Magic Quadrant for Secure Web Gateways

28 May 2013 ID:G00249600

Analyst(s): Lawrence Orans, Peter Firstbrook

VIEW SUMMARY

Malware detection and cloud services are two areas of continuing disparity among SWG vendors. Our market analysis of the vendors highlights key differences in these capabilities and other key functions.

Market Definition/Description

Secure Web gateways (SWGs) utilize URL filtering, malware detection and application control technology to protect organizations and enforce Internet policy compliance. SWGs are delivered as on-premises appliances (hardware and virtual) or cloud-based services.

We estimate that the combined SWG revenue of the Magic Quadrant participants in 2012 was $1.18 billion (which includes on-premises and cloud-based offerings). Revenue from solutions that lack full SWG functionality has been excluded (for example, URL filtering only or proxies sold without anti-malware protection). The market grew approximately 15% over 2011, which is in line with our estimate from the 2012 report. We anticipate that the market will grow 13% to 15% in 2013.

Eight of the 13 vendors in this analysis now offer a multitenant cloud service. However, the market is still dominated by on-premises solutions (86% share, based on revenue), with SWG as a service representing the remainder of the market (14%). Gartner's market share and growth rate estimate of the broader market for SWG proxy and URL filtering software can be found in "Market Share: Security Software, Worldwide, 2012."

The market is segmented between large enterprises and small or midsize businesses (SMBs). SMB solutions are designed for ease of use, cost-effectiveness and basic security protection. Large enterprise solutions protect against more-advanced threats, including the capability to detect targeted attacks.

Vendors are increasingly integrating content-aware data loss prevention (DLP) to monitor sensitive data. Cloud services are being driven by the need to protect mobile devices and secure remote-office connections.

Return to Top

Magic Quadrant

Figure 1. Magic Quadrant for Secure Web Gateways

ACRONYM KEY AND GLOSSARY TERMS

BYOD	bring your own device
DLP	data loss prevention
EPP	endpoint protection platform
ICAP	Internet Content Adaptation Protocol
IP	Internet Protocol
IPS	intrusion prevention system
NAC	network access control
PAC	proxy autoconfiguration
SaaS	software as a service
SIEM	security information and event management
SMB	small or midsize business
Span	Switched Port Analyzer
SSL	Secure Sockets Layer
SWG	secure Web gateway
TAP	test access point
UTM	unified threat management
VAR	value-added reseller

