Magic Quadrant for Secure Web Gateways

23 June 2014 ID:G00262738

Analyst(s): Lawrence Orans, Peter Firstbrook

VIEW SUMMARY

The SWG market is evolving rapidly as vendors respond to the mobility trend and the evolving threat landscape. SWG vendors are highly differentiated in their ability to deliver cloud-based services, and to protect users with advanced threat defense features.

Market Definition/Description

Secure Web gateways (SWGs) utilize URL filtering, advanced threat defense, legacy malware protection and application control technologies to defend users from Internet-borne threats, and to help enterprises enforce Internet policy compliance. SWGs are delivered as on-premises appliances (hardware and virtual) or cloud-based services. Vendors differ greatly in the maturity and features of their cloud-based services, and in their ability to protect enterprises from advanced threats.

The vast majority of enterprises still implement SWGs as on-premises appliances. Gartner estimates that, in 2013, 77% of SWG implementations were on-premises and 23% were cloud-based. Comparing these values to those from 2012 (86% on-premises and 14% cloud) indicates that cloud-based services are growing more quickly than on-premises appliances. Despite the rapid growth in cloud adoption, and the inevitable need to protect laptops and mobile devices as users bypass the corporate network to go directly to the Internet, the market for cloud-based SWG services is far from mature. Vendor differentiation remains high in key areas of cloud services, such as global coverage (number of countries and data centers), support for mobile operating systems and the ability to deliver hybrid (cloud and on-premises) implementations. In the Vendor Strengths and Cautions section below, the write-ups for each vendor highlight key characteristics of cloud-based support.

The evolving threat landscape has forced SWG vendors to respond by adding technologies to defend against advanced threats. There are several techniques for combating advanced threats (see "Five Styles of Advanced Threat Defense"), and sandboxing has emerged as the most commonly implemented approach by SWG vendors in 2013 and 2014. Some have implemented sandboxing with separate on-premises appliances, whereas others have taken a cloud-based approach. SWG vendors have added sandboxing by developing it internally, by licensing technology from OEM providers or by acquiring a sandbox vendor. In the Vendor Strengths and Cautions write-ups below, we analyze each vendor's approach to sandboxing and advanced threat defense.

Magic Quadrant

Figure 1. Magic Quadrant for Secure Web Gateways

EVALUATION CRITERIA DEFINITIONS

Ability to Execute

Product/Service: Core goods and services offered by the vendor for the defined market. This includes current product/service capabilities, quality, feature sets, skills and so on, whether offered natively or through OEM agreements/partnerships as defined in the market definition and detailed in the subcriteria.

