

STATE OF



**INTERNET
SECURITY**

Protecting the Network

TABLE OF CONTENTS

- Executive Summary 1**
- Introduction 3**
- Web Risks 4**
 - Overview 4
 - Exposing Company Data to Security Threats 7
 - Legal Liability and Regulatory Compliance 8
- Securing Web Access 9**
 - Overview 9
 - Employee Internet Use Policies 10
 - Technological Solutions 11
- Conclusion 15**
- About Webroot 16**
- About the Research 16**
- Appendix 17**
- Sources 19**

EXECUTIVE SUMMARY

Over time, many fundamental business activities – marketing, advertising, customer support, research – have become Web dependent. At the same time, the Web is now considered the number one delivery mechanism for malware. This poses a significant security challenge to companies around the world. Compounding that challenge is the advent of interactive Web technologies known as Web 2.0 (blogs, wikis, RSS feeds and similar elements that are woven together to form Web pages), which make it all the more challenging to differentiate legitimate content from those that pose a threat.



However, many businesses have not realized that the Web is the primary source of malware today and remain primarily focused on management of email-based threats. In fact, based on Webroot® research, over 70 percent of companies have email security in place, while email now accounts for only about 15 percent of incoming malware. Email threats and spam are still significant concerns, but on a relative basis, they present far less of a problem because the real threat is from Web activities. The vast majority of the threats, 85 percent, now come from Web sites; however, most companies do not have adequate Web security in place. Some companies even think they are protected because they have a URL filtering system, but URL filtering does not detect or stop malware; it only blocks access to inappropriate sites.

Industry research and data paint an alarming picture. Considering that 5 percent of heavily trafficked Web sites are harboring malware, 85 percent of malware now comes via the Web, and only 15 percent of companies are scanning for malware in inbound Web traffic – most companies are dangerously exposed to the serious threat of malware. Add to that the fact that almost 50 percent of companies do not block access to social networking sites (a hotbed for malware), that 45 percent of employees are spending 30-60 minutes a day on non-work related Web sites, and that almost half of businesses are not monitoring employee Web usage. IT departments are left struggling to clean up malware pouring through a gaping hole in their security strategy.

In May 2008, Webroot conducted a survey of 648 Web security decision makers for companies in Australia, Canada, the United Kingdom and the United States. The survey data indicates that businesses are gradually beginning to realize the threat posed by the Web – awareness is rising, but the urgency is still not fully understood. Highlights of the study include:

Web is the Number One Attack Vector

- Across the board, the Web was reported as a greater source of security threats than email:
 - more viruses and worms
 - more spyware
 - more security breaches that threatened legal compliance
 - more unintentional releases of private customer information
- One out of four Webroot survey respondents reported that in the past 12 months a Web-based threat:
 - compromised confidential company information
 - threatened sensitive online transactions
 - caused a Web server outage

The Web is now considered the number one delivery mechanism for malware.

Employee Actions Put Companies at Risk

- Three out of ten respondents reported that their companies' Web security was compromised in the past 12 months by employees:
 - using personal Web mail accounts
 - visiting social networking sites
 - downloading and viewing videos
- Over a third of respondents estimate that employees spend an hour or more per day on non-work related Web sites.

Regulations and Use Policies Are Not Enough

- Nearly half of companies surveyed are very or extremely concerned about data breaches and almost a third are concerned about the liability from inadvertently exposing employees to offensive Web content.
- One out of five respondents did not know which laws their company needs to comply with.
- The majority of companies surveyed have an employee Internet use policy, yet only 15 percent feel their company does the best job possible enforcing the policy.

INTRODUCTION

Just 20 years ago “the Web” as we think of it today did not exist. Ten years ago, the Online Computer Library Center researched the rapid growth of the Web and estimated that 2.6 million Web sites existed. Netcraft, based in the United Kingdom, runs a monthly Web server survey that found over 165 million Web sites in April 2008. With this exponential growth, the Web has become an intrinsic part of our business and personal lives. Companies around the world rely on the Web to market their products and services, communicate with investors, conduct research, advertise job openings and so many other actions fundamental to running a business.

