Cuadrante mágico para puertas de enlace web seguras

Publicado el 26 de noviembre de 2018 - ID G00 335718 - lectura de 35 minutos

Por los analistas Lawrence Orans, Peter Firstbrook

El mercado de la puerta de enlace web segura sigue estando dominado por los dispositivos; Sin embargo, el rápido crecimiento de los servicios en la nube se está convirtiendo en una fuerza disruptiva en el mercado. Muchos proveedores han agregado la funcionalidad de agente de seguridad de acceso a la nube a través de asociaciones o adquisiciones de tecnología.

Definición / Descripción del Mercado

El mercado de servicios de pasarela web segura (SWG) basada en la nube continúa creciendo más rápidamente que el mercado de SWG basados en dispositivos. (La tasa de crecimiento anual compuesta de cinco años [CAGR] para los servicios en la nube de SWG es del 32%, y la tasa de crecimiento anual de cinco años para los aparatos de SWG es del 5%.) Sin embargo, en 2017, se gastó más dinero para comprar aparatos de SWG (74% de ingresos del mercado) que los servicios de nube SWG (26%).

El principal impulsor para el crecimiento de los servicios de SWG en la nube es la rápida adopción de aplicaciones de software como servicio (SaaS), particularmente las dominantes (por ejemplo, Office 365 y Salesforce). En lugar de redirigir el tráfico web a través de costosas conexiones de conmutación de etiquetas multiprotocolo (MPLS), las empresas están implementando rupturas locales de internet desde oficinas remotas y enviando tráfico web directamente a internet. Este enfoque exige un cambio en la arquitectura de seguridad de la empresa, y la mayoría está optando por adoptar un servicio SWG basado en la nube. Un conductor secundario lejano para la adopción de estos servicios es la necesidad de proteger a los usuarios móviles cuando están fuera de la red corporativa.

Los corredores de seguridad de acceso a la nube (CASB) han surgido como un mercado adyacente a SWG ("Cuadrante mágico para corredores de seguridad de acceso a la nube"). Los SWG brindan visibilidad del comportamiento web de los usuarios, y los CASB brindan visibilidad del comportamiento de las aplicaciones SaaS de los usuarios (por ejemplo, las aplicaciones SaaS que han visitado y la clasificación de riesgo de esas aplicaciones). Muchos de los proveedores en este Cuadrante Mágico han adquirido proveedores de CASB, incluidos Symantec (Blue Coat adquirió Elastica y Perspecsys), Cisco (CloudLock), McAfee (Skyhigh Networks) y Forcepoint (SkyFence). Otros, incluidos Zscaler e iboss, tienen sociedades con Microsoft y su aplicación de seguridad en la nube CASB. En 2018, el proveedor de CASB Netskope agregó la funcionalidad básica de SWG a su servicio en la nube. Gartner cree que la visibilidad de la aplicación SaaS (y

otras funciones) provista por CASB es un elemento importante de la seguridad web, y enfatizamos las capacidades de CASB en mayor medida en nuestras puntuaciones de Completeness of Vision este año.

