Magic Quadrant for Secure Web Gateways

06 June 2016 | ID:G00279134

Analyst(s): Lawrence Orans, Peter Firstbrook

Summary

The market for secure web gateway solutions is still dominated by traditional on-premises appliances. However, cloud-based services continue to grow at a faster rate than appliances, leaving many vendors struggling to adapt.

Market Definition/Description

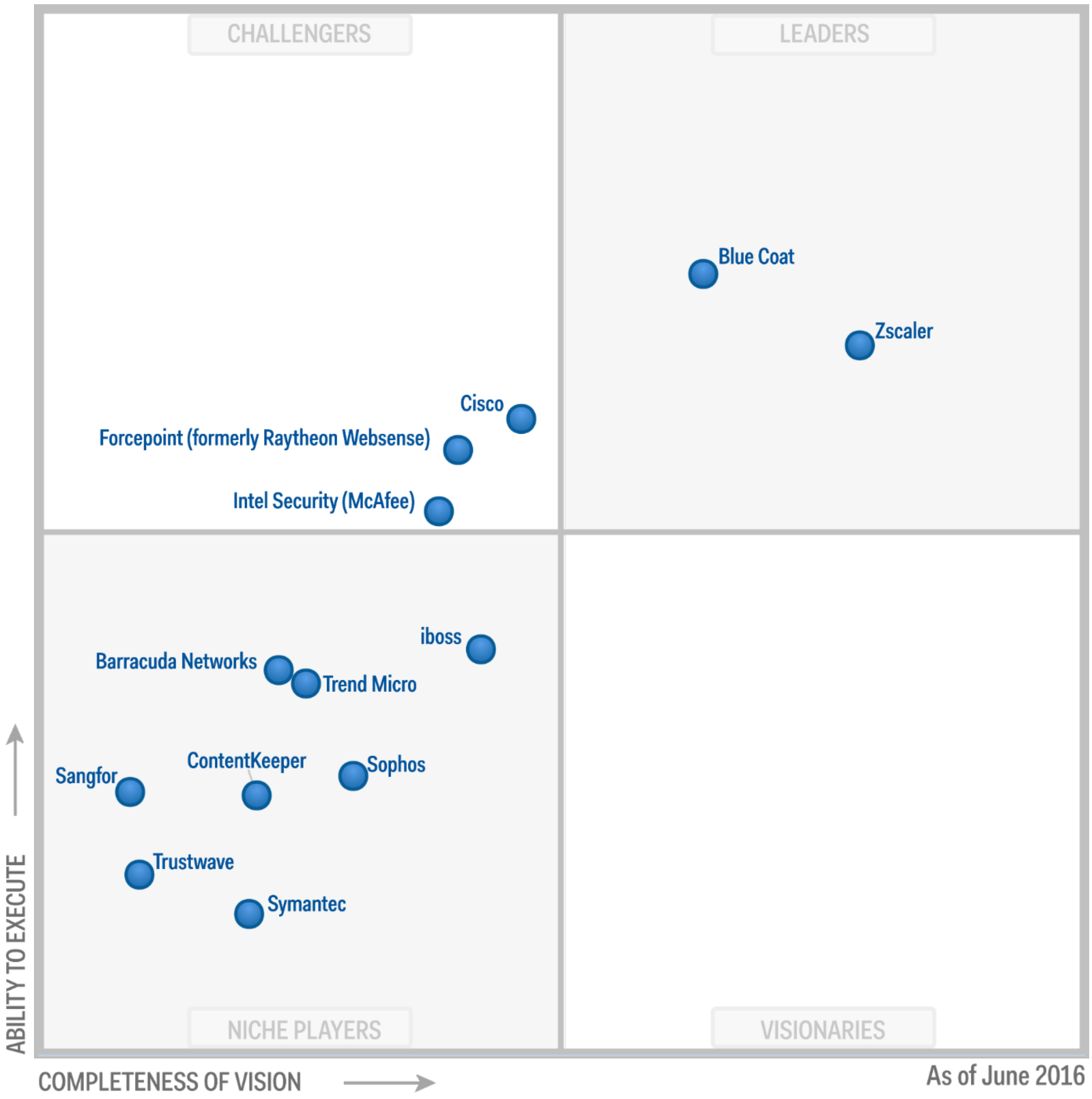
Secure web gateways (SWGs) utilize URL filtering, advanced threat defense, legacy malware protection and application control technologies to defend users from internet-borne threats, and to help enterprises enforce internet policy compliance. SWGs are implemented as on-premises appliances (hardware and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

As noted in the Market Overview section, cloud-based SWG services are growing more quickly than appliance-based solutions (SWG appliances still represent over 70% market share, as measured by revenue). There are two use cases for implementing a cloud-based SWG service. In the more common scenario, enterprises link multiple branch offices directly to the internet, to avoid backhauling web traffic over their MPLS backbones. The other use case is to protect mobile users, so that their web traffic flows through the SWG cloud service when they are off-network. Based on client inquiries, Gartner estimates that over 80% of cloud-based SWG implementations are driven primarily by the remote office use case. The distinction is important, because some vendors have built cloud services that are optimized for the remote office use case, whereas others have built cloud services that are optimized for protecting mobile users. This year, we awarded more Completeness of Vision points to vendors that emphasize the remote office use case and have the proven technology to support it (for example, tunneling traffic from a router to the cloud service). Vendors that emphasize the mobile user scenario, where every endpoint must be configured to send traffic to the internet, received fewer Vision points.

