Competitive Landscape: Secure Web Gateways

Published: 12 September 2017 **ID:** G00332575

Analyst(s): Lawrence Pingree, Ruggero Contu

Summary

The secure web gateway market is still transforming toward SaaS deployments as CASB and DNS services capabilities add new challenges to traditional providers. Technology strategic planners must pay attention to these new concepts to compete effectively in the future "as-a-service" market.

Overview

Key Findings

Secure web gateway (SWG) customers gain flexibility, management and performance advantages by adopting a pure cloud-based SWG solution or by leveraging a hybrid of on-premises hardware or virtual appliances with a cloud-based SWG.

Some providers are moving to a solution stack that adds cloud access security broker (CASB) functions as an integrated capability for their overall SWG solution, bolstering external SaaS access security capabilities.

Additional features such as cloud-based SWG connectivity via VPNs, Domain Name System (DNS) services enforcement and firewall capabilities like protocol-independent application control are now being coupled together as suites to compete with proxy-only SWG solutions, enabling broader threat defense and enforcement than traditional SWG solutions.

Recommendations

In order to exploit security market dynamics, technology strategic planners must:

Focus development efforts on SaaS editions of SWG offerings, and consider moving traditional appliance product development toward maintenance or minor enhancements.

Examine ways to leverage the combination of DNS and/or VPN-based network firewall enforcement methods to compete with emerging as-a-service solution concepts and to improve protection against threats beyond proxied HTTP, HTTPS and FTP protocols.

Evaluate the goal of delivering a consolidated service solution stack that brings together multiple emerging security solutions building toward a secure internet gateway (SIG) service platform concept.

Analysis

Market Definition

Secure web gateways (SWGs) consist of appliance and service-based web traffic inspection solutions that offer:

- URL filtering
- Advanced threat defense
- Legacy malware protection

SWG solutions are used to defend users from internet-borne threats, and to help enterprises enforce internet policy compliance. SWGs are implemented as on-premises appliances (hardware and virtual) or cloud-based SWG services, or as a hybrid offering (combining both on-premises appliances and cloud-based SWG services with complementing features). Vendors continue to differ greatly in the maturity and features of their cloud-based SWG services and in their ability to protect enterprises from advanced threats (see "Magic Quadrant for Secure Web Gateways").

Definitional SWG features

- Anti-malware
- URL filtering (category-based policy enforcement)
- Application identification and control
- User authentication (Lightweight Directory Access Protocol/application development [LDAP/AD] integration)
- Role-based access controls
- User reporting

Optional SWG features

- Endpoint agent (for traffic/proxy control)
- Network tunneling/virtual private network (VPN) support
- Web content caching
- Browser and device control
- Bandwidth management/quality of service (QoS)
- File sandboxing support (also known as network or malware sandboxing)
- Malware command and control blocking

Optional integrations

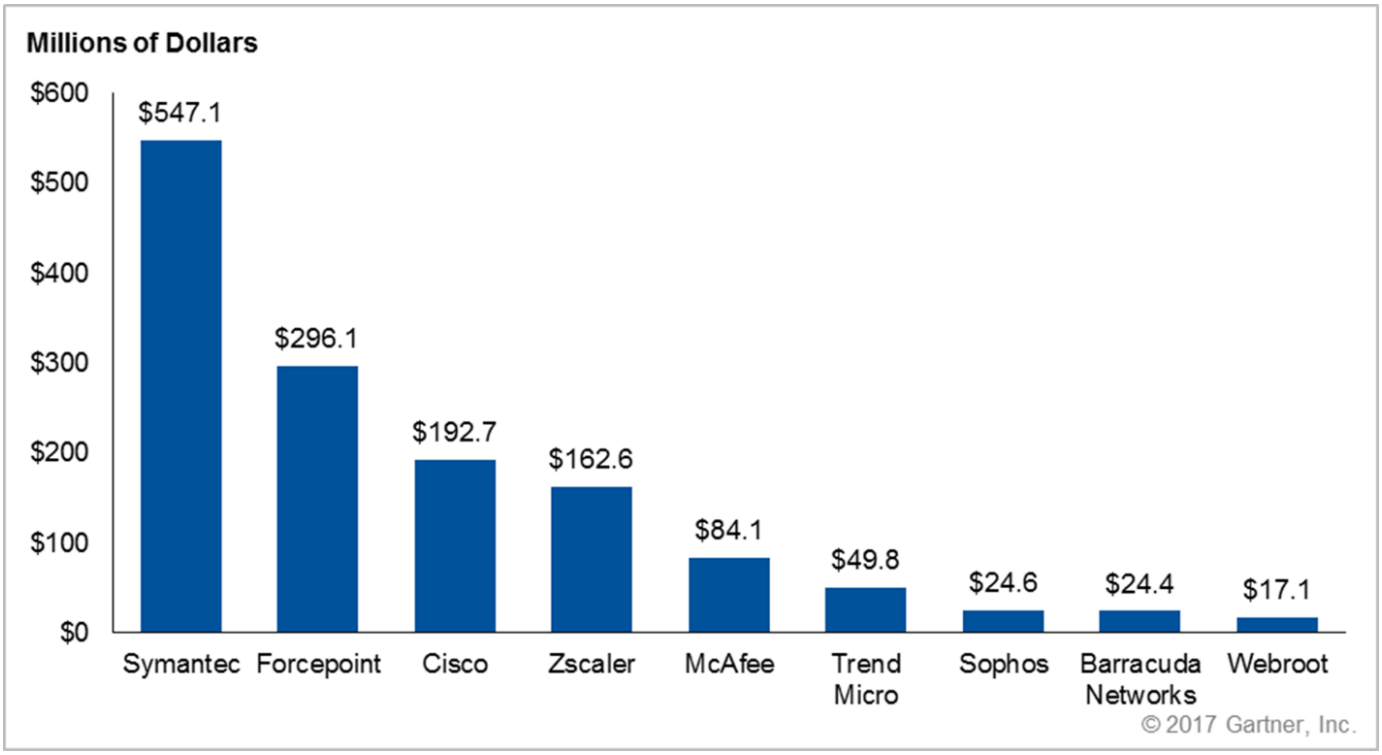
- Cloud access security broker
- Software-defined wide-area network (SD-WAN)
- Recursive DNS services
- Third-party threat intelligence

Competitive Situation and Trends

The SWG market now includes competitive pressures from many direct SWG market competitors from adjacent markets and competitors selling firewalls, DNS resolution services, cloud access security brokering and firewall as a service (FWaaS). In the SWG market, leading providers Symantec and Cisco face-off in a head-to-head battle between Symantec's proxy-based SWG appliances and services and Cisco's hybrid solution that leverages a hybrid of DNS and proxy capabilities. These two leading providers have acquired CASB solutions over the past several years, offering their own CASB solutions integrated with their SWG solutions to provide deeper control of SaaS applications. DNS-based resolver solutions have emerged into SWG solution stacks, because they offer complementary defense and compliance enforcement and because of the ease of deployment (simply replacing DNS resolvers). DNS resolution services do have weaknesses; for instance, they lack deeper content and URL inspection capabilities of proxy solutions. DNS resolver services, such as Cisco's Umbrella service, are being sold alongside traditional hardware and other SaaS delivery concepts as a suite of services in a service platform concept. In the case of Cisco's Umbrella solution, Cisco has combined both its proxy-based service and DNS-based inspection service into a single offering. This combined offering allows Cisco to take advantage of the performance of DNS for the bulk of inspected traffic, leveraging deeper content inspection advantages of HTTP/HTTPS proxying for only unknown or risky websites (a subset of its client's traffic), and helps it deliver higher performance to customers. Webroot, a small rival in the SWG market, recently released a new SaaS DNS resolver service as a replacement for its proxy-based appliance solution line as it pivots away from the SWG market. However, the trend in the overall security market to leverage DNS services is forcing some providers to seriously consider the competitive pressures of DNS-based resolver solutions to their SWG market offerings.

