

MarketScope for Multifunction Firewalls for Small and Midsize Businesses

Greg Young, Adam Hils

A distinct market exists for multifunction security appliances for SMBs, and many vendors provide all-in-one or multifunction firewall products that are similar; however, the differences in features and pricing make a product selection worthwhile.

WHAT YOU NEED TO KNOW

Small and midsize businesses (SMBs) have very different requirements than large enterprises for network security. Multifunction firewalls are not suitable for the enterprise, and SMBs do not usually require several best-of-breed network security appliances. The SMB multifunction firewall market is large, fragmented and highly dynamic, with vendors providing a common set of core safeguards; differentiating with new added safeguards, ease of installation and use; and addressing the realities of the SMB IT environment.

MARKETSCOPE

For the purpose of this research, Gartner defines SMB organizations based on number of employees (see Table 1).

Table 1. SMB Organizations Based on Number of Employees

Small Business Segment	Asia/Pacific	Europe	Latin America	North America
Small Business	20-99	10-49	10-99	20-99
Midsize Business Segment				
Low-End Midmarket	100-249	50-249	100-249	100-499
Upper-End Midmarket	250-499	250-499	250-499	500-999

Source: Gartner (June 2008)

Market/Market Segment Description

SMBs have network security appliance needs that differ substantially from large enterprise requirements. In contrast with large enterprises, which most-often deploy firewalls and other network security functions on distinct appliances to ensure optimal network performance and risk mitigation through multiple security "points of failure," SMBs often opt for "all in one" or multifunction security appliances built on the "anchor" technology of the firewall. Additional safeguards are added to the firewall, sometimes through a subscription fee.

The feature sets available with these SMB multifunction firewall products typically fall into three categories:

- Network security, comprising firewalls, intrusion prevention systems (IPSs)/intrusion detection systems and virtual private networks (VPNs)
- Web security, which includes Web antivirus and URL filtering
- E-mail security, including e-mail antivirus, instant messaging (IM) hygiene and anti-spam

In some cases, many of these features are available as part of the base product license; in others, they are available as add-on licenses. This diversity is typical of emerging, fragmented information security markets. As the market matures, the all-in-one pricing model will become the de facto standard.

The term unified threat management (UTM) is often used to describe products in this market; however, this term is pure marketing hype, because threats are never really "managed." The UTM label has also been co-opted by some vendors to describe their enterprise next-generation firewall offerings, diluting the term's relevance. This market is also distinguished from the enterprise and branch office firewall markets (see "Magic Quadrant for Enterprise Network Firewalls, 2H07").

Enterprises tend to select several best-of-breed appliances for network security. Branch office firewalls are considered part of the enterprise firewall network market because they are selected and deployed as extensions of the central firewalls and do not have the same features as those deployed in SMBs (for example, e-mail antivirus is often not used in branches where the e-mail servers are centralized, and managing a large number of firewalls is required in branches but not in an SMB). The term "anti-X" is also used in some vendor marketing to collectively refer to the antimalware and antivirus safeguards.

Overall, the worldwide SMB multifunction firewall market was approximately \$1.2 billion in 2007, with a forecast 35% to 40% compound annual growth rate through 2011. The SMB multifunction firewall market is a highly competitive, fragmented market, with more than 20 active vendors. This competition is complicated by the multiple individual safeguards within the same appliance: No vendor can provide best-of-breed functionality across all the safeguards, so many vendors share safeguards from the same OEM providers (for example, Sophos for gateway antivirus). Differentiation often comes in the form of integration between safeguards, licensing flexibility, management console/reporting and pricing. Successful vendors will:

- Focus on simplicity of deployment and operation.
- Provide proactive attention to channel partners in recognition that value-added resellers (VARs) will often be the greatest influencer for this market.
- Introduce new features just ahead of customer requirements.
- Provide pricing that encourages the adoption of new subscription-based safeguards, but with simplicity that does not require frequent changes in payment.
- Focus on SMB needs, rather than attempting to use downsized enterprise products and strategies.