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

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

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

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

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

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

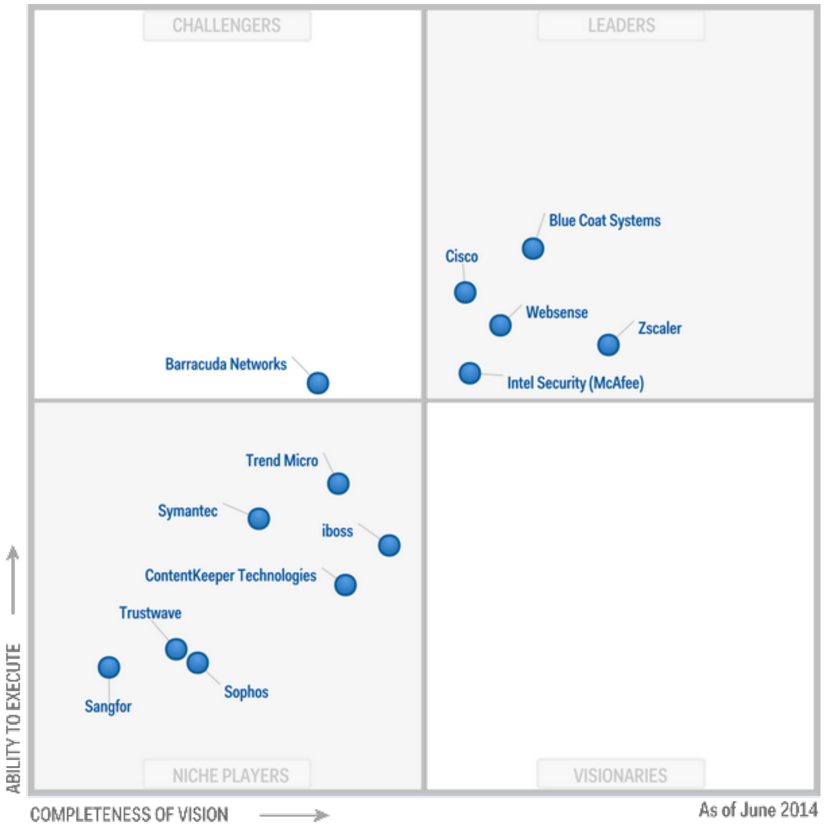
Completeness of Vision

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

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

Sales Strategy: The strategy for selling products that uses the appropriate network of direct and indirect sales, marketing, service, and communication affiliates that extend the scope and depth of market reach, skills, expertise, technologies, services and the customer base.

Offering (Product) Strategy: The vendor's approach



Source: Gartner (June 2014)

Vendor Strengths and Cautions

Barracuda Networks

Barracuda offers the Barracuda Web Filter appliances 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. In 2013, Barracuda gained a new CEO; later that November, it launched an initial public offering (IPO) and became a publicly traded company. In 2014, Barracuda agreed to license Lastline's cloud-based sandbox technology. Barracuda Web Filter appliances are good candidates for small or midsize businesses (SMBs) and cost-conscious enterprises.

Strengths

Barracuda offers a low-cost solution that is easy to use with competitive functionality. The vendor's Instant Replacement program, which provides next-business-day shipping of replacement units, includes a free appliance replacement unit every four years.

Application control is strong. In-line deployments of Barracuda's SWG enable it to filter all ports and protocols. Features include granular social media controls and social media archiving.

Barracuda provides a free, lightweight mobile data management (MDM) capability to simplify the management of policies on mobile devices running Apple iOS and Android.

Partnerships with wireless vendors Meru and Ruckus Wireless enable single sign-on (SSO). When a user authenticates to a Ruckus or Meru access point, the user's credentials are shared with the Barracuda SWG. The user's activity can be monitored on the Internet, without requiring the user to authenticate directly to Barracuda's SWG.

Cautions

The cloud-based service is missing a number of enterprise features. For example, it lacks IPsec support for traffic redirection, and it does not inspect Secure Sockets Layer (SSL) traffic.

Barracuda's integration with Lastline is in its initial phases, and is not yet tightly integrated. The initial integration lacks the ability to defend against targeted attacks (although it does improve Barracuda's ability to defend against zero-day threats).

Barracuda's advanced threat defense strategy is heavily dependent on the technology that it has licensed from Lastline, which is a small company. If Lastline's status changes, then Barracuda may need to revisit its advanced threat strategy.

Blue Coat Systems

Blue Coat was acquired by private equity firm Thoma Bravo in February 2012. Since the acquisition, Blue Coat acquired several security companies, including Netronome (SSL appliances) in May 2013,

to product development and delivery that emphasizes differentiation, functionality, methodology and feature sets as they map to current and future requirements.

Business Model: The soundness and logic of the vendor's underlying business proposition.

Vertical/Industry Strategy: The vendor's strategy to direct resources, skills and offerings to meet the specific needs of individual market segments, including vertical markets.

Innovation: Direct, related, complementary and synergistic layouts of resources, expertise or capital for investment, consolidation, defensive or pre-emptive purposes.

Geographic Strategy: The vendor's strategy to direct resources, skills and offerings to meet the specific needs of geographies outside the "home" or native geography, either directly or through partners, channels and subsidiaries as appropriate for that geography and market.

