

Webroot® Email Security Service

Better Email Protection. Simpler Management.

Spam now accounts for more than 96 percent of all email, and corporate email is responsible for over half of information leaks¹. Webroot® Email Security Service improves protection by filtering email in the cloud.

Spam and viruses are blocked before they reach your network, freeing up bandwidth and increasing security. Advanced email management policies help your company to meet compliance regulations and prevent data leakage. And because the service resides outside your network, you don't need to invest in additional hardware, software, or personnel to manage daily security operations.



Webroot Email Security Service

KEY BENEFITS

KEY FEATURES

LOWER TOTAL COST OF OWNERSHIP (TCO)

No hardware or software to purchase or manage
Predictable operating costs
Integrated suite of email protection, management and compliance services

INCREASED IT EFFICIENCY

Pay-for-use model scales easily to accommodate growth
Managed service reduces resource strain and increases IT capacity
Fast, low-risk service deployment

SIMPLIFIED MANAGEABILITY AND REPORTING

No hardware or software updates to manage
Web-based admin panel and summary dashboard offers total visibility, control and flexibility
On-demand, customizable reports demonstrate effectiveness and ROI

IMPROVED DATA SECURITY AND COMPLIANCE

In and outbound content and file type scanning
Pre-defined compliance dictionaries to help meet data security and compliance concerns
Optional policy-based encryption and archiving services

EFFECTIVE AND RELIABLE

Protects against 98% of spam and 100% of known and unknown viruses
Support available 24x7x365
99.999% uptime guarantee

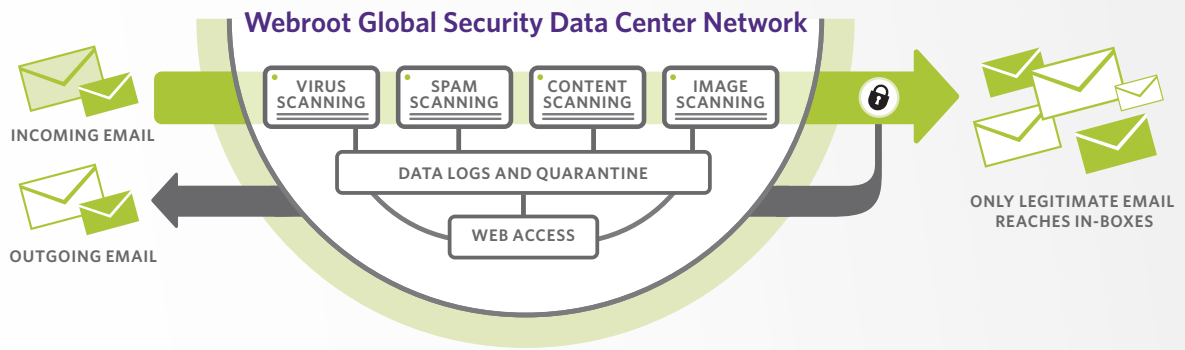


★★★★★ 5 out of 5 stars

"The SLA of 100% virus protection holds true and it provides as near to 100% spam filtering as you'll ever get. Add to that business continuity, encryption support, and optional email archiving and **you have everything your business will ever need.**"

—IT Director,
Webroot Email Security Customer

1 IDC, 2008



Features

Antispam

Keep spam off your network and out of corporate in-boxes. With seven different levels of spam detection and multiple best of breed email filters, Webroot guarantees elimination of 98% of all spam. And unlike other reputation services that provide only a binary 'good' or 'bad' rating, Webroot quantifies sender reputation based on granular trust ratings that automatically adjust over time (fig. 1). This mathematical model provides far more accurate and scalable detection than systems that simply employ a blacklist approach. Outbound spam protection locates and blocks infected machines from sending spam through the company network to help preserve your organization's reputation.

Antivirus

Eliminate concerns over fast-spreading email viruses with guaranteed protection against 100% of known and unknown virus threats. Webroot Email Security Service incorporates multiple signature, heuristic and zero-day engines to provide unmatched detection of viruses and variants (fig. 2). These powerful filters seek out and block new threats before they can infect your company's network environment.

Backscatter Protection

Backscatter occurs when a spammer spoofs a legitimate email address to send an unsolicited message to large distribution lists, causing the email server to flood an unsuspecting email address owner's mailbox with hundreds or thousands of failed delivery messages. To protect against this growing threat, Webroot employs an advanced technique called Bounce Address Tag Validation (BATV). Every sent message is marked with a timestamp and unique cryptographic signature that cannot be duplicated. Any failed delivery messages that do not reference this signature are then marked as spam and blocked from entering the user's mailbox.

