Magic Quadrant for Secure Web Gateway

Gartner RAS Core Research Note G00172783, Peter Firstbrook, Lawrence Orans, 8 January 2010

The SWG market continues to experience solid growth as enterprise customers scramble to improve defenses from an increasingly hostile Internet and safely use increasingly interactive Web applications.

WHAT YOU NEED TO KNOW

The secure Web gateway (SWG) is a critical tool for protecting endpoints from various forms of malware and other security risks, and for monitoring and controlling potentially dangerous Web traffic.

Proactive inbound and outbound security filtering technology should be the No. 1 consideration when selecting an SWG solution.

Ease of administration and scalable reporting is the second most important consideration, and there is significant differentiation in this aspect of solutions.

Organizations must consider mobile devices and smaller branch offices when selecting solutions, and highly weight Web security as a service (SecaaS) delivery capabilities.

Web application control and data loss prevention are important considerations for future-proofing investments; however, these features are not very mature or widespread.

MAGIC QUADRANT

Market Overview

The SWG market continues to evolve rapidly. Enterprise IT organizations are under business pressure to open up their networks to Internet applications, while struggling to keep Internet-connected endpoints free from malware. SWGs provide filtering and control over the Internet while enabling the broader use of beneficial interactive Web applications. As a result, security has eclipsed employee productivity monitoring (i.e., URL filtering) as a primary motivator of buyers in this market. SWG buyers are typically “Type A” security-conscious organizations in industries such as finance, government agencies, defense, high-tech and pharmaceuticals. However, we are starting to see more broad-based horizontal distribution of organizations looking at SWGs to improve their endpoint security posture. Typically, these mainstream adopters have been infected by malware, and an SWG represents the fastest and often least-expensive means to improve endpoint security to thwart future infections.

Innovation and feature development are still being driven by smaller, dedicated SWG companies; the traditional incumbent URL-filtering, antivirus and proxy cache vendors are still playing catch-up. Despite rapid feature development, we still find it difficult in this market to select vendors that satisfy buyers in all product features. Organizations should carefully consider their needs before they attempt to select vendors, and stay focused on needs during the selection process.

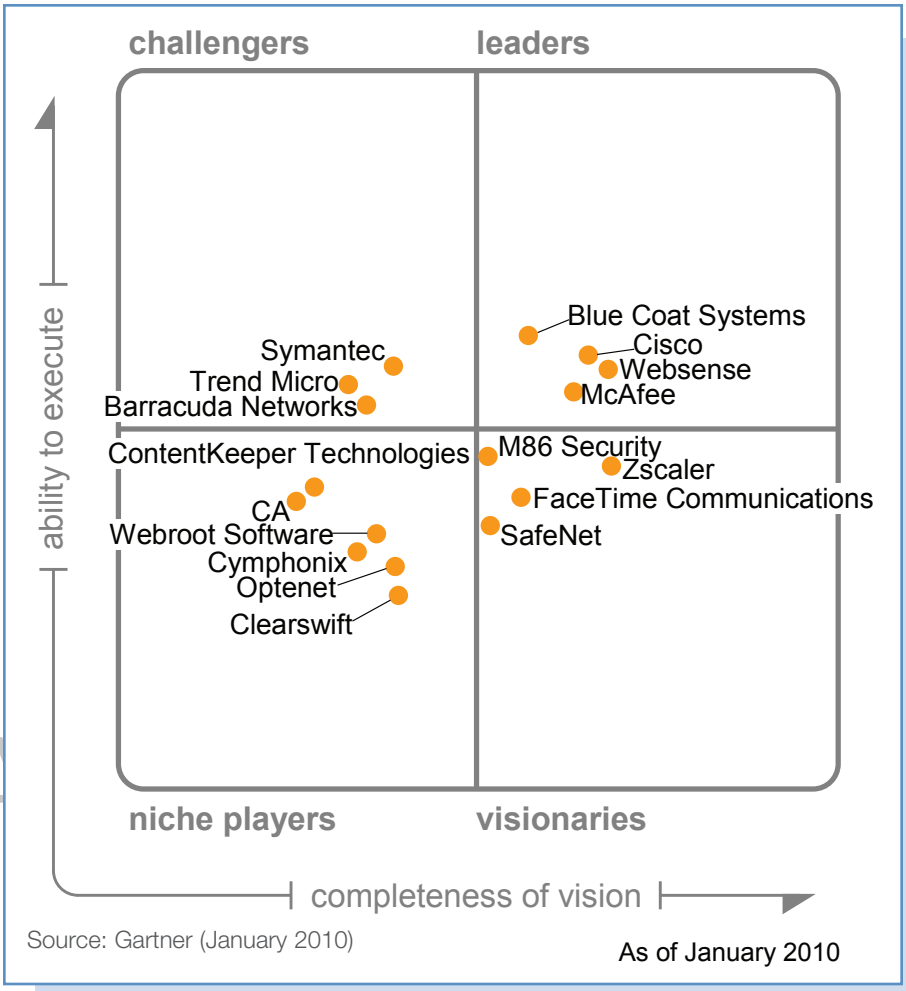
Gartner

Buyers should consider the URL categorization (particularly dynamic categorization) and security "service" or "subscription" aspect of the solution to be of critical importance, and look for vendors that have the resources to stay current with the rapidly changing content and threat landscape.

Security remains the No. 1 differentiator and primary purpose of an SWG. We put extra emphasis this year on real-time detection techniques that go well beyond file signature, URL categorization or static policy-based protection mechanisms. Unfortunately, real-time security detection methods are very difficult to evaluate and test, and no standard testing methodology has emerged. We recommend organizations test shortlist solutions in their networks to gather real-world results.

URL classification and reporting is a close second critical capability, especially given that most organizations would like to consolidate proxy, application control, security and URL filtering/reporting into a single solution, and leverage the existing URL-filtering budget. To do this, they need, at a minimum, to replicate existing reporting, and ideally improve on it with more-dynamic dashboards, graphical reporting and better custom report creation capabilities. As more and more Web content becomes user generated, organizations that are concerned about acceptable usage should seek out solutions that offer real-time content classification in the gateway based on keyword analysis and other indicators.

Figure 1. Magic Quadrant for Secure Web Gateway



Source: Gartner (January 2010)

As of January 2010

Web application control, and in particular bandwidth management of applications, is an increasing requirement as organizations try to keep costs down and improve critical application performance. Data loss prevention (DLP) continues to be a differentiator of solutions, and we expect that more SWG vendors will add DLP capability in 2010. However, enterprise needs for DLP are still embryonic, and buyers must be careful to consider DLP across all channels. DLP policy synchronization is one of the primary reasons for integration of Web and e-mail security gateways; however, this capability is still rare — even among providers with both solutions.

The delivery model for SWG solutions is expanding from traditional appliances and software, with the addition of virtual appliances that can operate on VMware and blade servers. The SecaaS market continues to heat up with significant enterprise interest as evidenced by increasing shortlist inclusions and acquisitions of SecaaS providers by traditional appliance vendors. During 2009, we have seen Symantec acquire MessageLabs; McAfee acquire MX logic; Cisco acquire ScanSafe; and Barracuda Networks acquire Purewire. The ability to protect and apply policy to mobile endpoints is a significant benefit of SecaaS providers as organizations seek to improve protection for these often infected devices. Currently, well more than 85% of SecaaS buyers are less than 1,000 seats, but adoption by larger organizations, including some with well more than 100,000 seats, is growing. Larger organizations typically see SecaaS

as a way to reduce network costs, as well as protect and manage mobile endpoints and smaller branch offices, while simplifying installation and ongoing management.

Market Definition/Description

The SWG market is a composite market made up of multiple security markets. URL filtering is the largest submarket. Other submarkets include antivirus filtering for Web traffic, proxy caches and dedicated multifunctional SWG devices. Market distinctions are rapidly blurring as submarket vendors maneuver to compete in the broader SWG market, making market size estimates more difficult. We estimate that the total composite market in 2008 exceeded $1.2 billion and was growing at a rate of 12% year over year. This is a significant decline from the 44% growth rate reported last year. This decline is due, in part, to changes in our market sizing methodology to more accurately reflect non-SWG revenue from multifunction market vendors, increasing price competition and slower-than-expected growth in 4Q08. We expect that the average market growth rate will increase to around the 15% range in 2010. This growth increase will be fueled partly by pent-up demand resulting from delayed projects. The dedicated SWG was the fastest-growing submarket, with approximately 80% year-over-year growth.

Inclusion and Exclusion Criteria

These criteria must be met to be included in this Magic Quadrant:

- Vendors must own unique content capability in at least one of these categories: URL filtering, anti-malware or application-level controls. This includes granular active content policies, dynamic classification of websites and Web "reputation" systems, in addition to traditional anti-spyware and anti-spyware engines and URL lists.
- Vendors must have at least 50 production enterprise installations.
- SWG products that offer firewall functionality — for example, multifunction firewalls (also known as unified threat management [UTM] devices) — are outside the scope of this analysis. These devices are traditional network firewalls that also combine numerous network security technologies — such as anti-spam, antivirus, network intrusion prevention system and URL filtering — into a single box. Multifunction firewalls are compelling for the small or midsize business (SMB) and branch office markets; however, in most circumstances, enterprise buyers do not consider multifunction firewalls as replacements for SWGs. Examples of vendors with multifunction firewall solutions include Astaro, Check Point Software Technologies, Fortinet and SonicWALL.
- Vendors that rebrand and sell complete SWG solutions are not included. For example, Google resells Cisco/ScanSafe. Google is not included in this analysis; but Cisco/ScanSafe is included.

Added

SafeNet acquired Aladdin, and Symantec acquired Mi5 Networks and MessageLabs. ZScaler and Optenet are new vendors added this year because they met the inclusion criteria.

