

# Magic Quadrant for Enterprise Network Firewalls

14 December 2011 ID:G00219235

**Analyst(s):** Greg Young, John Pescatore

## VIEW SUMMARY

The enterprise network firewall market is undergoing a period dynamic evolution, as effective next-generation firewalls are now increasingly necessary. Vendors that have addressed advanced targeted threats have seen gains in the market.

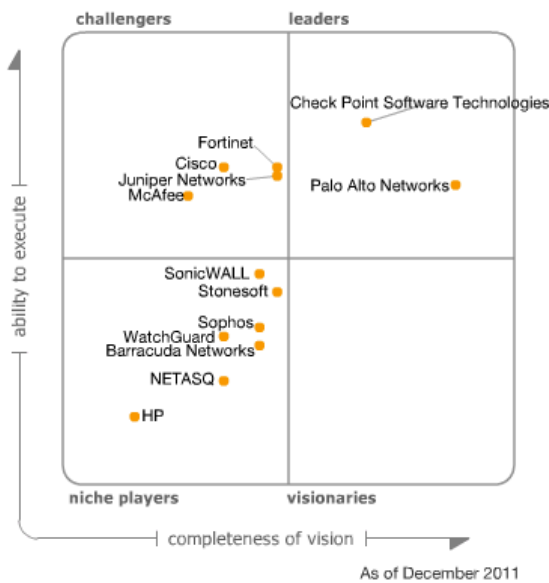
## What You Need to Know

The enterprise firewall market is one of the largest and most mature security markets. It is populated with both mature vendors and some more recent entrants. Changes in threats, as well as increased enterprise demand for mobility, virtualization and use of the cloud, have increased demand for new firewall features and capabilities. Organizations' final product selection decisions must be driven by their specific requirements, especially in the relative importance of management capabilities, ease and speed of the deployment, acquisition costs, IT organization support capabilities, and integration with the established security and network infrastructure.

[Return to Top](#)

## Magic Quadrant

**Figure 1.** Magic Quadrant for Enterprise Network Firewalls



Source: Gartner (December 2011)

[Return to Top](#)

## Market Overview

Firewalls are generally the first line of defense between untrusted networks (such as the Internet or connections to business partners). They limit the attack aperture for vulnerable PCs, servers and other infrastructure elements. Firewalls long ago became a "check the box" requirement in most compliance regimes for securing trust boundaries. Throughout the years, firewalls have continued to evolve to add deeper and more flexible inspection and enforcement capabilities as threats advanced, and to run at faster and faster throughput rates as network speeds increased.

In 2010 and 2011, Gartner saw market pressures accelerate the demand and available offerings for next-generation firewall (NGFW) platforms (see "Defining the Next-Generation Firewall") that provide the capability to detect and block sophisticated attacks, as well as enforce granular security policy at

## ACRONYM KEY AND GLOSSARY TERMS

<b>ASA</b>	Adaptive Security Appliance
<b>ASIC</b>	application-specific integrated circuit
<b>FPM</b>	firewall policy management
<b>FIPS</b>	Federal Information Processing Standard
<b>Gbps</b>	gigabits per second
<b>IPS</b>	intrusion prevention system
<b>ISP</b>	Internet service provider
<b>MFE</b>	McAfee Firewall Enterprise
<b>MSSP</b>	managed security service provider
<b>NGFW</b>	next-generation firewall
<b>SMB</b>	small or midsize business
<b>SSL</b>	Secure Sockets Layer
<b>SWG</b>	secure Web gateway
<b>UTM</b>	unified threat management

## EVIDENCE

The analysis in this report was primarily based on (1) interviews and interactions during firewall inquiries with Gartner clients since the last report, (2) surveys completed by vendors, (3) vendor briefings, (4) interviews with references provided by the vendor, and (5) supporting quantitative research on market share.

## NOTE 1 FIREWALL POLICY MANAGEMENT TOOLS

Third-party FPM vendors (such as AlgoSec, LogLogic, RedSeal Networks, Tufin, FireMon and Skybox Security) continue to exploit the absence of firewall consoles to optimize, visualize and reduce firewall rules and policies. Although the FPM market is still somewhat small, the customers requiring help with complexity are the very largest, and the market is growing. Additionally, very large enterprises usually have firewall products from different vendors — usually by accident via acquisition, rather than through choice, because a single vendor solution is usually the best choice. All FPM vendors support multiple firewall products, whereas almost no firewall vendor will manage a competing product and is expanding into managing other network security devices.

## 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

the application (versus port and protocol) level. As enterprises increase the use of Web-based applications — with more complex connections within applications, more complex data centers and more data being presented to customers — firewalls have had to keep up with features and performance to meet these changing needs. Gartner also saw increased enterprise demands for aggregate throughput rates of 5Gbps and higher, as well as demand for the ability to partition higher-capacity firewall platforms into multiple virtual firewalls.

Gartner also observed an acceleration of the trend for large distributed businesses moving away from backhauling or "home running" all branch-office Internet connectivity back through the headquarters firewall and toward allowing direct branch-office connectivity to the Internet for user Web surfing and the like. The majority of enterprises still look to their primary firewall vendors to provide the branch-office devices. With few exceptions, a single brand of firewall vendor is the best practice (see "Q&A: Is It More Secure to Use Firewalls From Two Different Vendors?"). However, many enterprises are moving their Web security gateway tier to cloud-based or as-a-service delivery to deal with mobile employee Web use, and are finding that this is also a very attractive approach for providing low-cost secure Web access to branch offices without requiring customer premises equipment. For simple branch offices, this enables the branch's point-of-presence router to be used for connectivity back to headquarters and the Internet without an additional firewall product.

Branch office firewalls and small or midsize business (SMB) firewalls continue to diverge as increasingly distinct products, along with relatively simple management tools to deploy and operate them (see "Magic Quadrant for Unified Threat Management"). In that midsize market, Gartner sees managed security service providers (MSSPs) as having increased influence over firewall and intrusion prevention system (IPS) product selection, as small businesses limit their hiring of expensive security personnel.

Acquisitions and initial public offerings were limited in 2010 and 2011 to the purchase of Astaro by Sophos (see "Astaro Acquisition Will Extend Sophos' Midmarket Security Offerings"). McAfee, which had acquired Secure Computing, was acquired by Intel, and SonicWALL was acquired by Thoma Bravo, an investment firm that owns several other security companies, such as Entrust and Tripwire. IBM ceased production of its Proventia product, but stated that it will enter the NGFW market at some point in the future. Sourcefire also announced plans to add NGFW capabilities to its product line, which had previously been dominated by IPS offerings. Gartner believes that 2012 will bring some additional acquisition activity, as larger vendors that are trying to compete in the network infrastructure markets against Cisco look to add network security products to their portfolios.