The Importance of the Web for Performing Business Functions	
Business Function	Extremely or Very Important
Providing customer support	46.3%
Marketing your company	44.6%
Accessing Web-based applications (e.g., CRM, HR, project management, employee benefits)	44.0%
Processing sales transactions or orders	42.1%
Gathering competitive intelligence	35.6%
Conducting market research	33.1%

Source: Webroot Web Security Survey, May 2008 (N=648)

Additionally, with the advent of more interactive Web technologies, often referred to as Web 2.0 applications, site ownership is much more decentralized, making it significantly more challenging to evaluate and block risky content and code. With the introduction of blogs and wikis and similar collaborative programs, many sites are much larger than their static HTML predecessors. Sites such as Facebook, MySpace and YouTube are counted as one Web site, while they are actually a collection of thousands of individual sites. Aside from user interactive sites, even “just content” sites often rely on a collection of content sources to display a single Web page. For example, RSS feeds and mashups are commonly used to combine data from more than one source and display as a single Web page. These points were reinforced in a 2007 Gartner report which states: “Web 2.0 has created a fundamental shift of content creation from trusted sources to anonymous collaborations such as wikis, blogs and social networking sites, which are much more likely to be infiltrated and infected by hackers.”

These changes in the ways the Web works and the ways businesses use the Web have provided malware purveyors with many more opportunities to insert their programs onto Web sites and proliferate them to users around the world. Additionally, the more interactive nature of many Web 2.0 applications increases the risks of data leakage, as sites with blogs and wikis provide numerous new opportunities for employees to purposely or inadvertently share confidential information or intellectual property with external audiences.

This edition of the State of Internet Security concentrates on the issues associated with protecting the perimeter. In conjunction with the report, Webroot conducted an email survey of 648 Web security decision makers from companies in Australia, Canada, the United Kingdom and the United States. The findings of this study are interspersed throughout the report.

There are over
165 million Web
sites in the world.

- Netcraft, April 2008

Web 2.0 has
created a
fundamental
shift of content
creation from
trusted sources
to anonymous
collaborations
such as wikis,
blogs and social
networking sites,
which are much
more likely to
be infiltrated and
infected by hackers.

- Gartner, 2007

Web Risks

Overview

Given all of the people working, shopping and interacting via the Web, it has become an obvious target for an increasingly sophisticated economy of nefarious people seeking ways to exploit the newest technologies to steal from others for their own profit. A 2008 IDC study reports that five percent of the most heavily trafficked Web sites have some sort of threat associated with them. The latest target: Web 2.0. In a 2007 study, Gartner found that most social networking sites do not monitor content for the hosting of malware, and that about half of companies allow employees unlimited access to social networking sites.



Just as companies are becoming more savvy about the risks posed by email and stepping up protection against that threat vector, the risks posed by employee Web use are increasing. Based on Webroot research, Web-borne malware increased over 500 percent in 2007, and 85 percent of malware is now distributed through the Web. Yet, awareness about this trend is only slowly beginning to rise. Gartner reported in 2007 that less than 15 percent of organizations scan inbound Web traffic for the presence of malware.

Source of Security Problems Experienced in the Past 12 Months		
Security Problem Experienced	Via Web	Via Email
Viruses or Worms	41.9%	39.3%
Spyware (Trojan horse, key logger, system monitor or root kit)	41.9%	34.8%
Security breach that threatened compliance with regulatory requirements	18.2%	16.2%
Unintentional release of private customer information	16.2%	14.9%
Loss of intellectual property	14.6%	14.3%

Source: Webroot Web Security Survey, May 2008 (N=648)

According to IDC's "Worldwide Web Security 2007-2011 Forecast," the Web will be increasingly used as the threat vector of choice by hackers and cybercriminals, and compromises of popular Web sites will become more common. Furthermore, IDC predicts a growing number of Web 2.0 sites will be extremely vulnerable to compromises. "Threat Report: the Trends and Changing Landscape of Malware and Internet Threats" issued by Forrester Research in June 2008 found that:

"A troubling trend is that Web users are now increasingly more likely to encounter malware at legitimate Web sites. This is a new phenomenon; malware was previously only on questionable sites (e.g., adult or gambling sites)."

One challenge for companies needing to protect themselves in a Web 2.0 world is that many of their IT professionals may still be unfamiliar with what that term means, or unsure about whether or how Web 2.0 applications are being used. While close to half of the Webroot survey respondents report their companies use one or more Web 2.0 applications, almost a third do not know whether their company does or not.

The Internet and Internet applications will be the primary source of malware infections in enterprises in 2008 and beyond.

- Gartner, 2007

The Web is, without a doubt, the single greatest source of spyware infections.

- IDC, 2007

Does Your Company Use One or More Web 2.0 Applications?	
Yes	47.1%
Don't know	29.4%
No	23.5%

Source: Webroot Web Security Survey, May 2008 (N=648)

Web-based threats had a moderate or major impact at four out of ten companies. In the past twelve months, over a third of companies dealt with Web-based threats that:

- slowed the speed of the network
- necessitated additional IT resources to manage Web security
- reduced employee productivity
- increased help desk time to repair damaged computers
- negatively impacted Web server performance
- disrupted business activities

Web-based threats disrupted business activities at over a third of companies surveyed.



