Magic Quadrant for Secure Web Gateways

Published 8 December 2020 - ID G00465133 - 36 min read

By Analysts Lawrence Orans, John Watts

Initiatives: Infrastructure Security

Vendors are expanding their core SWG solutions to add more security features, including CASB, zero trust network access, FWaaS and remote browser isolation. These broader portfolios will appeal to security and risk professionals seeking to consolidate security vendors.

This Magic Quadrant is related to other research:

Critical Capabilities for Cloud-Based Secure Web Gateways

View All Magic Quadrants and Critical Capabilities

Market Definition/Description

This document was revised on 10 December 2020. The document you are viewing is the corrected version. For more information, see the Corrections page on gartner.com.

The secure web gateway (SWG) market is getting more competitive as new vendors have entered from other markets and are seeking to compete with the entrenched vendors. In this year’s Magic Quadrant, we have added two new vendors — Netskope and QI-ANXIN Technology Group (which is based in China and only targets Chinese enterprises). However, we are closely watching other vendors, especially Palo Alto Networks, Fortinet (which acquired OPAQ Networks) and Bitglass. None of these vendors have built their cloud security services on a traditional proxy architecture, but Gartner expects that they will compete aggressively in the market for SWG and cloud-delivered security services.

The work-from-home trend has accelerated the adoption of cloud-based security services and the SASE Framework outlined in The Future of Network Security Is in the Cloud. Before COVID-19, we saw the growth of popular SaaS applications, such as Salesforce and Microsoft Office 365, drive “direct to internet” connections from branch offices, which also drove the adoption of cloud-based security services. Many enterprises are now seeking more than just a proxy service in the cloud, as they add zero trust network access (ZTNA), remote browser isolation (RBI), sandbox, firewall as a service (FWaaS), data loss prevention (DLP) and other cloud-based security services. Because the trend toward cloud-based security services is so strong, we have prioritized cloud services over appliance solutions when analyzing the vendors for this Magic Quadrant.

Magic Quadrant
Vendor Strengths and Cautions

Barracuda

Barracuda is a Niche Player in this Magic Quadrant. Based in Campbell, California, the vendor’s operations are heavily focused on North America, although it has customers in Europe and a smaller presence in the Asia/Pacific region. Barracuda provides a broad array of virtual or physical network security, storage, email security and productivity solutions, designed to target midsize businesses. Barracuda offers its Web Security Gateway (WSG) appliances and Barracuda Content Shield (BCS), plus an agent-based web filtering solution delivered as a cloud service.

In 2020, Barracuda integrated BCS and WSG to offer a single management interface to define and apply a uniform web filtering policy across on-premises appliances and BCS. Barracuda SWG products are good candidates for midsize businesses and cost-conscious enterprises looking for simple, easy-to-use SWG products both on-premises and in the cloud.
Strengths

- Barracuda has shown some improvement in its cloud support with enhanced hybrid capabilities by integrating the ability to manage policy across both WSG and BCS, and it recently added historical uptime status to its cloud status page.
- Gartner clients give high marks to Barracuda for ease of deployment, ease of administration, and quality and availability of end-user training.
- 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.
- Managed service provider 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 to manage customer accounts.

Cautions

- Cloud-based SWG is not a primary focus for Barracuda. The service does not provide an SLA, selective proxy function or other advanced features commonly found in other cloud-based SWGs. Barracuda focuses on endpoint proxy functions rather than proxying traffic to the cloud. BCS makes up a small part of its overall SWG revenue.
- 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 cloud access security broker (CASB) functionality and its BCS service lacks data loss prevention (DLP) support.
- Barracuda has not expanded its cloud offering to add additional SASE platform features such as FWaaS, RBI or ZTNA.
- BCS lacks agent support for iOS and Android.

Broadcom (Symantec)

Broadcom (Symantec) is a Visionary in this Magic Quadrant. Headquartered in San Jose, California, Broadcom completed its purchase of Symantec’s enterprise security division in November 2019. Symantec’s operations are geographically diversified, and its SWG customers are mostly large and very large organizations. The Symantec Enterprise Division offers appliance-based and cloud-based SWG solutions. In 2020, the vendor migrated its cloud-based Web Security Service (WSS) to Google Cloud Platform.