The firewall market remains a large market, with firewall/VPN revenue of approximately \$5.9 billion in 2010, an approximate 10% increase over the \$5.4 billion of 2009. Gartner estimates that total 2011 firewall revenue will be approximately \$6.3 billion. Most firewall vendors saw strong revenue growth over this period, as delayed firewall refresh from previous pent-up demand, and increased use of video and social networking drove up network bandwidth demands. As NGFW capabilities have dominated feature comparisons (as shown by Palo Alto Networks' rapid growth), price pressure has been reduced to some degree. However, the trends we identified last year of cloud and virtualization still continue to impact the market. Gartner saw increased demand for software-only versions of firewalls for use inside virtualized data centers, but most of this demand was directed toward incumbent firewall vendors. We do not see openings for virtual-only firewall vendors.

As NGFW products become more widely used, focus will shift toward manageability and scalability — until the next threat wave. 2012 will be the year most mainstream firewall vendors catch up to the smaller innovative vendors in feature count. The innovative vendors must show that they have the same management tools, as well as third-party ecosystem support and scale, as the larger vendors. Enterprises should continue to focus on threat-facing capabilities, throughput and manageability as key evaluation criteria for firewalls, with technical criteria typically weighted two times to three times cost criteria.

Firewall policy management (FPM) products (see Note 1) are a distinct, adjacent market. Gartner recommends FPM tools be considered where the complexity of the environment exceeds the firewall console capability, where the firewall rule base is exceptionally large or dynamic, where there is more than one brand of firewall in use, if a complex transition to another brand of firewall is planned, or if workflow tools are required as part of firewall rule management.

The Strategic Planning Assumptions for the enterprise firewall market are:

Virtualized versions of enterprise network safeguards will not exceed 2% of the market through 2012, or 20% through 2016.

Through 2015, more than 75% of enterprises will continue to seek security from a vendor different from their infrastructure vendor.

Less than 5% of Internet connections today are secured using NGFWs. By year-end 2014, this will rise to 35% of the installed base, with 60% of new purchases being NGFWs.

[Return to Top](#)

## MARKET DEFINITION/DESCRIPTION

The enterprise network firewall market represented by this Magic Quadrant is composed primarily of purpose-built appliances for securing corporate networks. Products must be able to support single enterprise firewall deployments and large deployments, including branch offices. These products are accompanied by highly scalable management and reporting consoles and products.

As the firewall market evolves from stateful firewalls to NGFWs, other security functions (such as network IPSs) and full-stack inspection, including applications, will also be provided within an NGFW.

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.

## EVALUATION CRITERIA DEFINITIONS

### Ability to Execute

**Product/Service:** Core goods and services offered by the vendor that compete in/serve the defined market. This includes current product/service capabilities, quality, feature sets and skills, whether offered natively or through OEM agreements/partnerships, as defined in the market definition and detailed in the subcriteria.

**Overall Viability (Business Unit, Financial, Strategy, Organization):** Viability includes an assessment of the overall organization's financial health, the financial and practical success of the business unit, and the likelihood of the individual business unit to continue investing in the product, to continue offering the product and to advance the state of the art within the organization's portfolio of products.

**Sales Execution/Pricing:** The vendor's capabilities in all presales activities and the structure that supports them. This includes deal management, pricing and negotiation, presales support and the overall effectiveness of the sales channel.

**Market Responsiveness and Track Record:** Ability to respond, change direction, be flexible and achieve competitive success as opportunities develop, competitors act, customer needs evolve and market dynamics change. This criterion also considers the vendor's history of responsiveness.

**Marketing Execution:** The clarity, quality, creativity and efficacy of programs designed to deliver the organization's message in order to influence the market, promote the brand and business, increase awareness of the products, and establish a positive identification with the product/brand and organization in the minds of buyers. This "mind share" can be driven by a combination of publicity, promotional, thought leadership, word-of-mouth and sales activities.

**Customer Experience:** Relationships, products and services/programs that enable clients to be successful with the products evaluated. Specifically, this includes the ways customers receive technical support or account support. This can also include ancillary tools, customer support programs (and the quality thereof), availability of user groups and SLA.

**Operations:** The ability of the organization to meet its goals and commitments. Factors include the quality of the organizational structure, including skills, experiences, programs, systems and other vehicles that enable the organization to operate effectively and efficiently on an ongoing basis.

### Completeness of Vision

**Market Understanding:** Ability of the vendor to understand buyers' wants and needs and to translate those into products and services. Vendors that show the highest degree of vision listen and understand buyers' wants and needs, and can shape or enhance those with their added vision.

**Marketing Strategy:** A clear, differentiated set of messages consistently communicated throughout the organization and externalized through the website, advertising, customer programs and positioning statements.

**Sales Strategy:** The strategy for selling products that uses the appropriate network of direct and indirect sales, marketing, service and communication affiliates that extend the scope and depth of market reach, skills, expertise, technologies, services and the customer base.

**Offering (Product) Strategy:** The vendor's approach to product development and delivery that emphasizes differentiation, functionality, methodology and feature set as they map to current and future requirements.

**Business Model:** The soundness and logic of the vendor's underlying business proposition.

**Vertical/Industry Strategy:** The vendor's strategy to direct resources, skills and offerings to meet the specific needs of individual market segments, including verticals.

**Innovation:** Direct, related, complementary and

The NGFW market will eventually subsume the majority of the stand-alone network IPS appliance market at the enterprise edge. This will not be immediate, however, because many enterprise firewall vendors have IPSs within their firewall products that are competitive with stand-alone IPS appliances, and are resisting truly integrating the functions and instead colocate them within the appliance. Although firewall/VPN and IPS are converging (and sometimes URL filtering), other security products are not. All-in-one or unified threat management (UTM) products are suitable for SMBs but *not* for the enterprise: Gartner forecasts that this separation will continue until at least 2015. Branch office firewalls are becoming specialized products, diverging from the SMB products.

As part of increasing the effectiveness and efficiency of firewalls, firewalls will need to add more blocking capability as part of the base product, to go beyond port/protocol identification and to move toward a service view of traffic.

Gartner has successively increased the Magic Quadrant evaluation weighting for NGFW features. This edition reflects a significant increase in the weighting of NGFW capabilities reflecting the changing markets and enterprise needs.

[Return to Top](#)

## Inclusion and Exclusion Criteria

### Inclusion Criteria

Network firewall companies that meet the market definition and description were considered for this report under the following conditions:

Gartner analysts assess that the company has an ability to effectively compete in the enterprise firewall market.

Gartner clients generate inquiries about the company.

The company regularly appears on shortlists for selection and purchases.

The company demonstrates a competitive presence in enterprises and sales.

Gartner analysts consider that aspects of the company's product execution and vision merit inclusion.

The vendor has achieved enterprise firewall product sales (not including maintenance) in the past calendar year of more than \$10 million and within a customer segment that is visible to Gartner.

### Exclusion Criteria

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

The company did not meet the inclusion criteria.

The company has minimal or negligible apparent market share among Gartner clients, or is not actively shipping products.

The company is not the original manufacturer of the firewall product. That includes hardware OEMs, resellers that repackage products that would qualify from their original manufacturers, as well as carriers and Internet service providers (ISPs) that provide managed services. We assess the breadth of OEM partners as part of the evaluation of the firewall, and do not rate platform providers separately.

