Magic Quadrant for Network Firewalls

Published 1 November 2021 - ID G00740145 - 60 min read

By Rajpreet Kaur, Jeremy D'Hoinne, **and 2 more**

As new use cases for network firewalls evolve, traditional firewall vendors are acquiring or developing offerings to fulfill them, and use-case-specific vendors are emerging. This Magic Quadrant assesses 19 providers to help you make the right choice for your organization's needs.

Strategic Planning Assumptions

By 2025, 30% of new deployments of distributed branch-office firewalls will switch to firewall as a service, up from less than 10% in 2021.

By the end of 2025, 35% of end-user spending on network firewalls will be within larger security deals delivered by enterprise license agreement (ELA) from the same vendor, up from less than 10% in 2021.

Market Definition/Description

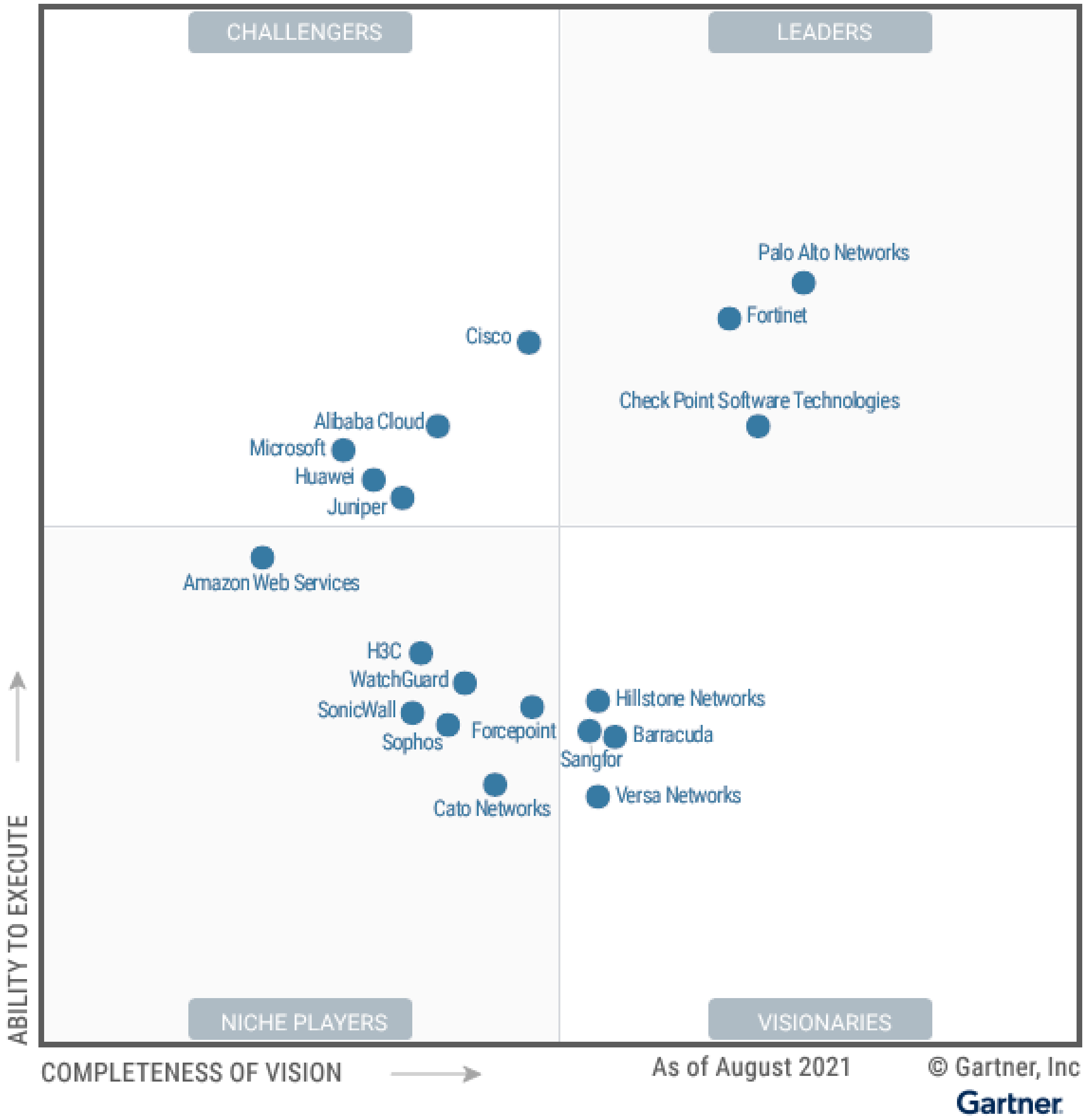
Network firewalls secure traffic bidirectionally across networks. Although these firewalls are primarily deployed as hardware appliances, clients are increasingly deploying virtual appliance firewalls, cloud-native firewalls from infrastructure as a service (IaaS) providers, and firewall as a service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

Vendor Strengths and Cautions

Alibaba Cloud

Alibaba Cloud is a Challenger in this Magic Quadrant. It offers a public cloud firewall called Alibaba Cloud Firewall, FWaaS and identity-based segmentation only for Alibaba Cloud customers. Alibaba Cloud Security Center enables centralized management of the firewall and other products offered by this vendor. Furthermore, the Ultimate edition of Alibaba Cloud Firewall has its own centralized manager. In addition to firewalls, Alibaba Cloud offers multiple security offerings, including, for example, distributed denial of service (DDoS) mitigation, a web application firewall, data protection and encryption, along with managed security services.

Recent updates have included the introduction of network services and multiple network-security-related features. Key highlights are the introduction of the Cloud Security Access Service (CSAS) in China, with application access control, URL control, zero threat network access (ZTNA) intranet access control and logging capabilities, a container firewall and virtual patching.

Alibaba Cloud Firewall is often shortlisted by Alibaba Cloud customers seeking an in-line stateful inspection firewall with threat inspection, application control and URL filtering capabilities. Alibaba Cloud Firewall is suitable for Alibaba customers looking for a mature cloud firewall with FWaaS capabilities.

Strengths

- **Market execution:** Of the public cloud vendors, Alibaba has the most mature firewall offering. It has mature features such as URL filtering, application control, network sandboxing and data loss prevention (DLP), and it can fulfill the FWaaS use case, too.
- **Offering:** Alibaba Cloud offers ZTNA as a stand-alone capability of CSAS. The vendor offers ZTNA clients for Windows and macOS, and for Android and iOS endpoints, thus covering both fixed and mobile devices.
- **Offering:** Alibaba Cloud offers agent-based microsegmentation, in addition to the network-based segmentation that public cloud vendors generally offer. The user can create business groups and user groups for segmentation and visualization.
- **Customer feedback:** Customers have given high scores to the advanced threat detection capability offered through an intrusion detection and prevention service (IDPS). They have also identified the logging available as granular.

