Magic Quadrant for Secure Web Gateways

Published 11 November 2019 - ID G00380121 - 35 min read

By Analysts Lawrence Orans, John Watts, Peter Firstbrook

Rapid growth of cloud-based secure web gateway services has become a disruptive force in the market. SWG vendors are adding cloud access security broker, remote browser isolation, firewall and other advanced features to enhance the security of their platforms.

Market Definition/Description

The rapid adoption of SaaS applications such as Microsoft Office 365, Salesforce and others is driving enterprises to adopt cloud-based secure web gateway (SWG) services. Enterprises are rearchitecting their WANs so that web traffic from remote offices flows directly to the internet (via local internet breakout connections), instead of backhauling it over expensive MPLS links to a centralized data center. As part of this rearchitecture, enterprises are utilizing cloud-based security stacks, so that web traffic from remote offices first flows through a cloud security service (mostly SWG services) before it reaches its final internet destination. A secondary driver for the adoption of these cloud services is the need to protect mobile laptops when they are off the corporate network.

We continue to see interest from enterprises seeking to integrate cloud access security broker (CASB) and SWG functionality. SWG vendors are responding to this trend, by either acquiring CASB technology or partnering with CASB providers (mainly Microsoft and its Cloud App Security service) to deliver more tightly integrated CASB and SWG solutions. CASB vendor Netskope is also addressing this trend, as it continues the development of its SWG solution introduced in 2018.

Gartner also sees growing demand for remote browser isolation (RBI) technology, which renders the image of a website in the cloud and sends an image to a user's browser (cloud-averse customers can also implement RBI technology in their own data centers). Mostly, customers are implementing RBI as a feature of SWGs, so that uncategorized or risky websites can be rendered via the RBI technology. However, some highly security-conscious organizations have completely replaced their SWGs with RBI technology.

Magic Quadrant

Figure 1. Magic Quadrant for Secure Web Gateways

Source: Gartner (November 2019)

Vendor Strengths and Cautions

Barracuda

Based in Campbell, California, Barracuda provides a broad array of cost-effective and easy-to-use virtual or physical network security, storage, email security and productivity solutions, designed to target midsize businesses. In June 2019, Barracuda terminated its Web Security Service and officially launched its replacement, Barracuda Content Shield (BCS). BCS is a cloud-based recursive DNS service. Barracuda also offers its Web Security Gateway (WSG) appliances, for customers that prefer on-premises solutions. These appliances are good candidates for midsize businesses and cost-conscious enterprises looking for simple, on-premises appliances. The BCS cloud service may also be a good option for the same

Strengths

- MSP partners benefit from Barracuda's integration of the BCS service and WSG appliances with the vendor's ECHOplatform, a centralized portal that enables managed service providers (MSPs) to manage customer accounts.
- Barracuda provides centralized policy management and reporting across all its appliances. Its CloudGen Firewall product includes SD-WAN functionality and simplifies web traffic redirection to the Barracuda WSG.
- Barracuda's appliance 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.
- Barracuda's Instant Replacement program, which provides next-business-day shipping of replacement units, includes a free appliance replacement unit every four years.

Cautions

- Dedicated focus on the midmarket has resulted in solutions that are missing or late with features favored by large enterprise customers. For example, Barracuda has yet to offer CASB functionality, and its BCS service lacks data loss prevention (DLP) support.
- Unlike some other cloud-based recursive DNS services, BCS does not support selective proxying. Competing solutions use this feature to enhance the accuracy of malware detection by providing deeper inspection for websites categorized as risky.
- Barracuda does not offer any hybrid functionality to simplify the management of a combination of its appliance and cloud-based solutions.
- The vendor's website for providing the status of its cloud-based BCS service is lacking when compared to other vendors in this market. It does not provide details (for example, downtime information) for each specific BCS point of presence.
- The dashboard for BCS does not assign severity indicators to threats.

Cisco

Cisco is a large network, infrastructure and security vendor, based in San Jose, California. Cisco offers an on-premises Web Security Appliance (WSA; hardware or virtual) and Cisco Umbrella, which provides recursive DNS security as well as a SWG, firewall as a service (FWaaS) and CASB functionality in a single cloud console called the Umbrella Secure Internet Gateway (SIG), released in July 2019. Cisco's security product portfolio includes many solutions and it has grown organically and through acquisition over the past few years. It offers endpoint security client Cisco AMP, Cisco AnyConnect (VPN client), Stealthwatch and Stealthwatch Cloud

Cisco focuses most of its SWG engineering efforts on its Umbrella product offerings. Its Cloud Web Security (CWS) is set for end of life in 2019 and customers are actively migrating away from the solution. Cisco's WSA is a good option for most midsize to large enterprises, especially those with an on-premises-only requirement. Umbrella is a good cloud option for most organizations.

