Magic Quadrant for Secure Web Gateway

Gartner RAS Core Research Note G00212739, Lawrence Orans, Peter Firstbrook, 25 May 2011, V3RA1 05272012

The growing malware threat continues to drive the SWG market. Solutions for detecting malware vary widely in sophistication, ranging from basic signature-based to advanced heuristics-based analyses. The market is still dominated by on-premises solutions, but cloud services are growing rapidly.

WHAT YOU NEED TO KNOW

Anti-malware capabilities should be the most heavily weighted criterion when evaluating secure Web gateways (SWGs). Bidirectional protection (blocking inbound malware and analyzing outbound traffic to detect compromised endpoints) is critical. Organizations that need the most advanced security protection should evaluate solutions that use non-signature-based techniques capable of detecting targeted malware. Organizations that have more basic security requirements can consider solutions that primarily rely on signature-based malware detection.

MAGIC QUADRANT

Market Overview

The Web 2.0 phenomenon and associated malware threats continue to drive the SWG market. Large and small enterprises now understand that they need perimeter-based anti-malware protection, and many organizations seek more granular policy controls for dealing with social networking. The market has responded with a range of options that broadly fits into two categories: on-premises equipment and cloud-based services (also known as "SWG as a service"). Each category includes diverse technology options. For example, on-premises equipment can be architected as a proxy (usually deployed to inspect only Web traffic) or as an in-line solution (deployed to inspect all traffic). The emerging SWG-as-a-service market also presents several architectural options for dealing with important functions such as authentication and traffic redirection. The vendors in the Magic Quadrant represent a broad spectrum of choices in this rapidly evolving market.

After assessing the SWG solutions in today's market, Gartner makes the following observations:

- Malware detection is the key differentiator in the SWG market. Most solutions provide a "cocktail approach," which includes traditional reactive techniques such as signature-based malware analysis and detection of known bad Web destinations, along with real-time techniques for detecting new and targeted threats. Site reputation analysis and real-time code analysis that look for common malware techniques in Web code (for example, JavaScript) are the most common approaches. The depth of these techniques varies considerably among solutions.

Gartner

- Strong capabilities for detecting outbound malicious traffic are rare. The ability to detect compromised endpoints, to block their outbound communications to a malicious command-and-control center, and to generate reports are important features for combating malware.

- URL categorization is an important market differentiator and should not be regarded as a commodity service. The ability to dynamically classify URLs is an important feature due to the exploding growth of the Web. Also, language support and geographical focus remain significant differentiators.

- Application control and social media policies have become higher priorities for enterprises. There are two types of Web applications: those that can be identified by URL (for example, FarmVille) and those that use unique protocols and client applications (for example, Skype). URL-based applications can be identified and classified, allowing for easy blocking or more granular control. The ability to block or manage applications such as Skype and instant messaging (IM) requires broader port/protocol inspection and special network traffic signatures.

- Reporting and ease of management, which vary significantly among vendor solutions, remain important decision criteria for SWG buyers.

Figure 1. Magic Quadrant for Secure Web Gateway

Source: Gartner (May 2011)

- Future requirements will focus on protection and control for an ever-increasing array of mobile devices and non-PC computing platforms. Interest in data leak prevention (DLP) capabilities and the protection and management of corporate cloud-based applications (for example, salesforce.com) is growing, but remains low.

- Form factor is also an important consideration. Most of the solutions in this analysis are hardware-appliance-based. We have observed growing interest in virtual appliances. Awareness and market share of solutions delivered as a service (software as a service — SaaS) are growing rapidly, primarily in organizations that have multiple distributed gateways, large percentages of roaming workers, and organizations that are attracted to the ease of implementing SaaS.

- We continue to see very little interest in SWG and firewall integration, although all the major enterprise firewall vendors and unified threat management (UTM) vendors have started to incorporate SWG functionality.

Market Definition/Description

The SWG market includes on-premises solutions and cloud-based SWG-as-a-service offerings. In 2011, we attempted to eliminate single-purpose proxy servers and URL revenue in our market-sizing estimates to get a more accurate reflection of the pure SWG market without the weight of legacy point products. Using this analysis, we estimate that, in 2010, the SWG market reached $817 million, a growth of 17% over 2009. The five-year compound annual growth rate is approximately 15%. In 2011, we estimate that the market will grow approximately 17% to just under $1 billion. The market is still dominated by the on-premises solutions (approximately 90%), with SWG as a service representing the remainder of the market (approximately 10%). However, the SWG-as-a-service segment is the fastest-growing segment (Gartner expects that it will grow 55% in 2011).

The SWG market is rapidly evolving into a segmented market, with some solutions optimized for small and midsize businesses (SMBs) and others optimized for large enterprises. SMB solutions are optimized for ease of use and cost-effectiveness, and provide security protection against basic threats. Large-enterprise solutions provide protection against more advanced security threats, and some include the capability to detect targeted threats.

Inclusion and Exclusion Criteria

Vendors must meet these criteria to be included in this Magic Quadrant:

- The solution must include the core requirements of an SWG: URL filtering, malware protection and application control. The vendor must own the technology for at least one of these components. Other components may be licensed from an original equipment manufacturer (OEM).
- Gartner analysts have a generally favorable opinion, based on analysis, about the company's ability to compete in the market.
- SWG products that offer firewall functionality — for example, multifunction firewalls (also known as 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 (IPS) and URL filtering — into a single box. Multifunction firewalls are compelling for the SMB and branch office markets; however, in most circumstances, enterprise buyers do not consider multifunction firewalls 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.
- The solution must integrate with a directory (for example, Active Directory) so that policies may be enforced on a role basis, and so that behavior can be monitored and reported on a per-user basis (as opposed to IP addresses).
- Vendors must have at least 50 production enterprise installations.

Added

- Phantom Technologies has been added, due to its growing presence in the SMB market.
- Sangfor has been added, due to its strong market position in China.
- Actiance replaces FaceTime Communications (the company renamed itself in 2010).
- Due to improvements made to its appliance-based SWG, Sophos now meets our inclusion criteria and has been added to the Magic Quadrant.

Dropped

- CA Technologies has been dropped. It does not offer an independent SWG offering (although its CA Gateway Security solution bundles e-mail and Web security into one solution).

Other Vendors That We Considered

- St. Bernard Software acquired Red Condor in 2010 and rebranded as EdgeWave, repositioning the company with a stronger focus on security and broader delivery models, including cloud-based services. Gartner will reconsider EdgeWave for inclusion in the 2012 Magic Quadrant for Secure Web Gateway.
- Microsoft has informed Gartner that it does not plan to ship another full version release of its SWG product, the Forefront Threat Management Gateway (TMG). The product is effectively in sustaining mode, with Microsoft continuing to ship Service Pack (SP) updates; the next one, SP2, is planned for 3Q11. Microsoft will also continue to support TMG for the standard support life cycle — five years of mainstream support and five years of extended support. In the SWG category, TMG will become less competitive over time, since Microsoft's goal is not to compete head-to-head with other vendors in that space. We believe that Microsoft will repurpose TMG technologies in other products and services as part of its overall cloud strategy.
- As a next-generation firewall, Palo Alto Networks offers some SWG functionality. However, as noted above, this analysis excludes solutions that are primarily firewalls. In "Next-Generation Firewalls and Secure Web Gateways Will Not Converge Before 2015," Gartner predicts that the evolution of complex threats will drive the need for separate network firewall and Web security gateway controls for most organizations through 2015.

- The OpenDNS Enterprise cloud offering provides a DNS-based URL-filtering solution. It is popular with consumers, school districts, some SMBs and other cost-conscious organizations, but it does not have the enterprise-class reporting features to be included in this analysis (that is, it does not integrate with Active Directory). Gartner will reconsider OpenDNS for inclusion in the 2012 Magic Quadrant for Secure Web Gateway.

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 with 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: The quality of the customer experience based on input from discussions with vendor references and Gartner clients.
- 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.

