G00247704

Magic Quadrant for Secure Email Gateways

Published: 2 July 2013

Analyst(s): Peter Firstbrook, Brian Lowans

The secure email gateway market is mature. Buyers should focus on strategic vendors, data loss prevention capability encryption and better protection from targeted phishing attacks.

Strategic Planning Assumption

Cloud-based (software as a service) deployments of the secure email gateway market will grow from 37% in 2011 to more than half of the market (by revenue) in 2016.

Market Definition/Description

Secure email gateways (SEGs) provide protection from email spam and malware, and also provide outbound email content inspection and encryption of emails.

The SEG market is mature. The penetration rate of commercial SEG solutions is close to 100% of enterprises. Buyers are becoming more price-sensitive; slightly less than 80% of recently surveyed reference customers (see Note 1) said that price was important or very important in their next SEG purchase.

The market growth rate has leveled off, and there are no significant market entrants or acquisitions — all classic signs of a mature market.

Despite the market maturity, companies can't do without SEG solutions. Global spam volumes declined again slightly in 2012[1] as spammers moved to other mediums, such as social networks, but spam still represents as much as 69% of email. Phishing and malware attachments also declined slightly in 2012; however, there is ample evidence that email is the preferred channel to launch advanced targeted attacks.

Better protection from targeted phishing attacks is the most critical inbound protection capability (98% of respondents indicated that this was an important or very important capability), but only a few vendors have advanced the state of the art against these attacks. Leading solutions are incorporating methods to double check — or better, proxy — URL links in email at the "time of click" rather than the time of delivery. These methods are more effective in detecting fast fluxing link-based malware/phishing attacks. To address attachment malware, leading solutions are adding the ability to strip active content (that is, Java and macros) from common document types (that is,

PDFs, Office) to neuter their malicious intent. More advanced solutions are actually executing suspicious files in virtual environments to detect malicious behavior and provide forensic information. Some vendors are also creating reporting that is specific to targeted attacks to provide forensic information about attacks and users' behavior. These reports are valuable for incident response as well as employee education.

Eighty-two percent of respondents to our 2013 survey indicated that bulk email filtering was an important or very important critical capability of their next SEG. Dissatisfaction with current bulk email capabilities is a significant pain point of existing solutions. End users don't care about the clinical definition of spam and are frustrated with the level of "unwanted" email in their inboxes. Most solutions include a "bulk" or "marketing" email classifier that can be used to quarantine this type of mail, but policy options are typically very coarse and could easily be improved. None of the vendors offer personal controls to enable end users to better manage their inboxes.

Interest in outbound email hygiene continues. Outbound capabilities, such as data loss prevention (DLP) and encryption, remain the most important feature differentiators. Forty percent of respondents indicated that they already use DLP, and 25% plan on adopting DLP in the next 24 months. Workflow for managing events and predeveloped content (that is, common identifiers, dictionaries and regulatory policies) are the main differentiators of DLP capabilities among vendors in this analysis. Thirty-nine percent of respondents already use email encryption beyond Transport Layer Security (TLS), while another 25% plan on adopting it in the next 24 months. Almost all the vendors in this analysis have some encryption capabilities; however, existing encryption customers are expressing frustration with the usability of encryption for senders and recipients, especially on mobile devices. A key consideration is the encryption solution's level of integration in the SEG management interface.

Significant interest in and deployment of virtual solutions and software as a service (SaaS) solutions continue. Leading vendors in this market are expanding their offerings vertically into adjacent markets (such as mailbox hosting, hosted archiving, e-discovery and continuity services), and horizontally into secure Web gateway (SWG — see "Magic Quadrant for Secure Web Gateway") solutions linked by common DLP and management. However, buyers' demand for these services from their SEG vendors is mixed, and purchasing decisions rarely coincide.

Magic Quadrant

Figure 1. Magic Quadrant for Secure Email Gateways

Source: Gartner (July 2013)

Vendor Strengths and Cautions

Barracuda Networks

Barracuda Networks is a private, California-based company that focuses on producing a range of economical, easy-to-use network appliances and SaaS solutions that are aimed primarily at small or midsize businesses (SMBs), as well as educational and government institutions. Barracuda continues to grow at above market rates. Barracuda Spam & Virus Firewall appliances are shortlist candidates for organizations that are seeking "set and forget" functionality at a reasonable price.

Strengths

- Barracuda continues to execute well, with respectable growth in an overall declining market. Recent improvements focus on large file attachment handling, configuration backup, better role-based administration and better encrypted email reporting.

- An optional cloud-based prefilter, which filters out obvious spam before final filtering, is done on-premises.
- Native basic pull-based encryption and DLP capability are included free of charge.
- Barracuda Control Center can manage multiple boxes, and comes as a free cloud-based offering or an on-premises appliance.
- Service prices are per box, rather than per user, making Barracuda a significant price leader.
- The vendor's email archiving solution has an interface with a consistent look and feel, and it can also be managed from the same Barracuda Control Center.

Cautions

- Barracuda does not offer any other third-party anti-malware engines, and techniques for advanced threat detection are missing.
- The user interface and reporting engine are long overdue for a refresh. The addition of customizable dashboards with hyperlinks to reports, better reuse of policy objects, simpler policy workflow and ad hoc reporting would be welcome.
- DLP is limited to keyword and regular expression filtering. It includes only limited, predefined DLP dictionaries, and is not object-oriented or group-policy-integrated. Workflow for compliance officers is limited.
- The included encryption capability is a good value, but it could be better optimized for mobile devices.

Cisco

Cisco continues to dominate the market for dedicated on-premises solutions for midsize-to-large organizations, but has lost some momentum. It offers three deployment options: hardware appliances, managed appliances and virtual appliances. Cisco enjoys strategic vendor status with many of its customers and is well-respected in the core network buying centers. It is a good candidate for midsize-to-large enterprise customers that are looking for best-of-breed functionality.

Strengths

- Cisco has excellent scalability/reliability, an easy-to-use management interface, deep policy control and very granular mail transfer agent (MTA) control capabilities.
- Its Outbreak Filters option provides unique targeted attack protection by scanning suspicious URLs at the time of click with Cisco Cloud Web Security. This year, Cisco has made improvements in its ability to detect low-volume spam attacks, as well as in assigning IPv6 addresses a reputation score.
- Cisco provides content-aware DLP capabilities with numerous predefined policies, dictionaries and identifiers, as well as a strong compliance officer interface. Integration with RSA Enterprise

Manager for DLP integration exists between Cisco's solutions and RSA, The Security Division of EMC's enterprise DLP.