Dropped

Marshal and 8e6 merged, and the newly formed company later acquired Finjan Software, and renamed itself M86 Security. Secure Computing was acquired by McAfee, ScanSafe was acquired by Cisco, MessageLabs and Mi5 Networks were acquired by Symantec, and Aladdin was acquired by SafeNet. These products now appear under the parent company. CP Secure was acquired by Netgear. Netgear is incorporating CP Secure's technology into its ProSecure unified threat management appliances, which don't meet the inclusion criteria for this Magic Quadrant.

Evaluation Criteria

Ability to Execute

Vertical positioning on the Ability to Execute (see Table 1) axis was determined by evaluating these factors:

- Overall viability — The company's financial strength, as well as the SWG business unit's visibility and importance for multiproduct companies
- Sales execution/pricing — A comparison of pricing relative to the market
- Market responsiveness and track record — The speed in which the vendor has spotted a market shift and produced a product that potential customers are looking for; as well as the size of the vendor's installed base relative to the amount of time the product has been on the market
- Customer experience — Quality of the customer experience based on reference calls and Gartner client teleconferences
- Operations — Corporate resources (in other words, management, business facilities, threat research, support and distribution infrastructure) that the SWG business unit can draw on to improve product functionality, marketing and sales

Table 1. Ability to Execute Evaluation Criteria

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

Source: Gartner (January 2010)

Completeness of Vision

The Completeness of Vision (see Table 2) axis captures the technical quality and completeness of the product and organizational characteristics, such as how well the vendor understands this market, its history of innovation, its marketing and sales strategies, and its geographic presence.

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

In the product evaluation, we ranked vendors on these capabilities:

- Malware filtering — The most important capability in this analysis is the ability to filter malware from all aspects of inbound and outbound Web traffic. Signature-based malware filtering is standard on almost all products evaluated. Consequently, extra credit was given for non-signature-based techniques for detecting malicious code and websites in real time as it crosses the gateway, as well as the range of inspected protocols, ports and traffic types. Products that can identify infected PCs and the infection by name, and enable prioritized remediation, received extra credit.

- URL filtering — Databases of known websites are categorized by subject matter into groups to enforce acceptable use and productivity and to reduce security risks. To displace incumbent URL-filtering products and "steal" allocated budget, SWG vendors will have to be competitive in this capability. Quality indicators, such as the depth of the page-level categorization, the real-time categorization of uncategorized sites and pages, dynamic risk analysis of uncategorized sites and pages, and the categorization of search results, were considered.

- Application control — Granular, policy-based control of Web-based applications, such as instant messaging (IM), multiplayer games, Web storage, wikis, peer-to-peer (P2P), public voice over IP (VoIP), blogs, data-sharing portals, Web backup, remote PC access, Web conferencing, chat and streaming media, is still immature in most products and represents a significant differentiator. We considered the number of named applications that can be effectively blocked by checking a box on the application category or a specific named application. The ability to selectively block specific features of applications and the presence of predeveloped policies to simplify deployment were given extra credit.

- Manageability/scalability — Features that enhance the administration experience and minimize administration overhead were compared. Extra credit was given to products with a mature task-based management interface, consolidated monitoring and reporting capabilities, and role-based administration capability. Features such as policy synchronization between devices and multiple network deployment options enhance the scalability and reliability of solutions.

- Delivery models — We looked at deployment options and form factors. Appliance and software are standard. Extra credit was given to vendors that offer multiple form factors, such as Virtual appliances for VMware or other hypervisors and/or SecaaS delivery models. We also looked at network deployment options, such as Proxy vs. in-line bridge, Internet Content Adaptation Protocol (ICAP) and Web Cache Communication Protocol (WCCP) compatibility.

- Related investments — We gave minor credit for vendors with related investments, such as e-mail integration and native DLP capability. Native DLP capability shows technical prowess and can be useful in tactical situations; however, integration with e-mail and/or dedicated DLP solutions is a more strategic feature.

Table 2. Completeness of Vision Evaluation Criteria

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

Source: Gartner (January 2010)

Leaders

Leaders are high-momentum vendors (based on sales and "mind share" growth) with emerging track records in Web gateway security, as well as vision and business investments that indicate they are well-positioned for the future. Leaders do not necessarily offer the best products for every customer project; however, they provide solutions that offer relatively lower risk.

Challengers

Challengers are established vendors that offer SWG products but do not yet offer strongly differentiated products, or their products are in the early stages of development/deployment. Challenger products perform well for a significant market segment, but may not show feature richness or particular innovation. Buyers of challenger products typically have less-complex requirements and/or are motivated by strategic relationships with these vendors rather than requirements.

Visionaries

Visionaries are distinguished by technical and/or product innovation, but have not yet achieved the record of execution in the SWG market to give them the high visibility of the leaders or those that lack the corporate resources of challengers. Expect state-of-

the-art technology from the visionary vendors, but buyers should be wary of a strategic reliance on these vendors and should monitor the vendors' viability closely. Given the maturity of this market, visionaries represent good acquisition candidates. Challengers that may have neglected technology innovation and/or vendors in related markets are likely buyers of visionary vendors. Thus, these vendors represent a slightly higher risk of business disruptions.

Niche Players

Niche player products typically are solid solutions for one of the three primary SWG requirements — URL filtering, malware and application control — but they lack comprehensive features of visionaries and the market presence or resources of the challengers. Customers that are aligned with the focus of a niche vendor often find such provider offerings to be "best-of-need" solutions.

Vendor Strengths and Cautions

Barracuda Networks

Barracuda Networks offers a range of inexpensive proxy-based appliances that leverage open-source technologies and enjoys high mind share in the SMB market due to extensive marketing and an effective sales channel. It continues to experience solid global growth, primarily with customers that have less than 1,000 seats. Barracuda recently acquired startup SecaaS SWG provider Purewire, and the company plans on using Purewire as a base for an expanded set of SecaaS offerings. Barracuda's solid growth and the acquisition of Purewire helped its execution score, moving it up into Challenger status this year. Barracuda Web Filter appliances are a good shortlist inclusion for SMBs looking for "set and forget" functionality at a reasonable price. The Barracuda (Purewire) SecaaS offering is also reasonable in supported geographies.

Strengths

- The Barracuda Web Filter's Web graphical user interface (GUI) is basic and designed for ease of use. Deployment is simplified with all settings in a single page with easily accessible suggested configuration settings and contextual help. The dashboard includes a summary of top reports, including infection activity, hyperlinked to the detailed reports. Real-time log information can be filtered by a number of parameters for easy troubleshooting. Malware protection is provided by open-source Clam AntiVirus, augmented with some in-house-developed signatures. The management console includes optional infection thresholds that can kick off alerts or launch a malware removal tool. Application controls include a fair number of IM networks, software updaters, media stores, remote desktop utilities, toolbars and Skype. The Barracuda Web Filter is one of the most economically priced solutions in this Magic Quadrant, and annual updates are priced per appliance rather than per seat.

- The Barracuda Web Security Service (formerly Purewire) offers a very clean and well-organized policy and reporting interface that is simple and logical. Dashboard elements all offer a consistent hyperlinked drill down into three levels of increasingly granular data. All security protection methods are included in the base price. In addition to using several signature and blacklist-based filters, the Web Security Service performs numerous advanced security checks, including page analysis, URL reputation, exploit kit detection, JavaScript analysis and bot detection. URL filtering is driven by the Barracuda database as well as dynamic filtering for uncategorized sites. Advanced options include coaching and password-protected bypass with custom blocking pages for each rule. The solution also allows quotas based on connection bytes and time limits. Application control includes several dozen named applications in four categories: browsers, IM, P2P file sharing, and streaming media that are based on request and response headers and traffic signatures. They also offer some options for Web browser control. The DLP capability includes five static DLP libraries/lexicons and Secure Sockets Layer (SSL) scanning by category

- Redirecting traffic to the Barracuda Purewire service is enabled with an optional on-premises caching appliance (hardware or virtual software) that caches traffic and provides for on-premises authentication, Microsoft Internet Security and Acceleration (ISA) plug-in, and a variety of direct connect and Active Directory configurations. The Barracuda Purewire Web Security Service also offers a tamper-proof software client for roaming laptop users that enforces remote/roaming traffic through a cloud service.

Cautions

- The Barracuda Web Filter appliance lacks enterprise-class administration and reporting capabilities. Advanced ad hoc reporting features are lacking, and custom reports are limited to filter settings on existing reports. The dashboard is not customizable. It offers only a single administration account and does not support role-based administration. Some policy features, such as file-type blocking, are very manual rather than menu-driven, and the overall workflow is feature-based instead of task-based. The appliance can only store six months of data; longer-term data storage or aggregated reporting across multiple boxes requires the Barracuda Control Center. Security threat reporting does not provide any guidance on the severity of a particular threat, nor does it provide links to more detail on the threats.

- Barracuda relies heavily on open-source databases for URL and antivirus filtering (Clam AntiVirus) supplemented with Barracuda's own research labs. However, Barracuda's research labs have not earned a strong reputation in the industry. Barracuda added the security researchers from Purewire to its roster; however, with the industry-standard antivirus vendors struggling to keep up with the increasing volume of threats, it will have to invest in more research capability to continue to improve.

- Purewire was an emerging startup when it was acquired, and Barracuda management has an ambitious road map for integration of the existing Barracuda backup service as well as building an expanding line of SecaaS offerings in several markets. The Purewire service still needs to mature to compete against the more-established SecaaS vendors in this space. The management interface is missing some enterprise options, such as expansive role-based administration, customization

of dashboard elements, quick links to tasks and full policy administration audit reporting. Security threat reporting would be improved with more information, such as severity, and more-detailed information about specific threats. Reporting is very basic and could be improved with more customization options. Predeveloped reports are too narrow and lack a single management summary report on activity. Purewire does not offer a zero-client footprint option with transparent authentication.