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 the market understanding evaluation, 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 reflect a solid commitment of resources to achieve that vision.
- In the offering (product) strategy 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 as it crosses the gateway (in real time), as well as for the range of inspected protocols, ports and traffic types. Products that can identify infected PCs, identify the infection by name and enable prioritized remediation also 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 budgets, 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, the dynamic risk analysis

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 (May 2011)	

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 (May 2011)	

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, 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 a 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 analyzed deployment options for on-premises solutions and SWG-as-a-service offerings. For vendors that offer both deployment options (otherwise known as "hybrid"), we considered the level of integration between the two approaches (for example, the ability to manage policies from a unified console). For on-premises proxy-based solutions, we evaluated the breadth of proxy features, including protocol support, Secure Sockets Layer (SSL) termination capabilities, and interoperability with third-party antivirus and content-aware DLP scanners (for example, Internet Content Adaptation Protocol [ICAP] support). For on-premises bridge-based offerings, we evaluated the solution's capabilities for packet filtering and the features that it enables, such as bandwidth control and outbound traffic analysis of non-HTTP/S traffic (which is used for malware detection). For SWG-as-a-service offerings, we considered the options for redirecting traffic to the cloud provider (for example, virtual private network [VPN], Generic Routing Encapsulation [GRE] tunnels, proxy chaining and other approaches) and authentication options (for example, support for Security Assertion Markup Language [SAML]).

- Related investments: We gave minor credit to vendors with related investments, such as e-mail integration and native content-aware 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.

- Innovation: This criterion includes product leadership and the ability to deliver features and functions that distinguish the vendor from its competitors. Advanced features, such as the ability to perform on-box malware detection of dynamic content (for example, JavaScript code), and the ability to pinpoint compromised endpoints by analyzing outbound traffic, were rated highly.

Leaders

Leaders are high-momentum vendors (based on sales and "mind share" growth) with established track records in Web gateway security, as well as vision and business investments indicating that they are well-positioned for the future. Leaders do not necessarily offer the best products and services 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 Challengers' 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 Leaders, or they lack the corporate resources of Challengers. Expect state-of-the-art technology from Visionaries, but buyers should be wary of a strategic reliance on these vendors and should closely monitor their viability. 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 Visionaries' products. Thus, these vendors represent a slightly 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 the comprehensive features of Visionaries and the market presence or resources of Challengers. Customers that are aligned with the focus of a Niche Players vendor often find such provider offerings to be "best of need" solutions. Niche Players may also have a strong presence in a specific geographic region, but lack a worldwide presence.

Vendor Strengths and Cautions

Actiance

Actiance was called FaceTime Communications in our previous Magic Quadrants, but transferred the name and trademark to Apple for its video calling application. Actiance is a privately held company, based in California, that has branched out from its start — selling IM security to North American financial institutions — to

the broader SWG market. In 2010, the company introduced an innovative offering, Socialite, as a module in its SWG for controlling, monitoring, recording and approving corporate social networking participation. Actiance is a good candidate for organizations looking for fine-grained Web 2.0 application controls and social media monitoring tools.

Strengths

- Actiance has strong dashboard and reporting capabilities, as well as a 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. The console also offers a unique, fully customizable heat map dashboard element that enables administrators to visualize traffic and events rapidly.

- Actiance has its own malware and application research capabilities, which are combined with malware databases from GFI Software (which acquired Sunbelt Software in July 2010). Actiance's Unified Security Gateway (USG) appliance can be deployed by connecting to a Switched Port Analyzer (SPAN)/ mirror port, can be deployed in line and can also interface with proxies via ICAP. When deployed in line, the USG can proxy HTTP/S, FTP and traffic from common IM services.

- Actiance has the broadest visibility and controls for Internet applications, with more than 5,000 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, Actiance offers the strongest control for Skype. A special plug-in to Skype clients enables it to detect and block malicious URLs within Skype IMs.

- Reporting on outbound threats is one of the best in this analysis, and includes specific detailed information on the malware (for example, name, threat rating and more) and links to Actiance's Web-based reference sites, spywareguide.com and applicationsguide.com.

- Actiance offers archiving capabilities for IM traffic, social media and HTTP/S traffic (such as Web mail and blog posts). For example, policies can be enabled to control and log all outbound content for Web 2.0 sites, including blog posts and social networking sites, and also for Web mail traffic. Policy options include taking a screen shot of the Web page for which the content-aware DLP policy is triggered. The logging can also be triggered by a 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.

- The Socialite module provides specific social network feature controls, preapproved content controls (moderation), and archiving for LinkedIn, Twitter and Facebook. Socialite is available as a module for Actiance's USG or through a SaaS option.

- Multiple USG appliances can be clustered to share a database, which then allows for a shared repository of configuration and reporting for multiple, geographically dispersed USG appliances. A separate reporting module can also provide for centralized reporting for multiple USG appliances.

- Customers can choose between two URL-filtering databases. Actiance's URL-filtering policy is average, but includes some advanced features, such as a coaching option for soft blocking, custom categories and custom URL additions. Enforcing safe search on popular search engines (Bing, Google and Yahoo) is also available.

Cautions

- Actiance's biggest challenge is improving its visibility and mind share against increasingly larger and more strategic competition. Despite an early focus on this market and a decent growth rate, it has failed to achieve a significant market share. It needs to rapidly expand its channel partners and client base, because it is at risk of becoming a Niche Player in the social network controls or the financial services market.

- Actiance's licensed URL-filtering capability does not offer the ability to dynamically classify uncategorized websites. URL-filtering updates default to daily, but can be customized to update as often as required.

- Actiance's content-aware DLP capability is weak and comes at an extra cost from the base license. Its keyword-filtering capability can be used to classify pages, but there is a shortage of predefined DLP lexicons, and users have to create and fine-tune their own categorization policies.

- Actiance's log search functionality is weak, and it is difficult to search on or isolate search terms.

- Actiance relies on signature engines or known bad URLs for malware detection, and has limited on-box capability to dynamically inspect Web pages for malicious intent.

- Actiance provides Web content caching on proxies, but does not offer bandwidth quality of service (QoS) options to improve the performance of priority applications.

Barracuda Networks

Barracuda Networks offers the Barracuda Web Filter — a range of inexpensive proxy-based appliances (hardware and virtual) that leverages open-source technologies — as well as the Barracuda Web Security Flex ("Flex") product, which allows any combination of SWG-as-a-service offerings and appliances. The company enjoys high mind share in the SMB market, due to its focus on the needs of this demographic, extensive marketing and effective sales channel management. It continues to experience solid growth, and is starting to move upmarket to larger enterprises. Barracuda Web Filter appliances are candidates for organizations seeking "set and forget" functionality at a reasonable price.

Strengths

- The Barracuda Web Filter's Web graphical user interface (GUI) is basic and designed for ease of use. Deployment is simplified; all settings are on a single page with easily accessible and 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 and by in-house-developed signatures. The management console includes optional infection thresholds that can kick off alerts or launch a malware removal tool. Barracuda offers basic content-aware DLP functionality at no extra cost.

- Application controls include a fair number of IM networks, software updaters, media stores, remote desktop utilities, toolbars and Skype.

- Bandwidth quotas can be leveraged to limit resource usage per day or per week.

- 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 Flex service component (formerly "Purewire") provides a very clean and well-organized policy and reporting interface that is simple and logical. All dashboard elements 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.

- Advanced options for Flex 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. The content-aware DLP capability includes five static libraries/lexicons and SSL scanning by category.

- Redirecting traffic to the service component of the Flex offering is optionally enabled with an on-premises Barracuda Web Filter appliance that caches traffic and provides for on-premises authentication, a Microsoft Internet Security and Acceleration (ISA) 2006 plug-in, and a variety of direct connect and Active Directory configurations. The Flex 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 some enterprise-class capabilities for management and reporting. 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. Although the solution saves searched keywords in the log, it is difficult to search the logs for this information or to report on it. It does not offer real-time dynamic classification of URLs.

