G00259855

Magic Quadrant for Secure Email Gateways

Published: 1 July 2014

Analyst(s): Peter Firstbrook, Brian Lowans

The secure email gateway market is fractured between providers of basic protection delivered by embedded functionality from incumbent email, firewall, or endpoint protection solutions; and vendors that focus on the state of the art in advanced attack and information protection.

Strategic Planning Assumption

The secure email gateway market will shift its emphasis from spam filtering to data protection, with 38% of the 2013 market share belonging to vendors focusing on data protection doubling to 75% of the market in 2017.

Market Definition/Description

Secure email gateways (SEGs) provide basic message transfer agent functions; inbound filtering of spam, phishing, malicious and marketing emails; and outbound data loss prevention and email encryption.

The SEG market is mature. The penetration rate of commercial SEG solutions is close to 100% of enterprises. Buyers are becoming more price-sensitive; 80% of recently surveyed reference customers said that price was important or very important in their next SEG purchase (see Note 1). 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 slightly again in 2013[1] as spammers moved to other mediums, such as social networks, but spam still represents as much as 66% of email. Phishing and malware attachments also declined slightly in 2013; however, there is ample evidence that email is the preferred channel to launch advanced targeted attacks.

Based on our analysis for this report, the SEG revenue from the Magic Quadrant vendors in 2013 was $1.3 billion, growing at roughly 7% over 2012. The total market (that is, including other vendors) is estimated to be $1.7 billion, growing at 4% over 2012. This suggests that market share is moving to the Magic Quadrant vendors. We anticipate continued, low single-digit growth (2% to 4%) for the overall market. Despite the low overall growth, we do see individual vendors that are taking market share. In particular, Proofpoint and Trend Micro recorded the largest increases, while

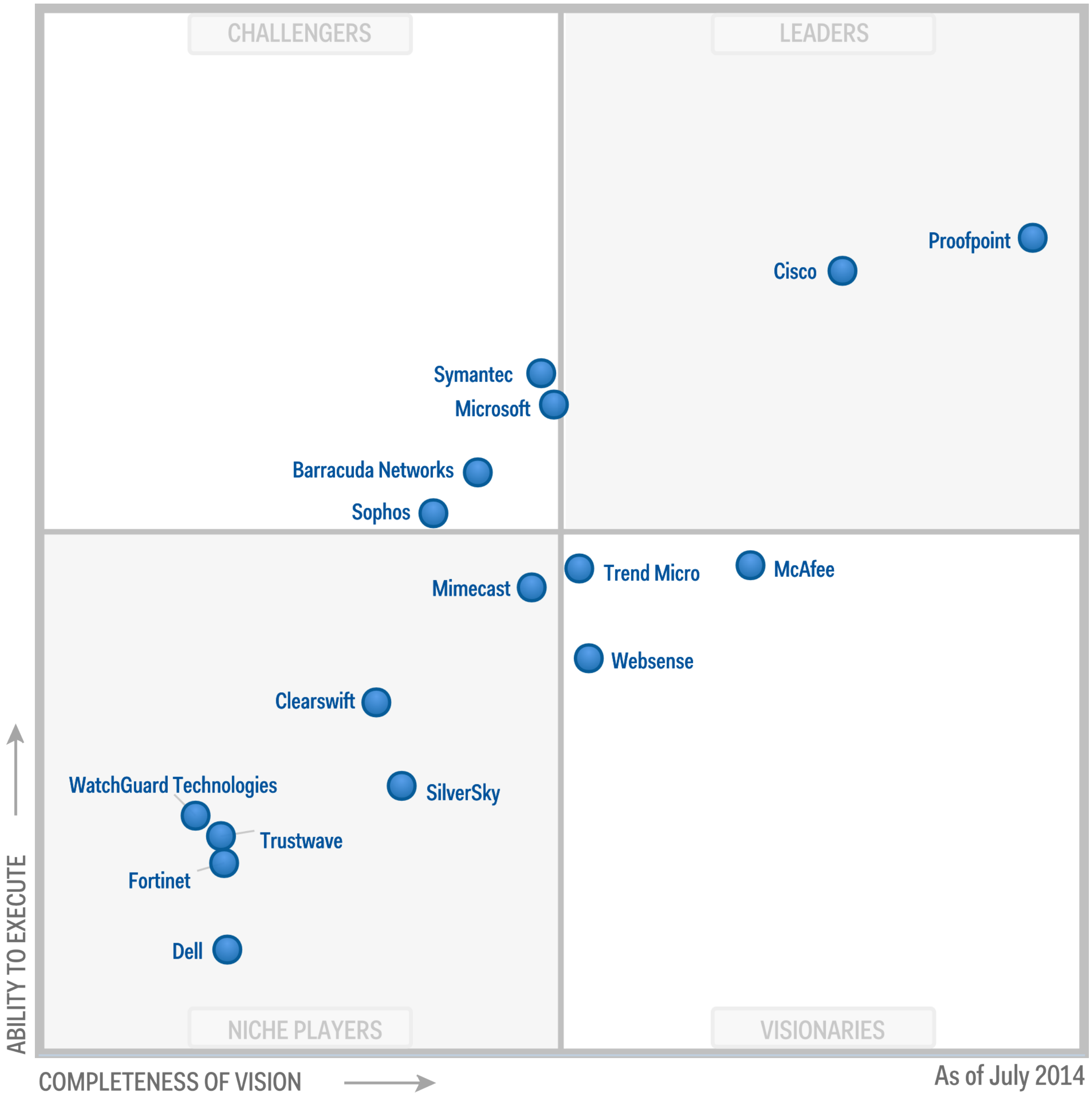
Google was the biggest market share loser — primarily due to its forced migration of customers to enterprise Gmail and then departing the market for new business.

