Magic Quadrant for Network Firewalls

Market Definition/Description

Network firewalls secure traffic bidirectionally across networks. Although these firewalls are primarily deployed as hardware appliances, clients are increasingly deploying virtual appliance firewalls, cloud-native firewalls from infrastructure as a service (IaaS) providers, and firewall as a service (FWaaS) offerings hosted directly by vendors.

Capabilities of network firewalls include:

- Application awareness and control
- Intrusion detection and prevention
- Advanced malware detection
- Logging and reporting

Magic Quadrant

Figure 1: Magic Quadrant for Network Firewalls
Source: Gartner (November 2021)

Vendors Added and Dropped

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

Added

- Alibaba Cloud
- Amazon Web Services
- Cato Networks
- Versa Networks

Dropped

- Stormshield
- Venustech

Inclusion and Exclusion Criteria

The inclusion criteria represent the specific attributes that Gartner analysts considered it necessary for vendors to fulfill in order to be included in this Magic Quadrant.

Vendors of network firewall functions covered by the Market Definition/Description section were considered for evaluation in this Magic Quadrant under the following conditions:

- Vendors had to have a presence at least in three regions, including their home region.
- Vendors offering hardware appliances as a part of their firewall offering must have made at least US$70 million in firewall-only revenue in 2020.
- Vendors only offering firewalls for single use cases must have made at least $20 million in firewall-only revenue.
- Vendors must have a proven track record of fulfilling the cloud security firewall use case.
- Gartner analysts must have assessed that they can compete effectively in the network firewall market.
- Gartner analysts must have determined that they are significant players in the network firewall market, on the basis of market presence, competitive visibility or technological innovation.
- Vendors must have the ability to meet more than one of the firewall deployment use cases mentioned in the Market Definition/Description section.
- Cloud service providers had to have a dedicated firewall offering.

Additionally, vendors had to demonstrate signs of global presence:

- Gartner must have received strong evidence that more than 10% of a vendor's customer base is outside its home region.
- Vendors had to offer 24/7 direct support, including phone support (in some cases, this is an add-on, rather than included in the base service).
- Vendors' appearances in Gartner client inquiries, competitive visibility, client references and local brand visibility were considered to determine eligibility for inclusion.

- Vendors had to provide evidence that they met the above inclusion requirements.

Evaluation Criteria

Ability to Execute

Gartner analysts evaluate vendors on the quality and efficacy of the processes, systems, methods or procedures that enable their performance to be competitive, efficient and effective, and to positively impact revenue, retention and reputation. The following criteria are used to evaluate Ability to Execute.

Product/Service: This includes service for, and customer satisfaction with, network firewall deployments. Strong execution means that a company has demonstrated to Gartner analysts that its products are successfully and continually deployed for emerging use cases and in multiple firewall deployments. 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 vendor's Ability to Execute. Sales are a factor. However, winning in competitive environments through innovation and quality of product and service is more important than revenue. Key features are weighted heavily. These include support for hybrid environments, strong performance, centralized management, advanced threat detection and prevention, and a platform-based approach. Integrated offerings to support different firewall deployment use cases are evaluated. Availability of firewalls across different regions is considered. Support is rated on the quality, breadth and value of offerings in relation to enterprise/cloud needs.

Overall Viability: This includes overall financial health, prospects for continuing operations, company history, and demonstrated commitment to the firewall and security markets. 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, wins against key competitors (which is compared with Gartner data). We consider the use of network firewalls to protect the key business systems of enterprise clients and the frequency of shortlisting by clients.

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

Market Responsiveness and Track Record: The vendor's 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: Competitive visibility is a key factor; it includes which vendors are most commonly considered to have top competitive solutions during the RFP and selection process, and which are considered top threats by other vendors. In addition to buyer and analyst feedback, this criterion examines which vendors consider others to pose

direct competitive threats by, for example, driving the market forward with innovative features co-packaged within firewalls or offering innovative pricing or support offerings. Unacceptable device or software failure rates, vulnerabilities, poor performance and a product's inability to survive to the end of a typical firewall life span are assessed. Significant weighting is given to the delivery of new platforms for scalable performance in order to maintain investment, and to the range of models to support various deployment architectures.

Customer Experience: Products, services and/or programs that enable customers to achieve anticipated results with the products evaluated. Specifically, this criterion considers the quality of supplier-buyer interactions, technical support and account support. The quality and responsiveness of the escalation process and transparency are important. This criterion may also cover ancillary tools, customer support programs, availability of user groups, service-level agreements and so on.

The most important factor is customer satisfaction throughout the sales and product life cycle. Also important are ease of use, platform approach, centralized management and protection against the latest attacks.

Operations: The ability of the organization to meet its goals and commitments. Factors include the quality of the organizational structure, skills, experiences, programs, systems and other vehicles that enable the organization to operate effectively and efficiently. Also considered are management experience and track record, and the depth of staff experience, specifically in the security market. Gartner analysts also monitor repeated release delays, frequent changes in strategic directions, and how recent organizational changes might influence the effectiveness of the organization.