The company's products sell as network firewalls, but do not have the capabilities, scalability and ability to directly compete with the larger firewall product/function view. Products that are suited for SMBs, such as UTM firewalls or those for small office/home office placements, are not targeted at the market this Magic Quadrant covers (enterprise) and are excluded.

The company has primarily a network IPS with a non-enterprise-class firewall.

The company has personal firewalls, host-based firewalls, host-based IPSs and Web application firewalls — all of which are distinctly separate markets.

Stand-alone network IPS appliances are a distinct market and are covered in Gartner's Magic Quadrant for Network Intrusion Prevention Systems.

[Return to Top](#)

### ADDED

No vendors were added.

[Return to Top](#)

### DROPPED

No vendors were dropped; however, name changes did occur. The 3Com/H3C entry has been renamed to HP. Astaro has been renamed to Sophos, and phion has been renamed to Barracuda Networks, to represent the acquiring companies. Gartner examined several vendors that did not meet the inclusion criteria, or were nonresponsive and did not have any significant visibility within the market. Sourcefire was not shipping a firewall at the time of the analysis of this report.

[Return to Top](#)

synergistic layouts of resources, expertise or capital for investment, consolidation, defensive or pre-emptive purposes.

**Geographic Strategy:** The vendor's strategy to direct resources, skills and offerings to meet the specific needs of geographies outside the "home" or native geography, either directly or through partners, channels and subsidiaries, as appropriate for that geography and market.

## Evaluation Criteria

### ABILITY TO EXECUTE

*Product or service:* This includes service and customer satisfaction in enterprise firewall deployments. Execution 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 products are successfully and continuously deployed in enterprises, and the company wins a large percentage in competition with other vendors. Companies that execute strongly generate pervasive awareness and loyalty among Gartner clients, and generate 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 quality of product and service is foremost over revenue. Key features are weighted heavily, such as foundation firewall functions, console quality, low latency, range of models, secondary product capabilities (logging, event management, compliance, rule optimization and workflow), and being able to support complex deployments and modern demilitarized zones. Having a low rate of vulnerabilities in the firewall is important. Logistical capabilities for managing appliance delivery, product service and port density matters. Support is rated on quality, breadth and value of offerings through the specific lens of enterprise needs.

*Overall viability:* Overall business viability includes overall financial health, prospects for continuing operations, company history, and demonstrated commitment in the firewall and 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 firewall revenue, competitive wins versus key competitors (which is compared to Gartner data on such competitions held by our customers), and devices in deployment. The number of firewalls shipped or the market share is not the key measure of execution. Instead, we consider use of these firewalls to protect the key business systems of enterprise clients and presence on competitive shortlists.

*Sales execution/pricing:* We evaluate the company's pricing, deal size, installed base and use by enterprises, carriers and MSSPs. This includes the strength of the vendor's sales and distribution operations. Pre- and post-sales support is evaluated. Pricing is compared in terms of a typical enterprise-class deployment, including the cost of all hardware, support, maintenance and installation. Low pricing will not guarantee high execution or client interest. Buyers want good results more than they want bargains. Cost of ownership over a typical firewall life cycle (three to five years) was assessed, as was the pricing model for (1) conducting a refresh while staying with the same product and (2) replacing a competing product without intolerable costs or interruptions. The robustness of the enterprise channel and third-party ecosystem is important.

*Market responsiveness and track record:* This evaluates the vendor's ability to respond to changes in the threat environment, and to present solutions that meet customer protection needs rather than packaging up fear, uncertainty and doubt. This criterion also considers the provider's history of responsiveness to changes in the firewall market and how enterprises deploy network security.

*Market execution:* Competitive visibility is a key factor, including which vendors are most commonly considered top competitive solutions, during the RFP and selection process, and which are considered top threats by each other. In addition to buyer and analyst feedback, this ranking looks at which vendors consider each other to be direct competitive threats, such as driving the market on innovative features copackaged within the firewall, or offering innovative pricing or support offerings. An NGFW capability is heavily weighted, as are enterprise-class capabilities, such as multidevice management, virtualization, adaptability of configuration and support for enterprise environments. Unacceptable device failure rates, vulnerabilities, poor performance and the inability of a product to survive to the end of a typical firewall life span are assessed accordingly. Significant weighting is given to delivering new platforms for scalable performance in order to maintain investment, and to the range of models to support various deployment architectures.

*Customer experience and operations:* This includes management experience and track record, as well as the 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, throughput of the IPS capability and how the firewall fared under attack conditions are also important. Succeeding in complex networks with little intervention (for example, one-off patches) is highly considered.

**Table 1.** Ability to Execute Evaluation Criteria

Evaluation Criteria	Weighting
Product/Service	Standard
Overall Viability (Business Unit, Financial, Strategy, Organization)	Standard
Sales Execution/Pricing	Standard
Market Responsiveness and Track Record	Standard
Marketing Execution	Standard
Customer Experience	Standard
Operations	Standard

Source: Gartner (December 2011)

**COMPLETENESS OF VISION**

*Market understanding and strategy:* This includes providing a track record of delivering on innovation that precedes customer demand rather than an "us too" road map. We also evaluate the vendor's overall understanding and commitment to the security and network security markets. Gartner makes this assessment subjectively by several means, including interaction with vendors in briefings and feedback from Gartner customers on information they receive concerning road maps. Incumbent vendor market performance is reviewed year by 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 the market directions will change. Understanding and delivering on enterprise firewall realities and needs are important, and having a viable and progressive road map and delivery of NGFW is weighted very highly. The NGFW capabilities are expected to be integrated both to achieve improved correlation and functional improvement.

*Sales strategy:* Sales strategy includes pre- and post-product support, value for pricing, and providing clear explanations and recommendations for detection events. Building loyalty through credibility with full-time enterprise firewall staff demonstrates the ability to assess the next generation of requirements. Vendors need to address the network security buying center correctly, and to do so in a technically direct manner, rather than selling just fear or next-generation hype. Channel and third-party security product ecosystem strategies matter insofar as they are focused on enterprises.

*Offering strategy:* This criterion focuses on a vendor's product road map, current features, NGFW integration, virtualization and performance. Credible independent third-party certifications include the Common Criteria for Information Technology Security Evaluation. Integrating with other security components is also weighted, as well as product integration into other IT systems. We also evaluate how the vendor understands and serves the enterprise branch office. Innovation such as introducing practical new forms of intelligence that the firewall can apply policy to are highly rated.

*Business model:* This includes the process and success rate for developing new features and innovation, and R&D spending.

*Vertical, industry and geographic strategy:* This includes the ability and commitment to service geographies and vertical markets, such as complex enterprise international deployments, MSSPs, carriers or governments.

*Innovation:* This includes R&D and quality differentiators, such as:

- Performance, which includes low latency, new firewall mechanisms and achieving high IPS throughput and low appliance latency

- Firewall virtualization and securing virtualized environments

- Integration with other security products

- Management interface and clarity of reporting — the more a product mirrors the workflow of the enterprise operation scenario, the better the vision

- "Gives back time" to firewall administrators by innovating to make complex tasks easier, rather than adding more alerts and complexity

Products that are not intuitive in deployments or operations are difficult to configure or have limited reporting, and they are scored accordingly.

