EMA Radar™ for Hosted Message Security Services: Q2 2011

Report Summary and Websense Profile

By Scott Crawford, Managing Research Director
Enterprise Management Associates (EMA)

June 2011

EMA Radar™ for Hosted Message Security Services: Q2 2011 (Report Summary and Websense Profile)

Table of Contents

EMA Radar™ for Hosted Message Security Services: Q2 2011 (Report Summary and Websense Profile)

Executive Summary

In 2010, Enterprise Management Associates (EMA) published *Security as a Service*, a research report examining the expansion of managed and professional IT security services, as well as the growth in what the report called "Security SaaS" or hosted security technologies. This report captured the appeal of hosted technologies that offer a number of advantages over on-premises approaches. In exchange for a predictable subscription, hosted approaches allow businesses to offload many of the burdens of security technology deployment and maintenance and the demands of keeping up with a dynamic threat environment. Hosted services also combine economies of scale with the centralization of much-needed security expertise, giving hundreds or thousands of businesses access to knowledge that can be difficult to find and retain.

In the 2010 *Security as a Service* report, the segment of the hosted security technology market showing the highest growth in use was one of the longest-established domains in the field – Hosted Message Security (HMS) services. These services filter out the enormous volumes of messages, mostly email, that burden organizations with unwanted spam and bring potentially malicious threats directly into the business. Today, they embrace a number of additional functionalities, from filtration of *outbound* messages that pose a business risk, to filtration of message-borne Web content, message encryption, archiving and email continuity services. HMS services also complement on-premises message security technologies when deployed in "hybrid" modes that enable organizations to take advantage of the combination that best suits their needs.

With the acquisition of a number of HMS leaders by major vendors over the last several years, the HMS landscape has entered the mainstream of vendor offerings for both the Small- to Medium-sized Business (SMB) and the enterprise. Today, HMS has become an important function of messaging, for businesses as well as for those who offer a broader range of hosted technologies such as hosted email services. It has become a well-established market that continues to show significant growth, making HMS an anchor for "Security as a Service" initiatives among a number of leading vendors, and deserves attention for the fuel it provides for the continued expansion of these initiatives in other domains.

In this EMA Radar Report, EMA evaluates nine of the leading vendors in Hosted Message Security services, for the value they offer both large enterprises and small-to-mid-sized organizations. Evaluations were conducted according to extensive criteria in Functionality, Deployment and Administration, Architecture and Integration, Cost Advantage, and Vendor Strength, giving prospective customers a wide- ranging view of leaders in this market, from those who excel in serving the enterprise, to those who offer high value to small and large organizations alike.

Introduction and Methodology

In the development of this Radar Report, EMA engaged nine top providers of Hosted Message Security solutions in a detailed analysis of the scope and capabilities of their offerings. All serve enterprise customers, but the spectrum of vendors researched is broad, from those with an extensive base of SMBs, to those whose offerings are part of the vendor's larger initiatives to provide a suite of services. Many also offer hosted messaging systems and solutions for message archiving, Web and data security. Still others offer office productivity solutions delivered "from the Cloud" and managed security services. While each vendor's range of capabilities in these other areas factor into its evaluation, hosted technologies available as standalone solutions for both inbound and outbound

filtering of messages for spam and management of multiple security risks are the central focus of this report. Because attackers can use messages to engage multiple vectors, such as links to malicious Web sites, in exploiting their targets, the report also considers the ways that message security has grown beyond email filtration alone. HMS solution providers covered in the report are: AppRiver, Google, McAfee, Microsoft, Mimecast, Perimeter E-Security and its USA.NET division, Proofpoint, Symantec and Websense.

The research for this report took an analytical approach, first determining the characteristics of an ideal HMS solution and then identifying candidate vendors based on EMA's knowledge of the market and feedback from IT customers. EMA then approached each vendor for an introductory overview of its HMS offerings. Each vendor that was selected for inclusion in the report was then asked to complete a survey that contained questions aimed at providing a quantitative and qualitative way for EMA to compare each vendor offering against its peers in a number of key areas, including Deployment and Administration, Cost Advantage, Architecture and Integration, Functionality and Vendor Strength.

An extensive survey questionnaire was developed and presented to solution providers for their input. EMA supplemented responses with dialog, product demonstrations, customer interviews and hands-on experience with offerings to ensure that each solution was represented fully, honestly, and fairly. After the surveys were completed, responses were collated and analyzed by EMA, which, along with actual experience with the vendor's offerings either in terms of hands-on evaluations, vendor demonstrations or both, yielded the final scoring contained later in this report. Finally, and importantly, EMA leveraged ongoing industry dialogs and extensive existing knowledge of the solution space to evaluate, consider, and validate each vendor's strengths and limitations in a manner that is focused on providing balanced, consistent insights across all vendors and solutions researched.

EMA has produced a report specially targeted at presenting and explaining Radar Reports in general: *How to Use the EMA Radar Report*, EMA, April 2010. The goal is to use a combined approach for quantitatively and qualitatively evaluating providers of solutions in a particular IT management functional area and presenting their relative differences in a clear, graphical format. Also included is a detailed discussion of individual criteria and how each participating solution provider rated versus those criteria.

EMA Radar™ for Hosted Message Security Services: Q2 2011 (Report Summary and Websense Profile)

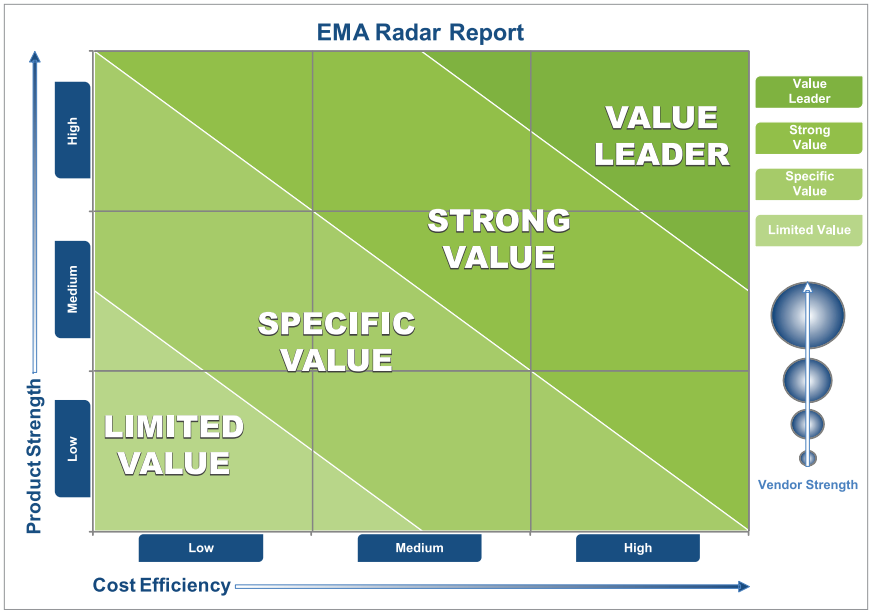


Figure 1: The EMA Radar is optimized to show how vendor solutions cluster in terms of two primary axes: Vendor Strength (architecture, integration, functionality) and Cost Efficiency (ease of administration, deployment, support & services, costs advantage)

