



Webroot® E-Mail Security SaaS *overview*

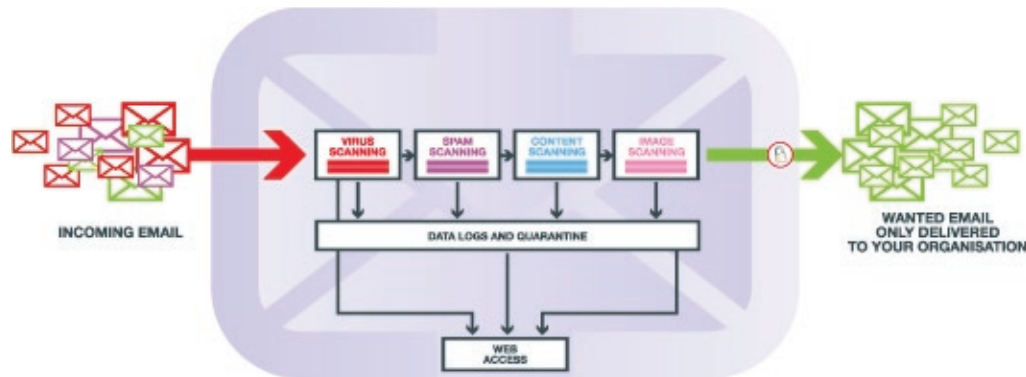
Webroot® E-mail Security SaaS

E-mail is the most vital method of communication for businesses around the globe. Most companies cannot fully function when e-mail is down. Increasingly, e-mail delivery systems strain under the rampant influx of spam, viruses and other malicious threats. Unwanted e-mail currently accounts for between 65 and 90 percent of daily traffic. The sheer volume of this unwelcome mail is an overwhelming drain on time, effort and resources.

Webroot® E-mail Security SaaS is a security service that resides outside your network, requiring no additional hardware, software, or personnel resources to manage daily security operations. It provides award winning in-the-cloud

e-mail management, protection and compliance services for more than 2.5 million people worldwide.

This powerful, flexible offering includes dynamic virus and spam filters to protect against 99% of e-mail spam and 100% of known viruses. Webroot's content filtering and data archiving capabilities prevent against data loss and help to fulfill compliance and data storage requirements. 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 e-mail communications environment.



Benefits of E-mail Security SaaS

BENEFIT	PROOF
Effective and Reliable	<ul style="list-style-type: none"> → Protects against 99% of spam and 100% of known viruses → Trusted by over 2 million users with 99% renewal rate → Support available 24x7x365 → 99.999% uptime guarantee
Low Cost	<ul style="list-style-type: none"> → No hardware or software installation or maintenance → Predictable, low risk operating costs
Fast, Easy Implementation	<ul style="list-style-type: none"> → Fast, low risk deployment → No user disruption → Deployment usually completed within one to four days
Save Time and Resources	<ul style="list-style-type: none"> → Integrated suite of e-mail protection, management and compliance services → No training or in-house expertise required
Real-time Reporting	<ul style="list-style-type: none"> → On-demand, customizable reports demonstrate effectiveness and ROI → Query anytime → Web-based admin panel and summary dashboard offers total visibility, control and flexibility

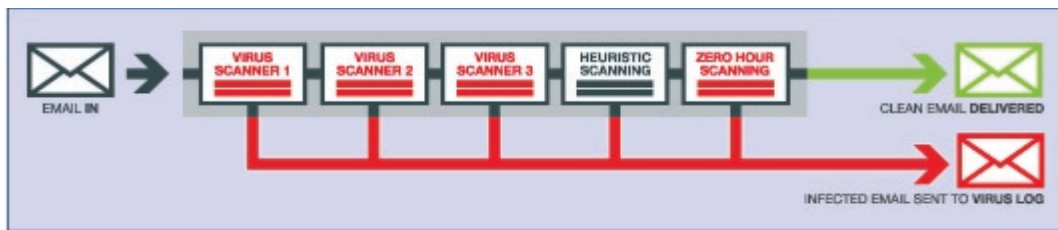
Webroot E-mail Security SaaS Features

- Anti virus
- Anti-spam
- Anti-phishing
- Encryption
- Content Control
- Image filtering
- Business Continuity
- Archiving