Figure 1 shows the top nine secure web gateway providers by estimated 2016 revenue.

Figure 1. Top Nine SWG Providers by Estimated 2016 Revenue (Millions of Dollars)



Source: Gartner (September 2017)

Note that Figure 1 above is based on Gartner's most recent Market Share for security software and combines the 2016 revenue for Blue Coat into Symantec's revenue. The companies iboss and ContentKeeper were not yet estimated in Gartner's published 2016 Market Share report and therefore are not present.

Current Trends

CLOUD-BASED SWG ADOPTION CONTINUES ALONG WITH HYBRID DEPLOYMENTS FOR "DIRECT-TO-NET" REMOTE OFFICES, POLICY SYNCHRONIZATION AND MOBILITY

The bulk of purchasing in the cloud-based SWG market is for "direct-to-net" connectivity to eliminate backhauling of connections and reduce costs associated with Multiprotocol Label Switching (MPLS) deployments. Mobile users and policy synchronization for hybrid deployments are a secondary driver in the market. SWG customers do find significant advantages with adopting a pure cloud-based SWG solution or by using a hybrid of on-premises hardware or virtual appliances along with a cloud-based SWG to deliver a consistent policy and improve performance for both mobile and remote office users. Cloud-based SWG services, if deployed widely and closer to mobile or remote office end-user locations (e.g., peered with the right internet services providers or in the right public cloud environments), typically offer substantially lower latency and better performance characteristics than that of backhauled traffic. SaaS offerings offer additional advantages such as easy SaaS service-chaining (where one service is tied to another in a chain) in order to deliver additional capabilities as a multiprovider or multiservice solution set (see "Market Trends: CSPs Must Deploy Dynamic Service Function Chain to Encompass the Agility Needs of Digital Business" and "Market Opportunity Map: Security and Risk Management Software, Worldwide"). Gartner believes that cloud-based SWG services are the most likely customer preference over the long term as organizations become more accustomed to leveraging them, compliance is addressed, and SaaS offerings are better monetized by providers. Technology strategic planners should focus development efforts on SaaS editions of their SWG offerings, and consider moving traditional appliance product development toward maintenance or minor enhancements.

SSL VISIBILITY MOVES MAINSTREAM

Based on telemetry (https://letsencrypt.org/stats/) from Let's Encrypt, as of 4 August 2017, at least 59% of internet sites are being loaded in the Firefox browser are using Secure Sockets Layer (SSL). Therefore, SSL is now considered a mainstream capability and almost a default protocol for the majority of internet activities. Industry reports indicate as high as 41% of attack or malicious traffic now leverages encryption for obfuscation, which means that traffic analysis solutions and web transaction solutions such as secure web gateways each must support the ability to decrypt SSL traffic to be effective. The biggest challenge for SWG providers is to prove out multitenancy, scalability and performance of their cloud-based SWG services when leveraging SSL certificates and decryption capabilities — including how these elements are handled in their hybrid SaaS service offerings. Providers must offer solutions for exempting certain sensitive sites from decryption, for example, banking, insurance and healthcare websites, especially for regional buyers in the United Kingdom and European Union and other locations where privacy laws are more stringent.

MIDMARKET MALWARE SANDBOX AND CONTENT DISARM AND RECONSTRUCTION CAPABILITIES CONTINUE TO EXPAND

SWG offerings continue to offer expanded capabilities for content inspection and include the extraction of files from web transactions. SWG technologies have focused heavily on integration with either their own malware sandbox services and on-premises appliances or integration with third-party malware sandboxing providers. The bulk of SWG competitors already have malware sandbox integrations, and the competition has moved toward user interface, quality of sandbox output and ability to rapidly integrate and respond to threats from the sandbox capabilities. Some recent inquiries with SWG providers indicate they are considering the addition of content disarm and reconstruction to enhance prevention capabilities. Gartner believes that there are some continuing greenfield opportunities in malware sandboxing, but these opportunities are largely focused in the midmarket and small organizations, while the majority of large enterprises have focused on stand-alone malware sandbox solutions (see "Improving Malware Protection Maturity by Using Attack Scenarios").

SOCIAL NETWORK CONTROL/VISIBILITY

In the SWG market, many providers offer some level of granular control over social network activities for target markets that allow for filtering traffic — for example, for file uploads, instant messaging and chat capabilities. These are the most often desired features in financial services, educational institutions, government entities and organizations that wish to protect children or enhance employee productivity. The control that URL and content-based filtering can exert on a user's use of social networks is significantly limited. Outside of the education vertical, Gartner customers tend to be most interested in the social network usage visibility and reporting features of SWG solutions to support human resources (HR), legal and security investigation use cases.

Emerging Trends

SWG CATEGORY BLOCKING AND THREAT DEFENSE COUPLED WITH DNS SERVICES

Through its OpenDNS acquisition, Cisco now offers DNS resolution services that are now coupled with and are directly competing with proxy-only solutions to enable internet inspection and blocking. A DNS resolution service, for example, can inspect host names being requested by individual endpoints during the DNS resolution process and compared them to a blacklist of Internet Protocol (IP) addresses, domain names or fully qualified domain names (FQDNs). DNS queries represent the first stage of the majority of valid communications on the internet. Therefore, DNS resolution services are ideal for the filtering of network traffic since each of these host addressing elements are often leveraged by malware authors as malware distribution points, malware communication conduits for command and control, or built into threat actor tools for the execution of attacks. However, the use of just IP addresses, domain names, host names and FQDN is not 100% effective at preventing attacks or communications on a stand-alone basis because good hosts can still contain malicious content. The use of DNS must be complementary to network-based enforcement solutions. DNS-based blocking and filtering do offer much higher performance and lower latency as a filter mechanism because they not only leverage small UDP packets (designed inherently to be the most optimally performing packets), but also because they do not require proxying and the complete transfer of content via a web connection. By leveraging IP and host name reputation capabilities, providers like Cisco are able to direct only relevant websites through web proxy services while the majority of traffic only leverages their DNS service for filtering — accelerating performance in lieu of adding some potential security risks. By coupling DNS with SWG web proxying, SWG service providers can widen their basic threat prevention and filtering capabilities beyond just HTTP, HTTPS and FTP. Technology strategic planners should seek ways to leverage both DNS and proxy-based

inspection methods in order to compete with this new emerging complementary capability to appropriately protect against advanced threats and improve SaaS performance. See "Assessing Secure Web Gateway Technologies," where Gartner examines the complementary nature of both DNS services for endpoint defense with URL inspection and proxy solutions for data loss prevention (DLP) and content inspection.