Strengths

- Customers of Cisco's web security products, either on-premises or in the cloud, have several options for advanced threat capabilities with extensive threat intelligence from its Talos organization.
- Cisco has integrated WSA and Umbrella into Cisco Threat Response (CTR), along with other Cisco and non-Cisco security products to correlate events to allow security teams to investigate the root cause of a security incident.
- Cisco's recursive DNS security offering in Umbrella has been consistently cited by clients for its ease of use and effectiveness. A customer can get started with a simple DNS server address change to add immediate cloud-based protections against malware, phishing, DNS tunneling exfiltration, command-and-control callbacks, and web filtering.
- Cisco offers a patent-pending Anycast feature for connecting to cloud SWG instances, which allows for connections to the cloud to be made from a single data center and fail over to another data center without intervention by the customer.

Cautions

- The recently released FWaaS offering, included in the same console as part of the SIG package, does not currently provide Layer 7 firewalling capabilities or intrusion detection and prevention system (IDPS) security.
- Hybrid deployments lack feature parity and seamless integration between the two products. For example, the policies share common categories, but must be managed separately. The WSA product features a robust DLP capability, whereas the cloud depends on the Cloudlock CASB for DLP.
- With the 2019 end-of-life support for CWS, Gartner clients that are existing Cisco customers are investigating Umbrella to replace CWS, but find that there is a lack of feature parity between the two. Organizations looking for a similar product should consider the new SIG Essentials offering; however, with its additional functionality, there can be an increase in cost.
- Although Cisco's recursive DNS service has proven 100% uptime since 2006, the addition of the SIG full inspection proxy has yet to prove the same capability. In addition, Cisco does not support Generic Routing Encapsulation (GRE) tunnels for connecting to its cloud service.

Based in Canberra, Australia, ContentKeeper offers a family of SWG appliances that are implemented in transparent bridge mode. Its primary markets are Australia, where it focuses on the government, large enterprise and education markets, and the U.S., where it focuses on the education market. In 2019, the vendor enhanced its reporting and dashboard functionality. ContentKeeper's performance-oriented appliances and its support for mobile devices, including 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

- ContentKeeper's new dashboard and reporting features provide clear visibility into a customer's environment. For example, a CIO dashboard shows a good high-level overview of web activity. Advanced features such as geofencing and application control (for example, blocking Tor traffic) can be easily configured.
- Strong support for mobile devices enables ContentKeeper to appeal to K-12 school districts and other organizations that issue Chromebooks and tablets to users.
- The bridge-based Secure Internet Gateway has been designed for high throughput. Customer references report that it operates at more than 3 Gbps.
- Support for TLS/SSL is strong. Customer references report that it can terminate and inspect TLS/SSL traffic with minimal impact on performance.

Cautions

- ContentKeeper is one of the smallest vendors in this Magic Quadrant, and it lacks the resources to compete as a leading security vendor in the SWG market.
- ContentKeeper's cloud service has a limited footprint, with only four points of presence (Canberra, Australia; Wellington, New Zealand; Dallas, Texas and Los Angeles, California). The cloud service also lacks some enterprise functionality, such as "one-click config" for Microsoft Office 365.
- At the time of this writing, the solution has no CASB functionality. ContentKeeper is in the early stages of integrating with Microsoft's CAS service.
- ContentKeeper has a limited presence outside the U.S. and Australia. Potential customers in Europe and other areas should validate ContentKeeper's ability to support them.

Forcepoint

Headquartered in Austin, Texas, Forcepoint sells a broad line of security products, including SWGs, secure email gateways, firewalls (including an SD-WAN feature), CASB, DLP, and insider threat and behavioral analytics. The SWG solution is available in an appliance form factor

unifies a DLP agent and an agent that forwards data from the endpoint to the Forcepoint firewall. Also in 2019, Forcepoint partnered with Ericom to offer a remote browser isolation service. Forcepoint is a good solution for enterprises seeking a single vendor for its secure web, email, DLP and CASB functionality.