Advanced threat defense is becoming increasingly important in the SWG market. Vendors must deliver on the promise that they are truly security products (or services) and not just web filtering solutions. Otherwise, they run the risk of being replaced, because customers have multiple options for web filtering and advanced threat protection. Web filtering is a commodity, and it is widely available as a feature of firewalls, intrusion prevention systems (IPSs) and unified threat management (UTM) systems. Advanced threat defense is also widely available as a feature of firewalls and from multiple vendors offering dedicated solutions. Nearly all the vendors in this Magic Quadrant offer advanced threat defense capabilities, but the quality and efficacy of the solutions vary widely.

Magic Quadrant

Figure 1. Magic Quadrant for Secure Web Gateways



Source: Gartner (June 2016)

Vendor Strengths and Cautions

Barracuda Networks

Based in Campbell, California, Barracuda Networks provides a broad array of cost-effective network and application security products, as well as storage and productivity solutions. In 2016, Barracuda rebranded its SWG appliances — they are now known as the Barracuda Web Security Gateway. The vendor also offers a cloud-based SWG service, known as the Barracuda Web Security Service. The Barracuda Web Security Gateway appliances are good candidates for small or midsize businesses (SMBs) and cost-conscious enterprises.

STRENGTHS

- Barracuda'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 comprehensive (700 applications), and includes granular controls for social media and Google Apps.
- Barracuda has simplified the challenge of traffic redirection by enabling its NextGen Firewall products to redirect web traffic to the Barracuda Web Security Gateway.
- Customers that purchase a Web Security Gateway appliance or the Web Security Service receive free remote filtering capabilities on Windows/Mac clients, as well as on mobile devices running Apple iOS. Barracuda's pricing model enables it to be the low-cost alternative in many competitive deals. It charges by appliance capacity, and it does not add a per-user subscription charge.

CAUTIONS

- Dedicated focus on SMBs has resulted in solutions that are missing features favored by large enterprise customers. Lack of support for authentication via SAML is an example of this trade-off.

- Barracuda's SWG appliances rely heavily on signatures for malware detection. There is very little real-time analysis of web content, such as static code analysis.
- Barracuda has shown minimal commitment to its cloud delivery option. It does not support a hybrid deployment model. One console is needed to manage on-premises appliances and a separate console is needed to manage the cloud service.
- Unlike leading cloud-based SWG services, Barracuda does not publish the status and availability of its service on a public-facing website.
- Barracuda's SWG offerings do not support advanced threat defense functionality. Neither the on-premises appliances nor the cloud service is capable of automatically depositing suspicious objects in Barracuda's network sandbox.

Blue Coat

Based in Sunnyvale, California, Blue Coat offers appliance-based SWGs and a cloud-based SWG service. It has the largest market share among SWG appliance vendors, and it has the overall largest market share among all vendors in this Magic Quadrant (based on revenue). Blue Coat publishes the availability and status of its cloud service . In addition to its SWG solutions, the vendor offers a network sandbox, available in an appliance form factor. Blue Coat also offers the SSL Visibility Appliance and the Security Analytics platform (a network forensics tool that operates with full packet capture). In May 2015, private equity firm Bain Capital completed its acquisition of Blue Coat from Thoma Bravo (also a private equity firm) for $2.4 billion. Bain Capital's stated intent is to prepare Blue Coat for a return to public markets. In July 2015, Blue Coat acquired Perspecsys, a cloud access security broker (CASB) with a focus on data security. In November 2015, Blue Coat acquired another CASB, Elastica, which provides a broader set of CASB functions. In November 2015, Blue Coat added a new product to its portfolio, Advanced Secure Gateway. It combines two products, ProxySG and Content Analysis System, into a single appliance. 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

- ProxySG is the strongest proxy in the market in terms of breadth of protocols and the number of advanced features. It also supports multiple authentication and directory integration options.
- Blue Coat's hybrid offering (cloud service and on-premises appliances) enables operations teams to manage most policies from a single console (although policies can be pushed only in one direction — from the cloud to on-premises appliances).
- Blue Coat provides strong support for SSL/TLS. All ProxySG models include SSL hardware assist, to offload processing from the main CPU. The stand-alone SSL Visibility Appliance can be used to decrypt SSL/TLS traffic and feed it to Blue Coat and non-Blue Coat security solutions (for example, data loss prevention [DLP], IPS and network sandboxes).
- Blue Coat's partnership strategy has enabled it to fill gaps in its product line. Partnerships with six endpoint detection and response (EDR) vendors help ensure that its customers can complement Blue Coat's network-based advance threat detection with an endpoint strategy. Partnerships with FireEye and Lastline enable customers to use their own sandboxes instead of Blue Coat's sandbox. A partnership with Cylance adds signatureless file inspection to Blue Coat's Content Analysis System.
- Blue Coat's ownership and integration of CASB technology gives it an early mover advantage in this emerging market.

