G00234572

Magic Quadrant for Secure Web Gateways

Published: 24 May 2012

Analyst(s): Lawrence Orans, Peter Firstbrook

Secure Web gateways support a wide range of functions. URL filtering and malware detection are the features most in demand. Mobile support, application control and data loss prevention are the emerging market drivers.

Market Definition/Description

A secure Web gateway (SWG) is a solution that filters unwanted and malicious software (malware) from user-initiated Web/Internet traffic, and enforces corporate Internet policy compliance. SWGs must, at a minimum, include URL filtering, malicious code detection and filtering, and application controls for popular Web-based applications. Native or integrated content-aware data loss prevention (DLP) is also increasingly included. SWGs have traditionally been appliances and software. However, the cloud-based SWG delivery model is growing rapidly.

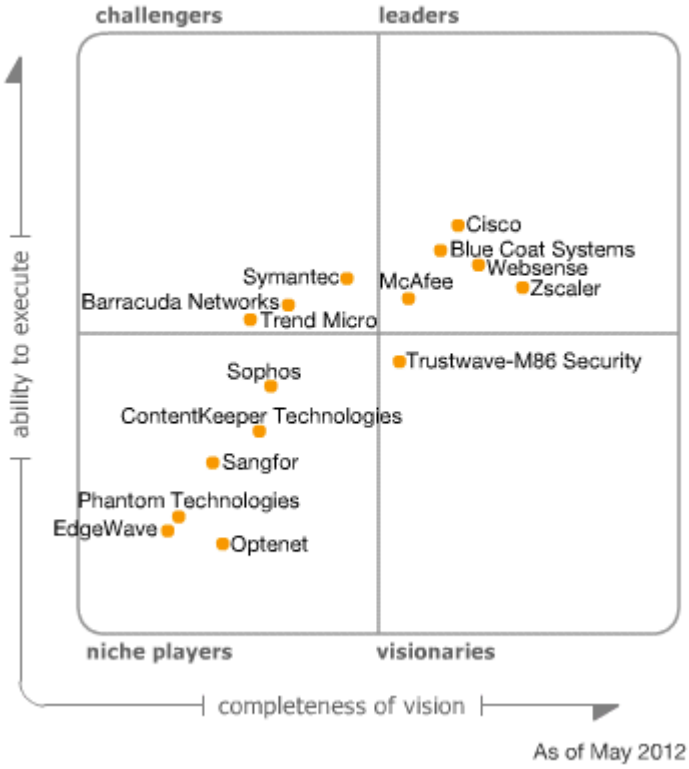
Gartner's market sizing includes on-premises solutions and cloud-based SWG-as-a-service offerings. In 2011, we eliminated single-purpose proxy servers and URL revenue in our market-sizing estimates to get a more accurate reflection of the pure SWG market without the weight of legacy point products. Using this analysis, we estimate that, in 2011, the SWG market reached $1.021 billion, a growth of 19% over 2010, which was slightly higher than our 17% estimate last year. The five-year compound annual growth rate is approximately 16%. In 2012, we estimate that the market will grow approximately 15% to just under $1.2 billion.

The market is still dominated by on-premises solutions (approximately 87%), with SWG as a service representing the remainder of the market (approximately 13%). However, the SWG-as-a-service segment is the fastest-growing segment (Gartner expects that it will grow 35% in 2012).

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.

Magic Quadrant

Figure 1. Magic Quadrant for Secure Web Gateways



Source: Gartner (May 2012)

Vendor Strengths and Cautions

Barracuda Networks

Barracuda Networks (based in Campbell, California) offers the Barracuda Web Filter appliance and the Barracuda Web Security Flex cloud service. These solutions can be combined for a hybrid implementation. Barracuda Web Filter appliances are good candidates for SMBs and selected large enterprises (particularly in the education and government verticals).

Strengths

- Barracuda offers a low-cost solution with good security functionality. Its prices can be half the price of competing vendors that target large enterprises.
- Both the cloud service and the appliance have a very easy-to-use interface with suggested configuration settings and contextual help.

- Application controls include numerous named applications and application categories. Nonbrowser applications, such as Skype, can be controlled with the appliance in in-line mode or with the Barracuda Web Security Agent for Windows and Macintosh computers.

Cautions

- Barracuda does not offer a choice of antivirus engines. Open-source ClamAV is the only option. Barracuda adds internally developed signatures, although its lab research team is relatively small.
- The Barracuda Web Filter appliance lacks some enterprise-class capabilities for management and reporting. For example, the dashboard is not customizable, and outbound infected-client reporting does not provide guidance on the severity of a particular threat or links to more threat detail.
- The Barracuda Flex cloud-based service is also missing a number of enterprise features. 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 be stored only in the cloud, not on the local devices.