It is often the perception that larger companies have additional resources and do a better job mitigating these risks. Based on the survey data, this may be the case for companies with over 2,500 PCs, but companies with 25 to 2,499 PCs reported higher levels of impact from Web-based threats than the smallest companies surveyed with 10 to 24 PCs.

Moderate or Major Impact Caused by Web-Based Threats in the Past 12 Months					
Impact on the Business	Companies' Number of PCs				
	10-24 (N=161)	25-99 (N=128)	100-499 (N=170)	500-2,499 (N=90)	2,500+ (N=99)
Slowed the speed of the network	34.8%	49.2%	52.4%	51.1%	39.4%
Additional IT resources needed to manage Web security	29.2%	46.1%	43.5%	50.0%	41.4%
Reduced employee productivity	32.3%	43.8%	42.4%	46.7%	40.4%
Increased help desk time to repair damage to computers	24.8%	39.1%	47.6%	50.0%	32.3%
Negatively impacted Web server performance	20.5%	36.7%	38.8%	46.7%	39.4%
Disrupted business activities	24.2%	35.2%	41.2%	42.2%	34.3%
Compromised confidential information	19.3%	35.2%	28.8%	41.1%	31.3%
Threatened sensitive online transactions	17.4%	30.5%	31.8%	40.0%	30.3%
Caused a Web server outage	17.4%	33.6%	29.4%	36.7%	29.3%

Source: Webroot Web Security Survey, May 2008

A greater number of companies with 25 to 2,499 PCs were impacted by Web threats than smaller or larger companies.

Exposing Company Data to Security Threats

Exposing the company to Web-based threats can have serious implications. One out of four Webroot survey respondents reported that a Web-based threat compromised confidential company information, threatened sensitive online transactions or caused a Web server outage in the past 12 months. Increasingly sophisticated Web site attacks that exploit browser vulnerabilities can seriously threaten sensitive company data, not only for the companies operating the compromised sites, but for anyone who visits them. Often employees' actions while at work or using a work computer compromise a company's Web security.

Three out of ten respondents reported that their companies' Web security was compromised in the past 12 months by employees using personal Web mail accounts, visiting social networking sites and downloading and viewing videos.

Companies Reporting Security-Compromising Web Activities by Employees in the Past 12 Months	
Using personal Web mail accounts	34.5%
Visiting social networking sites	29.8%
Downloading and viewing videos	29.6%
Shopping online	26.7%
Accessing Peer-to-Peer networks	25.8%
Downloading music	25.3%
Blogging	22.7%
Making personal travel arrangements online	22.1%
Visiting pornography sites	21.8%
Visiting gambling sites	19.1%

Source: Webroot Web Security Survey, May 2008 (N=648)

Over a third of respondents estimate that employees spend an hour or more per day on non-work related Web sites.

Estimated Daily Employee Time Spent on Non-Work Related Web Sites	
0 minutes	2.5%
1-9 minutes	4.9%
10-29 minutes	25.8%
30-59 minutes	23.9%
1 hour	21.1%
2 hours	7.6%
3 hours or more	4.3%
Don't know	9.9%

Source: Webroot Web Security Survey, May 2008 (N=648)

Almost a third of companies reported a Web-based threat compromised confidential company information.

Over a third of respondents reported their companies' Web security was compromised by employees using personal Web mail accounts.

37 percent of confidential information leaks occurred via the Web.

- IDC, 2008

Legal Liability and Regulatory Compliance

Governments in many parts of the world have instituted additional data protection measures that require companies to adequately protect the sensitive customer data in their possession. Non-compliance can expose companies to fines, sanctions and damaged reputations. Furthermore, the damage to the customer relationship as a result of any sort of breach can have far-reaching impact. Nearly half of companies surveyed are very or extremely concerned about data breaches and almost a third are concerned about liability from inadvertently exposing employees to offensive Web content. Yet, one out of five respondents did not know with which laws their company needs to comply.

Information Security Compliance Issues	
Compliance issue	Very or Extremely Concerned
Breaches of customer data	47.1%
Breaches of company data	46.3%
Breaches of employee data	41.3%
Liability from employee exposure to offensive Web content	30.7%

Source: Webroot Web Security Survey, May 2008 (N=648)

One out of five respondents did not know with which laws their company needs to comply.