The more a product mirrors the workflow of the enterprise operation scenario, the better the vision. Products that are not intuitive in deployment, or operations that are difficult to configure or have limited reporting, are scored accordingly. Solving customer problems is a key element of this category. Reducing the rule base, offering interproduct support and leading competitors on features are foremost.

**Table 2. Completeness of Vision Evaluation Criteria**

Evaluation Criteria	Weighting
Market Understanding	Standard
Marketing Strategy	Standard
Sales Strategy	Standard
Offering (Product) Strategy	Standard
Business Model	Standard
Vertical/Industry Strategy	Standard
Innovation	Standard
Geographic Strategy	Standard

Source: Gartner (December 2011)

**Leaders**

The Leaders quadrant contains a mix of large and midsize vendors, with the common element of making products that are built for enterprise requirements. These requirements include a wide range

of models, support for virtualization and virtual LANs, and a management and reporting capability that is designed for complex and high-volume environments, such as multitier administration and rules/policy minimization. An NGFW capability is an important element as enterprises move away from having dedicated IPS appliances at their perimeter and remote locations. Vendors in this quadrant lead the market in offering new safeguarding features, providing expert capability, rather than treating the firewall as a commodity, and having a good track record of avoiding vulnerabilities in their security products. Common characteristics include handling the highest throughput with minimal performance loss and options for hardware acceleration.

[Return to Top](#)

## Challengers

The Challengers quadrant contains vendors that have achieved a sound customer base, but they are not leading with features. Many Challengers are slow to work toward or do not plan for an NGFW capability, or they have other security products that are successful in the enterprise and are counting on the relationship, rather than the product, to win deals. Challenger products are often well-priced and, because of their strength in execution, vendors can offer economic security product bundles that others cannot. Many Challengers hold themselves back from becoming leaders because they are obligated to place security or firewall products as a lower priority in their overall product sets. Firewall market challengers will often have significant market share but trail smaller market share leaders in the release of features.

[Return to Top](#)

## Visionaries

Visionaries have the right designs and features for the enterprise, but they lack the sales base, strategy or financial means to compete with leaders and challengers. Most visionary products have a good NGFW capability but lack the performance capability and support network. Savings and high-touch support can be achieved for organizations willing to update products more frequently and switch vendors if required. Where firewalling is a competitive element for an enterprise, visionary vendors are good shortlist candidates. There are no Visionaries in this edition. Vendors that did not have NGFW capabilities are adding them in a defensive move, while those with strong NGFW offerings focused on manageability and usability. Gartner expects the next wave of innovation in this market to focus on better identification of malicious protocols at multi-Gbps rates.

[Return to Top](#)

## Niche Players

Most vendors in the Niche Players quadrant are smaller vendors of enterprise firewalls, makers of multifunction firewalls for SMBs, or branch-office-only product makers attempting to break into the enterprise market. Many Niche Players are making larger SMB products, with the mistaken hope that this will satisfy enterprises. Some enterprises that have the firewall needs of an SMB (for example, some Type C "risk-averse" enterprises) may consider niche products, although other models from Leaders and Challengers may be more suited. If local geographic support is a critical factor, then Niche Players can be shortlisted.

[Return to Top](#)

## Vendor Strengths and Cautions

### BARRACUDA NETWORKS

Barracuda Networks ([www.barracudanetworks.com](http://www.barracudanetworks.com)) acquired European firewall vendor phion in 2009. Barracuda has been primarily focused on selling to the low end of the midsize enterprise market at very aggressive price points. The former phion firewall is now branded as the Barracuda NG Firewall family across a range of appliances and a virtual version. Barracuda is assessed as a Niche Player for enterprises, mostly because it serves a set of placements well, usually in portions of EMEA or when the Leaders are otherwise not welcome. We do not see the Barracuda NG Firewall frequently displacing Leaders otherwise.

#### Strengths

The Barracuda NG Firewall is a good option for Barracuda customers who want to get a firewall product from the same vendor, especially those organizations that are outgrowing their current UTM and/or moving into point products.

The Barracuda NG Firewall unit support staff offer good local language support, especially in Germany, Switzerland and Austria.

Often, users comment that VPN tunnel setup was very easy and that they like the central management features.

#### Cautions

Barracuda customers are primarily SMBs that do not yet have well-established enterprise network security channels.

No vendor we surveyed listed Barracuda as a significant enterprise competitive threat.

Barracuda has not been seen competing in the NGFW shortlists of Gartner customers because of low visibility outside Europe.

Some users have commented that the initial setup can be more complex than needed, and that

the availability of training is limited when compared with competitors.

[Return to Top](#)

## CHECK POINT SOFTWARE TECHNOLOGIES

Check Point Software Technologies (see [www.checkpoint.com](http://www.checkpoint.com)) is a well-known, pure-play security company with the second largest firewall installed base (when support is included), and strong and broad channel support. Check Point has continued to expand its software "blade" strategy (that is, preloaded software modules enabled through subscription keys), as introduced in version R70. Check Point has recently undertaken a period of considerable product feature enhancement, and has introduced new blades and new performance levels. Gartner views this as a response to the significant threat posed by Palo Alto Networks. The indirect result of this R&D by Check Point has been significantly increased competitiveness versus other firewall competitors, such as Cisco and Juniper Networks.

The majority of enterprises choose to use Check Point-branded appliances, although options are also available for a software install on self-sourced servers, a virtual machine install (Secure Gateway Virtual Edition [VE]), or the remaining partners, such as Crossbeam. Check Point firewalls are essentially divided into three classes listed in increasing performance: UTM-1 for SMB or branch, the IP line legacy from the Nokia acquisition, and the high-end Power-1 appliance line. Check Point has not yet blended the IPSO and SmartCenter on Secure Platform OSs into a single OS under the announced Project Gaia. With the Direct Support option, customers can now receive all support directly from the company. Check Point is assessed as a leader for enterprises, because we continuously see the vendor competing and winning in demanding selections, following an NGFW development path that customers are asking for, and displacing competitors based on its features and channel strength.

### Strengths

Check Point scored high as a significant enterprise competitive threat by all vendors Gartner surveyed.

Check Point firewall management capabilities are valued highly by customers with a large number of firewalls with differing configurations. Check Point firewalls are most often seen in large and complex networks because of the capabilities of the SmartCenter management platform. Check Point usually scores the highest in console quality for selections that Gartner observes. Check Point has invested and continues to invest considerable intellectual property into the management console, in recognition of the importance configuration has to administrators in enterprise deployments. Provider-1 users we surveyed generally report a high level of satisfaction. Gartner sees premium-support-level customers, especially at the Diamond level, renewing their support at those same levels in recognition of the customized and easy access to support.