The Broadcom acquisition has created challenges for Symantec, with many Gartner clients reporting issues with service and support. Many Symantec value-added reseller (VAR) partners have been alienated by changes instituted by Broadcom. The net effect has been that when customers of the Blue Coat ProxySG appliances are ready to move to a cloud-delivered SWG service, many of them are choosing a new vendor. ProxySG appliances remain a strong option for large enterprise customers that
wish to remain with appliance-based SWGs as a portion of their SWG deployment. WSS remains a competitive cloud-based SWG service, but Symantec needs to fix its support issues and strengthen its channel partnerships so that WSS can compete effectively in the market.

**Strengths**

- The ProxySG and Advanced Secure Gateway (ASG) families continue to be the strongest appliance-based proxies in the market in terms of breadth of protocols and number of advanced features.

- Symantec owns many of the core technologies outlined in Gartner’s SASE Framework. For example, it owns RBI (from the 2017 acquisition of Fireglass), ZTNA (from the 2019 acquisition of Luminate), and CASB (from the 2015 acquisitions by Blue Coat Systems of Perspecsys and Elastica).

- The vendor has integrated its strong DLP technology across its proxy and CASB solutions. For example, one set of DLP policies can be established and enforced across the on-premises proxy, cloud-based WSS, email and CASB solutions.

- Symantec provides strong support for SSL/TLS. All ProxySG models include SSL hardware assistance 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**

- For the second year in a row, Symantec was voted the “most often replaced” in a Gartner survey of all vendors in the Magic Quadrant.

- 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 FWaaS solution. The technology is licensed from Fortinet, which leaves Symantec vulnerable should market forces change. (In July 2020, Fortinet acquired OPAQ Networks, a cloud-delivered security service that competes against WSS and other cloud-based security services.)

- Customer feedback indicates dissatisfaction with Symantec sales support and service support since its acquisition by Broadcom.

**Cisco**

Cisco is a Challenger in this Magic Quadrant. Based in San Jose, California, the company’s operations are geographically diversified, and its SWG customers range from small to very large organizations. It offers an on-premises Web Security Appliance (WSA; hardware or virtual) and Cisco Umbrella, which provides recursive DNS security as well as SWG, FWaaS and CASB functionality in a single cloud console called the Umbrella Secure Internet Gateway (SIG). Umbrella SIG is also offered as an integrated package with Cisco’s SD-WAN solution.
Cisco focuses most of its SWG engineering efforts on its Umbrella product offerings. In the past year, Cisco released the cloud-based SecureX extended detection and response (XDR) platform included with Umbrella subscriptions. Cisco's WSA is a good option for most midsize to large enterprises, and its Umbrella suite also targets midsize to large enterprises.

**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's Umbrella product offerings allow organizations the opportunity to deploy a simple, inexpensive, recursive DNS service today and migrate to full inspection proxies over time.

- Cisco offers an Anycast feature for connecting to cloud SWG instances, which reduces deployment time and enables automated failover.

- The vendor is consolidating its Cloudlock CASB and SWG into a single platform, which aligns with market trends observed by Gartner toward CASB and SWG products combining into a single, tightly integrated product offering.

**Cautions**

- Cisco was late to the market with a full proxy cloud offering and continues to catch up. The FWaaS offering within SIG released Layer 7 firewalling capabilities this year, but did not include intrusion detection and prevention system (IDPS) security features.

- Hybrid deployments lack feature parity and seamless integration between the two products. For example, the policies share common categories, but must be managed separately.

- As of this writing, Cisco's Umbrella SIG offering has limited geographic coverage. It is available in approximately 70% of Cisco's cloud data centers and only supports IPsec tunnel connectivity to approximately half of its total cloud data centers.