Regulations* with which Companies are Required to Comply	
Canadian Personal Information Protection and Electronic Documents Act (PIPEDA)	27.6%
U.S. Securities and Exchange Commission Rule 17	14.2%
Australian Federal Privacy Act	14.0%
U.S. Federal Rules of Civil Procedure	14.0%
Health Insurance Portability and Accountability Act (HIPAA)	11.1%
Payment Card Industry (PCI) Standard	10.8%
UK Data Protection Act	9.6%
Sarbanes-Oxley	8.8%
UK Companies Act	7.7%
Australian National Health Act	7.7%
EU Data Protection (Privacy) Directive	6.9%
UK Financial Services Act	6.3%
BASEL II Accord	3.9%
Gramm-Leach-Bliley	3.9%
Don't know	21.0%

Source: Webroot Web Security Survey, May 2008 (N=648)

In addition to compliance with data security laws, companies may be exposed to additional legal liabilities when they fail to secure Web access, as offensive Web-based content could support a hostile work environment claim.

* Information about these laws and regulations is included in the Appendix.

Securing Web Access

Overview

For many companies, a necessary business tool – the Web – also presents a serious business risk. Given the significant amount of spyware, viruses and other harmful malware propagated via Web browsing, the amount of time employees spend on the Web during work time and the business and legal implications associated with the potential compromise of company data, companies have an imperative to ensure Web access and interaction are secure.

Over three-fourths of survey respondents concur that Web-based threats are becoming increasingly sophisticated and malicious and that Web security requires a multi-layered approach. Yet, the constantly evolving nature of the threats presents a major challenge for IT departments. Over half of survey respondents feel that keeping Web security protection up-to-date is challenging, and 38 percent of survey respondents said their companies devote insufficient resources to Web security. In companies with fewer than 500 PCs, an even greater number of respondents feel insufficient resources are allocated to Web security.

Two things every company can do to better secure their access to the Web:

- Educate and monitor employees to minimize the risks they introduce to the company.
- Deploy and constantly maintain appropriate technological solutions.



Respondents that Agree or Strongly Agree with Each Statement	
Web-based threats are becoming increasingly sophisticated and malicious.	77.9%
Effective Web security requires a multi-layered approach.	76.4%
Mobile users who remotely connect to the corporate network are a greater security risk than users who connect locally.	61.4%
Keeping Web security protection up-to-date is challenging for my company.	56.2%
My company devotes insufficient resources to Web security.	38.0%

Source: Webroot Web Security Survey, May 2008 (N=648)

Response: "My Company Devotes Insufficient Resources to Web Security."				
By Number of PCs				
10-24 (N=161)	25-99 (N=128)	100-499 (N=170)	500-2,499 (N=90)	2,500+ (N=99)
42.2%	44.0%	41.4%	30.7%	24.2%

Source: Webroot Web Security Survey, May 2008 (N=648)

Over half of respondents feel keeping Web security protection up-to-date is challenging.

38 percent of respondents said their companies devote insufficient resources to Web security.

Employee Internet Use Policies

The majority of companies surveyed have an employee Internet use policy. Companies with 100 or more PCs are more likely to have an employee Internet use policy than companies with fewer PCs. Companies with 100 or more PCs are also more likely to monitor or audit how much time employees spend on Web sites than smaller companies, but less than half of all companies surveyed monitor or audit employee Web use. Small companies may be at particular risk, as over 40 percent do not have an employee use policy and the majority (70 percent) do not monitor or audit employee Web time.

Companies with an Employee Use Policy						
Response	Total (N=648)	Companies' Number of PCs				
		10-24 (N=161)	25-99 (N=128)	100-499 (N=170)	500-2,499 (N=90)	2,500+ (N=99)
Yes	72.8%	52.2%	67.2%	83.5%	85.6%	83.8%
No	21.5%	44.7%	24.2%	12.9%	6.7%	8.1%
Don't know	5.7%	3.1%	8.6%	3.5%	7.8%	8.1%

Source: Webroot Web Security Survey, May 2008 (N=648)

Only 15 percent of respondents gave their company an "A" for enforcement of their Internet use policy.

Companies That Monitor or Audit Employee Web Time						
Response	Total (N=648)	Companies' Number of PCs				
		10-24 (N=161)	25-99 (N=128)	100-499 (N=170)	500-2,499 (N=90)	2,500+ (N=99)
Yes	45.1%	70.2%	48.4%	39.4%	34.4%	19.2%
No	44.3%	23.6%	39.1%	55.9%	52.2%	57.6%
Don't know	10.6%	6.2%	12.5%	4.7%	13.3%	23.2%

Source: Webroot Web Security Survey, May 2008 (N=648)

While having these types of policies in place is an important step to mitigating the risks employees' Web browsing presents to the company, enforcing these policies is the key to their effectiveness. Only 15 percent of survey respondents gave their company's enforcement of their Internet use policy an "A." Effective technical solutions are essential to help enforce policies and provide a more stringent layer of protection.

