

Magic Quadrant for Secure Web Gateway

Peter Firstbrook, Lawrence Orans

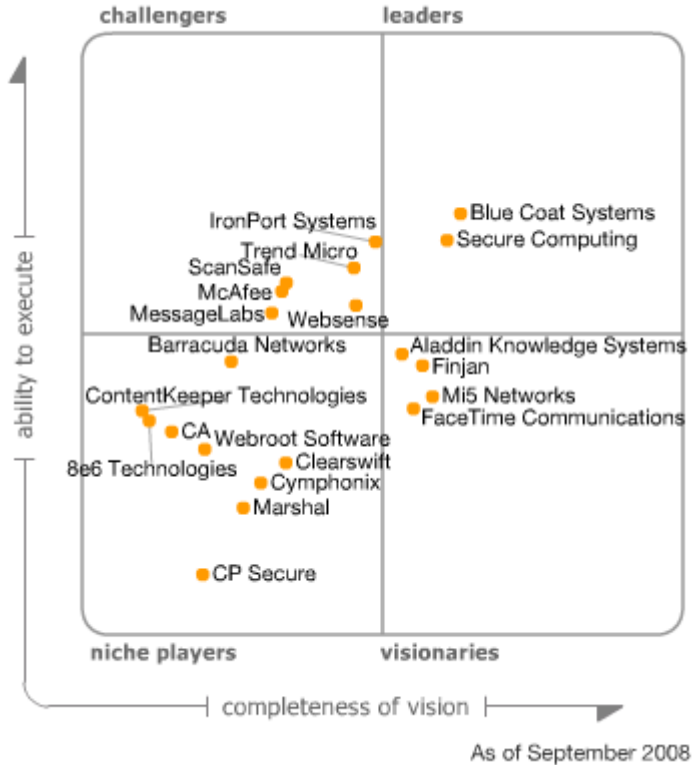
Secure Web gateway solutions protect Web-surfing PCs from infection and enforce company policies. Incumbent providers have been slow to respond to changing demands, while new vendors are struggling to get the right product mix and prove their mettle in the demanding enterprise market.

WHAT YOU NEED TO KNOW

- Organizations need to purchase a strategic product that has a road map coinciding with long-term needs — which would mean sacrificing current functionality — or accept a tactical solution that solves current needs and will likely need to be replaced in the midterm to long term.
- If URL-filtering reporting is a key requirement, then traditional URL-filtering vendors represent the best choice.
- Given that malicious software (malware) filtering is a key requirement, products must offer proactive "zero day" malware detection techniques that do not rely on previous knowledge of the malware, as well as signature-based detection techniques. Products should inspect bidirectional Layer 4 through Layer 7 network traffic across all ports and protocols.
- Application control is the least-mature secure Web gateway (SWG) feature.
- Large enterprises will have a smaller field of candidates to select from because of scalability and reliability demands.

MAGIC QUADRANT

Figure 1. Magic Quadrant for Secure Web Gateway



Source: Gartner (September 2008)

Market Overview

An SWG is a solution that filters unwanted software/malware from user-initiated Web/Internet traffic and enforces corporate and regulatory policy compliance (see "Introducing the Secure Web Gateway"). To achieve this goal, SWGs must, at a minimum, include URL filtering, malicious-code detection and filtering, and application controls for popular Web-based applications, such as instant messaging (IM) and Skype. Native or integrated data leak prevention (DLP) is also increasingly included.

This market is rapidly emerging as a stand-alone market from historically distinct markets, such as proxies/caches, URL filtering and antivirus gateways. Buyers should be careful not to blindly shortlist only vendors in the Leaders quadrant in this market. No product completely satisfies all functional categories in a single product, and buyers will definitely need to make some sacrifices (see "A Buyer's Guide to Secure Web Gateways"). Vendor road maps should be an important consideration.

Having a malware-filtering capability is critical as the Internet and Web become the major infection channels. Almost all organizations that implemented a bidirectional malware-filtering SWG found numerous adware, spyware and other malicious content on their networks. Surprisingly, numerous products we reviewed failed to identify infected end nodes on the

management dashboard and, instead, buried this critical information in reports. We gave extra credit to products that offered proactive and signature-based detection techniques, and those that had bidirectional Layer 4 through Layer 7 network traffic inspection across all ports and protocols, rather than being blind to all but proxied protocols.

The traditional URL-filtering vendors remain a good choice for scalable, granular Web use reporting, especially for larger organizations; however, new vendors are rapidly catching up in this criterion, and most can easily replace traditional solutions while providing more value. Application control is the most-immature SWG feature. IM, Skype and peer-to-peer (P2P) applications are the most-commonly supported; however, few SWG solutions can do more than block or allow access on a group or user level. Even fewer use application network signatures versus more-easily evaded URL or Internet Protocol (IP) address blocking. Secure Sockets Layer (SSL) traffic, in particular, is a notable blind spot for many SWG solutions.

Large enterprises will have a much-smaller field of candidates to select from because of scalability and reliability demands. Scanning large network pipes for malware with low latency is difficult. In-line scanners tend to scale best. The ability to seamlessly cluster and manage multiple appliances or software instances is rare (for example, Blue Coat Systems, Cisco/IronPort Systems and Secure Computing). One of the primary advantages of an e-mail security vendor in the Web gateway is the coordination of content policy across all communication channels; however, only a few vendors (for example, Clearswift, Marshal, McAfee and Trend Micro) actually share a common content inspection or DLP or data loss prevention policy across e-mail and Web traffic.

The form factor of SWG products is rapidly being transformed from software-based products to scalable appliances and to managed services (see "Pros and Cons of SaaS Secure Web Gateway Solutions"). We expect more virtual appliances that allow for server hardware standardization but still provide the low total cost of ownership (TCO) of appliances. Many appliance vendors plan to provide software as a service (SaaS) SWGs in the near term, and we anticipate hybrid solutions that allow for common management of appliances in the data center, with services to protect mobile users and branch offices. Some vendors offer client-side solutions to enforce policy on mobile devices; however, enterprises have been reluctant to manage yet another client-side software product, and we did not give this feature significant weight. Leading antivirus vendors that already have a client-side presence and management capabilities have the best chance to make this type of deployment model (in other words, gateway and client) successful, although we question their ability to dramatically improve security by running the same signatures in different places.

For a more complete list of desirable distinguishing features for RFPs and vendor demonstration analysis, see "A Buyer's Guide to Secure Web Gateways."

Market Definition/Description

The SWG market is an emerging composite market made up of multiple security markets. URL filtering is the largest submarket (roughly 40% of the total market size). Other submarkets include antivirus filtering for Web traffic (10%), proxy caches (27%) and dedicated multifunctional SWG devices (23%). Market distinctions are rapidly blurring as submarket vendors maneuver to compete in the broader SWG market. We estimate that the total composite market exceeded \$1 billion in 2007 and was growing at a rate of 44% year over year. Dedicated SWG vendors are the fastest-growing submarket, averaging 140% year-over-year growth. We expect average market growth rates to be in the 25% to 35% range for the next two years. This growth will be fueled by increased penetration of dedicated SWG devices, incremental feature revenue and the impact of appliance-based products replacing software.

URL filtering functionality is already deployed in roughly 75% to 95% of enterprise networks, while dedicated SWGs are deployed in less than 30% of enterprise networks. The URL filtering market will be cannibalized by the broader SWG market.