- Purewire only has data centers in Atlanta, Oakland, California, and London. Barracuda Networks has data centers supporting its Barracuda Backup Service (launched in November 2008) in Detroit, the District of Columbia and London. The company needs to invest in a global enforcement infrastructure and support presence outside the U.S. to appeal to global enterprise customers.

Blue Coat Systems

Blue Coat is one of the original proxy cache vendors, and has maintained a consistent dedicated focus on the demanding SWG market for large enterprise and service providers. Blue Coat, with its Mach5 products, is also a major player in the enterprise WAN optimization controller (WOC), which enables application acceleration. The company fell back slightly in Completeness of Vision compared with its peers in this Magic Quadrant due to a lack of focus on real-time malware detection in the gateway and lack of a SecaaS delivery solution. Blue Coat remains the overwhelming installed base leader in the enterprise proxy market and continues to show up on the majority of large enterprise shortlists.

Strengths

- The ProxySG product is well-tested for scalability and performance in the demanding large enterprise market, and includes numerous advanced proxy features, such as support for a long list of protocols, extensive authentication and directory integration options, raw policy scripting capabilities, command line interface in addition to a GUI, SSL decryption, support for ICAP, and centralized management and reporting. The company has one of the largest development and support organizations in this market.

- ProxySG supports nine URL-filtering databases, including its own, and four antivirus engines on its ProxyAV platforms — the most options of any vendor in the market.

- In addition to signature scanning, ProxySG exploits a frequently updated URL database (owned by Blue Coat) to detect known malicious URLs, and has static policy triggers to validate or limit active content (for example, ActiveX Controls or Java Applets) as well as limited active code analysis to detect unknown malware.

- Blue Coat maintains URL database freshness and relevance by automatically sending unclassified URLs to one of five data centers “in the cloud” for categorization and malware detection.

- Blue Coat is often one of the least-expensive URL-filtering options. Its URL-filtering pricing model is based on a one-time perpetual license fee plus annual maintenance charges.

- Blue Coat’s SSL termination capabilities (via an optional card on ProxySG) enable Blue Coat to terminate and decrypt SSL content and hand it off (via ICAP) to third-party devices, such as DLP scanners (Blue Coat partners with five DLP vendors), for further analysis.

- Blue Coat offers an endpoint agent (free of charge) that provides URL-filtering support (and application acceleration) for mobile workers.

Cautions

- Blue Coat is the only provider that requires antivirus processing on a dedicated appliance. The ProxyAV continues to be a liability in the SMB market, where it adds costs and requires integration with Blue Coat’s proxy appliance.

- Blue Coat’s lack of a SecaaS offering is a liability, given the rapid growth of the SecaaS market. In December 2009, Blue Coat announced plans to enter the SecaaS market in 2010 with an internally developed service.

- Blue Coat offers limited real-time, on-box malware and URL categorization technology. Blue Coat sends uncategorized URLs to its cloud-based WebPulse service for dynamic categorization and for malware analysis. This cloud-based approach is a valid method for detecting many forms of malware. However, the cloud approach limits Blue Coat’s ability to perform malware analysis on websites that require authenticated access (e.g., social networking sites). Alternatively, real-time on-box malware analysis, offered by several Blue Coat competitors, provides the advantage of analyzing content on-premises, which minimizes latency and provides better protection against targeted threats.

- Blue Coat cannot monitor all network traffic in its most commonly deployed proxy mode, but it can be configured in other modes to monitor all traffic.

- Although the management interface and reporting infrastructure is improving, smaller customers complain that it is still geared toward larger enterprises with extensive networking experience.

- Blue Coat lacks DLP capabilities on its ProxySG appliance, although it can integrate via the ICAP protocol with a range of third-party DLP solutions.

CA

CA’s proxy-based SWG product, WebFilter Proxy, is a component of CA Gateway Security, which includes e-mail security and provides a common management interface, as well as policy and reporting for Web and e-mail gateways. The CA WebFilter is a possible shortlist inclusion for SMBs looking for a suite solution that includes e-mail protection.

Strengths

- The Web and e-mail software appliances can be bundled together for smaller organizations or physically separated for larger organizations.
- Malware detection is provided by the CA anti-malware database team, which is one of the larger malware research organizations.
- URL filtering is provided using the McAfee database. It has some advanced features, such as self-authorization, time-based policy elements and basic application control based on URL classification.
- The WebFilter has strong native DLP capability for a SWG, including the ability to parse some document files for content checking, keyword dictionaries, regular expression matching and file binary detection.
- The management interface supports the broadest number of languages (10).
- CA Gateway Security is very reasonably priced.
- CA Gateway Security can be installed as a plug-in to Microsoft's ISA Server (proxy and multifunction platform).

Cautions

- Malware detection is provided by the same signatures as for e-mail and end nodes (different signatures at the SWG and at the desktop enhances security) and advanced, real-time threat detection is very limited. Indeed, CA's position is that the "gateway" is the wrong place to combat spyware.
- Some customers reported that the Gateway Security management console was difficult to use, with numerous applications and pop-up windows. Policy development is difficult to troubleshoot without an audit summary. Administrators or auditors must restep through the policy development process to spot errors or troubleshoot.
- The real-time graphical dashboard is weak, with a limited log view and some server statistics only. The reporting tool is required to view details; however, the dashboard is not linked to the reporter with any hotlinks. Administrators must open the reporting tool, "Reporter," and find the relevant report. Reports are very basic, and there are only a limited number of predeveloped reports. Included reports are not comprehensive, although it does also include a customizable report generator to create customizable reports. Report scheduling is provided by yet another application utility.
- Although the dashboard has outbound malware statistics, details are buried in a custom report and actions are limited. The ability to isolate and repair infected clients is lacking.
- URL filtering could benefit from more-advanced options, such as a coaching option, and bandwidth control or quality of service. Application blocking is URL-based or port blocking, and is not menu-driven.
- The proxy does not support SSL termination or ICAP, which limits its DLP capabilities (it cannot hand off SSL-encrypted content to a DLP sensor). Inbound and outbound malware can evade detection by port/protocol hopping or tunneling in HTTP/S.
- The proxy does not support native FTP.
- CA offers only software for Microsoft platforms, so it will be hard-pressed to match the ease of use of purpose-built appliances. Support and cost of the underlying Windows hardware and software should factor into the total cost of ownership calculation.

Cisco

IronPort (a Cisco-owned company) designed its S-Series proxy/cache from the ground up to address the multifunction requirements of a modern SWG and the scalability needs of demanding large enterprise customers. The S-Series appliance is rapidly maturing and experiencing very solid growth in the larger enterprise proxy/cache market. Cisco recently acquired the pioneering SWG SecaaS company ScanSafe. ScanSafe continues to execute well and has the largest market share in the SecaaS market including several organizations with well more than 100,000 seats. ScanSafe is expected to form the basis of an increasing array of Cisco SecaaS offerings, starting with the addition of e-mail. Cisco's credibility with the network operations team, the progressive development and market growth of the S-Series and the acquisition of the leading SecaaS provider moved Cisco into the Leaders quadrant this year. Cisco/IronPort S-series is a strong shortlist inclusion for large enterprise customers, while the ScanSafe solution is strong for any enterprise size. The eventual integration of these two will make a powerful hybrid combination.

Strengths

- The S-Series provides good on-box malware detection. It provides parallel scanning capabilities across multiple verdict engines for inbound as well as outbound security and content scanning. Signature databases are offered from Webroot and McAfee, and can be run simultaneously. Non-signature-based detection includes exploit filters that proactively examine page content, site reputation, bot network traffic detection, transaction rules and Cisco-generated threat center rules. It also uses a mirroring port (SPAN port) network interface card for out-of-band traffic analysis to detect evasive outbound phone-home traffic or application traffic. The S-Series is one of the few products that includes a full native FTP proxy and SSL traffic decryption.
- Cisco/IronPort's URL categorization engine is augmented with a dynamic classification engine for unclassified sites and user-generated content. The S-Series also offers application control using application signatures to identity and block/allow

a large collection of Web-based applications, including Skype and popular IM applications. The S-Series provides good DLP functionality with the combination of integrated on-box Data Security Policies and the choice of advanced DLP content scanning through ICAP interoperability with third-party DLP solution RSA and Symantec/Vontu. Policy options include the ability to block "posting" to Web 2.0 type sites.

- IronPort has numerous features to enhance the scalability of the S-Series for demanding large enterprise needs including native Active-Active clustering, centralized management for up to 150 servers per management server, appliances that can support up to 1.8 terabytes of storage with hot-swappable, Serial Attached SCSI (SAS) drives and RAID 10 configuration and RAID1 mirroring, six 1Gb network interface as well as a fiber option. In addition, the security scanning is enhanced by stream scanning, which enables scanning for larger or long-lived objects without creating the bottlenecks associated with buffer-based scanning.

- ScanSafe's Web-based management interface is clean and simple to use, even for nontechnical users. Customers commented on the ease of deployment in migrating to the ScanSafe service. The graphical dashboard is hyperlinked to filtered log views. Near-real-time customized reporting was significantly improved in the latest version with data mining capability. The service offers a real-time classification service to classify unknown URLs into a small set of typically blocked categories (for example, pornography or gambling). URL filtering is enhanced with some advanced functionality, such as bandwidth and time-based quotas, and a "search ahead" feature that decorates search engines with URL classification.

- ScanSafe offers simple outbound DLP functionality (dictionary keyword matching, named file detection and preconfigured number formats), and file hash matching can integrate with some enterprise DLP vendors.