EVALUATION CRITERIA DEFINITIONS

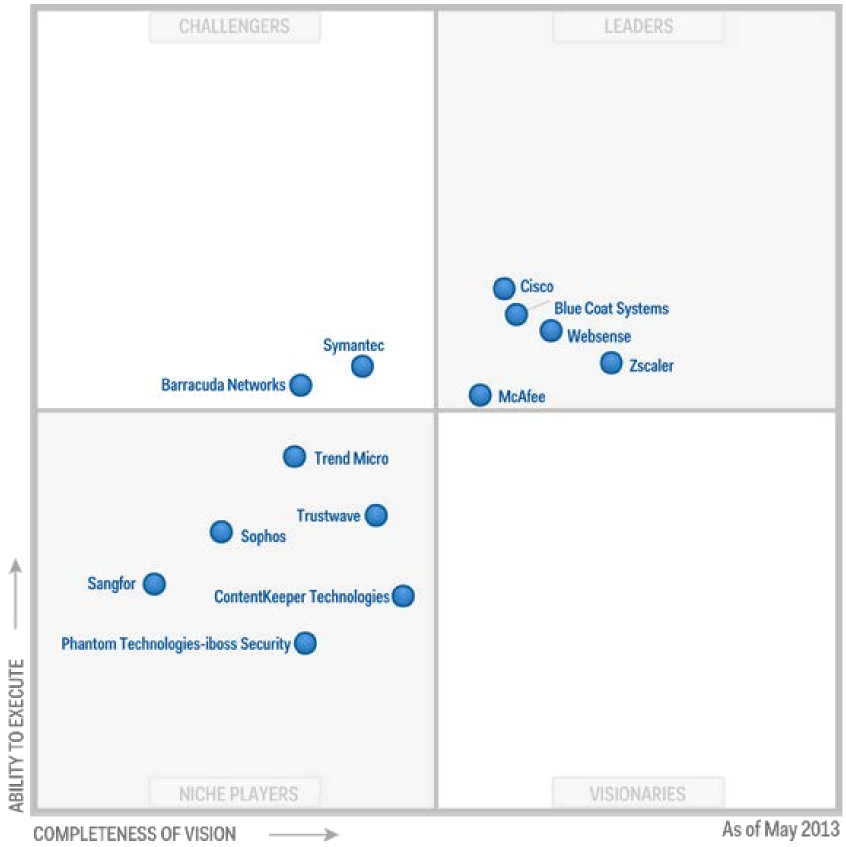
Ability to Execute

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



Source: Gartner (May 2013)

▲ Return to Top

Vendor Strengths and Cautions

Barracuda Networks

Barracuda Networks, which is based in Campbell, California, offers the Barracuda Web Filter appliance (hardware and virtual) and the cloud-based Barracuda Web Security Service. Barracuda customers typically implement its appliances in transparent bridge mode to view all network traffic, but the appliances can also be implemented in proxy mode. Barracuda Web Filter appliances are good candidates for SMBs and selected large enterprises (especially in the education and government vertical industries), particularly those that are budget-constrained.

Strengths

- Barracuda offers a low-cost solution that is easy to use with very competitive functionality.
- A partnership with Malwarebytes provides malware cleanup capabilities that can be initiated from the gateway.
- Application controls provide heuristic detection across all ports and protocols, with optional endpoint agents or in-line deployments.
- Social media controls, including optional archiving capabilities, are very complete.
- For mobile users, Barracuda offers several options for traffic redirection and authentication, including endpoint agents for recent versions of Windows and Mac OS X, and a safe browser option for Apple iOS.

Cautions

- Barracuda does not offer a choice of antivirus engines. Open-source ClamAV is the only option. Barracuda adds internally developed signatures, although its malware research team is relatively small.
- The Barracuda Web Filter appliance lacks dynamic URL categorization.
- Some enterprise-class capabilities for management and reporting are absent. For example, the dashboard is not customizable, and it only provides limited drill-down into logs or reports.
- The cloud-based service is also missing a number of enterprise features. For example, it lacks IPsec support for traffic redirection, and it requires an authentication appliance for directory integration.

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.

Return to Top

Blue Coat Systems

Blue Coat is in its second year as a privately held company, after private equity firm Thoma Bravo acquired it in February 2012. In December 2012, Blue Coat acquired Crossbeam Systems, a blade-server platform that integrates firewall, intrusion prevention system (IPS) and other security components. Blue Coat plans to port its SWG solution to the Crossbeam platform (no set date has been provided), and will continue to offer its dedicated hardware appliances and virtual appliances. The company also operates a cloud-based SWG service. In May 2013, Blue Coat acquired the SSL appliance product line from Netronome. Also in May 2013, Blue Coat announced its intent to acquire Solera Networks. Blue Coat is a very good candidate for most large enterprise customers.

Strengths

- Blue Coat's ProxySG remains the strongest proxy in the market in terms of breadth of protocols and the number of advanced features. It supports a long list of protocols (including SOCKS), extensive authentication and directory integration options, and the Online Certificate Status Protocol (OCSP).
- Blue Coat's cloud offering includes multitenant IPsec gateways, which enable it to support a wide range of mobile devices. Blue Coat agents are available for Windows, Mac OS X and Apple iOS.
- Blue Coat provides some integrated features with its cloud and on-premises solutions. Its Unified Reporting feature allows logs from the cloud service to be rolled up into an on-premises Blue Coat Reporter console. Its Unified Policy feature allows policy developed in the cloud to be synchronized with its on-premises appliances.
- Blue Coat offers strong reporting capabilities for its on-premises and its cloud-based services. Both solutions provided multiple canned reports and the ability to create custom reports.

Cautions

- The ProxySG appliance lacks on-box malware detection. Customers that want antivirus engine protection must purchase a separate appliance (ProxyAV). Malware protection is also provided by Blue Coat's "cloud assist" WebPulse service.
- The ProxyAV lacks advanced malware techniques, such as code emulation. Instead, it utilizes signature-based detection delivered by Blue Coat partners (a choice of four antivirus engines).
- 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.
- 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.