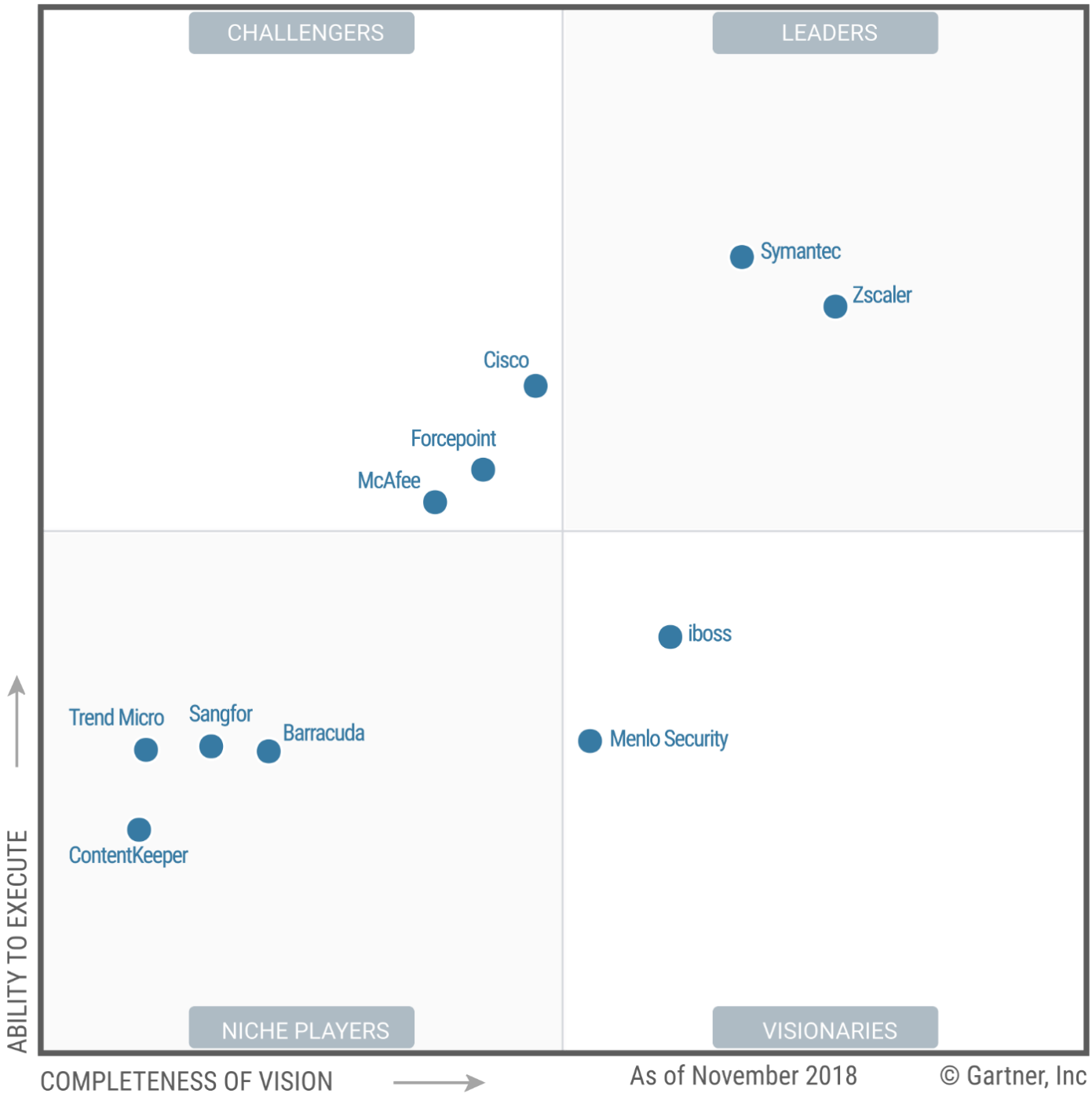
Gartner ha seguido monitoreando el impacto de las soluciones de aislamiento de navegadores remotos en el mercado SWG. Estas soluciones representan la imagen de un sitio web en la nube o en un dispositivo en el centro de datos del cliente, y envían esta imagen al navegador del usuario. Esta técnica protege los puntos finales de las amenazas web típicas mediante la ejecución y la representación de todo el contenido de forma remota. Lo ideal es que el navegador del usuario no genere ningún contenido malicioso y que la interacción web se pueda controlar de forma estricta.

Este año, Menlo Security, el mayor de los proveedores de aislamiento de navegadores remotos puros, calificó para ser incluido en este Cuadrante Mágico. También estamos siguiendo de cerca a Cyberinc y otros proveedores en este mercado. En julio de 2017, Symantec adquirió Fireglass, otro proveedor de aislamiento de navegador remoto, y ahora ofrece esta capacidad como una característica de su SWG.