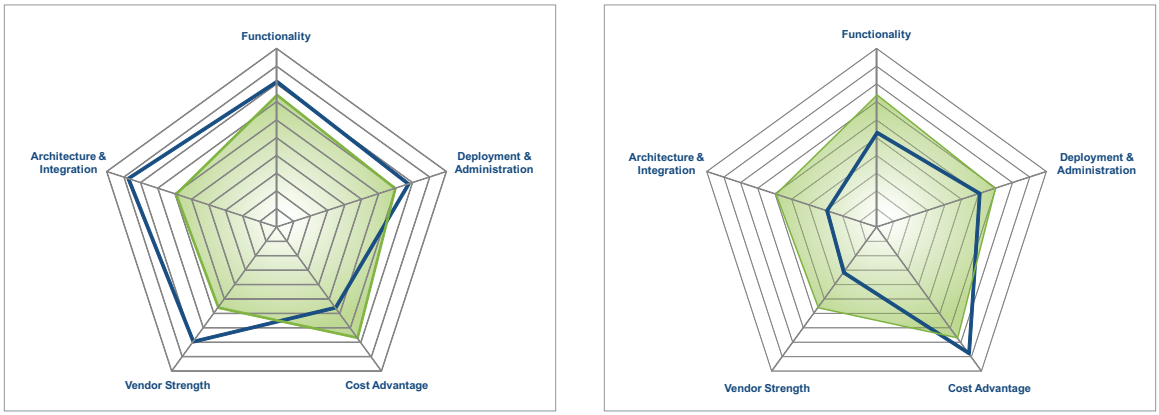


Figure 2: Radars for each vendor solution are included in the full report and show a five-axis contrast between the average profile and the vendor in question.

Quoting from *How to Use the EMA Radar Report*, "No analysis of this type can tell you which vendor is best for you. The data collected for an EMA Radar Report can certainly be used to make that determination, but it must be applied to the specifics of your current environment, level of maturity, and goals and priorities. Since the authors of any given Radar Report do not have your unique specifics, the Radar Report can only be a starting place and a guideline. It can inform you of the market and short-cut your process to developing a short list."

Why Focus Only on the Hosted Segment of Message Security Solutions?

The market of solutions for taming spam and defending businesses against message-borne threats includes leaders who dominate in on-premises as well as hosted technologies. Why focus a market assessment on just the hosted segment of the space?

The primary reason is the continued growth in hosted IT services in general, and hosted security services in particular, that deserve attention for the aspects of vendor evaluation unique to a hosted approach. On-premises solutions require a substantial commitment from the business for technology acquisition, expertise and support in deployment and operations. Many of these burdens are alleviated by hosted services – but the shift to a service provider requires a focus on aspects such as Service Level Agreements (SLAs) for availability and performance to assure the delivery of services expected.

In addition, when customers shift critical capability to a service provider (and few capabilities are as critical to *any* business as messaging), they need assurance of the provider's commitment to customer satisfaction and maintenance of a strong service offering going forward. Hence, indicators of well-established vendor strength and reliability become even more significant, while customer retention speaks to the ability of service providers to consistently satisfy customer expectations over time.

One of the most significant reasons for focusing on Hosted Message Security, however, is that its success has become a center of gravity for the ongoing expansion of "Security as a Service." The established market space of HMS and its continued growth have become foundational to the ambitions of a number of vendors who seek to extend leadership in Hosted Message Security into dominance of other aspects of security services that may well play a significant role in the evolution of what IT security will become. Vendors identified as leaders in this study, therefore, should be expected to play a leadership role in that evolution as well, and should be watched accordingly.

Those profiled in this EMA Radar who also offer on-premises technology are highlighted if they offer "hybrid" solutions that give customers a range of options for on-premises, hosted, or blended approaches – but in this report, the assessment is from the point of view of enhancing the value of *Hosted* Message Security, rather than seeing HMS as an add-on to on-premises offerings.

The Hosted Message Security Landscape

Ask any user of Internet technologies to name the top annoyance that prevents them from being able to conduct personal and business affairs effectively, and they will almost certainly describe the burden of dealing with unwanted email messages, or spam. Not only does the management of unwanted messages act as a productivity tax on users, the messages themselves pose a substantial threat to user and business security and data integrity.

The first spam message is believed to have been sent in 1978 when a Digital Equipment Corporation employee sent an unsolicited message to several hundred ARPANET recipients advertising the availability of a new computer model.[1] Unsolicited messages were not a real issue, however, until the

[1] http://www.newscientist.com/article/dn13777-happy-spamiversary-spam-reaches-30.html

emergence of inexpensive, standards-based, Internet-connected messaging systems in the mid-1990s. The convergence of Web technologies with messaging systems and HTML-formatted email further broadened the spectrum of risk.

Rapid increases in the availability of fast, inexpensive Internet connectivity, coupled with an explosion in the number of people with email addresses created low barriers of entry for spammers, who make money by enticing people to click on embedded email attachments and Web links for the purpose of advertising products, spreading computer viruses, spyware and other malware, and stealing user identities (phishing) to further criminal enterprises. Since the cost of sending spam is virtually zero, even a very low "hit rate" from spam can generate considerable profits. In addition to email spam, other unsolicited messages have emerged in virtually every form of online media, including instant messages, blogs, Web sites, and even mobile device text messages.

Even with attempts to legislate spam out of existence, including highly publicized awards and fines levied against convicted spammers, spam comprises over 80% of all email messages today, and according to Symantec's February 2011 *MessageLabs Intelligence* report, one in every 290.1 messages is malicious.[2] Spam costs organizations billions of dollars a year in terms of lost user productivity, wasted network bandwidth, server processing time, and IT resources wasted dealing with virus removal and other security incidents.

Message security technologies date back almost as long as messaging technologies themselves, and have long played a leading role in the ongoing war between the "white hats," legitimate owners and users, and "black hats," criminals that seek to obtain material gain by tricking users into giving them money, revealing personal data, or, in recent years, coercing an unwitting user into executing a threat that could take over the user's system or give the attacker privileged access to sensitive information assets. The quantity and complexity of spam and malicious messages has reached the point where users without message security can spend hours managing their email every day. In a business setting, this translates into thousands of hours of lost productivity every year, not to mention substantial increases in risk.

The first generation of message security solutions focused primarily on detecting spam, generally by installing PC-based software that scanned and identified spam messages as they were received by the endpoint, moving them into a separate folder for review. First attempts used "blacklisting" and "whitelisting," which were simple lists of known spammers and known legitimate senders (respectively). Messages from senders not on the whitelist, along with messages from known spammers, were automatically flagged and moved into a special spam folder.

The second generation of solutions added to whitelisting and blacklisting by leveraging text scanning algorithms such as Bayesian techniques that examined the entire message looking for key characteristics including misspelled words and grammatical errors. If a legitimate message was accidentally marked as spam (a false positive), or if an actual spam message passed through the filter and wound up in the user's inbox (a false negative), users could flag messages as such, and the system would attempt to learn from its mistakes.

These mechanisms proved relatively effective for a while, until spammers figured out ways to effectively circumvent them, generally by improving the structure and grammar used in the messages, coupled with sender address "spoofing," which made messages appear to originate from legitimate senders. It became evident that installing and maintaining message security software on every user PC was not

[2] http://www.messagelabs.com/mlireport/MLI_2011_02_February_FINAL-en.PDF

adequate from the perspectives of high maintenance costs, increased PC and network overhead, and the requirement to rapidly update detection algorithms.

Subsequent generations of message security moved detection and remediation logic to the messaging server or a standalone appliance or software gateway, typically located on-premises. This simplified the process somewhat from an end-user perspective, but still required frequent updates, onsite care-and-feeding and a substantial customer investment. The emergence of Software-as-a-Service (SaaS) techniques held considerable promise for relieving businesses of many of these burdens – and Hosted Message Security became a textbook example of the success of a SaaS approach.

