Gartner. Licensed for Distribution

Magic Quadrant pour les pare-feux réseau

Lecture minimale publiée 19 décembre 2022 - ID G00 761497 - 55

Par **et 1 de plus** Rajpreet Kaur , Adam Hils ,

Alors que les pare-feu réseau évoluent vers des pare-feu maillés hybrides avec l'émergence de pare-feu cloud et d'offres de pare-feu en tant que service, la sélection du fournisseur le plus approprié est un défi. Gartner évalue 17 fournisseurs pour aider les responsables de la sécurité et de la gestion des risques à faire le bon choix pour leur organisation.

Hypothèses de planification stratégique

D'ici 2026, plus de 60 % des organisations auront plus d'un type de déploiement de pare-feu, ce qui incitera à l'adoption de pare-feu maillés hybrides.

D'ici 2026, plus de 30 % des nouveaux déploiements de pare-feu distribués pour les succursales seront des offres de pare-feu en tant que service, contre moins de 10 % en 2022.

Définition/Description du marché

Gartner définit le marché des pare-feu réseau comme le marché des pare-feu qui utilisent l'inspection bidirectionnelle du trafic avec état (pour la sortie et l'entrée) pour sécuriser les réseaux. Les pare-feu réseau sont appliqués via du matériel, des appliances virtuelles et des contrôles natifs du cloud.

Les pare-feux réseau sont utilisés pour sécuriser les réseaux. Il peut s'agir de réseaux sur site, hybrides (sur site et cloud), de cloud public ou de cloud privé. Les produits de pare-feu réseau prennent en charge différents cas d'utilisation de déploiement, tels que les périmètres, les entreprises de taille moyenne, les centres de données, les clouds, les bureaux cloud natifs et distribués.

Les fonctionnalités des pare-feux réseau incluent la mise en réseau avancée, l'inspection et la détection des menaces et le filtrage Web.

Compétence de base:

- **Mise en réseau** : cela inclut la prise en charge des tables de routage avec la capacité de traduction d'adresse réseau de destination (DNAT) et de traduction d'adresse réseau statique (SNAT).

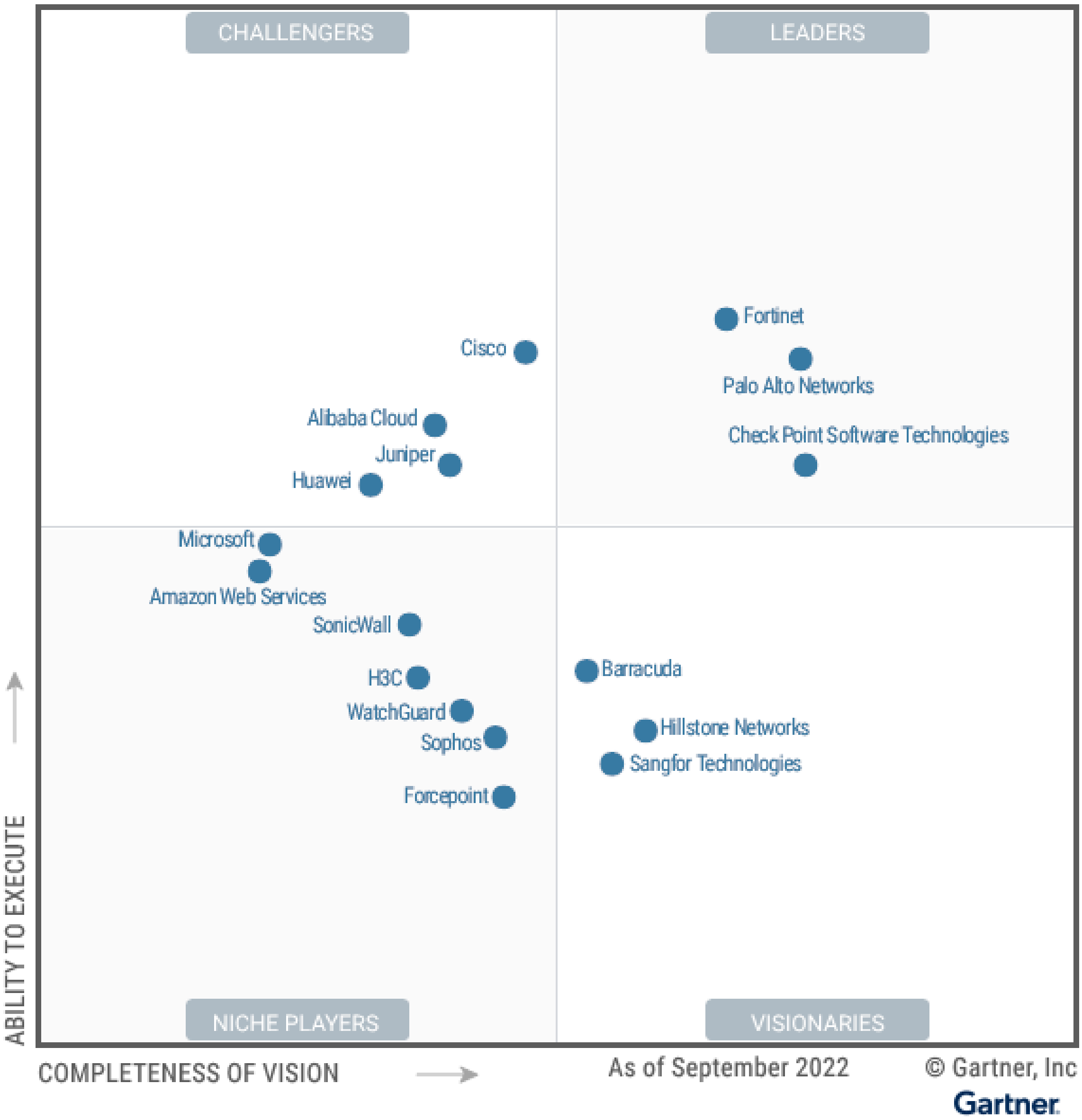
- **Inspection avec état** : cela permet d'inspecter le trafic en fonction de règles de pare-feu avec état.
- **Détection et inspection des menaces** : cela inclut le système de prévention des intrusions (IPS) et les capacités d'inspection des logiciels malveillants.
- **Filtrage Web** : cela inclut le filtrage du trafic sortant pour HTTP et HTTPS et les applications.
- **Journalisation et rapports avancés** : toutes les actions des administrateurs de pare-feu peuvent être consignées, et les rapports peuvent être personnalisés et exécutés en fonction de différents types d'objets et types de trafic. Des rapports granulaires basés sur les menaces et le filtrage Web peuvent être générés.

Fonctionnalités facultatives :

- **Internet of Things (IoT) security:** This is achieved either using a module built into threat detection controls or via a dedicated subscription integrated within network firewall offerings. Specific features may include discovery of IoT devices, risk analysis and dedicated rules to block attacks related to these devices. Also, IoT signatures as a part of IPS signature base.
- **Network sandboxing:** Network sandboxing monitors network traffic for suspicious objects and automatically submits them to the sandbox environment, where they are analyzed and assigned malware probability scores and severity ratings.
- **Zero trust network access (ZTNA):** Zero trust network access (ZTNA) makes possible an identity- and context-based access boundary between any user and device to applications.
- **Operational technology (OT) security:** This includes integrated or dedicated features related to protecting an OT environment. Stand-alone OT security offerings are not considered here. Features may include dedicated OT-related threat intelligence, dedicated IPS signatures for OT devices, support for supervisory control and data acquisition (SCADA) applications and threat inspection.
- **Domain Name System (DNS) security:** This secures traffic to DNS by offering monitoring, detection and prevention capabilities against DNS layer attacks.
- **Software-defined wide-area network (SD-WAN):** This provides dynamic path selection, based on business or application policy, centralized policy and management of appliances, virtual private network (VPN), and zero-touch configuration.