Otro mercado emergente que Gartner está siguiendo de cerca son los cortafuegos basados en la nube. Los proveedores en este mercado basan su tecnología subyacente en firewalls en la nube y ofrecen pilas de seguridad, incluido el filtrado de URL, sandboxing y otras funciones. Los proveedores en esta categoría incluyen Cato Networks, OPAQ, CenturyLink (Level 3 Communications y su servicio Adaptive Network Security) y Palo Alto Networks (GlobalProtect Cloud Service). Gartner ve principalmente estos servicios en el mercado medio, y sus conjuntos de características los posicionan para competir contra los proveedores de SWG.

Cuadrante mágico

Figura 1. Cuadrante mágico para puertas de enlace web seguras



Fuente: Gartner (noviembre de 2018).

Fortalezas y precauciones del vendedor

Barracuda

Con sede en Campbell, California, Barracuda ofrece una amplia gama de soluciones de seguridad de red virtual, física o virtual, rentables y fáciles de usar, diseñadas para el mercado de pequeñas y medianas empresas (PYME). En 2018, Barracuda terminó su sociedad de revendedor con Zscaler, e introdujo Barracuda Content Shield (BCS), un servicio de nube SWG basado en DNS. Los dispositivos Barracuda Web Security Gateway son buenos candidatos para pequeñas y medianas empresas y empresas preocupadas por los costos que buscan dispositivos sencillos locales o soluciones de proveedor de servicios de seguridad administrada (MSSP).

Fortalezas

- Los módulos de hardware Secure Sockets Layer (SSL) para dispositivos más grandes y la gestión de certificados y configuración recientemente simplificada facilitan la inspección del tráfico de Seguridad de la capa de transporte (TLS) / SSL.
- Barracuda proporciona administración centralizada de políticas y generación de informes en todos sus dispositivos. Su producto NextGen Firewall simplifica la redirección del tráfico web a Barracuda Web Security Gateway.
- El modelo de precios de electrodomésticos de Barracuda le permite ser la alternativa de bajo costo en muchos acuerdos competitivos. Se cobra por la capacidad del dispositivo y no agrega un cargo de suscripción por usuario.
- El programa de Reemplazo Instantáneo de Barracuda, que proporciona el envío al día hábil siguiente de las unidades de reemplazo, incluye una unidad de reemplazo de electrodomésticos gratuita cada cuatro años.

Precauciones

- El enfoque dedicado en el mercado mediano ha resultado en soluciones faltantes o tardías con características favorecidas por grandes clientes empresariales. Por ejemplo, Barracuda aún tiene que ofrecer CASB o la funcionalidad nativa de prevención de pérdida de datos (DLP).
- El BCS basado en la nube es un nuevo servicio que ha estado disponible solo desde septiembre de 2018. Los posibles clientes deben probar este servicio detenidamente antes de suscribirse. El BCS es el tercer intento de Barracuda de ofrecer un servicio SWG basado en la nube.
- Barracuda no ofrece ninguna funcionalidad híbrida para simplificar la administración de una combinación de sus dispositivos y soluciones basadas en la nube.

Cisco

Based in San Jose, California, Cisco offers an on-premises Web Security Appliance (WSA; hardware or virtual) and a DNS/proxy-based solution called Cisco Umbrella. Most engineering and go-to-market efforts focus on the Umbrella cloud security platform, with plans for continued integration with firewall, proxy, CASB, and WAN edge — for example, software-defined WAN (SD-WAN) capabilities — with connectors to Cisco network and virtual private network (VPN) products. Cisco's Cloud Web Security (CWS), a proxy-based service, is being phased out. Cisco's WSA is a good option for most midsize to large enterprises. Umbrella is a good cloud option for most organizations.

Strengths

- Customers of Cisco's web security suites have several options for advanced threat capabilities, and Cisco has extensive threat intelligence from its Talos organization.