Blue Coat Systems

Since the publication of last year's Magic Quadrant, Blue Coat has changed CEOs and has transitioned from a publicly traded to a privately held company. The new CEO joined the Sunnyvale, California-based company in August 2011 and replaced the previous CEO, who held the position for approximately one year. In February 2012, Thoma Bravo, a private equity firm, announced that it completed the acquisition of Blue Coat, in a deal that was valued at approximately $1.3 billion. Blue Coat offers a family of proxy appliances and a separate family of appliances that run third-party antivirus engines. It also offers a cloud-based SWG service. Blue Coat is a very good candidate for most enterprise customers.

Strengths

- The ProxySG product is well-tested for scalability and performance in large-enterprise environments. It also includes numerous advanced proxy features, such as support for a long list of protocols (including SOCKS), extensive authentication and directory integration options, raw policy scripting capabilities, and support for the Online Certificate Status Protocol (OCSP). The ProxySG can be configured as a reverse proxy.
- 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.
- Blue Coat's cloud-based WebPulse service uses the data that it collects from its ProxySG appliances, its K9 consumer service and its enterprise cloud service to track the networks and related infrastructure used by attackers to distribute malware. Blue Coat calls these "malware networks," and protects its customers from attacks launched from the malware networks that it has discovered.

- 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. Customers that also have licenses for Blue Coat's cloud service have the option to upload logs generated by ProxySG appliances to Blue Coat's cloud-based reporting service for unified reporting.
- Blue Coat owns strong application recognition technology that it gained through its acquisition of Packeteer, although it has been slow to integrate this capability in its ProxySG family.

Cautions

- Unlike several other vendors that offer cloud-based services and on-premises appliances, Blue Coat does not offer a "single SKU" price model that allows the option to mix and match cloud and on-premises Web-filtering licenses. Blue Coat customers must buy a separate license for both deployment methods, although it offers discounts to customers that purchase both services.
- Blue Coat's SMB strategy is incomplete. Unlike several other vendors that offer cloud-based SWG and secure email gateway (SEG) services, Blue Coat offers only an SWG service. The lack of a cloud-based SEG limits Blue Coat's opportunities in the SMB market, because many SMBs purchase cloud-based SWG and SEG services from the same vendor. In 2011, Blue Coat withdrew its ProxyOne appliance, aimed at the SMB market, three months after it began shipping.
- The ProxySG appliance lacks on-box malware detection. Customers that want protection from an antivirus engine must purchase a separate appliance (ProxyAV). Malware protection is also provided by Blue Coat's "cloud-assist" WebPulse 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, which is based in San Jose, California, offers appliance-based SWGs (IronPort S-Series) and cloud-based SWG services (via its 2009 acquisition of ScanSafe). The IronPort appliances are deployed as proxies. Cisco's IronPort S-Series appliances are very good candidates for most midsize and large enterprises, while the ScanSafe service is a good candidate for all enterprises.

Strengths

- The S-Series provides three choices for on-box signature databases (McAfee, Sophos and Webroot), all of which can be supported simultaneously. An "adaptive scanning" feature directs suspicious content to the anti-malware engine that is best optimized to scan the content.
- Cisco has added features to some of its networking products to ease ScanSafe implementation. Cisco customers with ISR G2 routers at remote offices can utilize a software "connector"

feature to redirect traffic and forward identity information to the ScanSafe cloud. Similarly, customers using the AnyConnect VPN Client for mobile workers can also redirect traffic and identity information to ScanSafe. Cisco plans to add the software connector feature to its ASA firewall in 2012.

- The IronPort appliance provides granular control for social networking applications, such as blocking posts to Facebook. The appliance can identify and block 13,000 Web-based applications (although it analyzes only port 80 traffic).
- Cisco offers broad support for mobile devices via its AnyConnect VPN Client, although there are some dependencies based on the OS version. It supports Windows Mobile, BlackBerry (through BlackBerry Enterprise Server [BES]), Mac OS and iPhone and iPad, and Android.

Cautions

- Cisco lacks 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.
- Because the IronPort appliance lacks the ability to analyze non-port-80 traffic, it cannot detect and block port-hopping applications, such as Skype and BitTorrent-based applications.
- The IronPort management console does not correlate outbound malware detection and lacks severity indicators to enable prioritized remediation.

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 in transparent bridge mode, and it also offers a cloud-based service. ContentKeeper is a candidate for organizations seeking SWG functionality in supported geographies.