- Cisco's has many cloud-based security services, but some are not tightly integrated. For example, Cisco offers Duo Beyond as a ZTNA product, but it is only partially integrated with Umbrella.

**ContentKeeper**

ContentKeeper is a Niche Player in this Magic Quadrant. 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. 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 on-premises or hosted web filtering and malware protection. In 2021, a key area of focus for ContentKeeper will be to tighten its integration with Microsoft's CASB service.
**Strengths**

- ContentKeeper’s 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, 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.

- Its cloud service has a much smaller footprint than its competitors. ContentKeeper’s cloud has only four points of presence distributed among the U.S., Australia and New Zealand. The vendor’s main cloud focus is to offer virtual instances of its appliances that customers must manage themselves in public or private clouds.

- Unlike many of its competitors, ContentKeeper has no SD-WAN partners.

- ContentKeeper has a limited presence outside the U.S. and Australia. Potential customers in Europe and other areas should validate its ability to support them.

**Forcepoint**

Forcepoint is a Challenger in this Magic Quadrant. Headquartered in Austin, Texas, the vendor’s operations are geographically diversified, and its SWG customers range from midsize to very large organizations. Forcepoint sells a broad line of security products, including SWGs, secure email gateways, firewalls (including an SD-WAN feature), CASBs, DLP and insider threat and behavioral analytics. The SWG solution is available in an appliance form factor and as a cloud service. In July 2020, Forcepoint announced its Dynamic Edge Protection suite of solutions, which includes the Cloud Security Gateway and private access (a ZTNA alternative to VPNs). In 2020, the vendor also provided more status and availability information about its cloud services via its website, and it enhanced its SLA. Forcepoint is a good solution for enterprises seeking a single vendor that offers an integrated suite of cloud-based security services.

**Strengths**

- Forcepoint’s pricing model 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
Caution

iboss

iboss is a Visionary in this Magic Quadrant. Based in Boston, Massachusetts, the vendor’s operations are mostly focused on North America, although it has a strong customer base in Europe, and smaller revenue streams from the Asia/Pacific region and Latin America. Its 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. The vendor supports IPv6, which has helped it win some opportunities with carriers. It has demonstrated an ability to win large deals when competing against leading SWG vendors, and iboss is a good option for small and midsize businesses (SMBs) and large enterprises.

Strengths
McAfee is a Challenger in this Magic Quadrant. Headquartered in San Jose, California, the vendor's operations are geographically diversified, and its SWG customers range from midsize to very large organizations. In October, 2020, McAfee launched an initial public offering (IPO).

McAfee introduced its Unified Cloud Edge (UCE) platform in February 2020. The core elements of UCE are the cloud-based SWG, CASB and DLP solutions. The vendor continues to sell its McAfee Web Gateway hardware appliances, and it offers a hybrid (cloud and on-premises) management solution. Also in February, McAfee gained a new CEO. In March, it acquired Light Point Security, an RBI vendor. McAfee’s UCE solution is a good candidate for most enterprise customers, particularly those that are already ePolicy Orchestrator users.

**Cautions**

- The vendor is an engineering-focused company, which Gartner believes has limited its growth. At the time of this writing, the Leadership Team page on iboss’s website does not include a chief marketing officer. Gartner believes that this lack of focus on marketing is a key reason that iboss’ name recognition lags behind several key competitors in the SWG market.

- Unlike several other competitors in this market, iboss does not own RBI technology. It partners with several small RBI vendors, but this partnership strategy leaves it vulnerable should market dynamics change.

- It does not own the CASB technology necessary to achieve API integration with popular SaaS applications such as Office 365, Salesforce 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 G Suite applications).

- The vendor needs to strengthen its sales and distribution channel. In particular, it needs more large ISP and managed security service provider (MSSP) partners to actively sell its solution. It has a partnership with Verizon, but it needs to add more Tier 1 partners.

## McAfee

McAfee is a Challenger in this Magic Quadrant. Headquartered in San Jose, California, the vendor's operations are geographically diversified, and its SWG customers range from midsize to very large organizations. In October, 2020, McAfee launched an initial public offering (IPO).