CAUTIONS

- Because Blue Coat's appliance-based SWG requires multiple components, it is an expensive offering. Blue Coat proxies require the Content Analysis System to deposit files in its Malware Analysis Appliance (a network sandbox). Customers pay extra for the Content Analysis System functionality, whether they purchase it as a dedicated appliance or they purchase Advanced Secure Gateway (integrated ProxySG and Content Analysis System). Blue Coat is one of the few vendors in this Magic Quadrant to charge extra for its reporting functionality and management console.
- Blue Coat lacks a cloud-based network sandboxing service.
- Blue Coat's strategy for on-premises DLP is weaker than several of its key competitors in this Magic Quadrant. Blue Coat does not own its DLP technology; it is licensed from Digital Guardian. Should Digital Guardian's status change, Blue Coat's DLP strategy could be negatively impacted.

Cisco

Cisco, based in San Jose, California, offers the Web Security Appliance (WSA; and virtual appliances) and a cloud-based service, Cloud Web Security (CWS). Cisco provides status and availability data for its cloud service . In 2016, the vendor introduced its hybrid solution by enabling its cloud service to configure and manage policies on Cisco SWG appliances. However, unified reporting is still evolving (see the Cautions). Cisco has also integrated its Cognitive Threat Analytics (CTA) with its appliances (previously, CTA was only available as a feature of Cisco's cloud service). Cisco states that it doubled the performance of its WSA appliances by optimizing proxy code and porting the solution to a new hardware platform. Cisco's WSA is a good solution for most midsize and large enterprises, while CWS is a good option for most enterprises.

STRENGTHS

- Cisco's SWG customers have several options for advanced threat capabilities, depending on their sophistication and budget. The appliances and the cloud service integrate with Cisco's Advanced Malware Protection (AMP) for an optional fee. Customers with advanced security operations teams have the option to adopt Cisco's CTA solution, which analyzes logs from Cisco's appliances and/or its cloud service to detect attacks.
- Configuring traffic redirection to CWS is easy on Cisco products that support the "connector" software. The Adaptive Security Appliance (ASA) firewall, Integrated Services Router (ISR) 4000 Series and Generation 2, and WSA all support this feature.
- The Layer 4 Traffic Monitor feature on the WSA enables visibility across all ports and protocols by connecting to a Switched Port Analyzer (SPAN) mirrored port on a LAN switch. By monitoring all traffic (not just web traffic), Cisco improves its malware detection capability.
- Mobile platform support is a strength of the CWS service for customers that have already implemented Cisco's popular AnyConnect Secure Mobility Client.

CAUTIONS

- Cisco has not demonstrated significant growth in the SWG market. Overall market share has been flat since 2009, the year that Cisco acquired its SWG technology (ScanSafe [cloud] and IronPort [appliances]).
- Policy support for hybrid mode is new since January 2016, and feature parity needs improvement in a few areas. Some appliance features (for example, native FTP) are not supported from the CWS cloud, and have been removed from the appliance when it is configured in hybrid mode. Cisco's path to hybrid has been slow due to separate underlying technology platforms from its acquisitions. (ScanSafe [cloud] and IronPort [appliances])
- The hybrid offering lacks unified reporting from the CWS cloud console (ScanCenter). Cisco's Web Security Reporting Application is required in the customer's environment to achieve unified reporting across the Cisco SWG appliances and cloud service.
- Cisco's support for DLP lags several of its competitors that target large enterprises. Its SWG appliance, the WSA, only supports context-based rules for basic DLP. The CWS cloud service lacks support for secure ICAP, which would allow customers to send content from CWS to an existing on-premises DLP solution.

ContentKeeper

ContentKeeper is based in Australia. It offers a family of SWG appliances, which are implemented in transparent bridge mode. Customers can also implement virtualized instances of its appliances in hosted environments. In 2015, ContentKeeper introduced a load balancing appliance, which is designed to support its SWG appliances. Gartner moved ContentKeeper backward in Completeness of Vision this year for two reasons: It continues to lack a shared, multitenant cloud service, and it has shown little progress in establishing itself as a leading security vendor (see the Cautions). ContentKeeper has been expanding its presence in North America, where it has focused on the education market. Its performance-oriented appliances, and its support for Chromebooks (a Chromebook extension redirects traffic to a ContentKeeper appliance), make it a good choice for K-12 schools that require Web filtering and basic malware protection.

STRENGTHS

- The bridge-based Secure Internet Gateway has been designed for high throughput. Customer references report that it outperforms other bridge-based SWGs that they have tested.
- Strong support for mobile devices enables ContentKeeper to appeal to K-12 school districts and other organizations that issue tablets to end users.
- Customer references report that ContentKeeper's appliances can terminate and inspect SSL/TLS traffic at rates of approximately 3 Gbps.
- ContentKeeper's load balancer appliance is a cost-effective alternative to industry-leading multipurpose load balancers (also known as application delivery controllers).