- Barracuda uses open-source databases for URL and antivirus filtering (Sourcefire/Clam AntiVirus), supplemented with Barracuda's own research labs. However, Barracuda Labs is still relatively small. It does not offer any other third-party anti-malware engines. Real-time analysis of Web threats is limited in the appliance-based solution.

- The Barracuda Flex offering still needs to mature to compete against the more established 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 inspection methods to detect outbound threats, 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. Log data can only be stored in the cloud, not on the local devices. Barracuda does not offer a zero-client footprint option with transparent authentication. The Flex service only offers an uptime service-level agreement (SLA). It does not support SAML authentication integration. The service does not have a global footprint and currently only has data centers in the U.S., the U.K. and Germany.

Blue Coat Systems

While Blue Coat Systems remains the overwhelming installed base leader in the enterprise proxy market, it faces a number of challenges. It was late with SWG as a service (launched in April 2011). In January 2011, it introduced an appliance, ProxyOne, targeted at SMBs, although Blue Coat must demonstrate that it can build an SMB-focused value-added reseller (VAR) partner channel that is capable of distributing the product. Blue Coat has a new CEO (as of August 2010). With its Mach5 products, Blue Coat also competes in the WAN optimization controller market. Blue Coat's ProxySG is a very good candidate for most enterprise customers. SMBs that are willing to take the risk on a new appliance can now consider the new ProxyOne.

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, a command line interface, 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 (Blue Coat WebFilter), and four antivirus engines on its ProxyAV platforms — the most options of any vendor in the market.
- Content-aware DLP support is available via an appliance based on technology licensed from a third party. The appliance interfaces with the ProxySG via ICAP.
- The Blue Coat Reporter provides flexible capabilities to create custom reports, and enables multiple ProxySG products to report log information back to an aggregated log database. Log search functionality is very good and easily allows searching for specific search terms.
- In addition to signature scanning, ProxySG uses a 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). ProxyAV has limited active code analysis to detect unknown malware.
- Blue Coat ProxySG appliances proxy (that is, they fully terminate and can apply policy to) popular IM services, P2P applications, streaming media protocols, FTP, Telnet, DNS and SOCKS v.4/v.5. Many competing solutions can only proxy HTTP/S traffic.
- Bandwidth management policies can be specified per protocol (for example, streaming media) and can be applied to users or groups. The ProxySG also optimizes bandwidth by stream splitting and caching.
- Blue Coat WebFilter is often one of the least expensive URL-filtering options. Its 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 content-aware 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 on Windows platforms.
- Blue Coat sends uncategorized URLs to its cloud-based WebPulse service for dynamic categorization and malware analysis. WebPulse's dynamic classification capabilities categorize all URLs, not just those that match a subset of inappropriate URL categories. Some malware may be detected in real time, whereas other malware checks are done in the background and the results are stored in the WebPulse cloud.

Cautions

- Blue Coat must deliver on its SWG-as-a-service offering and demonstrate that it can compete against security services from other cloud-based services, many of which have a head start of two years or more. Blue Coat must demonstrate that its partners can sell its service, and it must also demonstrate that it has the operational expertise to manage a cloud-based service.
- Blue Coat must demonstrate that it can build an SMB-focused VAR partner channel that is capable of distributing the ProxyOne appliance.
- Blue Coat lacks an e-mail gateway — all other SWG cloud providers in this Magic Quadrant own a cloud-based e-mail gateway.
- The ProxySG does not support on-box antivirus. A separate appliance, the ProxyAV, is necessary to perform antivirus scanning.
- The WebPulse "cloud assist" approach, which requires Blue Coat to actively probe suspect websites, can be bypassed by attackers who recognize a request from WebPulse. A sophisticated attacker will know how to respond to Blue Coat (and other "cloud assist" security vendors' probes) with good content, but will respond to typical end-user Web requests with malicious content. Blue Coat would benefit from more on-box malware detection, as offered by several of its competitors. The WebPulse cloud assist limitation only applies to ProxySG implementations, not to Blue Coat's SWG-as-a-service offering (the concept of cloud assist does not apply to a cloud-based service).
- Blue Coat cannot monitor all network traffic (which is helpful for detecting outbound malware) in its most commonly deployed proxy mode (known as explicit proxy), but it can be configured in other modes to monitor all traffic.

Cisco

Cisco offers appliance-based SWGs (IronPort S-Series) and cloud-based SWG services (via its 2009 acquisition of ScanSafe). Also, in 2009, Cisco acquired its own URL-filtering database (previously, it had licensed Websense's SurfControl database), and developed its own reporting capabilities so that its customers no longer needed to use a third-party package (Sawmill). In addition, Cisco offers hosted e-mail services under the IronPort brand. Cisco's strategy is to develop an integrated Web and e-mail cloud-based security service with a single console that would also manage its IronPort appliances. Currently, these components are not integrated, and each has its own management console, although they do share a common URL-filtering database. Cisco's IronPort S-Series appliances are very good candidates for most midsize and large enterprises, and the ScanSafe service is a good candidate for all enterprises.

Strengths

- The S-Series provides good on-box malware detection. It also provides parallel scanning capabilities across multiple verdict engines for inbound as well as outbound security and content scanning. Signature databases are offered from McAfee, Sophos and Webroot, and two of these can be run simultaneously. Non-signature-based detection includes exploit filters that proactively examine page content, site reputation, botnet network traffic detection, transaction rules and Cisco-generated threat center rules. The S-Series also uses a mirroring port (SPAN) 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 include a full native FTP proxy and SSL traffic decryption.

- IronPort has numerous features to enhance the scalability of the S-Series for demanding large-enterprise needs, including native active-active clustering and centralized management for up to 150 servers. S-Series appliances can support up to 1.8TB of storage with hot-swappable serial attached SCSI (SAS) drives, RAID 10 configuration and RAID 1 mirroring, and six 1GB network interfaces, 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.

- The S-Series provides good content-aware 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 solutions RSA and Symantec/Vontu. Policy options include the capability to block "posting" to Web-2.0-type sites.

- Application control on the S-Series is very strong, with the ability to identify and block 13,000 Web-based applications. The Traffic Monitor feature enables the S-Series to connect to a port-mirroring switch port, and to detect and block port-hopping applications. Granular control is provided for social networking applications, such as blocking posts to Facebook.

- Customers commented on the ease of deployment in migrating to the ScanSafe service. The graphical dashboard is hyperlinked to filtered log views. 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 classifications.

- Cisco provides native support for SAML in the IronPort S-Series and in ScanSafe. The S-Series creates SAML assertions to federate identity from the enterprise to SaaS applications. The ScanSafe service consumes SAML assertions and enables a transparent authentication process for organizations that have already implemented SAML single sign-on solutions.

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

- Cisco's AnyConnect 3.0 client integrates ScanSafe's agent. Cisco's large installed base of VPN customers will now have ready access to the ScanSafe cloud (provided they migrate to the 3.0 version of AnyConnect). Using AnyConnect 3.0, traffic is SSL-encrypted from the client to the ScanSafe cloud.

- Cisco's channel strength should help it ramp up some SWG opportunities. It has enabled all IronPort and Cisco partners to resell the ScanSafe cloud Web security service. Also, Cisco has included IronPort products as a core part of the standard certification for all Cisco security partners.

Cautions

- Cisco needs a unified management console for its on-premises IronPort appliances and ScanSafe cloud services to ease migration for customers that are interested in hybrid deployments.

- The IronPort management console needs improvement for highlighting and investigating infected endpoints. While it reflects the top malware threats that have been detected in the environment, it does not provide a correlated and prioritized malware effects report or dashboard widget that would help desktop administrators track down and remediate potentially infected machines. Also, it does not provide severity information for the threats that it has detected.

- The S-Series is one of the most expensive SWG appliances in the market, and Cisco charges extra for the Cisco IronPort Web Reputation Filters.