- Umbrella can now provide visibility into the SaaS, platform as a service (PaaS) and infrastructure as a service (IaaS) services that are in use, including risk and compliance information. Bypassing proxy inspection for known good cloud services enhances performance.
- Cisco has begun to integrate CASB functionality (from its 2016 acquisition of CloudLock) into its SWG solutions. The Umbrella console uses the technology to discover SaaS applications and assign a risk rating to each application, with the ability to block unwanted apps via the Umbrella policy. Customers do not need to purchase a CASB license to benefit from this feature. WSA customers can use their in-product navigation to configure CloudLock application discovery.
- Umbrella's DNS-based redirection to the cloud is simple to implement. Cisco AnyConnect includes a module for Umbrella to forward DNS traffic, as well as identities to the cloud service. Cisco also offers a stand-alone Umbrella roaming client and Cisco Security Connector (CSC) for iOS.

Cautions

- Cisco's acquisition strategy has resulted in a confusing array of products and options that are still only in the early stages of an integration. Not all features are available on all delivery forms.
- Most web requests in the Umbrella service are not proxied and inspected. When the selective proxy is used, malicious URL filters, plus Cisco AMP- and AV-based file inspection, are available, but file sandboxing and script detection are not. Sites not deemed potential threats by Umbrella's statistical and machine learning model or policy are accessed directly by the client with no in-line inspection. This direct access to the internet makes content sandboxing, granular application control, in-line data DLP, rate shaping, bandwidth quotas and full traffic analysis unavailable. For example, traffic to popular content storage sites (e.g., Dropbox and Google Drive) and web mail sites is not decrypted and inspected (because of their good reputation), despite their increasing use in phishing attacks.
- Hybrid deployments lack seamless policy integration. Cisco's Web Security Reporting Application is required in the customer's environment to achieve unified reporting across the Cisco SWG appliances and cloud service. Policy is separate.
- Umbrella log data cannot automatically be directly exported to a security information and event management (SIEM) system. It must be exported to an AWS S3 bucket, then from S3 to a SIEM. Cisco provides the required AWS S3 bucket at no additional charge.
- Umbrella support for Android lags its iOS and ChromeOS support for off-network users. The Cisco Security Connector, which provides DNS-based traffic redirection and DNS traffic encryption using native Apple APIs, is only available on iOS.

ContentKeeper

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 2017, ContentKeeper retired its sandbox appliance and moved its sandboxing functionality into the cloud. 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

- 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.
- Strong support for mobile devices enables ContentKeeper to appeal to K-12 school districts and other organizations that issue Chromebooks and tablets to users.
- ContentKeeper's load balancer appliance is a cost-effective alternative to industry-leading, multipurpose load balancers, which are also known as application delivery controllers (ADCs).

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. Prospective customers of its cloud sandboxing service should test its efficacy.
- ContentKeeper's cloud service has a limited footprint, with only three points of presence (Canberra, Australia; Wellington, New Zealand; and Los Angeles, California).
- The solution has no CASB functionality, and ContentKeeper lacks partnerships with CASB vendors.
- 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 and firewalls. The SWG solution is available in an appliance form factor (hardware and software) and as a cloud-based service. In 2017, Forcepoint acquired the Skyfence CASB business from Imperva and acquired user and entity behavior analytics (UEBA) vendor RedOwl.

In 2018, it introduced the V20000 G1 appliance to target large enterprises. Forcepoint claims that its performance is as much as 2.5 times faster than the V10000 appliance. At the same time, Forcepoint announced the end of sale for the X10G chassis. Forcepoint appliances are good options for MSEs or for larger organizations. The Forcepoint cloud service is a good option for enterprises that need to protect mobile employees.