According to Gartner's vendor survey, most of the SMB multifunction firewall replacements that vendors are doing are of legacy, firewall-only products from enterprise firewall market leaders: Cisco, Check Point Software Technologies and Juniper Networks. By the end of 2010, we expect to see significantly greater numbers of SMB multifunction firewalls displacing in-kind competitors. Vendors that have traditionally focused on smaller businesses as their core business and have a strong foothold there (such as Fortinet, SonicWALL and WatchGuard Technologies) are trying to move upstream and, therefore, usually name Cisco as their main competitor. Vendors looking to establish a greater presence in the lower-midmarket space consider SonicWALL and Fortinet their strongest competitors.

Enterprise firewall vendors have a slow success rate in this market because they are unable to adapt their business models and products to the smaller horizontal market with features such as a management console, which can be used by nonexpert users; a full range of safeguards in a single appliance; licensing for subscription-based, add-on safeguards that does not require frequent payment increases; and a support offering that is affordable and does not treat SMBs like a less-desirable class of customer. As part of our interviews with customers, we found that some SMBs were using a product that did not provide the option to add on a safeguard they

needed. These SMBs were left with the two undesirable choices of purchasing a second appliance or remaining vulnerable, and most were choosing to remain vulnerable.

Gartner's survey of vendors determined that dollar/Mbps of firewall throughput varied greatly, ranging from \$4 to \$15. No vendor we assessed yet has IPv6 support, although most have it on their road maps for 2010. In this MarketScope, we use the term "base product" to mean the initial product purchase without optional subscription services or add-on products.

This market will continue to grow, driven by the requirement to add new safeguards to counter new threats, and by the need for growing SMB companies to replace appliances for those with more capacity. Small and lower-midsize companies will continue to use the single multifunction appliance. Upper-midsize businesses will be candidates for stand-alone, best-of-breed appliances as they grow into enterprise-size and enterprise IT. The enterprise vendors will continue to struggle for market share and will not fully succeed unless they directly address SMB requirements across their business, and don't just offer downsized enterprise equipment with highly complex pricing schemes and overly complicated management.

Inclusion and Exclusion Criteria

Inclusion Criteria

SMB multifunction firewall companies that meet the market definition and description were considered for this MarketScope if they met the following conditions:

- Regularly appeared on SMB shortlists for final selection.
- Achieved SMB multifunction firewall product sales (not including maintenance and so forth) in the past year of more than US\$5 million within a customer segment that is visible to Gartner, or had at least 2,000 devices under paid support and maintenance.

Exclusion Criteria

SMB multifunction firewall companies that were not included in this MarketScope may have been excluded for one or more of the following conditions:

- There was insufficient information for assessment, and the company did not otherwise meet the inclusion criteria or is not yet actively shipping products.
- Products are not usually deployed as the primary, Internet-facing firewall (for example, proxy servers and network IPS).
- Products are built around personal firewalls, host-based firewalls, host-based IPS and Web application firewalls — all of which are distinct markets.

Excluded Vendors

Gartner excluded numerous vendors that did not meet the inclusion criteria — usually those that did not meet the revenue/supported devices criteria. Two vendors we excluded that merit mention are:

Juniper Networks

Juniper Networks asked not to participate in this MarketScope because it is focusing more on larger customers. Even so, SMB firewall vendors list Juniper as a top competitor, and many SMB customers include it in RFPs and evaluations. Gartner did not include Juniper in this assessment

because Juniper's focus on lower-end appliances is for branch office deployments in enterprises, rather than SMBs and SMB customers.

Microsoft

Microsoft asked not to have Microsoft Internet Security and Acceleration (ISA) Server included in this MarketScope. Gartner did not include Microsoft ISA Server because replacement products for ISA are forthcoming (in the form of the Forefront Threat Management Gateway product), and the current version does not include the all-in-one suite of safeguards seen in other vendors in this MarketScope.

Rating for Overall Market/Market Segment

Overall Market Rating: Strong Positive

The SMB multifunction firewall market is growing; however, heavy price competition means that individual vendors require discipline to stay in business. Innovation is somewhat limited in that the nature of the product platform is to add new features to generate revenue or gain competitive advantage, but at relatively low margins, making a potential product road map mistake costly.