Magic Quadrant

Figure 1: Magic Quadrant for Network Firewalls



Source: Gartner (December 2022)

Vendor Strengths and Cautions

Alibaba Cloud

Alibaba Cloud is a Challenger in this Magic Quadrant. Its Alibaba Cloud Firewall is a more mature cloud firewall offering than those of its direct cloud service providers (CSP) competitors, with features such as application control, URL filtering and advanced threat prevention. It also offers firewalls for emerging cloud use cases, such as container firewalls, and microsegmentation exclusively inside its offerings.

Alibaba Cloud is a cloud service provider with an extensive product portfolio. It offers a strong set of security controls. Alibaba Cloud Firewall is its cloud-native firewall offering.

Alibaba Cloud has made major updates in relation to its firewall traffic visualization capability and introduction of a DNS firewall. It has also expanded its points of presence (POPs) to more regions outside China.

Strengths

- **Support for emerging cloud firewall use cases:** Alibaba Cloud offers a mature container firewall module, the Alibaba Security Center-Container Firewall, that offers image security and runtime application security features. Additionally, the Alibaba Cloud Firewall offers mature microsegmentation capabilities as a part of its advanced licensing tier.

- **Product portfolio and market responsiveness:** Alibaba Cloud is a large CSP with an extensive product portfolio. It has a strong focus on expanding its security offerings and scores highly for market responsiveness, compared with its direct CSP competitors.

- **Unified endpoint client:** Alibaba Cloud offers a single client for its firewall VPN, secure access service edge (SASE) and endpoint detection and response (EDR) products, which makes management and vendor consolidation easier. Both cloud firewall and EDR products can be managed centrally from the Alibaba Security Center.

- **Advanced threat detection:** Alibaba Cloud Firewall offers network detection and response (NDR) capabilities, with integration between Alibaba EDR and the Alibaba Cloud Security Center, its extended detection and response (XDR) platform. Clients also have the option to purchase a direct managed security service. Alibaba Cloud also offers a dedicated DNS firewall for DNS security.

Cautions

- **Application control:** Although Alibaba Cloud offers strong support for regional applications, along with data loss prevention (DLP) capability, its firewalls lack support for applications such as Microsoft Office 365 that are widely used outside China. Hence, customers outside China must compare Alibaba Cloud’s application control with the applications they use, before finalizing a purchasing decision.

- **Geographic presence:** Alibaba Cloud has a major presence in China, but rarely appears on the shortlists of customers outside China. As a result, its product strategy focuses on Chinese requirements.

- **Third-party partnerships:** Alibaba Cloud’s strategy is to create its own native offerings. It therefore has only limited regional partnerships. It does not offer any firewall integration with third-party EDR, XDR and identity and access management (IAM) solutions.

- **Features:** Alibaba Cloud Firewall lacks support for Transport Layer Security (TLS) decryption. It also lacks fully qualified domain name (FQDN)-based traffic routing and redirection and IoT security features.

Amazon Web Services

Amazon Web Services (AWS) is a Niche Player in this Magic Quadrant. AWS Network Firewall, a native cloud firewall, offers basic features, compared with those of other network firewall vendors. There are also third-party firewall as a service (FWaaS) offerings that customers can purchase, including partner-managed firewall rules, via the AWS Marketplace.

AWS is a CSP. AWS Network Firewall is offered as a fully managed service on AWS's cloud platform. Other AWS security product families include IAM, network and application protection, data protection, incident response and compliance.

Significant recent features developed for AWS Network Firewall include enhanced east-west protection (traffic inspection between subnets in the same virtual private cloud), default deny/drop rules, strict rule-ordering configuration options, and AWS Firewall Manager support for centralized deployment.

Strengths

- **Customer experience:** AWS Network Firewall scores highly for high availability and automated scaling. Additionally, clients like the customization feature using AWS's managed rules. They identify the ease of use of these integral features as a primary reason for selecting AWS Network Firewall.

- **Pricing:** Clients value the simplicity of AWS Network Firewall's pricing model. Customers pay for the number of firewalls deployed and the amount of traffic processed. All customers receive Basic support free of charge.

- **Scalability:** AWS Network Firewall's performance, high availability and scalability provide distinct advantages over other firewall vendors' offerings. It offers built-in high availability to ensure all traffic is inspected and monitored consistently.

- **Ease of deployment:** Ease of deployment is achieved through many different features in AWS's firewall manager, such as automatic firewall provisioning, the ability to automatically deploy firewalls across accounts and zero-touch deployment.

Cautions

- **Product strategy:** AWS Network Firewall lags behind in terms of features, compared with competing offerings. As a result, AWS relies on partnerships with other vendors, such as Palo Alto Networks, that offer native AWS instances of partner vendor firewalls for customers who see limitations in AWS's firewall.

- **Consolidation:** Gartner clients generally do not consider AWS a desirable vendor for consolidation toward zero trust architecture. AWS lacks a native ZTNA offering. It has a complicated deployment scheme using AWS Virtual Private Cloud (VPC) to achieve microsegmentation, which limits its appeal to shortlists for emerging firewall use cases.

- **Feature gaps:** AWS Network Firewall does not support native network address translation (NAT) features and has no IPv6 support. It also has no ability to detect client-based applications and lacks granular application control.

- **Advanced threat detection:** AWS Network Firewall offers fewer vendor-researched proprietary signatures than other firewalls. Additionally, AWS lacks TLS decryption in its firewall.

Barracuda

Barracuda is a Visionary in this Magic Quadrant. It offers a range of firewall appliances focused on distributed offices and virtual appliances for public clouds within the CloudGen Firewall product line. Branch connectivity is a key market for Barracuda.

Barracuda's security offerings include firewalls, web application and API protection (WAAP) offerings, secure web gateways, ZTNA (for remote access to private applications) and secure email gateways.

Recent updates to Barracuda's firewall line include IoT, OT and cloud security features. Barracuda has, for example, added IPS, URL, content, antivirus and Secure Sockets Layer (SSL) inspection features to its CloudGen WAN product.

Strengths

- **Cloud and branch-office features:** Barracuda's CloudGen Firewall product line offers mature integration with native AWS and Microsoft Azure controls. Barracuda has added a FWaaS product, CloudGen WAN, to address the work-from-home and remote-office use cases. Barracuda has also introduced Secure Connector for IoT connectivity to Microsoft Azure, which is fully manageable via CloudGen WAN.

- **Firewall deployment modes:** Barracuda has delivered products for all major firewall modes — CloudGen Firewall for hardware and virtual; CloudGen WAN for FWaaS; Secure Connector for containerized firewall; and CloudGen Firewall (rugged) for industrial firewall requirements.

- **Pricing:** Barracuda's low-end appliances provide a very good total cost of ownership (TCO). The vendor's pool-based licensing enables administrators to assign software licenses across platforms as needed.

- **IoT features:** Barracuda has increased its ability to secure IoT environments by developing partnerships with Crosser, Nozomi Networks and SCADAfence. Barracuda also has a partnership with Crosser to run edge compute logic on some firewall devices.

Cautions

- **Virtualization:** Barracuda's hardware appliances do not isolate some features, such as VPN, Dynamic Host Configuration Protocol (DHCP), DNS cache and DNS interception, when running multiple virtual instances on the same appliance.

- **Multiple management portals:** Separate management consoles are exclusive to their environments. The FWaaS product, CloudGen WAN, must be managed through Barracuda's cloud management platform. CloudGen physical and virtual appliances must be managed with an on-premises firewall manager called Barracuda Firewall Admin.

