

TECHNOLOGY AUDIT

E-mail and Web Security SaaS




Webroot, Inc.

BUTLER GROUP VIEW

ABSTRACT

Webroot is an established security provider of Software as a Service (SaaS)-delivered e-mail and Web security suites. The e-mail security suite comprises anti-spam, anti-virus, content scanning for Data Loss Prevention (DLP), image scanning, continuity management for mails, e-mail archiving, and e-mail encryption. The Web security suite comprises anti-virus, anti-spyware, anti-phishing, application blocking, and URL filtering. Webroot has combined proprietary technology alongside a number of best-of-breed security point solutions into the aforementioned suites. The services are delivered through data centres across three continents (Europe, North America, and Australia), with full redundancy capabilities. The service suite is aimed at SMEs with between 100 and 5,000 users, and offers the benefit of Web and e-mail security without dedicated qualified in-house personnel and appliance and/or software installations. Overall, both services offer a good solution that Butler Group recommends as part of a more comprehensive security architecture comprising gateway and end point-based security solutions.

KEY FINDINGS

- | | |
|---|---|
|  Good policy management and reporting capabilities. |  Data centres across three continents with in-region automatic failover and backup provide a highly redundant physical architecture. |
|  Combines best-of-breed individual security components through extensive partnerships. |  Good support for mobile users; all Web requests can be configured to be routed through Webroot's service. |
|  Lack of support for some niche requirements of customer organisations. |  The Web security offering is relatively new; launched in mid-2008. |
|  Currently has 3 million SaaS security users and over 500 channel partners. | |

Key:  Product Strength  Product Weakness  Point of Information

LOOK AHEAD

The roadmap includes new features for e-mail security, including Policy-Based Encryption (June 2009), and new features for Web security, including quota-based policies for time spent surfing, bandwidth allocation, and number of sites visited (June 2009 release), among many others.

FUNCTIONALITY

Product Analysis

Webroot provides e-mail and Web security through the Software-as-a-Service (SaaS) delivery channel. The e-mail security suite comprises anti-spam, anti-virus, content scanning for Data Loss Prevention (DLP), image scanning, continuity management for mails, e-mail archiving, and e-mail encryption. The Web security suite comprises anti-virus, anti-spyware, application blocking, and URL filtering. Webroot has traditionally been a leading provider of anti-spyware and anti-malware technology, and entered the SaaS security space in late 2007 with the acquisition of SaaS security provider E-mail Systems. Webroot's services follow the standard per user per month subscription fee model (or equivalent, such as number of e-mail inboxes), and are bundled flexibly.

Webroot's approach to e-mail and Web security can be summarised as the assembly of multiple layers of in-house and third-party best-of-breed point security solutions into one platform. The multi-layered strategy utilises different approaches to combat a single threat. For example, the anti-spam engine uses a reputation-based system for source servers, collective spam reporting, content-based filtering, and Recurrent Pattern Detection. The e-mail security service utilises a messaging security platform that contains five different anti-virus engines, which also includes a heuristic filter to scan e-mails against real-time viruses, combined with seven separate layers of spam detection. The anti-spyware filters for Webroot's Web Security service are backed by Webroot's own anti-spyware engine – Webroot® Spy Sweeper – which protects over ten million desktops worldwide. The URL filtering engine has a continuously updated database of millions of URLs categorised into 12 main categories and 96 subcategories.

Webroot delivers its security services through data centres on three continents: Europe, North America, and Australia. Within each region, filtering is done locally for customers and is fully redundant to ensure high availability. Webroot claims that the e-mail service provides 99.999% system availability.

Webroot offers different levels of Service Level Agreement (SLA) around delivery time of message, up-time, and protection against malware and spam. Webroot also provides portal-based reporting on performance against SLAs.