Response: "What Grade Would You Give Your Company for Enforcement of its Employee Internet Use Policy?"					
A	B	C	D	F	Don't Know
15.0%	43.2%	28.8%	5.3%	3.4%	4.2%

Source: Webroot Web Security Survey, May 2008 (N=648)

Making policy enforcement ever more challenging is the large number of employees who work on laptops via remote access, increasing the risk of malware-infected laptops being brought back into the office and compromising the company network. These factors demonstrate that it is most important that companies employ best-in-class technical solutions to effectively protect business Web access.

Technological Solutions

Eighty percent of respondents report they currently filter inbound Web pages for malware and over 70 percent filter URLs for inappropriate Web sites; however, only 55 percent use a data leakage prevention solution at the gateway. Companies with 100 or more PCs are more likely than smaller companies to filter URLs and deploy data leakage prevention solutions.

Type of Web Security Deployed						
Response	Total (N=648)	Companies' Number of PCs				
		10-24 (N=161)	25-99 (N=128)	100-499 (N=170)	500-2,499 (N=90)	2,500+ (N=99)
Filter inbound Web pages for spyware and viruses	80.1%	80.7%	73.4%	84.7%	77.8%	81.8%
Filter URLs for inappropriate Web sites to prevent employee misuse of assets	71.9%	50.9%	65.6%	83.5%	81.1%	85.9%
Data leakage prevention solution at the gateway to block outgoing confidential information	54.9%	36.6%	53.9%	68.8%	55.6%	61.6%

Source: Webroot Web Security Survey, May 2008 (N=648)

The most commonly filtered sites are those that contain adult and sexually explicit content, gambling, dating and personals, chat rooms and violent/hate content. Among companies that deployed a data leakage prevention solution, the most commonly filtered sites are ones that provide chat rooms, email, file uploads and instant messaging.

URL Categories Filtered	
Adult & sexually explicit	88.2%
Gambling	76.6%
Dating and personals	67.4%
Chat rooms	65.9%
Violence and hate	65.0%
Games	53.6%
Social networking	50.4%
Advertisements	41.2%
Blogs	39.9%
Shopping	28.8%
Video	26.8%
Forums	24.2%
Toolbars	23.2%
Web-based email	23.2%
Sports	18.9%
Audio	17.4%
Travel (personal)	17.0%
Jobs	14.6%
Don't know	3.4%
None of the above	1.1%

Source: Webroot Web Security Survey, May 2008 (N=519)

Filters Used in Data Loss Prevention	
Chat Rooms	58.4%
Email	57.0%
Files uploaded to the Web	55.6%
Instant Messages (IM)	55.1%
Peer-to-Peer sharing	53.1%
Blogs	48.3%
FTP	43.0%
Web postings	41.6%
Telnet	33.1%
None of the above	1.4%
Other	0.2%

Source: Webroot Web Security Survey, May 2008 (N=466)

Only 55 percent of respondents use a data leakage prevention solution at the gateway.

While generic filtering approaches were relatively effective in a more static Web world, in the Web 2.0 world more sophisticated solutions are needed to provide:

- Filtering of inbound Web pages for spyware and viruses
- URL filtering of inappropriate Web sites to prevent employee misuse of assets
- Data leakage prevention at the gateway to block outgoing confidential information
- Granularity in access and policy management
- Immediate updates to respond to ever changing threats

An important trend in security software is Software as a Service (SaaS) solutions where customers do not need to buy, install and maintain software, but rather pay a subscription to a service.

The Webroot survey respondents were asked to rank the reasons their company adopted or would adopt a Web Security Software as a Service solution. Improving effectiveness against viruses, spyware and phishing attacks was the number one reason.

Reasons Companies Adopt or Would Adopt Web Security Software as a Service Ranked by Order	
1.	Improve effectiveness against viruses, spyware and phishing attacks
2.	Simplify the management of Web security
3.	Block inappropriate Web sites
4.	Protect mobile/remote users
5.	Reduce costs and burden on staff
6.	Reclaim bandwidth and improve network performance
7.	Set and maintain Internet use policies for compliance purposes
8.	Reduce total cost of ownership to my company
9.	Set company-wide user policies
10.	Flexibility in adding or deleting online security for new or departing employees
<i>Source: Webroot Web Security Survey, May 2008 (N=434)</i>	

For companies that want enterprise-class security but do not have the resources to build or manage a complex security solution, a SaaS-based alternative to traditional hardware and software security provides a better total cost of ownership (TCO). Web Security SaaS is designed to protect corporate and mobile users against Web-based virus, spyware and phishing attacks as well as enforce company Internet use and access control policies. Companies that use a perimeter SaaS solution are able to leverage the expertise of a dedicated security vendor focused on providing innovative solutions that are easy to manage, offer high levels of protection against Web-based threats, and minimize the time required by internal IT staff to manage a complex security environment.