Ancillary services, such as targeted attack prevention, data loss prevention (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.

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 concern when it will be appropriate to migrate to SaaS or cloud-based delivery services. SaaS-type solutions are generally less expensive for most organizations of less than 5,000 seats. Organizations not considering SaaS solutions often cite information confidentiality and reduced configuration flexibility as barriers to adoption.

Magic Quadrant

Figure 1. Magic Quadrant for Secure Email Gateways



Source: Gartner (July 2014)

Vendor Strengths and Cautions

Barracuda Networks

Barracuda Networks 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 slightly above market rates. Barracuda Spam Firewall appliances are shortlist candidates for organizations that are seeking "set and forget" functionality at a reasonable price.

Strengths

- Barracuda added an optional Avira Antivirus engine in addition to Clam AV, and now offers a cloud-based sandbox (from Lastline) to inspect suspect attachments at no additional charge.
- The solution offers an optional cloud-based prefilter, which filters out obvious spam before final filtering is done on-premises at no additional cost.
- Native basic pull-based encryption and DLP capability are included free of charge, and spam and malware services are based on appliance size, 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. The Barracuda Control Center is a free cloud-based offering that can manage multiple Barracuda Spam Firewall appliances and other Barracuda network appliances.

Cautions

- Barracuda is typically a fast follower rather than a leader in new functionality.
- The user interface and reporting engine are long overdue for a refresh (due in 3Q14). 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. DLP regular expressions are not the same across all Barracuda products.
- The included encryption capability is a good value; however, even though the pull email operates smoothly, it could be better optimized for mobile devices and does not include push options (see Note 2).

Cisco

Cisco remains the market share leader for dedicated on-premises solutions for midsize to large organizations, but has lost 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 Cisco customers.

Strengths

- Cisco's optional Outbreak Filters option provides targeted attack protection including time-of-click URL proxy filtering and a cloud-based file sandboxing solution called Advance Malware Protection (AMP). The recent acquisition of ThreatGRID will provide an on-premises sandbox appliance as well as better threat information exchange between Cisco products, partners and customers.
- Embedded URLs can be filtered according to the URL categories (that is, gambling, games, alcohol) to align with acceptable usage policies, as well as URL reputation.
- Cisco has excellent scalability/reliability, an easy-to-use management interface, very extensive policy control and very granular message transfer agent (MTA) control capabilities.
- 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 the enterprise DLP of RSA, The Security Division of EMC.
- Cisco 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.

Cautions

- The AMP sandbox overlaps with sandbox functionality from the recent acquisition of ThreatGRID, creating buying and convergence confusion.
- Reference customers noted a desire for better, more granular reporting and monitoring options.
- Cisco's focus on the needs of large enterprises doesn't always scale down well for SMBs.
- Cisco does not offer a multitenant SaaS solution. The hosted solution is too expensive for SMBs.
- Cisco spam filtering is highly reliant on reputation, which is less effective for lower-volume snowshoe spam.
- Cisco's hosted email offering has only four data centers in the U.S. and Europe so far.
- Email encryption supports only push-based encryption with a cloud-based key server. The overall encryption recipient experience was poor and overly complex. Mobile recipient experience was very poor.