Strengths

- Forcepoint's pricing structure provides a single SKU, which enables customers to choose the type of deployment (on-premises, cloud or hybrid). This approach allows customers to easily transition from an appliance to a cloud-based implementation at any time during their subscription. Virtual appliances are provided free of charge.
- Forcepoint provides basic CASB and DLP functionality in its core package. Customers have the option to purchase advanced functionality at an additional price.
- With its Forcepoint One Endpoint agent, the vendor has a good strategy for protecting mobile laptops. The unified agent supports the typical mobile worker scenario, where the employee is off the corporate network and can connect to a cloud-based proxy. The agent also provides additional flexibility by addressing use cases where the cloud-based proxy connection is blocked by network conditions (e.g., when the employee is a guest on another enterprise's network). By enforcing policy at the agent, customers can enforce their own blocking policies and monitor internet use, regardless of the network environment.
- The Cloud App Control module for SWG is an optional add-on that provides in-line (proxy) control for as many as 15 cloud applications, selectable by the customer. This is available for on-premises and cloud web customers, without requiring purchase of the full Forcepoint CASB service.
- Forcepoint has a strong offering for organizations that are interested in a hybrid SWG strategy (on-premises and cloud-based). Its management console provides a common point for policy management, and for reporting and logging in hybrid environments.

Cautions

- Unlike many other cloud providers in this market, Forcepoint's SLA does not address latency.
- Forcepoint lacks experience in supporting network tunnels (IPsec and GRE), which are the most common approaches for redirecting traffic to a cloud-based SWG service. Less than 5% of traffic to Forcepoint's cloud SWG travels over network tunnels. Customers planning to implement tunnels to Forcepoint's cloud should test this function carefully.
- The vendor's website for providing the status of its cloud-based service is lacking when compared to other vendors in this market. It does not provide historical details on a site-by-site basis for each specific data center.

user basis.

- At the time of this writing, Forcepoint's Web Secure Gateway appliance has the lowest Overall Rating score (4 out of 5) on Gartner's Peer Insights (for vendors analyzed in this Magic Quadrant with a minimum of 10 customer ratings).

iboss

Based in Boston, iboss' cloud solution is built on a proprietary, node-based technology, which it refers to as "containerized gateways." Customers have the option to adopt the public cloud service operated by iboss, or they can implement the same containerized gateways in their own private cloud. Customers in need of a hybrid solution can integrate their own private cloud with the iboss public cloud. In 2019, iboss expanded its application controls and reporting to secure application data at rest (for example, removing unauthorized files from Dropbox). The vendor has demonstrated an ability to win large deals when competing against leading SWG vendors, and it is a good option for small and midsize businesses (SMBs) and large enterprises.

Strengths

- The node-based approach of the cloud service is strong, because it enables a smooth transition from a private cloud (hosted or on-premises) to a public cloud or hybrid implementation. The solution is designed to offer all features and functions across any deployment model (on-premises, cloud or hybrid).
- Iboss' cloud architecture preserves the customer's source IP address after traffic exits the iboss cloud. This is helpful, because some SaaS providers apply policies based on a customer's source IP address.
- Iboss' partnership with Verizon enables it to deploy containerized gateways throughout Verizon's worldwide infrastructure (more than 110 points of presence). Verizon has also licensed the iboss technology as part of an OEM agreement.
- Iboss has demonstrated an ability to develop technology partnerships that enable it to quickly respond to market dynamics. Examples include Menlo Security, FireEye and Microsoft's Cloud App Security service.

Cautions

- Iboss does not own the CASB technology necessary to achieve API integration with popular SaaS applications such as Salesforce, ServiceNow and others. It relies on its partnership with Microsoft and its Cloud App Security service for this functionality (iboss has developed its own API integration for some Google applications).
- Iboss' partnership with Verizon is a positive step, but it needs more large internet service provider (ISP) and managed security service provider (MSSP) partners to actively sell its

- Iboss attributes a small percentage of its sales to the Asia/Pacific (APAC) region. Prospective customers in this area should validate that the vendor's partners are qualified to provide sales support.