- **Product strategy:** Barracuda lacks native EDR and offers only limited third-party integration with endpoint and network security vendors. IPS capability is provided, but it uses technology from Trend Micro on an OEM basis. All IPS signatures are developed via the third party, and the quantity of signatures is inferior to that of competitors.

- **Customer feedback:** Client feedback indicates that Barracuda offers limited reporting on content-filtering modules and that product management is a complex task.

Check Point Software Technologies

Check Point Software Technologies is a Leader in this Magic Quadrant. It is shortlisted for stand-alone firewall use cases by enterprise clients. In addition to firewalls, Check Point offers a broad array of security functionality with mature cloud-based centralized management. This makes it a strong candidate for organizations seeking a security platform solution.

Check Point offers a comprehensive security portfolio that features Quantum-branded hardware appliances and the Maestro hyperscale product line. Check Point packages its FWaaS as part of its Harmony Connect offering.

During the evaluation period for this Magic Quadrant, Check Point released new Quantum Lightspeed appliances, management appliances, midsize/branch firewalls and its "Titan" software release. It also enhanced CloudGuard Workload support to support OpenShift and Docker, while adding microsegmentation.

Strengths

- **Platform strategy:** Check Point offers complementary product lines, which help customers avoid operational complexities and threat coordination gaps that result from managing too many security vendors. All its products can be managed through its cloud-based centralized manager, Infinity Portal.

- **Data center use case:** Check Point has particular traction with large organizations that have large data centers and that appreciate the licensing flexibility and scalability inherent to the Maestro hyperscale line.

- **Pricing:** Check Point's pricing models are favorable for both large- and midsize-enterprise customers. Check Point offers subscription-based pricing to enable large enterprises to avoid major capital expenditure. A single SKU offering for midsize enterprises provides a wide range of security products in one bundle.

- **Advanced threat detection:** Check Point ThreatCloud coordinates malware discovery and intelligence across Check Point's various products and services. Check Point has one of the largest libraries of IPS signatures. It also has a large signature-based database to detect client-side applications.

Cautions

- **Sales and marketing execution:** Check Point is lacking in proactive presales teams, compared with its direct competitors. It also lacks awareness marketing, which results in potential customers looking elsewhere because they are unaware of Check Point's product strategy and updated product portfolio.

- **Product execution:** Check Point's cloud security posture management (CSPM) is not integrated with its on-premises firewall central management offerings.

- **Advanced networking:** Check Point's firewalls lack built-in SD-WAN capabilities. The vendor partners with SD-WAN providers for its FWaaS offering.

- **Product features:** Although Check Point has a large database of malicious URL threat intelligence, it does not support dynamic classification of uncategorized websites. This shortcoming creates operational complexity.

Cisco

Cisco is a Challenger in this Magic Quadrant. Cisco has a large product portfolio and its firewalls are often sold as a part of large deals.

Cisco is an infrastructure vendor. It has different firewall product lines for different deployment use cases: the Cisco Secure Firewall, Cisco Adaptive Security Appliance (ASA), Cisco Secure Workload and Cisco Meraki series. In addition, Cisco offers the Umbrella Secure Internet Gateway (SIG) for FWaaS, and industrial firewalls (the Secure Firewall Industrial Security Appliance [ISA] series).

Major updates in 2021 and 2022 have included native support for TLS 1.3 decryption; support for Cisco Secure Firewall Threat Defense in Alibaba Cloud and Alkira; and the cloud-delivered Secure Firewall Management Center. Cisco also added a managed subscription service for VPN, which enables Cisco to manage scale and change for users, with options including Umbrella SIG support.

Strengths

- **IoT/industrial control system (ICS) security:** Cisco offers IoT security, having formed a partnership with Rockwell to secure ICSs. Cisco has a dedicated IoT research team within the Cisco Talos Intelligence Group. Cisco Secure Firewalls receive building management and medical asset information from Cisco Digital Network Architecture's (DNA's) endpoint analytics.

- **Licensing:** Cisco has a diverse, flexible collection of licensing agreements that allow organizations to deploy whichever Cisco security solutions make sense for their use cases, in deals with favorable commercial terms.

- **Customer feedback:** Clients consider the SecureX cloud-based threat correlation solution platform included with Cisco products a strength. They praise Cisco for continuing to deliver above-average technical support.

- **Distributed-office use case:** Cisco offers Meraki firewalls to connect remote offices. These firewalls benefit from tight integration with Cisco Umbrella for SASE use cases. Ease of deployment is enabled by zero-touch provisioning, which also provides connectivity assurance with VPN monitoring. Cisco also offers a dedicated FWaaS offering through Cisco Umbrella.

Cautions

- **Multiple firewall product lines:** Cisco's firewall portfolio is confusing, with overlapping product capabilities. This can result in deployment of products with different operating systems, which increases learning curves and slows effectiveness.

- **Container firewall:** Cisco lacks a dedicated containerized firewall offering to protect containers. It offers the Cisco Secure Workload microsegmentation product line for container security.

- **Sales execution:** Cisco Secure Firewalls are generally sold as a part of bigger Cisco enterprise license agreement (ELA) deals and lack visibility in pure firewall deals. Although Cisco Meraki MX firewalls are popular for the distributed-office use case, Gartner does not see Cisco firewalls preferred on clients' shortlists for other use cases, such as cloud firewalls and data centers.

- **Customer feedback:** We hear feedback from Gartner clients that Cisco's reseller partners are not recommending Cisco Secure Firewalls because of legacy instability issues and buggy firmware. The firewall management GUI is a work in progress, and some Cisco clients report that the firewall management is comparatively weak. Additionally, clients find Cisco Secure Firewalls expensive when purchased outside an ELA deal.

Forcepoint

Forcepoint is a Niche Player in this Magic Quadrant. It offers firewalls focused on the distributed-office use case but missing features such as FWaaS and cloud-based management. It is mainly considered by distributed enterprises that are looking for appliance-based SD-WAN-enabled firewalls for their sites.

Forcepoint offers Forcepoint ONE (a security service edge [SSE] platform) and network security and data security products. Forcepoint Next-Gen Firewall (NGFW) is the name of its firewall product line.

Major feature updates during the past year related to Forcepoint's firewalls have included support for more public cloud platforms, improved application inspection performance, and the addition of remote browser isolation (RBI) capabilities and subscriptions, and content disarm and reconstruction (CDR) capabilities. Forcepoint has also introduced new firewall models for remote and branch offices.

Strengths

- **Distributed-office use case:** Forcepoint firewalls have built-in advanced SD-WAN capabilities with full IPv6 support, advanced dynamic routing and mature VPN management controls, and active-active clustering. These make them attractive for distributed offices.

- **Integration with Forcepoint ONE:** Forcepoint offers cloud-based service-chaining-based integration through an EasyConnect feature between Forcepoint firewalls and Forcepoint ONE. Features such as RBI and CDR integration strengthen its firewalls' advanced threat detection and prevention capabilities.

- **Mature application control:** Forcepoint offers mature application control, DLP and URL filtering features. Along with support for dynamic categorization of uncategorized sites, service chaining with Forcepoint ONE CASB (a cloud access security broker) makes application control more granular.

- **Customer feedback:** Forcepoint's on-premises firewall manager, the NGFW Security Management Center (SMC), is frequently praised by customers. It is a strong firewall management platform with granular management, zero-touch provisioning, VPN management and logging capabilities.

Cautions

- **Features:** Forcepoint lacks FWaaS features desirable for branch offices and roaming users. Its firewalls have limited IoT protocol support. It does not offer support for 5G on appliances.