Strengths

- A new pricing structure provides a single stock-keeping unit (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.
- Forcepoint has a good strategy for protecting mobile laptops. It offers two endpoint agents. The Proxy Connect agent supports the typical mobile worker scenario, where the employee is off the corporate network and can connect to a cloud-based proxy. The Direct Connect agent 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 Direct Connect agent, customers can enforce their own blocking policies and monitor internet use, regardless of the network environment.
- The Cloud App Control module (based on Skyfence technology) 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

- Forcepoint's cloud service traffic redirection strategy is still catching up to key competitors, as it completed adding IPsec support to all of its 27 data centers in 2Q17 and is now in beta with its Generic Routing Encapsulation (GRE) service. Customers that plan to implement Forcepoint's IPsec or GRE should test it carefully.
- Unlike many other cloud providers in this market, Forcepoint's SLA does not address latency.
- Forcepoint's sales and distribution channel lacks large, Tier 1 cloud service provider (CSP) and MSSP partners that actively sell its solution. Until Forcepoint establishes these partnerships, it will be at a disadvantage against many of its competitors.

iboss

Based in Boston, Massachusetts, iboss's cloud solution is built on a proprietary, node-based technology, which it refers to as "containerized gateways." This approach enables customers to adopt the public cloud service operated by iboss. They can also implement the same containerized gateways as a private cloud. Customers in need of a hybrid solution can integrate their own private cloud with the iboss public cloud.

In 2017, the company stopped selling appliances and converted its legacy appliance customers to the iboss cloud platform. Customers can still implement on-premises appliances, but they can't purchase them (see Strengths below). The on-premises appliances log into the iboss cloud and are managed from the cloud. In 2017 and 2018, iboss won several large deals, while competing against leading SWG vendors. iboss is a good option for SMBs and large enterprises.

Strengths

- The node-based approach of the new 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's partnership with Verizon (as of June 2018) enables it to deploy containerized gateways throughout Verzion'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.
- iboss's flexible pricing model is 100% subscription-based. Even customers that implement its appliances do not purchase the hardware — it is included as part of the annual subscription.

Cautions

- iboss does not own native CASB technology; however, it provides CASB functionality through its partnership with Microsoft Cloud App Security (CAS).
- iboss's native DLP support is not as broad as some other competitors in this market. iboss has enhanced its DLP offering through its integration with Microsoft CAS, but iboss provides native DLP support only for the web channel. Unlike some other competitors in this Magic Quadrant, it does not provide DLP support for endpoint or email channels.
- iboss's partnership with Verizon is a positive step, but it needs more large internet service provider (ISP) and MSSP partners to actively sell its solution.
- iboss has a limited presence in the Asia/Pacific (APAC) region. Prospective customers in this area should validate that iboss's partners are qualified to provide sales and technical 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 2017, McAfee acquired CASB vendor Skyhigh Networks. In 2018, the company terminated its Cloud Threat Defense service. McAfee's appliance solutions are good candidates for most enterprise customers, particularly those that are already McAfee ePolicy Orchestrator users. Its cloud-based SWG service is a good candidate for midsize customers that need to protect mobile users on Windows and OS X OSs.

Strengths

- MWG and WGCS have strong malware protection, due to embedded browser code emulation capabilities — 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 MVISION Cloud (formerly Skyhigh Security Cloud) offers strong CASB functionality, and the company has begun to extend existing integrations with MWG and WGCS. MVISION Cloud policies can be uploaded to and enforced by the MWG and WGCS.
- Malware detected by the MWG or the McAfee Advanced Threat Defense (ATD) sandbox can be submitted to the Threat Intelligence Exchange (TIE) server (a separate purchase) and shared with endpoints running the endpoint security client.
- McAfee's hybrid offering provides a single-pane-of-glass policy management option for customers looking to move into the cloud, while keeping their on-premises appliances.

Cautions

- McAfee has limited deployments with a tunnel-based approach for linking headquarters and remote offices to its cloud. McAfee customers primarily use an endpoint-based redirection approach.
- McAfee no longer operates a cloud-based sandbox. Customers can run their own cloud sandbox by implementing McAfee's virtual ATD solution in Microsoft's Azure or a private cloud environment. This option is not available in Amazon Web Services (AWS).
- The cloud service doesn't enable customers to specify a geographic location for log storage.
- McAfee needs to strengthen the sales and distribution channel for its SWG cloud service. It lists AT&T and America Movil as partners; however, it needs more Tier 1 communications service providers and MSSPs to actively lead and promote McAfee's cloud service.