As described in the 2010 *Security as a Service* EMA research report, the most successful hosted security technologies have two primary traits in common: they lend themselves to outsourcing because they are already largely externalized, and they pose no critical dependencies that cannot be readily resolved. Hosted Message Security meets both these tests. They filter messages that are already moving from, or to, external networks, and critical dependency risks can be mitigated by continuity services (which, in essence, are simply just another messaging relay service). These factors have spurred the success of the HMS market in particular, giving it a strong position as a center of gravity for the still-expanding realm of "Security as a Service."

Today, the quantity and sophistication of malicious messages continues to increase daily. Social engineering techniques, which attempt to trick users into clicking on malicious file attachments or giving up personal data (known as "phishing") are also on the increase, along with threats that combine multiple vectors such as a URL that downloads malicious content to the user's computer. In order to effectively combat these risks, multi-vector defenses were developed that combined antivirus (often using more than one vendor's AV engine), adaptive heuristics, whitelisting, blacklisting, file reputation and Web reputation services.

HMS solutions have many intrinsic benefits. They generally require organizations to change their Internet Mail Exchange (or MX) records so that inbound email flows first through the HMS servers, where scanning and filtration take place. Since only legitimate messages are transmitted to the HMS customer, substantial bandwidth is saved and risk is reduced. In addition, customer costs are reduced since no messaging infrastructure is required and the vast majority of message security tasks are performed by the service provider.

When architected correctly using a highly adaptable, scalable, real-time platform, updates can be distributed in minutes in response to emerging "zero-day" threats – providing protection ideally within hours if not minutes when new security issues emerge. HMS solutions are generally rapidly deployed and easily managed via a centralized, Web-based management console, reducing administrative overhead. And, since HMS solutions are also typically priced on a subscription basis, the purchasing and budgeting process is simplified.

The current state-of-the-art in HMS adds outbound message security to the inbound solution, providing the ability to scan messages being sent from the organization. The benefits of this approach are many, including ensuring that employees are not inadvertently sending spam messages and ensuring that sensitive corporate data is not being transmitted via email. The latter is an aspect of Data Loss Prevention (DLP), a capability increasingly seen in HMS solutions, considering their central role in communications and information sharing. Some vendors require a physical server or appliance located

at the customer premises so that scanning can take place before sensitive data crosses the corporate firewall. This is an aspect of what EMA defines as *hybrid message security*, where components for either inbound or outbound filtration (or both) are located both in the Cloud as well as on-premises. It should be noted that fully Cloud-based outbound security approaches can also be highly secure, so EMA does not consider an on-premise component an absolute requirement.

Assessing the Hosted Message Security Market

Today's message security challenges are daunting. The necessity of scanning virtually every message transmitted in or out of an organization for sensitive or explicit content, malicious file attachments and URLs, coupled with the rapid advance of sophisticated malware attacks, has resulted in the need for a robust, multi-vector defense.

The advent of hosted message security solutions, combining state-of-the-art security technologies into a centralized hosted service that can be deployed in anywhere, from minutes to days depending on the customer's scope of coverage, represented a significant leap forward. Today's HMS solutions serve as the first point of contact for inbound and, increasingly, outbound mail streams, processing all messages in the Cloud before sending them on to their destination. The ability to easily define centralized policies that apply to the entire messaging stream is also a key advantage.

Typical hosted message security services include the following features:

- Spam identification: Highly accurate spam and malicious message detection with accuracy equal to or greater than 99%, with ability to place suspect messages in quarantine so that users and administrators can review messages if needed.
- Virus and malware scanning: Automated scanning of all messages and attachments. Some vendors offer multi-engine AV scanning as well as the ability to perform deep attachment scans, including multiple file types and nested zip files.
- Reputation services: Adds file, user and Web reputation services to message scanning. Detects known threats embedded in messages, including blended threats, malevolent URLs, known spammers and malicious file attachments.
- Policy definition and enforcement: Ability to define and apply fine-grained policies on inbound and outbound messages, at global, group and even individual user levels.

In addition, the following services may also be offered:

- Message encryption: Encrypts messages both at rest and in transit. Preferably allows end-user message decryption via a number of mechanisms, including Web interface or email client plug-in, for example.
- Disaster recovery and message spooling: The ability to spool messages at the service provider in the event that the customer's messaging server(s) become unavailable. This provides messaging continuity in the event of disaster and connectivity issues. These features also allow messaging servers to be taken offline for maintenance without worrying about missed or bounced messages.
- Message archiving and e-discovery: The ability to store all messages on a long-term basis (generally up to 10 years) for backup and to support e-discovery. Speed and flexibility of archive searches are key considerations, since 10 years of message data can add up to a very large data set.

- Protection from malicious Web content: This is becoming one of the most significant realms of technology to be closely aligned with HMS, owing largely to the convergence of Web technologies and messaging. Most popular email clients have supported HTML-formatted mail for some time, but the increased use of Web-based platforms for collaboration and social networking as well as for messaging, office productivity and popular SaaS services heighten the need for alignment between these technologies.
- Data Loss Prevention (DLP): The ability to define policies that detect potentially sensitive data inside of messages (typically outbound), prevent them from being transmitted, and notify appropriate personnel. Examples of sensitive data include specific files, keywords, and personally identifiable data such as a national identity number. DLP should support the definition of policies at varying levels of granularity, and providing pre-built policies for specific compliance regulations is a plus.
- Hosted Mail Transport Agent (MTA): Provides a full turnkey messaging solution that requires zero on-site hardware.

The HMS market was pioneered by a number of startup companies that realized the market potential early on, including BlackSpider, FrontBridge, Postini, Proofpoint, MessageLabs, Mimecast, MX Logic and ScanSafe, to name but a few. As these upstarts gained traction in the market, many were rapidly acquired by larger security vendors seeking to add HMS capabilities to their existing portfolio. This included Microsoft (FrontBridge), Google (Postini), Symantec (MessageLabs) and McAfee (MX Logic). While a number of the industry pioneers are now a part of much larger organizations, several remain viable, independent vendors, including Mimecast and Proofpoint. There are also companies like Perimeter E-Security, and its USA.NET division, which represents the recent combination of two companies, one with leadership in managed security services, and another that has been a provider of hosted message security services for many years. This exemplifies how current "Security as a Service" trends often manifest in intersections of hosted technologies and providers of managed services and professional expertise.

Criteria

Anyone that has attempted to evaluate HMS solutions will be quick to note that this is a crowded market with many vendors that seem to offer very similar functionality. This is typically the case with technologies that have matured to the point where they have reached general acceptance in the market, and message security has clearly reached that point. Even so, there are many key characteristics that, when compared amongst various leading vendors, do yield differentiators.

In all EMA Radar Reports, EMA evaluates solutions based on five key areas: *Deployment and Administration, Cost Advantage, Architecture and Integration, Functionality* and *Vendor Strength*. The last category, perhaps the only one that is not self-explanatory, is focused on the market and industry presence, vision, and financial stability of the vendor. In each of the evaluation areas, EMA created a "superset" of capabilities spanning the known solutions in the marketplace, added questions about new and emerging areas, and balanced the result with standard comparators used across all EMA Radar Report projects.

The evaluation model used for this Radar Report on Hosted Message Security is presented as Figure 3.