- Log search functionality is weak on the S-Series, and it is difficult to search on or isolate search terms. ScanSafe, however, does provide the ability to search on search terms.

- Application control is weak with ScanSafe. Popular applications like Skype, IM and other common P2P applications cannot be controlled with policies.

- ScanSafe lacks bandwidth control capabilities.

- ScanSafe's content-aware DLP support is weak. Administrators can use basic dictionaries to monitor and alert on text strings, but the solution lacks more sophisticated data detection techniques, and lacks predefined dictionaries and policies.

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. Clearswift does not provide an SWG-as-a-service offering. Overall, Clearswift's primary advantages are its integration with its e-mail solutions and the provision of content-aware DLP across both channels, making the vendor a candidate for existing e-mail customers or EMEA buyers seeking both solutions from the same vendor.

Strengths

- Clearswift offers a clean, logical, browser-based interface for policy development and reporting for Web and e-mail that is easy to use, even for nontechnical users, with lots of context-sensitive recommendations and help functions. Multiple devices can be managed from any machine.

- Policy development for content-aware DLP is very good, and several policy constructs — Sarbanes-Oxley Act, Gramm-Leach-Bliley Act, Payment Card Industry Data Security Standard, U.S. Securities and Exchange Commission, accounting terms and stock market terms — are included. The same policy can be applied to Web and e-mail, and it is possible to intercept and copy/archive Web mail and IM traffic that trigger the 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 Lab and GFI Software (which acquired Sunbelt Software in July 2010). 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 (now owned by Symantec), augmented by real-time dynamic classification of uncategorized sites that would likely be blocked by liability concerns.

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

- In 2010, the company brought 24/7 customer support back in-house and built a new support portal. Clearswift also lowered its pricing scheme, moving to subscription-based pricing.

Cautions

- Clearswift remains primarily an EMEA brand, with a growing presence in Japan, but it does not enjoy significant brand recognition in North America. Its SWG revenue growth rate and market share remain very small.

- Malware detection is primarily limited to signatures and only in HTTP/S traffic. Although the solution provides some data on potentially infected machines inside the organization, it is not correlated or prioritized, nor does it have enough information on the suspected threat for quick remediation.

- Although the interface is simple enough to be used by nontechnical users, it is limited in detail for more technical enterprise users. The dashboard offers very limited customization. Reports are not linked to dashboard elements. Although the solution can edit existing reports, there is limited capability to create totally new reports. It does not have extensive role-based management and cannot limit administrative access to specific groups. Log search functionality is weak, and it is difficult to search on or isolate users' Internet search keywords for investigative analysis.

- 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 offer any bandwidth controls, except limiting file sizes.

- The proxy does not support ICAP or WCCP, and it does not support in-line/bridge mode deployments.

- Considering how long Clearswift has been offering DLP capability, it has not advanced to best-in-class capability, and continues to lack a comprehensive compliance workflow management interface.

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 in-line bridges. The company maintains its own URL-filtering database, and it provides a choice of third-party antivirus engines that run on the ContentKeeper appliance. It provides its own SWG-as-a-service plan and offers cloud-based e-mail protection through a partnership with Webroot. ContentKeeper is a candidate for organizations seeking URL-filtering capability and signature-based malware detection in supported geographies.

Strengths

- ContentKeeper offers a series of five appliances, the largest of which is based on IBM blade server technology, which ContentKeeper states 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. ContentKeeper provides basic IPS protection through a combination of third-party and internally developed 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 can dynamically classify unknown URLs.

- ContentKeeper provides a choice of three antivirus engines (BitDefender, Kaspersky and The Last Line of Defense), in addition to internally developed signatures that are included with the base system.

- ContentKeeper provides application control for more than 90 applications.

Cautions

- Malware detection and control are limited. Outbound malware detection lacks detail. It shows which malware-infected websites have been blocked, and provides a link to Google to display more information, but — unlike some other solutions — does not contain severity indicators or detailed information about infections.

- The SWG-as-a-service offering, which is agent-based and primarily targeted at SMBs, provides a limited capability to dynamically inspect Web pages for malicious intent.

- Data from geographically distant gateways is not aggregated in real time. However, real-time data can be obtained from each appliance, and syslog files can be imported from appliances on a scheduled basis to generate reports.

- The URL database needs more granularity. It only supports 32 categories, while 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 GFI Software (which acquired Sunbelt Software in July 2010) and Clam AntiVirus. The URL-filtering database is licensed from RuleSpace and enhanced through internally maintained updates. In 2010, Cymphonix released a new line of appliances with higher throughput to target midsize enterprises. Cymphonix is a candidate for SMBs seeking an 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 candidate for the kindergarten through Grade 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 Directory groups, or at a very precise level down to a specific host media access control (MAC) address 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 states has a maximum throughput rate of 1 Gbps. 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.

- The Network Conductor appliance aggregates log data and centralizes policy management, report generation and policy management for multiple, geographically dispersed Network Composer products.

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.
- Although the solution can edit existing reports, there is limited capability to create custom reports.
- Non-signature-based malware detection is limited.
- The solution has no ability to block posts to social networking sites.
- Application control is somewhat limited. For example, file transfers cannot be blocked from IM services.

M86 Security

While there is still work to do, in 2010, M86 Security made very good progress converging its various acquisitions into a cohesive product offering and company, while retaining much of the acquired talent and bringing aboard new management to move the company to the next level. M86 offers an appliance-based solution that can be augmented with a virtual server hosted by M86 for roaming users. The company just released a new version (v.10) of the Secure Web Gateway solution (formerly the Finjan solution), as well as the Security Reporter v.3. The combination of these products continues to be a good candidate for security-conscious organizations.

Strengths

- The Secure Web Gateway (based on technology from the Finjan acquisition) is a proxy-based appliance solution (hardware and virtual appliances). It has a native Web-based management interface for policy, configuration and reporting. M86 also offers an advanced consolidated reporting engine in a separate dedicated reporting appliance (from the 8e6 Technologies acquisition). The solution has a number of advanced enterprise features, such as administration roles that can limit visibility into data, audit logs, policy summaries and syslog integration. Policy development is object-oriented and can allow for very detailed policies. M86 Secure Web Gateway benefits from its own URL-filtering database. Policies can block posting to categorized websites (for example, social networks), and provide a limited capability to block some Web applications by name. M86 offers a hosted version of its virtual appliances in four data centers for use by remote access users in supported geographies when they're off the corporate network. This provides unified management of policies and reporting for on-premises and mobile users.
- The M86 Secure Web Gateway combines standard malware signatures — from a choice of Kaspersky, Sophos or McAfee — with very strong unknown-malware detection based on real-time code analysis, which scans an array of Web programming languages for malicious intent. It has very good capability for stripping or neutralizing the offending threats rather than blocking the entire page, which reduces help desk complaints. It can even block nonmalicious, but potentially unwanted, objects that have been downloaded from Web pages.
- Although the solution offers on-box reporting, larger enterprise customers will prefer to use the more scalable appliance-based reporting engine, which can support log consolidation of up to 32 enforcement nodes and 12TB of data on the largest appliance. The reporting engine is easily customized and provides an extensive collection of predeveloped reports, as well as an ad hoc reporting capability to create new reports. Searching the log is easy to do, and the solution saves user search terms. It also stores transaction IDs that are presented to users via blocked pages, and allows the help desk to quickly isolate events.
- M86 is launching an innovative offering that allows customers to create a custom YouTube portal that is limited to approved content only. The Secure Web Gateway has a zero post policy option that enables "read only" access to selected website or Web categories to prevent posting to social media or other interactive websites. The solution includes limited content-aware DLP capability, including the ability to detect content in attachments and perform lexical analysis on files and posts across HTTP/S or FTP.