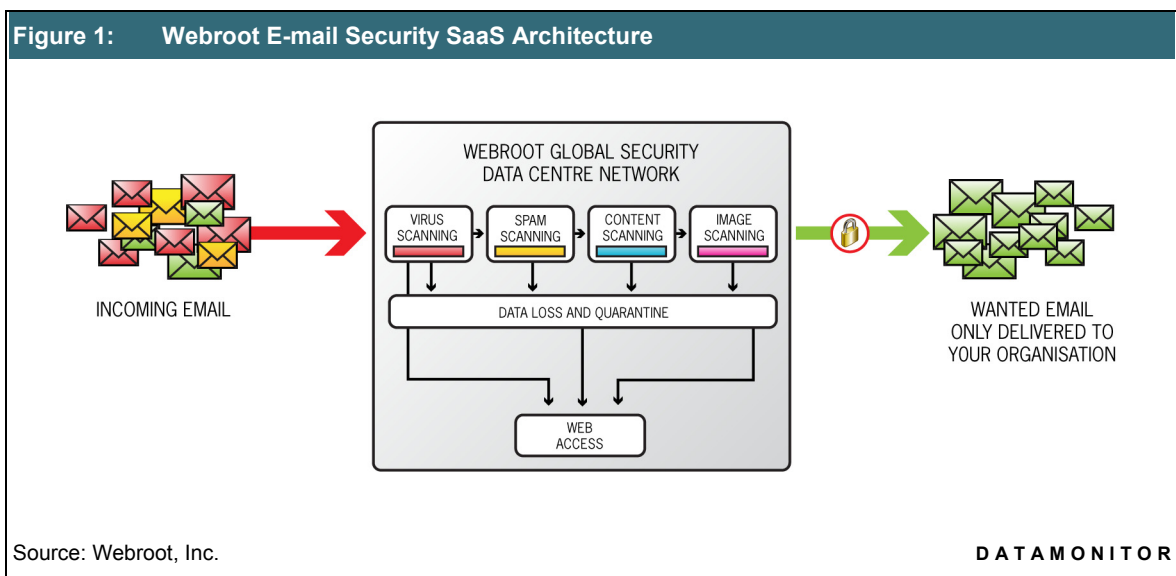
Webroot's management console supports capabilities such as: (i) Management Dashboard for real-time summary reports; (ii) control panel for granular visibility into every individual's e-mail and Web traffic data; (iii) access to audit logs; and (iv) ability to set e-mail and Internet use policies such as blocking certain Web applications and file types in order to preserve bandwidth.

Butler Group believes that given the growing complexity of security management, the onslaught of regulations, and the current economic climate, the adoption of SaaS-delivered and managed Web and e-mail security will grow. Webroot has certainly assembled a spectrum of proven security components, all driven through powerful management capabilities and an impressive delivery infrastructure. However, it is important to mention in this context, that the Web security suite is fairly new and was launched in late 2007 (with several significant new releases since that time). Butler Group believes that the company could communicate the low latency nature of its Web security solution a bit more, given the obvious concerns that client organisations and users would have. Butler Group has no hesitation in recommending Webroot's technology as a component of an overall gateway and end point solutions-based security architecture.

Product Operation

Webroot E-mail Security

The Webroot E-mail Security SaaS solution is a messaging security platform that consists of five different anti-virus engines, seven separate layers of spam detection (including protection against backscatter), and a rule-based content scanning engine that scans e-mail content and attachments based on custom or pre-existing compliance dictionaries. The service also supports an optional image scanning engine that prevents unwanted image content entering into the user's mailbox. The architecture is shown in Figure 1.