Evaluation Criteria

Table 2. Evaluation Criteria

Evaluation Criteria	Comment	Weighting
Offering (Product) Strategy	Product service and customer satisfaction in deployments. Considers factors related to getting products sold, installed, supported and in users' hands. Strong execution means that a company has demonstrated to Gartner analysts that it can successfully and continuously be deployed in SMBs and, ultimately, win a large percentage of deals when competing with other vendors. Companies that execute strongly generate pervasive awareness and loyalty among Gartner clients, as well as a steady stream of inquiries to Gartner analysts. Execution is not primarily about company size or market share, although those factors can affect a company's ability to execute. Sales are a factor; however, winning in competitive environments through innovation and product quality is foremost over revenue.	high

Evaluation Criteria	Comment	Weighting
Marketing Strategy	<p>This includes providing a track record of delivering on innovation that precedes customer demand rather than an "us too" road map, and can demonstrate an understanding and commitment to the SMB network security market. Gartner makes this assessment subjectively by several means, including vendor-briefing interactions and feedback from Gartner customers on information they receive about road maps. Incumbent vendor market performance is reviewed year over year against specific recommendations that have been made to each vendor and against future trends identified in Gartner research. Vendors cannot merely state an aggressive future goal; they must put a plan in place, show that they are following their plan and modify their plan as they forecast changes in market direction.</p>	standard
Innovation	<p>Innovation, including R&D, and quality differentiators, such as:</p> <ul style="list-style-type: none"> • Performance • Meeting customer requirements in a timely manner • Integration with other security products • Management interface and clarity of reporting <p>The more a product mirrors the workflow of the enterprise operation scenario, the better the vision.</p> <p>Products that are not intuitive in deployment or operations are difficult to configure, or have limited reporting scores. Solving customer problems is a key element of this category. Reducing the rules base, interproduct support and leading competitors on features are important.</p>	high

Evaluation Criteria	Comment	Weighting
Market Responsiveness and Track Record	The key factor is adding new products and features in response to customer needs, and a proven track record of meeting road map goals.	high
Customer Experience	<p>Customer experience and operations, including management experience and track record, and depth of staff experience specifically in the security marketplace. The greatest factor in this category is customer satisfaction throughout the sales and product life cycle. Low latency, channel support and how the firewall fared under attack conditions are also important.</p> <p>Key factors are weighted heavily, such as ease of use, console quality, add-on products beyond the firewall (VPN, antivirus and URL filtering), the range of models, secondary product capabilities (logging, event management and compliance), being able to support SMB deployments, and meeting channel and SMB requirements.</p>	high

Evaluation Criteria	Comment	Weighting
Product/Service	<p>Considers factors related to getting products sold, installed and supported. A company has demonstrated to Gartner that it is successfully and continuously deployed in SMBs, and wins a large percentage in competitive situations. Generate pervasive awareness and loyalty among Gartner clients. Not primarily about company size or market share, although those factors can impact success in this category. Sales are a factor, but winning competitive deals through innovation and quality is foremost. Key features are weighted heavily, such as ease of use, subscription model, channel service, console quality, add-on products range of models, secondary product capabilities (logging, event management, compliance), being able to support SMB deployments, and meeting channel and SMB requirements.</p>	high
Overall Viability (Business Unit, Financial, Strategy, Organization)	<p>Overall business viability, including overall financial health, prospects for continuing operations, company history, and demonstrated commitment in the SMB firewall and related security market. Growth of the customer base and revenue derived from sales are also considered. All vendors were required to disclose comparable market data, such as SMB firewall revenue, competitive wins vs. key competitors (which is compared with Gartner data on such competitions held by our customers) and devices in deployment. Firewalls shipped are not a key measure of execution. Instead, we consider the use of these firewalls to protect the key business systems of Gartner SMB clients.</p>	standard

Source: Gartner

Figure 1. MarketScope for Multifunction Firewalls for Small and Midsize Businesses

	RATING				
	Strong Negative	Caution	Promising	Positive	Strong Positive
Astaro				x	
Check Point Software Technologies			x		
Cisco			x		
Cyberoam				x	
eSoft		x			
Fortinet					x
IBM		x			
NETASQ			x		
Secure Computing			x		
SonicWALL					x
StillSecure		x			
Untangle				x	
WatchGuard Technologies				x	

As of 27 June 2008

Source: Gartner (June 2008)

Vendor Product/Service Analysis

Astaro

Differentiators/Strengths

Astaro offers a range of Intel-based appliances for SMBs. In addition, Astaro provides software for customer hardware, and a separate virtual appliance.