CAUTIONS

- ContentKeeper has shown minimal effort in establishing its reputation as a security vendor. For example, unlike other security companies, it does not publish a blog or white papers that educate security professionals and contribute to the industry's efforts to fight malware and advanced threats. This low-profile approach to security leads Gartner to question ContentKeeper's ability to compete as a leading security vendor in the SWG market, particularly with its sandboxing appliance. Prospective customers of ContentKeeper's sandbox appliance should carefully test the efficacy of its solution against competing products.
- ContentKeeper lacks a shared, multitenant cloud SWG service.
- The workflow tools for responding to malware incidents need improvement. The lack of severity indicators on ContentKeeper's

dashboard makes it difficult to prioritize malware alerts.

Forcepoint (formerly Raytheon Websense)

In January 2016, the company formerly known as Raytheon Websense rebranded itself as Forcepoint. The new entity includes the Stonesoft and Sidewinder firewall product families, which Raytheon Websense acquired from Intel Security. Forcepoint's strategy is to integrate Websense's Triton product line with Raytheon's Cyber Products division, and its newly acquired firewalls, to address the security issues of the enterprise market. Forcepoint offers SWG appliances (hardware and software) and a cloud-based service. It publishes the status and availability of its cloud service . In April 2016, Forcepoint's board of directors appointed a new CEO to lead the company. In the 2015 SWG Magic Quadrant, Websense was positioned in the Leaders quadrant. This year, Forcepoint is positioned in the Challengers quadrant, due primarily to a cloud strategy that limits its ability to compete for opportunities where large enterprises need to connect multiple remote offices to a cloud-based SWG service (see the Cautions). Forcepoint appliances are good options for midsize enterprises, and its cloud service is a good option for enterprises that need to protect mobile employees.

STRENGTHS

- Forcepoint 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. Recent improvements include customizable dashboards with drill-down capabilities that lead security analysts to relevant information.
- Forcepoint offers a cloud-based network sandbox (Threat Protection Cloud module — developed internally by Websense) and an on-premises network sandbox (Threat Protection Appliance — developed internally by Raytheon).
- Forcepoint has strong DLP technology. It uses the same DLP engine in its AP-Web and AP-Data offerings, which enables policy uniformity and an easy upgrade path from integrated DLP in AP-Web to the AP-Data gateway. Forcepoint also uses its DLP technology in its appliances and cloud service to inspect suspicious outbound traffic patterns (this feature does not require an additional licensing fee).
- Forcepoint has a good strategy for mobile support. A Forcepoint client for Windows and Mac OS X endpoints handles traffic redirection and authentication to the Forcepoint cloud service. AirWatch customers will benefit from an integration with Forcepoint that provisions certificates on mobile devices (Apple iOS and Android), and directs traffic to the Forcepoint cloud (via IPsec) when the user generates web traffic.

CAUTIONS

- The corporate restructuring of Websense into Forcepoint has presented some challenges. Development of advanced SWG features has slowed relative to market leaders. As a U.S.-based military contractor, Raytheon's ownership stake in the company may limit its appeal in some geographic areas .
- Forcepoint's cloud service lacks a strong approach for supporting large remote offices, due to its lack of commitment to a tunnel-based method for traffic redirection. IPsec and GRE tunnels are the most commonly used techniques among enterprises to redirect traffic from a remote location to a cloud-based SWG service. Forcepoint does not support GRE tunnels, and only 50% of its 20 data centers support IPsec. Forcepoint's most commonly used techniques for redirecting traffic from a customer's location to its cloud service are via PAC file and firewall port forwarding. Port forwarding is not an enterprise-class technique. It is challenging for Forcepoint to succeed with this strategy, when competitors have proven that they can successfully connect remote offices with a tunnel-based approach from a router or firewall.
- The console for the cloud-only service (Cloud Triton Manager) is different from the console that is used to manage the hybrid and on-premises solutions (Triton Manager). Customers that begin with a cloud-only service and add V-Series appliances later would need to switch to the Triton Manager console.
- Gartner rarely sees Forcepoint's X10G, a blade server appliance aimed at large enterprises, in competitive bids. Enterprises that are considering the X10G should carefully check references.

iboss

A privately held company based in San Diego, California, iboss introduced a newly rearchitected cloud solution based on container technology in January 2016. Customers can adopt the public cloud service operated by iboss, or they can implement the same container-based technology as a private cloud. Customers in need of a hybrid solution can integrate their own private cloud with the iboss public cloud. Only iboss customers can monitor the status and availability of the cloud service via a password-protected portal. The vendor also offers an internally developed advanced threat solution known as FireSphere. In 2016, iboss announced a data analysis module, using FICO's technology, to identify data anomalies and assign risk scores that indicate the severity of a threat. (FICO's technology is widely used in the financial industry to detect fraud.) In November 2015, iboss announced that it received a $35 million investment from Goldman Sachs. The vendor is a good option for SMBs and large enterprises.