- 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); The former PostX functionality will continue to be available via Cisco partner Totemo. Cisco continues to offer on-box push-based encryption.

Clearswift

Clearswift has a long-established presence in the SEG market, primarily in the U.K., Europe and Asia/Pacific. The company is expanding its focus to the data protection and information governance markets. In the SEG market, Clearswift offers hardware appliances, a bare-metal software and VMware/Hyper-V solutions, and a recently added managed service. Clearswift is a reasonable shortlist candidate for buyers looking for broader data protection and information governance solutions.

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 Clearswift DLP engine provides fast scanning of more than 150 file formats. It offers a selection of prebuilt patterns for common data types, as well as common Boolean and proximity operators. Recent improvements include structured data identification and redaction capabilities, including document sanitization to remove content in properties, and revisions and removal of active content. The Adaptive Redaction feature can be used to remove active code on inbound attachments.
- 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

- Recent management changes are starting to demonstrate improved execution; however, Clearswift's market share and mind share remain very low in a rapidly maturing market. Market presence is mainly limited to the U.K. and Asia/Pacific.
- Although the interface is easy to use for nontechnical users, it is limited in detail for more technical enterprise users. Reference customers reported a desire for improved reporting and policy granularity, as well as bulk import and export options.
- The native push-based encryption required the download and installation of an encrypted mail reader.

- Advanced encryption provided by Echoworx is not integrated with the native push-based encryption solution or the Clearswift management interface.

Dell

Dell SonicWALL offers a broad suite of network security solutions aimed primarily at midsize organizations. Its portfolio of products includes firewalls, virtual private networks and a range of 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 for existing or prospective 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 Security stack. Dell recently added hosted outbound protection and a European data center.
- 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 was the first vendor to offer 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. Dell partners with DataMotion for email encryption.

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 SonicWALL has a minimal market share of the SEG business, and it is a very small percentage of Dell's overall business.
- Dell continues to receive the lowest score in overall customer satisfaction compared with other vendors in this analysis. Reference customers commented on the necessity for better spam 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.

- Encryption is offered via an OEM of DataMotion. Push- and pull-based PDFs are difficult to view on a mobile device.

Fortinet

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

Strengths

- FortiMail recently added integration with the FortiSandbox appliance, which executes suspect code in a sandbox to detect malware. It also offers a cloud FortiSandbox option.
- 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. 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

- 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. Fortinet has a very small market share of the SEG business, and it is a very small percentage of Fortinet's overall business. Fortinet offers only its own antivirus scan engine, does not have a well-known research organization, and would benefit from more antivirus options.
- Fortinet is missing more-advanced MTA functions for larger enterprise or more-demanding environments. Fortinet does not provide a classification for marketing email.
- 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 still no SaaS deployment option. DLP functionality is relatively basic; it lacks good policy or compliance workflow, or deep content inspection capabilities.

McAfee

McAfee, part of Intel Security, has a broad range of endpoint and network security products that are increasingly integrated by a common malware sandbox function and a data exchange layer for threat context sharing. McAfee offers appliances, virtual, SaaS and hybrid deployment options. In this analysis, McAfee's execution score was impacted primarily by poor market growth, dropping it into the Visionaries quadrant. McAfee is a good choice for current 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) data feeds. Email protection optionally integrates with the on-premises malware sandbox and provides time-of-click on-box Web proxy. 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.
- Both push and pull encryption are included in the on-premises or hybrid version at no additional charge. McAfee Email Protection also supports the secure transfer of 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. McAfee customers can switch between on-premises and SaaS solutions without an additional charge. Email continuity is a feature of the SaaS offering.
- McAfee Content Security Suite, which includes email, Web and DLP products deployed as SaaS, virtual or both, is attractively priced.

Cautions

- McAfee has not significantly expanded its market share in the enterprise SEG market over the past three years, especially relative to its channel and brand. Interviews with Gartner clients and reference customers show that customer satisfaction remains lower than average. These issues continue to affect its Ability to Execute score.
- Reference customers cited spam accuracy as an issue. The malware sandbox is currently available only for on-premises deployments. A multitenant implementation is planned.
- 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 without the full McAfee enterprise DLP solution.