CLOUD ACCESS SECURITY BROKER INTEGRATION

Many SWG providers have begun to further integrate user monitoring, access, management, enforcement and visibility functions between SWGs and cloud access security broker (CASB) solutions. Several major providers have made acquisitions in the CASB market: Cisco acquired CloudLock in 2016, Blue Coat acquired Elastica and Perspecsys in 2015, and Forcepoint acquired Skyfence from Imperva in 2017. Symantec, through its acquisition of Blue Coat, now supports the ability in its management console solution to report on and have visibility into both its SWG solution and its CASB service in a combined user interface. This consolidation helps offer complementary but integrated capabilities unifying user threats protection with software as a service (SaaS) security and end-user internet activity compliance. As we see more organizations shift toward SaaS, Gartner expects to see SaaS management of both CASB and SWG functionality further consolidated under a single administrative and reporting interface. Technology strategic planners should seek to build and consolidate their SWG and CASB solutions to address the combined visibility and control needs for security and SaaS security supporting unified user interface with centralized policy, security analytics and user behavior monitoring. Product leaders should examine the ways that their existing service offerings can be combined into services suites in order to leverage multiple services in the same way that on-premises offerings have done in traditional technology features (see "Market Guide for Cloud Access Security Brokers").

INTEGRATION WITH THE ENDPOINT

Similar to what has happened in the network firewall market, SWG providers offer additional client benefits by integrating endpoint security technologies and capabilities, such as rapid response, quarantine and compliance assessment capabilities. Sophos offers integration between its SWG and its endpoint technology. A variety of SWG providers offer endpoint agents for deployment flexibility (e.g., maintaining traffic inspection), and some providers offer enhanced endpoint security features. Capabilities like these help bridge the endpoint and the network together in an orchestrated fashion. Although providers that focused heavily on network security have traditionally not done well selling endpoint technologies, there are significant benefits to integrating the technologies together. Since many organizations are focused on automation, bringing information together from both network and endpoint has advantages, such as correlation of threat activities or the ability to reduce privileges to access applications or internet websites if a host is noncompliant (see "Competitive Landscape: Endpoint Detection and Response Tools"). Technology strategic planners should seek ways to complement their SWG solutions with endpoint agent integration to enhance the security capabilities of their solutions beyond simple proxy redirection to more enhanced threat detection and response use cases.

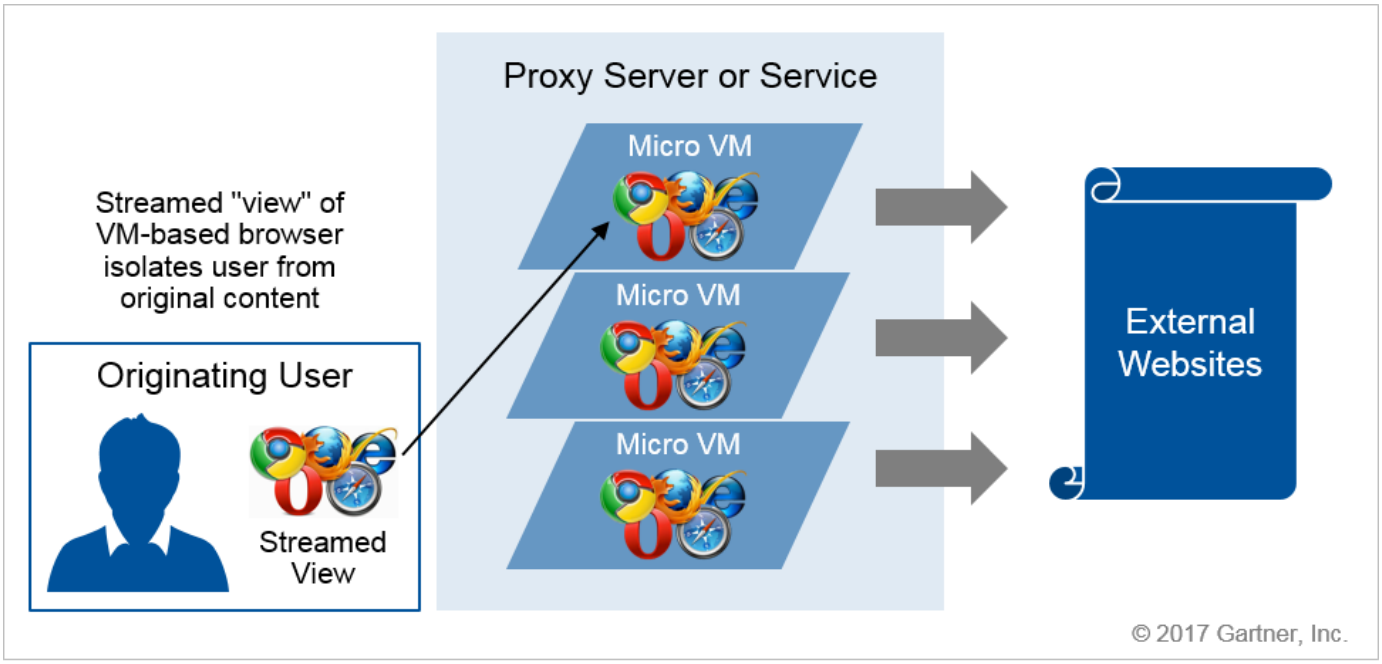
REMOTE BROWSER ISOLATION (ON-DEMAND)

Remote browser isolation (RBI) technology is emerging in the security market to help isolate users from potentially malicious web content (see "It's Time to Isolate Your Users From the Internet Cesspool With Remote Browsing"). RBI technology works by proxying browser connectivity through a gateway that leverages a micro-virtual machine (VM) instance of a

browser. This instance renders the isolated copy of the user's requested web content and provides a remote view to the individual user, similar to how screen sharing solutions such as Cisco WebEx work. The benefit that this capability offers is that unknown or suspicious website content can be isolated away from the actual end user's browser. In July 2017, Symantec announced the acquisition of Fireglass, a remote browser isolation provider from Israel, to augment its threat prevention capabilities in adjacent Symantec solutions — for example, its SWG technologies. Because of their proxy-based architectures, stand-alone RBI solution providers Menlo Security and Aurionpro have had to deploy their solutions using a service chain concept with already deployed SWG solutions. In order to compete more effectively against traditional SWG providers, these two RBI providers augmented their solutions with category-based filtering and other SWG features to displace traditional providers. Technology providers should consider the trade-offs of implementing isolation. For example, when sites do not work properly when isolated and may need direct access to the internet, providers must address end-user file download threats, usability and scaling issues related to content analysis (such as the use of file sandboxing and content disarm and reconstruction technologies). Technology strategic planners must evaluate RBI technology to enhance threat prevention capabilities in their SWG solutions in order to compete effectively in future SWG deals.

Figure 2 shows an example of remote browser isolation.

Figure 2. Remote Browser Isolation (RBI) Example



VM = virtual machine

Source: Gartner (September 2017)

INTEGRATED DLP (I-DLP) EXPANSION

Gartner estimates that by 2020, 85% of organizations will implement at least one form of integrated DLP (I-DLP), up from 50% today. Because secure web gateways are a common point of access for content, they are naturally a great fit for complementing endpoint DLP with SWG as the network-based enforcement mechanism for an overall DLP solution that enforces at the endpoint and at the network layer to prevent contractors and unmanaged systems from sending sensitive data. With the EU regulation of General Data Protection Regulation (GDPR) coming into

effect in May 2018, we anticipate more integration of DLP with SWGs, as the mandate includes browsing history as well as interactions with Web Real-Time Communications (WebRTC) occurring with unified communications as a service (UCaaS) and B2B and B2C interactions.