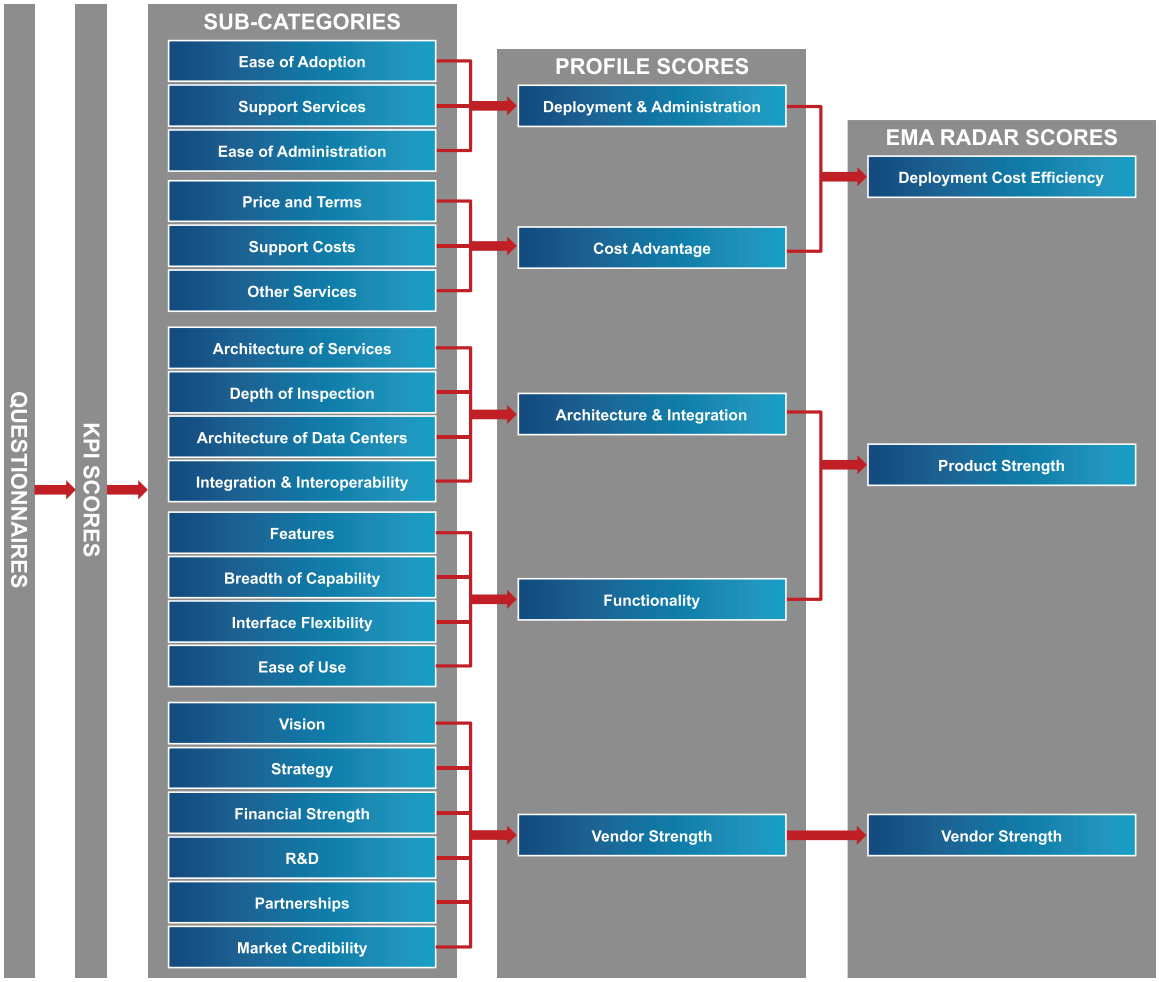


Figure 3: Assessment model for the EMA Radar for HMS

EMA has designed its Radar Reports to assist end users in the selection of IT management products and services. It is fundamental and critical that the reader understand this is a starting point for an in-depth evaluation, rather than a finishing point. There is neither a single set of characteristics nor any single solution that will satisfy all end users.

The EMA HMS Radar Report grades solutions on a broad set of criteria. The reader's task is to find the criteria that matter the most and select those vendors that scored best in those criteria. As guidance, EMA has assigned a Profile Score to the solutions across each of five main categories. Supplementing quantitative evaluation, EMA discusses offerings in detail in each vendor's individual profile included in this report.

Below are the key criteria used to evaluate HMS vendors against one another. In addition to being a leader in the market, the following inclusion and exclusion criteria were defined in order to determine viability for this research:

Inclusion Criteria

- Solution must offer message security capability as a hosted service, available independently of other hosted services, if any, that the vendor may offer (regardless whether integrated into or offered with other services such as hosted email), and providing, at a minimum, inbound message filtration via "cloud-based" technology.
- Solution must provide highly effective spam filtering with a high level of catch accuracy and low ratios of false positives and false negatives.
- Solution must provide multi-vector threat scanning, including detection of blended threats.
- Vendor maintains a significant portion of market share. At a minimum, vendors must support approximately 1 million end-user mailboxes and/or 2,000 customers throughout its services.
- Service must be quick and easy to deploy.
- Vendor is considered an industry thought leader.

Exclusion Criteria

- Does not provide its own HMS technology (regardless whether it provides other hosted or managed services, including managed or hosted email or third-party message security technologies).
- Vendor's HMS offering (or its acquisition(s) providing HMS services) has been in the market for less than one year prior to publication of this report.
- Does not maintain a high-level market presence or is not considered a market leader.
- Does not employ a significant research and development team.
- Lacks vendor vision, strategy and strength to be competitive in the EMA Radar evaluation.

Deployment and Administration

While a major advantage of the hosted delivery model is rapid deployment, there are still many tasks that must be performed in order to prepare for deployment, particularly since the HMS solution must typically be deployed alongside an existing messaging system. The duration and complexity of the HMS deployment and administration can vary widely by vendor, and for those organizations that wish to maximize their ROI, the following criteria must be considered:

- Account setup and provisioning process and speed.
- Licensing and billing options.
- On-site software or hardware required.
- Time required for initial deployment, differentiated by varying customer sizes.
- Professional services and training time required for a typical deployment.
- Variables that typically increase or decrease deployment time.
- Anticipated message flow and end-user disruption expected during the rollout, and ability to run the new HMS service in parallel with existing systems during initial deployment.

- The process for defining dashboards and reports.
- Quantity of ongoing administration required post-deployment.
- Support options provided (on-site, online, phone, etc.), and hours of support availability.
- Location of vendor support centers and languages supported.

Cost Advantage

Many organizations move to service-based offerings because they believe that they will save money over traditional on-premise solutions. To that end, evaluating the relative costs between vendors is an important criterion, and given two or more vendors that provide similar functionality, cost can be a key deciding factor. We asked each vendor to outline their pricing strategies at different levels such as per-user per-year (or per-month), by size of account, by agreement term, and so on. This measure is not an analysis of the Total Cost of Ownership (TCO) or Return On Investment (ROI), but it can be used as an objective guide to the relative cost between vendors.

Some of the cost criteria considered included:

- Pricing and licensing models.
- License terms such as length of contract.
- Flexibility to move from one pricing model to another.
- Maintenance costs above and beyond the basic purchase.
- Pricing and licensing for on-site hardware and software, if required.