Virus Protection

Our core anti virus solution comprises five best of breed identity-based engines, which are critical in the detection of viruses. However, as mass virus outbreaks tend to replicate and distribute at high speed, the time taken by identity-based anti virus vendors to capture, analyze and release tested

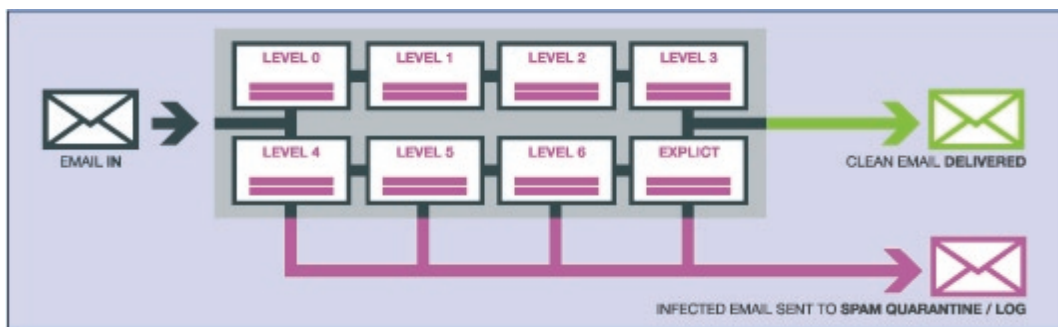
updates to the anti virus engines leaves organizations exposed to infection. To meet this challenge, our anti virus protection employs Zero Hour and heuristic filters to seek out and block 100% of new and known viruses.



Spam and Phishing Protection

With spam levels regularly being measured at between 65 and 90 percent of all corporate e-mail traffic, our technology effectively manages this unacceptable volume of unwanted e-mail. Careful attention to connection management and

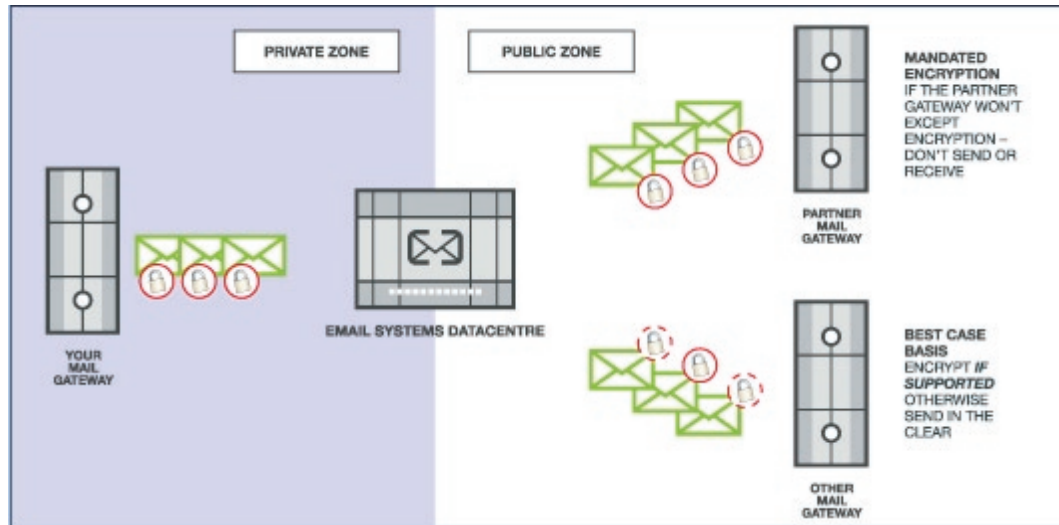
integration of multiple best of breed filters blocks the maximum quantities of spam and phishing e-mails with the lowest possible rate of false positives. We offer seven different levels of spam detection to catch 99% of all spam.