Solera Networks (full packet capture for network forensics) in May 2013 and Norman Shark (appliance-based sandbox) in December 2013. Blue Coat also introduced the Content Analysis System (CAS), an internally developed malware detection appliance that analyzes traffic forwarded to it by Blue Coat's ProxySG. In addition to its appliance-based offerings, Blue Coat offers a cloud-based SWG service. Blue Coat's appliances are good candidates for most large-enterprise customers, particularly those requiring highly scalable SWGs. Blue Coat's cloud service is a good option for most enterprises.

Strengths

The ProxySG is the strongest proxy in the market in terms of breadth of protocols and the number of advanced features. It supports a broad set of protocols as well as extensive authentication and directory integration options.

Blue Coat has made good progress in integrating the products that it has acquired. For example, its CAS can automatically deposit suspicious files in the Malware Analysis Appliance (sandbox). The CAS also integrates with FireEye's Web Malware Protection System (MPS; however, the CAS does not yet integrate with FireEye's NX series, which is the updated version of the MPS).

The Security Analytics solution (Solera Networks technology) integrates with the Malware Analysis Appliance (Norman Shark technology) and provides a forensic analysis of packets associated with a suspicious file.

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, Apple iOS and Android.

Cautions

Because Blue Coat's advanced threat defense solution requires multiple components, it is expensive. The ProxySG does not deposit suspicious files in the Malware Analysis Appliance. Customers must purchase the CAS if they want to automatically detect suspicious files and analyze them in the Malware Analysis Appliance.

Blue Coat's hybrid implementation of its cloud and on-premises offerings is incomplete. Policy synchronization is not bidirectional (it supports synchronization only from the cloud to on-premises appliances). Downloading logs from the cloud to on-premises appliances can be scheduled only hourly.

Blue Coat's Reporter application lacks severity indicators for prioritizing alerts.

Cisco

Cisco offers the appliance-based Web Security Appliance (WSA) and the cloud-based Cloud Web Security (CWS) service. The WSAs are implemented as proxies. In October 2013, Cisco completed its acquisition of Sourcefire; in May 2014, it announced its intent to acquire ThreatGRID, whose primary offering is a cloud-based sandboxing service. In February 2014, Cisco announced its cloud-based Cognitive Threat Analytics (CTA) feature, based on technology from its acquisition of Cognitive Security in February 2013. Cisco's WSA products are good options for most midsize and large enterprises, while the CWS service is a good option for most 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, Integrated Services Router (ISR) Generation 2 and WSA all support Cisco's "connector" software, which directs traffic to the CWS service. Traffic redirection is enabled via a menu item when configuring these appliances.

Mobile platform support is a strength of the CWS service for customers that have already implemented Cisco's popular AnyConnect client. The cloud service supports Windows, Mac OS X, Apple iOS, Android, Windows Phone 8 and BlackBerry.

Sourcefire's Advanced Malware Protection (AMP) technology is available as an option on Cisco's WSA and CWS service (separate license fees apply).

Cisco's intended acquisition of ThreatGRID and its sandboxing technology will complement the file-based advanced threat defense technology that it acquired from Sourcefire. Gartner expects that Cisco will integrate the WSA with a ThreatGRID-based appliance (but not before 2015), so that suspicious files can be further analyzed in a sandbox environment. The combination of file-based and sandboxing technologies should reduce false positives and improve the accuracy of malware and advanced threat detection.

Cautions

Cisco has been slow to integrate its cloud-based SWG (ScanSafe acquisition of 2009) with its on-premises SWG (IronPort acquisition of 2007). Customers seeking a hybrid cloud/on-premises solution will need two consoles. The consoles lack policy synchronization (to share policies between cloud and on-premises users). Log synchronization is not configurable by the customer, but on customer request, Cisco can automate log synchronization up to four times per day.

The CTA capability is not available to WSA customers. Only CWS customers can utilize the CTA functionality.

Getting maximum value from AMP requires implementing FireAMP Connector agents on network endpoints. The FireAMP Connectors are optional, but without them, the AMP-integrated SWG provides reduced monitoring and investigative functionality.