Cautions

- M86 continues to be challenged by addressing the needs of its very diverse customer base, which ranges from SMBs to very large enterprises across multiple industry segments, geographies and product interests. M86 is consolidating its product code base to deliver more integrated and seamless functionality across the product suite. Although growth has accelerated in 2010 and early 2011, the combined company market share over the past five years has been flat in a rapidly growing market. M86 must continue to improve its channel and recover best-of-breed mind share or risk being overshadowed by rapidly improving and more strategic competitors.
- M86's solutions are clearly still integrating, and the look and navigation are inconsistent. The collection of management interfaces has many different windows and applications that are not consolidated in a single portal. The reporting engine and dashboard on Secure Web Gateway are completely different from the capabilities of Security Reporter, and Security Reporter is an extra cost. Administrative access rights capabilities are inconsistent and uncoordinated across both devices.
- Although Security Reporter provides some data on potentially infected machines inside the organization, it is not correlated or prioritized, nor does it have enough information on the suspected threat for quick remediation. Secure Web Gateway console has better information than Security Reporter.

- Secure Web Gateway lacks more innovative features, such as dynamic URL classification, page reputation analysis, bandwidth control, advanced content-aware DLP identifiers, and predefined policies and lexicons.

- Bandwidth prioritization is on the road map, but for now, Secure Web Gateway is only able to restrict applications or URLs by time-of-day conditions.

- The M86 Secure Web Gateway has the ability to block or allow IM clients covering AOL, ICQ, MSN Messenger, Yahoo Messenger and Skype, but not to control specific features of these applications. Port evasive applications require network firewall assistance to force these applications through the gateway for control and monitoring.

- Content-aware DLP capabilities are limited to keyword analysis and do not include predefined policies, dictionaries, or lexicons, nor do they offer much workflow support for compliance officers.

McAfee

McAfee has three SWG solutions: the McAfee Web Gateway (MWG) appliances, SaaS Web Protection service, and its legacy Email and Web Security Appliance. This analysis focuses mainly on the flagship MWG product, which remains a very good candidate for most enterprise customers, especially those that are already McAfee ePolicy Orchestrator (ePO) users. The Web Protection service is a candidate in supported geographies.

Strengths

- The MWG Ajax/Web-based management interface is well-organized, is easy for technical users to navigate and deploy, 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 now integrated with McAfee's ePO management platform. MWG has a reporting application that offers tiered administration and ships with the Enterprise Edition of MySQL, or integrates with Microsoft SQL Server or an Oracle Database.

- McAfee has a solid antivirus research team. MWG has strong on-box malware protection through use of the McAfee Gateway Anti-Malware Engine, which uses McAfee's signature engine as well as real-time code analysis technology that scans a broad array of Web programming languages for malicious intent, and offers optional use of a third-party antivirus signature engine from Avira.

- 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. MWG offers integrated IM proxy functionality to block and control IM, and provides granular control of the posting of content to Web 2.0 sites.

- MWG includes SSL decryption, which will combine well with McAfee's strong, native, content-aware DLP capability.

- In addition to its standard appliances, MWG is also available as a virtual appliance and as a Blade Server form factor.

Cautions

- McAfee hasn't significantly expanded its market share in the SWG market since the Secure Computing acquisition, and it does not show up on Gartner client shortlists as often as we would expect, given McAfee's channel reach.

- McAfee still has a lot of work to do to integrate ePO with its DLP, e-mail and endpoint solutions to deliver the security and deployment advantages of a single solution. Although McAfee is a major DLP solution provider, DLP capabilities across the three SWG products is inconsistent, and integration with enterprise DLP is still a work in progress. Also, there is no meaningful coordination between the SWG product line and the McAfee Endpoint Protection Platform (EPP) client.

- Hybrid integration between the SWG-as-a-service appliance and the MWG appliance is still a work in progress; currently, the integration consists of the URL categorization engine, the same McAfee signature antivirus engine, the same Gateway Anti-Malware Engine, the same Global Threat Intelligence network, and report consolidation via McAfee's Web Reporter.

- MWG does not provide a correlated and prioritized malware effects report or dashboard widget that would help desktop administrators track down and remediate potentially infected machines inside the organization.

- MWG's management features are still maturing; however, the product does not offer dynamic classification of content in unknown sites beyond the security risk analysis. Some commands can only be executed via a command line interface, and some changes require a server reboot. The dashboard cannot be customized; it lacks a good raw log search capability. Also, the policy change audit log is very basic.

- Consolidated and advanced reporting functions require Web Reporter, 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 MWG; 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 have complained about the scalability of the reporting interface.

- The SaaS Web Protection service lacks enterprise features and the global reach of the leaders in this space because it only has eight data centers. McAfee's clientless transparent authentication only records IP addresses for reporting (rather

than user names). It does not offer transparent authentication for mobile devices. Only mobile devices that accept proxy settings and VPN clients are supported. SaaS Web Protection only offers an uptime SLA, and it does not yet support SAML for directory integration.

Optenet

Optenet is a private company that was spun off from the University of Navarra's Engineering Faculty and San Sebastian's Research Centre in San Sebastian, Spain. It provides its customers with a multitenant SWG, the Optenet WebSecure (that is, it enables service delivery to multiple customers using shared infrastructure), and an e-mail infrastructure solution primarily for carriers, managed security service providers (MSSPs) and large enterprises that want to create service offerings for their own clients. Optenet is a candidate for large organizations and service providers that plan on delivering a multitenancy SWG.

Strengths

- Optenet's 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 from 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/S, FTP, POP, SMTP and MMS on a variety of platforms, including Crossbeam Systems and Linux (Red Hat), as well as appliances. Optenet also offers a full client that does local filtering for malware and URL policy, and is synchronized with on-premises appliances.

- Optenet augments Kaspersky, Sophos and Snort, 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 Optenet's own URL database, which is 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 has a very small market share that is primarily centered in Southern Europe and Latin America, but it has little brand recognition or presence in other markets. It has a development and sales presence in the U.S., but expansion into the U.S. market has been very slow. Although the company has many small enterprise customers, the solution's primary advantage is multitenancy support that appeals primarily to telecommunications companies and large enterprises seeking to deliver MSSP-type service solutions to their clients.

- Log search functionality is weak, and it is difficult to search on or isolate search terms.

- Optenet provides a unified policy management console that includes firewall and IPS functions. Policies have the same structure, which simplifies administration. However, the inclusion of some firewall and IPS-specific configurations in the management policy can cause some confusion for SWG customers. Moreover, few of Optenet's customers use Optenet WebSecure as a primary firewall or IPS.

- Application control is good for client applications, such as P2P, and it supports the capability to create custom filters using firewall rules or custom URLs, but it would benefit from more predefined application controls.

- Optenet has the capability to create custom filters to effect some content-aware DLP functionality, but it does not include any predefined content or DLP workflow.

Phantom Technologies

Phantom Technologies, a privately held company based in San Diego, is a new entrant in this Magic Quadrant. Its proxy-based iBoss Web-filtering solution is available as a family of appliance-based platforms. Phantom owns its URL-filtering database. More than 95% of its customers are in North America. iBoss is a candidate for organizations that are based in North America.

Strengths

- iBoss includes a unique autorecord feature (up to three minutes) that enables a video playback for a sequence of events. Organizations can customize the event that triggers the autorecord feature. The capability can be used to confirm intentional versus unintentional user violations.

- Log search capabilities are strong. Search engine requests are highlighted clearly in the log (for example, Bing, Google, Yahoo and YouTube), and the actual text string entered by the user is stored and can be easily searched.

- Bandwidth controls are very flexible. Bandwidth quotas can be applied to a specific organizational unit in Active Directory, and they can also be assigned to a specific domain.

- iBoss provides application control for popular IM services and some P2P applications.

- Reporting capabilities are strong, particularly the ability to create custom reports. The reporting tool includes some unique features aimed at executive management, such as calculating the hourly cost of using the Web.

Cautions

- Malware detection capabilities are limited. Snort rules and Clam AntiVirus are used to detect problems and trigger alerts, but Phantom only has limited resources (a small team of researchers) to develop its own signatures.