Encryption

While e-mail is the most common method of communication in the modern world, it is inherently insecure and data is most vulnerable while it is in transit. The Managed Encryption Service provides an open standard encryption mechanism with no hardware or software purchase or maintenance required. Historically, reliable encryption has been unachievable for many organizations due to many interrelated issues – notably complexity, interoperability standards and, more recently,

the threat of data leakage and malware infiltration through un-scannable encrypted channels. Managed Encryption Services are provided using Transport Layer Security (TLS), a transparent mechanism for encrypting data on a peer-to-peer basis, such as between messaging servers. Webroot also offers desk-to-desk e-mail encryption via public and private keys for an added layer of security.



Content Control

Our Content Control management suite offers a powerful, customizable rules engine, which facilitates both content and event-based e-mail management while providing highly sensitive levels of control regarding inbound and outbound e-mail traffic. The service allows users to control where messages are sent and how they should be filtered based

on specified criteria. Rules can be set for a number of different situations, either as an individual occurrence or as a combination of complex business events. Besides standard e-mail actions such as block, copy, and redirect, rules can be used to alert or trigger other systems such as HR, CRM, ERP or workflow.

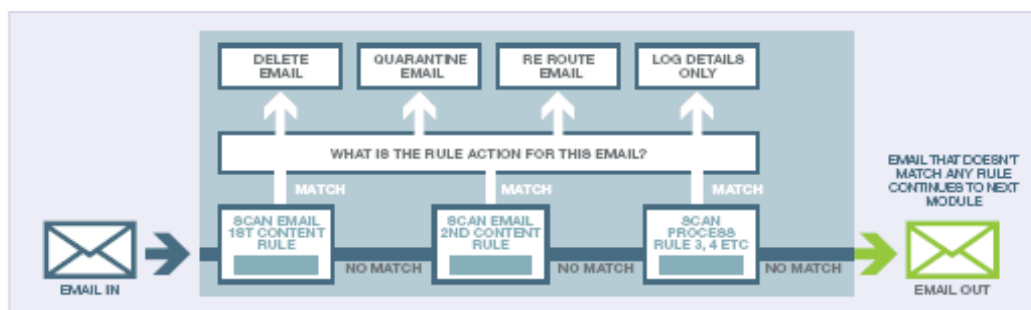
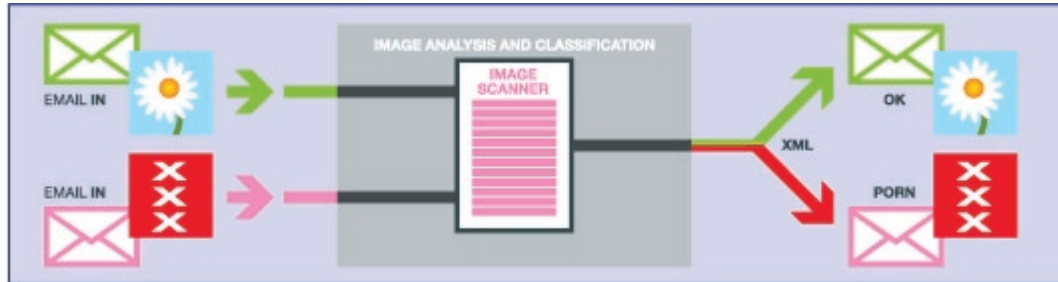


Image Protection

Increasingly, employers recognize that they have a professional obligation to minimize employee exposure to distasteful and offensive images coming to their inbox. Consequently, Webroot provides a filter specifically to address image analysis. When images are scanned, their dataflow (shape, color, texture, etc.) is converted into a digital signature

which is then compared against known pornographic images. If the image is similar to those blacklisted images, the e-mail content is classified as pornographic and action may be taken to either delete or quarantine the e-mail. All messages containing suspect images are logged.



Business Continuity

While most Business Continuity solutions only kick-in when a disaster occurs, our solution provides "always available" capabilities, ensuring that off-site resources are constantly active during normal operation as well as when disaster hits. The service enables 28 days of inbound and outbound e-mail

to be available from secure, mirrored data stores to end users via webmail. The webmail alternative allows users to send and receive e-mail from any browser worldwide, ensuring important communication is not lost during crises.

Archiving

A core element of any Business Continuity solution is Archiving. Archiving enables organizations to securely capture, store, and index all inbound and outbound e-mail traffic in

real-time. Once captured, these e-mails are stored in duplicate and geographically disparate data centers, thus protecting data against physical loss or corruption.