Architecture and Integration

The architecture and integration capabilities of an HMS solution are key indicators of the vendor's overall strength and maturity. EMA evaluated the HMS vendors on a number of points, including the following:

- Overall system design
- Scalability (and ability to rapidly scale as needed)
- Resilience to failure and disaster recovery plans
- Certifications and industry guidance utilized, such as SAS 70 Type II, ISO 27001/27002, TIA-942, MSAP, and ITIL
- Anti-malware engine design philosophy (internally developed, licensed from others, or both, including multi-engine strategies)
- Integration and interoperability capabilities:
  - User directory services
  - Web content filtration
  - Data loss prevention
  - Instant messaging services
  - Collaboration systems
  - Security incident and event management (SIEM) systems
  - Open APIs and SDKs available for custom integration

- Hybrid strategy:
  - Integration or interoperability with vendor's own on-premises technologies in:
    - Message security gateways
    - Web content filtration
    - Data loss prevention
    - Message data management (archiving, e-discovery, etc.)
- Automated user account management capabilities:
  - Integration with directory systems, databases, and HR systems for automated user provisioning/de-provisioning
- User and administrative identification and authorization mechanisms supported
- Customer messaging servers supported
- Hosted messaging server options

Functionality

The functionality provided by the hosted messaging service is the fourth major area of consideration. Key features evaluated included:

- Message hygiene and security:
  - Spam identification techniques
  - Spam catch ratio
  - False positive and false negative ratios
  - Total quantity of spam messages processed
  - Ability for end users to manipulate spam message queues
  - Ability for end users to easily identify false positives/negatives
  - HMS capabilities to adapt and learn from user corrective actions
  - Direct manipulation of blacklists and whitelists
  - Aspects of messages analyzed to trigger filtration
  - Encryption of messages, both at rest and in transit
  - Support for specific regulatory compliance requirements
- Administrative interface:
  - Overall administrative interface functionality and design
  - Flexibility in policy definition, particularly across different users, groups, geographic locations, etc.
  - Integration of administration with related, integrated or interoperable technologies such as Web content filtration or data loss prevention
  - Reporting and dashboard mechanisms

- Real-time reporting capabilities
- Emerging threat / zero-day notification and response capabilities
- Compliance reporting capabilities

- Web content filtration:
  - Vendor offers its own technology to protect end users from malicious Web content in messages
  - Packaging and integration of Web content filtration
  - Deployment mechanism, including on-site hardware or software required or complementary to a hosted service
- Data loss prevention (DLP):
  - DLP packaging and integration
  - DLP capabilities, including identification of sensitive data, logging/reporting, alerting, and blocking of sensitive data before it is transmitted
  - Deployment mechanism, including on-site hardware or software required or complementary to a hosted service
- Internationalization/localization:
  - Supported languages for end-user and administrative consoles
- End user interface:
  - Interface options, such as Web page, portals, or messaging client plug-ins
  - Support for mobile devices
- Policy definition options.

Vendor Strength

The final key evaluation criterion is vendor strength, which provides a measure of the vendor's maturity, financial stability, and potential for future growth and innovation. Areas evaluated include:

- Vendor vision and strategy:
  - Thought leadership
  - Competitive advantages and unique functionality
  - HMS design and infrastructure
  - Industry guidance and best practices used
  - Integration with other technologies and vendors
- Financial strength
  - Size of the company in all markets
  - Size of the company in closely related markets (such as security or hosted email services)
  - Size of the company specifically in HMS (Number of customers, mailboxes under management, etc.)
  - Public vs. private company

  - Venture funding
  - Type of SLAs offered and if financially punitive
  - Profitable and/or cash flow positive
  - Support structure, locations, language support and availability
- Research and development capabilities:
  - Percentage of R&D spend compared with revenues
  - Size of R&D organization
  - Amount of internally developed vs. licensed technologies
- Key partnerships and sales channels:
  - Number of partners
  - Revenue breakdown between direct and channel sales
- Market credibility:
  - Quantity of messages processed
  - Growth in customer quantity and messages processed
  - Demonstrated innovation and thought leadership
  - Customer base and composition

EMA Radar Map for Hosted Message Security Services

The HMS Services Radar Bubble chart shown in Figure 4 displays how the nine solutions studied in this report ranked in comparison to each other, in terms of Cost Efficiency (x axis) and Product Strength (y axis). The size of the "bubble" indicates relative measures of Vendor Strength.

Figure 4: Radar Map for HMS

All of the vendors in this assessment scored as "Strong Value" or better. This indicates that all exceeded rigorous EMA scoring criteria. The lack of results in other categories reflects two overall factors:

- The EMA Radar process itself has resulted in significant "self-selection." Vendors not prepared to invest the resources required to traverse the Radar process, those daunted by the rigor of the survey and dialogue, and those less certain of relative product strength declined to participate.
- Solutions in the "Specific Value" category in EMA Radar Reports typically exhibit strong results in one of the two dimensions of product strength or cost efficiency, or moderate scores in both. These solutions are typically best fit for use within specific environments or in certain defined operational scenarios. In general, the HMS market has both matured and broadened into general purpose solutions and multi-functional suites that embrace message filtration, antispam, antivirus and anti-malware threat mitigation, and a number of other security and messaging functionalities (described in more detail under "General Findings" below). Thus, given the current maturity of the market, few if any HMS services today are limited to offering "Specific Value" (or less) in any event.

There are, however, some significant players whose absence from this report deserves a mention. Cisco, for example, has a leadership position in the on-premises email security gateway product market through its IronPort products, and in March 2009 complemented this position with the introduction of its Cisco IronPort Email Security services. This past February, however, the company announced that it was terminating its hosted Cisco Mail service, raising questions as to its HMS strategy going forward.

On a more positive note, there are at least two vendors whose offerings were not covered because their HMS services have been in the market for less than one year. Regardless, their recent entry into the HMS arena should be noted by prospective customers for the impact they may have on HMS and hosted security services in the future:

- With its 2009 acquisition of Purewire, **Barracuda Networks** broadened from the security and message filtration appliance market to become a participant in the SaaS Web security gateway space. In December 2010, the company announced its SaaS-based Barracuda Email Security Service, providing both a pure "Cloud-based" HMS offering as well as hybrid integration with its Barracuda Spam &Virus Firewall. The company's execution in the on-premises market necessarily makes it a challenger to HMS leaders with this move, and a player to watch in the future.
- In July 2010, **Zscaler** complemented its SaaS-based Web security service with hosted email security, The move is part of the market's growing recognition of the disappearing distinctions between security for messaging and end-user protection from malicious Web-based content, given the prevalence of both HTML-enabled email and Web-based messaging. The synergy between email security and Web content filtration is influencing the direction of both on-premises and hosted message security solutions, and is described in the discussion of overall findings in this report. Even though its Web security offering has only been in the market since 2008, Zscaler claims "millions of users in 140 countries"[3] and reports accelerating traction for its integrated HMS offering. EMA expects Zscaler's market presence overall – and its impact on HMS in particular – to reflect its customers' acknowledgement of the value of such an integrated service going forward.

[3] http://www.zscaler.com/20100719_Press-Release-Email-Security-Launch.html

Distribution of Results

Two factors in general have clustered vendors in this study toward the top right of the Radar map:

- Due in large part to the "self-selection" process described earlier, the field of contenders in this report *are* many of the leaders in Hosted Message Security.
- In addition, the maturity and increasing commoditization of this space has tended to narrow differentiators between competitors. This also has the effect of magnifying smaller distinctions, and elevating the impact of factors such as price – which is further emphasized by the "on-demand" nature of hosted services. Deployment and maintenance costs are often sharply reduced by a SaaS model, making subscription costs even more significant.