Cautions

- **Product strategy:** Despite DevOps being the primary use case for cloud adoption, Alibaba Cloud Firewall lacks the continuous integration/continuous delivery (CI/CD) automation features that other cloud vendors offer.
- **Geographic strategy:** Although Alibaba Cloud has a major presence in China, its presence in Southeast Asia is limited, compared with other cloud players.
- **Customer feedback:** Surveyed customers have described the application control feature available with the firewall as basic. Alibaba Cloud Firewall supports local Chinese applications, but has no support for third-party applications like Office 365.
- **Product capability:** Alibaba Cloud Firewall does not offer Transport Layer Security (TLS) offloading capability. As a result, the IDPS engine has no visibility to decrypted traffic.

Amazon Web Services

Amazon Web Services (AWS) is a Niche Player in this Magic Quadrant. AWS is a global public cloud provider. It offers a number of network security controls for its public cloud customers, including Amazon Virtual Private Cloud (VPC) security groups and an Amazon VPC network access control list. The offering evaluated here is the AWS Network Firewall, which was released in November 2020. AWS Firewall Manager centralizes management of all AWS's firewall-related offerings, including its web application firewall and DNS firewall. In the past 12 months, AWS has extended availability of the AWS Network Firewall to all 23 of its regions.

AWS is a good candidate for organizations using the AWS cloud to consider, if they value seamless firewall integration with the AWS platform.

Strengths

- **Market execution:** Since AWS Network Firewall is a native offering, it is easier to deploy and comes with simple pricing models. Customers appreciate the solution's scalability, performance and single-click deployment with a baseline set of security rules. This is especially important for organizations with small security teams.
- **Product:** Amazon GuardDuty's integration with AWS Network Firewall provides automated threat intelligence for its Suricata and Snort open-source rules. This helps customers who want security capabilities beyond the firewall.
- **Customer experience:** AWS customers use the vendor's extensive product documentation to answer their questions, sometimes without involving support. If support is needed, it is available 24/7 globally and receives generally high marks from customers.
- **Product:** AWS Firewall Manager represents a single management source of truth for several network security products. It provides security administrators with a full picture of security policies across their AWS environment, thus easing the administrative burden.

Cautions

- **Innovation:** Although AWS has a large research and development (R&D) budget and many resources, the pace of innovation across its security offerings (including AWS Network Firewall) is slower than is the case with its direct competitors. AWS Network Firewall is a basic offering that lacks the ability to meet emerging firewall use cases and needs better integration with other security offerings.
- **Market understanding:** AWS lacks agent-based ID segmentation and features for FWaaS customers. Clients must use third parties for identity-based segmentation for their AWS cloud workloads.

- **Product strategy:** AWS's timeline for introducing mature firewall features lags behind those of its competitors. Features such as URL filtering, better administrative privileges and identity-based control are currently missing from AWS Network Firewall.

- **Product strategy:** Organizations cannot use AWS Network Firewall outside AWS environments. As more cloud-first customers move to multiple cloud deployments, they seek solutions that can work across hybrid cloud deployments.

Barracuda

Barracuda is a Visionary in this Magic Quadrant. It offers a firewall primarily for distributed offices and the public cloud use case within the CloudGen Firewall product line. It also offers FWaaS through its secure access service edge (SASE) offering, CloudGen WAN. Firewall Control Center is the centralized firewall manager and Firewall Insights is the reporting tool.

Recent updates include Internet of Things (IoT), operational technology (OT) and cloud security features. Highlights include integration of ZTNA (CloudGen Access) and the addition of security features to CloudGen WAN. Barracuda has also announced a partnership with Crosser to manage firewall configuration changes for OT environments.

Barracuda is suitable for distributed offices and OT security use cases. With mature cloud security features, CloudGen Firewall is good for connecting to a public cloud and for public cloud firewall use cases for AWS and Microsoft Azure.

Strengths

- **Product strategy:** Barracuda's CloudGen Firewall offers mature integration with native AWS and Microsoft Azure controls, compared with the majority of firewall vendors. Barracuda also offers FWaaS (CloudGen WAN) to address the work-from-home and remote-office use cases.

- **Market execution:** Barracuda's CloudGen Firewall comes with dedicated industrial firewall models that support supervisory control and data acquisition (SCADA)/OT protocols, and integration with SCADAfence (a continuous network monitoring platform for IoT and OT technologies). The vendor also offers partnerships with dedicated OT vendors.

- **Offering:** Barracuda has introduced ZTNA as a dedicated offering via the recently acquired Fyde. This offering is called CloudGen Access.

- **Customer feedback:** Gartner clients have often praised the ease of use and intuitive UI of Barracuda's CloudGen Firewall.

Cautions

- **Product:** Despite focusing on the cloud security use case, Barracuda does not offer a container firewall or ID segmentation.

- **Offering:** Barracuda lacks a cloud-based centralized manager for CloudGen Firewall. Also, it does not offer centralized management for CloudGen Firewall, CloudGen WAN or CloudGen Access.

- **Market responsiveness:** Barracuda lacks an endpoint security client. It offers advanced reporting through a third party, Stellar Cyber.

- **Customer feedback:** Clients using Barracuda have complained of a lack of granular reporting capabilities. In addition, they have described specific reporting for VPN connections as basic.

Cato Networks

Cato Networks is a Niche Player in this Magic Quadrant. It offers FWaaS through its Cato SASE Cloud product. Although there is a hardware component called Cato Socket for a software-defined wide-area network (SD-WAN), this component requires Cato’s cloud components. No stand-alone firewall or virtual appliance firewall is offered. The Cato Management Application manages all of Cato’s product offerings.

Recent updates focus on building SASE capabilities. ZTNA capabilities are now available in an agentless format, thus increasing the breadth of users that can be protected by Cato SASE Cloud beyond the SD-WAN use case.

Cato is a good option for distributed organizations looking for a simple and consolidated FWaaS and SD-WAN solution.

Strengths

- **Market understanding:** Cato was one of the earliest FWaaS providers in this market. Hence, it has years of experience with customers and real-world environments for this use case.

- **Product strategy:** Cato SASE Cloud consolidates edge capabilities into a single offering with a single configuration. Firewall, network, SD-WAN, VPN and ZTNA are well-converged in this offering, which simplifies configurations and reduces the risk of misconfiguration.

- **Offering:** Cato SASE Cloud wraps a complete SD-WAN and security stack in an integrated and cloud-supported package. The vendor offers a router and a firewall in a thin on-premises product as a gateway (Cato Socket).

- **Customer feedback:** Clients have highlighted ease of setup and operation as a strength of Cato’s product.