- **Visibility:** Forcepoint is not highly visible on the pure-firewall shortlists seen by Gartner, including those for distributed offices, at a time when more vendors are supporting this use case. Forcepoint also lacks visibility for cloud firewall use cases. Additionally, it lacks a dedicated container firewall.

- **Different endpoint agents:** Forcepoint offers two separate endpoint agents, namely the Endpoint Context Agent (ECA) for Forcepoint NGFW and the Forcepoint ONE Endpoint for its SSE solution. This makes it a less attractive vendor for customers looking for ease of management and consolidation.

- **Pricing strategy:** Despite having a large product portfolio, Forcepoint does not offer ELA contracts that cover its firewall product line and other products. The resulting licensing complexity and lack of ELA-based discounting discourages customers from consolidating on Forcepoint.

Fortinet

Fortinet is a Leader in this Magic Quadrant. It leads for appliance-based distributed-office use cases, thanks to its offer of mature SD-WAN and firewall capabilities in a single box.

Fortinet is a network security vendor with a large product portfolio. In addition to FortiGate, its firewall product, Fortinet offers SASE, networking and security operations products.

Major firewall-related updates in 2022 have included the introduction of ZTNA, an in-line sandbox and an in-line CASB. Fortinet has also enabled further integration between FortiGate and its network access control (FortiNAC), and introduced a security operations center (SOC) as a service, offered as a bundle with a FortiGate license.

Strengths

- **Integrated SD-WAN:** Fortinet offers built-in advanced SD-WAN and routing capabilities in FortiGate firewall appliances. Fortinet offers a complete SD-WAN package, with features including forward error correction, packet duplication, and intelligent and dynamic app routing.

- **Hybrid ZTNA deployment:** Fortinet offers flexible ZTNA deployment modes. ZTNA enforcement is part of the FortiGate operating system (FortiOS) and can be deployed on-premises or as a service as part of FortiSASE (a stand-alone offering). The vendor has also introduced an in-line CASB integrated with ZTNA capabilities.

- **Product portfolio:** Fortinet has a large product portfolio. It offers products for networking, network security and security operations. The majority of its products can be managed through a single management interface and offer integration through the Fortinet Security Fabric.

- **Centralized management:** Fortinet offers mature on-premises and cloud-based centralized management through FortiManager and FortiCloud, respectively. These offerings have feature parity and support centralized management of the majority of Fortinet's devices. FortiGate customers like the ease of management and configuration of Fortinet's firewalls.

Cautions

- **Customer feedback:** Feedback from some Gartner clients indicates that FortiGate firewalls do not lead in terms of price/performance. Clients that shortlist Fortinet for midsize-enterprise and data center use cases find its offerings to be more expensive than those of competitors.

- **Dedicated container firewall:** FortiGate lacks a native containerized firewall to protect container workloads. It offers container security through its FortiGate-VM firewalls and Calico integration.

- **Integrated FWaaS offering:** Fortinet lacks an integrated FWaaS offering. It offers FWaaS through FortiSASE as a dedicated product line, without any integration with FortiGate firewalls. FortiSASE comes with a dedicated management interface. Integration of FortiGate's built-in SD-WAN capability with FortiSASE is also lacking.

- **Visibility:** Fortinet appears less frequently on shortlists for cloud firewall and FWaaS use cases than its direct competitors. Fortinet is still considered primarily for its hardware firewall offering.

H3C

H3C is a Niche Player in this Magic Quadrant. It offers a full range of hardware firewalls, known as the SecPath series, for small, midsize and large environments. HC3 focuses on the Chinese market. It offers limited support for cloud providers outside China.

H3C has a diverse portfolio of security products, which includes offerings for the XDR, EDR, distributed denial of service (DDoS) and web application firewall (WAF) market segments. H3C CloudSecPath Firewall Service is its FWaaS offering. H3C is a good choice for enterprises looking for a security stack focused on the Chinese market.

Major updates in the past year have included new appliances in the F100, F1000, F5000 and M9000 lines. H3C has also enhanced its advanced threat detection and prevention features by adding support for dynamic authorization, encrypted transmission and sensitive data protection.

Strengths

- **Scalability:** H3C's firewalls enable highly scalable deployments. Up to 4,096 virtual instances are supported on H3C's hardware appliances. H3C CloudSecPath Firewall Service offers high capacity, with H3C claiming that it supports 200GB of throughput for 200,000 users.

- **Product portfolio:** H3C has a large security portfolio, which is chosen by many enterprises seeking consolidation. H3C offers products such as SecCenter CSAP for endpoint protection and CSAP Threat Discovery for XDR, which make it a desirable vendor for consolidation in China.

- **Firewall deployment modes:** H3C offers a complete firewall product line, including hardware firewall, virtual firewall, FWaaS, containerized firewall and industrial firewall. As a result, it is a good choice for enterprises seeking to consolidate on a single vendor for different firewall deployment modes.

- **Pricing:** H3C's pricing gives it a good five-year TCO, compared with many other vendors. Support is priced reasonably at only 10% of the list price. Some features, such as DLP, are included at no extra cost.

Cautions

- **Cloud-firewall-supported platforms:** H3C offers a cloud firewall for VMware and H3C cloud environments but lacks support for regional cloud providers like Alibaba and Huawei. It also lacks support for AWS, Microsoft Azure and Google Cloud Platform (GCP). H3C offers a container firewall, but it requires NGINX for enforcement.

- **Regional support:** H3C's firewalls rely on partnerships with regional vendors for VPN authentication and EDR integration. H3C offers granular social media controls for mainly local apps, such as WeChat and QQ, and limited support for applications such as Microsoft Office 365.

- **Centralized management:** The firewall central manager can scale to manage only a limited number of devices, as compared with H3C's direct competitors. The platform lacks support for zero-touch provisioning of branch firewalls.

- **Geographic presence:** The majority of H3C's sales are to the Chinese market and a few parts of Southeast Asia. It lacks presence in other regions.

Hillstone Networks

Hillstone Networks is a Visionary in this Magic Quadrant. It is well-suited to fulfill midsize-enterprise use cases in Asia/Pacific and to some Latin American customers, especially cloud-first organizations.

Hillstone's network firewall products are part of its edge protection product family. Hillstone's main offering is a network firewall, but it also offers microsegmentation, endpoint and server security, a WAF, an application delivery controller (ADC), XDR and DLP.

Hillstone has recently released several new hardware and virtual firewalls, as well as a virtual firewall that integrates with VMware NSX-T. New features include DNS security and a cloud data lake.

Strengths

- **Cloud-focused product strategy:** Hillstone has a cloud-first strategy that supports AWS, Microsoft Azure, GCP and Alibaba Cloud, as well as multiple China-based public clouds. Hillstone offers a microsegmentation solution and CloudArmour, a container firewall that can work in Kubernetes environments.

- **Advanced features:** Hillstone's ZTNA capabilities are integrated into all its network firewalls. A Hillstone NGFW acts as the ZTNA gateway, while a Hillstone SSL VPN client can be upgraded to a ZTNA endpoint. An additional subscription license is required to activate the ZTNA feature. Hillstone does ZTNA enforcement on the firewall.

- **IoT security:** Hillstone's IoT security can proactively detect IoT devices such as webcams, multimedia players and game consoles. It can provide risk analysis and control, and threat detection for traffic associated with these IoT assets, as inclusive features.

- **Geographic strategy:** Hillstone is using its strength in China to fund targeted sales opportunities in other regions. The number of Hillstone customers in Latin America and North America is small but growing.