- 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.
- The user experience to access push or pull emails via mobile can be poor, with awkward operation, and attached documents may not be viewable.

Microsoft

Microsoft has now consolidated all its SEG 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 building out the service capabilities with biweekly releases. Lack of target phishing protections forced Microsoft back into the Challengers quadrant this year. However, other recent improvements and a solid commitment to the market make it a de facto shortlist contender for all Exchange and especially Microsoft Enterprise Agreement customers.

Strengths

- Microsoft provides very tight integration of SEG functions with Exchange and Outlook. 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 and Outlook Web Access clients.
- EOP mirrors email across multiple data centers for redundancy. Microsoft supports geoboundaries of the U.S., EMEA and China for mail processing including failover.
- The release of Office 365 Message Encryption is a major improvement over previous Encryption solutions. This push-based encryption service leverages a Microsoft account password, enabling single sign-on for multiple senders and transparent authentication for users already authenticated to Microsoft services such as Office 365, Outlook, Skype, OneDrive and Xbox Live. Azure Rights Management stores the encryption keys in the region the customer is provisioned: North America, South America, Europe or Asia/Pacific. For U.S. government customers, the keys are stored in U.S. data centers.
- 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 accelerating feature improvements. However, it lags behind in advanced targeted attack detection techniques (that is, time-of-click URL filtering and malware sandboxing). Reference customer satisfaction with spam detection was very low. Some existing customers experienced transition issues with the migration from the legacy Forefront Online Protection for Exchange (FOPE) infrastructure to EOP (see "Forefront Online Protection for Exchange [FOPE] Transition Center").

- Microsoft does not support push-based encryption, although the HTML attachment provides a Web mail client look and feel. The Microsoft account setup experience is independent of the encrypted email flow. Forcing customers to create a Microsoft account may not be optimal for large-enterprise accounts. Encrypted emails and the account setup process are difficult to view on mobile devices.
- Microsoft's DLP capability is isolated to the email channel only (although SharePoint DLP was recently announced), and provides only regular expression and file fingerprint detection rules. Customization is supported only via the editing of an XML file.
- EOP does not allow end-user-specific blocklists directly from the spam quarantine or digest, although users can create and manage individual blocklists through Outlook/Outlook Web Access, with this information synchronized through directory synchronization and enforced in EOP.

Mimecast

Mimecast remains one of a few companies in this analysis that is solely dedicated to email security and management issues, including mailbox hosting. Its broader focus is more on the management of corporate unstructured data. The company is more end-user-focused than most in this report, with security options made available to end users through an Outlook plug-in. In this analysis, the company drifted back into the Niche Players quadrant due primarily to incomplete targeted attack protection. Mimecast is a good fit for organizations looking for archiving and SEG, and for those seeking to provide knowledge workers with email utilities to improve collaboration.

Strengths

- Targeted Threat Protection includes URL time-of-click protection, which checks the site for malware before a client is redirected, and provides granular reporting.
- Mimecast has a multitenant SaaS email infrastructure with simple administration for SEG, continuity and archiving. SaaS storage options are available from 12 data centers in the U.S., Canada, Europe, South Africa and Asia/Pacific. Role-based administration is expansive for federated customers with multiple domains to manage.
- 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. Archive, search and disaster recovery are also integrated with Outlook. Encryption is pull-based or Transport Layer Security (TLS), and can be invoked by end users via the Outlook plug-in policy. The new Large File Send product allows users to exchange files.
- 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.

Cautions

- Mimecast has a strong regional market presence in the U.K. and South Africa but very low market share overall. As buyers increasingly look for more-strategic integrated vendors, Mimecast will have a difficult time standing out in a crowded market.
- Mimecast has a small malware/spam research team. Thus, it is dependent on partners for a portion of its spam and malware detection capabilities. It does not offer a sandbox option for advanced targeted threat detection capability. Many organizations are reluctant to deploy additional Outlook plug-ins.
- The encryption service is difficult to use on mobile devices and does not include a push mechanism.
- The Large File Send capability requires deployment of the latest Outlook plug-in, or an app for Mac users.