Inclusion and Exclusion Criteria

The following criteria must be met to be included in this Magic Quadrant:

- Vendors must own unique content capability in at least one of the following categories: URL filtering, anti-malware or application-level controls. This includes granular active content policies, dynamic classification of Web sites 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, unified threat management (UTM) devices — are outside the scope of this analysis. UTM 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. UTMs are compelling for the small or midsize business (SMB) market; however, in most circumstances, enterprise buyers do not consider UTMs as replacements for SWGs. Examples of vendors with UTM solutions include Astaro, Check Point Software Technologies, Fortinet, Palo Alto Networks and SonicWALL.

Added

Vendors added this year include ContentKeeper Technologies, CP Secure, Cymphonix and Webroot Software. Other vendors initially considered for inclusion were BorderWare, Microsoft and Symantec; however, these vendors did not have all the required elements. Other vendors in the service market, such as Optenet, Purewire and Zscaler, were too new to the enterprise market for inclusion this year.

Dropped

Vendors dropped this year include St. Bernard and Sophos.

Evaluation Criteria

Ability to Execute

Vertical positioning on the Ability to Execute axis was determined by evaluating the following 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	low
Market Responsiveness and Track Record	high
Marketing Execution	no rating
Customer Experience	standard
Operations	low

Source: Gartner

Completeness of Vision

The Completeness of Vision 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 the following 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, 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 Web sites were 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 categorization of new sites/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 IM, multiplayer games, Web storage, wikis, 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. The ability to selectively block or manage features of applications based on numerous policy parameters and the presence of predeveloped policies to simplify deployment were given extra weight. In a mashed up, Web 2.0 world, it is difficult to say

exactly what constitutes an application, so customers shouldn't assume that any vendor will be able to control all forms of unwanted Internet activity.

- **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** — Appliance- and/or service-based delivery models get extra credit compared with software only, and extra credit was given to vendors that offer all three deployment types. Also, the quality of the form factor was considered (for example, appliances that fail when open and are hardware-optimized for the job). Software that comes as a virtual appliance gets credit compared with software that requires a base operating system (OS). For services, infrastructure quality was considered.
- **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	no rating
Marketing Strategy	no rating
Sales Strategy	low
Offering (Product) Strategy	high
Business Model	no rating
Vertical/Industry Strategy	no rating
Innovation	low
Geographic Strategy	low

Source: Gartner

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. Challengers' 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 tactical 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 higher risk of business disruptions.

Niche Players

Niche players' 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 providers' offerings to be "best-of-need" solutions.

Vendor Strengths and Cautions

8e6 Technologies

Strengths

- 8e6 Technologies is an appliance-only, URL-filtering solution vendor that targets primarily the education market and large enterprises.
- Its R3000-filtering appliances are positioned out of band, so they do not require integration with proxy caches or firewalls. URL blocking is achieved by sending a Transmission Control Protocol reset message to break a connection.
- The company offers two reporting appliances. Enterprise Reporter uploads logs from the R3000-filtering appliance and generates reports. Threat Analysis Reporter provides real-time monitoring of an organization's Web use and real-time alerting of policy violations.
- Enterprise Reporter can be used to show a user's intent when browsing the Internet. For the most-popular search engines, the R3000 records the text entered for a query, and Enterprise Reporter can display this text. Thus, users browsing inappropriate sites cannot claim that a bot or malware directed their browser to the inappropriate content.
- 8e6 was one of the first URL-filtering vendors to develop a set of signatures for detecting anonymous proxy use (to bypass URL blocking). In 2008, it expanded its signature library to detect and block traffic from online gaming, remote access and streaming media applications. The R3000 also includes signatures for blocking common IM and P2P applications.
- 8e6 offers a strong URL-filtering solution at a moderate price, particularly for organizations that value scalability and high-performance reporting.

Cautions

- The R3000 does not provide adequate malware protection. It does not scan content for malware, nor can it provide any proactive malware protection outside of blocking traffic to known malicious URLs.

- The solution requires three appliances (filter, historical reporter and real-time analysis reporter) to get full enterprise functionality. (Note that 8e6 offers the R3000IR appliance for customers with fewer than 1,500 users that integrate the R3000 Internet Filter and Enterprise Reporter, so only two appliances are required for smaller-size customers.)
- 8e6 cannot inspect SSL traffic but can detect destinations to block or allow traffic.
- The company lacks the ability to dynamically classify unknown URL addresses in real time.
- With its large installed base and its strong URL filtering capabilities, 8e6 would make an attractive acquisition target for another SWG vendor. As the SWG market evolves, and malware protection becomes a bigger driver for SWG purchases, 8e6 will need a partner that offers strong anti-malware capabilities.

Aladdin Knowledge Systems

Strengths

- Aladdin Knowledge Systems is an early solution provider in the SWG market, although it is perhaps better-known for its identity token business. The installed base of its SWG product line represents a good distribution of large and small enterprises across a wide geography.
- Aladdin offers four appliance models and a Virtual Appliance — a self-contained CD with a hardened Linux OS that installs on a standard Intel-based server and converts it into an appliance.
- The eSafe product line offers numerous flexible deployment options. It is usually deployed as an in-line bridge, but it can also function as a proxy — although it only provides proxy support for native HTTP and HTTP over SSL (HTTP/S), including FTP over HTTP. When deployed as an in-line bridge, Aladdin inspects all incoming Web traffic and detects protocols on all ports.
- Aladdin's heritage as an antivirus company shows in its relatively strong malware-filtering capabilities, which includes in-memory code emulation for analyzing suspicious code, vulnerability shielding, script analysis and SSL decryption. Network bridge deployment puts it in the path of more potentially malicious outbound traffic-evading standard ports.
- Application controls include an extensive list (500) of potentially unwanted applications by name and IM file attachment blocking.
- The eSafe appliances offer an optional URL-filtering database, which is licensed from IBM.
- Aladdin is a reasonable shortlist inclusion for all enterprise types.

Cautions

- Aladdin 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.
- Aladdin's management interface is due for an overhaul. It is still a Microsoft management console (MMC)-style console with numerous pop-up windows and is not task-based. The home page dashboard is basic and lacks action-oriented information.

- Reporting is weak compared with peers, eSafe Reporter is a separate Web interface from management and dashboard, and there are no hyperlinks for rapid drill-down into detail. Critical reports such as per-user report summaries and basic features such as pie charts are missing. There is no ad hoc report creation facility. Aladdin expects to launch a revised reporting version in 4Q08.
- URL filtering lacks some advanced features, such as coaching or softblocking ability.
- Some users report scalability problems with Aladdin's database, which leads to problems in generating reports.
- Aladdin has developed its own proprietary anti-malware engine. Aladdin's research team has not developed a strong reputation for developing threat signatures. While the industry-standard antivirus vendors are struggling to keep up with the increasing volume of threats, it will be difficult for smaller in-house research labs to continue to provide much more than emergency signatures for the most-prevalent threats.
- Aladdin does not have any native data leakage technology, although it can integrate via the Internet Content Adaptation Protocol (ICAP) to third-party data leakage solutions.

Barracuda Networks

Strengths

- Barracuda Networks offers a range of inexpensive proxy-based appliances. It manages to keep its costs low by using open-source technologies (for example, Clam AntiVirus and open-source URL filtering) and manufacturing its own appliances. Barracuda enjoys high mind share due to extensive marketing and an effective sales channel, and it is experiencing solid growth.
- Its Web graphical user interface (GUI) is basic and designed for ease of use. Deployment is simplified with all settings in a single page. 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, Skype, and applications listed by name and blocked by a network signature.
- URL-filtering controls include some advanced features, such as bandwidth consumption limits and time-based policies.
- The Barracuda Web Filter is one of the most economically priced solutions in this research, and annual updates are priced per appliance rather than per seat.
- Barracuda is a good shortlist inclusion, primarily for SMBs looking for "set and forget" functionality at a reasonable price.