Cisco's cloud service has a surprisingly small global footprint (15 countries), given Cisco's resources and the number of years it has been in the SWG market. Newer rivals have been more aggressive in global expansion. The cloud service also lacks support for IPsec.

ContentKeeper Technologies

ContentKeeper Technologies is based in Australia, where it has many large government, education and commercial customers. It offers a family of SWG appliances that deploy in transparent bridge mode, and it also provides a hosted cloud-based service. ContentKeeper's advanced threat solutions can be implemented on-premises or in its hosted cloud service. ContentKeeper is a good option for midsize and large organizations, and for K-12 schools in supported geographies.

Strengths

ContentKeeper has developed its own sandboxing technology, which gives it control of its advanced threat defense strategy by limiting its reliance on partnerships.

A bring your own device (BYOD) feature enables ContentKeeper's SWG to enforce Internet access policies for mobile devices and users. ContentKeeper agents and mobile apps support off-network devices (such as Windows, Mac OS X, Linux, iOS and Android).

ContentKeeper appliances support the ability to proxy and analyze SSL traffic.

Cautions

ContentKeeper lacks a shared, multitenant, IPsec-based cloud SWG service. It provides a hosted cloud offering, where customers run virtual appliances hosted in Amazon's cloud service (and in some ContentKeeper-managed data centers). Hosted offerings do not scale as dynamically as shared multitenant clouds.

ContentKeeper has yet to earn recognition as a leading advanced threat defense company. Prospective customers should carefully test the efficacy of its advanced threat capabilities against competing solutions.

The lack of severity indicators on ContentKeeper's dashboard makes it difficult to prioritize malware alerts.

Outside the Asia/Pacific region, ContentKeeper has a limited value-added reseller (VAR) channel. Prospective customers should carefully vet ContentKeeper VARs to ensure that they can provide adequate local support.

iboss

iboss offers a family of appliance-based platforms that are typically deployed in transparent bridge mode. It also offers a cloud-based service. In 2014, iboss began offering a cloud-based advanced threat defense service based on technology that it has licensed from Lastline. iboss is a good option for midsize and large enterprises, and for K-12 schools in supported geographies.

Strengths

iboss has integrated its SWG with the cloud-based sandboxing service that it licenses from Lastline. The iboss SWG can automatically deposit suspicious objects in the sandbox, and the iboss management console displays the results of the analysis.

Full SSL content inspection is provided agentless at the gateway, or with an optional agent-based solution on endpoints. The agent is a scalable approach that relieves the iboss appliance of the burden of managing certificates, and of terminating and decrypting SSL traffic.

iboss provides lightweight MDM functionality that helps enterprises configure Apple iOS and Android devices to use its cloud service.

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.

Cautions

iboss' cloud service lacks IPsec support for mobile devices, which is a common requirement for mobile users (remote offices can be supported via IPsec on routers and firewalls).

iboss' advanced threat detection strategy is heavily dependent on the technology that it has licensed from Lastline, which is a small company. If Lastline's status changes, then iboss may need to revisit its advanced threat strategy.

iboss has only a limited set of customers outside North America. As it begins a planned international expansion, prospective customers outside North America should validate that iboss partners are qualified to provide sales and technical support.

Intel Security (McAfee)

McAfee, which is now part of Intel Security, offers a family of on-premises SWG appliances (McAfee Web Gateway [MWG]) and cloud-based SWG services (SaaS Web Protection). The SWG appliances are most commonly implemented as proxies, although they can also be deployed in other modes, including in-line transparent bridges. In October 2013, Intel Security announced its Advanced Threat Defense appliance, which is based on technology from its acquisition of ValidEdge in February 2013. Intel Security's solutions are good candidates for most enterprise customers, particularly those that are already 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.

MWG integrates with the Advanced Threat Defense appliance. It automatically deposits suspicious files in the sandbox for analysis.

Intel Security has a good implementation of a hybrid cloud/on-premises solution. While policy synchronization is only unidirectional (from on-premises to the cloud), flexible controls enable some policies to be synced, whereas others are not. Log file synchronization can be configured in specified time intervals.