Proofpoint

Proofpoint continues to lead the market with R&D investments in innovative features and corporate acquisitions to complement its enterprise capability (for example, Sendmail Inc., Armorize Technologies and NetCitadel). It clearly has the sharpest focus on email security issues, resulting again in one of the highest growth rates in this market. 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. Proofpoint Essentials is a multitenant SaaS solution targeted at 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 Filter Effectiveness"). The company continues to invest in new, innovative techniques for spam detection, and gets high marks from reference customers.
- Proofpoint provides spam classifiers (adult, bulk mail, phish and suspected spam) to enable a more granular policy.
- Proofpoint's Targeted Attack Protection service provides time-of-click URL protection and Attachment Defense (stripping and sandboxing of email attachments), 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 also offers email continuity services.
- 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 very high, especially for fully loaded appliance packages. However, like other enterprise solutions, discounts are available.
- The Secure Share large file attachment portal and Proofpoint Encryption currently do not use the same authentication system. Encryption recipient experience on mobile devices is poor.
- Proofpoint, due to its corporate focus on more demanding large-enterprise customers and high prices, is a poor fit for smaller organizations that do not require advanced controls, although Proofpoint Essentials provides a simpler experience.
- 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. Other requested features improvements include searching of buffers, and dedicated appliance roles to separate mail processing from administration workloads.

SilverSky

SilverSky 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 — particularly financial services firms.

Strengths

- Since last year's Magic Quadrant, Targeted Attack Protection was bolstered by the addition of attachment sandboxing. SilverSky has added custom reporting, DKIM and SPF configuration, and configurable opportunistic TLS with pull-style encryption fallback.
- SilverSky has a single, easy-to-use interface for Exchange hosting, SEG security and archiving. Role-based access control was recently added, restricting SilverSky admins from accessing customer data without an invitation token.
- SilverSky provides good DLP and encryption functions. DLP policy is configured on one page with conditional drop-down lists and an object-oriented policy. Recent enhancements include regulatory policy content to simplify compliance policy without professional services. Native pull-based encryption capabilities are available.
- SilverSky is a good fit for financial services organizations because it is audited annually by the U.S. Federal Financial Institutions Examination Council (FFIEC).

Cautions

- SilverSky is best-suited for organizations looking for a hands-off approach or those seeking to outsource the entire email infrastructure. It has been relatively late in delivering enterprise features.
- The vendor does not offer time-of-click URL protection, and the sandboxing technique is new and relatively untested.
- Email encryption supports only pull-style encryption. SilverSky relies on partners Cloudmark and Symantec (Brightmail) for malware and spam detection. Reference customers' satisfaction with SilverSky's spam detection accuracy is mixed.
- Reference customers commented on the management interface rendering speed.

Sophos

Sophos has been in the SEG market since 2003, and recently entered the unified threat management (UTM) market with the acquisition of Astaro and Cyberoam Technologies. It has a relentless focus on simplifying the management of its solutions. Its current flagship solution, 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 and those seeking to consolidate network security into a single platform.

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.

- Recent improvements include support for DKIM and SPF, and improved Japanese and snowshoe (low volume) spam detection.
- 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 integrated to provide policy-based encryption, and included with the Email Protection — Advanced license. DLP is fully integrated with client and secure Web gateway (SWG) policy reporting and management.
- 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 does not provide attachment sandboxing or time-of-click URL protection for targeted phishing threats.
- Encryption options do not include pull-based encryption.
- DLP workflow is missing some features. 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 for email filtering, although one is planned for 2015.

Symantec

Symantec is one of the largest SEG vendors by market share. It has a broad range of mature SEG offerings, including hardware appliances, SaaS and virtual appliances (VMware and Hyper-V). Symantec also offers archiving, e-discovery and enterprise DLP solutions. In this analysis, Symantec drifted back in Completeness of Vision due to a lack of leading targeted phishing features and a confusing encryption strategy, and slightly down in Ability to Execute due to corporate management uncertainty, placing it in the Challengers quadrant. However, we still view the Symantec Messaging Gateway (SMG) and the Symantec Email Security.cloud service as 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. Symantec recently added a Disarm feature to the messaging gateway, which removes exploitable content from Microsoft Office and PDF attachments.
- Symantec Email Security.cloud provides outbound spam scanning for all customers.
- SMG offers complex content-filtering policy constructs, DMARC validation, and message-rate shaping controls.
- Symantec is a leader in the enterprise DLP market, and leverages the same content inspection engine and predefined content in its SEG solution. It continues to improve interoperability between the SMG and enterprise DLP product. The cloud-based DLP capability was improved with simpler, more effective policy creation and improved content and integration with the Symantec Web Security.cloud product.
- Symantec offers PGP encryption capability for on-premises deployments in addition to ZixCorp or Echoworx encryption solutions for cloud customers.
- SMG is offered as part of an endpoint and SWG package deal that is very attractively priced.