STRENGTHS

- The container-based approach of the new cloud service is promising, because it is designed to enable a smooth transition from a private cloud (hosted or on-premises) to a public cloud or hybrid implementation. The vendor states that it offers all features and functions across any deployment model (Gartner has not been able to validate this new functionality — see the Cautions).
- Bandwidth control is strong. The iboss console shows bandwidth allocation (for example, percentage of video streaming), and it also highlights the largest overall bandwidth users.
- The FireSphere service combines multiple malware detection capabilities, including NetFlow analysis and sandboxing technology.
- The new iboss GUI has a clean design, and it includes a dashboard with high-level statistics.

CAUTIONS

- The vendor's new solution has been completely rearchitected and has only been available since January 2016. Many of its early adopter customers are still in the beginning stages of deployment. At the time of this writing, Gartner was still in the process of validating iboss' overall functionality and its feature parity claims for hybrid mode. Prospective customers should carefully test the new offering.
- The vendor needs to demonstrate that it has the operational expertise to scale and manage a global cloud-based service. Prospective customers should check references and carefully monitor service-level agreements.
- The iboss cloud-based service lacks support for SAML, a popular authentication technique that many enterprises already have adopted to authenticate users to SaaS applications.
- The vendor's customer base still consists heavily of North American enterprises The Goldman Sachs investment should help fund international expansion, but prospective customers outside North America should validate that iboss' partners are qualified to provide sales and technical support.
- As iboss expands its offerings to the cloud, Gartner has concerns (based on feedback from several customers) about its service and support focus for its traditional appliance-based offerings.

Intel Security (McAfee)

Intel Security, based in Santa Clara, California, offers a family of on-premises SWG appliances (McAfee Web Gateway) and cloud-based SWG services (McAfee SaaS Web Protection). Intel Security publishes the status and availability of its cloud service . The SWG appliances are most commonly implemented as proxies, although they also can be deployed in other modes, including in-line transparent bridges. Intel Security also offers an appliance-based sandbox (McAfee Advanced Threat Defense) and a DLP solution. During 2015 and 2016, Intel Security has reduced its portfolio of security solutions. In November 2015, it sold its firewall products (technology that it acquired from Stonesoft and Secure Computing) to Raytheon Websense (now Forcepoint). In October 2015, it announced the end of life (EOL) for its McAfee email security solutions. Intel Security's appliance solutions are good candidates for most enterprise customers, particularly those that are already McAfee ePolicy Orchestrator users. Its cloud-based SWG service is a good candidate for Intel Security customers that seek to protect mobile users on Windows and OS X operating systems (see the Caution below about connecting office locations to its cloud).

STRENGTHS

- Malware detected by the McAfee Web Gateway or McAfee Advanced Threat Defense sandbox can be automatically blocked by endpoints running the Endpoint Security client (this capability requires that customers purchase the McAfee Threat Intelligence Exchange product).
- McAfee Web Gateway and McAfee SaaS Web Protection have strong malware protection due to embedded browser code emulation capabilities (the Gateway Anti-Malware feature). This feature provides the ability to adjust the sensitivity of malware detection. A rule-based policy engine enables flexible policy creation.
- 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 admins to selectively choose which policies are synced.
- Intel Security provides strong support for scanning SSL/TLS traffic with its McAfee Web Gateway appliance and its cloud-based service. For example, the solutions can be configured to automatically enforce SSL/TLS certificate decisions, so that end users don't have the option to accept an unknown or expired certificate.

CAUTIONS

- Intel Security's cloud strategy presents a challenging option for customers that wish to connect offices to a cloud-based SWG service. It has limited experience in supporting a tunnel-based approach for linking headquarters and remote offices to its cloud. Instead, it recommends an endpoint-based approach, where each device uses the McAfee Client Proxy to redirect traffic to its cloud.

- Intel Security lacks a cloud-based sandbox.
- McAfee Client Proxy is not integrated with the popular McAfee Endpoint Security client. Intel Security customers will need to install and support both software clients on users' devices.
- Intel Security's strategy for protecting mobile devices (iOS and Android) lags behind several key competitors. It lacks integration with a mobile device management vendor to simplify the provisioning of VPN profiles on mobile devices.

Sangfor

Sangfor is a network optimization and security vendor based in China. Approximately half of its revenue comes from its SWG products; the remaining revenue comes from its next-generation firewall, VPN, WAN optimization controllers and application delivery controller products. Sangfor's SWG comes in a hardware appliance form factor or as a virtual appliance, and it is implemented as an in-line transparent bridge. Nearly all the vendor's revenue is generated in the Asia/Pacific region. Sangfor is a candidate for organizations that are based in China and other supported countries in the Asia/Pacific region.

STRENGTHS

- Sangfor has strong application control features. It can apply granular policies to microblogging services, Facebook and other web-based applications, and it also has developed network signatures based on traffic patterns to block port-evasive applications like BitTorrent and Skype.
- The vendor's SWG includes a wireless controller, which is capable of managing Sangfor wireless access points. The controller includes a feature to detect and block unauthorized Wi-Fi hotspots in an enterprise wireless environment.
- Sangfor targets the retail vertical industry with a feature that pushes ads to shoppers while they are in the store. The ads are pushed according to SSID location.
- The vendor'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 does not offer a cloud-based SWG service.
- The Sangfor SWG lacks advanced threat defense capabilities. It does not integrate with the Sangfor cloud-based sandbox.
- The console dashboard lacks severity indicators to prioritize malware alerts.