Customers we interviewed liked the ease of installation and intuitive interface, with many default settings reducing configuration complexity to a minimum, and the fact that it integrates out-of-the-box with Active Directory and Novell eDirectory. In addition, companies can back the device up to a single file. An "up-to-date" feature calls back to Astaro daily for firmware updates using a "wizard" process.

Astaro is easy to configure for voice over IP security. The device understands the Session Initiation Protocol (SIP)/H.323 control connection, parses the control data, and opens up ports for the voice and video connections automatically. It also ensures that the voice and data connections get automatically shaped with quality of service (QOS) in the same traffic group as the control connection.

Base price includes appliance, firewall, IPS and VPN, with third-party Web and e-mail security feature packages available via subscription. Astaro's leverage and integration of a range of open-source components provide a competitive price point. The IPS is a Snort-based engine populated with IPS rules; not an ideal blocking solution, but it is consistent with the open-source strategy.

Astaro is assigned a rating of Positive for having good networking capabilities, albeit in a limited geographic base, and high user satisfaction for ease of use and automation.

Challenges

Astaro has little visibility outside Europe, although North American revenue is growing. And there is no access control for FTP by users.

Appropriate Use Cases

- Most SMB deployments
- Novell eDirectory environments

Rating: Positive

Check Point Software Technologies

Differentiators/Strengths

Check Point has two product ranges that overlap for the SMB market:

- Four models of the Safe@Office small business appliance line
- The UTM-1 line available as an appliance (UTM-1) or in software (VPN-1 UTM)

As a well-established, large, public company, Check Point offers a wide support network, healthy customer base and a range of platform choices. The Safe@Office line, produced by SofaWare Technologies (a Check Point company), includes virtual LAN support and options for Wi-Fi. Customers we interviewed expressed high satisfaction with the graphical user interface (GUI), especially during product installation. The UTM-1 includes firewall, VPN, IPS, gateway antivirus, anti-spam, URL filtering, and IM and peer-to-peer blocking. Customers report the GUI to be good, but the IPS as inaccurate.

We assigned a Promising rating to Check Point for good channel presence, brand and its focus on security; however, we did recognize the slower competitive adoption of the full all-in-one feature set, limited IPS capability and being listed often as the product replaced by competitors.

Challenges

Check Point is primarily focused on the enterprise, and positions the UTM-1 for branch offices rather than the SMB market. Upper-midsize customers will be well-served, but small businesses are likely to find better solutions with SMB-focused vendors.

The management of the two product lines is not interoperable, meaning that two consoles could be required where a company has multiple firewalls or a change in products when upgrading to a larger model.

Appropriate Use Cases

- Midsize businesses, especially where rapid growth in the business or infrastructure is expected and will require a firewall upgrade in the near term

Rating: Promising

Cisco

Differentiators/Strengths

The primary Cisco offerings for SMBs are the ASA 5505, 5510 and 5520 appliances, enabling the security features on the Cisco Integrated Services Router (ISR). The Linksys brand is also an

offering, although this consumer-grade product is suitable only for the smallest businesses and, like other enterprise-class vendors, there is no integration or interoperability between the two lines. Two hardware add-in modules are available for ASA: the Advanced Inspection and Prevention (AIP) module, which adds IPS; and the Content Security and Control (CSC) module for other anti-X features (such as URL filtering, antivirus, anti-spam and antispypware); however, both modules cannot be used concurrently in the same appliance. Users we spoke with mentioned that the inability to add memory causes performance problems when logging is activated in the device GUI.

Cisco has a huge networking installed base, a wide marketing and sales reach, and a large base of trained networking decision makers. The company also offers firewall, VPN and IPS capabilities in the Cisco ISR, although none of the other anti-X features are available.

Cisco is assigned a Promising rating in view of its channel strength and high market share, notwithstanding lack of feature parity in the SMB all-in-one firewall market and being listed as the product most replaced by competitors in our surveys. Enterprise-class management tools do not adapt well to the SMB market; however, Cisco's long-term road map for an improved SMB console is encouraging. Cisco has a vast geographic reach and has been moving well in replacing aging Cisco PIX firewalls in SMBs with the newer Cisco ASA platform. ASA customers reported Cisco's hardware to be reliable, but did not like the add-in module approach.

Challenges

Cisco lacks feature parity with comparable products. Many SMB IT staffs also find its product difficult to configure and manage.

