makers

Source: "Next Generation Secure Web Gateway," A commissioned study by Forrester Consulting on behalf of McAfee

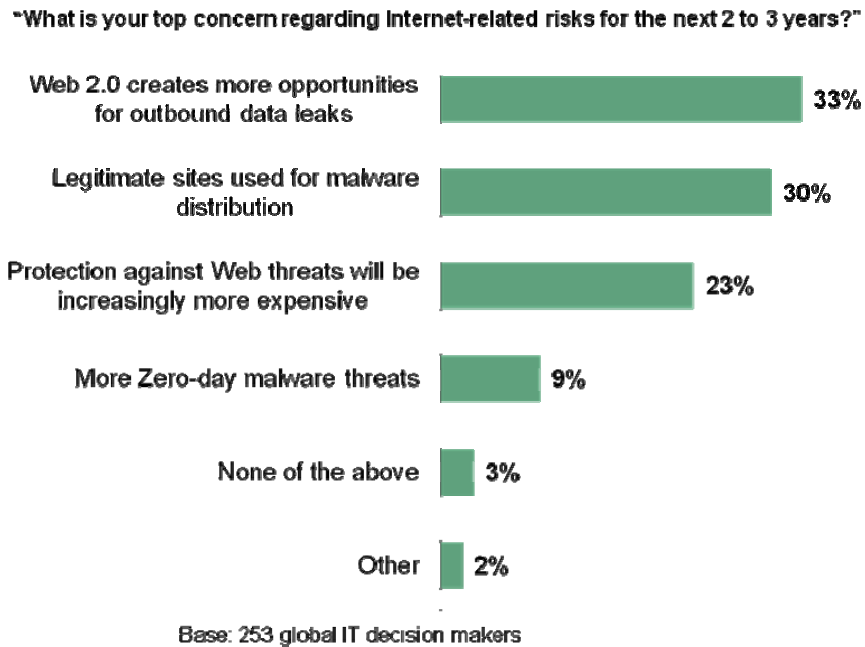
Users' View Of Emerging Internet Threats

We also asked the respondents to share their views of emerging Internet threats for the next two to three years. At the top of the list is Web 2.0 and increased risks for data theft, followed by legitimate sites used for malware distribution, and increased cost for Web protection (see Figure 28).

These data show users are fairly conscientious about Web 2.0 applications and its risks — 30% of companies view Web 2.0 a growing risk factor for outbound data leaks. Users are also aware of a newer trend of Web threats, which constitutes legitimate Web sites being used in malware distribution. This new trend is due to increased attacks on legitimate sites, which are then used as drones to disseminate malware to Web users. This phenomenon has rendered Web filtering based on URL only an ineffective and obsolete technology.

Our survey respondents also voiced concerns that, given these new trends, Web filtering will become increasingly more expensive — 23% believe the cost of Web filtering will increase.

Figure 28: Companies' Top Concern For Internet Risks For The Next Two To Three Years



Source: "Next Generation Secure Web Gateway," A commissioned study by Forrester Consulting on behalf of McAfee

Conclusions

This commissioned study surveyed 253 IT decision-makers in North American and European companies across SMBs and enterprises. The survey results point to a few significant trends, described as follows.

Web Filtering Is Not Just About Security; It Is A Business Initiative

As more and more Internet-related functions are bundled in the Web protocol, the role of Web filtering is changing from a security-centric function to a more business-related role. Companies are looking to Web filtering to perform QoS management of Web traffic, employee productivity control, SSO for in-the-cloud applications, and more fine-grained control over all types of Web content. Web filtering is no longer just about malware and security threats; it is squarely a business function and will remain so as long as Web communication is used for business purposes.

DLP Is Important But Not Practiced Universally

In this study as well as in other daily interactions with various user organizations, it is clear DLP is a top-of-mind concern for many organizations. Many companies have outfitted their email communications with some form of DLP capability. Web communication, however, remains a weak link. Despite the fact many companies in this survey consider data leaks an important business threat, only a small percentage is actually using DLP technologies in outbound Web communication.

Mobile Filtering Strategies Are Imminently Important

As our economy becomes increasingly global, mobile workers are increasingly common for many organizations. Our study reveals that many feel mobile filtering is an imminent requirement that should be fulfilled. However, traditional Web filtering techniques that sit on the gateway of the corporate network are cumbersome, to say the least, to extend to mobile filtering. SaaS and hybrid delivery models provide more promising architectures to accommodate mobile filtering. It is clear mobile filtering is a new requirement that Web filtering technologies must answer.

Users Should Look To Vendors With These Functionalities

Aside from understanding requirements, this study also revealed a number of deficiencies and flaws in the adoption and usage of Web filtering technologies: URL filtering is still the predominant technology; real-time content analysis is rarely practiced.

User organizations, in considering enhancements and next-generation Web filtering technologies, should look to vendors with these capabilities:

- **Specific Web malware detection.** Web malware is different from traditional virus. Many Web malware are script-based, and they can change rapidly and take on many different forms. Traditional signature-based scanning approach is less effective against Web malware. An effective strategy must include script analysis, code analysis, and even sandbox-based behavior analysis.
- **A solid in-the-cloud infrastructure.** Today's content security requires integrated analysis that spans Web, email, and even other protocols, including IM, P2P, and VoIP. A successful cross-protocol analysis relies on an in-the-cloud infrastructure that can look across traffic of different types and perform real-time or near-real-time analysis. Such an

infrastructure also provides a strong foundation for SaaS or a hybrid delivery model, which is likely to be more widely adopted in the near future.

- **Strong integration and consolidation strategy.** As indicated by our survey results, organizations — small and large — regard integration and consolidation an important content security strategy. Though many point solutions are still managed in separate silos today, the larger trend points to integration and consolidation. User organizations should consider vendors that have capabilities in multiple content protocols and have a strong integration strategy.
- **Fine-grained Web 2.0 application control.** Last but not the least, individual Web 2.0 application controls are emerging as an increasingly important function. To support this requirement, the vendor technology must have a way to differentiate Web 2.0 applications and provide flexible policy enforcement capabilities to perform usage, and also QoS management for these applications.

Appendix A: Methodology

To understand the challenges around security threats caused by Web 2.0 and live applications on the Web, Secure Computing commissioned Forrester Consulting to conduct an online survey with 253 respondents. Of these respondents:

- The companies were based in:
 - The US and Canada — 130 respondents.
 - Europe (including the UK, France, Germany, and Nordic countries) — 123 respondents.
- The respondents were IT decision-makers or influencers responsible for security issues.
- The companies had 500 or more Internet users.
- Forrester kept the names and the companies of interviewees confidential.
- Secure Computing was not identified as the sponsor.

Appendix B: Endnotes

¹ Further information on the acquisition of Secure Computing is available. Source: "McAfee, Inc. Completes Acquisition of Secure Computing," McAfee press release, November 18, 2008 (http://www.mcafee.com/us/about/press/corporate/2008/20081118_120000_j.html).

² In September 2007, Forrester Consulting conducted a commissioned study on behalf of Secure Computing. Forrester surveyed 153 IT and security professionals who are primary decision-makers about security technologies for their organizations. Their roles include director of IT, director of IT security, enterprise architect, information security officer, and network security architect. The organizations surveyed included enterprises with 1,000 employees or more. Fifty-seven percent of the respondents belong to organizations that have 5,000 or more employees.

³ According to the [latest statistics](#) from Netcraft, there are at least [185,167,897](#) live Web sites as of November 2008. Statistics are available at www.netcraft.com.