Cautions

- **Market execution:** As most traditional firewall vendors and other secure web gateway (SWG) vendors have started offering their own FWaaS, Cato is rarely seen on FWaaS shortlists.
- **Product strategy:** FWaaS is not currently the best fit for all environments — it works best for perimeter use cases, particularly in smaller environments. Hardware and virtual appliances are not available from Cato, which makes it impracticable for this vendor to support use cases inside data centers, whether private or public.
- **Market responsiveness:** Cato's SWG and cloud access security broker (CASB) capabilities are rudimentary and lack the breadth available with other firewalls. SWG and CASB are key components needed for SASE. Cato also lacks an endpoint protection platform (EPP) or endpoint detection and response (EDR) offering, something commonly available as an integrated component of other firewalls.
- **Customer feedback:** Clients have highlighted the higher costs of using Cato's subscription bundles, compared with other direct hardware firewall competitors used for distributed office use cases.

Check Point Software Technologies

Check Point Software Technologies is a Leader in this Magic Quadrant. It offers a comprehensive security portfolio that features Quantum-branded hardware appliances, such as the recently released Maestro Hyperscale product line. Check Point also offers virtual appliances and cloud security products under the CloudGuard brand, plus a FWaaS product that comes under the Harmony brand used for Check Point's SASE solutions. Check Point offers on-premises (Quantum Security Management) and cloud-hosted (Infinity portal) centralized management and monitoring products.

In the past 12 months, Check Point has released new Maestro appliances and container firewalls. Software features include autonomous threat prevention, which makes configuration easier, TLS 1.3 support with detection of fake Server Name Indication (SNI), and various improvements to management and monitoring consoles.

Check Point is a good candidate for shortlisting by organizations that have embarked on a hybrid transition with a wide range of on-premises and IaaS security needs. Its mature, security-focused management platform will help them handle complex change workflows.

Strengths

- **Customer experience:** Check Point has recently invested heavily in its distributed support workforce, and Gartner analysts have noticed an overall improvement in customers' satisfaction. Support scores remain higher in EMEA than in other regions.

- **Market execution:** Check Point offers a broad product portfolio and mature consolidation options. This is shown by offerings like Infinity SOC, which is its security orchestration, automation and response (SOAR) offering, and CloudGuard, its cloud security product.

- **Roadmap execution:** Check Point shows strong commitment to the appliance segment, as shown by regular hardware refreshes, performance improvements and architecture innovations (including Maestro).

- **Product strategy:** Check Point has a strong message and roadmap for high-security use cases. It continuously improves its threat inspection and content disarm and reconstruction (CDR), shared threat intelligence and comprehensive set of security features for identity-based segmentation.

Cautions

- **Sales and marketing execution:** Gartner believes that Check Point is losing market share as it grows more slowly than its direct competitors. Despite having a broad product portfolio and robust firewalls, it is gaining less traction in the market than its direct competitors.

- **Customer experience:** Customers are often unaware of Check Point's large range of security products beyond firewalls. Some say that the reason they switch to a different vendor is that they want to consolidate with a larger vendor.

- **Capabilities:** Check Point pursues a partnership strategy for advanced SD-WAN features, which puts it as a disadvantage when security teams expect their firewall vendor to provide more than basic quality of service (QoS).

- **Product offering:** Check Point was a late entrant to the container firewall market. Its container product still lacks application control, but does support URL filtering, threat prevention and autonomous access policy. It is integrated only with the cloud management console.

Cisco

Cisco is a Challenger in this Magic Quadrant. It offers multiple firewall product lines, including Cisco Secure Firewall (formerly Firepower), Cisco Secure Workload (formerly Tetration) and the Meraki MX series. In addition, Cisco offers Umbrella Secure Internet Gateway (SIG) for FWaaS, and industrial firewalls (the Secure Firewall Industrial Security Appliance [ISA] series). Cisco Secure Firewall Management Center (on-premises) and Cisco Defense Orchestrator (cloud-based) are their centralized managers.

During the evaluation period for this Magic Quadrant, Cisco released six Firepower Threat Defense (FTD) virtual appliances, a container firewall and Cisco Secure Managed Remote Access, a managed

VPN solution. Another important update is multicloud management and control with the integration of Secure Workload and Secure Firewall.

Cisco is suitable for organizations looking for a single vendor in order to consolidate a wide range of network and security technologies.

Strengths

- **Sales strategy:** Cisco has a diverse, flexible collection of security enterprise agreements that allow organizations to deploy whichever Cisco security solutions make sense for their use cases, in deals with favorable commercial terms.
- **Product execution:** Cisco has multiple offerings for different firewall use cases. It offers virtual firewalls for Oracle Cloud, in addition to AWS, Microsoft Azure and Google Cloud Platform. Its container firewall increases Cisco's relevance to cloud environments.
- **Customer experience:** Clients consider the inclusive SecureX extended detection and response (XDR) platform offering a strength. Cisco customers are offered SecureX XDR at no cost to detect, hunt and remediate threats.
- **Feature:** Cisco benefits from support for the Snort open-source intrusion detection system/intrusion prevention system (IDS/IPS) community. Snort 3 offers an enhanced signature set. Cisco Secure Firewall can be deployed as a stand-alone IDS/IPS.

Cautions

- **Product:** Although Cisco has promoted Cisco Defense Orchestrator (CDO) as its centralized cloud management platform for some time, CDO enables full management only of Cisco Meraki MX, Cisco Secure Firewall Threat Defense and Cisco Secure Firewall ASA products. It lacks management capabilities for Cisco Umbrella and Cisco Security Workload.
- **Sales execution:** Gartner usually sees Cisco Secure Firewall Threat Defense firewalls included in large Cisco Enterprise Agreement deals, as opposed to pure firewall deals. Despite the vendor's support for four public cloud platforms, and its release of new virtual firewalls and FWaaS through the Cisco Umbrella offering, Gartner rarely sees Cisco shortlisted for these emerging use cases.
- **Product strategy:** Despite having existing products that could address emerging security use cases, Cisco has not acted quickly enough to gain much market traction for these use cases. Cisco Umbrella still does not offer an integrated SASE approach and requires multiple different subscriptions, such as to Cloudlock (Cisco's stand-alone CASB), ZTNA in Duo Beyond, and an SD-WAN through Cisco Meraki.

- **Customer experience:** Some Cisco firewall clients identify the existence of multiple firewall product lines for different use cases and the lack of a platform approach as a reason to move to another vendor.

Forcepoint

Forcepoint is a Niche Player in this Magic Quadrant. During the evaluation period, it introduced several new firewall models, notably the N60 and N120WL at the low end. It also brought to market a new SASE offering. Other updates included increased SD-WAN performance to enable faster SD-WAN firewall edge connectivity, further enhancements to AWS and Microsoft Azure integrations, and an additional IPS engine to enable open-source signature compatibility with Snort.

Forcepoint's firewall appliance has built-in SD-WAN capabilities. Forcepoint also has several virtual appliance models. In addition to network firewalls, Forcepoint offers DLP, CASB and SWG product lines.