Table 1: Ability to Execute Evaluation Criteria

Evaluation Criteria ↓	Weighting ↓
Product or Service	High
Overall Viability	Medium
Sales Execution/Pricing	Medium
Market Responsiveness/Record	High
Marketing Execution	Medium
Customer Experience	High

Evaluation Criteria	Weighting
Operations	Medium

Source: Gartner (November 2021)

Completeness of Vision

Gartner analysts evaluate vendors on their ability to convincingly articulate logical statements about current and future market direction, innovation, customer needs and competitive forces. They assess how well these correspond to Gartner's view of the market.

Market Understanding: This is the vendor's ability to understand buyers' wants and needs, and to translate that understanding into products and services. Vendors with the strongest vision listen to and understand buyers' requirements, and can shape or enhance them with their added vision. They also determine when emerging use cases will greatly influence how technology has to work. Vendors with a better understanding of how changes in web applications affect security receive higher scores. Trends include support for hybrid environments and different firewall deployment use cases, centralized management and visibility, cloud security, cloud workload protection and automation.

Marketing Strategy: Clear, differentiated messaging consistently communicated internally, and externalized through social media, advertising, customer programs and positioning statements.

Sales Strategy: This includes preproduct and postproduct support, value in terms of pricing, clear explanations, and recommendations for detecting events, including zero-day events and other advanced threats. Building loyalty through credibility with full-time network firewall staff demonstrates the ability to assess the next generation of requirements. Vendors need to address the network security and/or cloud workload buying center correctly, and they must do so in a technically direct manner, rather than, in effect, just selling fear or next-generation hype. Channel and third-party security product ecosystem strategies matter insofar as they are focused on network security.

Offering (Product) Strategy: The vendor's approach to product development and delivery that emphasizes differentiation, functionality, methodology and feature sets as they map to current and future requirements. This criterion considers, for example:

- Support for hybrid environments
- Integrated support for multiple firewall deployment use cases

- Integration and automation with CI/CD pipelines beyond Open API integration playbooks
- Advanced threat detection and prevention capability
- XDR capability
- Platform approach
- Centralized management and visibility across environments with CSPM capabilities.
- Strong identity- and application-based control for work-from-home employees
- Easy-to-consume licensing models

Business Model: This includes the process and success rate for developing new features and innovation. It also includes R&D spending.

Vertical/Industry Strategy: This includes the ability and commitment to serve geographies and vertical markets.

Innovation: Direct, related, complementary and synergistic layouts of resources, expertise or capital for investment, consolidation, defensive or preemptive purposes, and the vision to support upcoming niche technologies. This criterion looks for product innovation and quality differentiators such as:

- A platform approach
- A strong vision and exceptional features for a particular firewall deployment use case that is leading the market
- Enhanced workload protection
- Features supporting hybrid environments and multiple firewall deployment use cases
- A centralized management and XDR interface to support different firewall deployment use cases with CSPM capabilities
- A strong offering for east/west traffic inspection, especially between workloads
- A strong FWaaS capability that extends to strong authentication and data protection capabilities Feature enhancements to secure work-from-home user traffic are also desirable
- Intuitive automation and CI/CD integration with workloads and a DevOps environment, beyond API integration
- Simplicity in relation to the management of network security policies across hybrid environments

- The ability to prevent zero-day attacks in real time

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

Table 2: Completeness of Vision Evaluation Criteria

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

Source: Gartner (November 2021)

Quadrant Descriptions

Leaders

The Leaders quadrant contains vendors that can shape the market by introducing additional capabilities, raising awareness of the importance of those capabilities, and being the first to do so. Leaders also have the potential to meet enterprise requirements for multiple firewall use cases in a single platform solution.

Leaders offer new features that protect customers from emerging threats. They meet the requirements of evolving hybrid networks, including public and private clouds. They provide expert capabilities, rather than treating firewalls as commodities. They have a

good track record of avoiding vulnerabilities in their security products.

Leaders offer innovative features to simplify configuration and management of firewall policies across hybrid environments. They commonly have the ability to handle the highest throughputs with minimal performance loss. Additionally, they often offer options for hardware acceleration, support for private and public cloud platforms, and form factors that protect enterprises as they move to new infrastructure form factors. Leaders offer the first features and capabilities to support emerging firewall use cases in depth. They take an integrated platform approach, instead of having multiple different product lines for different use cases with a lack of integration.

In addition to providing technology that is a good match for customers' current requirements, Leaders exhibit superior vision and execution with regard to likely future requirements and the evolution of hybrid networks.

Challengers

Challengers have sound reseller channels and customers, but do not consistently lead with differentiated next-generation capabilities. Many Challengers have not fully matured their firewall capabilities. They may have other security products that are successful in the enterprise sector and are counting on their existing relationships with customers, rather than their firewall products, to win deals.

Challengers' products are often well-priced and, because of strong execution, these vendors can offer economical security product bundles that many others cannot.

Many Challengers hold themselves back from becoming Leaders by giving their security or firewall products a lower priority within their overall product sets.

Challengers often have significant market shares, but may trail those with smaller market shares when it comes to releasing new features.