Strengths

- The Behavioral Analysis Engine (a feature of the company's flagship Web Security Gateway) provides signatureless malware detection and analyzes traffic across all TCP ports.
- ContentKeeper's "sandboxing" appliance runs virtualized instances of Windows XP and Windows 7. Downloaded files in several formats (Windows executables, PDF files, HTML files and others) are run in the virtualized operating systems and are flagged if they exhibit suspicious behavior.
- When deployed as an in-line transparent bridge, the appliance supports the ability to proxy Secure Sockets Layer (SSL) traffic. Basic intrusion prevention system (IPS) protection is provided through a combination of third-party and internally developed signatures.

Cautions

- ContentKeeper has limited brand awareness and visibility beyond Australia and some countries in the broader Asia/Pacific region.
- The URL database needs more granularity. It supports only 32 categories, while most competitors support more than twice as many categories (although custom categories can be added).
- Some customer references requested improvements to the product's graphical user interface (GUI).

EdgeWave

EdgeWave, a publicly traded company based in San Diego, is a new entrant in this Magic Quadrant. Formerly known as St. Bernard Software, the company rebranded itself in 2010 with a stronger focus on security. Its iPrism Web-filtering solution is available as a family of appliance-based platforms that are deployed in transparent bridge mode. The addition of several new senior managers in 2012 looks promising for the company. EdgeWave is a candidate for SMBs that are based in North America (approximately 95% of its customers are in North America).

Strengths

- The in-line transparent bridge mode enables EdgeWave to block outbound communications to known botnet command and control centers.
- EdgeWave provides granular policies to control the usage of Facebook and Twitter.
- EdgeWave has a large installed base in the K-12 vertical. The solution has strong proxy anonymizer detection and blocking features, which is an important criterion in this vertical.
- Customers commented on the ease of deployment and ease of use. EdgeWave provides video tutorials embedded in the iPrism interface.

Cautions

- EdgeWave's name recognition and branding have been weak (as measured by Gartner client inquiries).
- Malware reporting is limited. The GUI lacks a dashboard for providing real-time insight into malware status and traffic levels. The tool does not show malware severity indicators or threat details.
- EdgeWave doesn't support dynamic classification of uncategorized websites. Customers may manually submit a URL to EdgeWave's rating service (EdgeWave states that many sites are categorized within an hour).
- Mobile support is limited to Web filtering and does not include malware detection. For OS X and Windows systems, an agent sends a lightweight look-up to the cloud, which returns a block or

allow policy. The cloud does not proxy the Web request and, therefore, lacks the ability to dynamically inspect Web content.

McAfee

McAfee, a subsidiary of Intel, offers a family of on-premises secure Web gateway appliances (McAfee Web Gateway) and a cloud-based SWG service (SaaS Web Protection). The SWG appliances are configured as proxies. McAfee's solutions are good candidates for most enterprise customers, particularly those that are already McAfee ePolicy Orchestrator (ePO) users.

Strengths

- McAfee Web Gateway (MWG) has strong on-box malware protection, due to McAfee's signature engine and its signatureless behavioral, context-based malware detection capabilities. A rule-based policy engine enables flexibility and granular control, including the ability to adjust the sensitivity of malware detection.
- Application control for Web 2.0 is supported via the AppPrism database, which includes over 1,200 applications. Support for HTTP manipulation allows organizations to remove selected functions from Web applications (for example, certain features within LinkedIn, and posts or tweets from Twitter). External APIs for Web applications can be leveraged to provide additional data that can be used in MWG policies. For example, videos can be blocked from YouTube by leveraging the Google API for YouTube categorizations.
- McAfee has made progress in sharing its DLP technology across product lines. MWG ships with a number of preformatted dictionaries.
- A single "SKU" pricing model gives customers the flexibility to purchase a single Web gateway license, and to mix and match on-premises and cloud-based service models.

Cautions

- McAfee's cloud-based offering has been late with important features, particularly support for SSL, Security Assertion Markup Language (SAML) and IPsec termination (which is particularly helpful for mobile devices). It has a limited set of ISP and managed security service provider (MSSP) channel partners to help it sell its cloud-based service.
- McAfee hasn't significantly expanded its market share or mind share in the SWG market since the Secure Computing acquisition.
- Some customers complained about the scalability of Web gateway logging and reporting functions.

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. The company provides an appliance

platform that provides SWG, network firewall and email services, via a unified policy management console. It is a candidate for carriers, MSSPs, and large enterprises that want to create multitenant service offerings or private cloud offerings for their customers.