- Anti-virus Filters:** All inbound e-mail traffic is routed onto the Webroot e-mail service which passes the messages through a series of filters to scan and detect unwanted e-mails while passing on the legitimate traffic to the user's mailboxes. The solution uses a Message Transfer Agent (MTA) which receives the e-mail and passes it onto the anti-virus filters to scan the e-mail for possible viruses. Initially all mails are passed simultaneously through three individual identity-based detection engines which scan the e-mails, logs and removes those containing any virus, and passing on the legitimate e-mails onto the next scanning stage. The next stage involves a Zero hour scanning engine which, based on Recurrent Pattern Detection (RPD) technology, scans e-mails against real-time updates and then passes them through a heuristic scanning engine to match e-mails against existing signature patterns for already detected viruses and, if a match is found, the e-mail is removed and its details logged.
- Anti-spam Filters:** All e-mails are subsequently passed through the anti-spam filters which contain seven separate levels capable of performing fully automated spam detection. At the initial level Webroot assigns a reputation rating based on advanced statistical models for every server that sends e-mail messages, which is dynamically adjusted based on quantity and the type of e-mail sent, allowing mails from specific servers to be blocked even before they enter the Webroot server. All those messages sent to the Webroot server then pass through a filter which creates a unique signature value for each e-mail. These signatures are matched against a local database and if the signature is not classified as spam, it is then sent to a Central Spam Monitoring System (CSMS) located in each Webroot data centre, which analyses data, looks for similar e-mails, and performs further tests, after which the e-mail is classified as spam or legitimate.

All e-mail that has not been classified as spam after passing through the initial levels then pass through engines utilising technologies such as Collective Spam Reporting, content-based filtering, RPD, and are also checked against a global blacklist database of open relay servers and IP addresses before being classified as legitimate.

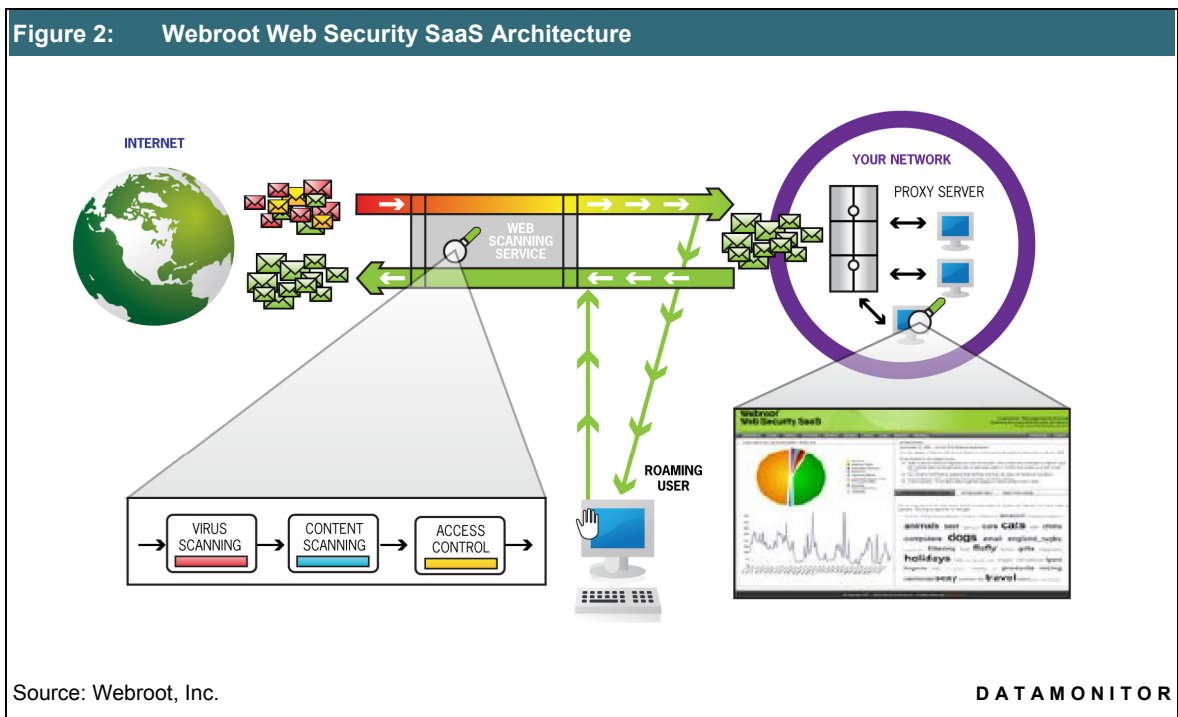
- **Content Control Engine:** Webroot then passes the e-mails through a content control engine, which offers users a customisable rules engine that allows administrators to set rules and control the flow of both inbound and outbound e-mails based on these rule sets. This engine allows users to define where messages are to be sent and also define the filtering criteria which range from size, words, identity, time, source, destination, and attachment type. The set rules can be applied as both individual occurrences or as a combination of conditions or events, and every event and quarantine log can be controlled, viewed, searched, and queried, in real-time via a secure Web control panel. The engine also allows users to alert or trigger other systems such as Human Resources (HR), CRM, ERP, or workflow apart from standard actions.
- **Image Scanning Filters:** Finally all e-mails are passed through the image scanning filter to scan images in the e-mail for possible pornography and to enforce organisational acceptable usage policies. The images are then scanned using an advanced image analysis engine to determine if they are pornographic in nature. If the images exceed the threshold set by the customer, then these messages can be either deleted or quarantined, and all messages containing suspect images are logged with alerts being sent to recipients and administrators while other legitimate mails are delivered to the user's mailbox.