The node-based approach of the cloud service is strong because it enables a smooth transition from a private cloud 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).

The vendor’s cloud architecture preserves the customer’s source IP address after traffic exits the iboss cloud. This feature enables SaaS providers to apply policies based on a customer’s source IP address.

The vendor’s cloud architecture allows its customers to dictate the timetable for implementing feature updates. This capability gives customers complete control over their change control windows.

It has demonstrated an ability to develop technology partnerships that enable it to quickly respond to market dynamics. Examples include FireEye and Microsoft’s Cloud App Security service.

- The vendor’s cloud architecture preserves the customer’s source IP address after traffic exits the iboss cloud. This feature enables SaaS providers to apply policies based on a customer’s source IP address.

- The vendor’s cloud architecture allows its customers to dictate the timetable for implementing feature updates. This capability gives customers complete control over their change control windows.

- It has demonstrated an ability to develop technology partnerships that enable it to quickly respond to market dynamics. Examples include FireEye and Microsoft’s Cloud App Security service.

- Unlike several other competitors in this market, iboss does not own RBI technology. It partners with several small RBI vendors, but this partnership strategy leaves it vulnerable should market dynamics change.

- It does not own the CASB technology necessary to achieve API integration with popular SaaS applications such as Office 365, Salesforce 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 G Suite applications).

- The vendor needs to strengthen its sales and distribution channel. In particular, it needs more large ISP and managed security service provider (MSSP) partners to actively sell its solution. It has a partnership with Verizon, but it needs to add more Tier 1 partners.

## McAfee

McAfee is a Challenger in this Magic Quadrant. Headquartered in San Jose, California, the vendor's operations are geographically diversified, and its SWG customers range from midsize to very large organizations. In October, 2020, McAfee launched an initial public offering (IPO).

McAfee introduced its Unified Cloud Edge (UCE) platform in February 2020. The core elements of UCE are the cloud-based SWG, CASB and DLP solutions. The vendor continues to sell its McAfee Web Gateway hardware appliances, and it offers a hybrid (cloud and on-premises) management solution. Also in February, McAfee gained a new CEO. In March, it acquired Light Point Security, an RBI vendor. McAfee’s UCE solution is a good candidate for most enterprise customers, particularly those that are already ePolicy Orchestrator users.
**Strengths**

- McAfee's UCE service has strong malware protection due to embedded browser code emulation capabilities and the Gateway Anti-Malware (GAM) feature. McAfee includes an integrated RBI feature for high-risk URLs (this feature is included in all UCE packages).

- McAfee owns strong CASB technology (from its 2017 acquisition of Skyhigh Networks) and strong DLP technology. It has integrated CASB application recognition technology within UCE to strengthen web security policies.

- The vendor has strong support for Microsoft Teams. Its DLP technology can block sensitive data (for example, credit cards) from being transmitted in Teams.

- McAfee states that its five 9s of availability SLA for the Web Gateway Cloud Service has not been violated in three years. McAfee's cloud service status trust page prominently displays the service availability statistics for the past 90 days.

**Cautions**

- McAfee's cloud lacks a presence in mainland China and Africa. Customers that need to support users in these geographies should carefully test McAfee's cloud service.

- Unlike several other leading competitors in this market, McAfee does not offer a cloud-based network firewall service.

- Unlike several other leading competitors in this market, McAfee does not offer a ZTNA service.

- McAfee's Web Gateway Cloud Service lacks FedRAMP certification.

**Menlo Security**

Menlo Security is a Visionary in this Magic Quadrant. Based in Palo Alto, California, the vendor’s operations are geographically distributed across North America, Japan and the Asia/Pacific region, and Europe. Menlo Security provides an isolation-based SWG platform that executes webpages on isolated browsers and mirrors the rendering to the end-user's machine. Menlo Security's SWG can be delivered on-premises or from the cloud. The vendor primarily utilizes Amazon Web Services (AWS) cloud to host its service.