Within this group, the overall division of the HMS market into two principal subgroups is apparent:

- **Security leaders and HMS specialists:** Prior to the acquisition of major players in the space over the past decade, the market was largely defined by pure plays that largely arose from the antispam space (still a significant aspect of HMS services). Today, that number has diminished, but Proofpoint, for example, continues to stand out not only with HMS as a primary offering, but as a vendor that has enjoyed particular success in the enterprise market and continues to show respectable growth. With acquisitions such as that of MessageLabs by Symantec, MX Logic by McAfee, and Websense's acquisition of SurfControl (which, in turn, had previously acquired BlackSpider), IT security market leaders brought HMS into their fold, defining what has become one of the pillars of "Security as a Service." Many of these vendors had previously built, or acquired, a strong position in on-premises message security technology – hence the "hybrid" combination of on-premises and hosted technology offered by many.
- **Hosted messaging vendors:** It is only natural that vendors of hosted email and messaging services would provide HMS as part of their overall value proposition. It enables these vendors to provide a more turnkey approach to the outsourcing of messaging services for their customers – yet few treat HMS as an incidental aspect of their business. Google, for example, acquired one of the early leaders in the space with Postini, and still maintains a dominant position in the market. Google is also an example of a vendor with a broader SaaS strategy, with HMS as a part of its Google Apps portfolio of online office productivity solutions – itself part of Google's larger ambitions "in the Cloud" that are further complemented by the company's unique position in the mobile technology market.

Those who focus more on Hosted Message Security and/or security technology as their primary market(s) tend in general to be higher in cost but richer in features and functions. Those who offer hosted messaging may take a different approach to Hosted Message Security in terms of aspects such as solution features (and resulting complexity); however, EMA believes that offering Hosted Message Security adds to the overall value of such a solution and enhances its Cost Efficiency, which is reflected in the Radar map.

It would be risky, however, to over-generalize perceptions of these groupings. For example, many in the aggressive pricing cluster are leaders in the SMB market. At the same time, however, vendors offering a wider spectrum of HMS capability also have a substantial SMB customer base. Similarly, more aggressively priced services have appeal to enterprises as well as SMBs, and may include offerings beyond HMS or security *per se*. Again, it is vital that the reader understand that an EMA Radar Report

is a starting point for an in-depth evaluation, rather than a finishing point. The reader's task is to find the criteria that matter the most to them and focus on those vendors that did well accordingly.

Some participants in the HMS market span more than one of these overall categories. As noted earlier, Perimeter E-Security's 2007 merger with USA.NET united security leadership in managed and professional services with hosted messaging and HMS, and remains in many ways a unique combination that emphasizes the company's primary emphasis on "Security as a Service" in contrast with more product-focused competitors.

General Findings

While fundamental services have become largely similar in many respects, changes are affecting the market that are driving convergence with close adjacencies and inviting new competition from those who see the "Security as a Service" opportunity.

Convergence with Web Content Filtration

One of the most significant aspects of service expansion evident in the HMS market is the increasing convergence of message security with URL filtration and protection from malicious or restricted Web content (sometimes referred to by EMA as "client-side Web security"). The value of this convergence first became evident in the increased proliferation of HTML mail several years ago.

Today, Web content in messaging is prevalent, and the Web has become a familiar vector for message-borne threats. Messages can contain both malicious URLs as well as legitimate URLs that have been compromised, often without the owner's knowledge. They may also contain links to legitimate sites that could pose a business risk for other reasons. At the same time, messaging is becoming an increasingly significant aspect of Web-based platforms such as social networking, collaboration, hosted office productivity, and SaaS-based resources. These trends have further heightened the need for augmenting message security with protection from malicious, high-risk or unauthorized Web content.

HMS vendors increasingly provide some form of protection against messages containing malicious Web content or URLs, either integrated directly with the HMS service, through managed services or third-party partnerships, or via techniques such as ICAP, the Internet Content Adaptation Protocol. For some such as Websense, this convergence is a primary aspect of their strategy, given the importance of Web content filtration to their core business.

Hosted Message Security and Data Loss Prevention

Most vendors also offer some form of exfiltration control to protect against the potential loss or "leakage" of sensitive information. However, there is not yet general convergence with "enterprise" Data Loss Prevention (DLP), primarily because of the intensive on-premises nature of enterprise solutions. These often involve technologies such as information discovery. which must have the capability to locate on-premises information resources.

For these reasons, most exfiltration controls deployed with HMS are limited to definitions of policy to restrict the exposure of structured data such as account numbers or other readily defined information. For more open-ended requirements, many providers offer a means to structure regular expression matching – but with some caveats, since poorly defined expressions could result in scans that bog down services for multiple HMS customers (hence why some such as Symantec only provide this capability under vendor supervision).

Regardless, many vendors provide reasonably impressive "dictionaries" of content that can be filtered from outbound messages, coupling these in many cases with "out-of-the-box" policies that enable customers to quickly deploy protection against exposure of common types of Personally Identifiable Information (PII) or potential violations of widely adopted mandates such as the Payment Card Industry (PCI) Data Security Standard (DSS) or, in the U.S., the Health Insurance Portability and Accountability Act (HIPAA).

There is, however, clearly an opportunity for vendors with strength in on-premises DLP to converge that strength with Hosted Message Security – and in many cases, the opportunity lies in the delivery of "hybrid" solutions that combine on-premises technology with hosted services.

Hybrid Solutions

A number of vendors with a significant presence in HMS also offer – or, previous to becoming participants in HMS, were particularly strong in – on-premises message security technology. Software solutions in that space have largely been eclipsed by appliance form factors – which, in turn, are at risk of becoming eclipsed themselves by the rise of Hosted Message Security services. For these vendors, the ability to offer both on-premises and hosted technology gives them a strategy to sustain their on-premises business while capitalizing on HMS, as well as an opportunity to give customers a continuum of offerings that best meet their needs.

One of the advantages of a hybrid approach is the ability to combine on-premises filtration of outbound content with the advantages of a hosted solution for inbound messaging. This enables customers to make the most of controls against sensitive data exfiltration such as DLP when deployed on premises, including the capabilities of enterprise DLP for sensitive information discovery. It also helps assure that outbound messaging is filtered before it leaves the boundaries of the business, reducing the risk of exposure in external networks. A hybrid approach to inbound filtering, meanwhile, may better integrate with on-premises messaging systems, or assure protection for sensitive inbound content all the way to the enterprise while providing the benefits of a hosted service for other aspects of inbound message control.

Many organizations have already deployed on-premises technology in close adjacencies such as client-side Web security or DLP. A hybrid approach enables these customers to extend the value of these investments while leveraging the advantages of HMS to enhance their messaging or security capabilities for both on-premises and remote or distributed users and groups.

For all these reasons, security leaders in particular have been particularly active in advancing hybrid approaches, with some such as Websense making an integrated hybrid approach across all three domains of message security, DLP, and its "anchor" technology of Web content filtration, a centerpiece of its strategy.

Serving SMBs vs. Serving the Enterprise

Given the appeal of HMS services to enterprises and SMBs alike, a dilemma emerges for vendors throughout the market:

- Enterprise customers clearly need broad, flexible and highly scalable solutions for meeting a wide range of requirements. At the same time, hosted solutions must offer benefits in deployment and administration in order to deliver the value customers expect from hosted services that promise to alleviate many of the burdens of on-premises technology.