Appropriate Use Cases

- Upper-midsize (500-1,000 employees), Cisco-oriented IT organizations where other Cisco security offerings are already in place

Rating: Promising

Cyberoam

Differentiators/Strengths

With a substantial installed base in India, Cyberoam has a full suite of safeguards: firewall, VPN, IPS and anti-X. The company differentiates on identity-based network access — which provides access control that links IP addresses with directory identity (such as Active Directory) — and bandwidth management, which is of interest where Internet connectivity is expensive or in short supply. Cyberoam has seven models of appliances in the CRi series for SMBs. It logs user behavior and provides a policy-based way of limiting access. Specifically, it targets user environments where the user-to-PC ratio is greater than 1:1. Education and healthcare are the top two vertical markets Cyberoam delivers to, and they are specific targets to enable Cyberoam to develop a defensible market niche.

Cyberoam is assigned a Positive rating due to its strong presence in Asia, which provides a defensible niche market and base for expansion into other markets. Cyberoam's products have unique features and serve some distinct vertical markets. They are also potentially disruptive to competitors that are trying to enter emerging markets. Balancing this is the challenge of moving into new markets and growing a more mature company infrastructure.

Challenges

Cyberoam must build a meaningful presence outside of Asia.

Appropriate Use Cases

- SMBs in the Asia/Pacific region, or the healthcare and education vertical markets

Rating: Positive

eSoft

Differentiators/Strengths

eSoft has four models, with list prices starting at \$799. eSoft InstaGate is focused on ease of deployment, and its safeguards include firewall, VPN and URL filtering. All the eSoft InstaGate safeguards and signature updates are developed in-house. All models include a liquid crystal display (LCD) front panel on appliances, which supports configuration without the requirement for remote management access, and an onboard e-mail server that includes Web mail.

A Caution rating is assigned to eSoft because, although a healthy mix of features is provided, the company's move into the security market is being met with skepticism by some buyers that the full suite of safeguards can be competitively delivered. InstaGate is for small businesses, and midsize companies will be better-served elsewhere. eSoft also declined to provide any financial information as part of the survey. The e-mail server is a differentiator for small business selections.

Challenges

eSoft has low visibility in the marketplace.

Appropriate Use Cases

- Small businesses with limited IT resources looking for an easy-to-deploy, all-in-one product

Rating: Caution

Fortinet

Differentiators/Strengths

Fortinet is well-established as an SMB multifunction firewall maker with a large model range. All Fortinet safeguards are developed in-house — they do not OEM products from others — and they have their own antivirus, URL and IPS signature research team. This do-it-yourself approach insulates Fortinet from the acquisitions and travails of partners, with the trade-off being a potential perception that not all services are able to compete as best-of-breed.

Fortinet has a strong presence in the Asia/Pacific region and North America, and has a well-developed console. Fortinet SMB appliances are application-specific integrated circuit (ASIC)-based, most are sub-1U size and they have a good number of physical ports. Some models include dual-WAN ports, so that a backup or dual Internet connection can be used without an external handler. Two small business models include a wireless access point. A firewall and VPN are standard, with all other services (antivirus, anti-spam, URL filtering and IPS) requiring subscription after the first year (most include one-year minimum support).

Fortinet was the second-most-named primary competitor among the vendors surveyed. The upper-midsize-targeted FortiGate-310B was recently released and includes a dedicated content ASIC to complement the ASIC. FortiGate-310B is expected to replace many current midsize models. Users we interviewed liked the range of features and the common look and feel across the console.

Fortinet is assigned a Strong Positive rating because it provides coverage for almost all SMB deployment scenarios, is competitively priced, and is highly visible to end users and competitors.

Challenges

Fortinet's expansion into the enterprise horizontal market will distract it from its SMB roots. To this point, Fortinet has done a good job in maintaining this balance, but it must continue to nurture its SMB channels with strong marketing and product development.

Appropriate Use Cases

- Most SMB deployments
- Fast-growing, upper-midsize businesses

Rating: Strong Positive

IBM

Differentiators/Strengths

IBM Internet Security Systems (ISS) has a strong enterprise security legacy powered by the X-Force security research team. The company has strong network IPS capabilities, and its SMB all-in-one firewall, the Proventia Network Multifunction Security product (formerly Proventia-M), contains that technology. In addition to firewall/IPsec VPN, IBM ISS offers internally developed Web filtering and anti-spam, the security and quality of which users we interviewed liked very much. However, some customers report problems with latency and performance when spam and HTTP filtering are turned on.