Menlo Security

Based in Palo Alto, California, Menlo Security is a new entrant this year. It provides an isolation-based SWG platform, and its new architectural approach executes webpages on isolated browsers and mirrors the rendering to the end user's machine. The dual-engine approach uses the

browser's Document Object Model (DOM) with Adaptive Clientless Rendering (ACR) or Pixel ACR 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 AWS cloud (more than 95% of Menlo's customers use the cloud service). Menlo 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) is a proactive way 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 licenses Webroot's URL classification database. Administrators can create and store compound searches and reports using Menlo's Insights analytics engine, and Menlo further provides an API for SIEM integration.
- If policy allows users to download content, executable files can be inspected by the Menlo sandbox (the OEM provider is Sophos). They can also leverage customers' Palo Alto Networks Wildfire and FireEye sandboxes already deployed, while documents can be converted into safe HTML/PDF files for local storage. Encrypted content, including TLS/SSL, is already decrypted in the cloud browser, which eases content inspection.
- Flexible policy for web traffic can restrict file downloads and web write privileges, enforce corporate-certified browsers and block nonbrowser traffic, such as command and control. Menlo's "Vulnerable Services" category dynamically classifies websites using vulnerable applications, such as WordPress 4.8 or Drupal 7, enabling policy isolation for this content.
- Menlo isolates email links and web mail to protect against malware and thwart spear-phishing attacks. It also actively warns users at "time of click" to prevent credential theft.

Cautions

- Menlo is an emerging vendor that's less mature than larger competitors. It has received more than $85 million in financing, and is growing rapidly; however, it is not yet cash-flow-positive.
- The cloud service is delivered on AWS, and is thus restricted to Amazon's geographic presence. Local off ramps are available to ensure the delivery of localized content, present sites in the appropriate language and deliver a transparent local experience.
- Menlo does not offer CASB or native DLP functionality.
- Laptops are connected via VPN or less secure proxy auto-configuration (PAC) files only. Menlo does not offer a local agent, but plans to by year-end 2018. Although it supports other traffic redirection methods, such as IPsec tunnels from remote offices, most of Menlo's customers use PAC files.

Sangfor

Based in China, Sangfor has two primary business units: network security and cloud computing. Within network security, SWG represents about half of its revenue. The remaining revenue in the network security business unit comes from its next-generation firewall (NGFW), VPN, WAN optimization controller (WOC), ADC and endpoint security products. Sangfor's SWG is named Internet Access Management (IAM). It comes in a hardware appliance form factor or as a virtual appliance, and it is implemented as an in-line transparent bridge. In 2018, the company introduced an SWG cloud service.

In 2017 and 2018, it has also added Sangfor Engine Zero, an artificial intelligence (AI)-based malware inspection engine; Neural-X, a threat intelligence and traffic/flow-based analysis for botnets; and ZSand, a sandbox for malware detection. 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, 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. Bandwidth utilization parameters can be specified for uplink and downlink traffic. This is an important feature in the APAC region, where bandwidth costs are high.
- Sangfor applies analytical techniques against the data it captures from user traffic. Customers can implement embedded apps, such as a UEBA feature that monitors the risky behaviors of users or Internet of Things (IoT) devices on the network. Third-party apps can access Sangfor's data through APIs. Sangfor offers a unique feature that reports on wasted electricity (electricity is expensive in China).

Cautions

- Sangfor's emerging cloud service is aimed at the midmarket. It has only seven points of presence, all within China. Users lack the ability to specify a geographic location for the storage of logs.
- Sangfor lacks CASB features and has no CASB partners.
- DLP support is weak. Sangfor does not provide the ability to block traffic, based on DLP alerts. Only monitoring features are provided.