Cautions

- Barracuda's hostile bid to acquire Sourcefire will likely detract valuable time and resources from Barracuda's executive team. Gartner also believes that the proposed deal lacks synergy because Barracuda competes in the SMB market and Sourcefire competes in the enterprise market. There will be little opportunity for Barracuda to sell its products to Sourcefire customers and vice versa.
- Barracuda Web Filter lacks enterprise-class administration and reporting capabilities. It does not support consolidated reporting and centralized administration for multiple appliances. Advanced ad hoc reporting features are lacking. 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.
- Barracuda relies heavily on open-source databases for URL and antivirus filtering (Clam AntiVirus). Although it supplements these databases with data collected from its customer base (it adds URLs and develops proprietary signatures to combat malware that it has detected), Barracuda's research labs have not earned a strong reputation in the industry. With the industry standard antivirus vendors struggling to keep up with the increasing volume of threats, it will be difficult for smaller in-house research labs to continue to provide more than emergency signatures for the most-prevalent threats.

Blue Coat Systems

Strengths

- Blue Coat Systems is the most mature vendor in this market. Its ProxySG product is well-tested for scalability and performance in the demanding large enterprise market. The company has one of the biggest development and support organizations in this market.
- Blue Coat's proxy appliances offer strong application and network acceleration capabilities, and its acquisition of Packeteer (April 2008) should enhance its ability to enforce security policies on a per-application basis.
- Its management dashboard is good and features customizable views and the ability to add preconfigured panels or edit panels, and move panels around.
- 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. Blue Coat's URL-filtering database is very competitive and has the ability to dynamically classify unknown URLs by sending the URL to one of three data centers "in the cloud," where it is analyzed.
- Blue Coat has some zero-day, malware-filtering capabilities. It can validate or limit active content (for example, ActiveX Controls or Java Applets) by policy. It can provide some active code analysis ability to detect unknown malware. The solution also provides a URL reputation score for unknown sites. The Blue Coat classification engine collects URLs from its customer base to detect malicious content and updates its ProxySG appliances every 20 minutes.
- Blue Coat's URL-filtering cost structure includes an upfront perpetual license fee plus annual maintenance charges. Blue Coat is often the least-expensive URL-filtering option.

- Blue Coat's ProxySG proxies more protocols than any other proxy in the market.
- ProxySG has extensive authentication and directory integration options.
- Blue Coat's SSL termination capabilities (via an optional card on ProxySG) enable Blue Coat to decrypt SSL content and hand it off (via ICAP) to third-party devices, such as DLP scanners (Blue Coat partners with four DLP vendors), for further analysis.
- Overall, Blue Coat remains the market share leader in the proxy market and is a strong solution for large enterprises.

Cautions

- Blue Coat's continued corporate emphasis is on network acceleration techniques, as evidenced by its acquisition of Packeteer, comes at the expense of a more robust security focus. This acquisition will divert focus and resources on Blue Coat's security efforts through at least mid-2009. Although Packeteer's application detection and rate-shaping technology will enhance Blue Coat's application control capabilities, it is unclear how much Packeteer functionality will make its way into the core ProxySG.
- Blue Coat reliance on an external anti-malware appliance is a liability in the SMB market, where proxy antivirus appliances add unnecessary costs and complexity. We anticipate that Blue Coat will have to undergo a significant OS redesign to compete with a single-box solution.
- Blue Coat's ability to detect infected endpoints is limited to detecting traffic to known malicious URLs. The proxy cannot isolate or clean infected machines and can only detect malware in traffic that is proxied. Evasive outbound "phone home" traffic may evade detection by port or protocol hopping.
- The management interface is a mix of applications — each with a different look and feel. Creating policy requires stepping through multiple tabs and pop-up windows. Although the management interface is very powerful, it is not user friendly. The Blue Coat Reporter product is a separate application that comes at an extra cost for the enterprise version. Some aspects of the management interface belie growth by feature rather than function (for example, threat reporting is not consolidated, and administrators must check reports from the URL logs and ProxyAV to get a good overview).

CA

Strengths

- CA's main SWG product, the Gateway Security WebFilter proxy, is a component of CA Gateway Security, which provides a common management interface, as well as policy and reporting for Web and e-mail gateways.
- Malware detection is provided by the CA eTrust anti-malware database.
- URL filtering is provided using the Secure Computing 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 excellent 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).
- The CA WebFilter is a shortlist inclusion for SMBs looking for a suite solution, along with e-mail.

Cautions

- CA's biggest challenge in the enterprise is offering buyers a suite that provides sufficient in-depth defenses. Malware detection is provided by the same signatures as for e-mail and end nodes. Zero-day threat detection is limited.
- The Gateway Security management console is confusing, 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.
- 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 and find the relevant report. Reports are very basic, and there are only a limited number of predeveloped reports. Included reports are not comprehensive. 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 filtering. Application blocking is URL-based or port blocking, and is not menu-driven.
- The proxy only supports HTTP and HTTP/S. There is no SSL decryption capability or native FTP proxy support. Inbound and outbound malware can evade detection by port/protocol hopping or hiding in HTTP/S.
- CA offers only software for Microsoft platforms, so it will be hard-pressed to match the performance, scalability and security of purpose-built appliances for larger data center customers. Support and cost of the underlying Windows hardware and software should also factor into the TCO.

Clearswift

Strengths

- Clearswift is a veteran secure e-mail vendor with a high profile in Europe, the Middle East and Africa (EMEA). It has integrated a proxy-based SWG into its e-mail security appliances and software.
- Its browser-based management interface provides a clean logical 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, and configuration is gradually implemented as users end their browsing sessions.
- Policy development for DLP is one of the best in this market and several policy constructs — that is, Sarbanes-Oxley Act (SOX), Gramm-Leach-Bliley Act (GLBA), Payment Card Industry (PCI) 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 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. It is augmented with some in-house preconfigured, policy-based code analysis.
- MIMESweeper Web is capable of SSL certificate validation, decryption and inspection.
- URL categorization is provided by the Websense database.
- 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.

Cautions

- Clearswift remains an EMEA brand and does not enjoy significant brand recognition in North America. Its market share in the SWG market is minimal, and its growth rate is well below the SWG market growth rate.
- Malware detection is primarily limited to signatures and only in HTTP/S traffic. The proxy cannot isolate or clean infected machines.
- URL-filtering policy options do not include advanced features such as time of day, bandwidth or quotas.
- Application control is limited to blocking URL destinations (and/or streaming protocols) and file type blocking. It cannot filter or manage evasive applications, such as Skype.
- MIMESweeper Web does not support in-line/bridge mode deployments, ICAP or Web Cache Communication Protocol (WCCP). Active configurations require Layer 4 load balancing or static proxy auto-configuration (PAC) file settings.

ContentKeeper Technologies

Strengths

- ContentKeeper Technologies is an Australian-based company with an SWG appliance that deploys as an in-line bridge. The main focus of the company is URL filtering, and the company maintains its own URL-filtering database.
- The ContentKeeper appliance includes a high-availability module that "fails open."
- Malware filtering is provided via signature feeds from F-Secure and others.
- ContentKeeper offers one of the most cost-effective URL-filtering solutions in the market.
- ContentKeeper appliances maintain a feedback loop with the ContentKeeper data center. On an hourly basis, the appliances receive updates to the URL database, and they send any unclassified URLs to the data center for analysis and classification.