IBM provides the option for antivirus from its OEM partner, Sophos. In January 2008, IBM ISS shipped a limited data loss prevention capability that searches for credit card numbers, addresses, Social Security numbers and custom expressions, and will alert and mask or block content.

With its third-quarter release, IBM ISS aims to provide Secure Sockets Layer VPN, WAN failover and load balancing, traffic shaping, and QOS features that will help the company reach better networking feature parity with several of its competitors.

IBM has also introduced managed services, providing all-in-one firewall services (called IBM Express Advantage) to provide management as part of a single purchase. IBM Express Advantage offerings can provide an access point for smaller customers to benefit from IBM ISS' security expertise without introducing a product with enterprise complexity in constrained-resource SMB IT organizations.

IBM is assigned a Caution rating because the company is first-and-foremost a software and services company, not a network security company. This has affected the ISS business overall. Furthermore, the enterprise success and focus of ISS has not been adapted to the SMB market. Competitors do not view IBM as a threat in this market, price is high and buyers do not often shortlist IBM. IBM's sales capability could be a strong competitive advantage if directed toward achieving an increase in market share after product feature parity was achieved and the ISS products were raised in visibility within IBM.

Challenges

There is continued uncertainty as to the future of the legacy ISS product lines, and the price range (\$999-\$19,900) is on the high end for SMBs, leaving significant portions of the market under-served. As a whole, IBM will be challenged to build channels and products to serve SMBs.

Appropriate Use Cases

- Upper-midsize environments where other ISS products are deployed
- Customers for whom security is the primary motivator, above performance and ease of use

Rating: Caution

NETASQ

Differentiators/Strengths

NETASQ provides a good mix of advanced network security features to drive network performance, and provides embedded OEM solutions such as antimalware from Kaspersky Labs, and URL filtering and antiphishing from Optenet. NETASQ's platform and operating system are proprietary, and intrusion prevention is done at the kernel (driver) level. NETASQ's five models targeting less-than-1,000-users enterprises have three or more WAN ports. Its pricing model is all-in-one (no fees for add-on modules), with all signature update fees included in the maintenance fee.

In Europe, the Middle East and Africa, NETASQ has a strong set of value-added distributors to help the company gain traction in local markets. It also has telecommunications partners that sell managed UTM services to their SMB customers.

NETASQ is assigned a Promising rating because it is more focused on general networking functions, balanced with good pricing. Although NETASQ has low competitive visibility, within Western Europe, it provides a good offering.

Challenges

NETASQ's business is almost entirely in Western Europe (mostly in France), which is a risk as larger competitors focus more on the European market. The company also does not emphasize IPS signatures, which some buyers use as a point of comparison. Explaining how protocol analysis and contextual signatures provide protection without touting traditional IPS signatures as a valid alternate approach is difficult when speaking to SMBs.

Appropriate Use Cases

- Upper-midsize European businesses that focus on network performance

Rating: Promising

Secure Computing

Differentiators/Strengths

Secure Computing is a publicly traded, well-established security company based in the U.S. Subsequent to the CipherTrust acquisition, Secure Computing develops most of the safeguards in the product in-house. Secure Computing, like Check Point and Cisco, maintains a distinct product line for small businesses. The SnapGear product line has a good adoption rate and six models, with tens of thousands of devices in deployment, mostly in North America. Customers cite ease of installation as a benefit. Nessus vulnerability scanning is included in the base product. The Type of Service (ToS) feature can prioritize by protocol type, and is useful for some denial-of-service protection and for enabling QoS. The SnapGear firewall has ICSA certification, and has a Dynamic Host Configuration Protocol (DHCP) and SIP proxy options. Secure Computing has a good track record of avoiding vulnerabilities in its products.

Secure Computing is assigned a Promising rating in light of easy product deployment cited by customers as "very plug and play," the increased capability of the former CipherTrust safeguards, and its focus on security, balanced with low visibility in competitions and an unclear strategy for the SMB market. Customers reported that they liked the Web interface, with their support experience being mixed yet improving.

Challenges

Secure Computing is primarily focused on the enterprise market, so serving the SMB market will remain a challenge, especially against SMB-focused competitors.