Visionaries

Visionaries lead in terms of innovation, but are limited to one or two firewall deployment use cases. They have the right designs and features, but lack the sales base, strategy or financial means to compete consistently with Leaders and Challengers. Sometimes, Visionaries have made a conscious decision to focus on a limited number of firewall use cases. Most Visionaries' products have good next-generation firewall capabilities, but are lacking in terms of performance and support networks.

Visionaries show strong vision and market-leading innovation in relation to, among other things, securing work-from-home users, ensuring the security of workloads, enabling east-west segmentation in public cloud and software-defined networking environments, and automating threat detection.

Niche Players

Most Niche Players have a primary installed base, or prominence, in a particular use case, such as data centers, telcos, distributed enterprises, SMBs or public IaaS. Some Niche Players that offer a firewall as a module, along with other services or components, focus on a particular use case.

Niche Players are lacking in terms of Ability to Execute because of their limited client bases, and they tend not to show much innovation. Some are confined to particular regions.

Context

Network firewalls have evolved into network firewall platforms to meet the firewall requirements of hybrid environments from the same vendor. Network firewall platforms can be defined as hardware firewalls (of different sizes), cloud workload protection firewalls and FWaaS offerings from the same vendor. They can sometimes be managed from a single centralized management interface, and have advanced reporting and analytics capabilities. They should also support different cloud security use cases, such as containerized firewalls and identity segmentation, and have advanced FWaaS capabilities, such as ZTNA and URL filtering. If a vendor's offerings are fragmented and do not reduce the operational complexity of managing different firewall use cases, they do not constitute a platform.

That said, use-case-specific vendors are also growing and are highly relevant, as network firewall platforms lack maturity for certain use cases and can create operational complexities. End users are inclined to evaluate, and sometimes adopt, these vendors for emerging use cases such as FWaaS, identity-based segmentation and cloud firewalls.

Market Overview

The network firewall market faces the challenge of fulfilling multiple use cases and overlapping requirements because of the growth of hybrid environments. Although basic firewall features have become commodities, specialization in new firewall use cases such as FWaaS, cloud firewalls and OT firewalls is differentiating vendors. With more and more firewall vendors adding products to their security portfolios, consolidation of different controls in security architecture on a single provider is becoming desirable. The first quarter of 2021 brought 13.3% growth in revenue, compared with the first quarter of 2020.

The different types of vendors in this market are as follows:

- **Large network security vendors:** These vendors have firewall offerings to meet the majority of firewall use cases and are working to expand their firewalls into firewall platforms. They are also expanding their security product portfolios by developing and acquiring products from overlapping markets, such as those for security operations, cloud workload protection platforms, web application and API protection, endpoint security, and SASE. Although these vendors are expanding their product portfolios, they are not doing so fast enough to match the pace of adoption of hybrid environments. As a result, clients still look for specialist vendors for specific firewall use cases. The majority of vendors in this Magic Quadrant are large network security vendors.

- **Use-case-specific firewall vendors:** As environments expand, so the need for firewalls for specialized use cases grows. Many of the controls required for these use cases either were not being offered by enterprises' incumbent network security vendors or had limitations. This situation led to the growth of vendors focused on one or two of the following use cases: (1) cloud security; (2) FWaaS; (3) distributed enterprise; (4) OT security.

- **Native players:** As security requirements have grown, infrastructure and network vendors have started offering full firewall capabilities as native controls. This gives end users in-line controls within an environment without integration issues.

As a result of the market's dynamics, buyers must:

- Recognize that buying products from the same vendor does not guarantee automation and reduced complexity. Gartner recommends that if the primary reason for consolidating on a single vendor is automation, integration and ease of management, you do not finalize purchases until you have evaluated the required features in your environment.

- Determine your primary firewall use case and evaluate vendors' capabilities for that use case, instead of just consolidating with your incumbent vendor. This is especially important for emerging use cases for SASE and identity-based segmentation, for which the maturity of capabilities varies. Clients often prefer a more mature vendor for these use cases.

- Refuse to accept complex ELA quotations that do not make sense to you. Always maintain your own list of SKUs and demand fully itemized pricing, instead of bulk-pricing numbers.

- Take account of the use cases that will evolve in the next one or two years if you plan to consolidate and simplify your security architecture by using fewer vendors. Request roadmap information from vendors with regard to these use cases.

- Remember that the security-as-a-service model may not reduce your TCO, so do not aspire to make savings from that approach. Calculate a realistic TCO during fresh life cycles.

- Understand that native/in-line controls offer better automation than those from third-party vendors.

Evaluation Criteria Definitions

Ability to Execute

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

Overall Viability: Viability includes an assessment of the overall organization's financial health, the financial and practical success of the business unit, and the likelihood that the individual business unit will continue investing in the product, will continue offering the product and will advance the state of the art within the organization's portfolio of products.

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

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

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

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

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

Completeness of Vision

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

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

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

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

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

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

Innovation: Direct, related, complementary and synergistic layouts of resources, expertise or capital for investment, consolidation, defensive or pre-emptive purposes.

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