

## I D C V E N D O R S P O T L I G H T

---

### Defeating Spam, Spyware and Spoofs Through Positive Authentication

November 2006

By: Chris Christiansen, Program Vice President, Security Products, and Services, and Laurie Seymour, Contributing Analyst

Adapted from *Worldwide Secure Content Management 2005-2009 Forecast Update and 2004 Vendor Shares: Spyware, Spam and Malicious Code Continue to Wreak Havoc*, by Brian E. Burke and Rose Ryan, IDC Doc #34023

Sponsored by: BoxSentry

---

*Enterprises struggle with the deluge of external and now internal threats to their networks. From spam to inappropriate Web browsing to spyware and key loggers, there is a deluge of threats directed at the enterprise. Blacklists and content filtering are becoming less and less effective. Positive Email Authentication, a somewhat different approach, reduces the odds from overwhelming to manageable.*

*In this IDC Vendor Spotlight, we look at Positive Email Authentication as a viable alternative or addition to the enterprise's current secure content management solution. We also explore the benefits and challenges of the role of BoxSentry's product, RealMail .*

### Spam/Spyware Onslaught Threatens to Overwhelm Enterprises

Enterprises struggle to stay ahead of spam, spyware and phishing. These threats infiltrate the organization, capture personal data, and expose confidential information about users and the organization. This puts the enterprise at risk for potential compliance violations of regulations such as Graham-Leach-Bliley Act, HIPAA, or Sarbanes-Oxley. The effects of these threats on the organization, such as theft of confidential information, reduction of bandwidth, impact to employee productivity, damage to corporate desktops, and increasing help desk burdens are forcing enterprises to take action.

As IT locks down networks with blacklists and content filters, user communication often becomes collateral damage. Increased use of blacklists and filters heightens the chance that legitimate email never makes it to the intended recipients. For non-English users, email from international businesses may be obstructed by exuberant blacklists. Once an enterprise is on a blacklist it can be exceedingly difficult to change its status, especially if English is not the enterprise's first language. The conflict between the need to protect the business from growing threats and the business' need to communicate effectively with customers and vendors must be reduced.

Global business is increasingly multilingual, yet many of the current spam/spyware/phishing tools are incapable of rising to the challenge. Content filters do not always have the sophistication to differentiate between legitimate non-English language email and spam. This problem is compounded as spam itself becomes more multilingual, making it even more difficult to separate good from bad mail. To complicate things further, very few spam/spyware tools are capable of processing multi-byte and Asian characters (such as Chinese, Japanese, Korean and Thai). Global businesses use multiple languages and multi-byte characters to communicate and, as such, security tools should address this need.

## **Positive Email Authentication Increases Communication and Protects Networks**

If blacklists and content filters are now creating new problems, then perhaps the new answer is positive authentication. Positive Email Authentication differs from blacklists and content filters because the philosophy is based on presuming the email is "innocent" before it is determined to be "guilty." With blacklists and content filters, all email is presumed guilty. Therefore, legitimate email is often blacklisted for the greater good of protecting the business. However, missing legitimate communications with vendors and customers is not good for the enterprise. IDC believes that while false positives are less than 5% of all email caught, even missing one crucial email could be devastating for business. One of the biggest benefits from using positive authentication is increased reliability of communication with customers and vendors, while keeping the spam, spyware, and spoofs out.

Positive authentication is best accomplished through a platform that integrates "accept" lists and complementary heuristics. Accept lists work by automatically passing through any email from a recognized sender or domain. These emails are assumed to be trusted and are expedited through the security system to their destination. This method significantly reduces, if not eliminates, the false positives caused by traditional content filters and blacklisting methods.

If a sender is not recognized, then a challenge is issued to the sender for self-authentication. Multi-language and multi-byte character support plays a key role in ensuring that the sender can respond in a timely manner, in their own language, and using a familiar (i.e., non-English) character set. Challenges from some security solutions are sent back in English only — the predominant language of most secure content management tools. However, if the challenge is sent back in both English and the native language of the sender, then the sender has much greater chance of correctly responding to the challenge and consequently having their email delivered.