Return to Top

Cisco

Cisco, which is based in San Jose, California, offers an appliance-based SWG and a cloud-based SWG service. In 2012, Cisco rebranded these solutions. The appliance-based product is now named Web Security Appliance (formerly IronPort) and the cloud-based service is now named Cloud Web Security (formerly ScanSafe). The Web Security Appliances (WSAs) are implemented as proxies.

In February 2013, Cisco acquired Cognitive Security, a startup company based in the Czech Republic. Cognitive analyzes NetFlow traffic and other data to detect advanced threats. Cisco plans to utilize Cognitive's technology in its Security Intelligence Operations, a threat and vulnerability analysis center that distributes security updates and reputation data to a range of Cisco products and services, including its SWG offerings.

Cisco's WSA products are very good candidates for most midsize and large enterprises, while the Cloud Web Security service is a good candidate for all enterprises.

Strengths

- Cisco has integrated a traffic redirection feature — a critical component of any cloud service — into some of its on-premises equipment. The ASA firewall, ISR G2 router and WSA all support Cisco's "connector" software, which directs traffic to the Cloud Web Security service. The configuration is enabled via a menu item on these appliances.
- Cisco provides several options for authenticating users to the Cloud Web Security service, including SAML. The connector implementations (noted above) also transport user credentials to the cloud.
- Mobile support is a strength of Cisco's cloud offering. The AnyConnect client supports Windows, OS X, Apple iOS, Android, Windows Phone 8 and BlackBerry. However, Cisco's cloud lacks support for IPsec, which is widely supported on mobile devices.
- In addition to Cisco's reputation database, the WSA provides three choices for on-box signature databases (McAfee, Sophos and Webroot), all of which can be supported simultaneously.

Adaptive scanning utilizes the anti-malware engine that is best suited for the content type.

- Cisco provides a very granular application control capability. The Cisco appliance includes a Switched Port Analyzer (Span) port to monitor and block outbound malicious traffic that evades the proxy.

Cautions

- Reports and dashboards do not provide sufficient information on outbound malware detection to enable prioritized remediation.
- Some customer references noted that reporting could be improved. Advanced reporting requires a Cisco version of Splunk at an extra cost.
- Cisco lacks a unified management console for its on-premises WSA appliances and its Cloud Web Security service to ease the management of hybrid deployments.
- Some customer references highlighted that Cisco needs to improve its Content Security Management Appliance's ability to centrally manage and control individual proxies.

▲ Return to Top

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 deploys in transparent bridge mode, and it also offers a hosted cloud-based service. In 2012, ContentKeeper opened a new office in North America in Orange Country, California. It also rebranded its family of appliances with the names Web Filter Pro and ContentKeeper Secure Internet Gateway (CK-SIG). ContentKeeper is a candidate for K-12 schools and for most enterprise customers.

Strengths

- The Behavioral Analysis Engine (a feature of CK-SIG) provides real-time and near-real-time analysis of Web objects using browser code emulation.
- ContentKeeper has developed "sandboxing" technology to analyze suspicious files and executables in a virtualized Windows environment. The solution produces detailed reports for each item that is analyzed. The sandboxing technology can be configured as a hosted service, or it can be run locally on an appliance. It comes as a standard feature in CK-SIG and may also be configured as a feature of Web Filter Pro.
- A bring your own device (BYOD) feature enables Web Filter Pro and CK-SIG to enforce access policies for mobile devices and users. Policies could include blocking Internet access or blocking applications (by filtering network traffic). Agents are available for off-network mobile devices. Supported operating systems include Windows, OS X, iOS, Linux and Android.
- ContentKeeper appliances support the ability to proxy and analyze Secure Sockets Layer (SSL) traffic. Antivirus protection and basic IPS are provided through a combination of third-party and internally developed signatures.