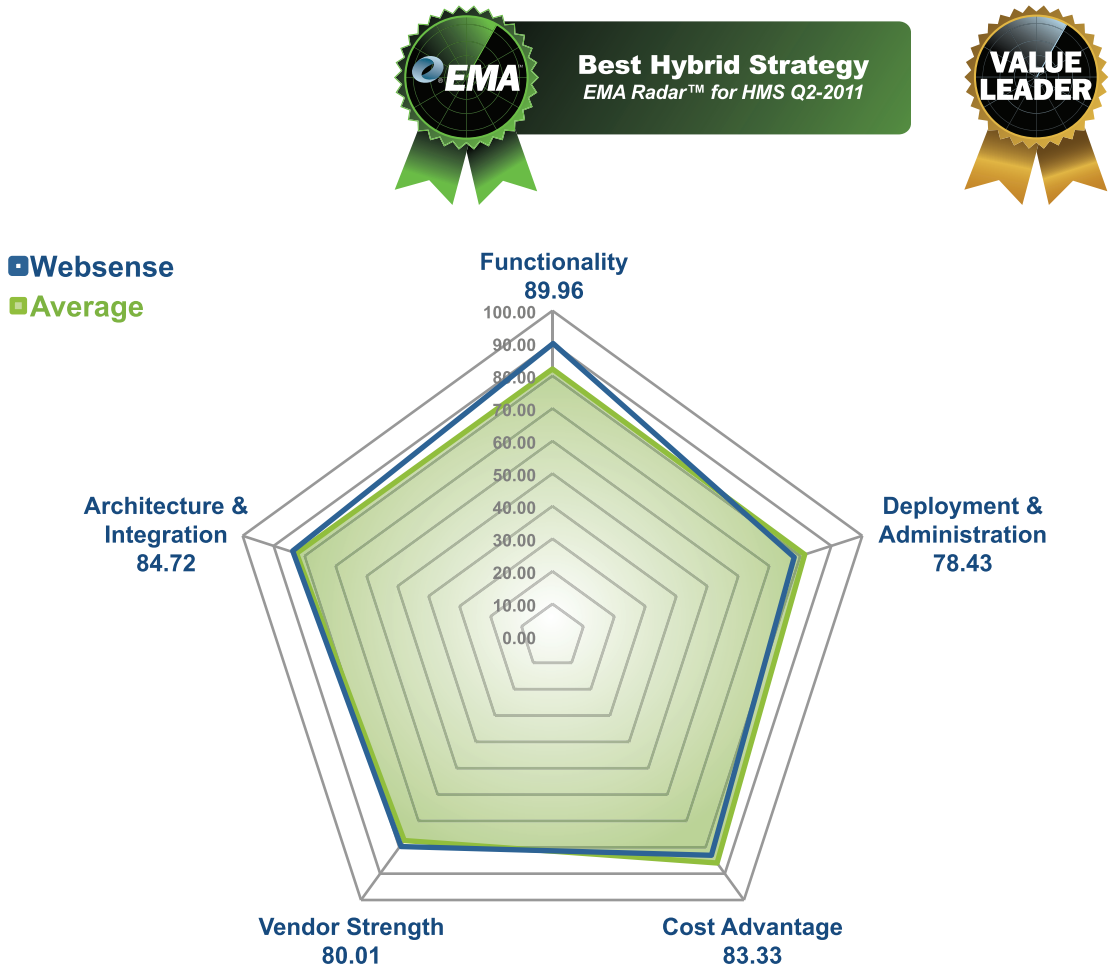
- Small- to medium-sized businesses, meanwhile, may place primary emphasis on ease of adoption and ease of use, and meeting a more general set of requirements common to businesses of all sizes. This does not mean, however, that SMBs must settle for mediocre solutions. They too expect enterprise-grade protection and responsive performance from messaging, particularly when their business places significant expectation on messaging in order to interact – or compete – with larger enterprises.

This raises a question for HMS service providers: How to satisfy the enterprise without losing the SMB business that has become a major customer base for nearly every vendor in the space? While most have emphasized the ease of deployment, administration and use valued by both SMBs and enterprises, some such as AppRiver have delivered services particularly valued by the SMB – which in many cases includes hosted messaging itself – while others such as Proofpoint have concentrated on the more varied needs of the enterprise for functionality and administrative flexibility.

Continued Growth

Lastly, but certainly not least, most of the vendors in HMS report growth that in many cases is more than respectable. Many measure growth in multiple ways between 25% and 50% annually, while longtime vendor AppRiver claims revenue growth in excess of 7x over the last five years. In March of this year, Symantec reported an impressive 171% year-on-year growth rate from 32,000 customers to 55,000 for its Symantec.cloud services, of which the former MessageLabs HMS service is a centerpiece. Clearly, hosted messaging and HMS represent centers of gravity for leading vendors, from which they can expand their reach into the potential of "the Cloud" and Security as a Service alike.

Websense Profile



Introduction

Websense, based in San Diego, California, was founded in 1994 and currently reports over 1,400 employees worldwide. The company went public in 2000 (NASDAQ: WBSN), and reported total revenue of U.S. $333 million for fiscal year 2010. Websense was profitable in 2010 and is growing.

Traditionally known for its strong Web content security solutions, Websense broadened its portfolio through a number of strategic acquisitions, including PortAuthority and SurfControl in 2007 (SurfControl having previously acquired BlackSpider's email and Web filtering managed services) and Defensio, a vendor of spam defense for blog sites, in 2009.

Today, Websense offers a trio of security services, including Web, email and data security offerings, all of which are offered as hosted, on-site (appliance), software or a hybrid combination. This is a strong combination, particularly from a message security perspective, as the combination of the company's

robust Web and message scanning technologies provides a very strong defense against blended threats – perhaps the strongest in the industry. Add to that a significant contender in Data Loss Prevention (DLP) functionality, and Websense is able to provide a comprehensive suite of services for companies of all sizes.

Architecture and Integration

From an architectural perspective, Websense has the strongest story to tell in terms of allowing customers to seamlessly transition from traditional software to appliance to hosted security services. The company's solutions are managed through a common Web-based management portal, regardless of which form factor(s) are in use.

Websense owns its own data center architecture, which adheres to the ISO 27001 information security management system standard, which is regarded as a more rigorous certification than the SAS II Type 70 certification to which many service providers adhere. Data center hardware is over-provisioned across 10 globally distributed data centers with fully redundant power, cooling and Internet connectivity so that the service runs at a maximum capacity of 50%, providing plenty of "headroom" to cover spikes in demand.

From an integration perspective, Websense works with virtually all common email systems and also provides integration with LDAP-compatible directory systems including Active Directory. The company provides many mechanisms for exporting its management data into other systems, although these mechanisms primarily involve file export-import processes.

The Websense HMS filtration architecture passes messages through multiple filters, depending on the level of service subscribed:

- Antispam: All Websense HMS customers receive the benefits of Websense antispam technologies that include network and sender reputation analysis, adaptive learning, URL analysis, heuristics, digital "fingerprinting" of distinctive message attributes, and optical recognition of image spam (a technique used to evade filters that only recognize text). Each message is given an aggregate score which is measured against a customer-defined threshold to determine appropriate action.
- Antivirus techniques: In addition to antispam, customers of Websense Hosted Email Security receive both inbound and outbound antivirus message scanning using multiple commercial engines. Supplementing these filters is the Websense ThreatSeeker Network, which continuously examines email and Web sites to detect indicators of emerging threats to help reduce the "zero-day" window of exposure between the appearance of new malware and its recognition in defense.
- Content Filtering: For customers of Websense Email Security and Content Control, Websense offers pre-defined dictionaries for filtering sensitive content that cover 20 topic areas in 12 languages. Pre-built templates for data privacy and compliance with regulatory requirements such as the PCI Data Security Standard enable rapid and straightforward deployment of protection for a number of content control priorities. Websense also offers regular expression matching for more finely grained requirements. Optionally, Websense also provides Websense Image Analysis, which uses advanced algorithms for real-time analysis of images embedded in or attached to emails for inappropriate content. Email messages and attachment content are inspected, and true file types are verified (regardless of filename extension). Messages can be quarantined, and delivery deferred for larger files.