Following the initial accept lists, advanced heuristics should review and eliminate non-authenticated email that is obviously spam, spyware or spoofs. Any remaining non-authenticated email not positively identified as spam should be put into quarantine for the user to either accept or refuse. The use of multi-linguistic and multi-byte character processing into the heuristics allows the enterprise to better identify the spam and spyware coming in with multiple languages that are often overlooked by conventional content filters and blacklists. Each step in this process reduces the likelihood of false positives while increasing the level of security and protection from network-based threats.

Phishing and spoofing attacks can also be well contained with positive authentication. When email is allowed into the network based only on its authenticated legitimacy, then phishing and spoofing email that may otherwise slip by content filters and conventional spam tools is much more likely to be identified and called out. Reducing phishing and spoofs is hugely important since more and more enterprises are subject to privacy and other regulations.

## **Market Trends and Considerations**

The secure content management market has shown very strong growth over the last several years. Viruses, spyware, spam and all manners of external and internal threats are driving the continued increase in the market year over year. IDC estimates the secure content management market will grow from US\$4.5 billion in 2004 to US\$10.5 billion in 2009. This represents an 18.7% compound annual growth rate (CAGR). Messaging security is second only to antispyware growth (30.9% and 45.9%, respectively) during the forecast period.

While viruses are still a major concern for organizations, it is spyware that is becoming a security and system management nightmare. IDC believes that more than three quarters of all corporate machines are infected with various forms of spyware. Given so many of the new and increasingly strict regulations affecting corporations, the idea of having spyware running rampant through their systems causes significant alarm for IT departments and their executives.

On the heels of spyware is spam; the bandwidth killing timewaster is crawling back up the ladder of importance once again. Email phishing attacks are now daily occurrences for any organization, especially the larger financial institutions and their customers. The convenience of email is drastically reduced by the oppressiveness of spam and phishing. IDC believes that zombie machines are taking over the distribution of spam, and that the vast majority of spam today is delivered through zombies unbeknownst to the senders.

Another major driver is threats arising from inside the organization. Employees, whether intentionally or not, are distributing confidential and sometimes personal and private information outside of the organization. This is a major problem for enterprises subject to privacy and protection laws. Many corporations are using OCC (outbound content compliance) to restrict the content that employees can send in/out/around their firms. Enterprise rights management (ERM) is another growing solution to limit exposure of sensitive data. ERM provides encryption-based solutions for enforcing corporate digital content use and access policies throughout the information lifecycle.

Finally, Web filtering has evolved from addressing a single class of employee distractions — access to inappropriate URLs — to more comprehensive Web security solutions that address a wide array of Web-based threats. Filtering has grown dramatically as website distributing spyware has increased explosively. The increasing number of new and poorly educated Internet users means that many spammers are being driven toward money hungry hackers and crackers looking to make an easy buck through spyware, phishing and Web browser vulnerabilities.

These trends continue driving growth in the secure content management market as enterprises struggle to find the right answers to their problems.

## **Profile of BoxSentry**

BoxSentry is headquartered in Singapore with offices in London, England, and Sydney, Australia. The firm began development on RealMail three years ago when the management team recognized that spam is no longer English-centric problem. In response, the team created technology focusing on the idea that email is a critical communication tool and that enterprises must be assured that legitimate email is received. BoxSentry's RealMail product addresses the concerns of the enterprise relating to communicating with customer and vendors in an expedient and reliable way.

BoxSentry's RealMail product is the recipient of a number of innovation awards: the Australian IT innovation awards, 2005, and Microsoft's Consensus Software awards, 2006. Version 2.0 is currently in production with new versions on a rapid release schedule. BoxSentry was spun out of WebGenie Software, and is privately held by Greenoak Capital Partners.