In September 2020, VMware announced that it will sell an SWG solution based on technology that it has licensed from Menlo. In the past year, Menlo introduced its own ZTNA product, Zero Trust Private Access, integrated with Azure Information Protection (AIP) to consume customer AIP sensitivity labels to apply to its DLP policies, and added its own native SaaS risk ratings for its CASB functionality. The vendor has many large-scale global enterprise and government deployments, and is a good choice for enterprises that give security high priority.

**Strengths**
The Menlo Security Isolation Platform (MSIP) offers RBI as a default, rather than by exception to protect endpoint devices from web-based attacks rendering mirrored or transformed content to the user's local browser.

Menlo Security offers a native DLP capability to inspect uploaded files and user inputs.

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.

Executable files that have been downloaded by the user can be inspected by the Menlo Security sandbox (the OEM provider is Sohpos). Menlo Security can send suspicious files to Palo Alto Networks’ WildFire or FireEye's sandboxing services.

### Cautions

- Menlo Security is smaller than most competitors in the SWG market. In addition, more SWG vendors now own and offer native RBI as a feature of their SWG platforms (typically deployed for limited use cases), competing more directly with Menlo Security.

- Although it 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.

- Menlo Security’s FWaaS does not provide support for Layer 7; it only provides support for Layer 3 and Layer 4.

- Menlo Security lacks full CASB functionality. It can isolate SaaS application access in forward proxy mode to apply CASB controls for SaaS access, but it does not integrate with SaaS applications via API (for data-at-rest DLP use cases).

### Netskope

Netskope is a Visionary in this Magic Quadrant. Based in Santa Clara, California, the vendor’s operations are heavily focused on North America, although it has customers in Europe and a smaller presence in the Asia/Pacific region and Latin America. Netskope began shipping a CASB offering in October 2013, and introduced its cloud-based SWG in March 2018 and a ZTNA product called Netskope Private Access (NPA) in 2020. Netskope is new to the SWG Magic Quadrant this year. It hosts its products on its NewEdge security cloud infrastructure, but also offers appliances for customers to deploy within their own data centers.

In the past year, Netskope expanded NewEdge from 14 data centers to 40 data centers while eliminating dependencies on public cloud infrastructure. Netskope is a good choice for enterprises of all sizes looking for cloud-based SWG that prioritizes advanced cloud SaaS with web DLP controls across SWG and SaaS applications.
Strengths

- Netskope has one of the most mature CASB products in the market today and has tightly integrated the SWG with the CASB policy to provide unified web security policies across general web and SaaS applications.

- The vendor has quickly grown its SWG business since its introduction in 2018. Gartner has observed significant interest in Netskope over the past year. It is increasingly being added to shortlists for SWG vendors, especially in cases where clients are looking for strong SWG and CASB integrated products.

- Netskope integrated DLP extends to SaaS and web, and can apply more advanced DLP features often seen from enterprise DLP suites, such as optical character recognition (OCR) and machine learning, to its DLP inspection engine to improve coverage and reduce false positive rates.

- Netskope offers its native security rating service, called Cloud Confidence Index (CCI), which provides web and SaaS insights and third-party risk ratings for tens of thousands of cloud apps.

Cautions

- Netskope's cloud service lacks some characteristics that are present in more mature SWG providers. For example, it lacks a public trust page for its cloud service that details the current cloud status and historical incidents and events. Netskope's SLA is not as strong as other vendors in the market.

- Most traffic to Netskope's cloud service is forwarded by agents that must be installed on a user's device. Customers planning to implement network tunnels (for example, IPsec or GRE) to redirect traffic to Netskope's cloud should test their implementations carefully.

- Netskope lacks some key features desired by customers of a cloud-based SWG, including a cloud-based FWaaS offering or native RBI product. Netskope offers Ericom Software as an OEM RBI product and can proxy chain to other RBI vendors.

- Netskope relies heavily on agents to steer traffic and has fewer SD-WAN partners today compared to other vendors in the market. Prospective customers looking for a SWG that is more tightly integrated with their SD-WAN provider should verify if their SD-WAN provider partners with Netskope.