McAfee

Headquartered in Santa Clara, California, McAfee offers McAfee Web Gateway (MWG), a family of on-premises SWG appliances, and McAfee Web Gateway Cloud Service (WGCS), a cloud-based SWG service. In 2019, McAfee reintroduced its cloud-based advanced threat detection (ATD) service (it had briefly terminated the service in 2018). McAfee's appliance solutions and its cloud service are good candidates for most enterprise customers, particularly those that are already McAfee ePolicy Orchestrator users.

Strengths

- MWG and WGCS have strong malware protection, due to embedded browser code emulation capabilities and the Gateway Anti-Malware (GAM) feature, which provides the ability to adjust the sensitivity of malware detection. A rule-based policy engine enables flexible policy creation.
- McAfee owns strong CASB technology (from its 2017 acquisition of Skyhigh Networks) and strong DLP technology. It has a good strategy to tightly integrate these technologies with its SWG (although it is only in the early stages of execution).
- McAfee is one of the first vendors in the SWG market to support the TLS 1.3 protocol in its cloud service and appliances.
- McAfee has strong support for Microsoft Teams. It can enforce DLP, threat protection and activity monitoring within Teams.

Cautions

- McAfee has limited deployments with a tunnel-based approach for linking headquarters and remote offices to its cloud. It lacks support for GRE tunnels, which is the most common form of traffic redirection to a SWG cloud service. McAfee customers primarily use an endpoint-based redirection approach.
- Unlike several other leading competitors in this market, McAfee does not offer a cloud-based firewall service.
- Policy synchronization can only be achieved by pushing policies on McAfee appliances up to the McAfee cloud. The synchronization is not bidirectional.
- McAfee needs to strengthen the sales and distribution channel for its SWG cloud service. It claims to have multiple Tier 1 communications service providers and MSSPs, but very few of

Menlo Security

Based in Palo Alto, California, Menlo Security provides an isolation-based SWG platform, which executes webpages on isolated browsers and mirrors the rendering to the end user's machine. A dual-engine approach uses the browser's Document Object Model (DOM) with Menlo Security's Smart DOM to ensure an optimal user experience. This eliminates malicious drive-by attacks and provides techniques that minimize the risk of downloaded files and password theft. The isolation-based solution can be delivered on-premises or from the Amazon Web Services (AWS) cloud (more than 95% of Menlo Security's customers use the cloud service). The vendor has several large-scale, global enterprise deployments and is a good choice for enterprises with a high priority on security.

Strengths

- The Menlo Security Isolation Platform (MSIP) applies remote browser isolation to protect endpoint devices from browser vulnerabilities, JavaScript redirects, Flash vulnerabilities and font/image vulnerabilities by rendering mirrored or transformed content to the user's local browser.
- Menlo Security offers DLP capabilities through an OEM partner. It has a strong capability to inspect uploaded files and all user inputs to a webpage, because of its unique architecture that does not depend on the proxy's ability to deconstruct user content as it is entered.
- The vendor isolates email links and attachments, including personal web mail, to protect against malware and thwart spear-phishing attacks. It also actively warns users at "time of click" to prevent credential theft.
- If policy allows users to download content, executable files can be inspected by the Menlo Security sandbox (the OEM provider is Sophos). The vendor can also leverage customers' Palo Alto Networks Wildfire and FireEye sandboxes already deployed, as well as other sandboxes via API integration, while documents can be converted into safe HTML/PDF files for local storage.
- Menlo Security supports HTTP/2 and QUIC natively because its remote browser instances are based on Chromium, unlike other SWGs, which must block the protocol to force a TCP connection.

Cautions

- Menlo Security is an emerging vendor that is less mature than larger competitors. It has received more than $160 million in financing, and is growing rapidly; however, it is not yet cash-flow-positive.
- The vendor depends on integration with partners such as Microsoft CAS and McAfee Skyhigh for CASB functionality, but it requires that the customer have a separate subscription for the

- Although Menlo Security offers an agent for managing traffic redirection on laptops, almost all customers still rely on less-secure proxy autoconfiguration (PAC) files only. The vendor does not offer a native mobile agent for Android or iOS, and it relies on unified endpoint management (UEM) tools to enforce PAC settings on those devices.
- The vendor does not provide FWaaS protection for all ports and protocols.
- Menlo Security's bandwidth controls lack common features, such as limiting file transfer size (the vendor's focus is on managing all video traffic from any website, and includes policy controls to predictably reduce video resolution and limit video bandwidth consumption).