Sophos

Based in the U.K., Sophos provides a broad range of network and application gateways, and an endpoint protection platform that it is converging into a unified security solution aimed primarily at small and midmarket enterprises. The Sophos Web Appliance (SWA) can be deployed in proxy or transparent in-line bridge mode, and the vendor also offers SWG functionality integrated into its UTM appliances. Sophos' acquisition of Mojave Networks (in 2014) forms the basis of its cloud-based SWG service. In 2015, Sophos introduced its cloud-based Sandstorm sandboxing service, which it licenses from a third party. Sophos' SWA automatically deposits suspicious objects into the Sandstorm sandbox, as does the Sophos email appliance. In 2015, Sophos also improved the performance of its SWA through a software rewrite. Small and midsize organizations, particularly those that are Sophos desktop customers, should consider the vendor's SWG solutions.

STRENGTHS

- Sophos' SWG pricing model is flexible and cost-effective. Customers pay per seat, and have the option to use the seat with the on-premises solution or the cloud-based service. Sophos provides a virtual appliance free of charge for users of its on-premises solution (customers can also purchase a hardware appliance from Sophos).
- Sophos places strong emphasis on service and support and ease of use. It optionally monitors customers' appliances and provides alerts for critical hardware conditions, such as high temperatures or faulty disk drives.
- Ease-of-use features include automated network and directory discovery, contextual help functions, and simple policy configuration.
- 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 (this feature is only available when the SWA is in proxy mode).

CAUTIONS

- Sophos does not support a hybrid deployment model. One console is needed to manage on-premises appliances and a separate console is needed to manage the cloud service.
- The cloud-based SWG service remains limited in terms of functionality and geographic coverage. For example, it does not integrate with Sophos' Sandstorm sandbox, and it has a small cloud footprint (only 12 data centers).

- Unlike leading cloud-based SWG services, Sophos does not publish the status and availability of its cloud-based SWG service on a public-facing website.
- The Sophos Web Appliance lacks support for some features (for example, ICAP and FTP proxy) that are often required in large enterprises.

Symantec

Symantec is based in Mountain View, California. In December 2015, it announced an EOL program for the Symantec Web Gateway appliance. Now, it's only SWG offering is Symantec Web Security.cloud. The vendor announced the availability of its Advanced Threat Protection solution in October 2015. In April 2016, it announced that its CEO will be stepping down, but that he will continue to serve as CEO until a successor has been appointed. The vendor's cloud-based SWG offering is a good option for Symantec SMB customers that only need basic SWG functionality.

STRENGTHS

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

CAUTIONS

- The next CEO will be Symantec's fourth since 2012, and Gartner believes that management turnover has limited Symantec's execution.
- Symantec makes it challenging for customers to connect their office locations to its cloud service. It lacks an agentless tunnel-based approach (IPsec or GRE), which is the most common for linking offices to an SWG cloud service. It recommends that customers implement the Symantec Smart Connect agent on every Windows device (it is not supported on Mac OS X) to redirect traffic to Symantec Web Security.cloud.
- The Symantec Web Security.cloud service does not integrate yet with the sandbox component of Symantec's Advanced Threat Protection solution.
- Symantec's strategy for supporting mobile devices needs improvement. Proxy autoconfiguration (PAC) files, which knowledgeable users can easily subvert, are needed to redirect traffic from Apple iOS, Android and Mac OS X devices to the Symantec.cloud SWG service.
- Symantec provides limited information about the status and availability of its cloud-based SWG service. It only shows an aggregate uptime percentage for the service, and, unlike many competitors, it does not include statistics on a per-node basis.

Trend Micro

Based in Tokyo, Trend Micro is a provider of endpoint protection, content protection and application gateway solutions. The vendor offers an on-premises virtual appliance solution, InterScan Web Security Virtual Appliance (IWSVA), and a cloud service, InterScan Web Security as a Service (IWSaaS). IWS can be implemented as a transparent bridge or a proxy, and can be optionally enhanced by Trend Micro's Deep Discovery network sandbox. In 2015, the vendor integrated its Smart Protection Server with IWSVA to provide it with access to malware and reputation data. It also added bandwidth shaping and quality of service (QoS) functionality to IWSVA to improve application performance. Trend Micro is a candidate primarily for organizations that already have a strategic relationship with the vendor.