Cautions

- Cisco will face some cultural and product integration challenges with ScanSafe, including refocusing the sales and channel on service selling, integrating the ScanSafe endpoint client with Cisco's remote access/AnyConnectVPN client, and delivering a unified IronPort/ScanSafe reporting and unified policy management console, which Gartner estimates will require, at minimum, six months.

- The S-Series has a strong foundational design; however, it still needs refinement of the management interface and is missing some advanced features. It is clearly designed for larger enterprises with demanding network requirements but does not scale down well for SMBs with simpler needs. Application control is not well instrumented and requires administrators to understand the network behavior of some evasive applications to build an effective policy. It does not provide bandwidth management or QoS options. Application control and QoS are scheduled to be addressed in 1H10. It lacks the ability to block certain functions in Web applications, such as Web mail and social networking. DLP is not yet integrated with the IronPort secure e-mail gateway appliances, although policy can be manually exported from the e-mail gateway and imported to the S-Series.

- The S-Series is one of the more expensive SWG appliances in the market, and Cisco charges extra for the SenderBase Web reputation filter.

- S-Series reporting is improving; however, it is still a weak spot. There is no ability to customize the on-box dashboards, nor is it always possible to drill down into detailed off-box (Sawmill) reporting from top-level dashboards. Per-user reports and forensic investigative reporting are weak. The appliances can store 30 days of on-box log data, but they offer limited reporting functionality. To generate reports from log data that is older than 30 days, users must export log data to a third-party log analysis and reporting package from Sawmill (requires a Windows server). The Sawmill package is also required to generate detailed per-user statistics, even for on-box-stored data. The M-series management server is the logical place for this reporting, and Cisco is expected to deliver this functionality during the next 12 months.

- ScanSafe's early leadership position and lack of competition has resulted in lethargic feature growth and innovation. It is beginning to change now that it is facing competition from more-nimble startups; however, product features and global presence should be better, given such an early lead in this market. We expect the infusion of Cisco resources will reinvigorate the company.

- ScanSafe's management interface is better suited for simple policy constructs. Setting up a policy may require multiple steps to implement a single rule. The policy is tied to specific protocols, and a troubleshooting policy is complicated by lack of readable summaries. It does not have the capability to create a reporting role that only has access to specific group data. Outbound threat information is minimal, lacking severity indicators or detailed information about infections. For laptop users, it does not have a zero footprint authenticated client solution. ScanSafe charges an extra fee for its Anywhere+ service (for roaming employees) and its IM Control service. Application control is limited and URL-based, rather than based on network signature protocol. Like other services and proxy products, ScanSafe can only see outbound traffic in HTTP traffic, and will miss evasive applications and malware.

Clearswift

Clearswift is a veteran secure e-mail gateway vendor with a high profile in EMEA. It has integrated its proxy-based SWG — Clearswift Web Appliance — with its e-mail security solution to provide cross-channel policy and consolidated reporting. Overall, Clearswift's primary advantage is its integration with its e-mail solutions and the provision of DLP across both channels, making it a good choice for existing e-mail customers or EMEA buyers looking for both solutions from the same vendor.

Strengths

- Clearswift offers a clean, logical browser-based interface for policy development that is easy to use, even for nontechnical users. E-mail and the Web are managed in the same console. Multiple devices can be managed from any machine.

- Policy development for DLP is very good and several policy constructs —Sarbanes-Oxley Act (SOX), Gramm-Leach-Bliley Act (GLBA), Payment Card Industry (PCI) Data Security Standard, Securities and Exchange Commission, accounting terms and stock market terms — are included. The same policy can apply to Web and e-mail, and it is possible to intercept and copy/archive Web mail and IM traffic that triggers DLP policy. Clearswift also provides strong policy audit and printable policy summaries for troubleshooting.

- Clearswift offers good reporting capability. All machines in a cluster are capable of local or consolidated reporting. Reports are active and include a hyperlink drill-down of details. Malware filtering is provided by Kaspersky and Sunbelt Software. It is augmented with some in-house, preconfigured, policy-based code analysis. The Clearswift Web Appliance is capable of SSL certificate validation, decryption and inspection. URL categorization is provided by the RuleSpace database augmented by real-time dynamic classification of uncategorized sites.

- Clearswift offers a good array of form factors including a dedicated hardware appliance, soft appliance for installation on any hardware, or as a virtual appliance for VMware, and has native ability to “peer” a cluster of appliances together.

Cautions

- Clearswift remains an EMEA brand and does not enjoy significant brand recognition in North America. Its market share in the SWG market is very small.

- Malware detection is primarily limited to signatures and only in HTTP/S traffic. It does not include out-of-band malware detection, and reporting is missing detailed threat information or severity indicators. The solution cannot isolate or clean infected machines.

- Enterprise management features such as group-level administration and reporting, customizable dashboards and log file searching are lacking. Centralized management is limited to supporting nine local boxes.

- Application control is limited to blocking URL destinations (and/or streaming protocols) and file-type blocking. It is possible to detect and block specific applications, but it requires the creation of custom rules within the appliance to identify and block based on the specific characteristics of the application found in the HTTP content. It cannot filter or manage evasive applications, such as Skype.

- It does not support in-line/bridge mode deployments, ICAP or WCCP.

- Pricing is very high relative to peers

ContentKeeper Technologies

ContentKeeper Technologies is based in Australia, where it has many large government and commercial customers. It offers a family of SWG appliances that deploy as an in-line bridge. The main focus of the company is URL filtering, and the company maintains its own URL-filtering database. Signature-based antivirus protection is licensed from Kaspersky, and is available as an integrated on-box offering. SecaaS-based e-mail security is available via an OEM partnership with Webroot. ContentKeeper is a good option for organizations looking for simpler URL filtering capability in supported geographies.

Strengths

- ContentKeeper offers a series of five appliances, the largest of which is based on IBM blade server technology, which the company claims has a maximum throughput rate of 14 Gbps. The appliances “fail open” due to a high-availability hardware module. In addition to supporting in-line bridge mode, the appliances also proxy SSL traffic and provide decryption capabilities. IPS capabilities are provided via Snort signatures.

- The Advanced Reporting Module (ARM) is an optional solution that provides good graphical analysis of log information, including the option to display data in bar and pie charts. The ContentKeeper appliances can be set to export data to the ARM in real time or on a periodic basis. The ARM may be deployed on the ContentKeeper appliance or off-box. Real-time monitoring and alerting are achieved through the ContentKeeper Monitor package. ContentKeeper provides strong bandwidth control capabilities. It provides bandwidth quotas and QoS features.

- All ContentKeeper appliances maintain a feedback loop with the ContentKeeper data center. On an hourly basis, the Web-only appliances receive updates to the URL database, and they send any unclassified URLs to the data center for analysis and classification. ContentKeeper appliances with the integrated antivirus support call in for updates every five minutes. The feedback loop is supplemented with URLs obtained via Web crawling techniques, and suspicious sites are further analyzed for malware.

- ContentKeeper provides application control for more than 90 applications.

- ContentKeeper offers one of the most cost-effective URL-filtering solutions in the market.

Cautions

- ContentKeeper has a weak presence in Europe and North America (more than 50% of its sales are in the Asia/Pacific region).
- Malware detection and control is limited. Only one option (Kaspersky) is offered for on-box signature-based malware protection. Outbound malware detection lacks detail. It shows which malware infected websites have been blocked, but — unlike some other solutions — does not contain severity indicators or detailed information about infections.
- The SecaaS offering, which is primarily targeted at SMBs, lacks several enterprise-class capabilities. User authentication and traffic forwarding (to the cloud) requires an agent on every endpoint (several SecaaS providers offer integration with domain controllers to avoid endpoint software). The SWG SecaaS offering provides limited application control and does not offer real-time malware detection.
- On-box reporting via the Monitor package and hyperlinks to the ARM for drill-down analysis needs improvement. ContentKeeper has plans to introduce an enhanced GUI in 2010.
- Uncategorized URLs are not classified in real time. Updates to the ContentKeeper appliances are dependent on configurable call-in parameters (one hour for Web-only appliances and five minutes for Web and antivirus appliances). The URL database needs more granularity. It only supports 32 categories; most competitors support more than twice as many categories (although custom categories can be added).

Cymphonix

Cymphonix, a privately held Utah-based company, was founded in 2004. The Cymphonix Network Composer is an appliance-based product that is mostly deployed as an in-line transparent bridge, but it can also be deployed as a proxy. Cymphonix licenses malware signatures from Sunbelt and Clam AntiVirus. The URL-filtering database is licensed from Rulespace and is enhanced through internally maintained updates. Cymphonix is a good fit for SMBs looking for a single SWG with advanced bandwidth management capabilities at a reasonable price. Its ability to detect and block proxy anonymizers (used to bypass URL filtering) makes it a good fit for the K-12 education environment.

Strengths

- Cymphonix offers one of the strongest bandwidth control capabilities in the SWG market. Its bandwidth-shaping policies can be nested within one another for more granular control. For example, users in a particular role can be assigned a maximum of 30% of available bandwidth for an Internet connection. This group can be further shaped, so that 10% of its bandwidth is assigned to IM, while 70% is reserved for mission-critical applications. Bandwidth shaping can be performed at a broad level for virtual LANs, IP ranges, and Active Director Groups, or at a very precise level down to specific Host MAC or IP address, Web category, specific URL, file type, mime type and user.
- The Network Composer includes more than 650 application signatures that can be used to build network policies for blocking or allowing applications. Applications can also be prioritized in terms of relative importance, using the bandwidth control capabilities described.
- Cymphonix offers a series of seven appliances, the largest of which the company claims has a maximum throughput rate of 200 Mbps. The appliances can be configured to “fail open.” In addition to supporting the in-line bridge mode, the appliances also proxy SSL traffic and provide decryption capabilities. Cymphonix also offers a useful free network utility that enables organizations to identify rogue and bandwidth hogging application traffic on their networks.
- The Web GUI is simple and easy to use, and the reporting capability is good. Tabs provide easy navigation to a collection of reports that can be modified, saved and scheduled, and reports provide hyperlink drill-downs that show more details. Policy management is easy to use, and includes numerous advanced functions to combine application-shaping and content-control policies to individuals or groups.
- In 2009, Cymphonix strengthened its reseller channel program and expanded into EMEA and Asia/Pacific.