Strengths

- Optenet is a fully multitenant solution by design, and can support a large number of users and scale using a number of deployment options (for example, proxy, Layer 2 bridge, router and traffic analyzer) and form factors (Crossbeam appliances and native 10 Gbps appliance). It also supports role-based servers that can combine or separate functions as needed (that is, enforcement, and management or reporting).
- Optenet's dashboard and management interface is the same for Web and email solutions. It is very customizable, enabling users to add different reports in numerous combinations.
- Optenet augments Kaspersky, Sophos and Snort with its own security analysis for emerging threats. Optenet also offers a full endpoint client that does local filtering for malware and URL policy, and is synchronized with on-premises appliances. Outbound threat reporting includes a severity indicator in a graphical format. Application control includes numerous named applications detected via its network signature.
- The solution also offers bandwidth management and quality of service (QoS) features, as well as a good network analyzer that provides network application visibility.

Cautions

- Optenet has a very small market share that is primarily centered in Southern Europe and Latin America, with an emerging presence in Asia/Pacific. It has very little brand recognition.
- The company's focus on multitenant architecture limits its appeal to a small subset of the enterprise market.
- It would benefit from more predefined application controls, which are reportedly due in 3Q12.

Phantom Technologies

Phantom Technologies is a privately held company based in San Diego. It offers a family of appliance-based platforms that are typically deployed in transparent bridge mode. Phantom is a candidate for organizations that are based in North America (approximately 95% of its customers are in North America).

Strengths

- Support for features aimed at the K-12 market has helped Phantom develop a strong installed base in the education market (approximately one-third of its revenue is from the K-12 vertical). For example, the iBoss Web Filter enables schools to easily allow access to YouTube's educational site, while blocking access to the main YouTube site.

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

- Support for mobile devices has some limitations. A cloud-based service requires the deployment of an on-premises appliance to handle policy management, reporting and other tasks. Phantom lacks a client for Android devices (although it offers clients for Windows, Mac OS X and Apple iOS devices).
- Malware detection capabilities are limited. Phantom has only limited resources (a small team of researchers) to develop its own signatures. Choices for antivirus engines are limited to Bitdefender or ClamAV (both can be combined with Snort rules). SSL traffic cannot be decrypted (although certificates can be inspected for misuse).
- 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 the Phantom cloud, and the results are pushed out to the iBoss installed base of appliances. The process is typically completed in under one hour.

Sangfor

Sangfor is a network equipment vendor based in China. Approximately half 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 comes in a hardware appliance form factor, and it is usually implemented as an in-line transparent bridge. All the company's revenue comes from the Asia/Pacific region, although it has goals to compete globally in 2012 and beyond. Sangfor is a candidate for organizations that are based in China and in supported countries in Asia/Pacific.

Strengths

- Sangfor's in-line transparent bridge mode enables flexible and granular bandwidth control capabilities. For example, bandwidth utilization parameters can be specified for uplink and downlink traffic.

- The URL-filtering database will appeal to Chinese customers, since 80% of its entries are Chinese URLs. In 2011, Sangfor began licensing a URL-filtering database from Commtouch, which enables it to better target English-speaking customers.
- Sangfor's application signature database lists more than 700 entries, including gaming, IM and peer-to-peer (P2P) applications. Administrators can block Web applications by category and name of the application.
- Sangfor has a large distribution channel in China, with more than 300 resellers and 25 distributions in large cities and most provinces.

Cautions

- Sangfor does not offer a cloud-based service for supporting mobile users.
- Sangfor supports two versions of its product, one targeted for the Chinese market and one targeted for English-speaking markets. Some features are added in the Chinese version of the product before they are added to the English version. For example, the English version of the URL-filtering database lacks the capability to dynamically classify uncategorized URLs. However, the Chinese version of the database does have this capability.
- The Sangfor appliance does not support Internet Content Adaptation Protocol (ICAP), thereby limiting its capability to send content to third-party scanners (such as DLP sensors or antivirus scanners).

Sophos

Sophos, which has executive offices in England and Massachusetts, improved its network security capabilities in 2011 with the acquisition of unified threat management (UTM) vendor Astaro, and made improvements in its appliance-based SWGs to appeal to larger enterprise customers. The Sophos Web Appliance (SWA) can be deployed in proxy or in transparent in-line bridge mode. Sophos is a candidate for most enterprise customers, particularly those that have already implemented Sophos' endpoint protection agents.