MWG provides strong support for scanning SSL traffic. It can be configured to automatically enforce SSL certificate decisions and remove the decision from end users (who almost always accept unknown or expired certificates).

In addition to its existing data loss prevention (DLP) support, MWG also protects sensitive data stored in public clouds from unauthorized access. It can automatically encrypt files transmitted to Dropbox and other file sharing and collaboration sites, and users cannot retrieve and decrypt files without going through the MWG.

Cautions

The SaaS Web Protection service does not support an IPsec-based multitenant gateway, which is a common requirement for supporting mobile devices.

Intel Security's mobility strategy needs improvement. Its McAfee Client Proxy for Windows is a strong solution, but it does not offer an endpoint client for Mac OS X. Also, Intel Security lacks partnerships with MDM vendors to enforce IPsec tunnels (to SaaS Web Protection) on mobile devices running iOS and Android.

Intel Security's cloud service has a surprisingly small global footprint (12 data centers), given its resources and the number of years it has been in the SWG market. Newer rivals have been more aggressive in global expansion.

Sangfor

Sangfor is a network equipment vendor based in China. Approximately half of its revenue comes from its SWG products; the remaining revenue comes from its firewall, VPN, WAN optimization controllers and application delivery controller products. Sangfor's SWG comes in a hardware appliance form factor, and it is 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 of 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.

A partnership with Aruba Networks enables SSO. When a user authenticates to an Aruba wireless LAN, the user's credentials are shared with the Sangfor SWG. The user's activity can be monitored on the Internet, without requiring the user to authenticate directly to the Sangfor SWG.

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

Cautions

Sangfor's SWG appliance lacks advanced threat defense capabilities.

Mobility is a weak spot for Sangfor because it does not offer a cloud-based SWG service.

Malware detection is basic and relies on a signature-based approach. The console dashboard lacks severity indicators to prioritize malware alerts.

Sophos

Sophos has a broad range of network gateways through native development, and from its acquisitions of Astaro in 2011 and Cyberoam Technologies in 2014. The Sophos Web Appliance (SWA) can be deployed in proxy or transparent in-line bridge mode. Sophos' SWG strategy is in transition. The vendor is working on integrating its stand-alone SWA functionality into its unified threat management (UTM) appliances, and it is also planning a multitenant cloud Web filtering service.

Strengths

Ease of use is a key design criterion for Sophos. Features include automated network and directory discovery, contextual help functions, and simple policy configuration.

Mobile users who are running the Sophos endpoint protection platform benefit from its local on-device enforcement of the URL filtering policy, without having to forward requests to the cloud.

Sophos is an established player in the malware detection market. The SWA uses Sophos-developed technology to perform a pre-execution analysis of all downloaded code, including binary files and JavaScript.

Sophos places a strong emphasis on service and support. It optionally monitors customers' appliances and provides alerts for critical hardware conditions, such as high temperatures or faulty disk drives.

Cautions

The SWA should be considered a tactical solution for the near term, given Sophos' strategy to transition its SWG functionality to a new platform.

Sophos lacks a multitenant cloud-based service that analyzes traffic and Web objects to detect malware.

The SWA is not integrated with a sandbox (Sophos does not offer a sandboxing solution).

The console lacks severity indicators to prioritize malware alerts.

Symantec

Symantec has two offerings in the SWG market: (1) the Symantec.cloud service; and (2) 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. In May 2014, Symantec announced that it would deliver an advanced threat protection solution that would be "generally available within the next 12 months." Symantec also announced a road map of advanced threat services that it will deliver in 2014. Symantec moved from the Challengers quadrant in 2013 to the Niche Players quadrant this year due to its slow response to the advanced threats trend, weakness in its cloud and mobile strategy, and uncertainty associated with its interim CEO's position. Symantec's SWG offerings are good options for SMBs that do not need a hybrid approach.

Strengths

- Symantec.cloud provides strong DLP support (a separate license is required) with the ability to configure flexible policies.
- Support for multiple languages broadens Symantec.cloud's appeal in many non-English-speaking countries.
- Symantec's SWG offerings benefit from its strong malware research labs and its Insight file reputation engine.