Symantec

Headquartered in Mountain View, California, Symantec offers appliance-based and cloud-based SWG solutions. The company has the largest market share among SWG appliance vendors, and it has the overall largest market share among all vendors in the Magic Quadrant (based on revenue). In August 2018, Symantec announced that it will lay off as much as 8% of its employees during its current fiscal year, as part of a restructuring effort.

In July 2017, Symantec acquired Fireglass, a remote browser isolation company. In June 2018, Symantec introduced its SD-Cloud Connector, an SD-WAN product that simplifies connecting remote offices to the Symantec Web Security Service (WSS). Also in June, Symantec announced the integration of the Symantec Endpoint Protection and SEP Mobile into WSS (this eliminates the need to add a separate agent for traffic redirection). Proxy Secure Gateway (SG) 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 Proxy Advanced Secure Gateway (ASG) families remain the strongest proxy 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 has implemented some integration between its SWG and CASB solutions. For on-premises appliances, the management console can display applications and risk scores. The SWG appliances can perform application control, based on this information. Symantec WSS also integrates with the CASB service, and the WSS can enforce policy based on shadow IT information from the CASB tool.
- Symantec offers remote browser isolation as a feature of its SWG solution, so that uncategorized URLs can be directed to the isolation technology and sent as images to a user's browser.
- The company 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 to Symantec and non-Symantec security solutions.

Cautions

- The Symantec product line 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.
- In September 2018, Symantec enhanced the graphical user interface (GUI) to its cloud sandboxing service. Gartner has yet to receive feedback on this new capability, so we advise

clients to test it carefully.

- For Symantec's WSS cloud service, the ability to configure the geographic locations where customers store logs needs improvement. Instead of customers selecting the location from a management console (the approach used by many competitors), the customer must direct Symantec's operations team to store the logs in a designated place.

Trend Micro

Based in Tokyo, Trend Micro is a provider of endpoint protection, content protection and application gateway solutions. InterScan Web Security (IWS) is a software-only solution that can be deployed on-premises, in the cloud or as a hybrid solution. The SWG console can be used to manage on-premises, pure-cloud or hybrid implementations. Trend Micro is a candidate primarily for SMB organizations 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 the support is good.
- Application control is strong. IWS appliances can set 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 the company's 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. Trend Micro 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 is missing live SIEM integration (support is planned by year-end

2018), and it has no geographic presence in the eastern European Union (EU), the Middle East or Africa.

- 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 be one of the fastest-growing and most innovative vendors in this market. It has the largest installed base of customers of any of the cloud-based SWG providers. The Zscaler Internet Access (ZIA) service includes NGFW, sandboxing, bandwidth control, DLP and other features. Zscaler Private Access is a software-defined perimeter (SDP) offering, that Zscaler positions as a VPN replacement solution. ZIA directly peers with most of the popular SaaS providers, including Office 365.

As a result of its initial public offering (IPO), Zscaler became a publicly traded company in March 2018. In August 2018, Zscaler acquired AI and machine learning technology and the development team of TrustPath. Zscaler will apply TrustPath's analytical techniques to its log data to improve Zscaler's threat prevention. Zscaler is a strong choice for enterprises seeking a cloud SWG service.

Strengths

- Zscaler applies all its malware detection engines to all content, including SSL/TLS traffic, regardless of site reputation or customer entitlements. With 55 billion transactions per day, this approach yields improved threat intelligence and site reputation verdicts. The optional sandbox reporting feature (Cloud Sandbox) provides alerting, malware analysis reporting and policy-based quarantining.

- 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 Private Access is an optional service that enables customers to replace their VPNs, while providing user-based access to specific applications inside customers' data centers or hosted in Microsoft Azure, AWS or Google Cloud.

- Zscaler continues to lead the market in innovative cloud features. The Nanolog Streaming Service provides the real-time export of logs to popular SIEM solutions. Zscaler's firewall service (outbound only) was the first among SWG vendors. Zscaler was the first cloud provider to provide availability statistics and throughput reporting.

- Zscaler now offers advanced DLP in the cloud with Exact Data Match capability supporting up to a billion cells per customer.