Forcepoint firewalls are good shortlist candidates for distributed office use cases where clients are looking for mature SD-WAN, VPN and centralized management capabilities. They have advanced clustering/high availability, and are also good candidates for midsize enterprises looking for a way to consolidate several SASE functions with a single vendor.

Strengths

- **Product execution:** Forcepoint continues to scale up its VPN capabilities. It has released the N60, a small, low-cost appliance to support more efficient distributed deployments. For its network firewall product line, Forcepoint has built a second IPS engine to allow for open-source signature compatibility with Snort rules.

- **Sales execution:** Forcepoint offers value in its flexible licensing model. Forcepoint firewalls include SD-WAN, clustering, threat intelligence, antivirus, VPN and IPS capabilities at no additional cost. It also offers ELAs for its entire security portfolio.

- **Customer feedback:** Forcepoint customers have praised its easy-to-understand and easy-to-use Security Management Center (SMC) management console, which has deep granular policy management capabilities.

- **Offering:** Forcepoint offers mature zero-touch provisioning, as its newly deployed network firewalls seek out the closest SMC and download policies automatically. In addition, Forcepoint's mixed-model clustering provides flexibility that allows customers to scale active/active performance.

Cautions

- **Product execution:** Forcepoint has yet to release a FWaaS into general availability, which complicates its SASE ambitions. In this respect, it lags behind major competitors, several of which have had a FWaaS for years to support organizations with small distributed offices and remote workers.

- **Industrial firewalls:** Forcepoint does not offer separate industrial firewalls, which limits its appeal in rugged environments and OT networks. Additionally, it supports only a limited range of OT protocols.

- **Offering:** Forcepoint lacks an identity-based segmentation offering. It also lacks a container firewall. Customers increasingly expect to get such solutions from their firewall vendor.

- **Marketing:** The market's awareness of Forcepoint is limited, and Forcepoint is rarely mentioned as a shortlist candidate by Gartner clients. Forcepoint does have some presence in U.S. and European federal government sectors, but it lacks consistent visibility in other markets.

Fortinet

Fortinet is a Leader in this Magic Quadrant. Its FortiGate firewall product line is available for all firewall deployment use cases. FortiGate is also available in virtual appliances for public cloud platforms. Fortinet recently released FortiGate FWaaS, following its acquisition of OPAQ, which has been rebranded as FortiSASE. FortiManager and FortiGate Cloud are Fortinet's centralized managers. FortiAnalyzer and FortiCloud are its centralized reporting tools. Fortinet has a broad security portfolio, which, in addition to firewalls, includes capabilities such as EDR, email security, web application firewall/web application and API protection (WAF/WAAP), network access control (NAC), deception, and identity and access management (IAM). Recent updates include the introduction of security operations center (SOC) as a service, SASE and ZTNA product offerings. Fortinet has also introduced enhancements to its URL filtering and advanced threat detection features. Additionally, it has introduced integration between network operations center (NOC) and SOC operations in the Fabric Management Center.

Fortinet is suitable for enterprises that have hardware-based firewall use cases with strong networking capabilities. It is also a good candidate for organizations seeking to consolidate solutions, because of its large product portfolio.

Strengths

- **Advanced networking:** Fortinet is a leading provider of networking and SD-WAN capabilities in the WAN edge market. FortiGate often replaces branch office routers and can manage Fortinet switches and wireless access points, which makes it able to consolidate and manage branch office network infrastructures.

- **Product strategy:** The platform approach of Fortinet Security Fabric continues to build an ecosystem of integrated components. Out-of-the-box integration and automation is available across much of the Fortinet security and network portfolio, resulting in reduced operational effort and fewer misconfigurations. Fortinet's firewall is integrated with web, cloud, email, CASB, deception, endpoint and NAC switches and wireless access points, all of which are managed from a single console.

- **Product:** Fortinet recently introduced FortiSASE with SD-WAN and FWaaS. It also offers a stand-alone identity-based segmentation product as a result of the acquisition of ShieldX Networks. FortiSASE and ShieldX are currently stand-alone offerings and cannot be managed by FortiManager.

- **Customer experience:** Gartner continues to see lower pricing as the primary reason to shortlist Fortinet's firewalls. The vendor's competitive price/performance ratio, combined with its simple pricing models, highlights its value and allows for realistic estimation of the total cost of ownership (TCO).

Cautions

- **Market execution:** Although Fortinet has a large security portfolio, Gartner does not encounter Fortinet firewall customers that are keen to adopt its other security product lines for consolidation. Gartner finds that Fortinet takes a less aggressive approach than other vendors when it comes to developing and upgrading other security products to compete with best-of-breed products.

- **Product offering:** Fortinet lacks a dedicated container firewall and offers basic management features through a plug-in to FortiManager. FortiManager also lacks integration with the OPAQ and ShieldX product lines.

- **Product execution:** FWaaS and FortiSASE are new stand-alone offerings resulting from the acquisition of OPAQ. Fortinet lags behind other vendors in terms of rollout of cloud points of presence (POPs) and geographic presence. Customers should check that Fortinet's current POPs meet their needs before investing in FortiSASE.

- **Customer feedback:** Gartner clients have expressed concerns about the recent FortiOS-related vulnerabilities announced by the Cybersecurity and Infrastructure Security Agency (CISA). The vendor did take immediate steps to fix these vulnerabilities, however.

H3C

H3C is a Niche Player in this Magic Quadrant. H3C offers a full range of hardware firewalls, known as SecPath, for small, midsize and large environments. SecPath is also available as a virtual appliance. H3C's FWaaS is SeerEngine-DC. Three central management solutions are available: iMC Security Service Manager, SecCenter Security Management Platform and SecCenter Cybersecurity Situational Awareness Platform.

H3C has continued to invest heavily in security and detection capabilities. Deception, user behavior analytics, workflows aligned with the Cyber Kill Chain and asset risk assessment are among the recent additions. Incremental improvements include web and DNS detection, and flagging of illegal content and weak passwords.

With a full set of firewall features and high throughput for data center appliances, H3C is suitable for large and midsize enterprises in China. H3C has partnered with the major public cloud providers in China to offer cloud-hosted services.

Strengths

- **Product strategy:** H3C has a strong set of firewall security features and has continued to invest in artificial intelligence (AI) detection, SecOps workflows and cloud security. The vendor offers the H3C SecCenter CSAP Threat Discovery and Security Operations Platform.
- **Market execution:** H3C has a dedicated offering for data center network use cases called the AD-DC solution. It is an SDN-based solution offering orchestration, automation and analytics using cloud computing. It also offers network-based microsegmentation capabilities.
- **Product portfolio:** H3C offers a broad range of network products that are ideal for network teams looking to undertake vendor consolidation. SD-WAN capabilities are strong and, when coupled with its FWaaS, should attract customers pursuing vendor consolidation. H3C's firewalls offer built-in WAF capability and vulnerability scanning. H3C also has a dedicated product line for industrial/OT security.
- **Customer feedback:** H3C clients in China consider the vendor's broad product portfolio and pricing as key strengths that encourage adoption for the purpose of consolidation. They have also praised the speed of its local support.