Figure 1 Advanced analyses ensure highly accurate spam detection.

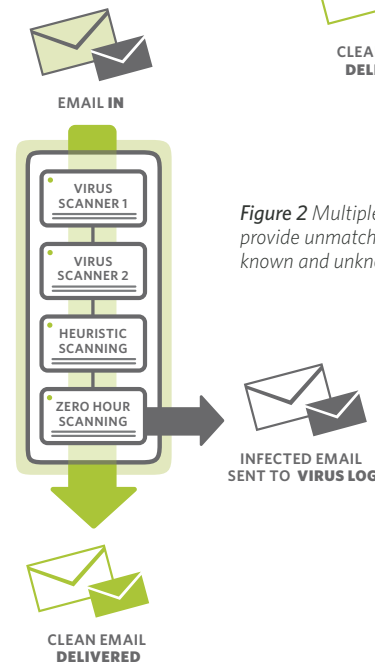
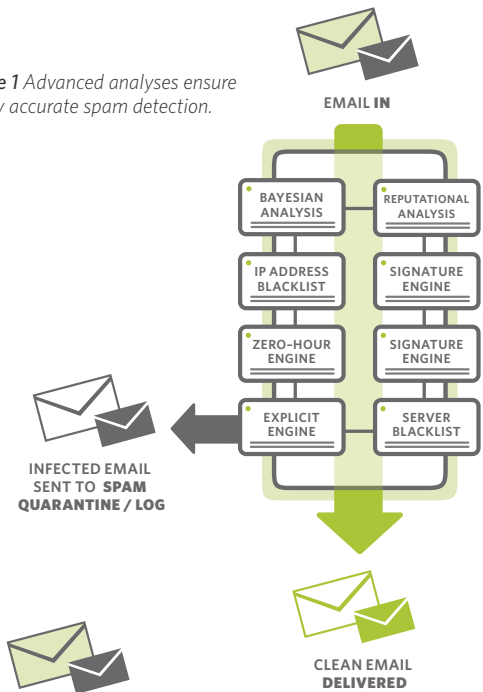


Figure 2 Multiple engines provide unmatched detection of known and unknown viruses.

Image Protection

Protect users against exposure to inappropriate images with a filter that specifically scans and analyzes images (fig. 3). Each image's dataflow (shape, color, texture, etc.) is converted into a digital signature which is then compared against a database of inappropriate images. If the image is similar to those blacklisted images, the email content is classified as inappropriate and action may be taken to either delete or quarantine the email. All messages containing suspect images are logged.

Data Security and Compliance

Prevent data loss and meet compliance with advanced content filtering abilities. Pre-defined and custom dictionaries make it easy to detect and control messages that include sensitive or inappropriate content (fig 4). Pre-configured dictionaries include key terms to help your company develop email policies to comply with HIPAA, GLBA, PCI-DSS, and other regulatory compliance measures. Dictionaries can use keyword scoring to trigger custom rules once pre-defined thresholds are met or exceeded. Administrators can also use Boolean operators to create custom rules by combining subsets or supersets of dictionaries.

Email Policy Management

Manage email policies for individual users or groups with a powerful, customizable rules engine. Administrators can control where messages are sent and how they should be filtered based on specified content or events (fig. 5). Set rules for a number of different situations, either as an individual occurrence or as a combination of complex business events. Besides standard email actions such as block, copy, and redirect, rules can be used to alert or trigger other systems such as HR, CRM, ERP or workflow. These highly granular levels of control simplify management and monitoring of inbound and outbound email traffic.

Fast Deployment and Guaranteed Service Availability

Customer deployment can be complete in one to four days and there are no costly hardware or equipment maintenance fees. Webroot also guarantees a 99.999% service availability to ensure that customers have access to a secure email communications environment.



Figure 3 Image scanning analyzes dataflow to detect inappropriate images.