The e-mail security service also provides additional capabilities included in its base offering for: (i) Message Tracking – wherein Webroot creates audit logs for every e-mail that can be later searched based on attributes such as date, time, sender, subject, etc.; and (ii) Encryption – wherein encryption is provided using Transport Layer Security (TLS) that encrypts data on a peer-to-peer basis ensuring e-mail security while in transit.

Customers can also add-on: (i) E-mail Archiving – which captures all e-mails, then indexes and stores them in geographically disparate data centres, thus ensuring that the data does not incur any physical loss or corruption; (ii) Business Continuity – which ensures that all off-site resources are always available, and in the event of local e-mail infrastructure failure end-users can access historical e-mails from data stores (all inbound and outbound e-mails that the organisation has processed over the previous 28 days), and current incoming mail can be queued for up to seven days (or longer on request); and (iii) Deep Content Scanning – which mitigates the risk of data loss via e-mail by inspecting content embedded within file attachments and remediating according to company policy. This provides the ability to scan content in over 300 different file types, including compressed files.

Webroot Web Security

All outbound customer Hypertext Transfer Protocol (HTTP) requests are routed through Webroot's global data centre network, which hosts pre-defined organisational policies that are adhered to before the user is allowed access to a particular URL. As soon as the request meets these policies, the data is examined for malware, spyware, and other 'crimeware' before being passed onto the end user's browser safely. The architecture is shown in Figure 2.



The Web Security service scans all HTTP and File Transfer Protocol (FTP) over HTTP requests to detect any viruses. The service utilises anti-virus engines along with a zero-hour heuristic filter that protects data against all detected viruses. The service provides anti-spyware protection backed by its own anti-spyware engine Webroot Spy Sweeper, which functions based on an automated threat research system called Phileas that utilises a patent-pending technology in order to scan and detect spyware quickly over the Web. The service also provides anti-phishing detection capabilities through advanced heuristics filters which identifies phishing sites in real-time.

Through its URL filtering engine the Webroot service enables organisations to efficiently filter all Web content entering into the organisational network based on Web site URL, Web application, attachment type, and file size. The Web security service also allows organisations to define access policies which can be applied based on user role and also based on time, date, and location. The administrators are allowed to set Web site access as 'Allowed', 'Blocked', or 'Coached'. Customised URL lists can also be created.