Cautions

- **Product strategy:** H3C has partnered with Chinese public cloud providers for hosted SASE solutions offered through those providers. Currently, H3C offers only a basic FWaaS in China.
- **Market execution:** H3C lacks a mature EDR offering. It offers endpoint protection and network detection and response (NDR) capabilities through separate product lines.

- **Sales execution:** Despite having a broad product portfolio, H3C lacks enterprise support agreements to benefit H3C clients and reduce multiyear licensing complexities.

- **Geographic strategy:** H3C is present primarily in China. Gartner does not see H3C shortlisted by clients outside China.

Hillstone Networks

Hillstone Networks is a Visionary in this Magic Quadrant. It offers multiple firewall product lines to meet different deployment use cases. It sells the CloudEdge virtual firewall, CloudHive identity-based segmentation, the hosted CloudPano FWaaS for service providers, and the containerized CloudArmour firewall. The Hillstone Security Management (HSM) Platform is its centralized firewall manager. Hillstone CloudView is its cloud-based security management system. Recent updates include a new firewall product line, a cloud data lake and a cloud threat analytics platform. In addition, Hillstone has made feature enhancements related to policy orchestration and improved its IP reputation database.

Hillstone is a good shortlist candidate for clients seeking to consolidate their network security and security operations architecture by using a single vendor in Asia and Latin America. CloudEdge and CloudHive are mature cloud security offerings for clients who want to secure their clouds.

Strengths

- **Product strategy:** Hillstone has a strong public cloud security strategy. As well as the CloudEdge virtual firewall, Hillstone offers the CloudArmour container firewall and the CloudHive identity-based segmentation offering.

- **Offering:** Hillstone recently introduced a cloud data lake and a cloud threat analytics platform to provide advanced reporting for Hillstone clients consolidating multiple products.

- **Customer feedback:** Customers frequently identify ease of use and simple pricing as strengths of Hillstone. They also like its support for public clouds, which enables them to consolidate with Hillstone as they extend beyond their data centers.

- **Sales execution:** Hillstone offers cost-effective firewalls with bundled pricing. As a result, it offers a better TCO than many other international competitors.

Cautions

- **Offering:** Hillstone does not offer a cloud-based centralized firewall manager. CloudEdge and CloudHive are stand-alone offerings and lack integration.

- **Offering:** Hillslone lacks a direct FWaaS offering. CloudPano is a hosted FWaaS offering sold directly by managed security service providers and local carriers in China. The vendor also lacks a native EDR offering.

- **Market responsiveness:** Hillstone's firewalls lack IoT security-related features, which more and more vendors are offering natively in their firewalls. The IDPS offered in Hillstone's firewalls lacks support for IoT-related vulnerabilities.

- **Customer feedback:** Hillstone customers have mentioned poor channel and partner support outside China. They want this support improved by means of direct vendor presence, especially in Latin America, as they increase their customer bases.

Huawei

Huawei is a Challenger in this Magic Quadrant. It offers different firewall product lines for different firewall use cases. USG and Eudemon are its hardware firewall product lines. The Huawei Cloud firewall is for virtual and cloud firewall use cases. Huawei offers different centralized managers: eSight, iMaster NCE and SecoManager. HiSec LogAuditor is its centralized reporting tool.

Recent updates enhance Huawei's advanced threat detection and SD-WAN capabilities. Highlights include improved hardware performance for higher USG firewall models and enhancements to Huawei Cloud firewall features.

Huawei is worth shortlisting for high-throughput firewall use cases, especially those of carriers and service provider customers. Clients seeking firewalls for Huawei Cloud deployments will find Huawei firewalls easier to deploy than competing offerings.

Strengths

- **Product:** Huawei offers the Huawei Cloud firewall and containerized firewalls for the Huawei cloud to support emerging firewall use cases. The Huawei Cloud firewall comes with native agent-based identity segmentation capability.

- **Market execution:** Huawei has a strong network security presence with carriers and service provider customers. Huawei has a focused product strategy to offer highly scalable firewalls for high-throughput use cases and virtual environments.

- **Customer feedback:** Huawei offers a strong price/performance ratio. This makes its firewalls (especially the higher models) cost-effective, in comparison with other vendors' relatively expensive offerings. Customers have highlighted Huawei's price/performance ratio as a strength.

- **Market responsiveness:** Huawei offers a direct managed detection and response (MDR) service. It is available via a self-service model, as well as through professional services offered by the vendor.

Cautions

- **Market execution:** Huawei's cloud security offering is largely confined to Huawei Cloud, which means it is not well-suited to cloud security needs outside China, where vendors like AWS and Microsoft (Azure) have strong market shares.

- **Offering:** Whereas the majority of competitors are focusing on introducing mature features to enhance OT/IoT security, Huawei firewalls do not have a focus on industrial and IoT use cases. Huawei does not offer any industrial firewalls or dedicated IoT security features.

- **Innovation:** Huawei lacks a direct FWaaS offering. Also, with cloud security native only to Huawei Cloud, Huawei has limited cloud security capabilities, which are confined to China.

- **Customer feedback:** Clients have reported that support outside China is often received through partners, which leads to longer response times. Clients have also reported that the client needs to improve application control features for non-Chinese applications used outside China. Organizations in North America still express concern about the geopolitical situation that has led to U.S. sanctions against Huawei, and they identify this as a reason not to shortlist Huawei.

Juniper

Juniper is a Challenger in this Magic Quadrant. Its firewall product line is the SRX series of next-generation firewalls, which is available as hardware appliances, virtual appliances (vSRX) and containers (cSRX). vSRX can be hosted on the customer's own hypervisor or run on AWS, Microsoft Azure, Google Cloud Platform, IBM Cloud Platform and Oracle Cloud Infrastructure. In addition to firewalls, Juniper offers security information and event management (SIEM), DDoS mitigation and threat intelligence.

Recent updates include enhancements to advanced threat detection capabilities, IoT security, and partnerships for industrial control system (ICS) and supervisory control and data acquisition (SCADA) environments.

Juniper firewalls are suitable for enterprises looking for an integrated network offering, including firewalls, from one vendor. The vSRX and cSRX firewalls are good candidates for public cloud security use cases.

Strengths

- **Product strategy:** Juniper continues to deliver on its strong networking focus, with security services available both for its firewall products and its networking infrastructure. Advanced Threat

Profiling and SecIntel are shared analysis and threat intelligence offerings that integrate with Juniper's SRX, MX, EX/QFX and Mist AP product lines.