- Phantom's non-signature-based approach to malware detection is very limited.

- Although the solution provides some data on potentially infected machines inside the organization, it is not correlated or prioritized, nor does it have enough information on the suspected threat for quick remediation.

- Uncategorized URLs are not classified in real time. They are sent for classification to one of two data centers (New York and Los Angeles), and the results are pushed out to the iBoss installed base of appliances. The process can take several minutes.

SafeNet

SafeNet targets the SMB market with its appliance-based eSafe Web Security Gateway solution, which is part of the company's Enterprise Data Protection (EDP) strategy. This approach combines encryption and multifactor authentication with the SWG and its native, content-aware DLP capability. SafeNet moved into the Niche Players quadrant (from the Visionaries quadrant) in 2011, primarily due to its SMB focus and some product shortcomings, as noted below. The eSafe solution is a candidate for midmarket enterprises in supported geographies.

Strengths

- The dashboard has extensive information in a graphical format with hyperlinked drill-down into detailed report information. The reporting engine contains more than 240 predefined reports, including graphical end-user activity reports. Incident analysis is easy with strong log file search functionality and drop-down pick lists of potential search terms.

- Due to its merger with Aladdin Knowledge Systems in 2009, SafeNet has strong malware-filtering capabilities, including in-memory code emulation for analyzing suspicious code, vulnerability shielding, script analysis, active content policy options and SSL decryption. SafeNet offers an optional Kaspersky engine. The eSafe Web Security Gateway solution 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 (nearly 600) of potentially unwanted applications. eSafe also supports blocking IM file attachments and enforcing acceptable browser types. eSafe provides basic content-aware 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 investigative 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 is unique, and although these are some of the components of an enterprise data security program, very few enterprises consider these domains together when making purchasing decisions. eSafe lacks many enterprise-class, content-aware 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.

- Policies for establishing time usage quotas are limited.

- Although the solution provides some data on potentially infected endpoints, it is not correlated or prioritized, nor does it have enough information on the suspected threat for quick remediation.

Sangfor

Sangfor is a new entrant in this Magic Quadrant. It is a network equipment vendor based in China, and its 2010 revenue was approximately $50 million (according to U.S. accounting standards). Sangfor states that 55% of its revenue comes from its SWG products, and the remaining revenue comes from its VPN, WAN optimization controllers and application delivery controller products. Sangfor's SWG is a proxy-based solution that comes in a hardware appliance form factor. All the company's revenue comes from the Asia/Pacific region, although it has goals to compete globally in 2011 and beyond. Sangfor has two versions of its Web-based console — a Chinese version and an English version. Features and enhancements are added to the Chinese version first, followed by the English version at a later date. Sangfor is a candidate for organizations that are based in China.

Strengths

- Sangfor provides flexible and granular bandwidth control capabilities. For example, utilization parameters can be specified for uplink and downlink traffic.
- Basic content-aware DLP functionality is performed on box. Several preformatted dictionary templates are included (some are specific to the Chinese market), and organizations can create their own keyword-based custom DLP policies.
- The URL-filtering database will appeal to Chinese customers, since 80% of its entries are Chinese URLs. Sangfor plans to offer an English-based URL-filtering list in 2011 via a partnering agreement.
- For antivirus support, organizations can choose from F-Prot or Sophos (both via an OEM agreement).
- Sangfor's application signature database lists more than 600 entries, including gaming, IM and P2P applications.
- Sangfor has a large distribution channel in China, with more than 300 resellers and 25 distributions in large cities and most provinces.

Cautions

- Although the solution provides some data on potentially infected machines inside the organization, it is not correlated or prioritized, nor does it have enough information on the suspected threat for quick remediation.
- The appliance lacks a hardware SSL accelerator.
- The proxy does not support ICAP, thereby limiting its capability to send content to third-party scanners (such as DLP sensors or antivirus scanners).
- The English version of the Web interface lacks the capability to customize the dashboard. However, the dashboard of the Chinese version can be customized.
- The English version of the URL-filtering database lacks the capability to dynamically categorize unknown URLs. However, the Chinese version of the database does have this capability.
- The process of combining reports from various geographically distant gateways into a single report is difficult. The data cannot be viewed in real time because of the manual process involved with exporting data from each gateway.

Sophos

Sophos, a leader in the enterprise endpoint protection platform (EPP) market, is gradually improving the features of its hardware appliance and virtual appliance SWGs to appeal to larger enterprise customers. Ambitious management has resulted in company growth and geographic expansion from its European base to the North American and global enterprise markets. Sophos is a candidate for SMBs seeking simple management and policy capabilities with good security.

Strengths

- Sophos is an established player in the malware detection market, and the Sophos Web Appliance (SWA) uses Sophos' Behavioral Genotype technology to detect previously unknown malware by performing a pre-execution analysis of all downloaded code, including binary files and JavaScript. Sophos also provides increasing integration with its endpoint solution. Today, it offers client-based URL protection from malicious websites. Future offerings (due in 1Q12) will provide full Web policy filtering at the endpoint, using cloud services to provide live URL lookups and policy synchronization.
- Sophos provides very simple products to understand and manage. The management interface provides "three clicks to anywhere" navigation. SWA is very easy to set up, with automated network and directory discovery, contextual help functions and simple to understand policy configuration. Sophos even optionally monitors customers' appliances and provides proactive assistance for critical conditions (for example, disk failures, overheating and power issues).
- Security URL classification is supplied by SophosLabs and augmented with SurfControl URL categorization data provided by Websense.
- SWA offers very good log search capability, including the ability to search for groups of keywords used in Google and other searches, and isolates search terms in reports for clarity. In addition, SWA has a completely ad hoc reporting capability to create totally new reports, which is also very good.
- Sophos continues to have a strong reputation for support and service from customers and its channel.
- Full inspection of encrypted HTTPS content and sessions is supported for all modes of deployment, including explicit proxy, transparent, WCCP and bridged modes of deployment.

Cautions

- Sophos has been gaining momentum in this market in recent years; however, its growth is mainly in the sub-1,000 seat level. It still doesn't appear often in hotly contested large enterprise deals. It needs to improve its marketing message and its product to gain more recognition among midsize to large enterprises.

- Sophos is still missing some enterprise features, such as dashboard customization, limitations on log visibility and comprehensive audit logs. Role-based administration is on its road map for mid-2011. Sophos also lacks advanced Web management features, such as bandwidth and application controls, while features such as blocking social posts (for example, in Facebook) and streaming media controls may not provide sufficient granularity for some enterprises.

- The URL-filtering feature does not provide dynamic classification, except for anonymizer proxy sites.

- Consolidated policy management and reporting across multiple appliances require Sophos Management Appliances.

- Although the solution provides some data on potentially infected machines inside the organization, it is not correlated or prioritized, nor does it have enough information on the suspected threat for quick remediation.

- Signature-based malware detection is limited to the Sophos engine. Some organizations may want to increase the diversity of signature-based protection by using different signature engines in the gateway and on the desktop.

- Although Sophos has some native DLP capability in the endpoint, it has not transferred that technology to the Web gateway solution, and it does not provide ICAP support for DLP integration.

- Sophos does not yet offer a native method to apply policy and protection to mobile and off-LAN devices. A client for Windows devices is due in 2011; however, it is integrated into the full Sophos EPP client.

Symantec

Symantec has two offerings in the SWG market: the Symantec.cloud SWG as a service (formerly MessageLabs) and the Symantec Web Gateway appliance. Symantec.cloud is the foundation for Symantec's cloud-based solutions, which also include secure e-mail gateway, archiving and disaster recovery, as well as hosted endpoint protection management and backup services. However, integration between these two SWG offerings is lacking. Symantec.cloud is a candidate for customers seeking a simple-to-use, service-based solution, especially if they are also interested in secure e-mail gateway security services. Symantec Web Gateway is a candidate for customers seeking a scalable, in-line appliance SWG, or for those looking to augment their existing proxy solutions with better security and application control.