Very similar to the E-mail Security service the Web Security service provides a customisable rules engine which facilitates the creation of user-, group-, and account-level policies in order to effectively manage the Web content flow. The engine allows administrators to set rules that allow access to audit logs that record individual Web page request made by users, block Web applications for network bandwidth consumption control, and also block all outbound files and attachments ensuring that there is no loss of sensitive data. Webroot also provides organisations with the ability to populate user-level settings by retrieving existing company policies by querying the Lightweight Directory Access Protocol (LDAP) server and retrieving all related attributes.

Web Security SaaS also extends the protection levels to mobile laptop users, by enforcing Internet policies irrespective of the location (outside the company network) from where they are trying to access data. These mobile users can be configured to authenticate directly with the Webroot service.

Both the E-mail and Web Security services provide administrators with a Web-based management console, which allows them to manage and obtain a real-time view of e-mail and Internet usage activities of all users.

Product Emphasis

In Butler Group's opinion, Webroot focuses on providing a SaaS offering for organisations looking to secure e-mail and Web access through a series of best-of-breed anti-malware, anti-spam, and URL filtering tools, bundled flexibility, and managed in a fairly controlled and granular fashion. The solution add-ons, such as e-mail archiving and business continuity management, and the company's roadmap (which includes additional DLP and encryption capabilities) point towards a focus on being the Small- to Medium-sized Enterprise (SME) 'one-stop shop' for all security concerns. Overall, Butler Group is impressed with the solution and believes that in terms of functional capabilities, delivery infrastructure, and depth of partnerships, Webroot is among the best in the SaaS-delivered Web and e-mail security solutions marketplace.

DEPLOYMENT

For solution implementation, knowledge of the company's domain environment, firewall settings, and the Internet use policy is required. Webroot's support and sales engineer teams work with customer IT staff and/or third-party systems integrators to facilitate service deployment and security policy set-up. Webroot reports that on an average the implementation time is less than a week.

Deployment can be staggered and the core service platform for e-mail security (which includes policy management and reporting UI, basic content control engine, and spam and virus detection capabilities) can be deployed initially and any combination of the following modules can be added later: deep content scanning, image scanning, e-mail archiving, e-mail continuity, and policy-based encryption (which is scheduled for release in June 2009). Webroot bundles its Web Security service offerings in the following three options:

1. **Total Web Protection Bundle:** includes Anti-virus, Anti-spyware, Application Blocking, URL Filtering, and Mobile User Protection. Webroot reports that this is most popular bundle, and 70-80% of customers select this option.
2. **Web Filtering Bundle:** includes URL Filtering, Application Blocking, and Mobile User Protection.
3. **Threat Protection Bundle:** includes Anti-virus, Anti-spyware, Advanced Reporting, and Mobile User Protection.

Additionally, the Webroot service also has an add-on Full Logging module that allows access to the entire Internet traffic logs.

Webroot provides frequent product and technical training, both Web-based and classroom delivered, for client organisations and reseller partners. Technical support is provided via Web, e-mail, or telephone on a 24x7 basis and these support services are backed by SLAs to guarantee customer response times.

Webroot points out that there are a number of issues that need to be addressed to limit the chances of a Webroot implementation not going ahead as planned: (i) perceived latency in Web traffic download; (ii) new content yet to be classified passing through the URL filter; and (iii) the inability to support specific requirements of customer organisations (e.g. the support of Apple installations for Web Security). In Butler Group's opinion most of these issues can be addressed by Webroot, but it is important that they are discussed in advance of any proposed implementation.

PRODUCT STRATEGY

Webroot targets the SME marketplace with between 100 and 5,000 seats. While the target market is horizontal, the nature of the offering leads to a bias towards highly regulated sectors such as financial, legal, and healthcare.

The route to market is both direct and through channel partners. Webroot leverages a channel-based approach in the UK and EMEA where reseller partners either drive new sales opportunities or leverage Webroot's lead generation programmes. The company follows a hybrid approach in North America, wherein large opportunities are pursued directly, and Webroot also uses its regional reseller partner network. One of the largest worldwide business partnerships is with Integralis, a large global reseller.