Strengths

- Sophos is an established player in the malware detection market. The Sophos Web Appliance (SWA) uses Sophos-developed technology to perform a pre-execution analysis of all downloaded code, including binary files and JavaScript.
- SWA has strong ease-of-use features that include automated network and directory discovery, contextual help functions, and simple policy configuration.
- Sophos has a strong reputation for support and service. It optionally monitors customers' appliances and provides proactive assistance for critical conditions.
- A unique endpoint solution synchronizes policy and Web logs of mobile devices (Windows and Mac OS X) with the appliances to protect off-network devices from Web threats.

Cautions

- Sophos does not appear often in hotly contested large enterprise deals, due in part to a weak marketing message.
- SWA is missing some enterprise-class features, such as dashboard customization, bandwidth management and ICAP support. Features, such as blocking of social media 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 of uncategorized websites.
- Reporting on compromised endpoints is not correlated or prioritized, nor does it have enough information on the suspected threat for quick remediation.
- The endpoint solution (noted above in Strengths) for mobile devices requires a full Sophos endpoint protection platform (EPP) client and gateway infrastructure. The client performs only payload inspection, not traffic analysis (for example, DNS traffic), which is often used to detect bot-compromised endpoints. Only Windows and Mac OS X operating systems are supported.

Symantec

Symantec (based in Mountain View, California) has two offerings in the SWG market: the Symantec.cloud service, and the Symantec Web Gateway appliance, which may be deployed as an in-line transparent bridge, as a proxy, or in switch port analyzer (SPAN) or test access point (TAP) mode. Symantec bundles a virtual version of its appliance with a suite offering that includes email and endpoint protection. Symantec is a good candidate for most enterprise customers.

Strengths

- Both the service and the gateway benefit from Symantec's malware research labs. Symantec's file reputation engine, known as "Insight," is used to deliver a reputation rating for all file attachments detected by its gateway appliance.
- Symantec.cloud provides the broadest array of cloud-based security services in this analysis, including email, IM, archiving, backup and management for Symantec Endpoint Protection clients. The Web service offers strong antivirus and service-level agreements (SLAs), and customers give it high marks for service and support.
- The Symantec Web Gateway is offered as both an appliance and virtual software for VMware environments. It can be deployed as an in-line bridge, which provides more visibility of malware and applications, but it also includes a proxy for HTTP and SSL traffic to provide more control of these protocols.
- The appliance's most notable feature is the reporting emphasis on outbound traffic that indicates the presence of specific malware and the severity and type of the threat. It also provides quick access to more detail, such as geolocation data, search terms, file names and types, malware encyclopedia, and removal information.

Cautions

- Symantec's market share is low, given its extensive brand recognition and channel resources.
- Symantec does not offer a unified console to manage policies for its Web Gateway appliance and Symantec.cloud service. Capabilities of the two solutions are very different, particularly when the appliance is deployed as an in-line transparent bridge and is able to base its malware detection on seeing all traffic. The cloud offering is always implemented as a proxy, and sees only the Web traffic that is redirected to it.
- Both solutions lack granular control for social media sites. Symantec.cloud lacks granular control for applications.
- The Symantec.cloud service lacks some enterprise features. It does not inspect SSL or proxy native FTP traffic. Endpoint redirection is limited to proxy autoconfiguration (PAC) files and is missing clients for iOS and Android. Outbound malware reporting is limited.
- The Symantec Web Gateway appliance lacks some enterprise-class features, such as a customizable dashboard and advanced policy options (such as coaching or self-authorization, time and bandwidth quota, or bandwidth rate shaping).

Trend Micro

Trend Micro is based in Tokyo. Its InterScan Web Security (IWS) solution is available as a software appliance and as a hardware appliance in select regions (it will be available globally in 2H12), and it can be implemented as an in-line transparent bridge or as a proxy. Trend Micro is a candidate for enterprises or SMBs that already have a strategic relationship with the company.

Strengths

- 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.
- The solution offers strong management features via its dashboard and separate reporting application. Customized reports can be created using open-source iReport and added as a dashboard element or in completely new tabs.
- Policy development and configuration are easy to use and provide a powerful scripting capability that can be used to block actions, such as posts to social media sites or file transfers. It also offers time of day, and time and bandwidth quota policy options.
- Application control includes over 400 Internet applications, including some P2P and IM traffic types that are detected by network signatures. Browsers, browser versions and plug-ins can be blocked by policy.

Cautions

- Despite Trend Micro's history in this market, it has failed to lead the market with enterprise-class features. IWS tends to be a suite component add-on, rather than a product that the channel will lead with, and we rarely see it in hotly contested large-enterprise deals.
- The company does not offer a cloud-based service for supporting mobile users, although it plans to offer one in 2012.
- IWS lacks several large-enterprise features, such as advanced role-based administration, policy summaries and synchronization with multiple different directory solutions. Outbound malware detection lacks severity indicators to enable prioritized remediation.
- The solution does not offer dynamic classification of uncategorized URLs.

