

## WHITE PAPER

---

### Web Security SaaS: The Next Generation of Web Security

---

Sponsored by: Webroot Software

---

Christian A. Christiansen      Brian E. Burke  
Gerry Pintel  
April 2008

### IDC OPINION

The demand for more comprehensive Web security solutions has been fueled by the increasing sophistication of Web-based threats that reach far beyond productivity, bandwidth, and liability issues. The Web has become the new threat vector of choice for hackers and cybercriminals to distribute malware and perpetrate identity theft, financial fraud, and corporate espionage. As most organizations are now reasonably protected against traditional email-borne malware, the Web has become the latest target for hackers to launch various types of malware attacks. As a growing number of Web 2.0 applications make their way into the enterprise, they bring with them even more security concerns and attack vectors. A recent IDC study found that two-thirds of organizations are currently using at least one Web 2.0 application (source: *Web 2.0 Applications Are Already in the Enterprise: Key Findings from IDC's AppStats Survey*, IDC #208944, October 2007).

Organizations of all sizes would agree that effective security requires a multilayered defense. However, the resources required to manage multiple security products can often overwhelm an IT department in the small and medium-sized business (SMB) environment. Many SMB organizations lack the in-house capabilities to keep up with the evolving threat landscape. These factors are driving the growing interest in software as a service (SaaS) security. The adoption of SaaS in the messaging security market has grown explosively over the past few years. IDC believes many SMB organizations will leverage the same SaaS benefits to address their Web security needs as well. In fact, a recent IDC survey found that Web security SaaS has the highest planned adoption rate (approximately 14%) over the next 18 months in business environments with 100–999 employees.

This paper describes the next generation of Web security. It outlines solutions that focus on increasing overall security effectiveness and reducing the burden on IT departments. It describes the challenges facing many SMB environments today and identifies critical elements that make for lower-cost and easier-to-manage Web security solutions. The paper highlights Webroot's SaaS security offering with a focus on Web security.

## METHODOLOGY

IDC has developed this white paper using a combination of existing market research, our existing knowledge base, and primary research in the cost-effective deployment of Web security systems. This primary research includes the results of meetings and briefings with Webroot staff in order to gain an in-depth understanding of Webroot's Web and email security software services.

Using this body of knowledge, we describe the overall business and technical challenges that SMBs face in dealing with Web security issues and provide guidance on the types of solutions that play a key role in addressing today's complex threat environment.

## SITUATION OVERVIEW

### Web Threat Environment

A growing number of malicious codes are exploiting weaknesses in protocols (e.g., HTTP, POP3, FTP, and HTTPS) and Internet browsers, and infected Web pages are becoming a more prominent way to exploit a site visitor's computer remotely without the visitor even having to physically click on any links or email attachments. The number of Web sites distributing malware has increased explosively as malware creators continue to extend their distribution channels. As a result, Web security is becoming a growing concern for organizations. IDC believes that Web-based attacks will continue to become more malicious and sophisticated. Web security solutions will therefore play an increasingly important role in ensuring security.