Appropriate Use Cases

- SMBs where security is valued over feature parity with other SMB firewall competitors

Rating: Promising

SonicWALL

Differentiators/Strengths

Vendors we surveyed listed SonicWALL most often as their primary competitor. SonicWALL appliances are ASIC-based, most are sub-1U size and they have a good number of physical ports. The management interface is clear, intuitive, includes wizards for common tasks, a packet capture option and hierarchical management roles. An "application firewall" feature is included; however, this is a protocol-blocking tool (for example, blocking BitTorrent) rather than a Web application firewall. With its E-Class Network Security Appliance (NSA) line, which is based on multicore processors, SonicWALL is trying to address upper-midmarket performance needs. More than 60% of SonicWALL's 1Q08 product revenue came from devices priced at less than \$1,500, with 12% coming from devices priced over \$5,000.

With its upcoming release of NSA 2400, SonicWALL aims to bring multicore performance with SMB-friendly pricing. Client satisfaction is generally high among Gartner customers using SonicWALL products, with customer friction occurring mostly when midsize customers outgrow the all-in-one product form — a problem common to many direct competitors.

SonicWALL is assigned a rating of Strong Positive because it's highly visible to end users and competitors, is focused on the SMB market with strong finances and releases features ahead of customer demand.

Challenges

SonicWALL is trying to address enterprise environments with its "E" series, which could distract the company from its SMB focus.

Appropriate Use Cases

- Most SMB deployments

Rating: Strong Positive

StillSecure

Differentiators/Strengths

The Cobia platform is an open-source project sponsored by StillSecure that includes selectable modules for network firewall, router, DHCP and a beta of an IPS module. Although it does not

have a General Public License, Cobia is generally free for use for users willing to source their own server hardware.

Although Cobia is new and does not have the full feature set of competing products, it represents an option for cost-conscious smaller businesses that want to combine networking and security, or as a platform for emerging security vendors to build products on.

StillSecure's Cobia is rated as a Caution because it does not have many of the features of traditional multifunction SMB firewalls; however, for network-savvy small businesses, it is an option.

Challenges

Most organizations will opt for appliances and will not have the expertise or the will to build their own firewall. Open-source blocking technologies (such as firewalls and IPS) have not had a high adoption rate.

Appropriate Use Cases

- Cobia can represent a cost-effective solution for the most cash-starved security budgets in small businesses.
- As a platform for third-party security products.

Rating: Caution

Untangle

Differentiators/Strengths

Untangle's model differs from most of its competitors. Aimed at the smallest businesses (less than 150 users) and the VARs that serve them, this open-source platform is downloadable at no charge. Optional service and support packages, as well as OEM relationships (Untangle recently announced an option for Virus Blocker powered by Kaspersky), generate revenue.

Even with paid support, Untangle is inexpensive. In addition to the paid support the company offers, it hosts an active community forum for support questions. Untangle has created close relationships with its channel and customers.

Untangle is assigned a Positive rating for small businesses because of the low entry price for customers and its strategy for opening up product licensing for adoption by other vendors.

Challenges

Untangle will be challenged to generate revenue and gain a broader base of paying customers. It also must maintain a high degree of customer touch as business grows, and it will need more-advanced features.

Appropriate Use Cases

- Very small businesses with no in-house IT capabilities, where price is the primary motivation

Rating: Positive

WatchGuard Technologies

Differentiators/Strengths

With 10 years experience in the SMB multifunction firewall market, WatchGuard has eight competitively priced, Intel-based firewall models in the "e-Series," starting as low as \$480 in the SMB market. The e-Series has three sub-classes — Edge, Core and Peak — with each line respectively providing greater throughput and processing. The company uses modular per-feature pricing to activate IPS, e-mail antivirus, anti-spam, URL filtering and Web antivirus. All features except for the firewall, IPS and VPN are resold from third parties.

WatchGuard is competitive in bringing new features to market early. It is customer-focused, has Evaluation Assurance Level (EAL)-4 Common Criteria certification and is increasing its market share. WatchGuard Firebox appliances include a cryptographic accelerator chip to ease the load on the processor from VPN handling, traffic shaping, QOS, multi-WAN support, high availability and DHCP relay.

Users we interviewed mentioned the robust firewall features in the appliances and the high-quality customer support.