Trustwave-M86 Security

In March 2012, Trustwave, based in Chicago, acquired M86 Security. Trustwave offers a diversified security portfolio, although its primary focus is as a PCI Qualified Security Assessor (QSA) and managed service company. Trustwave states that it will continue to sell M86 products and begin to offer SWG managed services. Trustwave needs to more clearly define its strategy for M86 and highlight how it will target highly security-conscious organizations (where M86 had been succeeding), as well as how it will focus on adding manageability features that strengthen its appeal to Trustwave's managed service customers. The Secure Web Gateway appliance is a proxy-based gateway for enforcement, policy management and log collection. Reporting functionality is delivered via a separate appliance. VMware appliance versions and endpoint clients enable a hybrid cloud approach. Trustwave-M86 Security also offers a cloud service hosted on Amazon EC2. Trustwave-M86 Security is a good candidate for security-conscious organizations.

Strengths

- Trustwave-M86 Security has strong real-time malware detection capabilities for detecting new and targeted threats. The solution can simulate client rendering to reveal complex attacks.
- 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 websites.
- Trustwave-M86 Security provides an innovative offering that allows customers to create a custom YouTube portal that is limited to authorized content.

Cautions

- The Secure Web Gateway lacks some advanced features, such as detailed infected-machine reporting, dynamic URL classification, bandwidth control, advanced application control and trending dashboards.
- The general appearance and navigation are inconsistent across gateway and reporting interfaces. Administrator roles and rights are not centralized.

- The Trustwave-M86 Security hybrid solution does not utilize a multitenant cloud offering. Instead, customers must deploy virtual servers in a cloud environment. Cloud choices include Amazon EC2, Trustwave-M86 Security's managed service or the customer's private cloud.
- M86's market share over the past five years has been flat in a rapidly growing market.

Websense

Websense, based in San Diego, offers a wide range of options in the SWG market. Its on-premises solutions include a URL-filtering-only service, as well as software-based and appliance-based SWGs that are commonly implemented as proxies. Websense also offers a cloud-based SWG service and a cloud-based email service. Websense owns DLP technology, which it offers as a stand-alone solution, and as an embedded option with its appliance-based Web Security Gateway (WSG) offering and its cloud-based WSG. Websense is a very good candidate for most enterprise customers.

Strengths

- Websense solutions may be deployed on a wide range of platforms, including software appliances and its own hardware appliances, the V5000, V10000 and the X10G (its new blade chassis introduced in 2012). In addition to being implemented as proxies, Websense solutions can also be deployed as SPAN or TAP connections on a LAN switch, as well as on numerous third-party network hardware platforms (for example, firewalls and proxies).
- Malware detection and prevention are embedded in all WSG products. The company uses its Advanced Classification Engine (ACE) technology for real-time browser code scanning, signature-based malware detection and traffic pattern analysis (based on input from its Network Agent sensors).
- The Network Agent component analyzes all traffic on a network segment, which enables Websense to monitor non-HTTP traffic for malware detection and application recognition. This feature can be used to set and enforce policies for P2P applications and other undesirable traffic. Network agents may be deployed on multiple LAN segments to gain broader visibility into network traffic.
- Websense has a strong offering for organizations interested in a hybrid SWG strategy (on-premises and cloud-based). Its Triton management console provides a common point for policy management and reporting in hybrid environments. The company offers a "single SKU" hybrid pricing model. Customers can purchase a single license, and implement it in a "mix and match" scenario (on-premises or cloud-based users).
- A focus on DLP has differentiated Websense from its competitors. For an additional charge, DLP modules run integrated ("on box") on Websense hardware and software appliances. Websense also uses the deep packet inspection capabilities of its DLP technology to inspect outbound traffic for malware behavior (this feature does not require a DLP license).

Cautions

- Not all of the data centers in Websense's cloud-based SWG offering support multitenant VPN access, an important feature for supporting mobile users. Also, the distribution channel for its cloud service would benefit from more ISP and MSSP partners.
- Competition from lower-cost URL-filtering providers and from alternative DNS-based Web-filtering services (for example, OpenDNS) is threatening the company's installed base in the K-12 market and in SMB environments. Approximately 20% of Websense's revenue is from its legacy URL-filtering service in these markets.
- Several Websense customers reported issues with its service and support. The complaints were from customers with a basic support package. Customers that purchased Websense's premium support offering appear to be satisfied.