For a typical Webroot SaaS solution, 100% of the purchase cost is the subscription licence cost and the pricing is per user per month based on an annual contract. The company also provides additional discounts based on number of users, additional years, and additional services with no additional maintenance and support costs. Webroot reports that the average value of a typical installation is approximately US\$8,500.

Webroot provides customers with multiple service releases annually. The company has an extensive roadmap which includes:

- **E-mail security:** enhanced e-mail archiving capabilities and additional mail continuity functionality (both scheduled for Q3/09), and a policy-based encryption module and enhanced Simple Mail Transfer Protocol (SMTP)-based DLP capabilities (both scheduled for Q2/09) to its e-mail security platform.
- **Web security:** enhanced logging and reporting capabilities incorporate additional outbound threat protection technologies to enhance DLP capability, add user quota capabilities (including time spent online, number of sites accessed, and bandwidth use), and also update URL filtering classification and Internet use policy enforcement capabilities.

COMPANY PROFILE

Founded in 1997, Webroot is headquartered in Boulder, Colorado, in the US, with a sizeable presence in Mountain View, California, and additional sales and support offices in Bracknell, Westerham, Amsterdam, Sydney, Paris, and Tokyo. Webroot is a privately owned with 340 employees. About 148 of these employees are engaged with the engineering/threat research function, while 85 of them handle sales and marketing, 61 handle customer support, and 46 are engaged with the IT and administration function. Webroot has over three million users for its SaaS services worldwide and key clients include: Manchester City Football Club; Access IT; Jelf Group; The Ajilon Group; Massachusetts Association of Insurance Agents; Glasgow Caledonian University; Stevens Aviation; Watson Goepel Maledy; and Dallas County Community College District.

SUMMARY

The SaaS-delivered security solutions market is an interesting space to watch. The market is still very nascent and populated with quite a few of the leading security vendors, although the model is yet to attract the network security behemoths. Butler Group believes that in Webroot’s target market, concerns related to privacy and latency will be increasingly balanced by considerations of lower capital costs, management overheads, and the risk of not managing security in the most optimal way possible. The key barrier to increasing SaaS adoption would be partnerships, as SaaS requires the sort of limited touch model that few resellers are familiar with, and SaaS delivered security requires a strong consulting support, as opposed to some SaaS-delivered business applications. Overall, Butler Group believes that in terms of functional breadth and delivery capabilities, Webroot is certainly among the best solution providers in the target market, and the company’s technology roadmap and strategic initiatives point towards continued relevance in the lower end of the SME market.

Table 1: Contact Details	
<p>Webroot Corporate Headquarters 2560 55th Street Boulder CO 80301 USA Tel: +1 (866) 612 4227 Fax: +1 (303) 442 3846 www.webroot.com</p>	
Source: Webroot, Inc.	DATAMONITOR

Headquarters

Shirethorn House,
 37/43 Prospect Street,
 Kingston upon Hull,
 HU2 8PX, UK
 Tel: +44 (0)1482 586149
 Fax: +44 (0)1482 323577

Butler Direct Pty Ltd.

Level 46, Citigroup Building,
 2 Park Street, Sydney,
 NSW, 2000,
 Australia
 Tel: + 61 (02) 8705 6960
 Fax: + 61 (02) 8705 6961

Butler Group

245 Fifth Avenue,
 4th Floor, New York,
 NY 10016,
 USA
 Tel: +1 212 652 5302
 Fax: +1 212 202 4684

Important Notice

This report contains data and information up-to-date and correct to the best of our knowledge at the time of preparation. The data and information comes from a variety of sources outside our direct control, therefore Butler Direct Limited cannot give any guarantees relating to the content of this report. Ultimate responsibility for all interpretations of, and use of, data, information and commentary in this report remains with you. Butler Direct Limited will not be liable for any interpretations or decisions made by you.

For more information on Butler Group’s Subscription Services please contact one of the local offices above.