Sangfor

Based in Shenzhen, China, Sangfor has two primary business units: network security and cloud computing. Within network security, SWG represents about one-quarter of its revenue. The remaining revenue in the network security business unit comes from its next-generation firewall (NGFW), VPN, WAN optimization controller (WOC), application delivery controller (ADC) and endpoint security products. Sangfor's SWG is called Internet Access Management (IAM). It comes in a hardware appliance form factor or as a virtual appliance. IAM is most frequently implemented in transparent bridge mode, and is also implemented in gateway mode (where it supports network address translation and other routing features). A small percentage of customers implement IAM in proxy mode.

In 2018, Sangfor added several security components to its cloud-based service, including NGFW, intrusion prevention system (IPS) and malware detection. The vendor also introduced SD-WAN capabilities. Also in 2018, it released a cloud-based management console, Platform-X, for managing IAM both on-premises and in the cloud. Sangfor also added a new Enterprise Mobility Management solution integrated with its cloud service, a closed-loop method for managing and controlling SaaS applications, and improved its DLP capability by adding features such as document discovery and optical character recognition (OCR). Nearly all of the vendor's revenue is generated in the APAC region. Sangfor is a strong candidate for organizations based in China and other supported countries in the APAC region.

Strengths

- Sangfor has strong application control features. It can apply granular policies to microblogging services, LINE, WhatsApp, Facebook and other web-based applications, and it also has developed network signatures based on traffic patterns to block port-evasive applications, such as BitTorrent and Skype. Due to its localized application database, Sangfor's application and URL visibility and control are particularly strong for the Asian market.
- The vendor's in-line transparent bridge mode enables flexible and granular bandwidth control capabilities. Policy controls can be configured based on users, applications, URL and traffic

- Sangfor's Business Intelligence is a big data analytics platform that is based on user traffic and behaviors. In addition, Sangfor SWG offers built-in user and entity behavior analytics (UEBA) features. The big data platform offers third-party integration as well as several built-in applications. For example, one application identifies abnormal behavior related to account sharing or account takeover.

Cautions

- Sangfor is behind many SWG competitors in CASB support. For example, it provides SaaS application discovery, but does not assign risk ratings to these applications. It also does not provide API integration with popular SaaS applications, nor does it partner with a CASB vendor to deliver the API integration.
- Sangfor does not currently provide a remote browser isolation service or integrations with partners to provide this capability natively from within its platform.
- Sangfor's cloud offering only has 10 data centers (all in China) today, and only offers a 99.95% SLA uptime guarantee for unplanned downtime. In addition, it does not support SAML-based authentication of users.
- To protect mobile Windows laptops, the vendor provides an agent that automatically connects to the Sangfor cloud service. All other operating systems require end users to establish a VPN tunnel to the Sangfor cloud service.

Symantec

In November 2019, Broadcom completed its acquisition of Symantec's enterprise security division for $10.7 billion.

Headquartered in Mountain View, California, Symantec offers appliance-based and cloud-based SWG solutions. It has the largest market share among SWG appliance vendors, and has the overall largest market share among all vendors in this Magic Quadrant (based on revenue).

In December 2018, Symantec announced that it will deliver a cloud-based firewall service based on technology that it is licensing from Fortinet. Gartner expects that this service will be generally available before the end of 2019. ProxySG appliances are good candidates for most large enterprise customers, particularly those requiring highly scalable SWGs. Symantec's cloud service is a good option for most enterprises, particularly those that require hybrid (cloud and on-premises) implementations.

Strengths

- The ProxySG and Advanced Secure Gateway (ASG) families remain the strongest proxies in the market in terms of breadth of protocols and the number of advanced features. They also support multiple authentication and directory integration options.

- Symantec's Web Security Service (WSS) cloud service has good support for Microsoft Office 365. Symantec peers traffic with Microsoft. Separate policies can be easily applied to various Office 365 applications (for example, SharePoint, Yammer and others).
- Symantec owns the remote browser isolation technology that it offers as a feature of its SWG. Uncategorized URLs can be directed to the isolation technology and sent as images to a user's browser.
- The vendor has integrated its DLP technology across its proxy and CASB solutions. For example, one set of DLP policies can be established and enforced across the cloud-based WSS and the CASB solution.
- Symantec 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 decrypt SSL/TLS traffic and feed it for inspection to Symantec and non-Symantec security solutions.