STRENGTHS

- Notable improvements in the IWSVA include integration with local Smart Protection Server, which hosts local malware and IP reputation data, and the introduction of bandwidth shaping and QoS for applications.
- The IWSVA and IWSaaS solutions are strengthened by Trend Micro's global threat intelligence, script analyzer capabilities and botnet detection. Optional offerings include the Deep Discovery sandbox appliance for on-premises malware analysis, and Damage Cleanup Services for remediation of compromised endpoints.
- A single licensing model allows customers to mix cloud and on-premises solutions, and a specific hybrid console provides an integration point for synchronizing policies and reporting for cloud and on-premises users.
- Application control is strong with IWSVA, and includes the ability to set time of day and bandwidth quota policies.
- Trend Micro's cloud-based SWG service has good geographic coverage for the Asia/Pacific region.

CAUTIONS

- The IWSaaS cloud service is missing some enterprise-class features, such as cloud-based malware sandboxing, security information and event management (SIEM) integration, and DLP support. It has limited geographic presence, with only 14 data centers in 10 countries.

- Trend Micro has three consoles for its SWG offerings: an on-premises-only console for IWS, a cloud-only console for IWSaaS and a separate console for the hybrid offering. This approach adds operational complexity as enterprises grow and evolve with the offerings.
- Unlike leading cloud-based SWG services, Trend Micro does not publish the status and availability of its cloud-based SWG service on a public-facing website.
- Trend Micro has limited experience in connecting branch offices to its cloud service. Its solution is optimized for protecting mobile endpoints.
- The IWSVA solution is missing some enterprise-class features (for example, outbound malware detection lacks detailed information on threats).

Trustwave

Trustwave is based in Chicago. It offers a diversified security product and managed security service portfolio, including application security, DLP, email security, Web application firewall, SIEM and network access control; in addition, it offers numerous managed security services. Its Secure Web Gateway appliance is proxy-based. Trustwave's SWG solutions may be good options for customers that already have one or more Trustwave products or services, or for those that are seeking an SWG managed service. Singtel acquired Trustwave in September 2015 and continues to operate it as a stand-alone business.

STRENGTHS

- The Trustwave Managed Anti-Malware Service provides deployment, policy management, security monitoring and alerting as a service for on-premises SWG installations.
- Research and insight from incident response investigations and penetration tests may enhance Trustwave's browser code emulation, which is the primary technology in its malware detection strategy. This feature enables the Trustwave solution to strip only suspect objects from otherwise legitimate web pages.
- Application control support for social media and cloud storage enables granular policy options.
- Trustwave's DLP engine is fully integrated with its Secure Web Gateway offering.

CAUTIONS

- Trustwave does not offer a cloud-based SWG service.
- Trustwave lacks the network sandboxing capabilities that many SWG vendors offer as optional features.
- 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 Secure Web Gateway product lacks the ability to block port-evasive applications, such as BitTorrent and Skype. Port-evasive outbound traffic to command-and-control centers cannot be blocked either.
- The dashboard console is weaker than many competing offerings. For example, it lacks severity indicators to prioritize malware alerts, and dashboard panels provide only limited customization.

Zscaler

Zscaler, based in San Jose, California, is a pure-play provider of cloud-based SWG services. Zscaler publishes the status and availability of its cloud service . In September 2015, Zscaler announced it had raised $110 million in its latest round (Series D) of financing. Since the publication of the last Magic Quadrant for SWGs, it introduced Zscaler Private Access, a service aimed at replacing VPNs. Zscaler also introduced its new endpoint agent, Zscaler App, which enables the most common mobile and portable devices to be protected by the Zscaler cloud service. Zscaler also introduced its Virtual Zscaler Enforcement Node (VZEN), which enables customers to deploy a Zscaler proxy in their own data centers. Zscaler continues to be the fastest-growing vendor in this market. Gartner estimates that Zscaler owns more than 50% of the market share (as measured by revenue) for cloud-based SWG services. The vendor is a good option for most enterprises seeking a cloud-based SWG.

STRENGTHS

- Zscaler applies all its malware detection engines to all content, including SSL/TLS traffic, regardless of site reputation. This approach yields improved filtering and up-to-date malware ratings on websites.
- Zscaler has, by far, the largest global cloud footprint, with more than 100 enforcement nodes in 30 countries.
- All Zscaler customers benefit from a network sandbox feature that analyzes executable and DLL file types. Customers have the option to purchase a more comprehensive sandbox feature (Advanced Behavioral Analysis), which analyzes a broader set of files. This feature also includes policy-based quarantining of suspicious files (for example, quarantine of an executable file from an unknown site).

- Zscaler continues to lead the market in innovative cloud features. The new Zscaler Private Access capability shows promise (see the Cautions) for enabling customers to replace VPNs. The Nanolog Streaming Service provides the real-time export of logs to popular SIEM solutions. Zscaler's firewall service (outbound-only) was the first among SWG vendors.

CAUTIONS

- As Zscaler expands and takes on new challenges, the vendor needs to demonstrate that it, and its partners, can adequately support all newly introduced features and functionality. Some capabilities were introduced only a few months before publication of this Magic Quadrant, and Gartner has received limited customer feedback on them. For example, Zscaler Private Access was announced in April 2016. The Zscaler App and the VZEN virtual proxy have only been available since December 2015. Prospective customers of Zscaler's new capabilities should test them carefully.
- Gartner estimates that Zscaler's advanced sandboxing and firewall services are selling at below a 25% attach rate to its core service offering. Zscaler's malware research team is still small, compared to its larger competitors, and its threat intelligence capability is not as comprehensive as that of others in this market. For these reasons, prospective customers should carefully test the efficacy of Zscaler's security services.
- The management console lacks severity indicators to prioritize outbound malware alerts. Also, information to aid in remediation is lacking.