Cautions

- **Cloud security:** Hillstone integrates with several public clouds using Hillstone virtual appliances, but does not offer CSPM to manage cloud-native firewall policies. Nor does it manage native security controls in SDN infrastructures such as VMware NSX and Cisco Application Centric Infrastructure (ACI).

- **Product strategy:** Hillstone's IPS capabilities are undifferentiated. Hillstone has a relatively small threat research team to develop custom rules for "in the wild" threats. Relative to most competitors, Hillstone has a small client-based application database, which limits the breadth of its Layer 7 awareness.

- **Price/performance:** Although Hillstone's firewall appliance prices may seem low, they are not low compared with those of many competitors. Throughput on the lowest-end firewalls is very low, and data center firewall prices are relatively high, considering the volume of traffic they can process.

- **Customer feedback:** Hillstone clients identify a lack of high-throughput and high-performing hardware devices as a weakness, compared with other Chinese regional vendors within the Chinese market.

Huawei

Huawei is a Challenger in this Magic Quadrant. A large product portfolio makes Huawei a desirable vendor for customers who want to consolidate. Huawei has different firewalls for different use cases. It often wins deals based on its price/performance.

Huawei is a large infrastructure vendor with a diverse product portfolio. Its firewalls, which include the USG series for enterprise and the Eudemon series for carriers, are part of its network security product portfolio.

Major updates in 2022 relating to Huawei's firewalls have included enhancements to routing, SD-WAN and sandboxing capabilities.

Strengths

- **Scalability:** Huawei has a large base of carrier and data center customers. As a result, it offers highly scalable appliances. Of all the vendors evaluated in this Magic Quadrant, Huawei offers support for the most virtual firewall instances in its dedicated hardware appliance models and scalable management console.

- **Cloud-native firewall:** Huawei offers a cloud-native firewall service for Huawei Cloud, as well as a container firewall service called the Container Guard Service (only for Huawei Cloud). The container firewall offers features such as container runtime security and image security with vulnerability management. It can be managed from a centralized console within Huawei Cloud.

- **Advanced threat detection:** Huawei offers threat correlation capabilities between its firewall, native EDR and XDR platforms. Clients can also utilize managed detection and response (MDR) services offered directly by Huawei, which are sold as Qiankun Border Protection and Response.

- **Pricing:** Huawei's firewalls have a competitive price/performance ratio. Their TCO is one of the lowest in the market. Huawei often wins deals on this basis.

Cautions

- **Regional partnerships:** Huawei's partners are mostly limited to Chinese companies. For example, its ZTNA offering can integrate with Bamboo Cloud's IAM solution, while, for EDR, Huawei has partnered with Jiangmin and Leagsoft.

- **Offerings outside Huawei Cloud:** Although Huawei offers virtual cloud firewall, container firewall and microsegmentation products, these are primarily for Huawei Cloud. Only recently has Huawei partnered with Microsoft Azure for a cloud firewall.

- **IoT security:** Huawei firewalls offer only basic IoT-related security. They lack features such as IoT discovery. Huawei only offers limited signature-based protection of regular IoT vulnerabilities through the IPS signature database in its firewalls.

- **ELA:** Despite having a large product portfolio, Huawei does not offer ELA-based deals. An ELA would make deals involving multiple years and multiple products easier for customers to understand and accept.

Juniper

Juniper is a Challenger in this Magic Quadrant. It has a broad firewall line covering many use cases and deployment types, including FWaaS and container firewalls. We typically see Juniper firewalls shortlisted along with Juniper networking products, which limits their market penetration.

Juniper offers a broad range of products, including networking and security products. It offers appliance-based firewalls in the SRX, vSRX and cSRX product lines. It also has a FWaaS offering. Other products provide security information and event management, DDoS mitigation and threat intelligence.

Recent updates have included the introduction of Security Director Cloud, Secure Edge (an SSE product) and Cloud Workload Protection. Juniper has also gained a cloud-based network access control product with the acquisition of WiteSand.

Strengths

- **Firewall deployment use cases:** Juniper's firewall product line, the SRX series, includes hardware appliances and virtual appliances (vSRX) with native mature SD-WAN support. A FWaaS is provided with the Secure Edge product, and a full-featured containerized firewall is included in the cSRX line.

- **Platform approach:** Juniper offers a single console to manage all its security products through its Security Director and Security Director Cloud. Juniper also offers Advanced Threat Prevention and SecIntel as shared threat intelligence offerings between its networking and firewall product lines.

- **IoT and OT security:** Juniper has demonstrated a focus on IoT security by enhancing its automated device fingerprinting and control. Partnership with Dragos and SEL provide threat detection and response capabilities for industrial applications within OT and SCADA environments.

- **Scalability:** Juniper offers high-throughput firewalls that maintain good throughput even while decrypting traffic. The Junos Space Security Director and Juniper Security Director Cloud, a centralized manager, can manage up to 25,000 Juniper devices, including firewalls, switches and routers.

Cautions

- **Visibility:** Despite having firewall offerings for all deployment use cases, Juniper is not as visible as its direct competitors on customer shortlists seen by Gartner. Juniper firewalls are shortlisted primarily by telecom carriers or for consolidation with Juniper's other network product lines.

- **Market responsiveness:** The network security market is highly competitive, with aggressive competition between vendors to identify key emerging use cases, such as FWaaS, ZTNA, cloud

security, SSE and security operations. Despite being a large network vendor, Juniper has been slow to identify such use cases and to introduce products for them.
- **Product strategy:** Juniper lacks a strong in-house security product portfolio, compared with direct competitors that are expanding their security product offerings aggressively. As a result, Gartner clients do not consider it a desirable candidate for security vendor consolidation.

- **Customer feedback:** Gartner clients identify slow responsiveness and a lack of innovation for emerging security use cases as reasons not to shortlist Juniper. They also find its prices high, relative to those of competitors. SD-WAN and DLP features are available, but at added cost.

Microsoft

Microsoft is a Niche Player in this Magic Quadrant. Its Azure Firewall is considered mainly by existing Microsoft clients seeking consolidation. Application teams looking for native firewalls for seamless integration with Azure workloads also prefer the Microsoft Azure Firewall.

The Microsoft Azure Firewall is available via two subscriptions: Standard and Premium. It can be centrally managed by Azure Firewall Manager and monitored using Azure Monitor and Microsoft Sentinel.

Microsoft continues to invest in security, as shown by the addition of DDoS management to Azure Firewall Manager and of WAF policies to Azure Firewall Manager. Additionally, Microsoft has added an IPS to its Premium subscription.

Strengths
- **Vendor consolidation:** Microsoft firewalls are widely considered by existing Microsoft customers who want to consolidate on a single vendor. Microsoft offers a range of security services, including Azure Firewall, Azure Web Application Firewall and Azure Active Directory, which can be deployed together.

- **Ease of use:** Microsoft Azure Firewall integrates seamlessly with other Azure-hosted services. It is less complex than third-party firewalls to deploy, as it is an in-line offering with inbuilt sizing and scaling.

- **Sales execution:** Microsoft has capitalized on customers' shifting of workloads to Azure by offering a simple firewall that meets basic needs. Gartner is seeing clients consider Azure Firewall for Azure workloads, and this Microsoft offering frequently competes with products from dedicated firewall vendors.

- **Customer experience:** Users identify ease of deployment as the leading reason to use Microsoft Azure Firewall. A strong secondary reason is its tight integration with the Azure ecosystem, which assists DevOps. Customers also appreciate Microsoft's credibility as a vendor and its support for the product.

Cautions

- **Innovation:** Microsoft is focused on integrating Azure Firewall with native Azure offerings, and lags behind in terms of introducing features to support emerging cloud firewall use cases. It lacks a dedicated container firewall offering. Microsegmentation is handled via security tags, rather than a firewall product.