In the Web 2.0 world, more sophisticated solutions are needed.

SaaS customers do not need to buy, install nor maintain software.

SaaS vs. Software vs. Appliances			
Issue	SaaS	Software	Appliance
Are additional purchases required?	No	Yes (Hardware and installation/configuration services)	Yes (Possibly a second device for backup)
Fast, easy implementation	Yes	No	No
Are customers protected from a single point of failure?	Yes	No	No
Are guarantees of accuracy and availability provided?	Yes	No	No
Will bandwidth improve as a result of usage?	Yes	No	No
Is unlimited spam storage space included?	Yes	No	No
Can the system cope with major increases of traffic?	Yes	No	No
Is it maintained, updated and supported?	Yes	No	No
Can the system protect against Denial of Service attacks?	Yes	No	Yes (limited)
Can the system protect against Directory Harvest attacks?	Yes	No	Yes (limited)
Will the system cope with new threats in real time?	Yes	No	No

As the Web has become the leading source for malware and data leakage, companies need to have in place a flexible, scalable Web security solution that provides an additional in-the-cloud layer of protection for corporate and mobile users. In addition, the right technical solution will help a company enforce its internal Internet use policies and protect against accidental data leakage. Key features and functions include:

- Access Control
- Flexible Policy Management
- Mobile User Protection
- Proactive Threat Protection
- URL Filtering

Access Control

Ensuring users only get access to the content they need not only protects them from potentially offensive material, but also protects organizations from vast amounts of wasted hours spent browsing the Internet for personal use. Access policies can be set at the individual user level and applied by time, date and location.

The right technical solution will help a company enforce its internal Internet use policies and protect against accidental data leakage.

Flexible Policy Management

A customizable rules engine to facilitate the creation of user, group and account level policies to enable internal Web content and Web threat management are most important to effectively managing a Web security solution. Robust and flexible policy management provides companies with the tools needed to enforce company Web use policies.

Mobile User Protection

Companies need to provide seamless and uninterrupted protection for mobile laptop users while they are outside the corporate network, without any additional hardware or server-based software. Mobile users can authenticate directly with the service without having to establish a VPN connection back to the corporate network. This provides seamless protection against viruses, spyware and phishing while also enforcing company Internet Use policies regardless of where an employee works – at home, airports, Internet cafes or hotels.

Proactive Threat Protection

With HTTP and FTP over HTTP traffic being scanned for virus and spyware attacks at the Internet layer, companies are able to eliminate Web-based threats before they reach the network gateway. Plus, large file downloads and bandwidth intensive Web applications, such as music and video files, can be prevented globally or by user. This protection reduces the burden on IT systems, increases available bandwidth and improves network security company-wide.

URL Filtering

To protect themselves from the risks associated with open Internet access, companies need to rely upon a best-of-breed URL filtering engine that categorizes millions of URLs, enabling organizations to effectively manage employee Internet access and use policies. Organizations can now help increase employee productivity, improve Web security for all users, reduce legal liability and save bandwidth costs.

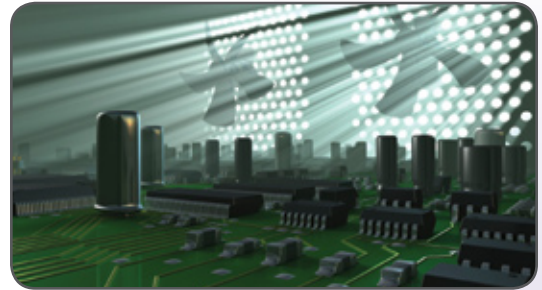
In addition to these features, a leading Web Security SaaS solution helps place a greater distance between the “bad stuff” and the company servers. A SaaS service model also lessens the burden on company resources, eliminates the need for managing constant software updates and significantly lowers the IT time required to maintain a comprehensive Web security solution.

Companies need seamless and uninterrupted protection for mobile laptop users.

A leading Web Security SaaS solution helps place a greater distance between “bad stuff” and the company servers.

Conclusion

Spyware, viruses and other malware transported via Web sites represent the most serious data security threat to companies today. Companies need to proactively leverage technology and appropriate business policies to protect themselves, their customers and their employees from the threats presented via the Web. A robust perimeter SaaS solution, layered with best-in-class desktop protection, is the best combination to effectively protect business Web access.



Web sites represent the most serious data security threat to companies today.