- **Offering:** Juniper has revealed a focus on the IoT security use case by enhancing its automated device fingerprinting and control. It has also announced partnerships with Dragos and Schweitzer Engineering Labs, to provide threat detection and response for industrial IoT applications within ICS and SCADA environments.

- **Market execution:** Juniper firewalls are available on a "pay as you go" (PAYG) basis on multiple public IaaS platforms, such as those of AWS, Microsoft (Azure), IBM and Google. This makes Juniper one of the few firewall vendors to support all the major public IaaS platforms on a PAYG basis. Its container-based firewall, cSRX, is available on the AWS container marketplace.

- **Scalability:** While Juniper offers high-throughput firewalls, its Junos Space Security Director and Security Director cloud, centralized manager, can scale to manage many different Juniper devices, including switches and routers.

Cautions

- **Product strategy:** Juniper focuses on networks more than security, and thus lags behind other firewall vendors in terms of security innovations and investments. It has a continuous product strategy that works to integrate its SRX firewalls with its network products. This makes Juniper more attractive to network teams than security teams.

- **Market execution:** Whereas other firewall vendors continue to expand their security product portfolios through acquisitions, Juniper does not show that level of security investment. It primarily works through vendor partnerships for capabilities like NAC, EDR and SWG, instead of expanding beyond its SRX firewalls.

- **Market responsiveness:** Although it does offer a managed firewall service, Juniper does not offer a cloud-based FWaaS. Nor does it offer a strong SASE service, despite the strong emerging use case for one.

- **Customer experience:** Gartner clients often identify Juniper's technical support and slower pace of innovation in security as their key reasons for moving to another vendor. They also state that Juniper's firewalls are expensive.

Microsoft

Microsoft is a Challenger in this Magic Quadrant. The Microsoft Azure Firewall offering is available as two subscriptions: Standard and Premium. It can be centrally managed by Azure Firewall Manager and monitored using Azure Monitor and Azure Sentinel.

Microsoft recently introduced the Firewall premium subscription. It has also added fully qualified domain name (FQDN) filtering to its network rules, and TLS decryption to its application rules.

Azure Firewall is a good candidate for organizations that need in-line firewall capabilities to protect their resources in Azure and that are looking to consolidate on Microsoft.

Strengths

- **Product:** The recently introduced Azure Firewall Premium adds URL filtering and IDPS features, thus expanding the scope of deployment to the FWaaS use case. A third-party SWG option is also available. Clients favor consolidation with their existing Azure Sentinel and Active Directory deployments.

- **Sales execution:** Adoption of Azure Firewall has grown much faster than the market average, as it is the easiest way to get an integrated firewall for Azure workloads. Gartner is seeing improved visibility of Azure Firewall in client shortlists for Azure workloads, and Microsoft's offering frequently competes with products from dedicated firewall vendors.

- **Customer experience:** Microsoft Azure users identify ease of deployment as a native firewall as a reason to use Azure Firewall. Availability in different regions of the world and in-line integration for the DevOps use case are also positives.

- **Pricing:** As Azure Firewall reproduces the Azure pricing model, with per hour and per volume subscriptions, organizations that use it often report their firewall costs as part of related infrastructure costs, and thus avoid additional internal negotiation.

Cautions

- **Innovation:** Despite having a large R&D budget and many resources, Microsoft lacks innovation in relation to firewall use cases. It offers fragmented security product lines, lacks a platform approach, and is missing mature features for emerging firewall use cases. It does, however, have great potential.

- **Market segmentation:** Like many IaaS providers, Microsoft cannot cover all firewall use cases. This puts Azure at a disadvantage when organizations are looking for a unified policy across hybrid or multicloud environments.

- **Market understanding:** Microsoft lacks strong offerings for two growing firewall use cases: agent-based identity segmentation and FWaaS. Furthermore, it is behind leading firewall competitors in terms of its progress to meet the requirements of these use cases.

- **Capabilities:** Azure Firewall lacks many of the secure connection methods that organizations like to use, such as Generic Routing Encapsulation (GRE) tunneling, proxy-based and software agents for remote users. Azure Firewall also lacks comprehensive IPv6 support. Additionally, clients want better integration of Azure Firewall with Azure Active Directory.

Palo Alto Networks

Palo Alto Networks is a Leader in this Magic Quadrant. It offers different firewalls for different deployment use cases: hardware firewalls (PA-Series), virtual firewalls (VM-Series), FWaaS (Prisma Access) and containerized firewalls (CN-Series). It also offers identity-based segmentation (Prisma Cloud). The firewall centralized manager is Panorama, which is offered both as hardware and as a virtual appliance. In addition to firewalls, this vendor offers endpoint security, cloud security and security operations products.

Recent updates include new features and enhancements across the firewall offerings. Highlights include new security subscriptions, namely IoT security, enterprise DLP, SaaS security and advanced URL filtering in the latest firewall firmware. Other key feature updates include enhancements to the IoT security feature, threat prevention, WildFire and DNS security.

Palo Alto Networks is shortlisted by enterprises looking for firewalls that offer multiple security services to detect advanced threats. Early adopters like this vendor’s pace of innovation. Palo Alto Networks is suitable for clients seeking to consolidate by using a single vendor for multiple security needs. However, it is the most expensive firewall vendor and therefore not suitable for price-conscious enterprises.

Strengths

- **Market execution:** Palo Alto Networks has continued to enhance its FWaaS service (sold as Prisma Access), which is now its most popular offering after its firewalls for work-from-home and branch office use cases. Prisma Access often encourages end users to select Palo Alto Networks.

- **Offering:** Palo Alto Networks’ containerized (CN-Series) firewalls support Kubernetes environments. They can be deployed in native Kubernetes and cloud-managed Kubernetes offerings, including Google Kubernetes Engine (GKE), Google Anthos, Azure Kubernetes Service (AKS), Openshift, Amazon Elastic Kubernetes Service (EKS) and VMware Tanzu.

- **Product:** Palo Alto Networks offers identity-based segmentation via an agent-based solution (Prisma Cloud Identity-Based Microsegmentation) for east/west segmentation across hosts and containers. It is offered as a stand-alone product with a dedicated centralized manager.

- **Customer feedback:** Gartner clients highly rate the quality of Palo Alto Networks’ presale engineers when it comes to helping them with proofs of concept and addressing their concerns.

They identify this as one of the primary reasons for choosing Palo Alto Networks in preference to other vendors.