Cautions

- Symantec has not integrated its cloud-based SWG (MessageLabs acquisition of 2008) with its on-premises SWG (Mi5 Networks acquisition of 2009). Customers seeking a hybrid cloud/on-premises solution will need two consoles. The consoles lack policy synchronization (to share policies between cloud and on-premises users) and log synchronization.
- If Symantec follows through on its plan to deliver an advanced threat solution "within the next 12 months," then it will be about one year behind its key competitors that have solutions today. The late entry limits Symantec's opportunities in large enterprises, many of which have already implemented advanced threat solutions.
- Symantec's cloud and mobile strategy needs improvement. The cloud service does not support IPsec, which is a common approach for supporting mobile devices. The Smart Connect agent is a strong solution for Windows endpoints, but it is not available for Mac OS X.
- The unresolved CEO position casts uncertainty over Symantec's strategic plans in SWGs and advanced threat defense. At the time of this writing, Symantec has an interim CEO. The company has already had three CEOs since 2012.

Trend Micro

Trend Micro offers an on-premises InterScan Web Security (IWS) solution (available as a software or virtual appliance only) and a new cloud service (InterScan Web Security as a Service, whose worldwide rollout was completed in April 2014). IWS can be implemented as a transparent bridge or a proxy. Trend Micro's Deep Discovery is an internally developed advanced threat defense solution based on sandboxing technology. It is available as a hardware appliance. Trend Micro is a candidate primarily for organizations that already have a strategic relationship with the company.

Strengths

- The IWS appliance can automatically deposit suspicious files in the Deep Discovery sandbox for analysis.
- A single console provides a simple approach for synchronizing policies for cloud and on-premises users.
- Trend Micro's Damage Cleanup Services can provide remote client remediation for known threats.
- Application control is strong with IWS, and includes the ability to set time of day and bandwidth quota policies.

Cautions

- Trend Micro's cloud-based SWG service is new and unproven. It was launched in the Asia/Pacific and Latin America regions in 4Q13, and only became generally available in North America in April 2014. Several enterprise-class features are still missing, including DLP support.
- Gartner rarely sees Trend Micro in competitive deals for SWG-only implementations.
- Logs from the cloud service cannot be automatically synchronized with logs from the IWS appliance. The cloud logs can be downloaded only manually by the customer from the Web management console.

Trustwave

Trustwave offers a diversified security product and managed services portfolio. Its Secure Web Gateway appliance (gained via the 2012 acquisition of M86 Security) is a proxy-based gateway that specializes in real-time malware detection. Trustwave's SWG solutions are good options for customers that already have one or more Trustwave products or services, or for those that are seeking an SWG managed service.

Strengths

- Trustwave has strong real-time browser code emulation, which is the primary technology in its malware detection strategy.
- Trustwave's DLP engine is fully integrated with its Secure Web Gateway.
- Social media support is strong and provides flexible controls for Facebook, Twitter, Google+,

LinkedIn and YouTube.

Cautions

- Trustwave does not offer a cloud-only SWG service. It discontinued the Trustwave Cloud Web Service in 2013, but continues to offer the Trustwave Secure Web Service Hybrid. The new service requires an on-premises policy server to synchronize with Active Directory.
- Support for mobile devices (iOS and Android) is weak due to Trustwave's lack of an IPsec-based multitenant gateway in its hybrid service offering.
- The dashboard console is weaker than many competing offerings. It lacks severity indicators to prioritize malware alerts. Dashboard panels provide only limited customization.
- The Secure Web Gateway lacks the ability to block port-evasive applications, such as BitTorrent and Skype.

Websense

Websense was acquired by private equity firm Vista Equity Partners in June 2013. In 2014, Websense began moving its headquarters from San Diego to Austin, Texas. Websense offers SWG appliances (hardware and software) and a cloud-based service. In October 2013, it announced RiskVision, an appliance that forwards suspicious files to Websense's cloud-based sandbox (known as ThreatScope). Websense appliances are good options for midsize enterprises, and its cloud service is a good option for most enterprises.