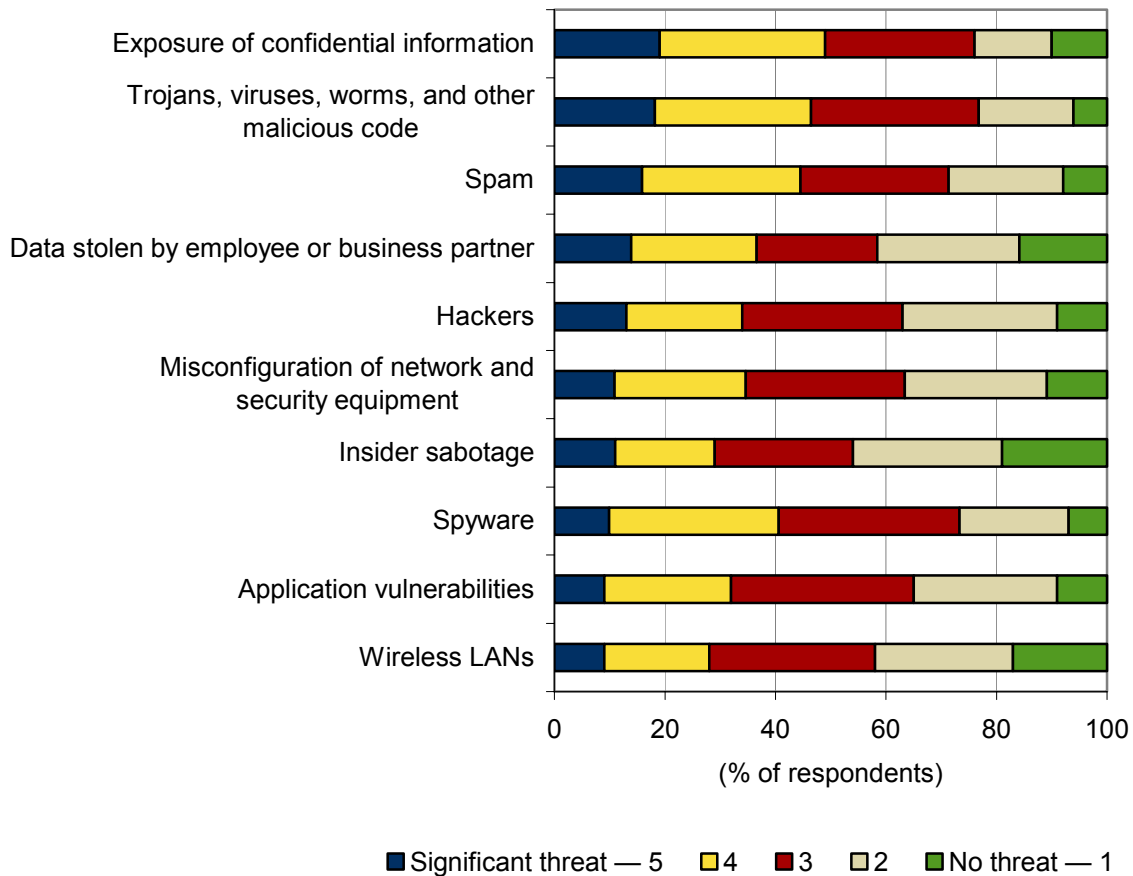
In IDC's 2007 annual security survey of IT and security professionals, participants were asked to rate the top threats to their companies' network security. Figure 1 displays the top 10 threats in 2007. IDC believes many of these threats are directly related to the Web, as follows:

- ☒ The exposure of confidential information is now the single greatest threat to enterprise security. Another recent IDC survey on information protection and control (IPC) showed that Web email or Web posting (e.g., message board, blog) accounted for 37% of information leaks. We also found that almost 70% of all organizations view Web 2.0 as a serious concern for data loss prevention (DLP). Government and industry regulations, such as HIPAA, Sarbanes-Oxley, Gramm-Leach-Bliley, and various SEC regulations are forcing corporations to secure the use of all electronic forms of communications, including the Web.
- ☒ Trojans, viruses, worms, and other types of malicious code ranked as the second greatest threat to enterprise security. Virus writers and hackers are increasingly leveraging the popularity of Web 2.0 sites in order to target the greatest number of users. The practice of hackers planting malicious code on legitimate Web sites is quickly becoming the norm. Hackers and malware developers are aggressively innovating ways to compromise popular Web 2.0 sites and others to install malicious code designed to steal personal and/or business confidential information.