INTEGRATION OF THIRD-PARTY THREAT INTELLIGENCE AND THREAT INTELLIGENCE PLATFORMS

Threat intelligence sharing and threat feed integrations with on-premises security solutions have been important topics for security programs and security leadership over the last several years. Although competitive providers in the adjacent firewall and security information and event management (SIEM) markets have already adopted integrations, SWG market providers have largely ignored the third-party threat intelligence needs of buyers. Support for third-party threat intelligence and/or integration with threat intelligence platform solutions is almost nonexistent in most SWG products, with only a limited number of SWG providers (for example, Cisco) having existing plans to integrate additional threat intelligence capabilities into their offerings. Cisco's Umbrella and McAfee's SWG solutions both offer third-party threat intelligence integration, which helps them compete in deals where the comprehensiveness of threat intelligence, prevention and detection capabilities is a critical buying criterion. Gartner believes that providers have a market opportunity to offer integration with third-party threat intelligence feed services and threat intelligence platform solutions to enhance their threat prevention capabilities and further monetize customer investments in threat intelligence (see "Competitive Landscape: Threat Intelligence Services, Worldwide, 2017").

Market Players

The providers included in this report are the top providers by Gartner-estimated market share revenue and/or are the most visible in Gartner inquiries and Gartner website search analytics.

The Future of Competition

The Secure Internet Gateway (SIG) Service Platform of the Future

The SWG market has been moving strongly toward service-based SaaS delivery models, growing at more than 30% for the past five years. Most providers have already announced cloud-based SWG offerings. However, if we look out onto the horizon, the plethora of security technologies offered as "stand-alone" products or solutions have begun to be increasingly less stand-alone when offered as SaaS solutions. For complex providers with larger portfolios, a multioffering service platform concept emerges.

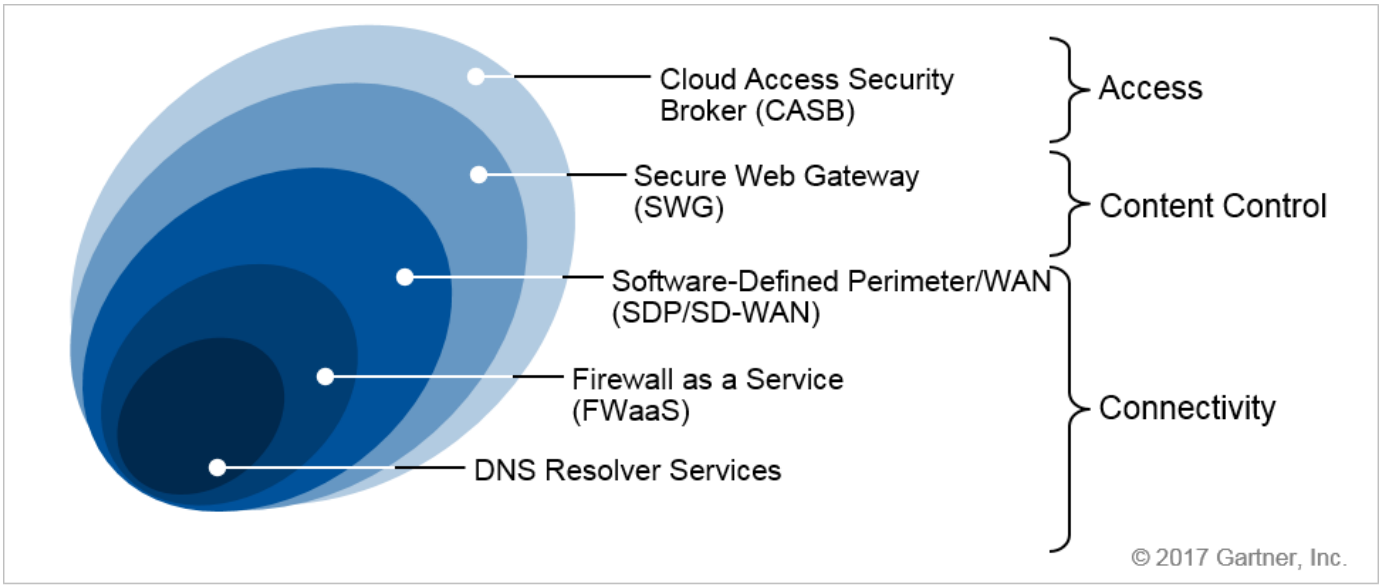
The combination of services and tight integration of technologies offered in SaaS solutions make them ideal for consolidation and unification. For example, secure DNS resolver services, SWGs, software-defined perimeters (SDPs), CASBs, FWaaS, two-factor "step-up" authentication, data protection, remote access and SD-WAN solutions can be combined, giving rise to a new solution bundling possibility. Gartner calls this new SaaS platform bundling concept a secure internet gateway (SIG) service platform, where individual services are sold as functional extensions of a broad, highly integrated set of security gateway services that complement each other as a bundled capability.

Tight couplings and integration between SaaS services and appliance form factors have already permeated the security markets over the past several years, and Gartner expects this trend to continue. The SIG service platform offers a new promise to its customers — a richer overall set of capabilities delivered by a single entity — that could potentially offset or displace some or all of the bulk of on-premises solutions of yesterday (especially for branch office locations) and stand-

alone SaaS offerings. Similar to how platform-based software or hardware appliance solutions eroded stand-alone single-function products, platform-delivered services offered as a SIG platform "service suite" concept can easily displace stand-alone versions of SaaS, on-premises software or hardware products. Gartner believes that providers in the security market must seek to build toward the SIG service platform concept in order to compete effectively in the future, especially as pure-play SaaS vendors further consolidate into larger entities.

Providers such as Cisco, Symantec and Zscaler currently appear best-positioned to take advantage of a consolidation, further integration and bundling of multiple service technologies (and already have been working on this) into a unified SIG service platform concept. Each of these companies offer broad-based portfolios and have scalable service platform architectures that can easily monetize new security service capabilities. Figure 3 below depicts a strawman outline of the SIG concept, which can address key customer needs for secure connectivity, content delivery, application access, visibility and control into a single service platform. The SIG platform concept represents a more comprehensive offering that can pivot to new security use cases and, more importantly, remain sticky for security providers over time as they incorporate additional features and security services. For information on the variety of services in the SIG concept, see "Hype Cycle for Cloud Security, 2017," "Hype Cycle for Threat-Facing Technologies, 2017" and "Hype Cycle for Enterprise Networking and Communications, 2017."

Figure 3. The Secure Internet Gateway (SIG) Service Platform (Future Concept)



Source: Gartner (September 2017)

Competitive Profiles

Barracuda Networks

MARKET OVERVIEW

Estimated 2016 SWG revenue: $24.4 million

Barracuda Networks, historically focused on midmarket, provides a broad array of network security, application security, storage and productivity solutions. Barracuda Networks sells its Barracuda Web Security Gateway (WSG) appliances and its Barracuda Web Security Service into the SWG market. The company's Barracuda WSG appliance line offers both hardware appliance and virtual appliance form factors ranging from as low as 25 concurrent user models through

25,000 and throughputs ranging from 5 Mb per second to 5,000 Mb per second. The Barracuda Networks WSG Appliances offer spyware and virus protection, advanced threat protection, social media control, application control, content filtering, and an endpoint client software to support mobility use cases (Barracuda Web Security Agent). The Barracuda Web Security Agent (WSA) supports both Windows and Mac OS X. The company also offers a Barracuda Safe Browser that enforces compliance and synchronization of policies with the Barracuda WSG for Apple iOS devices and a Chromebook security extension for supporting student mobility in the K-12 education vertical. For centralized management, the Barracuda WSG offers a central management SaaS through the Barracuda Cloud Control (BCC), a free web-based management portal, and includes support through Barracuda Central, a 24/7 security operations center that monitors and blocks emerging internet threats. The company's Advanced Threat Protection (ATP) is an additional optional subscription available with the latest WSG that offers full system emulation in order to inspect malicious behavior and identify new and advanced forms of malware.