Cautions

- Symantec was voted the "most often replaced" in a Gartner survey of all vendors in this Magic Quadrant.
- The Symantec product line of appliances is expensive, because it requires multiple components. Symantec is one of the few vendors in this Magic Quadrant to charge extra for its reporting functionality and management console.
- Unlike other leading competitors, Symantec does not own the core firewall technology in its planned FWaaS solution (Gartner expects this service to be available in 1Q20). The technology is licensed from Fortinet. Gartner advises prospective customers to test this new service carefully, particularly the level of its integration with Symantec's WSS.
- Symantec does not have complete feature parity between its cloud-based WSS and its appliances. For example, malware hashes from the Symantec sandbox can be pushed from the ProxySG to the Symantec Endpoint Protection solution. This feature is not supported in the WSS cloud service.

Trend Micro

Based in Tokyo, Trend Micro is a provider of endpoint protection, content protection and application gateway solutions. Trend Micro did not respond to requests for supplemental information. Therefore, Gartner analysis is based on other credible sources, including public information. InterScan Web Security (IWS) is a software-only solution that can be deployed on-premises, in the cloud or as a hybrid solution. It is commonly sold as part of a Smart Protection Complete Suite from the vendor, utilizing its machine-learning-powered XGen security

primarily for SMBs that already have a strategic relationship with the vendor, or those looking for an SWG as part of a broader security suite.

Strengths

- Trend Micro is an established vendor in the malware protection market. Its IWS solution protects against advanced threats. It includes machine learning (only for the cloud-based service), botnet detection and threat sandboxing. Cloud sandboxing and DLP are included in the cloud SWG at no extra cost.
- A single licensing model enables customers to mix cloud and on-premises solutions, and the management console provides an integration point for synchronizing policies and reporting for cloud and on-premises users. Most customers report that deploying and managing IWS is easy, and support is good.
- Application control is strong. IWS appliances can set the time of day and bandwidth quota policies, as well as integrate with URL filtering policy.
- Trend Micro's cloud-based SWG service has good geographic coverage for the APAC region.

Cautions

- Trend Micro did not participate in the Magic Quadrant process this year and does not provide Gartner with financial or license information that would allow us to track its progress in this market. Based on our analysis, Trend Micro is not growing its market share.
- Trend Micro rarely leads the SWG market with new features. Rather, it is often a fast follower.
- Its customers tend to value product integration over advanced functions within a specific solution. Trend Micro's Cloud App Security is a separate product that is not integrated with the IWS offering.
- InterScan Web Security as a Service (IWSaaS) cloud service lags behind the competition in several areas. For example, it only offers 99.99% availability via its SLA, compared to leading cloud SWG vendors that offer 99.999% availability guarantees.
- Trend Micro has limited experience in connecting branch offices to its cloud service. The cloud solution is optimized for protecting mobile endpoints. Most customers use PAC files to redirect endpoint traffic to the cloud service.

Zscaler

Based in San Jose, California, ZScaler continues to capture a majority of the cloud installed base for the SWG market as one of the few pure cloud vendors in the market today. The ZScaler Internet Access (ZIA) service includes a base service that can proxy and filter web traffic

features. ZScaler Private Access (ZPA) is a zero trust network access (ZTNA) solution that ZScaler positions as a VPN replacement. ZIA directly peers with most of the popular SaaS providers, including Microsoft Office 365.

In May 2019, Zscaler acquired Appsulate, a web isolation platform, and is working on full integration with its offering. Zscaler also achieved FedRAMP Authorized status in the past year for both the ZIA and ZPA offerings, and has now fully incorporated its 2018 TrustPath acquisition to improve Zscaler's cloud sandbox threat prevention speed and efficacy. Zscaler is a strong choice for midsize and larger enterprises looking for a cloud-based SWG service.

Strengths

- ZScaler applies all its malware detection engines to all content, including SSL/TLS traffic (when decryption is enabled), regardless of site reputation or customer entitlements.
- All customers can use basic Layer 3 and Layer 4 firewall policies across all ports and protocols, including basic DNS and network address translation (NAT) services. For an additional cost, the NGFW service allows application, user, group and location policies, and full logging.
- ZScaler is the first cloud-based SWG in this Magic Quadrant to achieve FedRAMP Authorized certification, which makes it an attractive option for U.S. federal government agencies.
- ZScaler provides basic in-line proxy CASB functionality in its solution for common forward proxy use cases, such as cloud application discovery and control, threat prevention, and DLP integration. In the past year, it has added Bitglass as a CASB partner, in addition to Microsoft CAS and McAfee Skyhigh.
- ZScaler's large cloud footprint includes locations that are typically underserved by competing cloud SWG services (for example, the Middle East, Russia and Africa).