Cautions

- **Pricing:** Palo Alto Networks has the most expensive product lines. The TCO of its firewalls exceeds those of other competitors. As the vendor adds more features, it offers them as separate software subscriptions. Additionally, SD-WAN support is offered as a separate licensed feature of its firewalls, whereas other vendors offer it as an inclusive, embedded feature.
- **Sales execution:** As Palo Alto Networks pushes more multiple-product deals to end users, its ELA contracts are becoming more complicated to understand. These contracts offered by the vendor lack transparency for clients because of the lack of clear part numbers.
- **Customer feedback:** Clients have identified deteriorating technical support as a disappointment. This is causing end users to purchase higher-tier support to achieve the quicker responses that they used to get before. Some customers have also identified higher maintenance costs as a reason to move away from Palo Alto Networks.
- **Feature:** Unlike most competitors, Palo Alto Networks does not offer a cloud-based centralized firewall manager. The VM firewall for Azure lacks support for Virtual WAN HUB on Azure. Prisma Cloud cannot be managed from Panorama; to manage Prisma Access from Panorama, clients have to install a plug-in.

Sangfor

Sangfor is a Visionary in this Magic Quadrant. It offers a broad range of hardware firewalls to suit the throughput requirements of small to large environments. Its NGAF firewall is also available as a virtual appliance. Sangfor Cloud Fortress Access is the vendor’s FWaaS solution and Sangfor Access is its SASE solution. Sangfor CWPP is its container firewall and identity segmentation offering. Sangfor Central Manager is the on-premises central management offering. Sangfor Platform-X is the cloud-based central management offering.

Recent additions to the Sangfor firewall focus on deeper security capabilities, including integrated deception and user and entity behavior analytics (UEBA) capabilities. Sangfor has also enhanced its threat detection capabilities.

Sangfor is a good choice for enterprises in China looking to consolidate by using a single vendor for firewall use cases. Its FWaaS and CWPP offerings make it a good choice for cloud security use cases, too.

Strengths

- **Product strategy:** Sangfor focuses on security and detection engines for its firewalls. AI is used for several of these engines. Development to enhance and fine tune its IPS and antivirus signatures has continued, and Sangfor recently added deception and UEBA-light capabilities. It also offers a mature EDR product.

- **Product portfolio:** Sangfor has a large portfolio of security products. Its FWaaS has been rebranded as Sangfor Cloud Fortress Access and its SASE offering as Sangfor Access. Other than firewalls, Sangfor offers NDR, an SSL VPN appliance, an SWG, endpoint security, mobile device management, advanced threat detection and a security management solution. Consulting, incident response and MDR services are also offered.

- **Market responsiveness:** Sangfor is a Chinese firewall vendor with a vision to offer strong cloud security offerings. Its FWaaS and SASE offerings deliver on that vision, but Sangfor's firewalls also have strong public cloud support, including for AWS Global, AWS in China, Microsoft Azure, Alibaba Cloud, Tencent Cloud, Huawei Cloud and Sangfor Cloud.

- **Offering:** Sangfor offers a dedicated product line, Sangfor CWPP, for container and identity segmentation and cloud security use cases.

Cautions

- **Geographic presence:** Sangfor has a major presence in China, but very limited presence in Southeast Asia and Africa.

- **Product execution:** Sangfor has 13 cloud POPs, almost all of which are in China. This is good for organizations that operate only in China but, otherwise, Sangfor's cloud services may not perform well.

- **Sales execution:** Gartner finds that although Sangfor has higher-end firewall models, it is more prominent in terms of the midsize use case than other firewall use cases.

- **Customer feedback:** Sangfor clients identify the built-in logging and reporting in its firewall product line as basic and lacking granularity. As a result, they have to purchase a dedicated reporting tool for advanced reporting capabilities.

SonicWall

SonicWall is a Niche Player in this Magic Quadrant. It markets three hardware appliance firewall product lines — the TZ, NSa and NSsp series — and a virtual appliance firewall product line, the NSv series. The NSv series can be hosted on the customer's own hypervisor or found in the marketplaces of AWS and Microsoft (Azure). Network Security Manager is its centralized management and reporting tool. In addition to firewalls, SonicWall sells integrated EDR, SEG, ZTNA and CASB capabilities.

Recent updates include multiple enhancements to the centralized manager, including rule optimization and SD-WAN workflow to simplify branch onboarding. SonicWall has also introduced centralized management for SonicWall Switch, SonicWall Access Point and SonicWall Next-Gen Endpoint.

SonicWall is a respectable candidate for midsize and small organizations looking for strong and good-value firewall capabilities, particularly if they are looking to consolidate branch security and network infrastructure.

Strengths

- **Product strategy:** SonicWall offers a consolidated branch offering with an SD-WAN-enabled firewall that can replace a branch router. SonicWall has also partnered with Perimeter 81 for a ZTNA offering, which is sold as SonicWall Cloud Edge.
- **Offering:** SonicWall offers a single management console for its multiple product lines, which makes operations and management easier for small and midsize businesses (SMBs). The firewalls, network switches, wireless access points and EDR endpoint agent offered by SoncWall can be managed through Network Security Manager.
- **Product:** SonicWall Cloud App Security helps shore up security for SaaS applications. This CASB functionality focuses on Microsoft 365 and Google Workspace, with another offering required to cover Box and Dropbox.
- **Customer feedback:** Customers have praised SonicWall’s single management interface for managing different SonicWall products. Additionally, they have identified cost-effective TCO as a reason to choose SonicWall firewalls.

Cautions

- **Market execution:** SonicWall’s execution for the emerging cloud security use case is slow, compared with its direct competitors. SonicWall lacks a container firewall and an identity-based segmentation offering. At the time of writing, it also lacks a FWaaS.
- **Product:** Although the NSv series includes many virtual appliances, SonicWall’s support for public cloud lags behind that of other vendors, with support for AWS and Microsoft Azure but not for Cisco ACI integration.
- **Positioning:** Owing to growing competition to meet demand for the SMB and distributed office use cases, Gartner rarely sees SonicWall shortlisted by prospective customers. Furthermore,

SonicWall has not expanded to fulfill other important firewall deployment use cases, such as those involving the cloud, data centers and FWaaS.

- **Customer feedback:** SonicWall clients have reported VPN instability as an occasional issue. They have also identified the recent vulnerabilities found in the SonicWall Secure Mobile Access product as a reason not to shortlist SonicWall, although the vendor took immediate steps to fix them.

Sophos

Sophos is a Niche Player in this Magic Quadrant. Its firewall product lines include Sophos Firewall (formerly XG). Sophos also continues to support its SG UTM product line for existing SMB customers. It also offers cloud security posture management (CSPM; Cloud Optix), and a centralized management portal (Sophos Central). Intercept X is the brand name for its endpoint and server protection (including for cloud workloads). Sophos also offers other security product lines, such as endpoint security, email protection and MDR services.

Recent updates have included a hardware refresh (XGS Series and SD-RED). Sophos has also continued to improve its integration with IaaS platforms and its centralized management and monitoring portals. Other features include performance improvements for its VPN and high availability, and refined TLS certificate management.

Sophos is a good candidate for shortlisting by organizations willing to integrate their endpoint and firewall security products, or that are highly distributed, with many on-premises offices.