- Its Advanced Reporting Module (ARM) is an optional off-box solution that provides good graphical analysis. The Content Keeper appliance can be set to export data to the ARM on a periodic basis.
- ContentKeeper offers a decent URL filtering solution in supported geographies.

Cautions

- ContentKeeper has a weak presence in Europe and North America (more than 50% of its sales are in the Asia/Pacific region).
- Some North American customers reported issues reaching the support organization, which is based in Australia (the quality of the support was fine; the problem related to time zone issues). In mid-2008, Content Keeper opened a U.S.-based office in an effort to improve North American sales and support.
- Some ContentKeeper customers reported that the product is not mature and that documentation was weak.
- On-box reporting is limited and is not linked (via hyperlinks) to the ARM for rapid drill down into details.
- ContentKeeper needs to improve the ease of use and graphical capabilities of its administration tool (management and configuration).

CP Secure

Strengths

- CP Secure was founded in 2002 by former Trend Micro employees. The company's flagship SWG product — Content Security Gateway (CSG) — is an in-line malware scanning appliance rather than a proxy.
- It can scan Web and e-mail protocols (for example, HTTP, HTTP/S, FTP, SMTP, IMAP and POP3) for malware using Kaspersky signatures. Its primary differentiator is its use of stream-based scanning technology, which minimizes latency.
- CP Secure offers several box choices for organizations from 100 to 5,000 users and can be scaled up to clusters of four boxes with internal load balancing. In single-box deployments, high availability of the Internet access is delivered via "fail-to-wire" settings.
- The management interface and malware reporting are basic and easy to use. CSG can be preconfigured and shipped to remote offices, and installation is simple.
- CSGs can run an on-box Websense agent and use Commtouch for rudimentary spam filtering.
- CP Secure is a potential shortlist inclusion for organizations looking for low-latency, signature-based malware scanning.

Cautions

- CP Secure is struggling to mature as a company. It has minimal market or mind share and is not growing. Despite its scalable architecture, the company has failed to sell to large-enterprise accounts. Management missteps in 2007 convinced numerous customers that the company was going out of business or pulling out of the U.S. market.

CP Secure needs to improve its operations and management to move to the next level, or sell its core technology.

- The USG product is still maturing and is missing numerous enterprise functions. Reporting is basic, and URL reporting must be done in the Websense console. USG can only report on the Websense update status. There are no authentication options for policy enforcement or use-based reporting. There is no central console for managing multiple appliances. SSL decryption is binary, not URL-category-based. There are no application control features.
- Malware detection is limited to signature-based scanning on inbound traffic, and only Kaspersky signatures are supported. It does not scan outbound traffic and has no ability to spot malware phone-home-type activity.
- Service and support are reportedly uneven. Customers with dedicated support engineers typically find they are knowledgeable and helpful; however, customers without them often find it difficult to get issues resolved.

Cymphonix

Strengths

- Cymphonix was started in 2004 with its first product focused on bandwidth-shaping technology. The customer base is mostly U.S. small to midsize government and education organizations.
- Network Composer is an appliance-based product that can be used as an in-line transparent bridge or proxy. The biggest competitive advantage of the Network Composer is its granular bandwidth-shaping policy options, which includes an extensive list (660) of applications that can be dynamically shaped and prioritized, in addition to content and group-level, rate-shaping policy options.
- 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 quick 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.
- URL filtering is provided through a combination of an internally maintained and/or third-party licensed database. Education customers appreciate Anonymous Proxy Guard, which provides multiple techniques to detect the use of anonymous proxies to evade URL filtering.
- Malware filtering is provided by signature-based detection from Sunbelt, software and open-source Clam AntiVirus. The product includes an ActiveX Spyware removal tool for remote client cleanup of known spyware infections.
- Application control includes 148 protocol-based application signatures.
- Cymphonix is a good fit for SMBs looking for a single SWG with advanced bandwidth management capabilities at a reasonable price.

Cautions

- Cymphonix is one of the smallest vendors in this analysis and has little market share or brand recognition. It is primarily focused on North American businesses.

- Malware detection is primarily limited to signatures from second-tier, anti-malware providers and only in HTTP traffic. There is no ability to strip malicious code in infected Web pages, just blocks. It cannot manage evasive applications, such as Skype.
- There is no centralized reporting/management interface for managing clusters or geographically dispersed gateways.
- There are no DLP capabilities or related e-mail protection products.
- There is no support for ICAP or WCCP.

FaceTime Communications

Strengths

- FaceTime Communications started in the IM security market and has branched out into the broader SWG market. It is a midsize company in this market. The company's installed base includes a significant number of large enterprise businesses, including many financial institutions, which were the primary market for IM solutions. The majority of clients are in North America.
- In 2007, FaceTime integrated previously separate edge and manager server roles into a single appliance in its Unified Security Gateway (USG) product. USG is primarily an in-line solution that proxies IM applications. A full HTTP proxy version is due in late 2008.
- FaceTime acquired XBlock Systems in 2005 with the X-Cleaner product and still relies on this research facility for its primary malware-filtering database. USG uses primarily a signature-based technique, along with some behavior-based detection techniques. Reporting on inbound and outbound threats includes the specific detailed information on the malware (for example, name, threat rating and more) and links to FaceTime's Web-based reference sites. The solution also boasts an auto remediate tool for remotely cleaning infections on the endpoint. FaceTime scans all traffic for malware, not just Port 80.
- FaceTime has the deepest visibility controls for Web 2.0 and Internet applications, including IM, P2P, anonymizers, IP television, gaming software, multimedia, remote administration tools, virtual worlds, VoIP, Web-based IM and Web conferencing. FaceTime can block or allow more than 23,000 Facebook applications and all major IM and P2P networks by name or categorization — many at the network protocol layer. FaceTime is one of the few vendors to offer full Skype control and management. A useful FaceTime utility is the RT Monitor discovery tool, which can help identify potentially malicious or unwanted applications that are on the network.
- Optional URL lists include Secure Computing's SmartFilter or Websense. FaceTime's URL-filtering policy is average with some advanced features, such as a coaching option for soft blocking.
- FaceTime GEM, a separate management module, provides a centralized management and reporting interface for multiple geographically dispersed USGs. In local clusters, multiple USGs can be clustered to share a database, which then allows for a shared repository of configuration and reporting.
- FaceTime offers good DLP and archiving capabilities for IM traffic, and will be expanding this to include other HTML traffic types, such as Web mail and blog postings by 2009.

- FaceTime is an outstanding choice for organizations looking for fine-grained Web communication application controls.

Cautions

- FaceTime is clearly in the middle of evolving from its IM-centric legacy to become a broader SWG solution, and it shows in the management interface, reporting and the lack of advanced features.
- USG is not a proxy server and cannot see SSL traffic.
- FaceTime's management interface is not very task-based or intuitive, and betrays growth by feature rather than a ground-up architecture designed for its current role. For example, setting a policy for P2P is different from setting a policy for IM. Policy development involves too many tabs and not enough reusable policy elements to simplify administration. Once the policy is complete, there is no clean summary page for auditing or troubleshooting.
- Log information is very granular; however, there is no graphical reporting on box. Detailed reports require exporting log files to a separate box and relying on SmartFilter reporter (which comes free with a SmartFilter license) or a third-party reporting tool, such as Crystal Reports. On-box reporting is too CPU-intensive and can only be scheduled for late-night job runs when the machine is less loaded. These on-box reports are table-based and not very business friendly or graphical.
- When the industry standard antivirus vendors are all struggling to keep up with the rapidly growing volume of threats, it will be difficult for smaller in-house research labs to go it alone. FaceTime would benefit from the addition of more-optional, third-party anti-malware signature engines.
- URL filtering would benefit from more-advanced features, such as bandwidth and time-based controls.