Check Point has a strong field of product options, such as VSX for virtualized firewalling, VE for running in virtualized environments, and its Eventia correlation product. SecurePlatform allows for a loading of the firewall, along with a hardened OS onto off-the-shelf server hardware. The wide availability of appliance and software options enables Check Point to meet the requirements for complex enterprise networks. Blade pricing has been priced less when compared with stand-alone or point solutions, especially IPS. The R75 release had a significant number of features and improvements, which increased competitive pressure significantly across the firewall market. Check Point has raised the quality of the IPS in the product significantly over that of SmartDefense and IPS-1, and performed favorably on third-party IPS testing by NSS Labs.

Check Point has good capability for servicing large enterprises with the combination of its Power-1 appliance line, having a VMware-certified version (VPN-1 VE) and VPN-1 UTM running in a container on ESX.

Check Point has the strongest third-party ecosystem of security products that integrate easily with Check Point's management platform.

### Cautions

High price is a common reason provided by Gartner customers for replacing or considering replacing Check Point firewalls. This is not an issue where a premium firewall function is required and justifies the investment. In firewall selections and support renewals, Gartner often hears that support pricing is complex, and price negotiations are difficult.

The Check Point Software Blade architecture has short-term attractiveness, but is a difficult long-term strategy option for enterprises. Enterprises are cautious about adding new functions to firewalls. With more than 13 blades now available, charging for features that are included by competitors is challenging. The Check Point 3D Security messaging is too abstract and does not align with or resonate with the firewall-buying market.

The vendor remains challenged in producing competitive network security products outside the firewall market.

Project Gaia has not yet been delivered (it is in beta with selected customers), meaning many clients must maintain two Check Point OSs and the associated complexity in licensing. Provider-1, which is popular with larger customers, has not been notably advanced or marketed.

[Return to Top](#)

## CISCO

Cisco (see [www.cisco.com](http://www.cisco.com)) has an exceptionally broad network security product portfolio. It has

strong product offerings across the network security, Web security and email security tiers. Although not outwardly visible to most customers, Cisco is going through a period of significant change in its firewall offerings. Cisco has continued to consolidate its security products into a single business unit, and Gartner believes Cisco has had a significant effort under way to develop an NGFW product (and accompanying appliances) as a successor to the Adaptive Security Appliance (ASA) firewall. Gartner believes that Cisco is in a strong position to launch data-center-specific security offerings, should Cisco choose to make this a key strategy. Cisco firewalls have not seen any noteworthy changes this year. An exception is that Cisco introduced new high-end models this year, including the 5585-X, which has been well-accepted by incumbent Cisco firewall users. Cisco is assessed as a Challenger for enterprises over the evaluation period, because we did not see it frequently displacing Leaders based on vision or feature, and it does not compete in the NGFW field. Instead, Cisco mostly wins competitive procurements through sales/channel execution or aggressive discounting for large Cisco networks when firewall features are not highly weighted evaluation criteria. ASA is available in four editions, which clearly define what safeguards are being purchased.

### Strengths

Cisco has significant market share in security (including having the largest market share for firewall appliances), has wide geographic support and is viewed as a significant (second-highest) enterprise competitive threat by the vendors we surveyed.

Gartner clients consistently rate the Cisco support network as excellent, and the most often cited reason for selecting or staying with Cisco security products. The vendor has strong channels, broad geographic support and the availability of other security products.

Its ASA has the option to add an IPS module (AIP-SSM) to replace a stand-alone IPS.

Cisco offers a wide choice in firewall platforms. The primary offering is the stand-alone firewall ASA, with firewalls also available via the Firewall Services Module blade for Catalyst switches, and on Cisco's Internetwork Operating System (IOS)-based Integrated Services Router.

The integration of reputation features across Cisco security products is a highly significant feature differentiator that is often missed in enterprise selections. Although many companies have reputation features, the breadth of the reputation feed is a critical quality factor.

### Cautions

Cisco firewall products are selected more often when security offerings are added to Cisco's infrastructure, rather than when there is a shortlist with competing firewall appliances. Cisco was listed by competitors as the product they most often replace.

Where Cisco firewalls were shortlisted, but not selected, the difficulty of using the management console, Cisco Security Manager (CSM), for basic configuration and management was consistently the factor most often cited.

The requirement to add a hardware module (the AIP-SSM) to add IPS capability to the ASA firewall appliance remains a barrier to deployment and a competitive disadvantage for branch-office deployments. The add-in module does, however, provide processing help with the deep inspection load. If the SSM module is used for IPS, then it cannot be used for other content inspection.

The ASA line is becoming somewhat dated, although Gartner expects Cisco to ship new models and software in 2012.

[Return to Top](#)

## FORTINET

California-based Fortinet (see [www.fortinet.com](http://www.fortinet.com)) has long focused on using purpose-built hardware to produce UTM appliances at strong price/performance points. Although the firewall features in its UTM products met most of the needs of firewall-focused large enterprise buyers, Fortinet's approach and philosophy continue to be focused on "everything in one box," which has caused its brand and channel support to be slow to evolve from its SMB base. However, Fortinet continues to make progress within the Gartner customer base, usually by expanding out from branch-office or retail deployments, and is seen winning some data center implementations. Fortinet is a significant threat to competitors in this market because of the company's hardware expertise, competitive pricing and steady revenue growth. Fortinet is a viable shortlist contender for most of the enterprise firewall market. It is assessed as a Challenger mostly because we see it displacing competitors on value and performance, but not often beating Leaders in mainstream enterprise selections. Fortinet has steadily been expanding its support offerings to be better aligned to the enterprise, including options for dedicated technical account managers.

### Strengths

Fortinet continues to get positive reviews for the delivery of new features and products, and clients report easy deployments. Fortinet has a large R&D team and uses this to outmaneuver competitors that often rely on OEM arrangements. This has enabled Fortinet to maintain road map agility, get to market quickly with both a new feature and one that is fully console-integrated, and better integrate features and avoid the pitfalls of partners that are acquired or change direction. This also has enabled Fortinet to expand its portfolio of nonfirewall network security offerings, which provides increasing cross-selling opportunities.

Fortinet continues to increase its wins against the larger firewall incumbents, and it gained additional footholds in emerging areas, such as in-the-cloud firewalls and with carriers/ISPs where high-end performance is required. Fortinet is price-competitive, especially when using multiple virtual domains, and appliance reliability is reported as very high. Fortinet has invested substantially in obtaining and completing certifications and testing suites (Common Criteria, Federal Information Processing Standard [FIPS], NSS Labs and ICSA Labs) that are appealing to

a wide array of customers.

Its firewalls have high-end performance from purpose-built hardware and a wide model range (more than 20 appliance models), including bladed appliances for large enterprises and carriers, as well as SMB and branch office solutions. Although many competitors are increasing their reliance on Intel for their future performance gains, Fortinet (much as in its software development) maintains control of its own dual processors — one application-specific integrated circuit (ASIC) for network security operations and the second for content inspection. The Advanced Mezzanine Card (AMC) expansion slot options for the enterprise-class models include an onboard security ASIC with additional ports or a hard drive providing investment preservation without having to resort to only appliance replacement, like many competitors. The AMC port options also minimize appliance replacement by being able to upgrade without replacing the whole box.