- It offers native policy-based email push encryption delivered on box or as a service with message recall, read receipt and message expiration; proprietary desktop-to-desktop encryption capabilities; support for iOS, Android and Windows platforms; and large file attachment handling.
- Cisco Email Security benefits from Cisco's installed base of network security appliances, and from Cisco Cloud Web Security (formerly ScanSafe), by collecting a massive amount of Internet traffic information to spot new malware and spam trends. Cisco's broad array of network security components makes it a strategic vendor for many organizations.

Cautions

- Cisco's transition to the general Cisco channel from dedicated IronPort sales representatives and email-specific channel partners will be rough for some users.
- Cisco's focus on the needs of large enterprises doesn't always scale down well for SMBs. The user interface can be confusing and unintuitive for less experienced operators.
- Cisco spam filtering is highly reliant on reputation, which is less effective for lower-volume snowshoe spam.
- Cisco's hosted email offering only has four data centers in the U.S. and Europe so far. Clients are unable to select the storage location for their data.
- While on-premises solutions offer local key management, the hosted solutions only offer key management from a U.S. data center. None of these solutions currently offer compliance with U.S. Federal Information Processing Standard (FIPS) Publication 140-2.
- Cisco put the PostX encryption appliance in end of sale, which eliminates pull functionality and support for Pretty Good Privacy (PGP) and Secure Multipurpose Internet Messaging Extensions (S/MIME); however, it continues to support on-box push encryption. The former PostX functionality will continue to be available via Cisco partner totemo.

Clearswift

Clearswift has an established presence in the email protection market, primarily in the U.K., Europe and Asia/Pacific. It has also branched out to the SWG market. New ownership and management are pushing the company in the direction of data protection and information governance. Clearswift offers hardware appliances, a bare-metal software and VMware/Hyper-V solutions. The combination of SWG and SEG with the provision of basic DLP capabilities across both channels makes Clearswift a reasonable shortlist candidate for buyers that are looking for on-premises SEG and SWG solutions from the same vendor.

Strengths

- The Web-based management interface provides centralized management, dashboards, and reporting for the Web and email products; a centralized reporting engine; and the content scanning engine. Nontechnical users will find it easy to use, and it has a lot of context-sensitive recommendations and help functions.
- The proprietary Clearswift DLP engine provides fast scanning of more than 150 file formats. It contains features to protect against denial-of-service attacks, and provides a selection of prebuilt patterns for common data types (PCI/personally identifiable information), as well as common Boolean and proximity operators.
- Users can manage their quarantines from any browser, or via an iPhone/iPad interface.
- Clearswift exploits Commtouch for a portion of its anti-spam capability, and has upgraded to the most recent engine.
- The solution includes a "bulk email" category, which is useful for reducing nuisance email.
- The ImageLogic detection engine for inappropriate and registered images is an extra utility service for organizations with this need.
- On-box encryption with support for S/MIME, PGP and password-protected email encryption, and with a built-in certificate store, was recently improved with automatic certificate, key extraction and lookup capabilities. The Echoworx partnership provides enhanced encryption capabilities via a Web portal ("pull") or mailbox ("push").

Cautions

- Clearswift is recovering its growth due to a focus on the core email and Web gateway business, and it is improving customer support; however, its market share and mind share are very low in a rapidly maturing market. The vendor is late to deliver industry-leading features and functionality. It does not directly offer a SaaS-based delivery model or vertical products, such as email archiving. As buyers increasingly look for more strategic integrated vendors, Clearswift may have a difficult time standing out in a crowded market.
- Although the interface is easy to use for nontechnical users, it is limited in detail for more technical enterprise users.
- Advanced encryption provided by Echoworx is not integrated with the management interface. It lacks any control or visibility of sent messages, and it lacks self-service configuration of the encryption experience.
- DLP enhancements are needed in the ability to describe sensitive content beyond regular expressions, along with support for more advanced detection techniques (such as partial document matching). Policy management, workflow reporting and event management are rudimentary.

Dell

Dell acquired SonicWALL and now offers a broad suite of SonicWALL network security solutions, including firewalls, virtual private networks, backup and a range of SEGs. It offers several SEG form factors, including hardware appliances, software and VMware versions, and hosted versions. Dell also offers a subset of SEG functionality that is delivered as SaaS prefilters for its unified threat management (UTM) customers. Dell is a candidate for shortlist inclusion — primarily for existing Dell SonicWALL firewall customers.

Strengths

- Dell is one of the largest resellers of Microsoft Exchange solutions, and, with SonicWALL, it is able to sell a full Hosted Email stack, including security.
- Dell has its own malware research team developing new spam signatures and detection techniques, which leverage data from its installed base of appliances. The solution also leverages contact databases and communication partners to lower false positives.
- Dell has the most advanced Domain-based Message Authentication, Reporting and Conformance (DMARC) support and reporting, which enables more precise and useful DomainKeys Identified Mail (DKIM) and Sender Policy Framework (SPF) message handling.
- The management interface is localized in a number of languages and easy to use. It has multitenancy support, and reporting is adequate for most organizations' needs.
- The solution includes basic content-aware DLP functionality with prebuilt dictionaries and number identifiers. The policy interface is easy to use with natural-language policy all on a single page.

Cautions

- It is difficult for any company to compete in many markets and across company segments — ranging from large enterprises to small offices — while providing market-leading features in each market segment. Dell does not provide any market-leading SEG functionality. Only a small percentage of its revenue is email-security-related. Its market share and mind share among Gartner customers are low.
- Dell's Ability to Execute score was largely impacted by a low score in overall customer satisfaction compared with other vendors in this analysis; however, we do note an improvement in this year's survey. Still, some reference customers commented on the necessity for better spam and malware detection accuracy.
- Dell does not offer any advanced malware detection techniques.
- The management dashboard interface is not customizable.
- DLP functionality is basic and supports only regular expression matching. Only two prebuilt dictionaries and a handful of number format identifiers are included. It does not include any predefined policy, and event management is rudimentary.

- At the time of this analysis, Dell did not have integrated encryption; however, it was embarking on a beta program for cloud-based encryption that is integrated with the management console.

Fortinet

Fortinet is a public company with a broad geographical market presence that offers a wide array of UTM and dedicated appliances for all organization sizes. It also offers an array of anti-spam technology in various forms, from client to UTM. This analysis, however, focuses on the dedicated SEG FortiMail appliances. FortiMail is a shortlist candidate primarily for Fortinet customers that are looking for a basic SEG solution.