QI-ANXIN Technology Group

QI-ANXIN Technology Group is a Niche Player in this Magic Quadrant. Based in Beijing, China, the vendor was founded in 2014 and was previously named 360 Enterprise Security Group (ESG). In addition to SWG solutions, the vendor competes in other cybersecurity markets, including endpoint, perimeter security, malware protection and big data analytics. QI-ANXIN focuses on selling SWG appliances to Chinese enterprises. It also offers a cloud service with a small footprint (all points of presence are in China). The SWG appliances can be implemented in transparent bridge mode or proxy mode. In 2021, a key area of focus for the QI-ANXIN Technology Group will be to strengthen its CASB support. The vendor is a good option for Chinese enterprises, particularly larger ones that will benefit from its scalable proxy appliances.
**Strengths**

- QI-ANXIN’s SWG appliances are high-performance proxies. The vendor states that its largest appliances have more than 300 Gbps of network processing capability and more than 100 Gbps of application-layer processing capability.

- The solution has strong support for application control. It can detect and apply policies to more than 3,600 applications. It can also implement granular policies for popular social media applications.

- Support for SSL/TLS traffic is strong, including native support for TLS 1.3 decryption. The management console provides good visibility into the distribution of encrypted traffic (for example, TLS 1.3, TLS 1.2 and others), and it highlights decryption algorithms in use.

**Cautions**

- The vendor’s cloud offering only has seven points of presence (POPs) today, all in China.

- CASB support is limited. The QI-ANXIN solution has no API integrations with popular SaaS applications.

- Support for advanced cloud security functionality is lacking. For example, the solution does not offer RBI or FWaaS functionality.

**Sangfor Technologies**

Sangfor Technologies is a Niche Player in this Magic Quadrant. Based in Shenzhen, China, Sangfor has two primary business units: network security and cloud computing. Within network security, SWG represents about 20% of its revenue. Sangfor’s SWG is called Internet Access Management (IAM). It comes in a hardware appliance form factor or as a virtual appliance. Sangfor also offers a cloud-based SWG.

In the past year, Sangfo introduced a new endpoint-initiated ZTNA product called Sangfor SDP. It also released a unified management platform for cloud and on-premises appliances called Platform-X. The vendor is a strong candidate for organizations based in China, particularly those that are midsize, and other supported countries in the Asia/Pacific region.

**Strengths**

- Sangfor has strong application control features for the Asian market. It can apply granular policies to social media services, such as 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.

- The vendor’s in-line transparent bridge mode enables flexible and granular bandwidth control capabilities. Policy controls can be configured based on users, applications, URLs and traffic quotas.

- Sangfor’s SWG offers built-in user and entity behavior analytics (UEBA) features and integration with its big data platform to enhance UEBA capabilities.
The vendor’s IAM solution integrates with other Sangfor security products, including DLP and endpoint security solutions.

**Cautions**
- Sangfor has significantly increased its number of cloud nodes from 10 to 51 in the past year, but they are all located in China. It also only offers an SLA for four 9s of availability.
- Sangfor’s CASB and ZTNA feature support is minimal. For example, it offers API integration with a limited number of popular SaaS applications (only Office 365 and Salesforce) at the time of this writing, and it started its ZTNA product as an on-premises-only service.
- Sangfor only supports proxy chaining for RBI and does not integrate partners to provide this capability natively from within its platform.
- To protect mobile Windows laptops, the vendor provides an agent that automatically connects to the Sangfor cloud service. Sangfor does not have an agent to connect Apple OSX, iOS and Android devices to its cloud service. Users must establish a VPN tunnel to connect these devices to its cloud service (PAC files can also be used for Android and iOS devices).