- Encryption: Customers of Websense Email Security and Content Control also have access to encryption on multiple levels. For server-to-server and server-to-client message communications, Websense supports TLS encryption on an "opportunistic" basis (i.e., when the peer supports it), or can enforce a policy requiring that messages only be delivered via TLS. For message content encryption between users and secure delivery to individuals, Websense also provides secure hosted messaging that restricts access to encrypted messages to authenticated users (see under Functionality below). Also available as an add-on is Websense Advanced Email Encryption, which essentially offers the ability to encrypt the email message and all associated attachments from sender to recipient.

Beyond Hosted Message Security, Websense has an ambitious vision for integrating its three main areas of technology focus. The company's TRITON initiative offers customers the ability to deploy a combination of integrated message security, client-side Web security, and Data Loss Prevention. This strategy is being progressively extended to the company's hosted solutions as well as its on-premises technologies (appliances, virtual appliances and software), giving Websense one of the most comprehensive strategies for attacking the primary aspects of message security, regardless how deployed. It also recognizes the importance of defense against Web-borne threats delivered via both inbound and outbound messaging. For these reasons, the company is recognized for "Best Hybrid Strategy" in this report, and should be expected to more seamlessly integrate these services and their user interfaces in the future.

The company processes a very high amount of email (reportedly 10 million messages an hour), and it consistently meets its SLAs that guarantee 99% spam catch rate, 100% detection rate for known viruses, 99.999% uptime, processing latency of 60 seconds or less (for non-spam messages less than 2 megabytes in size), and availability of email logs and quarantine five minutes or less after mail receipt.

Functionality

As indicated previously, a key benefit of Websense's offerings is integration between all of its offerings, regardless of which form factor or platform they run on. From a user's perspective, this is of course transparent, and this is mostly true for administrators as well. The current administrative portal does have a slightly different user interface for hosted services, but the company has indicated that this situation will be rectified in the next release of its software (coming in the very near future).

Websense's administrative portal is easy to use and provides a lot of functionality. While it is not radically different from competitors, it has a nice "Web 2.0" look and feel. Policies are easy to define, and the company provides a large number of pre-built policies that customers can easily leverage when needed. The end-user interface is also fairly typical – spam quarantine email messages are sent to users daily, and messages can be released from the quarantine directly from the quarantine message.

Websense also provides a variety of message content encryption services, which are easy to use. Policy-based encryption can be invoked to ensure that connection and/or message encryption is enforced. Encryption policies can be based on sender, recipient or sensitivity settings in Microsoft Outlook, to make encryption policy more transparent to end users. Individuals can also choose to manually encrypt messages by placing a keyword in the email subject line. Encrypted messages are delivered via an email message that directs the recipient to a secure Web site, and after a one-time registration, they can read and reply to the message. Attachments are also supported.

As mentioned earlier, one of Websense's strong points is DLP, arising primarily from its acquisition of PortAuthority in 2007. The company provides DLP functionality for outbound messages either through appliances or a hosted service, and a rich set of pre-built policies are available to aid in compliance with a wide variety of governmental regulations. In addition to standard text content scanning, Websense also supports attachment scanning (over 400 file types are supported) plus image scanning.

Deployment and Administration

Deploying the Websense HMS service is very typical. After setting up an account, customers are walked through configuration of the service, which involves signing into the administrative portal and reviewing default policies. The company indicates that many of its customers can leave most of the default policies intact. User accounts are created either manually, via a file upload, or by configuring synchronization with a directory server like Active Directory. Users may also be dynamically provisioned as legitimate email messages are received by the service. Customers then configure the Websense service to send legitimate email messages to their email server, and they must also configure their email server to accept email from the Websense servers. Customers then change their DNS MX record entries to redirect their email stream to Websense, and the system is online. Deployment is lengthened a bit if customers choose to deploy DLP, as additional rules may be required, as well as an optional appliance installation if desired.

Websense services are easy to administer. Role-based administration allows highly granular delegation of administrative duties to multiple personnel. For example, mail administrators can be provided a completely separate set of administrative screens from compliance officers, which review potentially sensitive email messages for policy violations. As indicated earlier, the Websense administrative portal is clean and straightforward.

Cost Advantage

Websense prices its base hosted message security and content control service at $18 per user, per year, which places it in the higher tier of pricing, but essentially in line with other vendors who focus primarily on the IT security market. The company offers multi-year discounts of 15% and 20% for two- and three-year commitments (respectively), with add-ons including the aforementioned advanced email encryption and image analysis.

Vendor Strength

Since Websense is a public company, it is easier to quantify the company's strength than many of its privately held competitors. The company is profitable, has a strong cash position, holds 173 patents on its technologies, and has over 40,000 customers worldwide.

Websense has a strong support organization, and support is available 24x7x365 by phone, email and Web. It also has a number of geographically located support centers, including North America, Australia, China and Western Europe. Support is included in the monthly subscription fee, although premium support packages are available for large customers that require an even higher level of responsiveness. As indicated earlier, Websense also provides a strong set of SLAs, which is a sign of a capable vendor.

Websense maintains research and development facilities in San Diego and Los Gatos, California; Reading, England; Beijing, China; Sydney, Australia; and Ra'anana, Israel. The company has a strong support and operations team, comprised of 325 people dispersed around the globe providing "follow the sun" monitoring of data center services, email, and security threat monitoring.

With a strong, global R&D and support organization, it is no surprise that Websense supports numerous languages and double-byte character sets, including most Western European languages, Chinese and Japanese in addition to English.

Strengths and Limitations

Websense strengths are:

- Visionary in its strategy for integrating Web, email and data security delivered as SaaS, on-premises technology, or hybrid (combination of SaaS and on-premises technology), and easy migration from software to appliance to Cloud-based service.
- Single management platform for on-premises and SaaS-based security solutions.
- Unique joint processing model that splits work between on-site appliance and Cloud resources.

Websense limitations are:

- Perception as a best-of-breed Web security company may hinder the company's image as a multi-capability security provider.
- Pricing above a number of vendors who also provide email hosting, but similar to other security leaders that focus on hosted and on-premises security technologies.

About Enterprise Management Associates, Inc.

Founded in 1996, Enterprise Management Associates (EMA) is a leading industry analyst firm that provides deep insight across the full spectrum of IT and data management technologies. EMA analysts leverage a unique combination of practical experience, insight into industry best practices, and in-depth knowledge of current and planned vendor solutions to help its clients achieve their goals. Learn more about EMA research, analysis, and consulting services for enterprise IT professionals, lines of business users, and IT vendors at www.enterprisemanagement.com or follow EMA on Twitter.

Corporate Headquarters:
5777 Central Avenue, Suite 105
Boulder, CO 80301
Phone: +1 303.543.9500
Fax: +1 303.543.7687
www.enterprisemanagement.com

2292-Websense-Summary.072611