Finjan

Strengths

- Finjan is a dedicated SWG provider with strong zero-day security technology in its proxy-based appliance Vital Security product line. The company has a respectable market share with a broad mix of customers in EMEA and the U.S., including numerous large enterprises.
- Finjan's primary differentiation is its real-time code analysis technology, which scans a broad array of Web programming languages (for example, HTML, JavaScript, VBScript and Java) for malicious intent. Although several other vendors have started to emulate this technique, Finjan has several core patents as well as deeper and broader techniques for catching more-obscure and complex malware. Finjan also provides granular policy controls to neuter potential harmful dynamic code actions. Units come preconfigured with an extensive range of security policies. More-traditional, signature-based scanning is provided via optional McAfee, Sophos or Kaspersky licenses.
- URL filtering is offered via a license of IBM or Websense URL databases.
- The Web GUI has a clean look with a customizable dashboard. Policy creation is aided by reusable policy elements, such as actions and warning. Advanced features, such as policy audit logs, coaching soft block options, transaction tracking numbers that enable

rapid drill down into event details for troubleshooting, and easy directory integration/authentication options, demonstrate product maturity.

- Application controls include numerous potentially unwanted applications (IM and P2P) by name or category.
- Large enterprises will likely rely on the new Finjan reporting server software for long-term storage and consolidated reporting and dashboard data. The reporting server provides a flexible custom report facility similar to Crystal Reports in design. The appliance can be set to export data to the reporting server on a periodic basis.
- Vital Security offers optional SSL decryption, and supports ICAP and WCCP deployments.
- Finjan is an excellent solution for companies looking for zero-day protection from Web threats.

Cautions

- Finjan is not a strong brand and has little presence in the Asia/Pacific region.
- Finjan's legal battles to defend its code-scanning technology may consume excessive management and financial resources.
- On-box reporting is basic. Larger enterprises that require long-term storage and consolidated reporting will find the on-box reporting limited and will likely rely on the new Finjan reporting server software that requires Windows and Structured Query Language (SQL) database licenses and hardware.
- Application control is weak. Only a few applications are named and policy is binary (block or allow-only). Some applications, such as Skype, require a technical brief and network adjustments to implement.
- The management console is only in English.
- Finjan has no related products or technical investments, such as DLP or e-mail, to draw on. More partnering in these areas would be beneficial.

IronPort Systems

Strengths

- IronPort Systems was acquired by Cisco in 2007; however, Cisco is keeping IronPort an independent operating company, with the exception of administration functions and the integration of IronPort's products into its sales channel, although IronPort maintains its own sales and support organization. Cisco/IronPort is a leader in the e-mail boundary security market and enjoys rapid growth in the very large enterprise market. Cisco/IronPort has extensive development support resources.
- The S-Series proxy appliance products were purpose-built for the emerging SWG market in 2007 and have been architected to offer parallel scanning capabilities across multiple signature databases. The products support signature databases from Webroot and McAfee.

- The S-Series also has a unique spanning port network interface card for out-of-band traffic analysis to detect evasive outbound phone-home traffic or application traffic, such as Skype.
- Cisco/IronPort's URL categorization engine (which it licenses from an established URL filtering vendor) is augmented with IronPort's own URL reputation data from its SenderBase reputation service.
- The S-Series also offers application control using application signatures to identify and block/allow a large collection of Web-based applications, including Skype and popular IM applications.
- The S-Series appliances have garnered strong "mind share" in the market and frequently appear on Gartner clients' shortlists.
- Cisco/IronPort is a strong shortlist inclusion for enterprise customers.

Cautions

- The S-Series has a strong foundational design; however, product immaturity is evident in advanced features.
- Reporting is a weak spot for Cisco/IronPort's S-Series. 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.
- Centralized management for the S-Series appliances is weak. Although Cisco/IronPort's M-Series management appliance can synchronize policy and configuration updates across multiple devices, fine-grained, role-based and hierarchical access (tiered administration) is lacking. Cisco/IronPort has plans to enhance its centralized policy and device management system in 4Q08.
- The range of protocols that the S-Series can proxy is limited. It can proxy HTTP and HTTP/S traffic, but it lacks the ability to natively proxy FTP, IM and streaming media protocols.
- The S-Series is one of the more expensive SWG appliances in the market, and Cisco charges extra for the SenderBase Web reputation filter.
- The S-Series lacks support for the ICAP protocol, so it lacks a standardized interface for handing off content to data leakage analyzers and other content analyzers.

Marshal

Strengths

- Marshal originally focused on the e-mail security boundary market, and it was an early entrant in the SWG market. The company has a small market share and is growing at approximately the market rate. Its customer base is primarily in the global SMB market.
- The full-featured management interface is .NET-based, MMC-type consoles that provide a centralized, real-time view of activity across multiple servers or easy drill-down views into specific server activity.

- Marshal has numerous reusable policy elements and is able to provide excellent policy summary information for compliance reporting and troubleshooting. Policies support Boolean operators, dictionaries, weights, locations parameters and other powerful policy constructs.
- The URL filtering can support dynamic on-the-fly URL categorization and traditional database filters, including Marshal's own Filter List or Secure Computing's SmartFilter. Both can be used simultaneously. The URL filtering also supports a custom, file-based filter that can be used for a custom-filtering policy.
- Malware protection is provided by integrating signature-based scan engines. Marshal can support up to seven scanners simultaneously, although each additional scanner consumes more resources and will increase latency if server capacity is constrained.
- DLP is good compared with other products in this market. WebMarshal can detect, unpack and scan a large range of files and includes numerous dictionaries (such as for profanity, resumes and confidential information). Regulatory-specific dictionaries are available for SOX, GLBA, PCI and the Health Insurance Portability and Accountability Act) and structured number formats (for example, social security numbers, stock and bond identifiers, and credit card numbers).
- Marshal is a good fit for existing Marshal e-mail customers and a good shortlist addition for SMBs.

Cautions

- Marshal's biggest challenge is improving its North American market and mind share.
- The management interface, although quite complete, is not easy to use, especially for nontechnical users. It is in English only, has a mixed look and feel, and overuses pop-up windows.
- Although Marshal's e-mail management interface has the same look and feel as the SWG, they are distinct interfaces. Although they can share policy elements or directories, they do so by importing rather than referencing, degrading some of the value of a unified vendor for Web and e-mail.
- The dashboard data is not hyperlinked to drill-down reports. Administrators have to switch to the reporting console to see drill-down information. Reports are table-based and should be more graphical. Creating ad hoc reports is not supported, and reports cannot be scheduled for distribution. Marshal is planning on releasing a new reporting interface in 4Q08.
- Marshal only offers a software-based proxy platform. It does not offer any other deployment options.
- Malware detection is primarily limited to signatures and only in HTTP/S traffic. The proxy cannot isolate or clean infected machines, and there is no ability to strip malicious code in infected Web pages. It can only block them.
- The management dashboard shows outbound malware traffic; however, detail is limited. Administrators must turn to the reporting engine to find action-oriented detail.
- Bandwidth rate shaping is not available but is due in the next version.

- Application control is limited to some IM and streaming protocols, although it identifies these applications by network signature.