Cautions

- ContentKeeper lacks a shared, multitenant, cloud-based SWG service. It provides a hosted cloud offering, where customers run virtual appliances hosted in Amazon's cloud service (and some ContentKeeper-managed data centers). Hosted offerings are not as flexible (for example, dynamic ability to scale) as shared multitenant clouds.
- While the vendor has made good progress in developing malware detection tools, these solutions are new, and ContentKeeper has yet to earn recognition as a leading malware research and product company. Prospective customers should carefully test ContentKeeper's anti-malware capabilities.
- Some customer references requested improvements to the solution's graphical user interface (GUI). In January 2013, ContentKeeper released an updated interface, although the console still lacks malware severity indicators for enabling prioritized remediation.

▲ Return to Top

McAfee

McAfee, a subsidiary of Intel, offers a family of on-premises SWG appliances (McAfee Web Gateway [MWG]) and a cloud-based SWG service (SaaS Web Protection). The SWG appliances are most commonly implemented as proxies, although they can be deployed in other modes, including in-line transparent bridges. In February 2013, McAfee announced its acquisition of ValidEdge, which makes a sandboxing appliance for detecting advanced malware and targeted attacks. McAfee's solutions are good candidates for most enterprise customers, particularly those that are already McAfee ePolicy Orchestrator users.

Strengths

- MWG has strong malware protection due to its on-box browser code emulation capabilities. The solution provides the ability to adjust the sensitivity of malware detection. A rule-based policy engine enables flexible policy creation.

- The SaaS Web Protection cloud service supports SAML for authenticating users.
- McAfee has integrated DLP technology across its product lines. MWG ships with a number of preformatted dictionaries.
- Application control is very strong. HTTP manipulation allows organizations to remove selected functions from Web applications (for example, blocking posts to social media sites).
- 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

- The SaaS Web Protection cloud service is missing an important traffic redirection option by not supporting IPsec.
- McAfee's mobility strategy needs improvement. It does not offer an endpoint client for Mac OS X. Its McAfee Client Proxy for Windows is a strong solution, but it has been late to support Windows 8 (a June 2013 release is planned). The lack of IPsec support in the cloud is also an impediment to supporting mobile devices.
- The cloud solution does not have the same level of policy granularity that is available with the on-premises appliance.

▲ **Return to Top**

Phantom Technologies-iboss Security

Phantom Technologies is a privately held company based in San Diego. It offers a family of appliance-based platforms (iboss) that is typically deployed in transparent bridge mode. It also offers a cloud-based URL filtering solution for mobile users. Phantom is a candidate for organizations that are based in North America (more than 90% 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 industry). For example, the iboss SWG Web filter enables schools to easily allow access to YouTube's educational site, while blocking access to the main YouTube site.
- Full SSL content inspection is provided utilizing an agent-based solution on endpoints. This is a scalable approach that relieves the iboss appliance of the burden of managing certificates, and of terminating and decrypting SSL traffic.
- 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.
- The iboss appliance uses DLP technology to identify high-risk behavior.
- Iboss includes a unique autorecord feature (up to three minutes) that enables a playback for a sequence of events. This feature is often used to confirm intentional versus unintentional user violations.

Cautions

- Phantom's cloud offering is limited to URL filtering decisions. It lacks a multitenant cloud-based service that analyzes traffic and Web objects to detect malware. An on-premises appliance is required to handle policy management and reporting.
- 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).
- Uncategorized URLs are not classified in real time.

▲ **Return to Top**

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. The company offers two versions of its SWG product: one aimed at the Chinese market, and one aimed at English-speaking countries. Nearly all the company's revenue comes from the Asia/Pacific region. Sangfor is a candidate for organizations that are based in China and in supported countries in the Asia/Pacific region.

Strengths

- Sangfor has strong application control features. It can apply granular policies to Facebook and other Web-based applications, and it has also developed network signatures to block port-evasive applications like BitTorrent and Skype.
- Sangfor's in-line transparent bridge mode enables flexible and granular bandwidth control

DOCKET ALARM

Explore Litigation Insights

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

Real-Time Litigation Alerts

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

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

Advanced Docket Research

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

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

Analytics At Your Fingertips

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

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

API

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

LAW FIRMS

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

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

FINANCIAL INSTITUTIONS

Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS

Sync your system to PACER to automate legal marketing.

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

fastcase®
Smarter legal research.