ABOUT WEBROOT

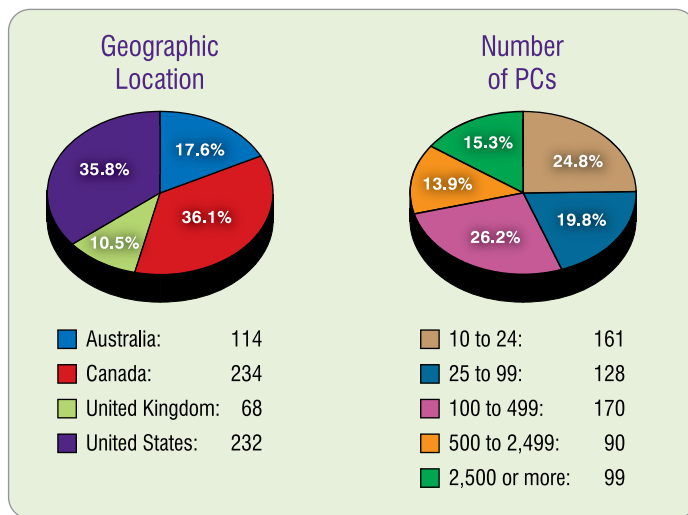
Webroot provides industry-leading security software and services to consumers, enterprises and small to medium-sized businesses worldwide. The Boulder, Colorado based company's newest software-as-a-service (SaaS) offerings, Webroot Web Security SaaS and Webroot E-Mail Security SaaS, provide better manageability, better value and better protection than any other Web or e-mail security solutions. Webroot's award-winning endpoint products, Webroot Antispyware Corporate Edition and Webroot Antispyware Corporate Edition with Antivirus, are comprehensive, centrally managed solutions that aggressively block, detect and eradicate malware on desktops across the network.



To find out more visit www.webroot.com or call 800.772.9383.

About the Research

In May 2008, Webroot sponsored online surveys of companies with 10 or more PCs or laptops in Australia, Canada, the United Kingdom and the United States. Survey Sampling International invited panel members who are Web security decision makers. With a total of 648 respondents, the margin of error is plus or minus four percentage points.



© 2008 All rights reserved. Webroot Software, Inc. Webroot, the Webroot icon and the Webroot tagline are trademarks or registered trademarks of Webroot Software, Inc. in the United States and/or other countries. All other trademarks are properties of their respective owners.

NO WARRANTY. Analysis based on research conducted by Webroot Software, Inc. The information is provided AS-IS. Webroot makes no warranty as to its accuracy or use, and nothing contained in this document constitutes legal advice. Any use of the technical documentation or the information contained herein is at your own risk. Documentation may include technical or other inaccuracies or typographical errors. Webroot reserves the right to make changes without prior notice.

Certain data is available upon request.

APPENDIX

Information about laws listed on page 8

Australian Federal Privacy Act of 1988

The Australian Privacy Act of 1988 is the country's federal privacy law setting guidelines for how business, government, individuals and health organizations handle information.

<http://www.privacy.gov.au>

Australian National Health Act of 1953

Under the auspices of the National Health Act of 1953, the Medicare and Pharmaceutical Benefits Program Privacy Guidelines were issued in 1997 that provide rules for the collection, use, disclosure and retention of personal medical information.

http://www.austlii.edu.au/au/legis/cth/consol_act/nha1953147/

BASEL II Accord

Basel II is a European-developed standard for the way financial institutions ensure the privacy of financial information when it is transferred across international borders. It also encourages financial institutions to lower operational risks by requiring a lower capital allocation when strong risk management policies are in place. As part of the risk mitigation plan, financial institutions must ensure that data and communication is secure, accessible and accurate.

<http://www.bis.org/publ/bcbsca.htm>

Canadian Personal Information Protection and Electronic Documents Act (PIPEDA)

PIPEDA protects personal data during commercial transactions, not just inside Canada but internationally. It also directs how information can be gathered and how it should be stored.

http://www.privcom.gc.ca/legislation/02_06_01_e.asp

EU Data Protection Directive

Often referred to as the EU Privacy Directive, the Data Protection Directive is one of the most well known legal standards requiring companies to protect sensitive information in their possession. Article 17 of the Directive requires: *Member States shall provide that the (data) controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction, alteration, unauthorized disclosure or access, in particular where processing involves the transmission of data over a network.*

http://ec.europa.eu/justice_home/fsj/privacy

Gramm-Leach-Bliley Act (GLBA) – U.S.

GLBA requires that companies which maintain credit information for customers be held accountable if that data is accessed or compromised by an unauthorized third party. Incidents of unauthorized network access and spyware, such as system monitors or Trojans, can raise concerns about noncompliance. It also governs the handling of nonpublic personal information about consumers..

