Ferris Research

The OEM Market for Anti-Spam Solutions

Ferris Research Product Brief

The OEM Market for Anti-Spam Solutions

Readers will be familiar with the idea of purchasing an anti-spam product or service. However, there is also an OEM market for anti-spam solutions. Here, the anti-spam technology is sold to a vendor that builds it into its own offering. This paper describes the OEM anti-spam market, and what OEMs look for. We also describe Mailshell's OEM offering.

Market Segmentation

Many different types of businesses can use OEM anti-spam technology. The main types of customers are:

- Anti-virus and other security software vendors.
- Vendors of content-scanning appliances that sit at the corporate Internet boundary.
- Messaging server and relay vendors. These devices may reside either within an organization's network, or at the Internet boundary.
- Hosted mailbox services; e.g., Hotmail and AOL.
- Desktop email client vendors.
- Vendors of specialized network devices, such as routers and firewalls.
- ISPs that want to cut down the email they're transferring.
- Vendors of systems that connect email with wireless access devices, such as PDAs and cell phones. Bandwidth is at a premium, and often there is a traffic-based fee for emails transferred, including spam.

Reasons To Purchase OEM Anti-Spam Technology

- *Enhance revenues*. Spam is a problem for many email users, and they are often prepared to pay for its suppression. Thus a vendor can offer an additional anti-spam fee-based option. The effect is to increase revenues per customer, with minimal additional sales efforts.
- *Reduce support costs*. Customers can call up to complain about spam, and providing support is expensive. Anti-spam technology can reduce the call level.
- *Reduce customer churn*. In some cases, spam levels can cause customers to abandon a service. By reducing spam, anti-spam technology can encourage customer retention.
- *Competitive pressure*. If a vendor's competitors offer spam control, catch up is necessary.

- *Smooth revenue stream*. Spam filtering is naturally a subscription business. As such, it can provide ongoing, predictable revenues, in contrast to "lumpy" product sales revenues.

Customer Requirements

Vendors in the market for an OEM anti-spam solution have the following requirements. They are in rough order of priority. Clearly, the specific requirements vary from customer to customer:

- *Effectiveness*. The solution should catch a high proportion of spam, with very few false positives.

- *Performance and throughput*. Processing rates need to be sufficient for end customers.

- *Support*. Good support should be provided to OEM technical staff by the anti-spam vendor, to provide advice and help troubleshoot problems. Some OEMs may want to buy custom services.

- *Integration*. Vendors want to easily integrate the OEM solution into their product. Things to consider include: technology platforms supported, application programming interfaces (APIs), memory footprint, processing speed, and the quality of the software development kit (SDK) (e.g., whether properly documented, whether error return codes are useful).

- *Reporting*. The system should be able to generate statistics, such as throughput metrics, message latency, and messaging debugging information.

- *Private labeling*. Vendors often wish to hide the fact that they have acquired a solution from another party. In addition to private-labeling the raw solution, it may be important that secondary infrastructure, such as support and a central clearinghouse, is invisible. Generally, support and update capabilities must appear to belong to the OEM.

Anti-Spam OEM Vendors

There is a wide variety of players in the OEM anti-spam market. A great many of these players sell solutions for corporations and end users. Faced with a glutted market, numerous anti-spam vendors have hit upon the idea of selling to OEMs. In such cases, the vendors concerned usually only have a tenuous, opportunistic commitment to OEMs, and have only one or two such customers. The net effect is that OEM revenues are spread across many vendors.

With that caveat, the leading options for OEMs appear to be Brightmail (recently acquired by Symantec), Commtouch, Mailshell, and open-source project SpamAssassin. Other OEM players include Cloudmark, FrontBridge, Mail-Filters, Postini, and SurfControl.

About Mailshell

Mailshell (www.mailshell.com) develops anti-spam software and sells only to OEMs. Its core software is the *Mailshell Engine*. This mainly detects spam based on whether:

- The message or similar messages are sent in bulk.
- Most people want the message.
- Most people consider the message offensive.
- The message is formatted or sent so as to bypass anti-spam rules or to be economical for spammers.

The Mailshell SDK is a multithreaded development library that integrates the Mailshell Engine with any product or application. It provides development classes that communicate with the Mailshell Engine, and allows OEMs to choose between dozens of additional configuration options.

The Lite version of the SDK uses less than 200K of code. It resides on the device, creates fingerprints of each incoming message, and compares them to fingerprints in Mailshell's shared, remote databases. As with the full SDK, for each message, Mailshell returns a probability between 0% and 100% that the message is spam.

Customers include Broderbund, CyberGuard/Webwasher, Panda Software, Oracle, Stalker (CommuniGate Pro), Aladdin Systems, Truste, and others. Mailshell is based in Santa Clara, Calif.