Cautions

- Although Gartner believes that Cymphonix is growing faster than the SWG market, it remains one of the smallest vendors in this Magic Quadrant and still has low market share and brand recognition.
- There is no centralized reporting/management interface for managing clusters or geographically dispersed gateways; one is scheduled for release in 1Q10.
- Some customers have complained about Cymphonix’s licensing model, which is based on IP addresses and not users. With the address-based model, printers, IP phones and non-browser-based devices must be manually identified and placed in an “exception list” so that they are not counted.
- Some customers reported excessive miscategorizations of URLs, although the 8.7 release in September 2009 replaced the categorization engine with the RuleSpace engine, which has less reliance on dynamic classification.
- There are no DLP capabilities or related e-mail protection products.
- There is no support for ICAP or WCCP.

FaceTime Communications

FaceTime, a privately held company based in California, started in the IM security market and has branched out into the broader SWG market. The company's installed base includes a significant number of large enterprise businesses, primarily in North America. These include many financial institutions, which were the primary buyers of IM security solutions. It has its own malware and application research capabilities, and the deepest visibility and controls for Web 2.0 type Internet applications. FaceTime's Unified Security Gateway (USG) appliance can be deployed by connecting to a SPAN/mirror port and in-line, and can also interface to proxies via the ICAP protocol. When deployed in-line, the USG can proxy HTTP/S and traffic from common IM and enterprise unified communications (UC) services. FaceTime is a strong choice for organizations looking for fine-grained Web application controls.

Strengths

- FaceTime revised its management interface during the past 12 months, and the resulting Version 3.0 has a significantly improved dashboard and reporting capability, as well as a more flexible and scalable object-based policy engine. The dashboard is fully customizable, and administrators can create their own look and feel, adding virtually any report as a dashboard element. All dashboard elements are hyperlinked to reports and log data detail. V3.0 also offers a unique fully customizable "Heatmap" dashboard element that enables administrators to visualize traffic and events rapidly.

- FaceTime has the deepest visibility and controls for Internet applications, with more than 4,000 named applications, including IM, P2P, anonymizers, IP television, gaming software, multimedia, remote administration tools, virtual worlds, VoIP, Web-based IM and Web conferencing. In particular, FaceTime offers the strongest control for Skype. A special plug-in to the USG appliance enables it to detect and block malicious URLs within Skype IMs.

- FaceTime continues to leverage its 2005 acquisition of XBlock Systems for a malware-filtering database, as well as an optional Sunbelt software malware database and a Web antivirus database from Sophos. USG also offers some behavior-based detection techniques. Reporting on inbound and outbound threats is very strong and includes the specific detailed information on the malware (for example, name, threat rating and more) and links to FaceTime's Web-based reference site, spywareguide.com.

- FaceTime offers good DLP and archiving capabilities for IM traffic and HTTP/S traffic (e.g., Web mail and blog posts). For example, policies can be enabled to control and log all outbound content for blog posts to social networking sites and also for Web mail traffic. Policy options include taking a screen shot of the Web page for which DLP policy is triggered. The logging can also be triggered by lexicon match (for example, log all credit card numbers posted to a social networking site). DLP capabilities can also be exploited for dynamic content-level blocking of offensive text content.

- Multiple USGs can be clustered to share a database, which then allows for a shared repository of configuration and reporting for multiple geographically dispersed USGs.

- Customers can choose between two URL-filtering databases. FaceTime's URL-filtering policy is average, but includes some advanced features, such as a coaching option for soft blocking.

Cautions

- FaceTime's biggest challenge is improving its visibility and mind share against increasingly larger and more-strategic competition. It needs to rapidly expand its channel partners and its client base, because it is at risk of becoming a niche provider in the financial services market.

- FaceTime's URL-filtering capabilities do not offer the ability to dynamically classify uncategorized websites, and URL-filtering updates are only provided daily (many vendors provide hourly or subhourly updates). DLP keyword filtering capability can be used to classify pages, but this capability is not predefined, and users would have to create and fine-tune their own categorization policies. There is no integrated URL client for mobile employees and no SecaaS solution.

- FaceTime relies on signature engines for malware and has limited on-box ability to dynamically inspect Web pages for malicious intent.

- FaceTime does not cache content and does not offer bandwidth QoS options to improve the performance of priority applications.

M86 Security

M86 Security is a newly formed company comprised of these four companies, all of which were independent as of October 2008:

- Marshal — E-mail and SWG solutions for the SMB market. Marshal's solutions are deployed as software or as appliances, and can function as a proxy or can be integrated with Microsoft's ISA Server.

- 8e6 — URL filtering for the K-12 and large enterprise market. The 8e6 solution is deployed as an out-of-band appliance attached to a "mirrored" port on a LAN switch.

- Avinti — Behavioral malware detection for e-mail security (M86 is now also applying the technology to analyze Web threats).

- Finjan — Proxy-based SWG with real-time code analysis technology for detecting Web-based malware. Finjan has a broad mix of customers (SMB and large enterprises) in EMEA and a more focused group of large enterprise customers in the U.S.

In November 2008, Marshal merged with 8e6 to become Marshal8e6. In April 2009, Marshal8e6 acquired Avinti, and in September it renamed itself M86 Security. In November 2009, M86 announced its acquisition of Finjan. M86's strategy of acquiring good malware detection technology, particularly Finjan, helped it earn Visionary status, although as we note, it faces challenges around product integration and cross-selling its solutions into new markets. The Finjan offering is M86's strongest enterprise SWG solution, and is a good shortlist inclusion for security-conscious organizations.

Strengths

- Through its mergers and acquisitions, M86 owns a broad base of SWG and secure e-mail gateway technologies. Marshal's historic product focus was in the SMB e-mail security market, and it also was an early entrant in the SWG market. 8e6 was a "pure-play" URL-filtering appliance vendor with solid performance and reporting capabilities for the K-12 market and for large enterprises. The acquisition of Avinti provided technology for runtime code analysis to detect malware. The Finjan acquisition gives M86 strong content analysis security technology in a proxy-based appliance. Finjan has been a pioneer in real-time code analysis technology, which scans a broad array of Web programming languages (for example, HTML, JavaScript, VBScript and Java) for malicious intent. M86 has moved quickly to provide some basic integration across the Marshal, 8e6 and Avinti products, by correlating threat information between its e-mail and Web solutions.

- The Finjan acquisition should progress relatively smoothly, since the CEO of M86 was previously the CEO of Finjan. Other executives have also worked at both companies, which should accelerate the process of forming a unified corporate culture.

- Finjan provides strong real-time malware filtering based on content inspection, good application control and some DLP capability in a proxy-based scalable appliance. Finjan has a good installed base in large security-focused organizations. The Finjan product is the strongest enterprise-class SWG solution in M86's product family and will serve as the platform for integrating M86's newly acquired technologies. Marshal offers secure e-mail gateways and an SWG solution in software and appliance form factors. It has several strengths as a stand-alone SMB-focused solution, including a strong management interface, reusable policy elements and good DLP support for multiple signature-based malware scanning engines.

- 8e6 solution has several strengths as a stand-alone URL filtering solution, particularly for real-time reporting and alerting of Internet usage, although this capability requires the Threat Analysis Reporter appliance and the Enterprise Reporter appliance to provide log analysis. It's URL filtering appliances are positioned out of band, so they install easily and do not require integration with proxy caches or firewalls (although, as an independent solution, 8e6 does not provide adequate malware protection).

Cautions

- M86's overall strategy will be challenging to execute. It will be difficult to compete in multiple market segments while integrating the technology from four different development teams into a cohesive product, with a unified management interface, while competing against the market leaders. M86 now consists of four previously independent companies with a combined customer base of companies ranging from SMBs to very large enterprises. M86's plans to grow its large enterprise business and to also maintain a strong SMB presence represents a difficult sales, marketing and product management challenge.

- In addition to the product integration challenges, M86 has plans to introduce SecaaS services, for e-mail and SWG. The e-mail SecaaS market is already mature, and the SWG SecaaS market is highly competitive and will mature quickly. Time to market is a serious issue.

- Finjan's on-box reporting is very basic and requires Windows and SQL database licenses for the reporting server. Larger enterprises that require long-term storage and consolidated reporting will find the on-box reporting limited. In 2010, M86 plans to utilize Linux-based technology that it acquired from 8e6 for its SWG reporting server.

McAfee

McAfee moves into the Leaders quadrant this year with the acquisition of Secure Computing. The McAfee Web Gateway (MWG) is the new name for the Secure Computing Secure Web Gateway, which Secure acquired from CyberGuard, which purchased Webwasher. It is now McAfee's flagship Web gateway appliances, although McAfee will continue to support its legacy e-mail and Web Security Appliance product primarily for SMB customers. This analysis focuses entirely on the flagship MWG product, which remains a solid choice for many enterprise buyers, especially those that are already McAfee ePolicy Orchestrator (ePO) users.