### Cautions

Where Fortinet was shortlisted but not selected in enterprises, the management capabilities were most often listed as the reason. However, where aggressive console use is not required, or where multiple firewalls share the same policy, the Fortinet console is highly competitive.

Post-sales service and support do not win Fortinet selections over competitors; however, support and enterprise sales have been steadily improving in the enterprise, especially for premium-level support.

Fortinet does not have a dedicated NGFW, but instead presents its UTM product, expecting a subset to be used. Fortinet's marketing that is focused on using UTM for enterprises undervalues Fortinet's enterprise offerings and steers away larger customers. Fortinet has historically defined enterprises as 500 users — about half the number used by Gartner and competitors. The UTM messaging also has enterprises excluding Fortinet from NGFW shortlists, even when the necessary capabilities (such as application control) are present.

Fortinet does not have a strong third-party security vendor ecosystem compared with the major enterprise firewall incumbents.

### [Return to Top](#)

## HP

Acquired in 2009 as part of HP's acquisition of 3Com, China-based H3C was formed as a joint partnership between Huawei and 3Com, and has been shipping firewalls since 2003. Now as part of HP (see [www.hp.com](http://www.hp.com)), it is leveraging this technology mostly in its current customer base. The HP F5000 and F1000, also called the A Series Firewalls, will be of most interest to China-based enterprises, especially where other H3C, 3Com or Huawei networking equipment is used. An add-in module for switches, the HP Threat Management Services zl module, is also available for the HP E5400 zl and E8200 zl series switches. HP is assessed as a Niche Player vendor primarily because of its geographic sales and presence, and the current absence of NGFW features, such as IPS and application control.

### Strengths

HP and legacy H3C have a strong regional presence in China and the Asia/Pacific region, and sales are increasing for incumbent HP networking customers.

There is a wide range of models (including a high-throughput, blade-based chassis), branch office models and enterprise models, all with a flat-fee URL model.

It has broad IPv6 support.

### Cautions

The former SecPath firewalls are not visible outside the Asia/Pacific region and have to address concerns from many geographies about relying on technology developed in China.

The firewall lacks certifications and third-party testing, such as Common Criteria for Information Technology Security Evaluation, which is usually seen in enterprise contenders.

HP's corporate changes, which include four CEOs in 13 months. The inclusion of the network security business in a software division continues to show that HP does not yet have a coherent network security strategy.

### [Return to Top](#)

## JUNIPER NETWORKS

Gartner sees Juniper Networks' firewalls (see [www.juniper.net/us/en](http://www.juniper.net/us/en)) mostly selected as an adjunct to the network infrastructure business by enterprises that are already Juniper customers. The move to Junos from ScreenOS and the SRX model line have been the most significant changes in the Juniper firewalls. Juniper also introduced AppSecure for application control and visibility. Juniper is assessed as a Challenger for enterprises, because we see Juniper selected in concert with other Juniper offerings, rather than displacing competitors based on its vision or features. During the evaluation period, Juniper appeared to focus more on other areas of its business and did not make significant advances with its firewall products. Juniper is, however, often shortlisted and/or selected in carrier, service provider and data center deployments, primarily because of price and high throughput on its largest appliances.

### Strengths

Appliance performance and range of models were most often listed by users as what they like about Juniper firewalls. Clients often comment on its positive performance and the reliability of

its products, including responsiveness of support, and the global support channel.

Good options exist for high-throughput, purpose-built appliances, especially in the higher-end SRX models, and Juniper expresses a clear road map for firewall and security customers. Juniper has shown development and security discipline in keeping the rate of vulnerabilities in the product low.

Juniper has strong branch office firewalls, complementing the enterprise products. Its branch-office firewalls include WAN optimization controller and an Avaya voice gateway.

Having routing in the firewall is of interest to a very narrow segment of customers.

### Cautions

Problems using Juniper's Network and Security Manager to manage SRX products were the most common criticism by Gartner clients since the last version of this Magic Quadrant. Secure Design is the planned new management product to replace Network and Security Manager.

As a network infrastructure vendor, Juniper is at a disadvantage selling into Cisco networks, where buying any Juniper security equipment can be resisted as a Cisco network equipment replacement.

Like most competitors, integration between IPS and the firewall is limited, and Juniper is rarely considered by customers looking for an NGFW.

During the evaluation period, Gartner observed an increase in complaints about Juniper firewall support — usually related to resolving complex configurations.

[Return to Top](#)

### MCAFEE

McAfee (see [www.mcafee.com/us](http://www.mcafee.com/us)) was acquired by Intel in early 2011 (see "Making Sense of Intel's Acquisition of McAfee"). It obtained its firewall products through the acquisition of Secure Computing in late 2008. The Sidewinder product has been renamed to the McAfee Firewall Enterprise (MFE). There are seven product models and a virtualized version. The MFE is certified for use on Crossbeam X Series blades and Riverbed Steelhead appliances. Application control has been added under the AppPrism feature name in v.8.0. Users report improvements in the firewall console quality under McAfee.

The road map for MFE is more important for consideration than the current features in the product. A re-engineered MFE integrated with the McAfee IPS on a purpose-built hardware platform will be the milestone for which to watch and a road map toward an NGFW. McAfee is assessed as a Challenger for enterprises, because we do not see it continuously displacing Leaders based on vision or feature, but instead through sales execution or value.

### Strengths

The TrustedSource feature blocks known bad IP addresses (from a dynamically updated list source) from connecting to the firewall, and is a significant differentiating feature. Although many companies have reputation features, the breadth of the reputation feed is a critical quality factor. The vendor's integration of reputation services across network, Web and email security product lines provides a strong cross-selling opportunity. The larger McAfee sales and channels have already increased MFE's presence in the market, while changes to the product are under way.

The McAfee Firewall Profiler provides guidance on firewall configuration and is included with the product. MFE has identity and geolocation options.

The Sidewinder firewall had a reputation for high security, making the MFE popular with some government-sector customers.

McAfee has more network security products across multiple markets than almost any competitor. The prospect of integrating these products represents potential "glue" between silo products, which few competitors can promise.

### Cautions

The Intel acquisition presents a significant risk of distraction for the McAfee network security unit. Although an arm's-length relationship has been established, other acquisitions of network security products by nonsecurity or non-network companies have been generally unsuccessful. Intel already collaborates and supports many other network security vendors that compete with McAfee, putting in place a potential conflict.

The McAfee IntruShield IPS engine, available in the stand-alone IPS appliances, is not yet integrated into the MFE. The current MFE IPS capabilities are not very competitive with leading NGFW vendors, especially for configuration and performance.

McAfee has a small range of models and models that are generally not suitable for the high end or data center deployments. The MFE has been primarily available on general-purpose servers, which is met with skepticism by network operations buying centers. McAfee is transitioning to purpose-built hardware, with the likely eventual goal of merging the MFE onto the McAfee IPS hardware, which is highly competitive.

MFE is rarely seen on Gartner client firewall shortlists; however, when it is, the time taken to navigate the general McAfee support system is the most often listed criticism heard from Gartner clients during the selection process.