**Zscaler**
Zscaler is a Leader in this Magic Quadrant. Based in San Jose, California, the company’s operations are heavily focused on North America and Europe. Zscaler primarily offers a cloud-based SWG. The Zscaler Internet Access (ZIA) service is its primary web traffic proxy offering. ZIA also offers optional services that add FWaaS, cloud-based sandboxing, bandwidth control, DLP and other features. Zscaler Private Access (ZPA) is a ZTNA product that Zscaler positions as a VPN replacement.

In the past year, Zscaler acquired Edgewise Networks, an identity-based microsegmentation provider, and Cloudneeti for CSPM. Zscaler also completed integration of Appsulate’s technology (acquired in 2019) into ZIA for RBI. It also released Zscaler Digital Experience (ZDX), its entry into the digital experience monitoring (DEM) space, and its out-of-band CASB solution. Zscaler is a strong choice for large organizations 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, protocols and locations, including basic DNS and network address translation (NAT) services. For an additional cost, the NGFW service allows Layer 7 application control, advanced DNS, user and group policies, and full logging.
- Zscaler provides 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, Zscaler added API integrations with popular SaaS providers to extend DLP functionality to data at rest within these applications.

- Zscaler's large cloud footprint includes locations that are typically underserved by competing cloud SWG services (for example, Canada, the Middle East, Russia and Africa).

**Cautions**

- Zscaler's expansion into adjacent markets, such as CSPM and DEM, shows that it is looking to expand its markets beyond its traditional base. Gartner advises existing and prospective Zscaler customers to monitor support and sales quality as vendors that expand beyond their core market run the risk of losing focus on existing products.

- Zscaler primarily focuses on larger enterprises. Gartner clients have reported frustration in dealing with the Zscaler sales cycle, especially if they are a midsize organization typically with less than 3,000 seats.

- Zscaler's optional integrated DLP feature only extends to web and FTP protocols for inspection, and does not offer some advanced features such as the ability to apply DLP rules using OCR.

- As Zscaler has increased its market share in the SWG market, it is increasingly targeted by competitors both from within and external to the SWG market for replacements based on price or differentiating features, such as advanced integrated DLP or more comprehensive security suites.

**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**

- Netskope qualifies for the Magic Quadrant according to the qualifications listed in the Inclusion and Exclusion Criteria section.

- QI-ANXIN Technology Group qualifies for the Magic Quadrant according to the qualifications listed in the Inclusion and Exclusion Criteria section.

**Dropped**

- Trend Micro no longer meets the $20 million revenue target specified in the Inclusion and Exclusion Criteria section.

**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 intrusion prevention systems that offer URL filtering and malware protection have been excluded. This Magic Quadrant analyzes solutions that are optimized for SWG functionality.

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

**Honorable Mentions**

**Akamai** — This vendor expanded its SWG portfolio in 2020 by introducing its proxy-based solution (it had already been offering a recursive DNS service). We excluded Akamai from this Magic Quadrant because it does not yet meet the $20 million revenue target specified in the Inclusion and Exclusion Criteria section.

**Bitglass** — This vendor introduced its SWG solution in 2020, and it does not yet meet the $20 million revenue target specified in the Inclusion and Exclusion Criteria section. In 2021, Gartner expects Bitglass to compete for SWG opportunities against many of the vendors in this Magic Quadrant.

**Fortinet** — This vendor acquired OPAQ Networks, a provider of cloud-delivered security services, in July 2020. OPAQ's service was based on firewall technology. Gartner expects Fortinet (OPAQ) to compete against many of the vendors in this Magic Quadrant in 2021. Fortinet is not included in this Magic Quadrant because the exclusion criteria applies to solutions based primarily on firewall technology.
Palo Alto Networks — The vendor’s Prisma Access is a cloud security service based on firewall technology. Palo Alto Networks is aggressively targeting customers seeking cloud-based security services, and it is already competing against many of the vendors in this Magic Quadrant. It has been excluded because the exclusion criteria applies to 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 are weighted more heavily than appliance-based products, due to the growing customer adoption of cloud-based services. CASB functionality is also a heavily weighted feature.

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 or service that potential customers are looking for.