Interesting Aspects of the Offering

- *OEM focus*. Unlike other OEM suppliers, Mailshell just sells to OEMs, and doesn't sell to end customers.
- *Focus on SDK*. The SDK was developed in-house and is extensively documented.
- *No channel conflict*. Because Mailshell doesn't sell to end customers, an OEM won't find its sales staff in competition with the firm. That's not true of most of the other OEM suppliers.
- *Established OEM business*. Mailshell has more than 20 clients.
- *Internationalization*. Mailshell has capabilities and filters for foreign languages, including date formatting and Asian double-byte character sets. Spam used to be primarily an English problem, but this is changing.
- *Mobile/small devices*. The Lite version of the SDK is for small and mobile devices. To keep the footprint small, the anti-spam signature database is either stored in the customer vendor's network, or on Mailshell's own systems. The Lite version is mainly used in desktop/remote routers, firewalls, and the like. Given the cost of mobile bandwidth, filtering spam on a mobile device, rather than upstream, makes little sense.

- *Platforms*. The Mailshell SDK is available for many platforms, namely, Linux, Solaris, FreeBSD, Mac OS X, Windows, Solaris (Sparc and Intel), and HP-UX. There are plug-ins for Outlook, Outlook Express, Exchange Server, Domino Server, and Sendmail.

- *Stability*. Mailshell is profitable and has never received venture financing. It is probably substantially more stable than many of its competitors.

In summary, Mailshell is a serious contender in the OEM space. Vendors looking for OEM anti-spam should definitely evaluate its offering.

Contacts

- Eytan Urbas, VP Marketing, +1 (415) 348-8728 x116, eytan@mailshell.com.

Authors: Lee Benjamin, David Ferris
Editor: David Ferris

Research Note Sponsored by Mailshell

Mailshell commissioned this document with full distribution rights. You may copy or freely reproduce this document provided you disclose authorship and sponsorship and include this notice. Ferris Research independently conducted all research for this document, retaining full editorial control. The purpose of this document is to describe the sponsor's offering and put it in its industry context. All products and services have their weaknesses, and those of Mailshell are not discussed in this document.

Ferris Research

Ferris Research is a market research firm specializing in messaging and collaborative technologies. We provide business, market, and technical intelligence to vendors and corporate IT managers worldwide with analysts located in North America, Europe, and Asia/Pacific.

To help clients track the technology and spot important developments, Ferris publishes reports, white papers, bulletins, and a news wire; organizes conferences and surveys; and provides customized consulting. In business since 1991, we enjoy an international reputation as the leading firm in our field, and have by far the largest and most experienced research team covering messaging and collaboration.

Ferris Research is located at 408 Columbus Ave., Suite 1, San Francisco, Calif. 94133, USA. For more information, visit www.ferris.com or call +1 (415) 986-1414.

The Ferris Research User Panel

The User Panel consists of IT professionals who work with messaging and collaborative technologies, providing services to their organizations' users. People join to share experiences with other people like themselves, learn from each other, and keep current on news and trends.

If you provide technical support for an email system, and you are not a member of the User Panel, you can join and learn more about the User Panel at www.ferris.com/url/userpanel.html. There is no charge to join.

Recent Reports From Ferris Research

Spam: Corporate Practices and Priorities in 2004
Email Records Management Survey: Guidelines, Technologies, and Trends
New Trends in Spam
The Impact of CAN-SPAM on Legitimate Direct Marketers
Upgrading From Exchange 5.5 to 2003: A Financial Case Study
Bonded Sender: A Program for Legitimate Emailers
Gwava and GroupWise Security
Spim: Spam Over Instant Messaging
Gmail: Google's Entry Into the Webmail Market
Microsoft Tech-Ed 2004: A Messaging Perspective
The Cost of Migrating From Exchange 5.5 to Exchange 2003
Exchange Server Reliability
Electronic Privacy and Security Regulations
A Survey of Exchange Installations: Key Statistics
CIO Messaging Concerns and Priorities
Recent Innovations in Macintosh Collaboration
FrontBridge TrueProtect Email Boundary Security Service
Cloudmark's Spam "Immune System": Fighting Spam With Genetic Algorithms
The State of Email Denial-of-Service Attacks
Instant Messaging: Current Status, Key Trends
How Not To Be a Spammer – Updates
The Growing Threat of Questionable Patents
Bayesian Filters for Spam Control
Another Alternative to Exchange Servers at Branch Sites
Lotusphere 2004
TCP/IP Bandwidth Shaping as an Anti-Spam Measure
URL-Based Spam Filtering
Reputation and Spam Control
Are Spam Laws Working?
Microsoft's Caller ID for Email Proposal
LinuxWorld NY 2004: A Messaging Perspective
Update on IBM/Lotus Workplace
TotalBlock: New Challenge/Response Anti-Spam Technology
Microsoft Exchange Edge Services
Exchange 5.5 Migrations: Issues and Best Practices
How Not To Be Seen as a Spammer
Notes/Domino 4/5 to 6 Migrations: Issues and Best Practices
Email Migration Costs

October 2004. Report #508