- **Feature gaps:** Microsoft Azure Firewall lacks multiple features that are desirable in a cloud firewall and that are offered by competitors. There is no support for IPv6, no sandbox and no signature-based application control.

- **Performance:** Network traffic throughput drops by 90% when an IPS with TLS is enabled. Microsoft does, however, provide an option to add sites manually to the list in order to bypass TLS decryption.

- **Customer feedback:** Customers indicate that the Premium firewall subscription is expensive, documentation is subpar, with a lack of training material, and logging lacks support for debugging issues.

Palo Alto Networks

Palo Alto Networks is a Leader in this Magic Quadrant. It has the most visible firewall for different firewall use cases, judging from Gartner client inquiries. With the recent introduction of the PA-400 series, Palo Alto Networks' firewalls have become good candidates for use by midsize enterprises.

Palo Alto Networks is a security vendor with a large product portfolio. In addition to its most popular firewall product line, the PA-Series, the vendor has SSE, cloud security and security operations product lines.

Major firewall-related updates over the past year have included the release of two major firmware releases with enhancements to URL filtering, DNS security, IoT security and threat prevention. The vendor has also introduced AIOps and enhanced the DLP features of its firewalls.

Strengths

- **Product portfolio:** Palo Alto Networks has a large product portfolio. Gartner often sees contracts from this vendor for multiple product lines, in addition to firewalls. Prisma Access (SASE) and Cortex Data Lake (XDR) are frequently shortlisted along with firewalls.

- **Deployment modes:** Palo Alto Networks supports multiple forms of firewall deployment, with its PA-Series (hardware firewalls), VM-Series (virtual firewalls), Prisma Access (FWaaS), Cloud NGFW (a cloud-native firewall for AWS) and CN-Series (containerized firewalls). This makes it a good choice for hybrid environments, where clients want a single firewall provider.

- **Advanced security features:** Palo Alto Networks' firewalls score highly for advanced security features. The vendor offers strong threat detection and prevention capabilities. Its IoT Security subscription offers autodiscovery of IoT devices. Palo Alto Networks also offers advanced DNS security and 5G security features.

- **FWaaS:** Palo Alto Networks' FWaaS offering, Prisma Access, continues to mature and supports full SSE capabilities, including a secure web gateway (SWG), a CASB and ZTNA. It can be managed as a plug-in for Panorama (an on-premises centralized manager) or as a stand-alone cloud-based management offering.

Cautions

- **Technical support:** Gartner has received consistent feedback from Palo Alto Networks customers indicating a decline in the quality of its technical support, with especially long escalation cycles being associated with Level 1 support. As a result, customers often feel the need to upgrade their support to a higher tier that offers a faster SLA but is more expensive.

- **Cloud-based manager:** Palo Alto Networks' cloud-based firewall manager, used for distributed-office and centralized-management use cases, is not on a par with on-premises management. Its cloud-based manager is used primarily for the Prisma Access product line and "generation 4" models of hardware.

- **Customer feedback:** A few Gartner clients have reported connectivity and routing issues with Prisma Access services. This feedback comes particularly from users of its FWaaS and of the GlobalProtect service of Prisma Access (as it relates to firewall clients).

- **Opacity of ELA contracts:** Palo Alto Networks offers multiple types of license, such as an ELA and credit-based licenses, but its quotations often lack transparency. They mostly include bulk pricing and lack clarity in terms of itemized part numbers with itemized costs.

Sangfor Technologies

Sangfor Technologies is a Visionary in this Magic Quadrant. This China-based vendor appeals to enterprises in Asia/Pacific and EMEA (especially the Middle East) that want to consolidate their security products by using a single vendor.

Sangfor's network firewall products are all part of the Next Generation Application Firewall (NGAF) product line, which also includes WAF functionality. In addition to network firewalls, Sangfor has a broad range of security offerings for WAAP, SASE, ZTNA, IAM, endpoint security, microsegmentation and cloud workload protection.

Sangfor has recently released several new hardware firewall appliances. New features include a cloud deception subscription to improve attack detection. Sangfor also offers a fully integrated network firewall with its ZTNA and SASE products.

Strengths

- **Platform approach:** Sangfor builds products that can be managed together. Its Platform-X cloud management platform can manage Sangfor's network firewall, Endpoint Secure and microsegmentation solutions, together with Sangfor's SWG and SD-WAN capabilities.

- **IoT security:** As part of its Essential License Suite, Sangfor offers differentiated IoT signatures, including support for IP camera protocols. Sangfor supports IoT asset classification, access control, protocol identification and control, weak-password detection and IoT vulnerability detection on surveillance networks.

- **Scalability:** Sangfor Central Manager, the vendor's on-premises central management appliance, is highly scalable. A large number of devices can be administered from a single console.

- **Pricing strategy:** As a vendor with many large customers, Sangfor uses its ELA as a strategic product packaging tool. It typically offers heavy discounts, flexible terms on virtual firewall deployments, and new product additions during the ELA term, with a true-up at renewal time.

Cautions

- **Advanced networking:** Sangfor's firewalls lack 5G support. This is a significant shortcoming for customers in China, several other Asia/Pacific countries and parts of the Middle East, where 5G infrastructure is mainly found.

- **Public cloud integration:** Sangfor lacks integration with the Microsoft Azure and GCP public clouds that are popular in many regions.

- **Threat detection:** Sangfor has fewer IPS signatures than other firewall vendors evaluated in this Magic Quadrant, and no machine learning analysis is performed in conjunction with the IPS to improve detection efficacy. In addition, Sangfor lacks integration with third-party tools to improve malware detection.

- **Geographic strategy:** Sangfor has very little presence outside Asia and the Middle East. Other regional competitors evaluated in this Magic Quadrant are more often considered and deployed in Latin America.

SonicWall

SonicWall is a Niche Player in this Magic Quadrant. It is a strong candidate for selection by midsize enterprises, for which it offers strong security and represents good value. Its native SD-WAN capabilities with a FWaaS make it a good choice for distributed-office and remote access use cases.

SonicWall offers three hardware appliance firewall product lines — the TZ, NSa and NSsp series — and a virtual appliance firewall product line, the NSv series. In addition to firewalls, SonicWall sells integrated EDR, secure email gateway, ZTNA and CASB capabilities.

Recent updates include enhancements to the centralized manager, including rule optimization and SD-WAN workflow to simplify provisioning of branch-office firewalls. SonicWall has also introduced centralized management for SonicWall Switch, SonicWave Wireless Access Points and SonicWall Capture Client.

Strengths

- **Distributed-office use case:** SonicWall offers native SD-WAN capabilities in all its firewall models and the SonicWall Network Security Manager. It also offers Cloud Edge Secure Access, a SASE offering with FWaaS, ZTNA, network access control and CASB features desirable for the distributed-office use case.

- **Pricing:** SonicWall offers competitive pricing, which makes it a good choice for midsize enterprises. SD-WAN functionality is included in all its appliances at no additional cost. DLP functionality is part of the base package, also with no additional cost.

- **Customer feedback:** Customers have praised SonicWall's single management interface for managing different SonicWall products. Additionally, they have identified low TCO as a reason to choose SonicWall firewalls.

- **Centralized management:** SonicWall's Capture Security Center (CSC) is a "single pane of glass" management portal for SonicWall products, including its firewalls and Cloud Edge Secure Access offering. It simplifies administration.

Cautions

- **Visibility:** Gartner sees SonicWall primarily on the firewall shortlists of midsize enterprises. It lacks visibility for other use cases, especially the distributed-office use case (despite having native SD-WAN capabilities and an FWaaS offering) and the data center use case.