### ***Attributes and Strengths***

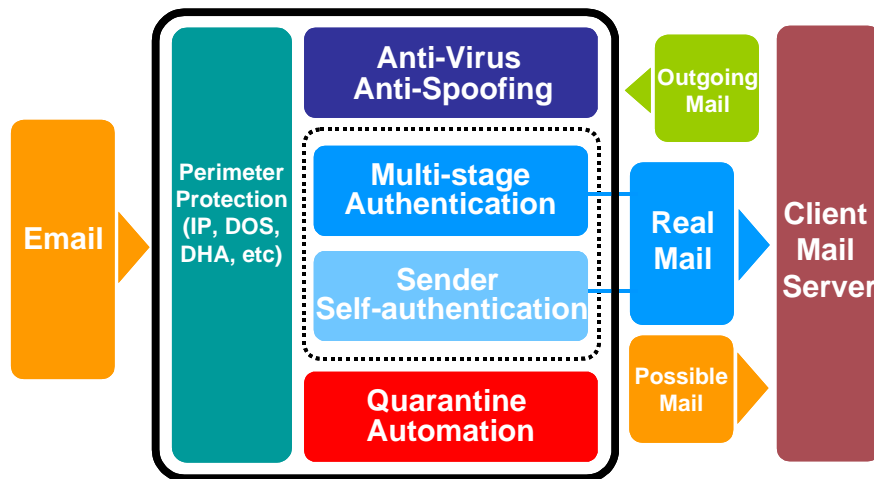
BoxSentry's RealMail provides a positive email authentication, multi-lingual, multi-byte character capable solution for effectively separating legitimate email from spam and spyware. RealMail has a patent-pending heuristic method based on artificial intelligence principles to ensure that critical emails are delivered appropriately. This protects legitimate emails from being caught as "false positives," yet still protects the organization from unwanted threats of spam, spyware, and spoofs.

As language barriers are a leading cause for communication consternation in global businesses, RealMail has focused on providing its solution in over 20 languages, including double-byte and Asian character languages such as Chinese, Japanese, Korean and Thai. This language flexibility benefits users, but it also helps the administrators because they can manage email security in their own native language. Multiple languages and Asian language support greatly increases the application's ability to distinguish spam from legitimate email and reduces false positives.

RealMail's multi-tier protection offers the enterprise flexibility and expediency in ensuring delivery of legitimate email (see Figure 1). After virus and spyware scans, pre-authenticated emails are delivered to the user immediately. Because viruses and spam are removed at the server level, it reduces network bandwidth by eliminating many of the threats before they reach the corporate network. Even if a virus comes from a trusted source, it is eliminated instead of being sent to the user. The user then receives a note stating that an email from a trusted source was deleted.

**Figure 1**

BoxSentry's RealMail Secure Messaging Solution



Source: BoxSentry and IDC, 2006

Unauthorized mail is checked against pre-authentication rules and third-party trusted authentication sources. It is reviewed by heuristics and those that can be positively identified as spam are suppressed. For email assessed as "likely to be genuine," RealMail generates a single challenge email that is automatically sent in both the sender's native language as well as English. This email requests the sender to self-authenticate. The sender can respond to the challenge in English or native language. RealMail's Send Self-Authentication (as illustrated in Figure 1) expedites the authentication process. Also, it eliminates confusion and miscommunication due to language barriers. Once authenticated, all further email from the sender will be expedited.

A further layer of heuristics is then applied to the remaining email to positively identify spam. Based on RealMail's heuristic algorithms, it is able to identify and stop spam in over 20 different languages. Any remaining email not positively identified as spam is quarantined. Where there is a chance that the email may be legitimate, the user is automatically notified and asked if they wish to review or receive the email from the unknown sender. Users can accept the mail with a "one click" release mechanism. Through staged segmentation of email utilizing its positive authentication platform and heuristics technology, and with its combination of authentication mechanisms, RealMail seeks to reduce mail volumes so as to improve network efficiency, enhance user productivity, reduce IT administration, and protect genuine business communications.