McAfee

Strengths

- McAfee is a stalwart of the anti-malware market and is increasing its attention on the SWG space. It launched v.5 of its Web security management interface in May 2008.
- McAfee offers Web security in a combined e-mail and Web security gateway appliance or as a stand-alone Web security appliance. For high-volume customers, it recently launched a blade server appliance version. These products can be explicit proxies or bridge mode installations.
- With the launch of v.5 software in May 2008, McAfee finally moved to Web GUI from Java. E-mail options are managed in the same interface. The reporting and policy interface is significantly improved, and installation is also improved with a wizard-like installation process.
- DLP is provided by keyword blocking of HTTP posts (including blocking search string keywords). The Web product shares keyword dictionaries and number formats with an e-mail-enabling common policy across both channels.
- McAfee's primary URL filtering is the ability to create a manual URL list. Most customers will benefit from the optional Secure Computing URL database. McAfee also offers URL reputation information from SiteAdvisor.
- McAfee's SWG is a basic offering that will appeal primarily to dedicated McAfee SMBs that favor suites.

Cautions

- McAfee's biggest challenge in the enterprise is offering buyers a suite that provides sufficient defenses in depth. Malware detection is provided by the same McAfee signatures as for e-mail and end nodes. Zero-day threat detection is limited.
- Surprisingly for a malware company, outbound phone-home malware traffic detection is buried in reports rather than in the home page dashboard and is limited to traffic to known malware sites rather than real-time protocol inspection. The proxy cannot isolate or clean infected machines, and there is no ability to strip malicious code in infected Web pages. The proxy can only block malicious code.
- Significantly, McAfee lacks scalability features for globally distributed organizations, such as centralized configuration and reporting for multiple servers and native, high-availability load balancing (the exception is the Blade server version, which does include failover and load balancing). Current clustering provides a master-slave, load-sharing scenario; however, the master becomes a single point of failure, and management features are sometimes not scalable. For example, group policy requires administrators to know the directory query string rather than a drop-down list of available groups, and block pages are tied to specific policy rather than reusable policy objects. Advanced reporting features, such as distributing customized reports and report distribution to a directory, are lacking.

- The v.5 management interface will not integrate into McAfee's centralized management console, ePolicy Orchestrator (ePO) until 4Q08. ePO integration will help solve some of the global management issues.
- There is little protocol-based application control, and McAfee cannot manage evasive applications, such as Skype.
- Although the management interface works on e-mail and the Web (and the policy can reuse dictionaries), specific policies are applied to e-mail or HTTP but not both at same time.

MessageLabs

Strengths

- MessageLabs, the largest dedicated SaaS secure e-mail gateway vendor, launched its own SWG service in 2007.
- Its Web GUI is simple and easy to use. It has the same look and feel as its e-mail interface.
- Dashboard data and summary data are kept for 12 months; however, detailed data is kept for only 30 days, unless operators export this data to a SQL database or negotiate longer storage terms from MessageLabs.
- Caching popular sites and adding gzip compression are used to accelerate Web site delivery and minimize latency.
- Malware is filtered using simultaneous McAfee and F-Secure antivirus scanners, as well as MessageLabs' Skeptic, a heuristic analysis engine that shares threat intelligence gleaned from malicious e-mail traffic.
- The URL database is licensed from Websense, and MessageLabs augments it when it discovers URLs that have been identified as containing malware.
- MessageLabs customers give it high marks for service and support. The service offers strong virus, latency, uptime and support service-level agreements, including a 100% uptime guarantee.
- 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. The company's solutions are recommended for existing MessageLabs e-mail security clients.

Cautions

- The dashboard and reporting features are basic. Detailed reports are only table-based raw data in a comma-separated values (CSV) format. There are few parameters to adjust to create custom reports and no ability to save or schedule reports. Advanced reports would require exporting CSV data to a third-party reporting engine. MessageLabs is planning significant enhancements to its reporting engine in 1Q09.
- Some customers reported that the management portal can be unresponsive during peak load periods, and it can take up to several hours for policy changes (such as unblocking a site) to propagate to all data centers. However, MessageLabs has been aggressively addressing infrastructure issues, and we expect these to be resolved.

- MessageLabs' proxy supports HTTP and HTTP/S but does not provide native support for FTP or other protocols. Outbound malware can evade detection by port/protocol hopping.
- Application control is limited and based on URL destination rather than network/protocol signatures.
- 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. The URL policy would benefit from advanced options, such as self-authorization, coaching and bandwidth limitations.
- More options for enabling PC redirection to the closest MessageLabs data center would be better. MessageLabs provides a Squid-based proxy software and a Microsoft ISA plug-in. Laptop users have to be redirect to the corporate LAN, or have a hard-coded (PAC files) proxy setting in Internet Explorer.
- Reporting details are only stored for 30 days, while summary data is stored for 12 months for trend analysis. Customers seeking longer-term storage must export report data to their own infrastructure or purchase MessageLabs' Enhanced Data Retention service for longer-term storage.
- Like other SaaS services, MessageLabs' pricing is expensive relative to on-premises SWG offerings for those that do not have multiple offices.

Mi5 Networks

Strengths

- Although Mi5 Networks is one of the youngest vendors in this analysis, its Webgate appliances are maturing rapidly, and the company is getting high levels of interest in large security-conscious enterprise accounts.
- Mi5 has one of the best management interfaces in the market. Policy creation is done on single-page view with intelligent options based on previous selections. The dashboard and reporting interface is also excellent. Most notable is the reporting emphasis on outbound traffic that indicates the presence of malware and the easy access to more detail. Dashboard data is hyperlinked to relevant reports, which include more hyperlinked drill-down data. Reports include severity indicators to prioritize remediation, a quick link access to remediation options and granular details (for example, geolocation data, search terms, file names/types and cross-referencing to greatly aid forensic analysis).
- Mi5 provides a centralized server for configuration and consolidated reporting, and long-term storage of log data.
- Mi5 is an in-line or bypass traffic scanner, which enables bidirectional malware scanning of most ports and protocols (SSL is due in 4Q08) 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.
- The Webgate appliance uses Sophos and Sunbelt Software scan engines and remediation tools, along with its own network behavior detection techniques, which include Botnet and malware phone-home detection.

- Protocol-level application control was added since last year 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. Mi5 plans to add Secure Computing's URL database later in 2008.
- Mi5 is an excellent fit for security-conscious organizations that want inbound protection and endpoint infection detection without replacing or redesigning the network path.

Cautions

- Mi5 faces competition from larger established vendors, and it still needs to build a strong channel organization to gain visibility and brand awareness in the enterprise market.
- The company must be careful to manage its growth during the critical transition from a startup to an operating company and ensure that service levels do not slip.
- The company has only a limited history of producing fast, accurate signatures or zero-day detection techniques. More options for malware engines and URL filtering databases would be an improvement.
- URL-filtering capabilities could be improved with coaching or self-authorization, and more time and bandwidth options.
- Mi5 has no related products or technical investments, such as DLP or e-mail to draw on. More partnering in these areas would be beneficial.
- SSL decryption is missing.

ScanSafe

Strengths

- ScanSafe was the first company to launch "in the cloud" SWG services, including URL filtering, malware scanning and application control. It continues to expand rapidly with a broad mix of enterprise customers primarily across North America and EMEA. Its early innovation in the SaaS model was a large part of its visionary status in last year's Magic Quadrant. ScanSafe moved into the Challengers quadrant in this year's Magic Quadrant primarily to reflect the growing acceptance of SaaS services and increasing competition, rather than any degradation in its service.
- Its 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. Advanced reports can be modified and scheduled for distribution in numerous file formats.
- ScanSafe offers a real-time classification service for unknown URL addresses. It attempts to classify the unknown URLs into a small set of categories (for example, pornography, gambling and a few others).
- ScanSafe's channel partners include AT&T and Sprint — both of which extend ScanSafe's reach beyond North America to EMEA and the Asia/Pacific region. Google is another major ScanSafe channel partner with an international reach.