- ☒ Spam has risen back up the list to number 3 on the top threats to enterprise security. The pure volume of spam continues to rise at a rapid pace, and malicious attacks are becoming more sophisticated (e.g., blended threats that combine spam, spyware, viruses, and other malware in their attacks). Spammers are increasingly using spam to lure users to malicious Web sites. One of the latest trends in Web-based threats is the use of encryption to hide malicious code and evade detection.
- ☒ Spyware continues to be both a security management nightmare and a system management nightmare. Theft of confidential information, loss of productivity, consumption of large amounts of bandwidth, corruption of desktops, and a spike in the number of help desk calls related to spyware are overwhelming many IT departments. Spyware has continued to evolve from a mischievous hobby to a moneymaking criminal venture that has attracted a new breed of sophisticated hackers and organized crime. The Web is without a doubt the single greatest source of spyware infections, a claim supported by Webroot internal data that suggests 85% of all spyware and virus infections are delivered via the Web.

**FIGURE 1**

Top 10 Threats to Enterprise Security



Source: IDC, 2008

## FUTURE OUTLOOK

### SaaS to the Rescue?

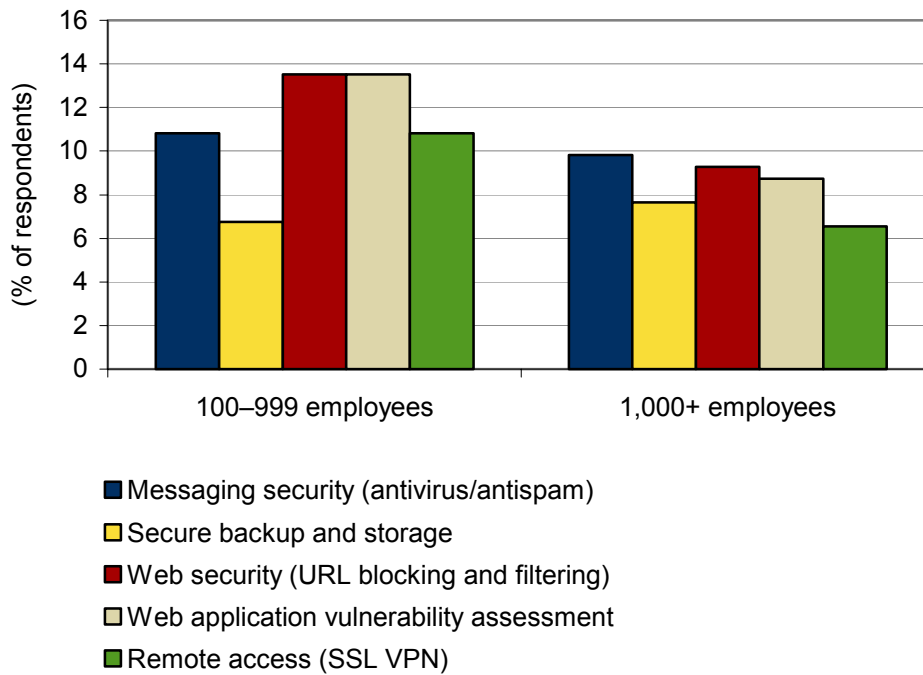
As network and application vulnerabilities continue to grow in the presence of an increasingly aggressive and sophisticated mix of attack vectors, companies continue to struggle with balancing the survival needs of their businesses and investing in security technologies and hiring uniquely qualified staff to maintain them. Many companies, especially in the SMB segment, lack the in-house capabilities to keep up with the changing security landscape and challenges. For these companies, a SaaS approach to securing their businesses is fast becoming an attractive alternative.

To date, most of the security investment in SaaS has been in the messaging security market. However, according to our latest survey results, that's about to change. Our survey found that Web security has the highest planned adoption rate (approximately 14%) over the next 18 months in business environments with 100–999 employees (see Figure 2). It's also becoming a very interesting area of investment in the large enterprise environment (1,000+ employees).

**FIGURE 2**

#### Top 5 SaaS Security Opportunities by Company Size

Q. For which, if any, of the following security solutions is your company likely to employ a SaaS model over the next 18 months?