Cautions

- Despite its market share and channel reach, Symantec rarely appears on large-enterprise shortlists. A majority of SMG acquisitions are bundled deals. 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.
- Despite its notable malware research capability, Symantec is late to the market with common advanced targeted threat features such as time-of-click URL filtering or virtual sandboxing of attachments or advanced reporting (some of which is due in 1H15). The Disarm feature is available only in on-premises solution.
- There is very little integration between the various Symantec email products or between the cloud and on-premises solutions. Symantec recently reorganized the cloud and on-premises offerings along with secure Web gateway products into a new Gateway Security Group business unit, which should provide better integration across these product lines going forward.
- Symantec DLP integration is improving for SMG; however, Symantec Email Security.cloud does not integrate with the enterprise DLP solution.
- Symantec's encryption proposition requires simplification. In addition to in-house PGP for on-premises, it licenses encryption capabilities from ZixCorp and Echoworx for the cloud SEG offering. Symantec has improved the tracking and reporting of encrypted messages and is introducing new advanced capabilities, but should strengthen self-service configuration to further improve the management experience.

Trend Micro

Trend Micro is a major provider of threat and data 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, 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 including targeted attack protection demonstrate a renewed SEG focus, moving it into the Visionaries quadrant. Trend Micro remains a shortlist candidate for most organizations.

Strengths

- Trend Micro has a large and well-respected malware and spam research team. The optional Deep Discovery Email Inspector provides a malware and URL sandbox analysis.
- 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.
- Trend Micro's DLP management policy and reporting is centralized across its endpoint, Web and email solutions. IMS provides native push-based (HTML) encryption with SaaS key management.
- 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. It also added URL classification policy options.

Cautions

- Almost half of Trend Micro customers acquire the solution via a bundled deal with the endpoint, rather than a dedicated competitive analysis of prospect solutions. Several reference customers requested more granular reporting and longer log retention periods. They also asked for better centralized management for multiple sites, simpler updating, and uncomplicated and more intuitive configuration. Role-based administration is not domain-specific or group-specific, and there is no DLP compliance role. Deep Discovery Email Inspector does not address time-of-click malicious URLs.
- 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 those for the on-premises solution. 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, and the registration process is overly complex and not mobile-device-friendly.

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 Trustwave Secure Email Gateway (formerly known as M86 MailMarshal Secure Email Gateway) and email archiving. Trustwave Secure Email Gateway 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.
- Trustwave'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 or Sophos is provided as an option.
- DLP capability was recently upgraded to version 2 based on Vericept's DLP engine and content classifications.

Cautions

- Trustwave has small market share and has not significantly improved on the MailMarshal product that it obtained as part of the acquisition of M86 Security, and has not 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.
- 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.

WatchGuard Technologies

WatchGuard is better-known for its multifunction firewalls, but it offers a combined email and Web gateway appliance named Extensible Content Security (XCS). WatchGuard's primary user base is SMBs. However, the XCS SEG solution has a good mix of midsize- and large-enterprise customers. WatchGuard XCS is a good shortlist option for current 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 benefits from wizards to simplify deployment and management, a frequent task screen.
- Recent improvements include support for IPv6, internationalized language and Hyper-V.
- 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 national IDs.
- Encryption is provided by an OEM agreement with Voltage Security.

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. There are no targeted phishing attack protection techniques. The management dashboard could be improved with more enterprise-focused features such as centralized quarantine search.
- 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.
- Advanced encryption provided by Voltage Security is not integrated with the management interface. Voltage requires a mobile app to view encrypted messages on a mobile device. App passcode is different than email passcode, complicating the experience.
- WatchGuard does not have SaaS offerings, although it is designed for and used in some MSSP offerings.