Strengths

- The MWG Ajax/Web-based management interface is well-organized, easy to navigate and deploy for technical users, and offers numerous advanced management features such as granular role-based administration, data anonymization, FTP command filtering, object-oriented policy, native centralized management and user quotas. MWG is gradually being integrated with McAfee's ePolicy ePO management platform. MWG has a reporting application that offers tiered administration and ships with enterprise version of MySQL or integrates with Microsoft SQL or an Oracle Database.

- MWG has strong on-box malware protection with a choice of Avira or McAfee's signature engine, as well as some zero-day security technology, which includes real-time code analysis technology that scans a broad array of Web programming languages for malicious intent. The URL categorization engine is augmented with its own TrustedSource URL reputation data.

- McAfee has a solid antivirus research team and data feeds from its TrustedSource reputation system, which has been expanded to cover URLs clear.

- MWG includes several advanced URL-filtering policy features, such as progressive lockout, which senses multiple bad URL requests and locks out Internet access. Bandwidth quotas, coaching and soft blocking are also available.

- The product includes SSL decryption, which will combine well with McAfee's strong native DLP capability. Management integration with e-mail security will provide a benefit, especially with DLP administration.

- In addition to its appliance-based offerings, McAfee has relaunched Secure computing SecaaS Web Protection Service and ported MWG to the McAfee Content Security Blade Server architecture to meet large enterprise/ISP needs. McAfee also recently acquired MXLogic, which offers e-mail and Web security; however, we expect the Secure Computing SecaaS platform to replace the MX logic Web filtering infrastructure.

Cautions

- McAfee still has lots of integration work to do to integrate with ePO and its DLP, e-mail and endpoint solutions to deliver the security and deployment advantages of a single solution.

- Long-term McAfee customers have suffered from very inconsistent support experiences throughout mergers. It will take time for McAfee support to gain enough experience to offer a good support experience. Premium support is recommended.

- Management features are still maturing, and customer references indicate that product documentation is lacking. Some commands can only be executed via a command line interface, the dashboard cannot be customized; it lacks a raw log search capability, the policy change audit log is very basic, and the solution lacks the ability to review policy in a single page. Some changes require a server reboot.

- Outbound malware reporting is still absent on the dashboard in any detail, and reports do not include severity indicators, trending information, or quick links to detailed threat information or automated remediation.

- Consolidated and advanced reporting functions require the Web reporting product, which is a separate application with a different look and feel from the management interface, and it does not have hyperlinks from the dashboard logs or reports on the appliance. The basic Web Reporter version is included with the appliance; however, the Premium version is required for advanced features, such as delegated administration and ad hoc reporting. The number of canned reports is low, and some reports do not have obvious features, such as pie graph options. Some customers complained about the scalability of the reporting interface.

Optenet

Optenet, a new entrant into this Magic Quadrant, is a private company spun out of the University of Navarra's School of Engineering in San Sebastian, Spain. The company is the only one in this Magic Quadrant that offers a product-based, multitenant (i.e., enables service delivery to multiple customers using shared infrastructure) SWG and e-mail infrastructure solution (Note that SecaaS vendors all offer multitenancy). It is primarily aimed at carriers, managed security service provider (MSSPs) and large enterprises that want to create SecaaS service offerings for their own clients. Optenet is a strong shortlist contender for large organizations and service providers planning on delivering a multitennancy SecaaS-type solution.

Strengths

- Optenet's recently launched Ajax-based dashboard and management interface is the same for Web and e-mail solutions. It is very customizable, enabling users to add different reports in numerous combinations. Hyperlink drill-downs allow fast movement form the dashboard into active reports and log data. Most report elements can be right-clicked for context-aware options. Role-based management includes four roles. Policy auditing and policy review capabilities are very good. Optenet also offers a command line interface and direct policy script editing for more-proficient users.

- The solution can be deployed in bridge and proxy/cache mode or WCCP and ICAP, and provides malware filtering for HTTP, FTP HTTPS POP SMTP and MMS on a variety of platforms, including crossbeam and Linux (Red Hat), as well as appliances.

- Optenet augments Kaspersky, Sophos and Snort Signatures, with its own security analysis for emerging threats. Outbound threat reporting includes a severity indicator in a graphical format.

- Application control includes numerous named applications detected via network signature detection. The solution also offers bandwidth management and QoS features, as well as a good network analyzer that provides network application visibility.

- URL filtering is provided with its own URL database augmented by a dynamic categorization engine. SSL decryption enables dynamic classification of encrypted content. Spanish URL categorization, in particular, is strong. It also has an image analyzer for pornography detection.

- Optenet is very attractively priced.

Cautions

- Optenet's client base is primarily centered in southern Europe, and it has little brand recognition or presence in other markets. It has an office in the U.S., and is aggressively planning expansion. Although the company has numerous small enterprise customers, the solution is designed primarily for the needs of telecoms and large enterprises.
- Options for redirecting mobile clients to the service are very limited, and a globally roaming user is not always automatically directed to the nearest available data center.
- The inclusion of some firewall and IPS-specific configuration in the management policy can cause some confusion.
- Application control does not include any ability to block specific features.
- The outbound security reporting does not include any information type of threats or any detailed threat information.
- The solution does not include any DLP capability.

SafeNet

In March 2009, SafeNet and Aladdin merged under common management as a result of Aladdin's acquisition by Vector Capital (SafeNet's private equity owner). Aladdin was better known for its identity token business, but it was an early entrant in the SWG market. The eSafe Web Security Gateway solution is now part of SafeNet's Enterprise Data Protection (EDP) strategy, which combines encryption and multifactor authentication with the SWG and its native DLP capability. Aladdin had a good cross-section of enterprise customers mostly in EMEA, and also had a presence in North America and the Asia/Pacific region. Its growth rate stalled by our analysis in 2008, bringing down its execution score. eSafe is a reasonable shortlist inclusion for midmarket enterprises in supported geographies.

Strengths

- eSafe has significantly improved its dashboard, reporting and management interface from last year focusing on midmarket needs for lower administration. The dashboard has extensive information in a graphical format with hyperlinked drill-down into detailed report information. The reporting engine was improved with more than 240 predefined reports, including graphical end-user activity reports. Incident and forensic analysis is easy with strong log file search functionality with drop-down picklists of potential search terms.
- Aladdin's heritage as an antivirus company shows in its strong malware filtering capabilities, which includes in-memory code emulation for analyzing suspicious code, vulnerability shielding, script analysis, active content policy options, and SSL decryption. Aladdin added an optional Kaspersky engine in 2008. The eSafe Web Security Gateway is usually deployed as an in-line bridge, allowing it to see all network traffic, but it can also function as a proxy.
- Application controls are above average and include an extensive list (more than 450) of potentially unwanted applications. It also supports blocking of IM file attachments and enforcing acceptable browser types. eSafe provides basic DLP protection with consistent policies across e-mail and Web traffic. It can monitor, log and alert on files attempting to leave the organization, and it supports archiving of outbound content for forensic purposes.

Cautions

- eSafe continues to struggle with brand awareness, especially in North America and overall with its SWG product mind share, and growth is slower than the overall market. Safenet's strategy of combining the eSafe SWG with encryption and identity and access management (IAM) is embryonic, and although these are some of the components of a enterprise data security program, very few enterprises currently consider these domains together when making purchasing decisions. eSafe lacks many enterprise-class DLP features.
- Despite significant improvements in the management interface and reporting engine, some enterprise features are still lacking. The dashboard is not customizable, and with the volume of reports available, it would be beneficial to have a "favorites" tab. Policy creation is not object-oriented and will be difficult to scale for organizations with numerous policy exceptions. The eSafe products lack bandwidth control capabilities, such as enforcing bandwidth utilization policies. Policies for establishing time usage quotas are limited and there is no coaching or soft-blocking capability. Outbound malware reporting is weak, the dashboard has no outbound threat information and predefined reports lack severity indicators or detail that would aid in remediation. eSafe does not provided dynamic classification of uncategorized URLs in real time.

Symantec

Symantec entered the SWG market in 2009 with two major acquisitions. The company acquired SWG and e-mail security SecaaS provider MessageLabs (October 2008) and appliance provider Mi5 Networks (April 2009). Mi5 is now a part of the Symantec Enterprise Security Group and has been relaunched as the Symantec Secure Web Gateway (SSWG). MessageLabs is a good shortlist inclusion for customers looking for a simple-to-use, service-based solution, especially if they are also interested in e-mail security services — especially existing MessageLabs e-mail security clients. SSWG is a good shortlist inclusion for customers looking for a scalable, in-line appliance SWG or those looking to augment their existing proxy cache solutions with better security and application control.

Strengths

- MessageLabs is one of the leading SecaaS secure e-mail gateway vendors, and its Web GUI has the same simple and easy-to-use interface as the e-mail service, making it a good choice for customers looking for both services. We expect that Symantec will gradually build on MesssageLabs as its strategic foundation for various SecaaS offerings, starting with Symantec's existing online net backup service and introducing a

hosted endpoint protection platform (EPP) management server service. MessageLabs has expanded its footprint and now has nine datacenters for the Web Security Service, (Arizona, Virginia, London, Amsterdam, Frankfurt, Hong Kong, Tokyo, Osaka and Sydney) and expects to increase that number to 11 in 2010. We anticipate this expansion will continue with management interface localization, and greater local sales and support, due to the Symantec channel.

- MessageLabs customers give it high marks for service and support. The service offers strong antivirus, latency, uptime and support service-level agreements. Caching popular sites and adding gzip compression are used to accelerate website delivery and minimize latency. Malware is filtered with Symantec's own antivirus scanner as well as the F-Secure engine, augmented by MessageLabs' Skeptic malware filters. The URL database is licensed from Websense, and MessageLabs augments it when it discovers URLs that have been identified as containing malware. MessageLabs also offers a hosted enterprise IM solution and IM hygiene services that include malware filtering, stripping malicious URL links, DLP and file transfer blocking.