Source: IDC, 2008

### ***SaaS Will Help Ease the Pain***

Many IT departments continue to experience budgetary pressures with regard to proper staffing levels while simultaneously being asked to provide higher levels of network accessibility, business continuity, and a higher degree of security. IT departments are tasked with the challenging role of ensuring business continuity even as they are being asked to secure a rapidly increasing pool of protocols (e.g., Web, email, instant messaging) with constrained administration staff sizes. The cost associated with training the IT staff on multiple security consoles can be a burden for corporate IT budgets and staff. This is especially true in the SMB environment. IDC believes there are many business and technical benefits for SMBs to consider SaaS as part of their security infrastructure.

The business benefits of a SaaS security approach include:

- Fixed annual service fees for Web security
- Simplified and predictable annual budgeting for security
- Reduced administrative workload for security
- No need for additional purchase of hardware
- No need for software license acquisitions
- No implementation costs

The technical benefits of a SaaS security model include:

- Web filtering of traffic that occurs "in the cloud" so that dangerous and unwanted traffic never reaches the business' infrastructure
- Maximized network bandwidth that is achieved as a result of the out-of-band elimination of unwanted and dangerous traffic
- Centralized and granular security policy management and enforcement
- HTTP and FTP traffic scanning and filtering
- Up-to-date signature- and heuristic-based virus and spyware scanning technologies are applied
- URL blocking to manage user browsing
- Centralized alerts and reporting
- Consistent protection for roaming PCs

IDC believes businesses will continue to seek operational cost-cutting measures. SaaS will play a key role in reducing administrative and support costs and, ultimately, in reducing the total cost of ownership (TCO) of managing multiple security technologies. The bottom line from a business perspective and an IT perspective is reducing the cost of managing the perimeter security side of the IT infrastructure. We believe corporations will look for SaaS security solutions that can address both cost and security concerns to an equal degree.

### **Hybrid Security: Foes Become Friends**

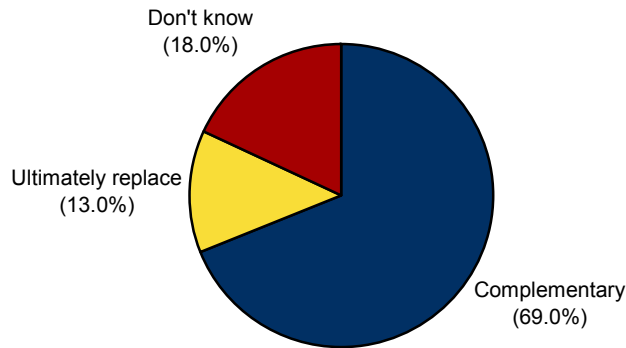
Hybrid has become the latest buzzword in the information security market, especially in regard to messaging and Web security. In the past, hosted Web and messaging security services competed directly with their on-premise counterparts. In almost all cases, it was a choice of one or the other. Today, many organizations are embracing a hybrid approach to Web and messaging security that leverages the benefits of an in-the-cloud SaaS offering with on-premise software and/or appliance-based solutions. IDC believes this layered architecture provides a higher degree of security and addresses more security requirements compared with a single deployment model. We expect hybrid security solutions to integrate multiple technologies through a centralized management console. This will give organizations a single point of management to enforce security policies.

Almost 7 out of 10 respondents (69%) feel that SaaS solutions are complementary to existing security solutions, whereas 13% say they will ultimately replace existing solutions (see Figure 3).

**FIGURE 3**

#### SaaS: Complementary or Replacement?

Q. *Do you believe software as a service (SaaS) solutions are complementary to existing security product solutions, or will they ultimately replace existing security product solutions?*