Websense

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. Virtual versions of the Email Security Gateway are now available. Triton can also be deployed in a monitor mode with Websense's RiskVision technology, allowing customers to quickly evaluate their security posture
- Websense offers good targeted attack protection by leveraging cross-product threat intelligence, including malicious URL analyses at the time of click, cloud-based ThreatScope File Sandboxing and drip DLP protection to detect data leaked in smaller chunks. Reporting has been improved to address targeted attack analysis, and Websense provides a built-in phishing education service.
- Websense offers very strong DLP capabilities for this market. It includes numerous predefined DLP content dictionaries in 12 languages, plus additional compliance templates for common regulations. DLP capability is fully integrated across Web, email, and endpoint for management reporting and policy.
- Websense recently built native on-premises encryption capabilities to provide pull encryption at no additional cost, as well as an optional push-based OEM of Voltage for push-based encryption.
- 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. The cloud service has 20 data centers located in 14 countries.
- 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. Websense growth in the enterprise market is primarily driven by customers looking for converged SEG, SWG and DLP to leverage their shared threat intelligence capabilities.
- 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. Some have already been implemented, including increased resources. All are expected to be complete by the second half of 2014.
- CES message search is not quite in real time and could experience as much as a five-minute delay.
- Pull encryption experience is different from push, with different authentication mechanisms. 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. Voltage requires a mobile app to view

encrypted messages on a mobile device. The app passcode is different from email passcode, which complicates the experience.

- The cloud-based encryption solution and DLP solution are not as fully featured as the on-premises offering. Websense is investing in cloud-based DLP to achieve parity with the on-premises offering.
- The Triton user interface looks dated compared to other products in this evaluation. A new cloud-based user interface with a modern look and feel is due out in 3Q14, along with an improved reporting experience.

Vendors Added and 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's appearance 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. It may be a reflection of a change in the market and, therefore, changed evaluation criteria, or of a change of focus by that vendor.

Added

No new vendors were added this year.

Dropped

No vendors were dropped this year.

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, Social Security numbers, 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 SEG 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 reference channel resellers' relative satisfaction with the company and product, averaged over the past three years.
- **Market responsiveness/record** measures 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 and the revenue and customer growth rate of the solution over the past fiscal year.
- **Customer experience** measures the quality of the customer experience based on customer reference surveys as well as 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.
- **Product or service** was not weighted on this axis because of its overweighting in the Completeness of Vision axis. As such, readers should consider Ability to Execute as an evaluation of the organization's business success.

Table 1. Ability to Execute Evaluation Criteria

Evaluation Criteria	Weighting
Product or Service	Not Rated
Overall Viability	High
Sales Execution/Pricing	Medium
Market Responsiveness/Record	High
Marketing Execution	Medium
Customer Experience	High
Operations	Medium

Source: Gartner (July 2014)

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 truly innovative new features or merely functionality that other vendors have long provided.
- We heavily weighted the **offering (product) strategy** features of the vendors' flagship solutions in the Completeness of Vision criteria. Product features that Gartner deemed most important were:
  - Reference customer satisfaction with anti-spam and anti-malware effectiveness over the past three years
  - Investment in targeted attack detection, such as URL time-of-click protection and attachment sandboxing
  - Marketing and graymail classification and personalized controls for the management of this type of unwanted email
  - DLP capabilities
  - Encryption capabilities

  - Delivery form factor options
- **Innovation** scoring provides an extra boost to vendors that are consistently leading the market with innovation rather than following.
- **Geographic strategy** scoring reflected the extent to which a supplier was truly global in scale or was restricted to business in select markets.

Table 2. Completeness of Vision Evaluation Criteria

Evaluation Criteria	Weighting
Market Understanding	Medium
Marketing Strategy	Not Rated
Sales Strategy	Not Rated
Offering (Product) Strategy	High
Business Model	Not Rated
Vertical/Industry Strategy	Not Rated
Innovation	Medium
Geographic Strategy	Medium

Source: Gartner (July 2014)

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 more pragmatic approach to market direction. Therefore, they may not be aggressive in offering new features until they are challenged by customers and potential customers. 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. Often, products are bundled to gain market share.