Strengths

- FortiMail's widget-based management interface is customizable, easy to use and similar to other Fortinet products. FortiManager can manage up to 40 Fortinet devices, and FortiAnalyzer provides centralized log storage dashboards and reporting.
- The FortiGuard cloud-based sandboxing service uses behavioral attributes to detect malware by executing them within a virtual environment. Suspicious files can be submitted automatically to the new hosted service for further scanning and detailed status reports.
- FortiMail provides a number of high-availability and scalability features, such as native clustering, load balancing and high-throughput FortiMail hardware appliances.
- Basic DLP capability and identity-based push and pull encryption are included free of charge in the standard FortiMail feature set.
- Appliance-based, rather than user-based, service pricing makes FortiMail very affordable.
- On-box or off-box policy-based message archiving is fully indexed and available from the FortiMail management interface.

Cautions

- Fortinet offers very basic SEG functionality, and is missing more advanced MTA functions for larger enterprise or more demanding environments. Improvements since our last analysis have focused on managed security service provider (MSSP) functions, and planned improvements are focused mostly on better integration with other Fortinet systems.
- Fortinet only offers its own antivirus scan engine, although it does well in Virus Bulletin Reactive and Proactive (RAP) tests. It does not have a big or well-known research organization, especially when compared with the Leaders in this Magic Quadrant.
- The FortiAnalyzer component is required for in-depth, per-domain report and log access across multiple logs in a single interface. However, this component costs extra. Disposition information to show why email is quarantined is more cryptic than users would like.
- There is no SaaS deployment option, although it is in the planning stage.

- DLP functionality is relatively basic; it lacks good policy or compliance workflow, or deep content inspection capabilities.

McAfee

McAfee, a subsidiary of Intel, has a broad range of endpoint and network security products. It consolidated its two on-premises gateway solutions in v.7.0 (now v.7.7), which is a free version upgrade that is supported on hardware appliances that are less than three years old. McAfee also offers blade server appliances with free additional virtual appliances, integrated hybrid email security (with single management and reporting), and SaaS-based SEG, archiving and disaster recovery services. McAfee is a good choice for an integrated hybrid solution, to augment the security of hosted mailboxes, and for existing McAfee customers and prospects looking for an integrated suite of security products.

Strengths

- McAfee's respected threat research team consolidates message, network, Web and file reputation data into its Global Threat Intelligence (GTI) technology. The time-of-click URL redirection for targeted threat protection is very good. We particularly like the "safe preview" capability.
- McAfee Email Protection's native DLP capability is strong and leverages the abilities of its stand-alone, enterprise-class, content-aware DLP offering. McAfee provides numerous predefined policies and dictionaries as part of the base product, and it supports self-defined content for policy creation.
- Basic encryption methods (TLS, S/MIME and PGP gateway encryption) are supported, along with push (secure envelope) and pull encryption. McAfee Email Protection also supports the secure transfer of arbitrarily large files via its encrypted email pull capability.
- The SaaS offering provides a simple, clean, Web-based interface that is very easy to use. It is hosted in seven geographies, and the service can lock message traffic to a specific geography to avoid processing traffic in foreign legal environments. The time-of-click URL redirection targeted threat protection is very good. We particularly like the safe preview option. The time-of-click URL redirection capability is included in the base package, and policy-based pull/push email encryption — which includes the DLP capabilities — is an optional add-on. McAfee customers can switch between solutions without any additional charge.
- McAfee Content Security Suite bundles of secure email, Web and DLP in a combined package that can be deployed in SaaS, appliances or hybrid for a single price can be very attractive.

Cautions

- McAfee has not significantly expanded its market share in the enterprise SEG market over the past three years, and interviews with Gartner clients and reference customers show that customer satisfaction remains lower than average. These issues affect its Ability to Execute score in this analysis.

- McAfee has some promising sandboxing technology for its on-premises appliances for targeted threats, but it was not in general availability at the time of this analysis. McAfee does not yet make use of its cloud Web Gateway technology for time-of-click protection for these appliances.
- Native DLP compliance workflow is weak, it does not offer a compliance-specific role to restrict view to compliance issues, and it does not allow for log annotation.
- Several reference customers pointed out the need for reporting improvements.
- McAfee offers the choice to host encrypted email in only one of the seven data center geographies. No options are offered for on-premises key management, which is automated by McAfee. Currently, there is no compliance with key management standards.

Microsoft

Microsoft has now consolidated all its anti-spam capabilities into its SaaS-based Exchange Online Protection (EOP) product. Microsoft's dominance in the email market makes it a strategic provider of SEG solutions, and it is making big strides in integrating and improving the service. However, it is not as polished as the other Leaders.

Strengths

- Microsoft is capable of tighter integration of SEG functions with Exchange/Outlook than its competitors are. EOP is part of the Office 365 admin center, which provides centralized management of Microsoft cloud services. EOP management concepts will be familiar to Exchange administrators. Exchange Server 2013 and Exchange Online include much improved DLP capabilities that are tightly integrated with the Outlook client.
- EOP mirrors email across multiple data centers for redundancy. Microsoft supports in-geography mail processing for two geographies: the U.S. and the European Union.
- EOP also offers Exchange Hosted Encryption, a solution that is based on Voltage Security technology.
- Microsoft Active Directory Rights Management Services (AD RMS) has been added as an option for end-to-end email encryption services, with Microsoft Windows Azure Active Directory Rights Management services as the hosted equivalent. Windows Azure Active Directory Rights Management services offer native, policy-based, on-premises email push encryption with message recall, read receipt and message expiration.
- EOP is included in Exchange Enterprise CAL with Services licenses and in Microsoft Enterprise CAL Suite. Buyers should check their license entitlements before they consider alternatives.

Cautions

- Microsoft is not on the leading edge of functionality in this market, and has been slow to offer major new improvements. We anticipate an acceleration of feature improvements as Microsoft embraces a cloud-first agile development model.

- Navigating Microsoft licensing can be difficult. EOP is bundled with other services, but it is also sold separately; however, Gartner clients report difficulty in getting sales to provide EOP-only quotes.
- Microsoft is migrating all customers from the legacy Forefront Online Protection for Exchange (FOPE) to the new EOP starting in 3Q13, which will cause extra work for existing customers (see "Forefront Online Protection for Exchange [FOPE] Transition Center").
- Specific advanced targeted threat protection features, such as time-of-click URL protection or active content stripping, are absent.
- EOP does not allow end-user-specific blacklists.
- In-geography-only routing is available only in the U.S. and the EU. While on-premises solutions offer local key management, the hosted solutions only offer key management from the U.S.
- Microsoft AD RMS only supports Windows mobile platforms and is not useful for sending messages to external recipients.
- Buyers that have not standardized on Active Directory require Forefront Identity Manager to consolidate directories into a single addressable entity for synchronization with the EOP service.
- Although the DLP capability has been updated, it still lacks some of the more advanced features of other solutions, such as lexicon, file matching and fingerprinting.
- The Exchange Hosted Encryption solution is not integrated with the management console, and lacks self-service configuration of the encryption experience as well as significant control or visibility of sent messages.
- Policy changes take some time to propagate through the EOP network, which lacks a feedback loop to certify that the changes have been implemented.