- The appliance-based SSWG is most commonly deployed as an in-line bridge (it may also be deployed out of band, on a mirrored port), which enables bidirectional malware scanning of most ports and protocols, and provides for simple network implementation. Scale is achieved by correctly sizing the appliance for the network (up to 1 Gbps), or using a load balancer to deploy multiple boxes to get beyond 1 Gbps. In-line deployment allows for very broad protocol-level application control with binary control (blocking/allow) and policy control of a large number of named applications, such as P2P, IM, games and remote access. URL filtering is provided by an optional IBM URL database.

- SSWG has strong management interfaces. Policy creation is done on single-page view with intelligent options based on previous selections. The dashboard and reporting interface is also strong. Most notable is the reporting emphasis on outbound traffic that indicates the presence of specific malware, the severity and type of the threat, and quick access to more detail. Dashboard data is hyperlinked to relevant reports, and logs with granular details (for example, geolocation data, search terms, file names/types and cross-referencing to greatly aid forensic analysis). SSWG provides a centralized server for configuration and consolidated reporting, and long-term storage of log data. Symantec replaced the Sophos and Sunbelt scan engines and remediation tools (previously licensed by Mi5) with its own scan engine and URL blacklist, while retaining Mi5's network traffic detection techniques, botnet, malware phone-home detection, and inbound content inspection.

Cautions

- The Symantec acquisition adds significant resources to MessageLabs, but also introduces a number of potential distractions from its core mission. Symantec is planning a slow and methodical integration, but, at the same time, it plans to expand its range of SecaaS services and create integrated deployment capability with the SWG and Symantec's endpoint protection clients. In the near term, this introduces some disruption risk. Symantec will also face some cultural challenges with MessageLabs, particularly in refocusing its sales and channel teams on service/selling.

- Despite initial successes, Mi5 lost significant market momentum due to the Symantec acquisition, which it is only now beginning to regain. Symantec faces credibility challenges with network equipment buyers after its poorly executed withdrawal from the network firewall and IPS markets. While Symantec owns the necessary technical components of an SWG solution, it has yet to demonstrate that its SWG business can grow at the same pace or faster than the overall market.

- The MessageLabs services have suffered from slow feature development to enhance the management interface, especially for a service provider. The dashboard and reporting features haven't changed significantly since last year, and reporting has been cited as needing significant improvement by customers. Outbound malware reporting is minimal and does not show severity indicators or threat detail yet. Links to Symantec's threat library and correlated data showing high-risk PCs would be an improvement. The service only supports relatively simple policies and does not allow conditions. There is no way to print policies for reporting audit or troubleshooting purposes, although customers can request a printed copy from the MessageLabs help desk team. The URL policy would benefit from advanced options, such as self-authorization, coaching and bandwidth limitations. Application control is very limited and based only on URL destination rather than network/protocol signatures. IM hygiene and application control are offered as a separate service and not included in the basic package.

- Symantec's decision to substitute its own malware scanning engine (Mi5 had licensed Sunbelt and Sophos) in the SSWG was shortsighted and is limiting to organizations that already use Symantec signatures at the desktop (using different signatures on the SWG and at the desktop is a stronger defense-in-depth model). While we appreciate SSWG's intuitive management interface, its unique design can cause some problems for larger enterprises. For example, it is difficult to add users to multiple groups for policy, the dashboard is not customizable and some customers complained that they couldn't configure complex granular policy or integrate with less-common directory environments. SSWG does not proxy applications or offer a cache, although this is in the road map for 2010. SSWG application control can be improved, such as blocking social networking and blog postings, and granular Web application function control. The solution would benefit from the IM control capability Symantec acquired from IMlogic — currently in the e-mail gateway. SSL decryption is still missing, although this is in the road map for 2010. Advanced policy options, such as coaching or self-authorization, time and bandwidth quota or bandwidth rate shaping, are missing.

- Symantec faces the overall challenge of integrating three security products into an SWG solution with a unified management console. In addition to MessageLabs and Mi5, Symantec also owns DLP technology from its Vontu acquisition.

Currently, Symantec has some interoperability between Vontu and the MessageLabs Web Security Service; however, Gartner expects that full integration of DLP capabilities with its more comprehensive Vontu technology will require a six- to 12-month integration effort, and will necessitate evolving packaging and pricing as Symantec attempts to balance single-channel DLP needs with enterprise market needs.

Trend Micro

Trend Micro is the only EPP vendor that has a long history of focus on antivirus for the Web gateway market. As a result, it has a respectable market share with global enterprises. However, the company has not sufficiently invested in advanced features that differentiate its Interscan Web Security Suite (IWSS) SWG offering and allow it to break into the Leaders quadrant. Still, Trend Micro is a respected shortlist inclusion for midsize and smaller organizations.

Strengths

- The management interface is significantly improved in the recently launched V5, with a very customizable Adobe Flex dashboard environment and significantly improved advanced reporting. New customized reports can be created using open-source iReport and added as a dashboard element or in completely new tabs. Dashboards provide quick hyperlinked drill-down into detailed logs. In distributed environments, a centralized IWSS instance can act as a consolidated reporting engine/database and remove a task from the scan engine to improve and consolidate local performance.

- Malware detection is provided by Trend Micro's signature database, and reputation service is augmented by its in-the-cloud "smart protection network." Trend Micro's damage cleanup service can provide remote client remediation for known threats. IWSS offers a quarantine disposition action for parking suspicious files or blocked FTP file types. Suspicious files can be automatically sent to Trend Micro labs for analysis.

- Trend Micro offers its own URL categorization database and offers time of day, and time and bandwidth quota policy options. Application control includes some P2P and IM traffic types that are detected by network signatures.

- The IWSS family of products offers numerous product platform options (for example, Crossbeam integration, Linux, Windows, Solaris and VMware virtual appliance) and numerous deployment options (for example, ICAP, WCCP, transparent bridge, and forward and reverse proxy). Multiple IWSS products can be pooled or clustered with automatic policy synchronization for increased redundancy and scale.

Cautions

- Despite Trend Micro's history in this market, it has failed to lead the market with enterprise-class features. This has allowed the more aggressive competition to steal mind share, particularly in large enterprises. Trend Micro needs to invest in advanced product features if it wants to regain momentum in the SWG market.

- IWSS is software-based — it does not offer an SWG hardware appliance. Trend Micro's SecaaS solution has not been successful. IWSS solutions are still lacking in numerous large-enterprise features, such as advanced role-based administration, policy summaries and multiple directory synchronization. Bandwidth control is limited to quotas only. The outbound malware detection report, which is significantly improved in V5, still lacks severity indicators to enable prioritized remediation.

- Application control is limited to binary blocking of some P2P, IM and URL categorization blocking. Trend Micro does not have any onboard DLP, although it does offer an endpoint DLP solution.

- Like other EPP vendors in this market, Trend Micro's biggest challenge in the enterprise is offering buyers a suite that provides sufficient "defenses in depth." Malware detection is provided by the same signatures as for e-mail and end nodes.

- There is no ability to protect off-LAN devices without OfficeScan EPP or apply URL filtering policy/reporting for mobile devices.

Webroot Software

Webroot Software is better known for its endpoint spyware protection solutions; with the acquisition of Email Systems in 2007, the company is offering e-mail security and Webroot created its own SWG services via a SecaaS offering. Webroot is a good shortlist inclusion for SMBs looking for service provider options in supported geographies.

Strengths

- Malware protection is provided by Webroot and a Sophos malware signature database. Nonsignature threat detection capabilities include an anti-phishing engine, as well as heuristic-based JavaScript, XSS, Shellcode, and polymorphic attack analysis. Webroot has had considerable experience and a strong track record in the area of Web-borne malware detection, which has been the company's focus since its inception in 1997.

- Webroot operates three data centers — in the U.S., U.K. and Sydney, Australia — and uses Amazon infrastructure in the eastern U.S. and Dublin, Ireland. The service uses compression and HTTP translation to accelerate content from the data center to end users to minimize latency. HTTP traffic is redirected to these proxies via a local proxy or firewall settings, a client proxy setting or a client software agent. The mobile client is easy to use and configurable via the cloud-based centralized management console, it is not proxy auto-configuration (PAC) file-based, nor does it require an authentication server on premises.

- The Web management interface provides centralized management of Web and e-mail service, is user friendly and can be administered by nontechnical users. The unique graphical view of its URL-filtering policy is especially easy to understand. It provides a granular role-based administration rights capability,

and good role-based policy and policy audit logs. Log search capability is also very good. Log data includes the search term query string and has a link to the search results, which is a good feature to help understand user intent.

- Policy options include blocking certain files by type and size, and a soft block function that enables users to visit a blocked category for a length of time. Quota-based policies can be configured to limit the amount of bandwidth used in a specified time window. The URL filtering provides an anonymous proxy detection capability.

- The service includes search results (Google, Yahoo, MSN Live Search and Ask.com) decorated with security warnings and URL categorization icons.

Cautions

- Webroot has had initial success in the SMB market (fewer than 1,000 seats), but has failed to get the attention of the larger enterprise customers. It needs to improve its enterprise feature set and expand its global footprint and channel to break out of its SMB niche. Although Webroot has done a good job of catching up to the state of the art in the management console and feature set, it has not yet distinguished itself with any outstanding differentiated feature that would move it into the Visionaries quadrant.