Strengths

- The Symantec.cloud Web GUI has the same simple and easy-to-use interface as the e-mail and IM security services, making it a good choice for customers seeking multiple services. Symantec.cloud has 10 data centers for the Web security service. The service offers strong antivirus, latency, uptime and support SLAs, and customers give it high marks for service and support.

- Symantec.cloud recently added usage quotas and expanded the management interface languages (now English, German and Japanese). It has decent reporting capability that includes flexible, ad hoc reporting with easy custom group creation. Malware is filtered with Symantec's own antivirus scanner as well as the F-Secure engine, and augmented by MessageLabs' Skeptic malware filters. The Websense URL database has been replaced with Symantec's own solution (from the RuleSpace acquisition), which offers limited dynamic classification for 15 types of typically blocked categories. Symantec also recently released the "Smart Connect roaming agent," which forces traffic to the nearest data center.

- The appliance-based Symantec Web Gateway 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 by 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/allowing) and policy control of a large number of named applications, such as P2P, IM, games and remote access.

- Symantec Web Gateway has strong management interfaces. Policy creation is done on a single-page view with intelligent options based on previous selections. The dashboard and reporting interface are 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 aid investigative analysis). Symantec Web Gateway provides a centralized server for configuration and consolidated reporting, as well as long-term storage of log data. Symantec replaced the Sophos and GFI Software (which acquired Sunbelt Software in July 2010) 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. Threat intelligence and rule creation have been transitioned to Symantec's Global Intelligence Network and Security Technology and Response teams. The URL database is still licensed from IBM, but we expect this solution to adopt the RuleSpace data in 2011.

Cautions

- Symantec has been very careful not to disrupt the MessageLabs business as a result of the acquisition, and despite the new branding as Symantec.cloud, it continues to operate relatively independently. We anticipate that this will continue; however, the pressure to integrate back-end functions will be strong and could potentially increase performance risk.

- Integration between the Symantec.cloud, the Symantec Web Gateway appliance, the Symantec Endpoint Protection Client and the Vontu DLP platform is still limited.

- Symantec did not increase the global data center footprint or management interface localization as aggressively as anticipated, and now finds itself behind several competitors in global reach.

- 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 2010, and customers have said that reporting needs significant improvement. Reports are relatively static and do not allow for drill-down and drill-up capabilities, log search is not possible in the management interface, and it does not allow restrictions on what group data is visible to administrators. Outbound malware reporting is minimal and does not yet show severity indicators or threat details. Links to Symantec's threat library and correlated data showing high-risk PCs would be improvements. The service only supports relatively simple policies and does not allow conditions, which means it takes several rules to create granular policy. The URL policy would benefit from advanced options, such as self-authorization and coaching. Application control is very limited and based only on URL destination rather than network/protocol signatures; also, it has only a very limited number of named applications for use in building policies. It does not offer SAML directory integration.

- Signature-based malware detection is limited to the Symantec detection engine. Some organizations may want to increase the diversity of signature-based protection by using different signature engines in the gateway and on the desktop.

- Symantec Web Gateway's unique design may cause problems for some larger enterprises. For example, it is difficult to add users to multiple policy groups, and the dashboard is not customizable and does not integrate with less common directory environments. Symantec Web Gateway does not proxy applications or offer a cache; although it was on the road map for 2010, it will not be delivered until the first half of 2011 (currently, it is in public beta). Symantec Web Gateway application control can be improved by blocking social networking and blog postings, and by using granular Web application function control. The solution would benefit from the IM control capability that Symantec acquired from IMlogic — which is currently in the e-mail gateway. SSL decryption is still missing; although it was on the road map for 2010, it will not be delivered until the first half of 2011 (currently, it is in public beta). Advanced policy options (such as coaching or self-authorization, time and bandwidth quota, or bandwidth rate shaping) are missing.

Trend Micro

Trend Micro has a long history of focusing on antivirus for the Web gateway market. As a result, it has a respectable market share with global enterprises. InterScan Web Security Virtual Appliance (IWSVA) is offered only in software solutions for virtual servers or bare metal installations. However, the company has not sufficiently invested in advanced features that differentiate its SWG offering and allow it to break into the Leaders quadrant. Trend Micro is a candidate for SMBs that already have a strategic relationship with the company.

Strengths

- The management benefits from a very customizable Adobe Flex dashboard environment and a significantly improved Advanced Reporting and Management solution. 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 and searchable logs. In distributed environments, a centralized Advanced Reporting and Management solution instance can act as a consolidated reporting engine/database and remove a task from the scan engine to improve and consolidate local performance. The solution can redact user names from reports and restrict administrators' visibility to managed groups.

- Policy development and configuration are easy to use and provide a powerful scripting capability that can be used to block actions such as social network posts or file transfers.

- Malware detection is provided by Trend Micro's signature database, script analysis, and a reputation service that is provided by its in-the-cloud Smart Protection Network. Trend Micro's Damage Cleanup Services can provide remote client remediation for known threats. IWSVA 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. It also 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.

- Total cost of ownership is improved with Trend Micro's use of its software virtual appliance platform, which allows a bare metal install on customer-owned hardware or on VMware ESX/Microsoft Hyper-V. IWSVA has multiple deployment options including ICAP, WCCP, transparent bridge, and forward and reverse proxy with automatic policy synchronization across clusters.

Cautions

- Despite Trend Micro's history in this market, it has failed to lead the market with enterprise-class features. This has allowed its more aggressive competition to steal mind share, particularly in large enterprises. IWSVA tends to be a suite component add-on, rather than a product that the channel will lead with, and we rarely see IWSVA in hotly contested large-enterprise deals. Trend Micro needs to invest in advanced product features if it wants to regain momentum in the SWG market.

- IWSVA is software-based and does not offer an SWG hardware appliance or an SWG-as-a-service solution. There is no native capability to protect and manage the Web traffic of off-LAN devices.

- IWSVA solutions are still lacking in numerous large-enterprise features, such as advanced role-based administration, policy summaries and synchronization with multiple different directory solutions. Bandwidth control is limited to quotas only. The outbound malware detection report lacks severity indicators to enable prioritized remediation. Although the solution can edit existing reports, it cannot isolate search keywords in logs or reports. It does not offer dynamic classification of URLs.

- Application control is limited to binary blocking of some P2P, IM and URL categorization blocking. Policies to block specific applications or application features require a high level of understanding of the application specifics and are relatively coarse. Trend Micro does not have any SWG DLP, although it does offer an endpoint content-aware DLP solution.

- Signature-based malware detection is limited to the Trend Micro engine. Some organizations may want to increase the diversity of signature-based protection by using different signature engines in the gateway and on the desktop.

Webroot

Webroot, which is well-known for its endpoint spyware protection solutions, has a rapidly growing cloud-based SWG and secure e-mail gateway (SEG) offering. Webroot is a candidate for SMBs seeking service provider options in supported geographies.

Strengths

- HTTP traffic is redirected to Webroot's cloud 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.

- In 2010, Webroot acquired URL classification vendor BrightCloud, which provides URL classification, website reputation and security risk analysis.

- The Web management interface provides centralized management of Web and e-mail services, is user-friendly and can be administered by nontechnical users. The graphical view of its SWG 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 certain 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.

- Malware protection is provided by Webroot and a Sophos malware signature database. Nonsignature threat detection capabilities include an anti-phishing engine, client Web application vulnerability scanning, as well as heuristic-based attack analysis. Webroot has had considerable experience with 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.

- The service provides security warnings and URL categorization icons on search results pages (Google, Yahoo, Bing and Ask.com) to warn users of unsuitable links in search results.