HOW THIS PROVIDER COMPETES

Barracuda Networks, most known for its advertising campaigns within airports and in-flight video segments, competes by leveraging its extensive global channel and direct sales force. The company's partnerships include Vandis, Altinet, Fujitsu Network Solutions and others across the globe to deliver sales across its portfolio of products and solutions. Throughout 2016 and into 2017, the company has gone through a major transition to SaaS and support in its product lines for cloud and virtual deployments, and its SWG portfolio was not excluded. In mid-2016, the company announced the appointments of Hatem Naguib as senior vice president and general manager for its security business and Ezra Hookano as vice president of channels for specifically the task of growing its business in the cloud. In late 2016, the company updated its WSG product line to version 11.0, enhancing its advanced threat detection capabilities, improving SSL inspection capabilities and adding policy enforcement on Chromebooks for K-12 to support its education vertical sales. In March 2017, the company launched the new Barracuda Web Security Service through a partnership with Zscaler. The service is sold and supported by Barracuda through its network of channel partners.

Typical estimated costs for 5,000 users (three years)

On-premises deployment model:

Barracuda Web Security Gateway Model 910 x 2: $47,998

Energize Updates: $40,298

Instant Replacement: $33,098

Advanced Threat Detection: $30,598

Total Gartner estimated cost (three-year contract): $151,992

Cloud-delivered deployment model:

Barracuda Web Security Service: $405,000

Total Gartner estimated cost (three-year contract): $405,000

Cisco

MARKET OVERVIEW

Estimated 2016 SWG revenue: $192.7 million

Cisco is a large, broad-based network and security technology provider. The company actively sells its Cisco Web Security Appliance (WSA) as a traditional SWG and Cisco Umbrella as a SIG into the web security market. Cisco WSA can be managed by using a SaaS management console called Cisco Defense Orchestrator, which unifies policy with Cisco Umbrella, or by using an on-premises management console called the Cisco Content Security Management Appliance (SMA), which unifies management with Cisco Email Security Appliances. In the hardware appliance line of the WSA, Cisco offers four models — its Cisco WSA S190, S390, S690 and S690X. In addition to physical appliance model, Cisco WSA is also available as virtual models (S100v, S300v and S600v) and can be deployed using various hypervisor technologies, such as Kernel-based Virtual Machine (KVM), ESXi from VMware and Hyper-V. In the cloud security service of Umbrella, Cisco offers three core packages: Professional, Insights and Platform. The Cisco solutions also report integration with Cisco's Cognitive Threat Analytics (CTA), Cisco's Advanced Malware Protection (AMP), and third-party threat intelligence via Umbrella API or WSA external feeds, which help identify malware and command and control infrastructure to block data exfiltration and advanced threats.

HOW THIS PROVIDER COMPETES

Cisco competes by leveraging its broad-based portfolio and extensive global sales channel. Recently, the company has been leveraging the attractiveness of its Cisco enterprise license agreement (ELA), a buying program that allows organizations to adopt, scale and pay for Cisco software as they grow or change needs. This new software sale concept has allowed Cisco to grow its software subscriptions more quickly and eliminate repetitive contract negotiations that often extend or delay closing of deals or has limited future software-based technology adoption by customers in the past. One key element to the Cisco ELA is that it allows customers to have portable software subscriptions while they change their hardware deployments, improving the flexibility for the channel and the customer. Cisco also couples its security sales with its managed service offering to address its customers' employee resource demands, enabling the offering to monitor, manage and provide threat detection and event triage for its customer base. This paired offering places pressure on channel providers that offer competitive managed security services. With the new Cisco Umbrella service, the company offers threat defense as well as category-based filtering, but the ease of deployment and complementary nature of DNS- and IP-layer enforcement with intelligent proxy allow it to sell either adjacent to its SWG business into new accounts or cross-sell each of its solutions independently. A new route to market for Cisco Umbrella is a joint offer with Verizon, branded as Verizon DNS Safeguard. Verizon DNS Safeguard integrates the Verizon Threat Research Advisory Center with Umbrella's cloud security and is being sold by Verizon Business Markets (VBM) and Verizon Enterprise Solutions (VES). The company is currently more actively focused on selling its Umbrella solution in net-new customer accounts and upselling its Advanced Malware Protection (AMP) solution as a core product enhancement in both existing WSA and Umbrella accounts. The company has continued to evolve its security business over the past several years, including various security-specific acquisitions to add to its solution breadth, further complementing its network, switch and cloud computing businesses.

Typical estimated costs for 5,000 users (three years)

On-premises deployment model:

WSA S690 Web Security Appliance with Software x 2: $23,716

Web Premium software bundle (three years): $105,556

Advanced Malware Protection (three years): $219,120

Support and maintenance: $3,635

Total Gartner estimated cost (three-year contract): $352,027

Cloud-delivered deployment model:

Umbrella platform: $635,400

Total Gartner estimated cost (three-year contract): $635,400

Forcepoint

MARKET OVERVIEW

Estimated 2016 SWG revenue: $296.1 million

Forcepoint, now the second-largest provider in the SWG market, actively sells its Forcepoint Web Security Cloud and Forcepoint Web Security solutions into the SWG market. The Forcepoint Web Security Cloud consists of 27 data centers deployed across six continents in 18 countries. The Forcepoint SWG solutions include capabilities such as URL filtering, application control, social network controls, SSL decryption, signature-based anti-malware, DLP integration and malware sandbox capabilities to detect advanced threats. The Forcepoint Advanced Classification Engine (ACE) is included standard with all Forcepoint Web Security appliance, hybrid and cloud service products. ACE leverages a predictive analytics engine to identify zero-day issues and to deliver real-time security ratings and other advanced threat detection capabilities. The Forcepoint solution is capable of leveraging its on-premises appliance line of products in a hybrid fashion with its cloud service to continue to enforce remote access control policies on mobile users. Forcepoint recently completed an acquisition of the CASB business Skyfence from Imperva to integrate with its web security and DLP product lines and further extend its offerings to address buyers' cloud and SaaS security concerns. Forcepoint continues to go through transformations in its marketing and product naming after its spin-off from Raytheon. According to 2016 Gartner market share estimates, Forcepoint is the second-largest SWG provider in the market, with roughly 75% of its business coming from North America and Europe and an estimated 25% of its business coming from Asia/Pacific and the rest of the globe.