Cautions

- At the time of this writing, Zscaler is not yet shipping its internally developed out-of-band CASB technology that provides API integration with popular SaaS applications. In the past, it has relied on CASB partners for this functionality.
- ZScaler primarily focuses on midsize and larger enterprises. Gartner clients have reported frustration in dealing with the ZScaler sales cycle, especially if they are a small organization.
- Gartner clients report that Zscaler's services can be expensive, particularly when they add multiple optional features (for example, advanced sandboxing, firewall, and DLP functionality).
- The basic cloud sandbox service only handles .exe and dynamic-link library (DLL) files from

- Zscaler is not a good choice for enterprises that prefer an on-premises, appliance-based SWG. Although it offers its Private Service Edge to extend its cloud onto the customer's premises to enable hybrid deployments, the strategic focus of the vendor is its cloud-based service.

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

None

Dropped

None

Inclusion and Exclusion Criteria

The following 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, NGFW devices and IPSs that offer URL filtering and malware protection have

- 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.

Vendors We Are Watching

Netskope — In 2018, Netskope introduced its cloud SWG service. Netskope did not meet the financial or installed base metrics to be included in this Magic Quadrant.

Palo Alto Networks — Palo Alto's Prisma Access is a cloud security service. It has been excluded from this Magic Quadrant because the exclusion criteria exclude solutions based primarily on firewall technology.

Evaluation Criteria

Ability to Execute

Product or Service: This is an evaluation of the features and functions of the vendor's SWG solution. Cloud services, CASB functionality and ATD are weighted heavily to reflect the significance that enterprises place on these capabilities.

Overall Viability: This criterion 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. A vendor's market share is a heavily weighted factor for this criterion, followed by its overall growth

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.

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 Gartner Peer Insights data, Gartner's SWG customer reference survey 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

Evaluation Criteria ↓	Weighting ↓
Marketing Execution	Medium
Customer Experience	Medium
Operations	Not Rated

Source: Gartner (November 2019)

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. It 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 ATD, CASB and cloud-based services were rated highly, because these capabilities are evolving quickly and are highly differentiated among the vendors.

Geographic Strategy: This evaluates the vendor's strategy for penetrating geographic locations 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 ↓
Innovation	Medium
Geographic Strategy	Low

Source: Gartner (November 2019)

Quadrant Descriptions

Leaders

Leaders are high-momentum vendors (based on sales and mind share growth) with established track records in SWGs, as well as 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 portfolios. 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 (VAR) channel to sell on-premises appliances. They have also developed partnerships with ISPs and carriers to sell cloud services, often 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 or application control — but they lack the comprehensive features of Visionaries, and the market presence or resources of Challengers. Customers that

"best of need" solutions. Niche Players may also have a strong presence in a specific geographic region, but lack a worldwide presence.

Context

The SWG market is mature, and it is segmented between large enterprises and SMBs. Solutions aimed at SMBs are designed for ease of use, cost-effectiveness and basic security protection. SMB solutions are often offered as a bundled package with an email security solution and/or an endpoint offering. 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

Although cloud-based SWG services continue to grow 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 2018 was $2.0 billion, which represents a 26% growth rate over the 2017 market size of $1.6 billion. We estimate that cloud service revenue represented approximately 41% of the total in 2018. Cloud services have experienced a 26% five-year CAGR, whereas on-premises appliances have achieved a 7% five-year CAGR. We anticipate the growth rate for traditional appliances/software will be around 7% in 2019, while cloud service revenue will continue to grow by approximately 25%. The overall (appliances and cloud service) market growth rate will be approximately 26% year over year.

Growth in on-premises solutions will be driven mostly by existing customers upgrading physical appliances to accommodate growing web traffic volume. Cloud growth will primarily come from the replacement of on-premises solutions, and will be bolstered as enterprises add more-advanced security features (for example, remote browser isolation, sandboxing, outbound firewall services, etc.).

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,

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.

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.