[Return to Top](#)

## NETASQ

NETASQ (see [www.netasq.com](http://www.netasq.com)) has been a pure-play network security vendor headquartered in France for more than a decade, selling firewalls, vulnerability management and messaging security gateways. NETASQ products mostly appeal to midsize companies and EU-based enterprises. All NETASQ firewall products are in two product lines. The U Series has eight models, and two appliances in the enterprise-labeled NG line. Virtual versions are also available in the V line. NETASQ is assessed as a Niche Player for enterprises, mostly because it best serves SMBs, and agencies in portions of EMEA or when the Leaders or Challengers do not have the usual advantages.

### Strengths

By not using traditional signatures and, instead, focusing on heuristics, NETASQ has innovated on an IPS path that is different from mainstream UTM vendors, which has positioned it more uniquely for countering new kinds of attacks. Users report that they like its policy-based management and real-time policy warning.

It is VPN-certified for "EU restraint" use in the EU, which is of interest to governments and agencies looking for simpler procurement.

NETASQ gets good marks from midsize enterprises for features and ease of use, and has good channel support in EMEA.

NETASQ users comment to Gartner that the branded training and EU support are very good.

### Cautions

The majority of NETASQ's penetration, visibility and channel is focused in EMEA, especially France.

Although having a good feature set, NETASQ has not been part of NGFW selections as seen by Gartner because of the company's low visibility outside France.

Some users have commented to Gartner that managing large numbers of devices and VPN configurations is difficult within the interface.

[Return to Top](#)

## PALO ALTO NETWORKS

Palo Alto Networks (see [www.paloaltonetworks.com](http://www.paloaltonetworks.com)) has been selling enterprise firewalls for four years. A privately held company, Palo Alto Networks has been a significant disruptive influence in the firewall market during the evaluation period. This disruption was a result of focusing on replacing incumbent firewalls by closely integrating firewalls and IPSs of high quality, while adding application identification and inspection to meet emerging needs, all in a unified and tightly integrated engine. The company founder and CTO also has credibility as a co-inventor of the stateful firewall, and part of the founding team of a leading competitor, Check Point Software Technologies. Palo Alto Networks started in the market with behind the firewall placements to add application control; however, almost all deployments Gartner sees are firewall replacements.

Palo Alto Networks' high-performance NGFW functionality continues to drive competitors to react in the firewall market. It is assessed as a Leader mostly because of its NGFW design, redirection of the market along the NGFW path, consistent displacement of Leaders and Challengers, and market disruption forcing Leaders to react. With a unified single-pass inspection engine, rather than a design of passing traffic to submodules, Palo Alto Networks has maintained performance with relatively few models.

### Strengths

Palo Alto Networks continues to demonstrate effective application identification (App-ID), allowing for categorizing, blocking and rate-shaping of applications, particularly within HTTP and HTTPS. In the competitive situations that Gartner observes, Palo Alto Networks usually scores highest for application categorization and ease of configuration in the management console.

Gartner customers report that Palo Alto Networks' appliance performance in most deployments is as advertised in specification sheets, and the management console is improving at a rate faster than competitors.

The firewall and IPS are closely integrated, with App-ID implemented within the firewall and throughout the inspection stream, obviating unnecessary IPS deep inspection or "hairpinning" — inefficiently passing traffic between modules. The IPS rated well in third-party testing by NSS Labs.

Palo Alto Networks generated the most firewall inquiries among Gartner customers in 2010 and 2011 — almost more than all other firewall vendors combined — essentially dominating the enterprise conversation in NGFW. High customer loyalty and satisfaction are observed from early adopters.

### Cautions

The PA series of firewalls does not yet have Common Criteria EAL-4+ for Information Technology Security Evaluation for the firewall; however, EAL-2 certification was recently received.

Palo Alto Networks has a limited number of models when compared with competitors. The company does not have products in adjacent security markets, which would allow for cross-selling opportunities. Fast growth has challenged its support infrastructure, which the company responded to with opening another U.S. support center. The company has room to develop a third-party product support ecosystem.

Opportunistic selling into the secure Web gateway (SWG) and URL-filtering market can confuse some customers that Palo Alto Networks is not a firewall company, or allow it to be considered for UTM selections, for which it will not compete well in (for example, small businesses).

Gartner has heard anecdotal performance issues, with appliances at the highest end, that customers deploy advanced NGFW policies on high-speed heterogeneous traffic.

[Return to Top](#)

## SONICWALL

SonicWALL (see [www.sonicwall.com](http://www.sonicwall.com)) is a California-headquartered security company. In 2010, SonicWALL was acquired by Thoma Bravo, an investment firm that owns other security companies, such as Entrust and Tripwire. Although the majority of SonicWALL's business has been selling UTM to midsize businesses, it has introduced the SuperMassive line, which is squarely aimed at the high end at very competitive price/performance points. Other SonicWALL security products include Secure Sockets Layer (SSL) VPN, email security gateways, clean wireless and backup/recovery offerings. The company's firewall offerings are in four branded lines: SuperMassive, E-Class NSA, NSA and TZ. SonicWALL is assessed as a Niche Player for enterprises, because it serves a set of placements other than classic enterprise firewall deployments well (for example, retail and upper-midsize businesses), and we do not see it often displacing Leaders.

### Strengths

SonicWALL's competitive prices have resulted in strong solutions for wide remote-office deployments (such as in retail outlets) and SMBs.

The company has the reputation and track record of strong channel support. SonicWALL has improved its enterprise go-to-market ability, rather than attempting to push an SMB UTM upmarket, by aligning product lines specifically to the horizontal — SuperMassive for data centers, service providers and ISPs, and the E-Class NSA for enterprises.

The SuperMassive line has achieved market traction in high-end deployments, such as carriers and service providers, where firewall throughput, low latency and price are foremost. Historically, SonicWALL has been more focused on software. This move to hardware engineering has given it credibility in more enterprise selections. These gains are also evident in the performance shown in the E-Class platform using a purpose-built, stream-based deep inspection microprocessor design.

SonicWALL recently enhanced application identification/inspection, under the name Application Intelligence and Control. Performance monitoring by core provides good device capacity management.

The move to private company status after being acquired by Thoma Bravo (see "Thoma Bravo Buy to Boost SonicWALL Stance in Security Market") has allowed SonicWALL the flexibility to plan R&D and hardware engineering efforts that will have longer-term benefits. Greater collaboration with other Thoma Bravo companies could, however, be a future lever to better compete with vendors that have broader product portfolios.

### Cautions

Most of SonicWALL's firewall and other security product lines have been primarily SMB-focused and not competitive in most enterprises. SonicWALL does not yet have a broad enough enterprise channel, support and management console features to be considered in competition with Leaders and become a bigger part of the NGFW conversation.

Gartner rarely sees SonicWALL in most Type A and Type B enterprise firewall selections.

SonicWALL scored low as a significant enterprise competitive threat by the vendors we surveyed, and it has low visibility in the Gartner customer base. Although it has a good NGFW feature set, SonicWALL has not been part of NGFW selections as seen by Gartner. Keeping the NSA brand on the E-Class line has created some customer confusion as to whether the product is an SMB UTM or an enterprise-class firewall.