Market 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 and feedback from Gartner clients during inquiries with analysts.
Table 1: Ability to Execute Evaluation Criteria

<table>
<thead>
<tr>
<th>Evaluation Criteria</th>
<th>Weighting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Product or Service</td>
<td>High</td>
</tr>
<tr>
<td>Overall Viability</td>
<td>High</td>
</tr>
<tr>
<td>Sales Execution/Pricing</td>
<td>NotRated</td>
</tr>
<tr>
<td>Market Responsiveness/Record</td>
<td>Medium</td>
</tr>
<tr>
<td>Marketing Execution</td>
<td>Medium</td>
</tr>
<tr>
<td>Customer Experience</td>
<td>Medium</td>
</tr>
<tr>
<td>Operations</td>
<td>NotRated</td>
</tr>
</tbody>
</table>

Source: Gartner (December 2020)

Completeness of Vision

Market Understanding: This is the SWG vendor’s ability to understand the buyer’s 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 ZTNA, 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

<table>
<thead>
<tr>
<th>Evaluation Criteria</th>
<th>Weighting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Market Understanding</td>
<td>Medium</td>
</tr>
<tr>
<td>Marketing Strategy</td>
<td>NotRated</td>
</tr>
<tr>
<td>Sales Strategy</td>
<td>High</td>
</tr>
<tr>
<td>Offering (Product) Strategy</td>
<td>High</td>
</tr>
<tr>
<td>Business Model</td>
<td>NotRated</td>
</tr>
<tr>
<td>Vertical/Industry Strategy</td>
<td>NotRated</td>
</tr>
<tr>
<td>Innovation</td>
<td>Medium</td>
</tr>
<tr>
<td>Geographic Strategy</td>
<td>Low</td>
</tr>
</tbody>
</table>

Source: Gartner (December 2020)

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 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. Often, Visionaries represent good acquisition candidates. Thus, these vendors represent a slightly higher risk of business disruptions.

**Niche Players**
Niche Players’ products typically are solid solutions in the use cases of URL filtering or malware detection, but they lack the comprehensive features of Visionaries, and the market presence or resources of Challengers. Niche vendors 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**
After analyzing the combined 2019 revenue of the SWG Magic Quadrant vendors, Gartner has determined that the overall size of the market is $2.17 billion. Approximately 54% of the revenue is from appliance-based products and the other 46% is from cloud-based services. However, if the two Chinese vendors (QI-ANXIN Technology Group and Sangfor) are excluded (the revenue from these vendors is heavily weighted toward appliances), then the revenue split between appliances and cloud services is nearly equivalent.

As the adoption of cloud-based security services grows, Gartner has observed a trend where enterprises seek to consolidate their security vendors. In a traditional data center with security appliances, it is still common to see a best-of-breed approach for vendor selection. However, when moving to cloud-based security services, Gartner has observed that enterprises often limit their cloud security providers to one or two vendors. Today, it’s still common for an enterprise to select Vendor A for its SWG service and Vendor B for its CASB service. However, as the SWG and CASB markets continue to converge, Gartner expects that enterprises will increasingly select a single vendor for SWG and CASB services. In many cases, they will also use the same vendor for other security services, including ZTNA, RBI, DLP, FWaaS, sandboxing
and others. Operationally, it is more challenging for enterprises to manage multiple cloud-based security vendors than it is to manage multiple appliance-based vendors. This is a key driver for the vendor consolidation phenomenon that Gartner has observed among the adoptees of cloud-delivered security services.

**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.

**Document Revision History**

- Magic Quadrant for Secure Web Gateways - 11 November 2019
- Magic Quadrant for Secure Web Gateways - 26 November 2018
- Magic Quadrant for Secure Web Gateways - 12 June 2017
- Magic Quadrant for Secure Web Gateways - 6 June 2016
- Magic Quadrant for Secure Web Gateways - 23 June 2014
- Magic Quadrant for Secure Web Gateways - 28 May 2013
- Magic Quadrant for Secure Web Gateway - 25 May 2011
- Magic Quadrant for Secure Web Gateway - 8 January 2010