HOW THIS PROVIDER COMPETES

Forcepoint competes by leveraging its large channel business and its partnerships with CDW, SHI International, IBM in Australia and Optiv, which comprises the majority of its product and services sales. In 2016, the company focused on expanding its ability to proactively block high-risk cloud applications and individual cloud applications. Gartner expects the company to continue to further leverage its Skyfence acquisition, positioning its CASB solution alongside its SWG solution as an integrated offering in order to entice solution suite purchasing in its product lines. A significant portion of customers who adopt the Forcepoint SWG product lines also integrate its DLP solution into its products, which also allow customers to apply DLP policies with the Forcepoint DLP endpoint solution. Its integration between its DLP and SWG solutions has been a driving force for the adoption and sale of its solutions. Forcepoint continues to focus its sales efforts on its cloud service offering instead of its on-premises appliance product lines. Forcepoint leverages its secure cloud that complies with strict regulations and offers a wide range of cloud connectivity and tunneling options in order to close deals.

Typical estimated costs for 5,000 users (three years)

On-premises deployment model:

V10000 G4 Appliance x 2: $21,995

Forcepoint Web Security: $337,500

Web DLP: $144,180

Total Gartner estimated cost (three-year contract): $503,675

Cloud-delivered deployment model:

Forcepoint Web Security Cloud: $445,500

URL filtering

SSL

Application control

Social

DLP

Standard support included

File sandboxing: $168,750

Mobile device support (Forcepoint Mobile Security):$60,750

Extended reporting, 12 months: $81,000

Total Gartner estimated cost (three-year contract): $756,000

iboss

MARKET OVERVIEW

Estimated 2016 SWG revenue: Gartner does not have a current market share estimate at this time.

The company iboss sells its Distributed Gateway Platform into the SWG market. The iboss solution offers capabilities such as network traffic anomalies detection, malware sandboxing, web security, SSL decryption, bandwidth optimization, user authentication, reporting and analytics in a single node-based architecture. The iboss solution is delivered as a platform built with separate, distinct functional node-based architectural elements, including gateway nodes that perform proxying, scanning and enforcement. Its reporting nodes store security events and provide drill-down reporting and a cyber-risk score node that provides behavioral risk scores for devices and network users. The iboss offering supports stream-based content scanning across all ports and protocols, along with category and user-based filtering, as well as mobile device management and integration with network access control and software-defined networking (SDN) technologies. iboss also offers outbound firewall and network traffic inspection capabilities, and intrusion prevention capability.

HOW THIS PROVIDER COMPETES

iboss competes by leveraging its node-based concept and combining it with a SaaS subscription model to deliver a variety of functions including SWG, outbound firewall, network anomaly detection and intrusion prevention capabilities in a single solution. The company focuses heavily on marketing its node-based concept along with articulating a story around eliminating backhaul costs and offering on-demand scalability. In January 2016, the company added a variety of new leaders to its sales and channel teams as it works to expand its presence globally, funded by a $35 million funding round from Goldman Sachs Private Capital Investing group. In April 2017, the company announced its new packaging model that included a SaaS subscription combined with its flexible node-based architecture in a single SaaS license. The company was recently named a visionary in "Magic Quadrant for Secure Web Gateways."

Typical estimated costs for 5,000 users (three years)

On-premises and cloud-delivered deployment model:

iboss (Core)

Total Gartner estimated cost (three-year contract): $240,000

McAfee (Formerly Intel Security)

MARKET OVERVIEW

Estimated 2016 SWG revenue: $84.1 million

McAfee (formerly Intel Security) actively sells its McAfee Web Gateway and McAfee Web Gateway Cloud Service (a cloud-based SWG) into the SWG market. The company also offers a hybrid McAfee Web Protection subscription that includes the ability to deploy appliances and leverage its SaaS offering to support mobility use cases and policy synchronization. The McAfee solution includes zero-day malware detection and reputation and category-based filtering, along with integration with its advanced threat defense and threat intelligence sharing solutions. The company's virtual appliance options support VMware and Microsoft Hyper-V hypervisors and have been criteria EL2+ and Federal Information Processing Standard (FIPS) 140-2 Level 2 certified. The company offers encryption key storage through a variety of hardware security modules (HSMs), including Thales e-Security's nShield HSMs. The company offers integration with the McAfee DLP product for network-based DLP enforcement of HTTP, HTTPS and FTP protocols and also offers CASB-light functionality. The McAfee solution also offers a lightweight agent technology called the McAfee Client Proxy, which enables roaming users to pivot inspection between the on-premises appliances and SaaS service.

HOW THIS PROVIDER COMPETES

McAfee leverages its broad portfolio of security technologies and solutions spanning advanced threat detection, endpoint protection, data security, security operations and network security to compete against others in the SWG market. Over the past several years, the company has gone through dramatic changes in its executive management team and its organizational structure, most recently being spun out from Intel as an individual entity in 2017. The company has been disrupted by these moves, but publicly promises a brighter future with new security acquisitions and in-house technologies on the horizon. The company continues to leverage its extensive Security Innovation Alliance (SIA) partner ecosystem to entice buyers who seek to leverage McAfee solutions alongside innovative best-of-breed security startups and complementary solutions.

Typical estimated costs for 5,000 users (three years)

On-premises deployment model:

WBG-4500-D x 2 (appliances): $13,993

WPSICE-AA (hybrid subscription): $310,500

Hardware support and maintenance: $23,988

Total Gartner estimated cost (three-year contract): $348,481

Cloud-delivered deployment model:

McAfee Web Gateway Cloud Service (cloud-only): $412,500

Total Gartner estimated cost (three-year contract): $412,500

Sophos

MARKET OVERVIEW

Estimated 2016 SWG revenue: $24.6 million

Sophos is a broad-based portfolio provider of security technologies, spanning network, web and endpoint including firewalls, SWG and endpoint protection platform software as well as consumer endpoint protection. In the SWG market, Sophos offers several solutions, including its Sophos Web Gateway, a SaaS offering, and the Sophos Web Appliance, which consists of both virtual and hardware appliance options. The company's SWG solutions support URL filtering based on 88 site categories, geolocation, user, group and time-based filter policies, and provide control of social web application features. The Sophos appliance lineup includes appliances with support for up to 150 users with its WS150 appliance and support for up to 5,000 users with its WS5000 appliance, which has support for scalable load-balancing.

In 2016, the company released a new version of the Sophos Web Appliance version 4.3 that added enhanced reporting and the ability to submit files manually to the Sandstorm sandbox feature. The company continues to work toward consolidating all of its SWG solutions together into a hybrid initiative, where customers will be able to select the inspection point deployment styles they prefer and manage them centrally in the Sophos Central cloud management platform. The company plans to move customers to its new URL categorization database as it migrates its customer base to its hybrid deployment solution, which is also focused on improving its URL classification and blocking capabilities. The integration of the company's acquisition of Invincea in February 2017 significantly enhances the company's advanced malware detection capabilities beyond detection signatures and malware sandboxing and improves the telemetry provided to both security operations and incident response personnel using Sophos solutions and its Sophos Central management platform.

HOW THIS PROVIDER COMPETES

The Sophos SWG business is largely dominated by North America and EMEA, supporting more than 90% of its SWG revenue. Sophos offers a free service that provides around-the-clock remote monitoring to notify customers of potential issues with their Sophos SWG solution. Although the company is working to address these issues, Sophos is currently at a disadvantage in some competitive large-enterprise deals because it lacks security policy synchronization integration between its on-premises SWG appliances and its SaaS solutions to support user mobility use cases. Sophos also does not currently support internet content augmentation protocol (ICAP) in

its appliances, so it cannot integrate with network DLP solutions that need this protocol to function. However, Sophos Web Gateway itself provides data loss prevention using keyword scanning.