Strengths

- Websense has a strong offering for organizations that are interested in a hybrid SWG strategy (on-premises and cloud-based). Its Triton management console provides a common point for policy management, reporting and logging in hybrid environments.
- Websense's Web Security Gateway automatically deposits suspicious files in the ThreatScope cloud sandbox, which was developed in-house by Websense.
- Websense has extended its DLP technology to its cloud service. The deep packet inspection capabilities of its DLP technology are used to inspect outbound traffic for malware behavior. This feature, which was previously only available on Websense appliances, does not require a DLP license.
- The Websense cloud service supports multiple options for traffic redirection (including IPsec), and multiple options for user authentication (including SAML v2).

Cautions

- Websense's SWG product portfolio limits the vendor to a primarily midmarket customer base. Gartner estimates that the V5000 and V10000 appliances contribute approximately 95% of Websense's revenue for SWG appliances. Gartner rarely sees Websense's X10G, a blade-server appliance aimed at large enterprises, in competitive bids. Enterprises that are considering the X10G should carefully check references.
- Websense continues to experience challenges with its service and support organization, based on feedback Gartner has gathered from several Websense customers. Gartner believes that some of the support issues were the result of disruption associated with Websense's corporate relocation to Texas. Prospective customers should verify service-level agreement commitments with Websense's service and support organization.
- The console for the cloud-only service is different from Websense's Triton console, which is used to manage the hybrid and on-premises solutions. Customers that begin with a cloud-only service and add appliances later (for example, to improve responsiveness in bottleneck locations) would need to switch to the Triton console.

Zscaler

Zscaler is a pure-play provider of cloud-based SWG services. It continues to be one of the fastest-growing vendors in this market. In 2014, Zscaler introduced Shift, a cloud-based service that uses DNS to direct traffic through its cloud platform. Shift provides a subset of the security features offered in Zscaler's flagship offerings, and is focused on use cases such as protecting guest Wi-Fi/hot spot users and virtual desktop security. Zscaler also offers a cloud-based sandbox that analyzes suspicious objects that are automatically deposited by its SWG services. These and other innovations have resulted in a strong Completeness of Vision score. Zscaler is a good option for most enterprises that are seeking a cloud-based SWG.

Strengths

- Zscaler has the largest global cloud footprint for SWG vendors, with more than 100 policy enforcement nodes in 28 countries, including a strong presence in the Middle East and South America.
- Zscaler provides flexible implementation options by offering the broadest set of choices for traffic redirection (including IPsec) and authentication (including SAML). Flash cookies enable agentless authentication for mobile users on supported devices. On Android, Samsung Knox integration enables automatic redirection of Knox enterprise container traffic to Zscaler.
- Zscaler applies all its malware detection engines on all content, including traffic encrypted via SSL, regardless of site reputation.
- At the time of this writing, Zscaler is the only SWG cloud-based service to expose its cloud uptime and event statistics to the public via its trust.zscaler.com portal.
- A streaming log service provides near-real-time import of logs from the cloud to on-premises servers, where they can be analyzed by a security information and event management solution.

Cautions

- Implementation of Generic Routing Encapsulation (GRE) tunnels for traffic redirection can be complicated by older network gear, lack of capacity and misconfiguration (all network-based redirection techniques, such as IPsec, have these challenges). All enterprises should have preimplementation consultations with Zscaler or its partners to address these commonly known issues.
- Zscaler encourages the use of proxy autoconfiguration (PAC) files for Windows and Mac OS X systems for mobile employees, but knowledgeable users can subvert PAC file traffic redirection. Also, port-evasive applications (such as Skype, BitTorrent and some malware) will not be forwarded to the Zscaler network from endpoints that rely only on PAC files.
- Zscaler customer support has improved with a new service and support team, and a more mature operations management process, but support via resellers may be less consistent.
- The management console lacks severity indicators to prioritize malware alerts.