- URL filtering is enhanced with some advanced functionality, such as bandwidth and time-based quotas.
- 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.
- The service includes a "search ahead" feature that decorates search engines with URL classification.
- ScanSafe's service provides application control to block a wide range of P2P applications.
- ScanSafe's service is an excellent alternative to customer premises SWG solutions, particularly for organizations with a high percentage of mobile workers and/or numerous remote offices.

Cautions

- 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.
- ScanSafe has a straightforward pricing model (per user/per month, no separate support/maintenance fees), but it can be expensive relative to other SWG offerings, especially those that do not have multiple offices. In addition to its Web-filtering/malware-scanning bundle, ScanSafe charges an extra fee for its Anywhere+ service (for roaming employees) and its IM Control service.
- Reporting details are only stored for 45 days, while summary data is stored for 12 months for trend analysis. Customers seeking longer-term storage must export report data to their own infrastructure or negotiate for longer-term storage.
- Scheduled reports are much better than live reports, which are basically filtered log views. Scheduled reports cannot be run in real time. They are batch jobs that run when the service is less taxed.
- Application control is limited and URL-based, rather than a network signature protocol.

Secure Computing

Strengths

- Secure Computing offers a broad collection of network devices, including firewalls, secure e-mail and Web gateways. The company is increasingly integrating these products with a common management and reporting framework. Its SmartFilter URL database is widely deployed on its mature line of SWG, on its Secure Firewall and in numerous competitive solutions.
- In June 2008, Secure Computing announced a SaaS Web security solution that provides Web reputation filtering and anti-malware protection to add to its traditional appliance-based offerings.

- The Web-based management interface is well-organized and easy to navigate and deploy for technical users, and offers granular role-based administration. It can have a designated central appliance to manage multiple slave boxes in a single cluster.
- Secure Computing has strong on-box malware protection, including 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 SmartFilter URL categorization engine is augmented with its own TrustedSource URL reputation data.
- Secure Computing offers traditional signature-based scanning via optional licenses from McAfee, Sophos or Secure Computing's own signatures (which are based on the Avira signature engine and is supplemented with Secure Computing's signatures).
- Secure Web includes several advanced URL-filtering policy features, such as progressive lockout, which senses multiple bad URL requests and locks out Internet access. Bandwidth quotas, reusable policy elements, coaching and soft blocking are also available.
- Secure Computing has a new reporting application that offers tiered administration and ships with MySQL or integrates with an Oracle database.
- The company has a strong native DLP capability, and management integration with e-mail security is a plus.
- Secure Computing is a strong choice for any enterprise.

Cautions

- Secure Computing's code analysis, zero-day malware detection technique is subject to a patent infringement legal action from Finjan. In March 2008, a U.S. District Court found that Secure Computing infringed on some Finjan patents. Secure Computing is appealing the decision and has also filed a counter claim that Finjan infringed on its patents. Although Secure Computing says that it is prepared with a full set of contingency plans that will not impact customers or sales, the company may become distracted defending itself.
- Secure Computing has a sizable revenue stream from a broad array of products; however, it lacks significant brand recognition. In 2008, Secure Computing renamed several key product lines in an effort to strengthen its core brand and defocus acquired brand names.
- Some Secure Web (formerly Webwasher) customers have commented that manageability features are still maturing and that product documentation is lacking. Some commands could only be executed via a command line interface, although Secure has plans to enhance its GUI.
- Consolidated and advanced reporting functions require the Web reporting product.
- The Web Reporter is a separate application with a different look and feel from the management interface, and it does not have hyperlinks from the dashboard on appliance logs/reports. 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 premium version requires an SQL or Oracle database.

- Secure Computing won several large SWG deals in 2007 and 2008, but it still needs to demonstrate in production deployments that its Secure Web appliances meet the scalability and performance demands of very large data centers.

Trend Micro

Strengths

- Trend Micro is one of the few antivirus vendors that has a long history of focus on the Web gateway market. As a result, it has a respectable market share with global enterprises.
- The InterScan Web Security Suite (IWSS) family of products offers numerous product platform options (for example, appliance, Crossbeam integration, Linux, Windows, Solaris, virtual appliance and services) 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.
- 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 local performance and consolidate.
- Malware detection is provided by Trend Micro's signature database. Trend Micro recently launched an in-the-cloud signature database to improve signature freshness and speed. Trend Micro also benefits from its Web Reputation service. Trend Micro is the only vendor to provide Web and e-mail reputation services, as well as extensive malware research capacity.
- Trend Micro's damage cleanup service can provide remote client remediation for known threats.
- InterScan Web Security 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.
- Its management dashboard includes active real-time graphs and hyperlinks to monthly or daily reports. Summary reports are easy to access in tabs across the top.
- Application control includes some P2P and IM traffic types that are detected by network signatures.
- Trend Micro is a respected shortlist inclusion for any enterprise.

Cautions

- 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. Zero-day threat detection is limited to local heuristics.
- The company has a bewildering array of SWG products, and features and options are not consistent across the product family.

- Trend Micro's appliance solutions (with the exception of Crossbeam) have difficulty scaling to large-enterprise needs. IWSS lacks internal load-balancing to improve native clustering.
- The management interface is not very intuitive to use with excessive use of radio buttons and click boxes, and it is not recommended for nontechnical people. The reporting capability is disappointing. It lacks drill-down hyperlinks, customization or graphing options. The next version (due in 3Q08) plans to support Crystal Reports-type capabilities and performance improvements.
- A major missing component for scalability is a centralized manager for configuration and reporting. Trend Micro's Control Manager can monitor the IWSS products and provide high-level summary reports and managed signature distribution, but detailed configuration must occur in the IWSS Web GUI. It is possible to do this by pointing multiple hosts to one instance and have that act as a centralized manager.
- Application control is limited to binary blocking of some P2P and IM plus URL categorization blocking.
- Surprising for a malware company, the outbound malware detection report, which indicates the presences of dangerous malware inside the network, is buried in a report rather than displayed as a real-time dashboard element. This is especially frustrating when Trend Micro offers a remote damage cleanup service.
- Trend Micro's URL policy options are limited. Time parameters are not very customizable and there are no bandwidth rate shaping options, just quotas.
- Advanced features, such as transparent authentication, SSL decryption options and DLP, are notably missing.

Webroot Software

Strengths

- Webroot Software is better known for its Endpoint spyware protection solutions; however, with the acquisition of Email Systems (November 2007), the company is offering e-mail security and SWG services via a SaaS offering.
- Malware protection is provided by Webroot and a Sophos malware signature database. Webroot has had considerable experience and a strong track record in the area of Web-born malware detection, which has been the company's focus since its inception in 1997.
- Webroot operates three continental data centers (in the Asia/Pacific region, the U.K. and the U.S.). HTTP traffic is redirected to these proxies via a local proxy or firewall settings, a client proxy setting or a client software agent.
- 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.
- 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. The URL filtering provides an anonymous proxy detection capability.

- The service uses compression and HTTP translation to accelerate content from data center to end users to minimize latency.
- The service includes search results (Google, Yahoo, MSN Live Search and Ask.com) decorated with security warnings and URL categorization icons. Log data includes the search term query string and has a link to the results, which is a good feature to help understand user intent.
- Webroot is a good shortlist inclusion for SMBs looking for service provider options.