Mimecast

Mimecast remains one of a few companies in this analysis that is solely dedicated to email security and management issues. However, it has ambitions to solve more complex end-user problems, such as improving email collaboration and file sharing, and also aims to enhance the end-user experience and the value of the information flowing through the gateway. Mimecast is a good fit for organizations looking for archiving and SEG, and for those looking to provide knowledge workers with email utilities to improve collaboration.

Strengths

- Mimecast has a multitenant SaaS email infrastructure with simple administration for archiving and SEG services. It is hosted in 10 data centers in the U.S., the U.K., South Africa and the Channel Islands.
- Mimecast provides a set of email utilities via its Outlook plug-in, making it seamless for end users to manage their email without leaving Outlook. This integration allows users to specify

how messages are handled at the gateway by using message actions that enable users to choose encryption types, what stationery to apply, document conversion options and large file attachment handling. Archive, search and disaster recovery are also integrated with Outlook.

- DLP and encryption capabilities are available at an additional cost, and are adequate for most compliance tasks. DLP includes attached file content analysis, and comes with numerous dictionaries available for import. Encryption is pull-based or TLS, and can be invoked by end users via the Outlook plug-in or policy.
- Mimecast provides the new ability to create multiple isolated administrators for one domain based on Active Directory group, Active Directory attributes or destination MTA.
- Message tracing is enhanced by a rolling archive that enables administrators to search any part of an email, including the body.

Cautions

- Mimecast has very low market share. As buyers increasingly look for more-strategic integrated vendors, Mimecast will have a difficult time standing out in a crowded market.
- Mimecast only has a small malware/spam research team. It is dependent on partners for a portion of its spam and malware detection capabilities. It does not offer any advanced targeted threat detection capability, although a time-of-click URL inspection feature is due in 4Q13.
- Many organizations are reluctant to deploy additional Outlook plug-ins.
- List pricing for basic SEG services at lower volumes (less than 501 seats) is above average. DLP, encryption and setup costs are extra.
- The DLP capability could be improved with embedded dictionaries and policies that are updated by Mimecast, rather than downloadable. The vendor does not support partial hashes or referenced data, and it can't import or export rules or events to enterprise DLP solutions. Policy creation and compliance workflow could be improved.

Proofpoint

Proofpoint continues to lead the market with innovative features and a singular focus on email security issues — resulting in one of the highest growth rates in this market and improving its Ability to Execute score in this analysis. In addition to SEG capabilities, the company offers archiving, document discovery/governance and large file transfer. Proofpoint's flagship email security solution, Proofpoint Enterprise, is available as a hosted service; as on-premises appliances, virtual (VMware) appliances and software; or as a hybrid combination of these versions. A new, slimmed-down SaaS product — Proofpoint Essentials, from the vendor's acquisition of Mail Distiller — is targeted for SMBs. Proofpoint is a very good candidate for organizations looking for a full range of best-of-breed SEG functionality in supported geographies.

Strengths

- Spam and malware accuracy has always been a consistent Proofpoint strength, and the company is one of the few that publicly reports its anti-spam effectiveness (see "Proofpoint Anti-Spam Effectiveness"). Proofpoint provides spam classifiers (adult, bulk mail, phish and suspected spam) to enable more granular policy. The company continues to invest in new techniques for spam and spear phishing detection through its Targeted Attack Protection service, which provides time-of-click URL protection as well as excellent reporting on targeted attack activity and user response rates.
- The Web-based management interface continues to be one of the best in the market, with numerous innovations and unique features. We particularly like the completely customizable dashboards for each administrator.
- Proofpoint offers integrated, push-policy-based encryption that incorporates the features traditionally associated with pull offerings, and it is optimized for BlackBerry, iOS, Android and Windows platforms. The solution also supports TLS, S/MIME and PGP secure email delivery.
- DLP features are very strong and include numerous prebuilt policies, dictionaries, number identifiers, and integrated policy-based encryption. Policy development is object-oriented and similar across spam and DLP. The DLP quarantine is very sophisticated for a channel solution, and it includes highlighted policy violations as well as the ability to add comments to incidents. DLP policy can be enforced on Web traffic via a dedicated network sniffer or by Internet Content Adaptation Protocol (ICAP) integration with a proxy server.
- SaaS data centers are located in the U.S., Canada, Germany and the Netherlands. Proofpoint claims that its hosted services provide protection of privacy and compliance with a number of regimes covering personal, health and credit card data. Hosted key management is the norm, but on-premises key management is also possible. All solutions have achieved FIPS PUB 140-2 Level 1.

Cautions

- Proofpoint's dedicated focus on email is a strength and a weakness. Although it continues to define best-of-breed functionality in a rapidly maturing market, best of breed often becomes overkill to some customers. Concurrently, numerous enterprise buyers are looking for opportunities to consolidate product purchases around fewer, more strategic vendors.
- Proofpoint continues to have a smaller market and mind share outside North America.
- Proofpoint's list prices are high, although, like other enterprise solutions, discounts are available.
- Proofpoint, due to its corporate focus and high prices, is a poor fit for smaller organizations that do not require advanced controls. The addition of the Proofpoint Essentials product should help; however, Mail Distiller had little presence outside the U.K. The archiving service does not yet have a shared management interface with the hosted or on-premises solutions, and customers commented that the hybrid experience should be more seamless.

- Despite improvements in reporting, Proofpoint still lacks a completely ad hoc reporting capability.

SilverSky

SilverSky was formed in January 2013 with the rebranding of previously merged Perimeter E-Security and USA.NET. The converged company provides a broad range of SaaS and managed network security services, as well as Exchange hosting, archiving and SEG services. It is ideally suited to U.S.-based organizations that are looking for a full-service email infrastructure solution.

Strengths

- SilverSky has a single, easy-to-use interface for Exchange hosting, SEG security and archiving.
- It provides good DLP and encryption functions. DLP policy is configured on one page with conditional drop-down lists and an object-oriented policy.
- SilverSky offers professional services to assist in DLP policy creation or other aspects of email security and management.
- Native pull-based encryption capabilities are available.
- SilverSky is a good fit for financial services organizations because it is audited annually for U.S. Federal Financial Institutions Examination Council (FFIEC) standards by an audit firm that is under FFIEC supervision.

Cautions

- SilverSky is better suited for organizations looking for a hands-off approach. Enterprise features such as configurable dashboards, custom reporting, role-based administration and advanced MTA features are missing.
- Email encryption only supports pull-style encryption and does not have an Outlook plug-in to enable users to select encryption. TLS encryption is available; however, configuration is not exposed in the management interface and requires users to open a support ticket.
- SilverSky data centers are limited to the U.S.
- SilverSky relies on partners Cloudmark and Symantec (Brightmail) for malware and spam detection. Reference customers' satisfaction with SilverSky's spam detection accuracy is mixed.