Source: IDC, 2008

## Convergence of Web and Messaging Security

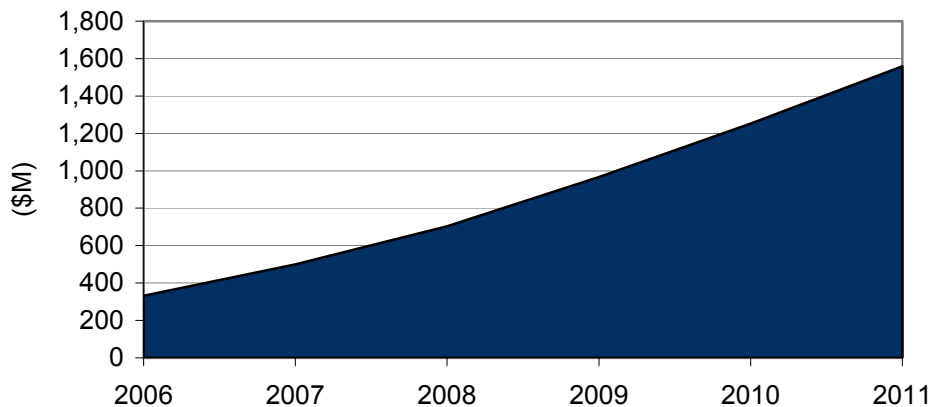
### **WAM**

Because of the blended nature of today's more sophisticated threats, the need for security vendors to address both Web and messaging (WAM) protocols is becoming more critical. IT departments are constantly under pressure to stay ahead of financially motivated cybercriminals launching sophisticated attacks (e.g., blended threats that combine spam, spyware, viruses, malicious URLs, and other malware in their attacks). The ever-changing threat landscape ensures the need for continued investments in security technologies that can address the blended threat environment. IDC believes SaaS represents a great opportunity to deliver multitier protection against blended threats that combine the use of the Web and email as attack vectors. We predict that many organizations, especially SMB environments, will look for solutions that can address both Web and messaging threats.

IDC research has shown that SaaS spending for Web and messaging security reached \$331 million in 2006 (see Figure 4). The market is expected to continue increasing at a compound annual growth rate (CAGR) of 36% through 2011 and reach almost \$1.6 billion. As SMBs and other businesses continue to look for more cost-effective means of monitoring, protecting, and managing their security infrastructures, SaaS offerings will continue to be an attractive option.

**FIGURE 4**

### Web and Messaging SaaS Forecast



Source: IDC, 2008

## WEBROOT OVERVIEW

---

### **Perimeter Security SaaS Solutions from Webroot**

For companies that want enterprise-class security but do not have the resources to build or manage a complex security solution, Webroot provides a SaaS-based alternative to traditional hardware and software security products at a better TCO.

Webroot Perimeter Security SaaS solutions include Webroot Email Security SaaS, designed to reduce the management headaches of maintaining an on-premise email security solution while providing protection against spam, viruses, distributed denial of service (DDOS), and other network-based attacks, and Webroot Web Security SaaS, 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 Webroot Perimeter Security SaaS solutions 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 email and Web-based threats, and minimize the time required by internal IT staff to manage a complex security environment. All Webroot solutions are also backed by a global team of highly trained security specialists to help ensure business continuity and uptime.

#### ***Webroot Web Security SaaS***

As the Web has become one of the more dangerous threat vectors used to distribute malware, Webroot has introduced a flexible and scalable Web security SaaS solution that provides an additional in-the-cloud layer of protection for corporate and mobile users. Webroot Web Security SaaS not only protects users from Web-based threats but also helps a company enforce its internal Internet usage policies and protect against accidental data leakage. The following sections describe the features of the Webroot solution.

#### **Management**

The ability to centrally monitor, manage, and report on individual and group Web-based activities is a core component of the Webroot Web Security SaaS solution. A Web-based management console allows IT administrators to manage policies at a granular level extending down to the individual user. Detailed reports on Internet and Web application use allow organizations to better understand Internet usage trends and employee productivity.

The Webroot management console also provides a dashboard that offers real-time visibility into Web access by URL category, blocked sites, and blocked viruses over a predefined time period. Additional reports providing more granularity into individual and group activities are also available in real time through the reporting interface.

The Webroot service also provides easy integration into a company's existing network infrastructure. Technologies such as LDAP can be used to synchronize user details into the management console for subsequent application of user-based policies.

## **Access Control**

Webroot Web Security SaaS provides IT administrators with the ability to enforce company Internet usage policies through application of individual or group policies that allow or restrict Web site and Web application access based on functional area, physical location, and time of day. Enforced policies help to ensure that users have access only to the content and applications they need to perform their jobs.