Typical estimated costs for 5,000 users (three years)

On-premises deployment model:

Sophos Web Appliance WS5000 Gateway x 2: $31,990

Sophos SM5000 Management Appliance x 1: $10,995

Software license subscription: $150,000

Total Gartner estimated cost (three-year contract): $192,985

Cloud-delivered deployment model:

Sophos Web Gateway: $150,000

Sophos Sandstorm (sandboxing): $75,000

Total Gartner estimated cost (three-year contract): $225,000

Symantec (Formerly Blue Coat)

MARKET OVERVIEW

Estimated 2016 SWG revenue: $547.1 million

In August 2016, Symantec closed the acquisition of Blue Coat. Both Symantec and Blue Coat had extensive SWG solutions and product portfolios in the security market. The merger of Blue Coat into Symantec makes the combined company the largest provider by market share in the SWG market, with more than $500 million in revenue. The company now actively sells its ProxySG, Advanced Secure Gateway, Virtual Secure Web Gateway and Cloud-Delivered Web Security Service into the SWG market. Symantec also offers an advanced threat detection capability with its add-on Content and Malware Analysis advanced malware sandbox solution. Postacquisition, the company integrated both the Blue Coat and Symantec global threat intelligence networks together, including intelligence from the Symantec email security and endpoint security solutions, to enhance the company's overall threat detection and prevention capabilities across its portfolio of products, including its SWG solutions. Symantec offers appliance products designed for as few as 500 users per appliance up to 50,000 users per appliance and supports highly-available deployment options. The Symantec ProxySG appliances can be managed centrally via the Symantec Security Platform — Management Center solution, which can also manage its SSL Visibility, Content Analysis system, Malware Analysis appliance, Mail Threat Defense and PacketShaper products. The Symantec Cloud-Delivered Web Security Service also offers integration with the Symantec CloudSOC CASB platform service to enhance its overall protection for SaaS and web security into an integrated service offering.

Note: Our revenue estimate for this provider is a representation of combined revenue from our 2016 estimates of Blue Coat and Symantec.

HOW THIS PROVIDER COMPETES

Symantec competes leveraging its large global channel provider network and its strong position across multiple security technologies and solutions. The combined Blue Coat and Symantec businesses allow the company to sell an extensive suite of security solutions, using attractive

one-stop shopping security suites and services. In December 2016, Symantec filed a lawsuit against rival Zscaler to defend several of its patents in web security, data loss prevention, threat prevention, access control and antivirus. In 2017, Symantec extended its lawsuits to include additional network-based security technologies. Zscaler denies these claims. In May 2017, Symantec cut ties with Tech Data and extended its relationships with Synnex and Westcon-Comstor. On 6 July 2017, the company announced the acquisition of Fireglass, which provides remote browser isolation. The Fireglass acquisition allowed Symantec to deliver enhanced threat prevention for unknown or suspicious websites through a variety of its web protection solutions and other offerings, further differentiating it from others in the SWG market that it now dominates. Symantec positions its web security portfolio as an ecosystem of technologies that it claims works together to protect organizations. Symantec has been focused on integrating and selling its SWG-based advanced threat detection and content analysis system in conjunction with its endpoint protection and remediation products to entice customers to buy multiple aspects of its portfolio. The company claims that its SWG technologies are used by more than 70% of top global organizations. Postacquisition, the company has focused heavily on highlighting the combined threat intelligence that the Blue Coat acquisition has brought to the Symantec family of products.

Typical estimated costs for 5,000 users (three years)

On-premises deployment model:

ASG S400-20 Appliance x 1: $85,000

ASG S400-20 Appliance x 1 (cold standby): $8,800

URL filtering/categorization subscription: $63,750

Network Monitor and Network Prevent for Web (DLP): $247,500

Support and maintenance: $267,350

Total Gartner estimated cost (three-year contract): $672,400

Cloud-delivered deployment model:

Cloud service suite — web, mobile and hosted reporting for one year: $21.33 per user

Total Gartner estimated cost (three-year contract): $106,650

Trend Micro

MARKET OVERVIEW

Estimated 2016 SWG revenue: $49.8 million

Trend Micro is a broad-based provider with security technologies in cloud security, network security and user protection. Trend Micro has offerings for small businesses up to large enterprise organizations. In the SWG market, Trend Micro sells its InterScan Web Security Virtual Appliance and its InterScan Web Security as a Service offerings. The company's virtual appliance provides anti-malware, advanced threat detection, zero-day exploit prevention, botnet defense and bandwidth management, along with category-based URL filtering and application control functionality. For its advanced threat detection, the company has its Trend Micro Deep Discovery malware sandbox solution and leverages threat intelligence from its global Smart Protection Network. The company's SWG solution also supports an add-on DLP module to extend DLP capabilities to the network layer from its endpoint DLP capabilities. Multiple InterScan virtual

appliances can be managed centrally by Trend Micro Control Manager (TMCM) solution and support clustering for high availability. Although Trend Micro has an on-premises virtual appliance, Trend Micro is now focused on selling its new hybrid solution called the InterScan Web Security Hybrid (IWSH). The offering can manage Trend Micro's SaaS-based SWG service, on-premises appliance and virtual appliance options and synchronize the policy across all of these solutions for mobility use cases. From a delivery perspective, the Trend Micro SaaS-based offering leverages both Amazon Web Services (AWS) and dedicated hosting providers in specific regions to deliver worldwide coverage across 16 data centers globally.

HOW THIS PROVIDER COMPETES

Trend Micro leverages its global sales channel and broad portfolio of security offerings to offer one-stop shopping for its client base. Roughly 95% of transactions with Trend Micro are through the Trend Micro channel rather than direct sales. In 2016, the company improved its integration with the Trend Micro Control Manager solution to exchange real-time threat detection signatures, and added SaaS-delivered malware sandbox, SaaS DLP integration, enhanced detection support for Office 365, social media control granularity and improved HTTPS granularity to help the solution compete in deals with SSL decryption or other important selection criteria. Throughout 2016, the company heavily focused on ransomware prevention because of the inordinate amount of ransomware that organizations have had globally during the past year. The company also partnered with Interpol and helped take down several cybercrime syndicates in relation to these efforts throughout 2016. In October 2016, the company announced a new marketing initiative and vision for its offerings that center around a new marketing theme called XGen security. Trend Micro describes XGen as "a blend of cross-generational threat defense techniques that intelligently applies the right technology at the right time, resulting in more effective and efficient protection against a full range of threats." This new marketing message and an increase in the use of machine learning for threat detection have been effective in helping Trend Micro change overall customer perceptions of its "technology freshness" in the security market against emerging alternative startup providers across its portfolio.

Typical estimated costs for 5,000 users (three years)

On-premises deployment model:

Recommended hardware: $7,500

Software licenses: $60,000

Integrated DLP: $24,000

Total Gartner estimated cost (three-year contract): $91,500

Cloud-delivered deployment model:

InterScan Web Security as a Service: $240,000

Total Gartner estimated cost (three-year contract): $240,000

Trustwave

MARKET OVERVIEW

Estimated 2016 SWG revenue: $10.0 million

Trustwave is a broad-based technology and managed security service provider with a portfolio that spans network security, content security, endpoint security, database security, application security and security operations. In the SWG market, Trustwave sells its Trustwave Secure Web Gateway solution, which includes managed, SaaS, virtual appliance and hardware appliance deployment options. Trustwave's SWG solution offers real-time code analysis, zero-day malware prevention, malware behavior analysis, dynamic URL categorization and reporting and analytics of web usage. Its solution includes features for monitoring and controlling web usage, including application control, and control of a variety of enterprise SaaS applications and social network websites such as Facebook, Twitter, Google+ and LinkedIn. The Trustwave Security Reporter product can be used in conjunction with the SWG appliances to provide enhanced reporting for investigation and analysis. Trustwave is known for the managed security services it sells alongside most of its technology deals and for its threat research organization SpiderLabs, whose threat intelligence is fed directly into Trustwave's security solutions.