Sophos

Sophos has been in the SEG market since 2003, and recently entered the UTM market with the acquisition of Astaro. It has a relentless focus on simplifying the management of its solutions. Its current flagship solution, the Sophos Email Appliance, is offered as hardware and virtual appliances. The company plans to consolidate the SEG features of its various product lines into a more focused

offering based on its network security platform. Sophos is a shortlist candidate for SMBs and larger enterprises looking for basic, low-administration, appliance-based solutions.

Strengths

- The management interface is very easy to use for a nontechnical user. Dashboards are very graphical and allow for some level of linked drill-down into log or reporting data.
- The included appliance-monitoring service allows Sophos to proactively monitor box health, install new version updates and provide optional remote assistance, thereby simplifying management.
- DLP and encryption are included with the Email Protection — Advanced license.
- Secure PDF Exchange (SPX) encryption functionality provides a push-based, password-protected PDF file encryption scheme with multiple options for senders to customize the recipient user experience.
- Sophos gets very high marks for customer service and support.

Cautions

- Sophos' focus on providing simple-to-manage appliances can be limiting for larger organizations. Advanced enterprise-class features (such as dashboard customization, log data visibility restrictions and advanced reporting) are all missing or weak. Sophos does not allow for per-user sending limits. Sophos still does all configuration of DKIM or SPF rules.
- Sophos offers no document stripping or time-of-click URL protection for targeted phishing threats.
- Encryption options do not include pull-based encryption.
- DLP workflow is weak. There is no compliance officer role or a specific quarantine to enable compliance-related workflow, such as building cases, annotating events or custom actions for email. Notifications for policy compliance are created for each event, rather than created as objects and referenced in policy.
- Although Sophos includes its SEG product with several suites, it does not yet provide a common interface to manage and monitor multiple products.
- Despite a focus on SMB customers, Sophos still does not offer a SaaS-based delivery option, although one is reportedly planned for 2014.

Symantec

Symantec is one of the largest SEG vendors by market share and continues to grow faster than the market. It has a broad range of mature SEG offerings, including hardware appliances, SaaS and virtual appliances (VMware). Symantec also offers archiving, e-discovery and enterprise DLP

solutions. The Symantec Messaging Gateway (SMG) and the Symantec Email Security.cloud service are good shortlist candidates for most organizations.

Strengths

- Symantec has a very large and sophisticated malware research team that has access to a significant amount of telemetry data from its very large consumer, Internet service provider, SMB and enterprise customer base.
- Bulk marketing classifiers help to move nuisance email into a separate quarantine.
- Symantec Email Security.cloud now provides outbound spam scanning for all customers.
- Symantec Email Security.cloud includes real-time link following to filter advanced threats.
- Symantec offers complex content-filtering policy constructs, such as negative-filtering conditions, multiple simultaneous content-filtering policies and early exit branches to stop further processing.
- SMG is offered as part of an endpoint and SWG package deal that is very attractively priced.
- Symantec is a Leader in the enterprise DLP market, and leverages the same content inspection engine and predefined content in its SEG solution. Recently, it improved the synchronization of the SMG quarantine management, incident status and workflow with the enterprise DLP solution, and improved content in the cloud solution.
- Symantec offers PGP encryption capability in addition to a partnership with ZixCorp or Echoworx.

Cautions

- Symantec has not been aggressive in releasing new product features, and the on-premises gateway is not the most polished solution for very large enterprises. The SMG administration could be refreshed with a more up-to-date customizable widget-based interface, better reporting and email disposition summary, and less-dense DLP policy configuration.
- SMG, an on-premises solution, has not released any specific advanced targeted threat solutions, such as time-of-click URL filtering or virtual sandboxing of attachments; however, a solution that strips active content from possibly malicious documents (that is, Office and PDF) is due in 4Q13.
- There is no management interface that can integrate across on-premises and service offerings for hybrid deployments, or offer pricing that allows users to swap between deployment types. Integration of other mail-related Symantec products, like archiving and e-discovery and the SEG product, is mostly limited to reporting and does not extend to the policy layer.
- DLP integration is improving for workflow, but not content synchronization. Symantec Email Security.cloud does not integrate with the enterprise solution.

- The licensed encryption solutions are not integrated with the management console; they lack self-service configuration of the encryption experience and significant control or visibility of sent messages.
- Depending on how the customer procures the service, Symantec support can be through the reseller channel rather than via direct access to Symantec, which can result in delays and an inconsistent support experience.

Trend Micro

Trend Micro is a major provider of anti-malware protection solutions, and was an early entrant in the SEG market. Its InterScan Messaging Security (IMS) deployment is offered on a broad range of delivery form factors, including software (Windows, Linux, Solaris and Exchange), virtual appliances (VMware and Hyper-V), software appliances for installation on any bare-metal hardware, and a SaaS and hybrid offering. Trend Micro also offers robust mail server security, which provides tools for security tasks that can't be accomplished at the gateway. Recent initiatives demonstrate a renewed SEG focus. Trend Micro remains a shortlist candidate for most organizations.

Strengths

- Trend Micro has a large and well-respected malware and spam research team, and it was one of the first vendors to address advanced targeted threats with the optional Deep Discovery Advisor (formerly called Dynamic Threat Analysis System [DTAS]), which inspects suspect files in a sandbox.
- Software and virtual versions come with an optional hybrid deployment choice, which provides reputation and coarse content filtering with integrated on-premises quarantine, management and reporting.
- Trend Micro offers a widget-based graphical management interface that each administrator can customize with predefined widgets.
- IMS provides native push-based (HTML) encryption with SaaS key management.
- Trend Micro's DLP management is centralized across its endpoint, Web and email solutions.
- Trend Micro's mail server security product, ScanMail, offers targeted attack prevention and URL scanning, and also includes a new feature called "Search and Destroy" for the eradication of malicious or noncompliant email from the mail store.

Cautions

- Several reference customers requested more granular reporting and longer log retention periods. They also requested better centralized management for multiple sites, simpler updating, and simpler and more intuitive configuration.
- Role-based administration is not domain-specific or group-specific, and there is no DLP compliance role.

- The SaaS offering is focused on SMBs. It does not offer archiving, mailbox hosting or disaster recovery/continuity services. Some, but not all, of the service's component parts are the same as the on-premises solution's.
- Corporate and user allow-lists are not synchronized between the SaaS-based prefilter and the enterprise solution, although they can be imported and exported.
- Native IMS DLP workflow capabilities are weak without integration with Trend Micro's Control Manager console.
- Encryption does not include a pull version.
- Deep Discovery Advisor does not address time-of-click malicious URLs.