Zscaler

Zscaler (based in San Jose, California) is a pure-play provider of cloud-based SWG services. The company is the fastest-growing vendor in this analysis, albeit as a startup vendor. The company earned the strongest score in Completeness of Vision due to a highly scalable cloud-based proxy and logging system that delivers strong content inspection and log consolidation and storage capabilities. Its cloud service has the largest global footprint for SWG vendors, with a total of 47 globally distributed enforcement nodes. It also allows for "private node" and "private cloud" deployments. Zscaler is a very good candidate provider for most enterprises.

Strengths

- Zscaler has strong reporting capabilities, which enable drill-down into detailed analysis. The dashboard has a unique "compared with 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.
- Zscaler has several methods for redirecting endpoints to the service. It was the first vendor to offer authenticated redirection to the cloud without a software client. It also offers a client-based redirection agent for higher security on unmanaged devices and VPN redirection for mobile devices (iOS and Android). Its support for SAML enables single sign-on.
- The company offers granular security controls. SSL support is a default option, unlike some other cloud-based services where, due to performance concerns, it must be selectively enabled. Zscaler also provides several advanced security checks, including page analysis and script analysis. Unsupported browsers, browser versions or plug-ins can be blocked according to policy.
- Zscaler provides flexible policy-based controls of social media and Web-based applications, such as IM, blogs, streaming media and Web mail. It also supports bandwidth control.

Cautions

- Compared with its larger competitors, Zscaler has only a limited number of dedicated malware researchers.
- Although Zscaler 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 management interface is missing full customization of dashboard elements. DLP capability is still limited and could be improved with more predefined content and workflow.
- Zscaler's approach to 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, will not be forwarded to the Zscaler network on clients that rely on PAC files.
- Generic Routing Encapsulation (GRE) tunnels, the most commonly deployed technique to redirect traffic to the Zscaler cloud, are not supported on some common network devices (for example, Cisco's ASA firewall). Zscaler does support other redirection options.

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.

Added

- EdgeWave, formerly known as St. Bernard Software, has added new security features and now meets our inclusion criteria.

Dropped

- The following vendors did not meet the revenue threshold as outlined in the Inclusion Criteria section below (this criterion was added in 2012):
  - Clearswift
  - Cymphonix
  - Webroot
- Actiance has repositioned the company to focus on social media and Web 2.0 application control.
- SafeNet has repositioned the company to focus on its data protection products for the data center and for cloud and virtualized environments

Other Vendors That We Considered

- 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. Microsoft will 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.

Inclusion and Exclusion Criteria

Inclusion Criteria

This Magic Quadrant analyzes solutions that are optimized for SWG functionality. Vendors must meet these criteria to be included:

- Provide all three components of a secure Web gateway (see below), and own the technology for at least one of these components. Other components may be licensed from an OEM:
  - URL filtering
  - Anti-malware protection
  - Application control capabilities
- Classify English-language websites into URL categories.
- Generate at least $10 million in SWG product revenue in the latest fiscal year.

Exclusion Criteria

The following categories of vendors have been excluded from this Magic Quadrant:

- UTM and next-generation firewall vendors. These solutions are optimized for port/protocol filtering, and lack the content analysis focus of SWG offerings.
- URL-filtering-only vendors that lack malware detection capabilities.

- Vendors that license complete SWG products and services from other vendors. For example, ISPs and other service providers that "white label" cloud-based SWG services from other vendors.

Evaluation Criteria

Ability to Execute

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

- **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.

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 2012)

Completeness of Vision

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

- In the evaluation of market understanding, we ranked vendors on the strength of their commitment to the SWG market in the form of strong product management, their vision for the SWG market and the degree to which their road maps reflect a solid commitment of resources to achieve that vision.
- In the evaluation of offering (product) strategy, 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 of uncategorized sites and pages, and the categorization of search results — were considered.
  - **Application control:** Granular, policy-based control of Web-based applications — such as IM, multiplayer games, Web storage, wikis, P2P, public voice over IP (VoIP), blogs, data-sharing portals, Web backup, remote PC access, Web conferencing, chat and streaming media — is still immature in most products and represents a significant differentiator. 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, SSL termination capabilities, and interoperability with third-party antivirus and content-aware DLP scanners (for example, 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, VPN, GRE tunnels, proxy chaining and other approaches) and authentication options (for example, support for SAML).

- **Related investments:** We gave minor credit to vendors with related investments, such as email integration and native content-aware DLP capability. Native DLP capability shows technical prowess and can be useful in tactical situations; however, integration with email 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.