Vendors Added and 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's appearance 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. It may be a reflection of a change in the market and, therefore, changed evaluation criteria, or of a change of focus by that vendor.

Added

None

Dropped

None

Inclusion and Exclusion Criteria

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

- Vendors must provide all three components of an SWG:
  - URL filtering
  - Anti-malware protection
  - Application control capabilities
- Pure-play URL filtering solutions have been excluded.
- The vendor's URL filtering component must be primarily focused on categorizing English language websites.
- Vendors must have at least $15 million in SWG product revenue in their latest complete fiscal years.
- Vendors must have an installed base of at least 2,000 customers, or aggregate endpoint coverage of at least 5 million seats.

UTM devices and next-generation firewall devices that offer URL filtering and malware protection have been excluded. This Magic Quadrant analyzes solutions that are optimized for SWG functionality.

Vendors that license complete SWG products and services from other vendors have been excluded. For example, ISPs and other service providers that offer cloud-based SWG services licensed from other providers have been excluded.

Evaluation Criteria

Ability to Execute

Product or service: This is an evaluation of the features and functions of the vendor's SWG solution. Malware detection and advanced threat defense functionality will be weighted heavily to reflect the significance that enterprises place on these capabilities.

Overall viability: This includes an assessment of the overall organization's financial health, the financial and practical success of the business unit, and the likelihood that the business unit will continue to invest in the product.

Sales execution/pricing: This is a comparison of pricing relative to the market.

Market responsiveness/record: This criterion reflects how quickly the vendor has spotted a market shift and produced a product that potential customers are looking for; it is also the size of the vendor's installed base relative to the amount of time the product has been on the market.

Marketing execution: This is the effectiveness of the vendor's marketing programs, and its ability to create awareness and mind share in the SWG market.

Customer experience: This is the quality of the customer experience based on reference calls and Gartner client teleconferences.

Table 1. Ability to Execute Evaluation Criteria

Evaluation Criteria	Weighting
Product or Service	Medium
Overall Viability	High
Sales Execution/Pricing	Medium
Market Responsiveness/Record	Medium
Marketing Execution	High
Customer Experience	Medium
Operations	Not Rated

Source: Gartner (June 2014)

Completeness of Vision

Market understanding: This is the SWG vendor's ability to understand buyers' needs and translate them into products and services.

Sales strategy: This is the vendor's strategy for selling to its target audience, and includes an analysis of the appropriate mix of direct and indirect sales channels.

Offering (product) strategy: This is an evaluation of the vendor's strategic product direction and its road map for SWG. The product strategy should address trends that are reflected in Gartner's client inquiries.

Innovation: This criterion includes product leadership and the ability to deliver features and functions that distinguish the vendor from its competitors. Innovation in areas such as advanced threat defense and cloud-based services were rated highly, since these capabilities are evolving quickly and are highly differentiated among the vendors.

Geographic strategy: This is the vendor's strategy for penetrating geographies outside its home or native market.

Table 2. Completeness of Vision Evaluation Criteria

Evaluation Criteria	Weighting
Market Understanding	Medium
Marketing Strategy	Not Rated
Sales Strategy	Medium
Offering (Product) Strategy	High
Business Model	Not Rated
Vertical/Industry Strategy	Not Rated
Innovation	High
Geographic Strategy	Low

Source: Gartner (June 2014)

Quadrant Descriptions

Leaders

Leaders are high-momentum vendors (based on sales and mind share growth) with established track records in SWGs, as well as with 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; however, they 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. Buyers should expect state-of-the-art technology from Visionaries, but be wary of a strategic reliance on these vendors and closely monitor their viability. 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's 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

The market is segmented between large enterprises and SMBs. Solutions aimed at SMBs are designed for ease of use, cost-effectiveness and basic security protection. Solutions aimed at large enterprises provide tools and detailed reports that security operations teams can use to respond to advanced threats and malware alerts.

Market Overview

We estimate that the combined SWG revenue of the Magic Quadrant participants in 2013 was $1.31 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 11% during 2013, and we anticipate that the market will grow 10% to 12% in 2014.