WatchGuard is assigned a rating of Positive because of its increased investment in engineering and support, and its focus on the SMB deployment realities and customer satisfaction, albeit with limited competitive visibility.

Challenges

Since going private in 2007, WatchGuard has been in a rebuilding mode. As it tries to execute on its larger-customer (up to 5,000 users) firewall vision, it will be continually challenged to maintain its SMB product focus. WatchGuard must overcome customer perceptions of uncertainty about company viability.

Appropriate Use Cases

- Most SMB deployments

Rating: Positive

RECOMMENDED READING

"Magic Quadrants and MarketScopes: How Gartner Evaluates Vendors Within a Market"

Acronym Key and Glossary Terms

AIP	Advanced Inspection and Prevention
ASIC	application-specific integrated circuit
CSC	Content Security and Control
DHCP	Dynamic Host Configuration Protocol
EAL	Evaluation Assurance Level
GUI	graphical user interface
IM	instant messaging

IPS	intrusion prevention system
ISA	Internet Security and Acceleration
ISR	Integrated Services Router
ISS	Internet Security Systems
LCD	liquid crystal display
NSA	Network Security Appliance
QOS	quality of service
SMB	Small and midsize business
ToS	Type of Service
UTM	unified threat management
VAR	value-added reseller
VPN	virtual private network

Vendors Added or Dropped

We review and adjust our inclusion criteria for Magic Quadrants and MarketScopes as markets change. As a result of these adjustments, the mix of vendors in any Magic Quadrant or MarketScope may change over time. A vendor appearing in a Magic Quadrant or MarketScope one year and not the next does not necessarily indicate that we have changed our opinion of that vendor. This may be a reflection of a change in the market and, therefore, changed evaluation criteria, or a change of focus by a vendor.

Gartner MarketScope Defined

Gartner's MarketScope provides specific guidance for users who are deploying, or have deployed, products or services. A Gartner MarketScope rating does not imply that the vendor meets all, few or none of the evaluation criteria. The Gartner MarketScope evaluation is based on a weighted evaluation of a vendor's products in comparison with the evaluation criteria. Consider Gartner's criteria as they apply to your specific requirements. Contact Gartner to discuss how this evaluation may affect your specific needs.

In the below table, the various ratings are defined:

MarketScope Rating Framework

Strong Positive

Is viewed as a provider of strategic products, services or solutions:

- *Customers:* Continue with planned investments.
- *Potential customers:* Consider this vendor a strong choice for strategic investments.

Positive

Demonstrates strength in specific areas, but execution in one or more areas may still be developing or inconsistent with other areas of performance:

- *Customers:* Continue planned investments.
- *Potential customers:* Consider this vendor a viable choice for strategic or tactical investments, while planning for known limitations.

Promising

Shows potential in specific areas; however, execution is inconsistent:

- *Customers:* Consider the short- and long-term impact of possible changes in status.
- *Potential customers:* Plan for and be aware of issues and opportunities related to the evolution and maturity of this vendor.

Caution

Faces challenges in one or more areas.

- *Customers:* Understand challenges in relevant areas, and develop contingency plans based on risk tolerance and possible business impact.
- *Potential customers:* Account for the vendor's challenges as part of due diligence.

Strong Negative

Has difficulty responding to problems in multiple areas.

- *Customers:* Execute risk mitigation plans and contingency options.
- *Potential customers:* Consider this vendor only for tactical investment with short-term, rapid payback.

REGIONAL HEADQUARTERS

Corporate Headquarters

56 Top Gallant Road
Stamford, CT 06902-7700
U.S.A.
+1 203 964 0096

European Headquarters

Tamesis
The Glanty
Egham
Surrey, TW20 9AW
UNITED KINGDOM
+44 1784 431611

Asia/Pacific Headquarters

Gartner Australasia Pty. Ltd.
Level 9, 141 Walker Street
North Sydney
New South Wales 2060
AUSTRALIA
+61 2 9459 4600

Japan Headquarters

Gartner Japan Ltd.
Aobadai Hills, 6F
7-7, Aobadai, 4-chome
Meguro-ku, Tokyo 153-0042
JAPAN
+81 3 3481 3670

Latin America Headquarters

Gartner do Brazil
Av. das Nações Unidas, 12551
9º andar—World Trade Center
04578-903—São Paulo SP
BRAZIL
+55 11 3443 1509