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	Low

Source: Gartner (May 2012)

Quadrant Descriptions

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 or 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.

Context

When selecting an SWG vendor, plan to phase in multiple security functions over time. Beyond the common requirements of URL filtering and reporting, most enterprises have an immediate need to enhance their protection from malware. Gartner's survey data and inquiry trends indicate that support for mobile workers (mainly via cloud-based services), application control and DLP are functions that many enterprises will add in 2013 and 2014. The market is far from mature, and

vendor support for these advanced features varies widely. Enterprises should prioritize future SWG requirements and develop in-house expertise in those areas to identify the vendors whose road maps most closely match their needs.

Market Overview

The secure Web gateway market continues to evolve rapidly and is marked by large differences in the quality of malware detection, cloud services and hybrid functionality (integration of on-premises equipment with cloud-based services). The quality of DLP support and application recognition, which are secondary SWG features that are requested less often by customers, also varies widely in today's market. The dynamic threat environment and the complexity of supporting diverse mobile devices pose great challenges to the vendors and are key reasons why the market will remain highly differentiated through at least 2015.

Vendors offer a wide range of capabilities for malware detection. Solutions at the lower end of the spectrum rely heavily on open-source signatures (for example, ClamAV). Solutions at the higher end of the spectrum use advanced techniques, such as sandboxing and real-time code scanning. The majority of vendors fall into a middle category, where vendors license signatures and data from multiple sources to assist in malware detection. Antivirus engines, reputation data, and lists of known botnet command and control IP addresses are common examples of the components that are often used by vendors in this middle category.

Mobility support remains a work-in-progress. Corporate policies for protecting company-owned laptops are well-defined. Companies with above-average levels of security consciousness redirect Web traffic from laptops to a cloud-based SWG service. When the company owns the laptop, it doesn't need to get permission from the employee to redirect Web traffic to the security cloud. The company either installs an agent on the laptop, or it can use an agentless (cookie-based) approach. Employee-owned tablets and smartphones present a different challenge. Most companies still don't have formal bring your own device (BYOD) policies, and they have yet to mandate agents, special-purpose browsers and other approaches for redirecting traffic to the security cloud. Differences in mobile operating systems further complicate the traffic redirection challenge and have resulted in widespread differentiation among cloud vendors for mobile support. Organizations that anticipate the need to protect mobile endpoints of all varieties (laptops, tablets and smartphones) need to press vendors for road map plans.

Cloud-based SWG services continue to be a disruptive force in the market. The early days of cloud adoption were driven primarily by SMBs, but now, large enterprises are also moving to the cloud, particularly those with many remote offices. These organizations cite bandwidth savings from providing direct Internet access, instead of backhauling traffic over Multiprotocol Label Switching (MPLS) links, as a key driver for embracing cloud services. Another key driver for cloud adoption is the protection afforded to mobile workers while they are off the corporate network.

Although cloud services have grown rapidly, many enterprises prefer to stay with the traditional approach of on-premises SWG solutions. Gartner estimates that, in 2011, revenue from on-premises solutions contributed 87% of the SWG market revenue. Privacy concerns continue to be

an obstacle to cloud adoption, particularly from large multinational companies that are uneasy about the possibility that sensitive log data may be stored in foreign countries.

Recommended Reading

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

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

"Analyze Secure Web Gateway Pricing Models to Negotiate a Favorable Contract"

"A Buyer's Guide to Secure Web Gateways"

"Introducing the Secure Web Gateway"

"Pros and Cons of SaaS Secure Web Gateway Solutions"

Acronym Key and Glossary Terms

BYOD	bring your own device
DLP	data loss prevention
ePO	ePolicy Orchestrator
GRE	Generic Routing Encapsulation
GUI	graphical user interface
HTTP/S	HTTP over SSL
ICAP	Internet Content Adaptation Protocol
IP	Internet Protocol
MSSP	managed security service provider
PAC	proxy autoconfiguration
P2P	peer-to-peer
QoS	quality of service
SMB	small and midsize business
SPAN	switch port analyzer
SSL	Secure Sockets Layer
SWG	secure Web gateway
TAP	test access point
UTM	unified threat management
VoIP	voice over IP

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.

Regional Headquarters

Corporate Headquarters
56 Top Gallant Road
Stamford, CT 06902-7700
USA
+1 203 964 0096

Japan Headquarters
Gartner Japan Ltd.
Atago Green Hills MORI Tower 5F
2-5-1 Atago, Minato-ku
Tokyo 105-6205
JAPAN
+ 81 3 6430 1800

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

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

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