[Return to Top](#)

## SOPHOS

Acquired by desktop security software vendor Sophos ([www.sophos.com](http://www.sophos.com)) this year (see "Astaro Acquisition Will Extend Sophos' Midmarket Security Offerings"), German firewall vendor Astaro has been shipping firewall products since 2001. Astaro takes a unique approach by leveraging open-source components and focuses primarily on software. Upper midsize businesses (for example, 250 to 999 employees) are most suited to use the Astaro Security Gateway. Gartner believes that Sophos will be the primary go-to-market channel for the Astaro Security Gateway, focusing on current Sophos customers that are starting to outgrow a UTM but do not yet have large enterprise firewall needs. Gartner observes Astaro usually scoring highly where price is the primary factor, Sophos products are already in place, and the throughput requirements are not at the higher end (for example, large enterprises). Sophos is assessed as a Niche Player for enterprises, mostly because it wins over Leaders in some selections based on features or with a very specific channel.

### Strengths

Astaro's leverage and integration of a wide range of open-source components provide an attractive price point. There is no extra charge for the management product, and of great interest, it offers a free basic firewall version for use in VMware.

Users like Astaro's clustering features and price, and ease of installation is reported as a strong point.

The Astaro Security Gateway is available as an appliance or software load, and as a certified Amazon Virtual Private Cloud connector. Astaro now has application control.

Subsequent to the Sophos acquisition, strong growth in its firewall business has been experienced, and Astaro has SWG and email security gateway offerings. Customer satisfaction is generally high, especially with postsale technical support. Deployments in North America have increased.

#### Cautions

The Astaro firewall has limited visibility outside of EMEA and is not often seen in enterprise selections in the Gartner client base. Its UTM focus is less a match for enterprises and better for SMBs. Astaro is short on enterprise features (such as supporting multiple firewall instances in the same appliance) and usually competes with other SMB firewall vendors.

Users would like improved reporting, and the most voiced criticism was the difficulty of use and slow responsiveness of the management interface. The Astaro VPN does not have FIPS 140-2 certification.

Sophos was not listed by any vendor we surveyed as a significant enterprise competitive threat, and has not been highly visible on NGFW shortlists among Gartner clients.

[Return to Top](#)

#### STONESOFT

Headquartered in Finland, Stonesoft (see [www.stonesoft.com](http://www.stonesoft.com)) has been expanding its operations into North America and other geographies, especially Eastern Europe. Stonesoft is focused on network security and has been very innovative in analyzing threat evasion techniques. Introduced in 2011, the Stonesoft NextGen Firewall product is offered across a wide range of appliances. Stonesoft is assessed as a Niche Player for enterprises, because it serves a set of placements well — usually for strong central management or where protection against evasive attacks is key. Stonesoft also provides stand-alone IPS and SSL VPN products. StoneGate v.5.3 introduced application awareness and user identity.

#### Strengths

Stonesoft's threat research concerning evasive attacks has increased security credibility and visibility for the company and products.

It is a security-focused vendor, and has demonstrated very good appliance performance and throughput. This year, Stonesoft introduced the FW-315, a smaller device for branch offices and environments such as process control locations.

Stonesoft offers a virtualized firewall version that is certified for VMware. Both can be run under the Stonesoft Management Center.

It offers support for clustering, very robust high availability and 3G backup connection capability.

Support pricing is slightly lower than the industry average, and it has a loyal customer base.

#### Cautions

Stonesoft has limited market visibility and channel strength outside of EMEA, and it has low visibility within the Gartner customer base, although its firewall and company revenue has increased.

Although Stonesoft NGFW has many next-generation features, it has not been very visible in Gartner client NGFW shortlists.

[Return to Top](#)

#### WATCHGUARD

WatchGuard ([www.watchguard.com](http://www.watchguard.com)) is a Seattle-based network security company that has primarily seen success in selling UTM products to midsize enterprises. Its XTM series of products span performance and feature ranges demanded by large enterprises, but WatchGuard's branding, channel support and management capabilities tend to be more oriented toward smaller businesses. A well-established security-focused company, WatchGuard also has products that include SSL VPN and the XCS SWGs. The XTM-branded firewall models fall into two categories. The XTM 2 Series and XTM 5 Series are UTM, and the XTM 8 Series and the XTM 1050 and 2050 models are targeted for the enterprise. WatchGuard is assessed as a Niche Player for enterprises, because it serves a set of placements other than classic enterprise firewall deployments well, and we do not see it often displacing Leaders.

#### Strengths

WatchGuard's strong price/performance has enabled it to win price-sensitive competitions across retail, branch-office and remote-office deployments.

Users report high satisfaction with the reporting function in the WatchGuard management console. WatchGuard has taken steps to better enter the enterprise arena such as achieving FIPS 140-2 certification for the VPN, and adding application control, and user identity features. Enterprise models are correctly targeted at NGFW, rather than UTM functionality.

It has better-than-market-average integration between the IPS and the firewall, such as having IPS blocks result in subsequent source blocking at the firewall. It has a low rate of product vulnerabilities.

Channel partners and customers rate the company highly. Having a specific management

console for MSSPs is a competitive factor. A software key to unlock appliance performance for some models can minimize appliance downtime when upgrading.

### Cautions

Common Criteria for Information Technology Security Evaluation are not yet in place for all WatchGuard firewalls.

Gartner rarely sees WatchGuard in most Type A and Type B enterprise firewall selections.

WatchGuard scored low as a significant enterprise competitive threat by the vendors we surveyed and has low visibility in the Gartner customer base. Although having a good NGFW feature set, WatchGuard has not been part of NGFW selections as seen by Gartner.

Having the XTM model brand for all appliances has created enterprise customer confusion as to whether the products are suitable for them.

### [Return to Top](#)

---

© 2011 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. or its affiliates. This publication may not be reproduced or distributed in any form without Gartner's prior written permission. The information contained in this publication has been obtained from sources believed to be reliable. Gartner disclaims all warranties as to the accuracy, completeness or adequacy of such information and shall have no liability for errors, omissions or inadequacies in such information. This publication consists of the opinions of Gartner's research organization and should not be construed as statements of fact. The opinions expressed herein are subject to change without notice. Although Gartner research may include a discussion of related legal issues, Gartner does not provide legal advice or services and its research should not be construed or used as such. Gartner is a public company, and its shareholders may include firms and funds that have financial interests in entities covered in Gartner research. Gartner's Board of Directors may include senior managers of these firms or funds. Gartner research is produced independently by its research organization without input or influence from these firms, funds or their managers. For further information on the independence and integrity of Gartner research, see "Guiding Principles on Independence and Objectivity" on its website, [http://www.gartner.com/technology/about/ombudsman/omb\\_guide2.jsp](http://www.gartner.com/technology/about/ombudsman/omb_guide2.jsp).

---

[About Gartner](#) | [Careers](#) | [Newsroom](#) | [Policies](#) | [Site Index](#) | [IT Glossary](#) | [Contact Gartner](#)

---