Trustwave

Trustwave offers a diversified security portfolio, including a focus on compliance and managed security services. It has accumulated a number of security products, including SEG (MailMarshal) and email archiving. MailMarshal is a shortlist candidate for Trustwave customers.

Strengths

- The Windows-based management interface is capable and offers some advanced features, such as task shortcuts, scripting and support for batch file workflow commands. Role-based and multitenant management capabilities are a core strength.
- MailMarshal's Blended Threats Module uses time-of-click URL protection, which exploits the SWG proxy service. By default, it uses an automatically updated whitelist of communication recipients and connecting IP addresses to reduce false positives.
- Antivirus protection from Kaspersky Lab, McAfee, Norman or Sophos is provided as an option.
- Existing DLP capabilities — which include basic, regular expression matching and some predeveloped policies, dictionaries and number formats — will be augmented by Trustwave's enterprise DLP solutions.

Cautions

- Trustwave has small market share and has not significantly improved on the MailMarshal product, or gained any discernible sales growth since the acquisition.
- The solution has three management interfaces with little integration. There are limited dashboard elements with no hyperlinked drill-downs into reports. The policy interface is a legacy Windows application with a pop-up, Windows-style workflow.
- DLP capabilities are limited to a keyword analysis and do not include many predefined policies, dictionaries or lexicons, nor do they offer much workflow support for compliance officers.

- On-box encryption is limited to TLS, and advanced encryption (provided by ZixCorp) is not integrated with the management interface. Thus, advanced encryption lacks any control or visibility of sent messages, as well as self-service configuration of the encryption experience.
- Trustwave does not yet offer a SaaS service; however, there is one in development, and deployment is planned for 3Q13.

WatchGuard

WatchGuard is better known for its multifunction firewalls, but it offers a combined email and Web gateway appliance (including virtual) called Extensible Content Security (XCS). WatchGuard's primary user base is SMBs. However, the XCS SEG solution has a good mix of midsize and large North American enterprise customers. WatchGuard XCS is a good shortlist option for existing WatchGuard customers.

Strengths

- XCS provides SEG and SWG functionality in the same appliance (hardware or virtual version), and relevant policies can be set for both channels in the same management interface. The management interface was improved with more wizards to simplify deployment and management, with a frequent task screen, and with improved message tracking and reporting.
- XCS provides native clustering that creates a virtual machine mail queue. The message queue is mirrored across devices in clustered deployments for high availability.
- The DLP policy is shared across Web and email traffic. It includes financial and medical term dictionaries, as well as predefined number formats for common data types, such as credit cards and SSNs.

Cautions

- WatchGuard's mind share and market share remain very small. It is difficult for any company to compete in many markets and across many company segments — and to provide market-leading features in each market segment. Only a small percentage of WatchGuard's revenue is related to email security.
- The management dashboard could be improved with more enterprise-focused features.
- DLP policy could be improved with more predeveloped dictionaries and policies for common regulations, as well as better quarantine management options for compliance officers and broader content support (improvements are expected in 3Q13).
- Advanced encryption provided by Voltage Security is not integrated with the management interface.
- WatchGuard does not have SaaS offerings, although it is designed for and used in some MSSP offerings.

Websense

Websense announced plans to be purchased and taken private by Vista Equity Partners in June 2013. This acquisition could provide Websense with more access to capital, as well as an opportunity to reorganize and retool for longer-term growth without the quarterly demands of stock investors. Although it is perhaps better known for its SWG solutions, Websense has a growing presence in the SEG market with a SaaS offering (Websense Cloud Email Security [CES]), an appliance solution (Websense Email Security Gateway) and a hybrid solution (Websense Email Security Gateway Anywhere). All these solutions are based on the flagship Triton management interface, which combines SEG, SWG and enterprise DLP functionality in a single, unified content security solution. Websense is a good candidate solution for buyers that are looking for integrated SWG and SEG functionality, as well as advanced DLP capability.

Strengths

- All the various Websense solutions are tied together with the Triton management interface and reporting engine, which allows more customization in the latest version.
- Websense offers good targeted attack protection, with malicious URL analyses at the time of click, static code analysis of suspicious documents and drip DLP protection to detect data leaked in smaller chunks. Websense Email Security Gateway v.7.8 includes a virtual sandbox to analyze suspicious attachments in the cloud.
- The cloud service has 16 data centers located in 12 countries.
- Websense offers very strong DLP capabilities for this market. It includes numerous predefined DLP content dictionaries in 12 languages, plus additional compliance templates for items such as PCI Data Security Standard (DSS), state data privacy laws, the U.S. Health Insurance Portability and Accountability Act (HIPAA) and the Gramm-Leach-Bliley Act.
- Websense offers an archival service (via an OEM partner), and also a disaster recovery/business continuity service that provides an Outlook Web Access-type inbox and outbox.
- Websense Email Security Gateway is one of the few solutions in this report that enables administrators to view a false-negative and false-positive report in the dashboard.

Cautions

- Websense has a long history in the Web security market, but its mind share and market share in the SEG market are comparatively low. However, Websense is showing good growth in the enterprise market, primarily among customers that are looking for converged SEG, SWG and DLP.
- The Triton appliance is relatively new (announced in 2010). The Triton management interface can be very complex and involves numerous steps to create policies.
- Some customers have expressed frustration with support and service, so Websense is investing in improvements in these areas.

- CES message search is not quite in real time and could experience as much as a five-minute delay.
- Advanced encryption provided by Voltage Security is not integrated with the Triton management interface. Thus, it lacks any control or visibility of sent messages, and the self-service configuration of the encryption experience.
- The cloud-based encryption solution and DLP solution are not as fully featured as the on-premises offering.

Vendors Added or Dropped

We review and adjust our inclusion criteria for Magic Quadrants and MarketScopes as markets change. As a result of these adjustments, the mix of vendors in any Magic Quadrant or MarketScope may change over time. A vendor appearing in a Magic Quadrant or MarketScope one year and not the next does not necessarily indicate that we have changed our opinion of that vendor. This may be a reflection of a change in the market and, therefore, changed evaluation criteria, or a change of focus by a vendor.

Added

SilverSky is a new entrant in this year's analysis because it added a dedicated SEG product.

Dropped

Google is withdrawing from the stand-alone SEG market and migrating its remaining customers to a variation of enterprise Gmail. As a result, we have dropped Google from this analysis. Enterprise Gmail customers will continue to benefit from integrated SEG services, as in the past.