BoxSentry's RealMail does not just do its job alone. Available either as an appliance or a managed service, it is modular and integrates well with other security technologies. A key feature of RealMail is its flexibility. It can complement a customer's existing solution's architecture as either an integrated part of the architecture or run along side of it, or can be a complete standalone solution. In addition, customers can choose to integrate RealMail with their current antispam/antivirus engines. Recent product developments mean that RealMail can now sit ahead of the existing antispam/antivirus service, acting exclusively as an Email Authentication System, governed by the customer's pre-assigned rules. Thus, customers can continue to use their existing engines to filter email independent of RealMail, with no need to displace their incumbent vendor's products unless they choose to do so. In this way, RealMail becomes a new, value-adding component to an overall multi-layered approach to email security.

Installing RealMail is a straightforward task. With a minor amount of set-up, including language selection and importing of accept list, the tool is up and ready to use within a few hours. Accept lists are easily generated through the import of existing lists of addresses, and bolstered by industry reputation lists. Once loaded, the accept lists are automatically maintained based on the user's email behavior. They are built upon one of the most basic assumptions: that any outgoing mail recipient is added to the sender's accept list.

### ***Challenges and Opportunities***

While BoxSentry offers significant benefits, it also faces some challenges:

- **BoxSentry is a relatively new player in the market and will need to improve market awareness.** BoxSentry is working closely with local security companies in different countries and plans to partner with OEMs and others in order to expand product awareness and channels.
- **IT is suspicious of challenge and response email security.** The RealMail platform enables the challenge and response layer to be used by the administrator on an optional basis. BoxSentry will need to emphasize the benefits in reduced mail volume, simpler administration, reduction in malware, and prevention of false positives. Although to date challenge and response has been unpopular, IDC believes it will increasingly become a more important part for protecting the network.
- **BoxSentry may face resistance to their philosophy that email is innocent until proven guilty.** It is a big shift in thinking to move from restricting email based on it being "bad" to evaluating email based on the presumption that it is "good." As most organizations' strategies are based on keeping out the bad, BoxSentry will need to work hard to ultimately prove that a different approach has equal, if not more, value than what is considered conventional practice. However, it is exactly this type of challenge that could make RealMail shine.

### **Conclusion**

It is well known that spam, spyware, and phishing/spoofing are accelerating enterprise problems. Conventional tools based on culling known threats are becoming less effective as the frequency of new blended attacks increases almost daily. Positive authentication methods are a potential solution to this problem, and represent a new category of email security solution.

By working to identify trusted senders and emails, the technology spends its time and resources delivering good mail to recipients, ensuring unknown messages are properly authenticated, and enabling users to take control of their own email. This allows the system to focus on ensuring that communication between the sender and receiver is protected and expedient.

A solution such as BoxSentry's RealMail is an eloquent way to address the challenges enterprises face in protecting communications with vendors and customers, particularly with global business operating in multiple languages. Its language capability and flexibility means RealMail should make a robust addition to an already established solution, or a complete solution on its own. If BoxSentry continues upon the development path it has taken, then RealMail should thrive and grow in the secure content marketplace.

---

#### A B O U T T H I S P U B L I C A T I O N

This publication was produced by IDC Go-to-Market Services, Asia/Pacific. The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis independently conducted and published by IDC, unless specific vendor sponsorship is noted. IDC Go-to-Market Services makes IDC content available in a wide range of formats for distribution by various companies. A license to distribute IDC content does not imply endorsement of nor opinion on the licensee.

#### C O P Y R I G H T A N D R E S T R I C T I O N S

Any IDC information or reference to IDC that is to be used in advertising, press releases, or promotional materials requires prior written approval from IDC. For permission requests contact the GMS information line at +65.6829.7749 or gmsap@idc.com. Translation and/or localization of this document require an additional license from IDC. For more information on IDC visit [www.idc.com](http://www.idc.com). For more information on IDC GMS visit [www.idc.com/gms](http://www.idc.com/gms).

Global Headquarters: 5 Speen Street Framingham, MA 01701 USA P.508.872.8200 F.508.935.4015 [www.idc.com](http://www.idc.com)

Copyright 2006 IDC. Reproduction without written permission is completely forbidden.