<http://www.ftc.gov/privacy/glbact/glbsub1.htm>

Health Insurance Portability Act (HIPAA) - U.S.

HIPAA requires that the privacy of medical records be adequately protected against unauthorized access and misuse. It applies to all paper and electronic records that contain information relevant to an individual's medical history. Specific retention requirements vary from five years to the life of the patient.

<http://www.cms.hhs.gov/HIPAAGenInfo/Downloads/HIPAAALaw.pdf>

Payment Card Industry (PCI) Standard

The PCI standard for data security includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures including:

- Build and maintain a secure network
- Protect cardholder data
- Maintain a vulnerability management program
- Implement strong access control measures
- Regularly monitor and test networks
- Maintain an information security policy

The PCI standard provides details about how to best fulfill each of these objectives. Specific elements of the standard, such as ensuring that antivirus programs can protect against other forms of malicious code such as spyware and adware, offers important guidance for all companies, even those that do not accept credit cards as a form of payment.

<https://www.pcisecuritystandards.org/>

Sarbanes-Oxley Act of 2002 (SOX) – U.S.

SOX compliance has become a central focus of corporate governance initiatives. SOX requires that all publicly-traded companies include specified risk assessment and audit controls that cover such areas as data security policies.

<http://www.sec.gov/about/laws/soa2002.pdf>

UK Companies Act

The UK Companies Act states the accounting records and other paperwork requirements to demonstrate accuracy in company transactions. As records are increasingly created in electronic form, and email often constitute the business record of a transaction, retention policies must be fulfilled.

http://www.opsi.gov.uk/acts/acts2006/ukpga_20060046_en_1

UK Data Protection Act of 1998

The Act sets out the guidelines for obtaining, holding, using or disclosing personal information. It specifies the storage, retention and destruction of electronic personal information and security pertaining to the transfer of personal data.

http://www.opsi.gov.uk/acts/acts1998/ukpga_19980029_en_1

UK Financial Services Act

Administered by the Financial Services Authority (FSA), the Act sets guidelines for storing, retrieving, or deleting electronic files, including email, Web pages and other e-documents.

http://www.uk-legislation.hmso.gov.uk/acts/acts2000/ukpga_20000008_en_1

U.S. Federal Rules of Civil Procedure (FRCP)

FRCP amendments detailing electronic discovery requirements and obligations to preserve and produce electronically-stored information were implemented in 2006.

<http://judiciary.house.gov/media/pdfs/printers/110th/civil2007.pdf>

U.S. Securities and Exchange Commission (SEC) Rule 17

SEC Rule 17 includes requirements for broker-dealers organizations to retain all emails pertaining to trading activity for six years, and that these emails are preserved in a way that maintains access to them.

<http://www.sec.gov/rules/final/34-44992.htm>

SOURCES

Industry Analyst Reports

The Growing Web Threat

Peter Firstbrook
Gartner, Inc.
April 2007

Pros and Cons of SaaS Secure Web Gateway Solutions

Peter Firstbrook
Gartner, Inc.
April 2007

Social-Networking Sites Present Real Business Risks and Benefits

Peter Firstbrook
Gartner, Inc.
March 2008

Threat Report: The Trends and Changing Landscape of Malware and Internet Threats

Chenxi Wang, PhD
Forrester Research, Inc.
June 2008

Web Security SaaS: The Next Generation of Web Security

Christian A. Christiansen, Brian E. Burke, Gerry Pintal
IDC
April 2008

Worldwide Web Security 2007–2011 Forecast

Brian Burke
IDC
April 2007

News Stories

“As Their Dependence on Email Grows, Some Firms Find Ever-Bigger Problems”

Herald Tribune
August 30, 2001

“‘Best in Class’ Firms Show Value of Security”

Bank Technology News
February 2008

“Data Security and Tort Liability”

Journal of Internet Law
January 2008

“Malicious Programs Hit New High”

BBC News
February 8, 2008

Digital Fear: The Internet as a Tool for Crime and Terrorism

Business Roundtable
Washington, D.C.
September 2007

“Most Malware is Launched from Legit Web Sites”

ComputerWorld
January 28, 2009

“Security Dominates IT Agenda in 2008”

NetworkWorld
January 7, 2008

“Threat Level: Elevated”

Telecom Asia
March 2008

“Web 2.0 Sites a Thriving Market for Malware”

PC World
July 2008



The Best Security
in an Unsecured World™

Webroot Software, Inc.
P.O. Box 19816
Boulder, CO 80308-2816
USA
www.webroot.com
Phone: 800.772.9383
Fax: 303.442.3846
Business Sales & Support: 800.870.8102