



Webroot® E-Mail Security SaaS

Small to Medium Business

Email Protection for the Small to Medium Business

The Challenge

Technology is essential to small to medium sized businesses (SMB). To compete effectively it is essential to use flexible methods of communication such as email. Unfortunately, this opens the business to new and increasing threats. SMBs face a daunting challenge when it comes to IT security. Spam, viruses, spyware and other attacks target the SMB specifically because most cannot afford the security expertise and equipment to protect their data and employees against such threats. Small to medium businesses are highly cost conscious and have little time to deal with the problems associated with email. Many recent surveys, studies and industry reports indicate that keeping up to date with security solutions and new threats while keeping the costs low was an ongoing concern for smaller firms. With so many issues involved in starting and running a business, keeping track of IT and security can easily be overlooked. Small to medium businesses require a 'set and forget' solution that provides peace of mind at an affordable price.

The Solution

Webroot® offers SMBs the same level of security and protection usually only afforded to larger businesses, via a service that requires no hardware or software and that protects against major email threats.

- Webroot offers a service that filters email traffic on the Internet. Consequently, any attack would have to breach Webroot's large and resilient data centers before they could reach the customer. Every client benefits from the industry leading expertise, systems and hardware that Webroot runs and updates.
- Various packages are available offering services, support and pricing that are appropriate to the smaller business. A risk-free, no obligation 14 day trial period allows customers to prove the benefits of the service at no cost.

Webroot Email Security SaaS provides options to cover email filtering, email archiving, personal email encryption and business continuity, ensuring that customers are able to access and use email in the event of a mail server outage.

- Customer email is protected by the expertise of our security specialists who monitor and tune the systems around the clock. For example, each email is scanned by five antivirus engines, ensuring total protection against infection.
- The service is delivered at a fixed yearly price, regardless of the quantity of spam or virus attacks that you are protected from. Should your spam increase dramatically, you have no need to worry about upgrades or extra costs. As new enhancements and developments are added to the base protection services, the system is automatically upgraded for you at no extra cost.

Did You Know?

- 85 percent of viruses gain entry to a network through email and spam (10,000 new/modified viruses appear each year)
- Although businesses have antivirus protection, 68 percent still get infected (DTI / PricewaterhouseCoopers)
- Viruses are still the number one reason for reported security incidents (DTI's Information Security Breaches Survey 2006)
- Spam now represents over 95 percent of all Internet email traffic (BBC News)
- Over 40 percent of emails at work are non-business related (IDC research)
- Inappropriate Web and email usage is the second largest cause of reported security incidents (DTI's Information Security Breaches Survey 2006)
- 52 percent of organizations reporting misuse of Internet resources (DTI's Information Security Breaches Survey 2006)
- 80 percent of a company's data can be found in the company's email store after just one year

With spam and virus mails reaching record levels, 80% of companies now believe that spam results in decreased productivity. Additionally, pornographic or distasteful emails can cause offense to employees and pose a legal threat to employers of all sizes, who may be held accountable for such exposures. Every business has a responsibility to employees to protect them from exposure to offensive content.

"To keep up with the latest threats, Web filtering must incorporate 'on the fly' malware detection and blocking capabilities. Organizations that need an effective strategy to keep unwanted content out and sensitive content in should look to a solution that offers zero-hour malware detection, high performance filtering, and outbound content filtering capabilities." - Forrester Research

Webroot Software, Inc. – World Headquarters
2560 55th Street
Boulder CO 80301 USA
www.webroot.com • 800.870.8102

Webroot Ltd. – EMEA Headquarters
Cart Lodge, Squerryes, Goodley Stock Road
Westerham, Kent TN16 1SL, UK
www.webroot.com/uk • +44 (0)870 1417 070

Webroot Software Pty Ltd. – APAC Headquarters
Level 11, Tower B, 821 Pacific Highway
Chatswood NSW 2067 Australia
www.webroot.com • +61 (0)2 8448 8144 • 1.800.029.234

© 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 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 and Webroot makes no warranty as to its accuracy or use. 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.