Other Vendors

This Magic Quadrant is not intended to be an exhaustive analysis of every vendor in this market, but rather a focused analysis of solutions that are most interesting to the majority of our clients. Other vendors were not included in this analysis because they do not fit the technical inclusion criteria. Sendmail is one vendor that has a respectable, large enterprise presence, but it takes a unique approach by offering a platform that enables enterprises to plug in various email security applications from other vendors. This approach enables enterprises to build their own solutions from component vendors, while offering an overall management framework and underlying scalable messaging transfer agent. Vendors such as AppRiver, Axway, Eleven and Spamina focus on a particular geographic or vertical market niche.

Inclusion and Exclusion Criteria

- The solution must have its own proprietary capabilities to block or filter unwanted email traffic.
- Supplementing the solution with third-party technology is acceptable.

- The solution must provide email virus scanning via its own or a third-party antivirus engine.
- The solution must provide basic intrusion prevention.
- The solution must offer email encryption functionality beyond TLS on its own, or via a third-party relationship.
- The solution must offer the ability to scan outbound email according to a set of basic vendor-supplied dictionaries and common identifiers (for example, SSNs, credit card numbers, bank account numbers and routing numbers).
- Vendors must have at least 2,000 direct (not via OEM) enterprise customers in production for their email security boundary products, and at least $10 million in revenue.
- Multifunction firewalls (also known as UTM devices) are outside the scope of this analysis, unless the SEG function can be purchased separately from the firewall function. These devices are traditional network firewalls that also combine numerous network security technologies (such as anti-spam, antivirus, network intrusion prevention systems and URL filtering) into a single box. Multifunction firewalls are compelling for the SMB and branch office markets. However, in most circumstances, enterprise buyers do not consider multifunction firewalls to be replacements for SEGs.

Evaluation Criteria

Ability to Execute

Vertical positioning on the Ability to Execute axis was determined by evaluating the following factors:

- Overall viability was given a heavy weighting because this is a mature and saturated market. Overall viability was considered not only in terms of the vendor's overall company revenue, channel reach, management team and resources, but also in terms of the importance of the email security unit to the company.
- Sales execution/pricing scores reflect a comparison product sales growth rate relative to the market during the analysis period.
- Market responsiveness and track record measured the speed at which the vendor has spotted a market shift and produced a product that potential customers are looking for. It also measured the size of the vendor's installed base.
- Marketing execution scores reflect the frequency with which Gartner customers are aware of a vendor or vendor's specific offering in this market. Vendors with well-known brands score well in this metric, as do vendors whose brands are closely associated with products in this market.
- Customer experience measured the quality of the customer experience based on reference surveys and Gartner client teleconferences. We incorporated research and reference call data on support responsiveness and timeliness, quality of releases and patches, and general experiences when installing and managing the product and service on a day-to-day basis.

- The operations score reflects the corporate resources (that is, management, business facilities, threat research, and support and distribution infrastructure) that the SEG business unit can draw on to improve product functionality, marketing and sales. We also took into consideration the focus and transitions of the SEG teams in acquired companies.

Table 1. Ability to Execute Evaluation Criteria

Evaluation Criteria	Weighting
Product/Service	No Rating
Overall Viability (Business Unit, Financial, Strategy, Organization)	High
Sales Execution/Pricing	Standard
Market Responsiveness and Track Record	High
Marketing Execution	Standard
Customer Experience	High
Operations	Standard

Source: Gartner (July 2013)

Completeness of Vision

The Completeness of Vision axis captures the technical quality and breadth of the product, as well as the vendor's organizational characteristics that will lead to higher product satisfaction among midsize-to-large enterprise customers, such as how well the vendor understands this market, its history of innovation and its geographic presence.

In market understanding, we ranked vendors on the strength of their commitment to this market in the form of strong product management, their vision for this market and the degree to which their road maps reflect a solid commitment of resources to achieve that vision.

We heavily weighted the product features of the vendors' flagship solutions in the Completeness of Vision criteria. Product features that Gartner deemed most important were:

- Anti-spam and anti-phishing effectiveness and investment in malware research, especially targeted attack detection
- Management and reporting functionality
- DLP capabilities
- Encryption capabilities
- Delivery form factor options

Other functionalities or solutions relevant to the buyer in the supplier's target market (such as archiving, disaster recovery and file transfer) were also taken into account.

Table 2. Completeness of Vision Evaluation Criteria

Evaluation Criteria	Weighting
Market Understanding	Standard
Marketing Strategy	No Rating
Sales Strategy	No Rating
Offering (Product) Strategy	High
Business Model	No Rating
Vertical/Industry Strategy	No Rating
Innovation	Standard
Geographic Strategy	Standard

Source: Gartner (July 2013)

Quadrant Descriptions

Leaders

Leaders are performing well, have a clear vision of market direction and are actively building competencies to sustain their leadership positions in the market. Companies in this quadrant offer a comprehensive and proficient range of email security functionality, and show evidence of superior vision and execution for current and anticipated customer requirements. Leaders typically have a relatively high market share and/or strong revenue growth, own a good portion of their threat or content-filtering capabilities, and demonstrate positive customer feedback for anti-spam efficacy and related service and support.

Challengers

Challengers execute well, but they have a less-defined view of market direction. Therefore, they may not be aggressive in preparing for the future. Companies in this quadrant typically have strong execution capabilities, as evidenced by financial resources, as well as a significant sales and brand presence garnered from the company as a whole or from other factors. However, Challengers have not demonstrated as rich a capability or track record for their email security product portfolios as vendors in the Leaders quadrant have.

Visionaries

Visionaries have a clear vision of market direction and are focused on preparing for it, but they may be challenged to execute against that vision because of undercapitalization, market presence, experience, size, scope and so on.

Niche Players

Niche Players focus on a particular segment of the client base, as defined by characteristics such as a specific geographic delivery capability or dedication to a more limited product set. Their ability to outperform or be innovative may be affected by this narrow focus. Vendors in this quadrant may have a small installed base, or may be limited (according to Gartner's criteria) by a number of factors. These factors may include limited investment or capability to provide email security threat detection organically, a geographically limited footprint, or other inhibitors to providing a broader set of capabilities to enterprises now and during the 12-month planning horizon. Inclusion in this quadrant does not reflect negatively on the vendors' value in the more narrowly focused market they service.

Context

- The total market revenue is peaking as it reaches saturation and primary feature maturity. Buyers should focus on more strategic vendors that will continue to accumulate market share.
- Consider the incumbent cloud-based email platform from Microsoft, which will typically offer "good enough" spam and malware protection for most organizations; however, additional providers may be necessary for advanced DLP, encryption and protection from more advanced threats.
- SaaS solutions are very attractive to organizations with less than 5,000 seats due to a lower total cost of ownership (TCO), lower customization requirements and a lack of resources to manage solutions. SaaS solutions are also attractive to larger organizations that favor outsourcing, as well as those that have highly distributed IT facilities and appreciate the ease of deployment and standardization that SaaS solutions provide. Hosted appliances can emulate the TCO and other advantages of SaaS, but without the sacrifice in advanced policy options.
- Pay careful attention to outbound email requirements such as DLP and encryption. These features are very differentiated across products.
- Organizations that are concerned about targeted attacks should consider attack prevention capabilities such as time-of-click URL protection and attachment sandboxing or code stripping as primary differentiators.