Cautions

- Webroot has had initial success in the SMB market (fewer than 1,000 seats), but has failed to get the attention of larger enterprise customers. It needs to improve its enterprise feature set and expand its global footprint and channel to break out of the 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. 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. Outbound threats are in static reports, but not in real-time dashboard views, and threat information is restricted to threat types or names of known threats. 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. The cloud-based SWG service does not offer SAML directory integration.

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

- The solution does not offer dynamic classification of Web URLs.
- Like other SWG SaaS providers, Webroot's inbound and outbound malware detection is limited to HTTP traffic types that are redirected to the service.
- Webroot's agentless solution requires a user name and password combination to authenticate each Web session.

Websense

Websense offers a wide range of options in the SWG market, from basic URL filtering to software and appliance-based SWGs, and cloud-based services for e-mail and Web security. Websense also owns DLP technology, which it offers as a stand-alone solution and also as an embedded option with its Web Security Gateway (WSG) solution. Websense is a very good candidate for most enterprise customers.

Strengths

- Websense has a strong distribution channel that enables it to target large enterprises and SMBs.
- Websense offers a unified console that is capable of managing a hybrid SWG solution (on-premises and SWG as a service).
- Websense owns all the core technology in its products, with the exception of third-party antivirus signatures.
- The Websense WSG provides extensive on-box, non-signature-based methods for detecting malware and advanced persistent threats (APTs).
- The Network Agent component, which is positioned on a port-mirroring port, analyzes all traffic on a network segment, which enables Websense to monitor non-HTTP traffic for malware detection. Many organizations use this feature to set and enforce policies for P2P applications and other undesirable traffic.
- The Websense Triton solution's management console is one of the best in the market and is consistent across all its offerings. 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 and time-based restrictions for Web surfing.
- 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.
- Websense's Defensio technology, which protects blogs and social networking sites from spam, malware and other threats, provides another source of signatures for the ThreatSeeker Network.
- Application control includes more than 150 applications, such as IM and chat, streaming media, P2P file sharing, e-mail and collaboration based on network signatures.
- The acquisition of PortAuthority in 2007 provided Websense with strong DLP technology, which is included in its SWG and enables granular, content-aware policy and reporting. Data detection techniques are complete, and the product includes a broad range of predefined dictionaries and data usage policies.
- For its cloud-based service, Websense supports SAML with its included VMware TriCipher solution integration.
- Websense is one of the few vendors that can offer software, appliances, client software and SWG as a service. 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

- With only two appliances, the V5K and the V10K, Websense's SWG appliance family is limited. It needs to broaden this product line and add higher-performing appliances and lower-performing appliances to provide a stronger fit for a range of opportunities.
- Agentless transparent authentication is not supported for mobile users. They must authenticate to the service by providing their e-mail addresses and a Websense-specific passwords. If a mobile endpoint has the Websense client, then the user will be automatically authenticated and traffic will be redirected to the Websense cloud.
- Some of Websense's VAR partners are complacent and simply aim to renew traditional URL-filtering licenses, instead of upselling more advanced SWG functionality.
- Although the solution provides some data on potentially infected endpoints, it is not correlated or prioritized, nor does it have enough information on the suspected threat for quick remediation.

Zscaler

Zscaler is a SaaS provider of SWG and SEG services. The company is the only one to separate policy administration, reporting and enforcement, enabling each element to scale independently. Zscaler moves into the Leaders quadrant in 2011 due to the demonstrated success of its unique architecture, rapid feature development, global rollout of enforcement nodes, and impressive growth in numerous global markets among small and very large enterprise clients. Zscaler is a very good candidate for most enterprise customers.

Strengths

- The Flash-based management interface for Web and e-mail services is easy to use, even for nontechnical administrators. Zscaler is strong in the reporting category. Reports are based on live data and allow very rapid drill-down into detailed analysis. Custom reports can be created and run instantaneously. User names can be redacted from reports. Zscaler's NanoLog technology reduces log size by a factor of 50, enabling very fast reports and longer retention of detailed data. The Analyze tool allows an administrator to set filters on any field and retrieve matching log data in a few seconds, and save views as favorites for repeat queries. Super categories (liability, productivity, bandwidth and malicious) allow faster usage analysis. The dashboard has a unique "compared to industry peers" report, which shows relative data compared with averages for Zscaler customers. Zscaler is the only solution that 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 easy to use and logical. All policy is user-based and follows roaming users, allowing immediate service at the nearest enforcement node (cloud-based proxy appliance).

- Zscaler has several methods for redirecting clients. It was the first vendor to offer authenticated redirection to the cloud without a software client. Now, it also offers a client-based redirection agent for higher security on unmanaged devices. It also supports standards-based GRE tunnels, and can host customer proxy autoconfiguration (PAC) files. Zscaler also supports SAML for directory integration. Juniper Networks' SRX, ISG and SSG firewalls provide simple interfaces to connect to Zscaler using GRE tunnels. Zscaler also integrates with Juniper's Junos Pulse mobile protection solution to connect mobile devices or laptops to Zscaler's cloud.

- 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, plug-ins or browser versions. Zscaler augments its security coverage with feeds from partnerships with Microsoft, VeriSign, Qualys and others.

- Application control includes numerous named applications that can be blocked using a combination of destination URLs and some network signature analysis. Companies under pressure to liberalize productivity filters can allow Web 2.0/social networking page views while blocking posting to these sites, as well as allow optional content-aware 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 enable fast global deployments. It already has the largest global footprint of data centers (by far) with a total of 50, and it is adding one new location per month in 2011. It also allows for "private node" and "private cloud" deployments for very large organizations, service providers, or organizations in unique geographies.

- Zscaler customer support continues to get high marks from customers for fast response rates and a very technically knowledgeable support staff.

Cautions

- Zscaler has handled its rapid growth very well so far, but it must continue to invest ahead of demand for customer support. Although it is one of the fastest growing vendors in this market, it lacks the resources of its larger competitors.

- Although its enforcement nodes are widely dispersed geographically, the reporting and policy data resides only in the U.S. and the Netherlands so far, although expansion is expected to follow customer demand for local storage.

- The management interface is missing full customization of dashboard elements. Although it provides some data on potentially infected machines inside the organization, it is not correlated or prioritized, nor does it have enough information on the suspected threat for quick remediation. While providing more than 16 different filters, the log filter functionality lacks the ability to search on or isolate search keywords.

- Not all network devices support GRE tunnels, which is Zscaler's preferred method of traffic redirection. For example, Cisco's ASA firewall does not support GRE tunnels, thereby requiring customers to use alternate forwarding techniques or their gateway routers instead of the firewall. Zscaler is in the process of deploying IP security (IPsec) VPN termination capability across its cloud.

- Clientless PAC file redirection can be disabled by users or malicious software, and only redirects traffic from applications (that is, browsers) that use the proxy settings. Evasive client applications, such as Skype and P2P or malware, may not

be forwarded to the Zscaler network on clients that rely on PAC files. Zscaler has a client that can enforce proxy PAC file settings, but it does not stop evasive traffic from bypassing the Zscaler network. The new IPsec VPN connection method should alleviate this concern in the future.

- There are no native FTP application controls, but the service supports stand-alone FTP clients as well as FTP over HTTP.
- Compared with its larger competitors, Zscaler only has a limited number of dedicated malware researchers.
- The SWG solution comes in five different packages, and buyers must be aware that capabilities such as content-aware DLP, bandwidth control, Web 2.0 controls and APT protection are only available in the premium-price packages.
- Dynamic classification of websites is limited to a subset of URL categories (for example, potential legal liability and malware hosting sites).

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	
DLP	data leak prevention
ePO	ePolicy Orchestrator
GRE	Generic Routing Encapsulation
GUI	graphical user interface
HTTP/S	HTTP over SSL
ICAP	Internet Content Adaptation Protocol
IM	instant messaging
IP	Internet Protocol
PAC	proxy autoconfiguration
P2P	peer-to-peer
SMB	small and midsize business
SSL	Secure Sockets Layer
SQL	Structured Query Language
SWG	secure Web gateway
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, 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 website, 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.