Company justification to create and enforce Internet use policies might include preventing access to potentially offensive material that, if exposed within a business environment, may lead to complex human resource issues; eliminating the download of large music and video files to help preserve network bandwidth and save costs; and removing access to social networking and other Web 2.0 sites that are highly subject to malware and phishing attacks.

While Webroot Web Security SaaS will classify millions of URLs into numerous main categories and subcategories, customized allow and deny lists can also be applied to help better enforce Internet use policies. The URL database is continually updated to reflect the most up-to-date listing of known dangerous Web sites.

## **Threat Protection**

To help eliminate Web-based threats before they reach a company's network, Webroot Web Security SaaS provides in-the-cloud scanning of all inbound HTTP and FTP traffic to protect against virus, spyware, Trojans, worms, and other types of malware attacks. Traffic is scanned using various signature and heuristic techniques to ensure protection against known and unknown threats.

Web sites known to contain phishing attacks are also blocked based on the Webroot URL filtering engine, helping to ensure that employee and company data remains protected.

As exposure of confidential information has become one of the greatest threats to company network security, Webroot Web Security SaaS also provides IT administrators with the ability to restrict users from sending outbound documents such as Word, Excel, and PDF files. This helps companies not only protect confidential company data but also comply with government and industry regulations such as HIPAA, Sarbanes-Oxley, and Gramm-Leach-Bliley.

## **Mobile User Protection**

In addition to protecting corporate workstations, Webroot Web Security SaaS also extends the same real-time threat protection and access control policies to mobile laptop users. Because these mobile protection capabilities are included as a core feature of the Webroot offering, there is no need for additional VPN clients, hardware, or software. Employees are protected and company Internet usage policies can be extended, regardless of working location — at home, on the road, at the airport, or at a coffee shop. Authentication of mobile users and connection to the Webroot Web Security SaaS service is also transparent. This helps to ensure a seamless experience for all employees, regardless of location.

Providing Web threat protection for mobile users will help an organization to mitigate the risk of malware-infected laptops being brought back into the office and compromising the company network.

## **CHALLENGES/OPPORTUNITIES**

Cost-effective security is becoming essential to SMBs. The Webroot SaaS solution provides an excellent complement to the basic perimeter products already installed in the majority of organizations, but it cannot serve as the only defense. Perimeter and endpoint security remain essential building blocks upon which the Webroot solution offers a valuable complementary protection layer.

With the Web becoming an increasingly complex threat vector for hackers, malicious applications, and vulnerability exploits, organizations require a more holistic and integrated approach to combat emerging threats from the Internet. Given that Web 2.0 exposes organizations to both inbound and outbound security threats, IDC believes effective Web security solutions must analyze traffic bidirectionally. IDC believes the rise of Web 2.0 in the workplace represents a great opportunity for Webroot. We expect hackers to increasingly target the growing number of nonsecure Web 2.0 sites that are extremely vulnerable to compromises.

## **CONCLUSION**

SMBs, because of their near complete focus on running their businesses and battling competitors, are less likely to maintain highly skilled security staffs. Without dedicated security professionals, SMBs are finding it much more difficult to successfully defend, on an ongoing basis, against the constantly changing Web threat ecosystem.

In addition, the constant squeeze on budgets makes it doubly difficult for SMBs to invest in staff and resources to maintain adequate protection against these threats.

IDC research has shown that SaaS security offerings, such as those from Webroot, provide SMBs with viable, highly effective and cost-effective solutions to protect their businesses from Web and email breaches. Webroot's comprehensive and proven Web security SaaS offering should be investigated by any organization that requires assistance in maintaining its Web security.

---

## **Copyright Notice**

External Publication of IDC Information and Data — Any IDC information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate IDC Vice President or Country Manager. A draft of the proposed document should accompany any such request. IDC reserves the right to deny approval of external usage for any reason.

Copyright 2008 IDC. Reproduction without written permission is completely forbidden.