Market Overview

Based on our analysis for this report, the SEG revenue from the Magic Quadrant vendors plus Google grew at 1.9% in 2012 to $1.4 billion. We anticipate continued, low single-digit (2% to 3%) growth for the overall market. Despite the low overall growth, we do see individual vendors that are taking market share. In particular, Proofpoint and Symantec are growing at double-digit rates, while Google was the biggest market share loser — primarily due to its forced migration of customers to enterprise Gmail and then departing the market for new business.

Ancillary services, such as DLP and encryption, are the main drivers of growth, while traditional spam and virus-filtering services, as well as other license and subscription revenue, are declining. The increase in suite bundling, especially with hosted mailboxes, will blur the SEG market, making future growth and market size difficult to identify. As more business goes to Microsoft and Google for cloud mailboxes, those vendors will effectively increase their SEG market share to the detriment of all other vendors, because hygiene services come bundled with the mailboxes.

Vendors in the Leaders and Challengers quadrants account for approximately 87% of the market.

The increase in acceptance of the SaaS delivery form factor continues. We continue to be bullish on this form factor and note that most of the vendors in this analysis now offer a SaaS-type delivery option. Moreover, approximately 80% of client inquiries are regarding when it will be appropriate to migrate to the SaaS or cloud-based delivery services. However, we notice that SaaS is more attractive to smaller organizations and very large federated organizations. Midsize organizations (that is, 5,000 to 20,000 seats) don't see significant advantages or economies of scale, and remain concerned about confidentiality.

Recommended Reading

Some documents may not be available as part of your current Gartner subscription.

"Magic Quadrants and MarketScopes: How Gartner Evaluates Vendors Within a Market"

"MarketScope for Email Systems, 2011"

"The Cloud Email and Collaboration Services Market, 2011 Update"

"Moving Email and Web Security to the Cloud"

"Guidelines for Selecting Content-Aware DLP Deployment Options: Enterprise, Channel or Lite"

"Email Encryption: Protecting Your Content When Sending to External Recipients"

Evidence

[1] Symantec's "2013 Internet Security Threat Report, Volume 18"

This research was based on:

- A Magic Quadrant survey sent to vendors in April 2013
- An online survey of 96 vendor-supplied reference customers conducted by Gartner in May 2013
- An online survey of 31 vendor-supplied reference value-added resellers conducted by Gartner in May 2013
- Inquiry calls and other interactions with Gartner clients

Note 1 Gartner Online Survey Results

Gartner conducted an online survey of 96 vendor-supplied reference customers in May 2013. Forty-three percent of respondents had more than 5,000 seats, and 24% had fewer than 1,000 seats. Sixty-six percent of respondents were self-identified as being "responsible for daily operation, policy configuration and incident response"; 28% were responsible for "selection of the SWG solution"; and 6% said that they "get reports and help set policy."

Evaluation Criteria Definitions

Ability to Execute

Product/Service: Core goods and services offered by the vendor that compete in/ serve the defined market. This includes current product/service capabilities, quality, feature sets, skills and so on, whether offered natively or through OEM agreements/ partnerships as defined in the market definition and detailed in the subcriteria.

Overall Viability (Business Unit, Financial, Strategy, Organization): Viability includes an assessment of the overall organization's financial health, the financial and practical success of the business unit, and the likelihood that the individual business unit will continue investing in the product, will continue offering the product and will advance the state of the art within the organization's portfolio of products.

Sales Execution/Pricing: The vendor's capabilities in all presales activities and the structure that supports them. This includes deal management, pricing and negotiation, presales support, and the overall effectiveness of the sales channel.

Market Responsiveness and Track Record: Ability to respond, change direction, be flexible and achieve competitive success as opportunities develop, competitors act, customer needs evolve and market dynamics change. This criterion also considers the vendor's history of responsiveness.

Marketing Execution: The clarity, quality, creativity and efficacy of programs designed to deliver the organization's message to influence the market, promote the brand and business, increase awareness of the products, and establish a positive identification with the product/brand and organization in the minds of buyers. This "mind share" can be driven by a combination of publicity, promotional initiatives, thought leadership, word-of-mouth and sales activities.

Customer Experience: Relationships, products and services/programs that enable clients to be successful with the products evaluated. Specifically, this includes the ways customers receive technical support or account support. This can also include ancillary tools, customer support programs (and the quality thereof), availability of user groups, service-level agreements and so on.

Operations: The ability of the organization to meet its goals and commitments. Factors include the quality of the organizational structure, including skills, experiences, programs, systems and other vehicles that enable the organization to operate effectively and efficiently on an ongoing basis.

Completeness of Vision

Market Understanding: Ability of the vendor to understand buyers' wants and needs and to translate those into products and services. Vendors that show the highest degree of vision listen and understand buyers' wants and needs, and can shape or enhance those with their added vision.

Marketing Strategy: A clear, differentiated set of messages consistently communicated throughout the organization and externalized through the website, advertising, customer programs and positioning statements.

Sales Strategy: The strategy for selling products that uses the appropriate network of direct and indirect sales, marketing, service, and communication affiliates that extend the scope and depth of market reach, skills, expertise, technologies, services and the customer base.

Offering (Product) Strategy: The vendor's approach to product development and delivery that emphasizes differentiation, functionality, methodology and feature sets as they map to current and future requirements.

Business Model: The soundness and logic of the vendor's underlying business proposition.

Vertical/Industry Strategy: The vendor's strategy to direct resources, skills and offerings to meet the specific needs of individual market segments, including vertical markets.

Innovation: Direct, related, complementary and synergistic layouts of resources, expertise or capital for investment, consolidation, defensive or pre-emptive purposes.

Geographic Strategy: The vendor's strategy to direct resources, skills and offerings to meet the specific needs of geographies outside the "home" or native geography, either directly or through partners, channels and subsidiaries as appropriate for that geography and market.

GARTNER HEADQUARTERS

Corporate Headquarters
56 Top Gallant Road
Stamford, CT 06902-7700
USA
+1 203 964 0096

Regional Headquarters
AUSTRALIA
BRAZIL
JAPAN
UNITED KINGDOM

For a complete list of worldwide locations,
visit http://www.gartner.com/technology/about.jsp