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

- Buyers in more demanding organizations that favor best-of-breed solutions should focus on inbound targeted attack protection and outbound DLP and encryption functionality, which are major differentiators.
- Buyers looking for encryption should extensively test encryption capability of prospective solutions. Recipient experience varies dramatically and mobile recipient experience can be excruciatingly painful. In our limited test, seven of 16 messages failed to open on the initial attempt.
- Exchange customers, especially those with premium licensing or enterprise agreements, should definitely consider the integrated Microsoft Exchange Online Protection capability, which provides "good enough" spam and malware protection, DLP and basic encryption for most organizations. Microsoft also has a robust road map. Other incumbent solutions from Google, endpoint protection vendors or UTM vendors will also present a good opportunity for good enough performance at reasonable suite-based prices.
- 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.

- More demanding organization should look for hosted appliance offerings that can emulate the TCO and other advantages of SaaS, but without the sacrifice in advanced policy options.

Market Overview

Better protection from targeted phishing attacks is the most critical inbound protection capability (97% of respondents indicated that this was an important or very important capability). More SEG vendors this year are incorporating targeted phishing detection methods. The two most popular methods include time-of-click URL filtering and attachment sandboxing. Time-of-click URL filtering techniques 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. Sandboxing is a technique that executes 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.

Seventy-five percent of respondents to our 2014 survey (see Note 1) indicated that bulk email filtering will be 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. A recent ISP test[2] showed that on average, 75% of email delivered is bulk email. 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. Several vendors are incorporating personal controls to enable end users to better manage their inboxes in future versions, and dedicated vendors such as Vade Retro can provide an add-on bulk mail solution.

Interest in outbound email hygiene continues. Outbound capabilities, such as data loss prevention (DLP) and encryption, remain the most important feature differentiators. Slightly less than 40% of respondents indicated that they already use DLP. Although interest has remained high in adding this functionality, over the past several surveys we note that actual DLP usage has not grown significantly since 2012. 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.

The use of encryption by survey participants jumped significantly this year as 52% of respondents indicated they already use email encryption beyond TLS (see Note 1). Only 22% indicated they had no plans for encryption. However, existing encryption customers are expressing frustration with the usability of encryption for senders and recipients, especially on mobile devices. Indeed, our analysis resulted in numerous failed messages and very frustrating experience on mobile devices. A key consideration is the encryption solution's level of integration in the SEG management interface. Support for both push- and pull-based encryption is also desirable (see Note 2).

Significant interest in and deployment of virtual solutions and 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 (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.

Gartner Recommended Reading

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

"How Gartner Evaluates Vendors and Markets in Magic Quadrants and MarketScopes"

"Addressing Targeted Phishing and Data Loss"

"Microsoft Office 365 Finally Breaks Free From Its On-Premises Legacy"

"Exchange 2013: A Bridge to the Microsoft Cloud"

"2013 Buyer's Guide to Content-Aware DLP"

"Define the Use Case Before Investing in Email Encryption"

Evidence

This research was based on:

- A Magic Quadrant survey sent to vendors in April 2014
- An online survey of 107 vendor-supplied reference customers conducted by Gartner in April and May 2014
- Three online survey of 90 vendor-supplied reference value-added resellers conducted by Gartner in May 2012, May 2013 and May 2014
- Inquiry calls and other interactions with Gartner clients

[1] Symantec's "Internet Security Threat Report 2014," Volume 19, April 2014

[2] Vade Retro ISP test, June 2014

Note 1 Gartner Online Survey Results

Gartner conducted an online survey of 107 vendor-supplied reference customers in April and May 2014. Fifty-two percent of respondents had more than 5,000 seats, and 24% had fewer than 1,000 seats. Sixty-three percent of respondents were self-identified as being "responsible for daily operation, policy configuration and incident response"; 32% were responsible for "selection of the SWG solution"; and 5% said that they "get reports and help set policy."

Note 2 Push vs. Pull Encryption Techniques

"Push"-based encryption describes solutions that deliver the sensitive content directly to the recipient's email inbox as an encrypted attachment, generally PDF or HTML documents. Push solutions allow the recipient more control over the received content and are generally easier to use for the recipient.

"Pull"-based encryption describes solutions that host the sensitive content in a Web server and include only a URL in the email inbox. The URL redirects the user to the Web portal for authentication and provides a Web mail-like inbox experience for the recipient to view encrypted messages and potentially reply to the sender. Pull solutions can be integrated with, and drive traffic to, corporate websites and provide the sender with more control over the content.

Evaluation Criteria Definitions

Ability to Execute

Product/Service: Core goods and services offered by the vendor for 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: 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/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 to 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