Cautions

- Zscaler does not own native CASB functionality. However, it receives basic application discovery and risk ratings from its two CASB partners (Microsoft CAS and McAfee Skyhigh).
- Customers that do not pay for the cloud sandbox service will have only .exe and dynamic-link library (DLL) files from suspicious sites analyzed. All customers get sandbox inspection of all .exe/DLL files from suspicious sites. For all other types of destinations and file or document types, Zscaler includes information about the malware in the logs. However, policy-based blocking, detailed malware analysis and patient-zero alerting require subscription to the company's advanced Cloud Sandbox feature.
- Zscaler's firewall service can analyze traffic that originates only from a customer's network. It does not analyze externally originated traffic (for example, traffic destined for the customer's website).
- Zscaler's malware research team is relatively small, compared with its larger competitors.
- Zscaler is not a good choice for enterprises that prefer an on-premises, appliance-based SWG. Although it offers a virtual appliance to enable hybrid deployments, the strategic focus of the company 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

Menlo Security

Dropped

Sophos has shifted its product strategy, and its stand-alone SWG products no longer meet the inclusion criteria for this Magic Quadrant.

Inclusion and Exclusion Criteria

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

- Vendors must provide all three components of an SWG:
  - URL filtering
  - Anti-malware protection
  - Application control capabilities

- Pure-play URL filtering solutions have been excluded.
- The vendor's URL filtering component must be capable of categorizing English language websites.
- Vendors must have at least $20 million in SWG solution revenue from enterprise customers in their latest complete fiscal year. Revenue resulting from equipment sales to service providers, for the purpose of building infrastructure to deliver services, does not apply. (The target audience for the Magic Quadrant is enterprises, not service providers.)
- Vendors must have an installed base of at least 3,000 customers or aggregate endpoint coverage of at least 5 million seats.
- UTM devices, NGFW devices and IPSs that offer URL filtering and malware protection have been excluded. This Magic Quadrant will analyze solutions that are optimized for SWG functionality.
- Vendors that license complete SWG products and services from other vendors have been excluded. For example, ISPs and other service providers that offer cloud-based SWG services licensed from other providers have been excluded.

Evaluation Criteria

Ability to Execute

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

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

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

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

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

Table 1: Ability to Execute Evaluation Criteria

Evaluation Criteria ↓	Weighting ↓

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

Source: Gartner (November 2018)

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

Geographic Strategy: This is 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

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

Source: Gartner (November 2018)

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 are aligned with the focus of a Niche Player vendor often find such provider's offerings to be "best of need" solutions. Niche Players may also have a strong presence in a specific geographic region, but lack a worldwide presence.

Context

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 2017 was $1.6 billion, which represents a 16% growth rate over an adjusted 2016 market size of $1.4 billion (see Note 1). We estimate that cloud service revenue represented approximately 26% of the total in 2017. Cloud services have experienced a 32% five-year CAGR, whereas on-premises appliances have only grown by 5% during the same period. Growth rates in the SWG market have been on a steady decline from the peak growth of 23% reached in 2010. We anticipate the growth rate for traditional appliances/software will be around 5% in 2018, while cloud service revenue will continue to grow at a robust 15% to 20% rate. The overall (appliances and cloud services) market growth rate will be approximately 10% 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. Both cloud and on-premises will benefit from additional spending for more-advanced security features (i.e., network sandboxing and other ATD technologies).

Note 1
Market Statistics Calculation Factors

This year, we received more-complete data from several vendors. This led us to recalculate our 2016 market statistics. The 2016 numbers now indicate that 21% of market revenue was from cloud-based SWG services, and 79% was from appliances.

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.

Estrategia geográfica: la estrategia del proveedor para dirigir los recursos, habilidades y ofertas para satisfacer las necesidades específicas de las geografías fuera del "hogar" o la geografía nativa, ya sea directamente oa través de socios, canales y subsidiarias según corresponda para esa geografía y mercado.