Strengths

- **Product offering:** Integration between Sophos’ firewall and endpoint (Synchronized Security) augments the firewall’s capabilities by improving application visibility, malware detection and forensics analysis.

- **Customer experience:** Customers have given Sophos good scores for ease of use, especially in relation to the policy management interface. Customers using the Intercept X endpoint and Sophos Firewall identify their integration as a strong-enough differentiator to remain with the vendor and recommend it to others.

- **Sales execution:** Sophos receives good scores from customers for the quality of its presales activities. The vendor has built a broad portfolio of solutions and reaches customers with more than one of its products.

- **Pricing strategy:** Already competitive in terms of TCO, Sophos has improved its price/performance position with the refreshment of its firewall appliances.

Cautions

- **Market segmentation:** Gartner rarely sees Sophos on the largest enterprises' shortlists or shortlisted for hybrid data center scenarios. It did not improve its visibility in these segments during the evaluation period.

- **Product strategy:** Sophos has yet to become a credible security vendor for the security of cloud assets. It lacks a native FWaaS offering and ZTNA. Sophos Firewall cannot yet be deployed as a container. IaaS tags can only be used as visibility indicators in the CSPM product, not when building a Sophos Firewall policy rule.

- **Capabilities:** Sophos Firewall lacks virtual configuration instances within a single hardware appliance and does not support a hardware security module. It does not offer ruggedized appliances but supports some OT protocols. Sophos Central does not yet include centralized management for advanced SD-WAN features.

- **Customer experience:** Gartner has noted an increase in negative feedback about the timeliness of Sophos' support since the beginning of the pandemic. Additionally, customers with hybrid environments want better answers from the vendor's team and documentation portal.

Versa Networks

Versa Networks is a Visionary in this Magic Quadrant. Its primary firewall offering is a FWaaS, part of its SASE product line. As an established network vendor, Versa also offers on-premises firewalls within its Versa Secure SD-WAN appliances, which are available with tiered licenses (the Next Generation Firewall [NGFW] tier being a full network firewall subscription). Versa Concerto is the company's centralized management and reporting portal.

Recent updates include the introduction of CASB, DLP, advanced threat protection (ATP) and Host Information Profile services to its SASE offering, Versa SASE.

Versa is a good candidate for shortlisting by existing SD-WAN clients of Versa and by others that want a robust SD-WAN with a FWaaS.

Strengths

- **Market understanding:** Versa is focusing on the SASE use case, with FWaaS, ZTNA and SWG capabilities. FWaaS is an emerging use case for distributed offices and roaming users. Versa SASE supports proxy, GRE tunnel and agent-based Versa gateways and SD-WAN overlay tunnel deployment models.

- **Feature:** As a mature network vendor, Versa offers mature routing capabilities for its on-premises gateways. It offers a mature SD-WAN and QoS with 5G security support, which makes it suitable for clients looking for an integrated SD-WAN with firewall.

- **Product:** Versa takes a platform approach to its firewall product offerings. Network, firewall FWaaS and reporting are offered and managed through a centralized management product called Versa Concerto, which reduces operational complexity for existing Versa clients that want to expand with the same vendor.
- **Customer feedback:** Customers have highlighted multitenancy and zero-touch provisioning as strengths of Versa Secure SD-WAN appliances. They have also highlighted Versa's strong routing capabilities as a reason to shortlist it.

Cautions

- **Product strategy:** Versa's on-premises firewall is primarily for high-bandwidth edge deployment use cases. It is integrated with Versa Secure SD-WAN appliances, which are aimed at service providers and large enterprises only.
- **Product strategy:** Versa's primary firewall offering is its SASE product, and, as a result, it lags behind in terms of product strategy for other emerging use cases. Versa does not offer dedicated container firewall and identity segmentation product lines.
- **Product:** Versa lacks a dedicated EDR offering. As a result, it lags behind in terms of mature XDR capabilities.
- **Customer feedback:** Customers have highlighted the need for Versa to improve its direct presence in different regions and to raise the quality of its presales team as it is competing with security vendors.

WatchGuard

WatchGuard is a Niche Player in this Magic Quadrant. It offers firewalls for SMB and branch office use cases. The name of its firewall product line is WatchGuard Firebox. It also offers virtual firewalls for AWS, Azure and virtualized environments. WatchGuard Cloud (cloud) and WatchGuard System Manager (on-premises/virtual) are the vendor's centralized firewall managers. WatchGuard Cloud Visibility (cloud) and Dimension (on-premises/virtual) are its centralized reporting tools.

Recent updates include enhancements to Firebox management and cloud management of SD-WANs and VPNs, direct integration with AuthPoint and an endpoint product, and endpoint integrity enforcement for mobile VPNs.

WatchGuard is worth shortlisting for SMB and hardware-based distributed firewall use cases.

Strengths

- **Feature:** WatchGuard has continued to enhance its threat detection capabilities. It offers a threat detection and response cloud-based threat correlation portal. This portal offers combined threat-intelligence-based analytics through WatchGuard's endpoint agent, host sensor and firewall, and covers both network and endpoint-based events.
- **Product:** WatchGuard has enhanced its cloud-based firewall manager. It now offers zero-touch and firewall rules management for firewalls.
- **Offering:** WatchGuard offers mature EDR through a Panda security offering integrated with WatchGuard Cloud. It also offers a lightweight endpoint client for users as an alternative to Panda security for basic endpoint protection.
- **Customer feedback:** WatchGuard customers have identified the quality of its 24/7 support and its intuitive interface as strengths.

Cautions

- **Offering:** WatchGuard lacks a direct FWaaS offering, despite having a focus on distributed-office and remote-work use cases.
- **Sales execution:** As more vendors focus on SMB and distributed-office use cases, clients are increasingly interested in using a single vendor for all their firewall use cases. Consequently, WatchGuard is not frequently shortlisted by Gartner clients.
- **Product strategy:** Although WatchGuard offers virtual firewalls for AWS and Azure, it lacks a mature cloud security product strategy. It lacks container firewall and identity segmentation offerings. Despite offering an endpoint client, WatchGuard does not offer mature integration of this product with its firewalls.
- **Customer feedback:** WatchGuard customers have identified its native logging and reporting features as basic. They have also observed dashboard information lagging behind logging information in terms of updates.

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
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

Evaluation Criteria	*Weighting*
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.

Although Gartner research may address legal and financial issues, Gartner does not provide legal or investment advice and its research should not be construed or used as such. Your access and use of this publication are governed by Gartner’s Usage Policy. Gartner prides itself on its reputation for independence and objectivity. Its research is produced independently by its research organization without input or influence from any third party. For further information, see "Guiding Principles on Independence and Objectivity."

About Careers Newsroom Policies Site Index IT Glossary Gartner Blog Network Contact Send Feedback