Vendors Added and Dropped

We review and adjust our inclusion criteria for Magic Quadrants as markets change. As a result of these adjustments, the mix of vendors in any Magic Quadrant may change over time. A vendor's appearance in a Magic Quadrant 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

No vendors were added to this Magic Quadrant.

Dropped

No vendors were dropped from this Magic Quadrant.

Inclusion and Exclusion Criteria

These criteria must be met 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 capable of categorizing English language websites.
- Vendors must have at least $20 million in SWG solution revenue from enterprise customers in their latest complete fiscal year. Revenue resulting from equipment sales to service providers, for the purpose of building infrastructure to deliver services, does not apply (the target audience for the Magic Quadrant is enterprises, not service providers).
- Vendors must have an installed base of at least 3,000 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 will analyze 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	High
Overall Viability	High
Sales Execution/Pricing	Not Rated
Market Responsiveness/Record	Medium
Marketing Execution	High
Customer Experience	Medium
Operations	Not Rated

Source: Gartner (June 2016)

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 roadmap 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, as 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	High
Offering (Product) Strategy	High
Business Model	Not Rated

Evaluation Criteria	Weighting
Vertical/Industry Strategy	Not Rated
Innovation	Medium
Geographic Strategy	Low

Source: Gartner (June 2016)

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. In addition to offering strong SWG products and/or services, Leaders have built effective sales and distribution channels for their entire product portfolio. Leaders that offer on-premises and cloud services have recognized the strategic importance of a two-pronged sales and distribution channel. They have established a traditional value-added reseller channel to sell on-premises appliances, and they have also developed partnerships with ISPs and carriers to sell cloud services, oftentimes as an add-on to bandwidth contracts.

Challengers

Challengers are established vendors that offer SWG products. Challengers' products perform well for a significant market segment, but may not show feature richness or particular innovation. In the SWG market, Challengers may also lack an established distribution channel to optimally target customers for cloud-based services. Buyers of Challengers' products and services 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 Player 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

This year, the Visionaries quadrant remains empty again. Because of the growth in cloud-based SWG services, we heavily weighted these services when scoring the Completeness of Vision criteria. Vendors that have a strong strategy for their cloud service, and that also have a cloud-focused sales and distribution channel, scored well in Vision. Successful sales and distribution channels include carriers, ISPs and managed security service providers, because they have proven to be effective partners in selling cloud SWG services. None of the Niche Player vendors in the 2015 version of the Magic Quadrant improved enough in Vision scoring to move into the Visionaries quadrant this year.

Market developments in 2015 may have a future impact on the market. In February 2015, Allot Communications acquired Optenet, an SWG vendor that primarily targeted the service provider market. In November 2015, Akamai acquired Bloxx, an SWG vendor that primarily targeted the education sector. Neither Allot Communications nor Akamai met the inclusion criteria for this Magic Quadrant. Gartner will monitor the progress of these vendors during the next few years to determine whether they are eligible to be included in future updates to this Magic Quadrant.

Market Overview

Although cloud-based SWG services are growing rapidly, the overall SWG market is still dominated by the sale of on-premises appliances. We estimate that the combined revenue of the SWG Magic Quadrant participants in 2015 was $1.4 billion, which represents an 11% growth rate over an adjusted 2014 market size of $1.24 billion (see Note 1). We estimate that cloud service revenue represented approximately 27% of the total in 2015. Cloud services have experienced a 35% five-year compound annual growth rate, while on-premises appliances have only grown by 6% during the same period. Blue Coat and Zscaler are responsible for the majority of the overall SWG market growth.

The enterprise SWG market is roughly 80% penetrated, and the growth rate of new seats is slowing. As a result, we anticipate overall SWG Magic Quadrant participants' market growth in the 5% to 10% range for 2016; however, we expect cloud services to continue to outperform on-premises solutions with growth in the 10% to 20% range. Growth in on-premises solutions will be driven mostly from existing customers upgrading physical appliances to accommodate growing Web traffic volume. Cloud growth will primarily come from the replacement of on-premises solutions. Both cloud and on-premises will also benefit from additional spend for more advanced security features (i.e., network sandboxing and other advanced threat defense technologies).

Note 1
Adjustment to 2014 Market Statistics (as Reported in the 2015 Secure Web Gateway Magic Quadrant)

We downgraded the 2014 market share attributed to cloud services as a result of improved transparency from vendors with regard to on-premises versus cloud versus hybrid revenue mix. We also downgraded the 2014 market size, due to a methodology change. Market size has been derived only from the estimated revenue of vendors that have been included in this Magic Quadrant.

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 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.

About

Careers

Newsroom

Policies

Privacy

Site Index

IT Glossary

Contact Gartner