Cautions

- Although Webroot has made considerable investments in this market in terms of acquisitions, staffing and planning, it is relatively untested in this market. It has virtually no experience providing a SaaS-type service, and it acquired only a small staff with Email Systems. The company is competing against significantly better-capitalized and higher-profile companies in an increasingly crowded SWG SaaS market. Execution throughout the next 12 months will be critical to see whether the company can make the transition.
- Malware detection is limited to HTTP traffic types.
- Reporting is basic, with limited advanced functions. There is no ability to create ad hoc reports, save report settings or schedule a report for distribution. Blocked pages and allowed pages are not reported in a single, end-user summary report. Reports do not offer multiple chart types — only bar charts and tables. By default, the service only stores four weeks of log data, and there is no way to automate the export of data, which makes it difficult to create long-term trend reports. However, it is possible to manually create a CSV file and export it.
- Outbound threats are displayed in log views only. No reports or real-time dashboard views of this data are provided. There is no automated capability to isolate an infected PC.
- URL-filtering options are basic. There are no bandwidth or quota options. The service only offers four block pages, making it difficult to create regional block pages for global companies. There is no user-readable policy summary for auditing or troubleshooting.
- Application control is limited to blocking URLs of registration servers, and the solution offers limited DLP capability (blocking file types); however, the e-mail service does, and Webroot has plans for converging this functionality.
- Reporting details are only stored for 30 days, while summary data is stored for 12 months for trend analysis. Customers seeking longer-term storage must export report data to their own infrastructure or negotiate for longer-term storage.
- Webroot has competitive pricing for a SaaS service; however, like other SaaS services, pricing can be expensive relative to on-premises SWG offerings for those that do not have multiple offices.

Websense

Strengths

- Websense is aggressively expanding its focus from the traditional URL-filtering market to e-mail boundary security and DLP markets. At the same time, Websense is transitioning its core products to compete in the more holistic SWG market.
- With the acquisition of SurfControl, Websense is the largest dedicated vendor in the SWG market, with almost 30% of the market share; however, there is some overlap with other vendors' market share because a large percentage of other SWGs' platforms license Websense's URL signatures. The company has a solid North American and EMEA presence in companies of all sizes and a strong distribution channel.
- The company offers the widest range of product and delivery options. 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. As part of the SurfControl acquisition, Websense also acquired a SaaS solution for Web and e-mail filtering that competes favorably with the other SaaS solutions. Websense is planning to provide integrated management, which would enable a hybrid solution.
- Websense's management console is one of the best in the market. Navigation is task-based, and reporting 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. Dashboard information is customizable and includes hyperlink drill downs into more-detailed reporting data. Policy can be developed in a single pane without annoying pop-up windows. Policy parameters are rich and workflow is logical.
- As expected, URL policy parameters are extensive and include options such as bandwidth, time restrictions and quotas. Optional category-based SSL traffic decryption is included to filter encrypted Web traffic.
- Application Control includes more than 115 applications, such as IM and chat, streaming media, P2P file sharing, mail and collaboration. Some applications can be filtered on network signatures, but most are URL-based.
- The new Web Security Gateway includes malware filtering that goes beyond Websense's traditional URL security risk classifications. New techniques include signature analysis, vulnerability shielding and sandboxing of suspicious code.
- Websense offers strong outbound data controls for DLP as an additional module that enables granular data-based policy and reporting. Data detection techniques are complete, and the product includes several predefined dictionaries and policies.
- Websense is a good shortlist inclusion for any size company. It failed to make the Leaders quadrant because the Web Security Gateway with real-time malware detection capability is new and relatively untested in the enterprise market.

Cautions

- The major challenge for Websense will continue to be digesting its two major acquisitions of 2007, PortAuthority (see "Websense to Enter CMF Market With PortAuthority Acquisition") and SurfControl (see "Acquisition by Websense Will Consolidate URL Filtering Market"). Although there are significant benefits to integrating

e-mail and DLP into the Web gateway, the market for these converged products is in its early stages, and there is considerable rationalization and integration before Websense customers will be able to recognize these benefits.

- Although Websense recently purged its product portfolio, it still has a large array of products with diverse features and numerous optional modules. Buyers must be careful to understand which marketed benefits apply to products under consideration and ensure that quoted prices include expected features. For example, all DLP capabilities in the SWG are reliant on integration with the Data Security Suite (which is not included) and Websense Security Filtering, which blocks sites classified as a security risk and is an add-on module to Websense Enterprise Edition.
- Websense's Web Security Gateway proxy solution is new in the market. (The Crossbeam WebBlazer product was the first product to include the Inktomi proxy technology in 4Q06; however, it has not seen broad deployment yet.) The Web Security Gateway can only proxy HTTP/S traffic. Inbound and outbound malware can evade detection by port/protocol hopping. Websense malware detection techniques are new and relatively unproven on the individual enterprise gateway, although they have been used in Websense's data center threat seeker network.
- When the industry standard antivirus vendors are all struggling to keep up with the rapidly growing volume of threats, it will be difficult for in-house research labs to go it alone. Websense would benefit from the addition of more optional, third-party anti-malware signature engines.
- Some Websense customers have reported that first-level support is lacking. (However, those that paid for premium-level support were satisfied.)
- Websense is generally more expensive than its counterparts for similar functionality and continues to be the only URL-filtering vendor to charge extra for URLs of sites that are security risks.

RECOMMENDED READING

"A Buyer's Guide to Secure Web Gateways"

"IronPort Buy Will Make Cisco a Major E-Mail Security Player"

"Acquisition by Websense Will Consolidate URL Filtering Market"

"Websense to Enter CMF Market With PortAuthority Acquisition"

"Introducing the Secure Web Gateway"

"Pros and Cons of SaaS Secure Web Gateway Solutions"

"The Growing Web Threat"

"NetCache Buy by Blue Coat Would Narrow Proxy Cache Market"

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

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
GUI	graphical user interface
HTTP/S	HTTP over SSL
ICAP	Internet Content Adaptation Protocol
IM	instant messaging
IP	Internet Protocol
MMC	Microsoft management console
OS	operating system
PAC	proxy auto-configuration
P2P	peer-to-peer
PCI	Payment Card Industry
SaaS	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
UTM	unified threat management
VoIP	voice over IP
WCCP	Web Cache Communication Protocol

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.

Evaluation Criteria Definitions

Ability to Execute

Product/Service: Core goods and services offered by the vendor that compete in/serve the defined market. This includes current product/service capabilities, quality, feature sets, skills, etc., 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 of the individual business unit to continue investing in the product, to continue offering the product and to advance the state of the art within the organization's portfolio of products.

Sales Execution/Pricing: The vendor's capabilities in all pre-sales activities and the structure that supports them. This includes deal management, pricing and negotiation, pre-sales 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 in order 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, 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, etc.

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

Completeness of Vision

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

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

Sales Strategy: The strategy for selling product 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 set 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 verticals.

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.

REGIONAL HEADQUARTERS

Corporate Headquarters

56 Top Gallant Road
Stamford, CT 06902-7700
U.S.A.
+1 203 964 0096

European Headquarters

Tamesis
The Glanty
Egham
Surrey, TW20 9AW
UNITED KINGDOM
+44 1784 431611

Asia/Pacific Headquarters

Gartner Australasia Pty. Ltd.
Level 9, 141 Walker Street
North Sydney
New South Wales 2060
AUSTRALIA
+61 2 9459 4600

Japan Headquarters

Gartner Japan Ltd.
Aobadai Hills, 6F
7-7, Aobadai, 4-chome
Meguro-ku, Tokyo 153-0042
JAPAN
+81 3 3481 3670

Latin America Headquarters

Gartner do Brazil
Av. das Nações Unidas, 12551
9º andar—World Trade Center
04578-903—São Paulo SP
BRAZIL
+55 11 3443 1509