HOW THIS PROVIDER COMPETES

In the SWG market, Trustwave competes by leveraging its portfolio concept, zero-malware guarantees, combined managed security services and integration with other Trustwave solutions to compete with its rivals. Trustwave often competes with the prowess and branding of its SpiderLabs research organization as well as its history as a one-stop shop for managed security, security operations and security monitoring center services. Trustwave has nine global security operations centers (SOCs). Throughout 2016, Trustwave added several new leaders to its organization, including a new head of global alliances, global channel chief, chief financial officer, head of product management, and head of global sales. In October 2016, the company announced partnerships in Japan with Singtel and TIS as it attempts to expand in the country and new security operations centers in Australia and Japan; Trustwave has been expanding its business, marketing and sales efforts in the Asia/Pacific region during the past year. In June 2017, the company announced availability of its Trustwave Secure Cloud Gateway services, delivering its SWG solution as a SaaS offering and its Trustwave Secure Email Gateway Cloud.

Typical estimated costs for 5,000 users (three years)

Gartner was unable to obtain pricing information for a pricing analysis for Trustwave solutions.

Webroot

MARKET OVERVIEW

Estimated 2016 SWG revenue: $17.1 million

Webroot sells a portfolio of security products including endpoint security, web security and network security solutions. In the SWG market, the company now sells its SecureAnywhere DNS Protection service (replacing its former SecureAnywhere Web Security Service). The Webroot SecureAnywhere DNS Protection service allows organizations to control up to 82 URL categories and filters dangerous and questionable URLs and domains that host malware, phishing and adult websites. Webroot claims it analyzes and categorizes websites at the rate of more than 5,000 URLs per second and scans the entire Internet Protocol version 4 (IPv4) space and in-use Internet Protocol version 6 (IPv6) addresses, classifying more than 95% of the internet three times per day. Filtering policies can be based on IP address, dynamic IP or both.

HOW THIS PROVIDER COMPETES

Webroot primarily sells its SecureAnywhere DNS Protection services to midsize or large enterprise organizations as well as the company's managed service provider partners. Webroot is also well-known as an OEM provider of threat intelligence and dynamic URL categorization capabilities, often provided to and embedded into competitive offerings. The company often leverages its comprehensive IT, file and URL reputation threat intelligence capabilities to entice customers to buy its solutions over others; it regularly touts its OEM business as a sign of technical prowess.

Typical estimated costs for 5,000 users (three years)

On-premises deployment model:

Webroot has no on-premises deployment model.

Cloud-delivered deployment model

Webroot SecureAnywhere DNS Protection: $145,000

Total Gartner estimated cost (three-year contract): $145,000

Zscaler

MARKET OVERVIEW

Estimated 2016 SWG revenue: $162.6 million

Zscaler is a cloud-based SWG provider with a wide range of offerings and features, including URL filtering, advanced threat defense (from malware, malicious URLs and phishing sites), sandbox, internet access management, SSL inspection, remote access, data loss prevention, cloud application visibility and granular controls, bandwidth control and outbound firewall inspection. The company markets its SWG solution as a platform concept with varying subscription pricing plans available for specific use cases. The company claims it is running physically across more than 100 data centers around the globe, including roughly 50 public data centers and peering with thousands of content providers, including Microsoft for Office 365, Google, Amazon and most of the major service providers in 22 of those data centers to enhance its service performance. Beyond the Zscaler SaaS offering, the company also offers virtual Zscaler Enforcement Nodes (VZENs) and Private Zscaler Enforcement Nodes (PZENs) to extend its offerings to on-premises where necessary. The VZEN and PZEN are full-featured on-premises appliance form factors of the Zscaler SWG that help Zscaler customers comply with regional regulations or organization mandates. The Zscaler cloud-based SWG service also supports integration with security information and event management (SIEM) from its patented Nanolog Streaming Service.

HOW THIS PROVIDER COMPETES

Zscaler is known for its creative marketing programs executed at leading security conferences, where it demonstrates moving away from appliances by placing potential buyers with a sledgehammer in front of competitive appliances and allowing the potential buyers to destroy them. Zscaler primarily competes by leveraging long-term subscription services through its extensive channel where it derives a significant portion of its revenue. The company also leverages and derives revenue from its extensive relationships with service providers, including BT, AT&T, Verizon, Orange Business Services, T-Systems, Vodafone, Singtel and Tata Consultancy Services. In 2016, the company focused primarily on sales execution and partnerships, increasing the scale of its global cloud multifold and technical improvements to the Zscaler

platform — for example, offering additional granularity to its role-based access and enhancements to its policy configuration and user interface. In February 2016, the company partnered with CASB providers CipherCloud, CloudLock (now part of Cisco) and Skyhigh Networks. In August 2016, Zscaler expanded its shared threat intelligence detection capabilities through a partnership with AlienVault. In 2017, Zscaler has maintained a more aggressive product and partnership roadmap with the announcement of partnerships with notable SD-WAN providers Viptela, VeloCloud, Riverbed and Citrix, and it continues the expansion of its SaaS delivery locations in Europe, Latin America, China and North America.

Typical estimated list price for 5,000 users (three years)

On-premises deployment model:

Zscaler offers no on-premises deployment model pricing.

Cloud-delivered deployment model:

Web business suite: $407,100

- Proxy
- Firewall
- URL filtering
- SSL inspection
- Antivirus
- Advanced threats and file sandboxing
- Cloud application visibility and control
- Mobile reporting
- Browser and plug-in controls
- Zscaler App for protecting roaming user

Total Gartner estimated cost (three-year contract): $407,100

Other Notable Secure Web Gateway Providers

Akamai Technologies (Bloxx); Citrix; ContentKeeper; Cyren; EdgeWave; F5; ReSec; Sangfor; Smoothwall

Notable Secure DNS Resolver Providers

Akamai Technologies; BlueCat; Cisco; Comodo; CrowdStrike; Neustar; Nominum; Infoblox; ThreatSTOP; Verisign

References and Methodology

To prepare this research, primary and secondary resources were used extensively. Besides surveys, we used additional industry sources to verify the accuracy of the information. Gartner estimates were calculated using telemetry from survey results, publicly available list pricing and vendor-provided guidance during interviews or other correspondence. Sources of data used by Gartner include, but are not limited to, the following:

Interviews with technology providers

Estimates from reliable industry representatives

Articles in the general and trade press

Published company financial earnings reports

Various companies, government agencies and trade associations may use slightly different definitions of product categories and regional groupings, or they may include different companies in their summaries. These differences should be kept in mind when making comparisons between data and numbers provided by Gartner and those provided by other research organizations.

Definitions

Cloud-based — Capabilities offered as a software as a service (SaaS). Not to be confused or conflated with virtualized appliance options for public or private cloud infrastructure.