- **Product features:** SonicWall supports only limited virtual instances — desirable for data center use cases — on its hardware appliances. It supports fewer categories of web application than other vendors evaluated in this Magic Quadrant. SonicWall lacks a native XDR offering; instead, it offers integration with third-party XDR platforms.

- **Cloud firewall:** SonicWall's support for public clouds lags behind that of other vendors in this Magic Quadrant, with support for only AWS and Microsoft Azure; there is no support for GCP. A pay-as-you-go option is not available for Azure. SonicWall lacks a container firewall and a microsegmentation offering.

- **Customer feedback:** SonicWall clients have indicated that the firewall product's reporting capabilities are limited and lack granularity. They have also experienced long delays after contacting technical support.

Sophos

Sophos is a Niche Player in this Magic Quadrant. Its product strategy and platform-based approach, focused on the needs of midsize enterprises, offer strong integration between its firewalls and EDR. Sophos is gradually expanding its cloud security product lines.

Sophos has network security, endpoint security, cloud security and MDR offerings. Its firewall offerings come under different product lines. Sophos' firewalls and Intercept X endpoint security offering are its most popular products.

Major firewall-related updates over the past year have included the introduction of the Sophos XGS series of hardware firewalls, and the launch of a Sophos ZTNA offering and new software subscriptions. Sophos has also improved XGS performance and enhanced SD-WAN orchestration.

Strengths

- **Platform approach:** Sophos offers its firewall, EDR and XDR as a unified platform with strong integration, centralized management and correlation capabilities. It offers a single cloud console with a single endpoint agent to manage both products.

- **Midsize-enterprise use case:** Sophos' strategy and sales execution focuses on midsize enterprises. In addition to consolidating its firewall and EDR functionality, Sophos has introduced managed threat response and rapid response services for clients looking to outsource MDR services.

- **Cloud-based centralized manager:** Sophos offers a single, cloud-based centralized manager to manage all its products. This makes management easier.

- **Customer feedback:** Customers often identify Sophos' customer support and mature product documentation as key strengths. Sophos has introduced context-sensitive help, guided tutorials and embedded how-to videos to further improve the product administration experience.

Cautions

- **Visibility:** Sophos is generally visible to midsize enterprises, but is less commonly used for other firewall use cases. This is despite Sophos having a separate offering for ZTNA and a cloud firewall that includes a container firewall.

- **ELA:** Despite having a broad product portfolio, Sophos does not offer ELA pricing, even though this is desired by clients aiming to consolidate products with the same vendor. Instead, Sophos offers a simpler multiyear consumption model.

- **Features:** Sophos does not offer a FWaaS, even though one is desirable for use cases involving branch offices and roaming users. It also lacks support for 5G in its firewalls, which are SD-WAN-enabled.

- **Customer feedback:** As competition between vendors grows in the midsize-enterprise market, some Gartner clients find Sophos expensive, compared with other vendors that sell to midsize enterprises.

WatchGuard

WatchGuard is a Niche Player in this Magic Quadrant. It delivers firewalls for midsize-enterprise and distributed-enterprise use cases. In addition to the Firebox firewall, WatchGuard has a virtual appliance (FireboxV) and a virtual appliance designed specifically for public cloud environments (Firebox Cloud).

WatchGuard Dimension is this vendor's on-premises firewall management solution. All WatchGuard security products can be managed by WatchGuard Cloud, its cloud-based console. Other products in WatchGuard's security portfolio offer multifactor authentication (MFA), secure Wi-Fi and endpoint security.

WatchGuard has recently released several new firewall hardware appliances. Examples of new features include Firebox integration with WatchGuard's MFA and secure Wi-Fi products, and load-sharing capabilities for the vendor's on-firewall SD-WAN functionality.

Strengths

- **Product strategy:** In the past few years, WatchGuard has switched from a traditional value-added reseller (VAR)-based go-to-market strategy to a managed service provider (MSP)-focused strategy. This refocus has led the vendor to make WatchGuard Cloud service-provider-friendly and easy to use, while also being scalable across multiple end-user customers per service provider.

- **Endpoint integration:** WatchGuard's Firebox firewall is managed in conjunction with its endpoint security products. The vendor has a process called ThreatSync that collects event data from WatchGuard firewalls, endpoint sensors and threat intelligence feeds, analyzes the collective data, and assigns threat scores.

- **OT security:** WatchGuard has a ruggedized network firewall that is sometimes used in certain manufacturing and utility environments. The vendor also includes SCADA signatures in its Basic Security Suite and Total Security Suite feature bundles.

- **Pricing strategy:** Under the FlexPay licensing model, WatchGuard offers the choice to purchase its firewalls using upfront payments, WatchGuard Points or WatchGuard pay-as-you-go, which is unique in the traditional capital-expenditure-based firewall appliance market.

Cautions

- **IaaS security:** WatchGuard has public-cloud-friendly firewalls only for AWS and Microsoft Azure. In this regard it lags behind most competitors, which usually support three or more infrastructure as a service (IaaS) providers. The lack of GCP support limits WatchGuard's opportunities to serve "born in the cloud" midsize enterprises, which sometimes choose Google as their infrastructure provider.

- **FWaaS and ZTNA:** Many small and midsize Gartner clients inquire about FWaaS as an alternative to traditional branch-office firewalls. WatchGuard, however, does not offer a FWaaS. It also lacks a ZTNA offering.

- **Product strategy:** WatchGuard lacks offerings for emerging cloud security use cases, such as containerized firewall and microsegmentation. As a result, it lacks visibility in shortlists seen by Gartner, beyond those of midsize organizations looking for hardware firewalls.

- **Advanced networking:** At the time of this analysis, WatchGuard has not delivered any 5G-supporting firewalls. This limits its uptake in many regions that have built extensive 5G infrastructure.

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

None.

Dropped

- Cato Networks
- Versa Networks

Inclusion and Exclusion Criteria

The inclusion criteria represent the specific attributes that Gartner analysts thought it necessary for vendors to have 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 must have hardware/virtual appliances or cloud-native firewalls as their primary firewall products.
- Vendors must have presence at least in three of the following regions, including their home region: Asia/Pacific, North America, Latin America, Europe, Middle East.
- Vendors offering a hardware appliance/virtual appliance as their primary firewall product offering must have generated at least $70 million in hardware appliance/virtual appliance firewall-only revenue in 2021.
- Vendors must have a track record of meeting the needs of public cloud use cases.
- Gartner analysts must have assessed that the vendors can effectively compete in the network firewall market.
- Gartner analysts must have determined that the vendors are significant players in the network firewall market, due to their market presence, competitive visibility or technological innovation.
- Vendors must have the ability to meet more than one network firewall deployment use case mentioned in the Market Definition/Description section.
- Public cloud vendors must have a dedicated firewall offering.

Exclusion criterion:

- Gartner considered vendors that offer FWaaS as their primary firewall product line to be ineligible for inclusion in this Magic Quadrant.

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 vendors' Ability to Execute.

Product or 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.

Subcriteria:

- Ability of product to meet the needs of, and specialize in, different network firewall use cases.
- Platform approach.
- Support is evaluated by the quality, breadth and value of an offering (or offerings) specifically in relation to enterprise and cloud use cases.

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.

Subcriteria:

- Customer feedback on pricing.
- Transparency of contracts.
- Bundled-pricing models that are clear and easy to understand.
- Competitive TCO.
- Strong presale and postsale support and services.

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.

Subcriteria:

- Timely introduction of new features to meet customers' requirements.
- Ability to support emerging use cases, such as SASE, cloud security and IoT security.
- Timely partner integrations to support customers' demands.