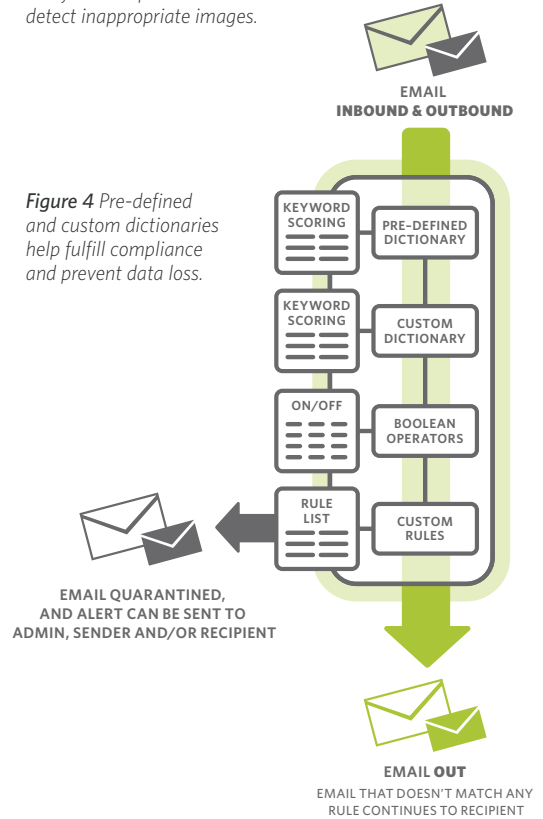


Figure 4 Pre-defined and custom dictionaries help fulfill compliance and prevent data loss.

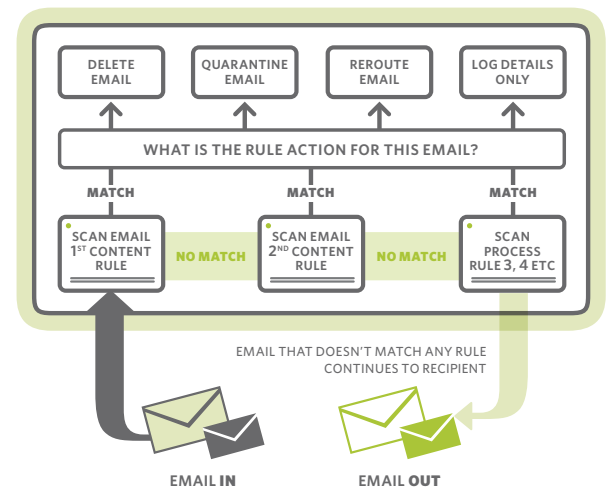


Figure 5 A customizable rules engine provides highly granular levels of control.

Additional Services

Email Archiving

Improve compliance and expedite e-discovery with Webroot Email Archiving Service. With unlimited data storage in the cloud, the service enables you to securely capture, store and index all inbound and outbound email traffic in real-time. Once captured, these emails are stored in duplicate and geographically disparate data centers, protecting data against physical loss or corruption.

Email Encryption

Meet legal, compliance and regulatory standards by automatically encrypting email messages based on company email policy. This policy-based encryption service expands data loss prevention capabilities and improves the secure handling of confidential company data. Customizable encryption policies allow automatic email encryption based on existing administration rules. Users can also encrypt communications on an as-needed basis. Messages are sent securely even if the recipient does not have encryption capabilities, eliminating the need for users to manage encryption keys.

Deep Content Scanning

To further help mitigate data loss concerns and ensure the confidentiality of company information, Deep Content Scanning inspects content embedded within file attachments and remediates according to company policy. This powerful mechanism provides the ability to scan content in over 300 different file types, including compressed files.

Business Continuity

Add Business Continuity to ensure availability to critical business communications in the event of email server failure. The service provides end user access to up to 28 days of inbound and outbound email to be made available from secure, mirrored data stores via a webmail portal. And the easy-to-use portal allows users to send and receive email from any browser worldwide, ensuring important business communication is not lost during periods of downtime.



Gain instant insight into email traffic and blocked threats.

WHY WEBROOT?

Webroot is a global company with a history of delivering innovative security solutions to millions of businesses and consumers. Our best-of-breed technology has won numerous awards and our SaaS solutions protect over three million users worldwide. As one of the largest privately held companies in the Security SaaS market, Webroot has multiple data centers and support offices across the US, Europe, Japan and Australia. To guarantee the highest level of service, all Webroot Security Services are backed by local technical support teams and Service Level Agreements (SLAs) that are among the best in the business.

SEE THE BENEFITS FOR YOURSELF!
To schedule a free trial or demo,
call 866.915.3208, or visit
www.webroot.com/business.

Webroot Software, Inc. - USA
2560 55th Street
Boulder CO 80301 USA
www.webroot.com • 866.915.3208

Webroot International Ltd. - EUROPE
Alexandria House, The Sweepstakes, Ballsbridge
Dublin 4, Ireland
www.webroot.com/europe • +44 (0)870 141 7070

Webroot Software Pty Ltd. - APAC
Level 20, Tower A, 821 Pacific Highway
Chatswood NSW 2067 Australia
www.webroot.com.au • +61 (0)2 8448 8144 • 1.800.029.234

© 2010 All rights reserved. Webroot Software, Inc. Webroot 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.

webroot

The Best Security
in an Unsecured World™

USA-0710-1.0