- The dashboard is very basic and static, with little customization. There are no hyperlinks to drill down into the detail from dashboard elements. Reporting is basic, with limited advanced functions. There is no ability to create ad hoc reports, although administrators can change options on the 25 report templates to get different slices of data. Reports do not offer multiple chart types — only bar charts and tables. Outbound threats are in static reports, but not in real-time dashboard views, and threat information is restricted to threat types. There are no links to malware encyclopedia information or severity indicators. There is no user-readable policy summary for auditing or troubleshooting. Limited customization capability makes it difficult to create regional block pages for global companies.

- Application control is limited to blocking URLs of registration servers, and the solution offers no DLP capability.

- Like other SWG SecaaS providers, inbound and outbound malware detection is limited to HTTP traffic types that are redirected to the service.

Websense

Websense has a long history in the Web filtering market, and the company dominates the market for URL-filtering software. The acquisition of SurfControl in 2007 added a SecaaS offering now called Websense Hosted Web Security Gateway (HWSG). Websense's first proxy-based multifunction SWG solution, "Websense Web Security Gateway (WSG) — released just prior to last year's Magic Quadrant — is gaining traction now that it has been released in an appliance form-factor. Websense's dedicated focus on the SWG market, its market share, the breadth and depth of its initial offerings and the success of its proxy-based SWG platform moved it into the Leader quadrant this year. Given the breadth of its product family, Websense is a good shortlist inclusion for any size company.

Strengths

- Websense's URL-filtering solution has a solid North American and EMEA presence in companies of all sizes, and a strong distribution channel that enables it to target large enterprises and SMBs. The introduction of its proxy-based SWG solution gives Websense the ability to up-sell its installed base from the URL-filtering solution to the broader SWG capability, and gain more account ownership and loyalty in the process. The company is primarily focused on the Web gateway market, and has extensive experience and resources dedicated to detecting Web-borne malware. With the exception of the third-party signatures, Websense owns all the core technology in its products. It is well-positioned to execute on its road map to offer hybrid (customer premises-based and SecaaS-based) SWG solutions that can be managed by a unified policy console.

- Websense's management console is one of the best in the market and is consistent across all its offerings (except the SecaaS solution). Navigation is task-based, and policy creation is intuitive and easy to use. There is a useful customizable toolbox element that enables common tasks to be consolidated into a single menu. The dashboard includes hyperlink drill-downs into more-detailed reporting data. Policy can be developed in a single pane, with extensive parameters and a logical workflow. URL policy parameters are broad, and include options such as bandwidth, time restrictions and quotas. Optional category-based SSL traffic decryption is included to filter encrypted Web traffic.

- In addition to third-party malware signatures and the Websense database of infected URLS, the WSG provides very extensive on-box, real-time malware content analysis to detect suspicious code fragments and other signs of infection.

- Application control includes more than 125 applications, such as IM and chat, streaming media, P2P file sharing, e-mail and collaboration based on network signatures. Websense's Network Agent provides an out-of-band network analyzer that enables the combined solution to monitor all traffic (not just traffic destined for the proxy) for malware application and DLP violations, and provides overall traffic analysis capabilities.

- The acquisition of PortAuthority in 2007 provided Websense with strong DLP technology, which is now offered as an additional module that enables granular content-aware policy and reporting. Data detection techniques are complete, and the product includes several predefined dictionaries and policies.

- Websense is one of the few vendors that can offer software, appliances, client software and SecaaS. Websense software solutions can run on Windows, Linux and Solaris, as well as on numerous third-party network hardware platforms (firewalls and proxies). In addition, Websense has partnered with Crossbeam, Celestix Networks, Resilience and HP for preinstalled solutions.

Cautions

- Despite significant technology investments, Websense still needs to prove that it can make the transition from a relatively uncontested software-based URL-filtering vendor to a multiplatform SWG vendor in a much more hotly contested market against significantly more strategic competitors. While Websense has a significant installed base, up-selling clients to the WSG platform or service creates opportunities for the competition to get a foot in the door.

- The WSG appliance and software is still not widely deployed, and early feedback regarding service and support from v10000 customers has been mixed. It needs to add various sizes of appliances to appeal to the SMB market. Some aspects of Websense's reporting need improving. Specifically, outbound malware reporting is lacking in actionable detail, and scheduled reports lack more-visual graphs.

- Websense needs to add more data centers to improve the geographic coverage of its SecaaS service, particularly in the Middle East and Asia/Pacific. Websense is busy overlaying the same management interface as the appliance and software to the SecaaS service, which will allow customers to move seamlessly from appliances to services or use a hybrid approach. However, the service dashboard would benefit from more performance metrics and service-level commitments.

- Websense is more expensive than its counterparts; however, it generally matches competitive prices in large, contested deals.

Zscaler

Zscaler is a new SecaaS vendor in the SWG market in 2009. The company invested significant resources in a unique multitenancy architecture that disconnects policy administration, reporting and enforcement, enabling each element to scale independently. It is now investing in rapid feature development, global rollout of enforcement nodes and sales presence, resulting in impressive growth in numerous global markets among small and very large enterprise clients. Zscaler is a very strong choice for any organization interested in a SecaaS SWG solution.

Strengths

- The management interface (Flash-based) is easy to use, even for nontechnical administrators. All reports are dashboards and are based on live data and allow hyperlinked drill down into detailed log data. Zscaler's Nanolog technology reduces log size by a factor of 50, enabling very fast reports and longer retention of detailed data. The dashboard has a unique "compared to industry peers" report, which shows relative data compared to averages for Zscaler customers. Zscaler provides latency statistics for each stage of a round trip Web request, enabling fast troubleshooting as well as SLA-compliance monitoring.

- The policy manager is very easy to use and logical. All policy is user-based and follows roaming users, allowing immediate service at the nearest enforcement node.

- Zscaler has several methods for redirecting clients that are very simple to set up. It is the only vendor to offer redirection with authentication without a software client on mobile devices. It also supports standards-based Generic Routing Encapsulation (GRE) tunnels, and can host customer PAC files.

- Zscaler offers two levels of security protection. In addition to using several signature and blacklist-based filters, Zscaler has numerous advanced security checks including page analysis, URL reputation, and script analysis. Zscaler provides reporting and policy options to enable organizations to block unsupported or vulnerable browsers or browser versions.

- Application control includes numerous named applications that can be blocked using a combination of destination URL and some network signature analysis. Companies under pressure to liberalize productivity filters will appreciate the option to allow Web 2.0/social networking page view while blocking posting to these sites, as well as optional DLP, which is adequate for most organizations' corporate or government-compliance needs. Zscaler offers granular, policy-based control of Web-based applications, such as IM, blogs, streaming and Web mail, including QoS bandwidth control.

- Zscaler's unique architecture and highly scalable purpose-built enforcement nodes enables fast global deployments. Its SecaaS offering already has the largest global footprint of data centers (among all SecaaS SWG vendors in this Magic Quadrant) and continues to expand. It also allows for "private node" and "private cloud" deployments for very large organizations, service providers, or organizations in unique geographies.

Cautions

- Although Zscaler has had early market success competing against other SecaaS startups, the market will be different in 2010 with the Cisco/ScanSafe and Barracuda/Purewire deals. Now, it is competing against more-mature organizations with better-established sales and support organizations. For the most part, these competitors are able to offer a broader portfolio of solutions, as well as multiple delivery form factors and hybrid offerings.

- While most of Zscaler's customers in 2009 were from the SMB market, it also won several large deals that were greater than 100,000 seats. Zscaler needs to prove its ability to successfully deploy and support these large enterprise customers.

- Zscaler does not offer e-mail security or other services for companies looking to consolidate SecaaS vendors (e-mail spam and virus filtering is scheduled for 1Q10).

- Although its enforcement nodes are widely geographically dispersed, the reporting and policy data reside only in the U.S. and England so far. The company has plans to add reporting and policy servers to its Asia/Pacific data centers in the future.

- The management interface is missing full customization of dashboard elements. Report information about threats could be improved. Outbound threats reports do not include any severity indicator or link to detailed information about threats, and there is no consolidated threat report with drill-down data. In particular, a consolidated and prioritized report on outbound traffic indicating action items for PC operations would be useful (i.e., combination of application and security traffic types).

- There are no native FTP application controls, but it does support stand-alone FTP clients as well as FTP over HTTP.

- Clientless redirection methods for laptops are lightweight and easy to use, but not tamperproof. Like other SecaaS offerings, application control and outbound threats that do not use port 80, and 443 (HTTP, HTTP/S) can evade detection unless all traffic is redirected to Zscaler.

Vendors Added or Dropped

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

Acronym Key and Glossary Terms

ARM	advanced reporting module
CSG	content security gateway
CSV	comma-separated values
DLP	data leak prevention
EMEA	Europe, the Middle East and Africa
ePO	epolicy orchestrator
GLBA	Gramm-Leach-Bliley Act
GRE	Generic Routing Encapsulation
GUI	graphical user interface
HTTP/S	HTTP over SSL
ICAP	Internet Content Adaptation Protocol
IM	instant messaging
IP	Internet protocol
IWSS	Interscan Web Security Suite
MMC	Microsoft management console
OS	operating system
PAC	proxy auto-configuration
P2P	peer-to-peer
PCI	Payment Card Industry
SecaaS	Security software as a service
SMB	small or midsize business
SSL	Secure Sockets Layer
SOX	Sarbanes-Oxley Act
SQL	Structured Query Language
SWG	secure Web gateway
TCO	total cost of ownership
USG	unified security gateway
UTM	unified threat management
VoIP	voice over IP
WCCP	Web Cache Communication Protocol

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 and skills, whether offered natively or through OEM agreements/partnerships as defined in the market definition and detailed in the subcriteria.

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

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

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

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

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

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

Completeness of Vision

Market Understanding: Ability of the vendor to understand buyers' wants and needs and to translate those into products and services. Vendors that show the highest degree of vision listen 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 Web site, 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.