LICENSED FOR DISTRIBUTION

Gartner

Magic Quadrant for Secure Email Gateways

2 July 2013 ID:G00247704

Analyst(s): Peter Firstbrook, Brian Lowans

VIEW SUMMARY

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.

Market Definition/Description

This document was revised on 26 July 2013. The document you are viewing is the corrected version. For more information, see the Corrections page on gartner.com.

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

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.

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.

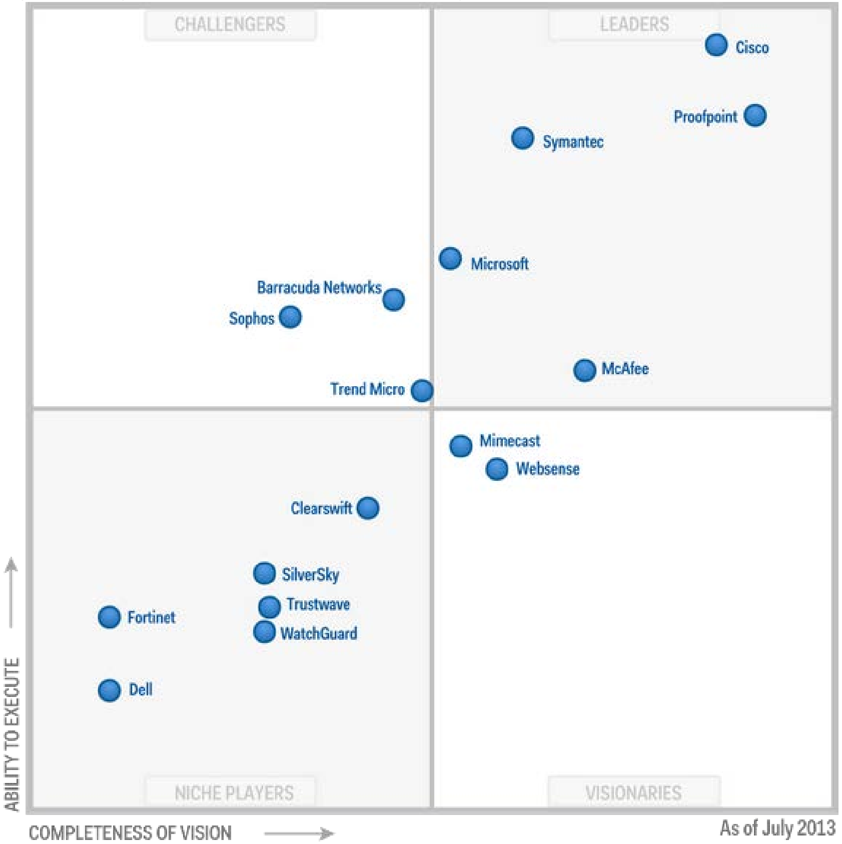
mobile devices. A key consideration is the encryption solution's level of integration in the SEG management interface.

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.

▲ Return to Top

Magic Quadrant

Figure 1. Magic Quadrant for Secure Email Gateways



As of July 2013

Source: Gartner (July 2013)

▲ Return to Top

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.

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.

- 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.

▲ Return to Top

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.
- 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.

▲ Return to Top

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.

▲ Return to Top

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.

Return to Top

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.

Return to Top

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

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS

Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS

Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS

Sync your system to PACER to automate legal marketing.

WHAT WILL YOU BUILD? | **sales@docketalarm.com** | **1-866-77-FASTCASE**