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.

Subcriteria:

- Visibility of the vendor on clients' shortlists.
- Extent to which end users are migrating away from the vendor.
- Extent to which the vendor's marketing faces direct competition.
- End users' awareness of the vendor's brand.

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.

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. Trending feedback — positive or negative — on a vendor's product(s) or support — is weighted highly as well.

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.

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 (December 2022)

Completeness of Vision

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

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.

Subcriteria:

- Ability to understand and add features in response to customers' requirements for different use cases.
- Ability to understand and respond to customers' product- and market-related requirements.
- Ability to meet timelines imposed by customers' requirements.

- Support for hybrid environments and different firewall deployment use cases, platform approach, centralized management and visibility, cloud security, cloud workload protection, and automation.

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

Subcriteria:

- Ability to provide clear messaging that resonates with customers' use cases and requirements.
- Ability to communicate effectively with sales and distribution channels, end users and different kinds of buyers on features, product firmware, vision and focus on evolving use cases, in order to build a brand.
- Strong, clear messaging on evolving use cases.

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

Subcriteria:

- Effective sales and pricing models to meet the requirements of clients for different deployment use cases.
- Clear and transparent pricing models.
- A comprehensive channel and partner strategy to sell to multiple deployment use cases.
- Approach to the network security and/or cloud workload buying center.

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.

Subcriteria:

- Development of strong features to enhance threat prevention.
- Integrated features and automation, rather than a broad product portfolio with overlapping products.
- Strong features and enforcements to support all the network firewall use cases.

- Mature product integrations with partners to enhance network firewall capabilities for environments featuring, for example, OT, branches/campuses, cloud security and work-from-home users.

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.

Subcriteria:

- Platform approach.
- Strong vision and exceptional features for particular firewall deployment use cases.
- Feature maturity.
- Integration with overlapping products.
- Use of technology to detect and prevent threats.
- Exceptional, differentiating features and innovation to support one or more network firewall use cases.

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.

Table 2: Completeness of Vision Evaluation Criteria

Evaluation Criteria	***Weighting***
Market Understanding	High
Marketing Strategy	Medium
Sales Strategy	Medium
Offering (Product) Strategy	High

Evaluation Criteria	***Weighting***
Business Model	Medium
Vertical/Industry Strategy	NotRated
Innovation	High
Geographic Strategy	Medium

Source: Gartner (December 2022)

Quadrant Descriptions

Leaders

The Leaders quadrant contains vendors that can shape the market by being the first to introduce additional capabilities and raise awareness of the importance of those capabilities. Leaders have the potential to meet enterprises' 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 may be 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 for, or prominence in, a particular use case, such as those involving data centers, telcos, distributed enterprises, midsize enterprises and 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

As networks evolve, network firewall vendors continue to expand their product portfolios to cover overlapping security markets and attract buyers seeking consolidation. However, buying from the same vendor does not necessarily guarantee simplicity and centralized management.

Appliance-based firewalls remain relevant for multiple firewall use cases. Hardware appliance renewals continue to be pretty stable. There is demand for high-throughput hardware firewalls, especially for data center and enterprise perimeter use cases.

FWaaS is in growing demand for remote use cases, whether they involve branch offices or homes. Consolidation is also apparent in this regard, with SSE, which combines CASB, ZTNA and SWG functionality, becoming more of a requirement. Branches with high throughput requirements or compliance limitations continue to choose hardware appliances for the branch-office use case. (Stand-alone FWaaS vendors do not appear in this year's Magic Quadrant, as demand for their products is insufficient to warrant inclusion.)

Vendors innovating for cloud security use cases are gaining traction, as there is a strong demand for cloud firewalls (both cloud-native firewalls and container firewalls). Hence we include cloud service providers in this Magic Quadrant.

The sales execution/pricing criterion is weighted significantly because of consistent feedback from clients about its importance and frequent increases in the prices of network firewalls. More complex contracts, higher renewal costs and higher TCO are causing dissatisfaction among clients.

Market Overview

The network firewall market remains one of the largest security markets, and has been evolving along with the broader security market. As a result, multiple factors now drive the network firewall market.

The rise of hybrid environments is the key factor behind vendors' introduction of multiple firewall deployment types, such as FWaaS and cloud-native. There is growing demand to secure on-premises environments, multiple cloud environments and remote users with firewalls.

Interest in zero trust is favoring the selection of single firewall vendors that can help enterprises achieve a ZTNA, so that they do not have to use multiple vendors. Clients expect mature integration capabilities when purchasing overlapping technologies from the same vendor.

There is huge interest in visibility and control of east-west segmentation policies and enhanced security operation integrations.

Advanced security capabilities remain a key driving factor, as threat vectors are using more sophisticated means of attacking hybrid workforces and cloud networks. Most vendors are trying to develop or acquire products that offer these capabilities, but they face strong competition from best-of-breed vendors that offer granular capabilities for this specific use case.

The network firewall market has evolved to include the following segments, each of which has a specific set of features:

- **Cloud firewalls:** These firewalls from cloud infrastructure vendors are designed for cloud-native deployment as separate virtual instances or in containers. Container firewalls can also secure connections between containers.

- **Hybrid mesh firewalls:** These are platforms that help secure hybrid environments by extending modern network firewall controls to multiple enforcement points, including FWaaS and cloud firewalls, with centralized management via a single cloud-based manager.

- **Firewall as a service (FWaaS):** A FWaaS is a multifunction security gateway delivered as a cloud-based service, often to protect small branch offices and mobile users.

Other key observations about this market:

- Customers continue to give negative feedback about the increasing price of network firewall offerings. Only regional vendors seem to be offering simple and competitive pricing. Other vendors continue to increase their prices regularly.
- Advanced threat detection and prevention remains an important shortlisting criterion. Network firewall vendors have been enhancing their features in this area, with key enhancements relating to IoT security and DNS security.
- More vendors have introduced cloud firewall offerings, although these have differing levels of maturity. Container firewalls are still offered by only a limited number of vendors.
- Vendors may identify the introduction of FWaaS offerings as a priority, but more are introducing ZTNA and/or SWGs first.
- Although vendors claim strong integration between their network firewalls and other overlapping product lines, Gartner finds these integrations to be very basic.
- Data center network firewall vendors continue to introduce higher-performing boxes.
- All the firewall vendors evaluated in this Magic Quadrant offer native SD-WAN capabilities in their firewall appliances.
- As midsize enterprises are becoming hybrid-environment organizations, their need for mature security is prompting a rise in security budgets. As a result, midsize-enterprise firewall use cases seem to be growing, with more vendors introducing appliances and bundled licensing to attract these enterprises. There is now strong competition to win their business.

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.

Stratégie géographique : la stratégie du fournisseur pour orienter les ressources, les compétences et les offres afin de répondre aux besoins spécifiques des zones géographiques en dehors de la zone géographique "d'origine" ou d'origine, soit directement, soit par l'intermédiaire de partenaires, de canaux et de filiales, selon les besoins de cette zone géographique et de ce marché.

Learn how Gartner can help you succeed

Become a Client

© 2023Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. and its affiliates. This publication may not be reproduced or distributed in any form without Gartner's prior written permission. It consists of the opinions of Gartner's research organization, which should not be construed as statements of fact. While the information contained in this publication has been obtained from sources believed to be reliable, Gartner disclaims all warranties as to the accuracy, completeness or adequacy of such information. 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." Gartner research may not be used as input into or for the training or development of generative artificial intelligence, machine learning, algorithms, software, or related technologies.

© 2023 Gartner, Inc. and/or its Affiliates. All Rights Reserved.