Magic Quadrant for Network Firewalls

Published 9 November 2020 - ID G00456338 - 55 min read

Network firewalls are evolving to secure newer use cases, including cloud and sudden shift to growing remote workforce. Firewall vendors have been slow in responding to growing hybrid networks with a lack of appropriate product offerings and related support.

https://www.gartner.com/explore/magic-quadrant

Strategic Planning Assumptions

By 2025, 30% of new distributed branch office firewall deployments will switch to firewall as a service, up from less than 5% in 2020.

By year-end 2024, 25% of firewall end-user spend will be contained within larger security "platform" deals delivered by enterprise license agreements (ELAs), up from less than 5% today.

Market Definition/Description

Gartner defines the network firewall market as composed primarily of firewalls offering bidirectional controls (both egress and ingress) for securing networks. These networks can be on-premises, hybrid (on-premises and cloud), public cloud or private cloud. The product has the capability to support one or more firewall deployment use cases, such as perimeter, small and midsize businesses (SMBs), data center, cloud, and distributed offices.

This market is no longer restricted to appliance-only vendors. and extends to vendors offering virtual versions and firewall as a service (FWaaS), offered as native firewall controls or dedicated offerings by public and private cloud vendors.

Network firewalls can also offer additional capabilities, such as application awareness and control, intrusion detection and prevention, advanced malware detection, and logging and reporting.

This Magic Quadrant includes the following types of network firewalls:

- Purpose-built physical appliances
- Virtual appliances
- Embedded firewall modules
- Firewall controls delivered from infrastructure as a service (IaaS) platform providers
- Dedicated FWaaS (Note: FWaaS is a service directly hosted and sold by the vendor, and is not a hosted firewall service offered by managed security service providers [MSSPs], telcos or any other partner).

Magic Quadrant

Figure 1. Magic Quadrant for Network Firewalls

Source: Gartner (November 2020)



Vendor Strengths and Cautions

Barracuda

Barracuda is a Niche Player in this Magic Quadrant. Its firewall product line is called Barracuda CloudGen Firewalls. It has dedicated firewalls for operational technology (OT) and industrial control system (ICS) use cases.

This year, Barracuda has introduced Barracuda CloudGen WAN, hosted on Microsoft Azure as a secure SD-WAN offering. Other updates include Firewall Insights, which is Barracuda's analytics and reporting product offering, and enhancements to cloud IaaS support and Internet of Things (IoT) security.

Barracuda focuses on public cloud IaaS and distributed office use cases for its firewalls. Hence, Barracuda CloudGen Firewalls are a good candidate for enterprises looking for mature public IaaS firewall features and integrated native SD-WAN and VPN features.

Strengths

- **Market execution:** Barracuda CloudGen Firewalls offer better support features for Amazon Web Services (AWS) and Microsoft Azure platforms as compared to other firewalls. These capabilities include support for Azure Operations Management Suite (OMS), Azure Security Center (ASC), Azure Sentinel and AWS Amazon CloudWatch, which most other firewall vendors fail to offer.
- **Product strategy:** Barracuda is a good shortlist candidate for the distributed office use case, with integrated SD-WAN and mature VPN capabilities. The vendor regularly introduces enhancements to these features. Recently, it introduced Barracuda CloudGen WAN, hosted on Microsoft Azure as a secure SD-WAN offering.
- **Pricing:** Barracuda CloudGen Firewalls win on pricing versus features. Their subscriptions are bundled and come with inclusive basic technical support. This makes them desirable firewalls for SMBs, for which pricing is one of the key shortlisting criteria.
- **Product strategy:** Apart from dedicated firewalls for OT and ICS use cases, Barracuda also offers secure connector products for IoT device connectivity. These connectors provide centralized management and access through Barracuda's firewall centralized manager — Firewall Control Center — of various IoT devices. CloudGen Firewall products offer support for OT protocols such as S7+, IEC 61850, IEC 60870-5-105, Modbus and DNP3.

Cautions

- **Product strategy:** Despite Barracuda offering multiple security product lines, it offers no integration with CloudGen Firewalls, hence not offering operational simplicity to clients consolidating toward a single vendor.
- **Sales execution:** Gartner doesn't see ELA deals promoted by the vendor for clients that want to consolidate toward Barracuda for their multiple security solutions. All the firewall deals are generally stand-alone ones, while other vendors that offer multiple security product lines are promoting ELAs for pricing simplicity for their clients.
- **Market responsiveness:** Despite a strong focus on the distributed office use case, the vendor doesn't offer a cloud-based firewall manager. Barracuda has recently launched a

secure SD-WAN service hosted in Microsoft Azure that includes cloud-based management not currently available with its CloudGen Firewall.

- **Customer feedback:** Gartner clients have reported below-satisfactory technical support feedback, contradictory to excellent support feedback that clients used to cite a few years ago.

Check Point Software Technologies

Check Point Software Technologies is a Leader in this Magic Quadrant. Its firewall product is its main security product line; its new Quantum Security Gateways series offers firewalls for all use cases, including containers. CloudGuard Connect is the FWaaS offering. Major updates include extending support for cloud security and enhancements around threat prevention, performance and support for IoT security. The vendor has also introduced the centralized cloud-based management portal Smart-1 Cloud, Infinity portal and FWaaS.

Check Point firewalls are good shortlist candidates for enterprises with a cloud security focus. The vendor also offers high-performing firewalls for the data center use case. Check Point leads in centralized management capabilities and integration with its endpoint security and mobile security product lines.

Strengths

- **Centralized management:** Launched in April 2020, and still too recent to have received customer feedback, Smart-1 Cloud offers feature parity with the Smart-1 on-premises console. Check Point Smart-1's console appeals especially to managed security service provider customers and prospects, and distributed enterprises.
- **Policy management:** In the hybrid world, where firewall vendors face stronger competition from network security policy management tools for their ability to manage IaaS native controls and multiple brands, Check Point has a strong base of faithful and satisfied users, praising the policy editors and the recent improvement in the R80.x versions.
- **Product strategy:** Check Point has accelerated the pace of its cloud security execution, including the integration of CloudGuardDome9, a cloud security posture management solution, and CloudGuard Workload serverless security.
- **Threat prevention:** Check Point continues to improve its threat detection capabilities. Customers using Threat Extraction, the content disarm and reconstruction feature that is part of the SandBlast bundle, welcome the addition of web downloads as a new layer of protection for employees.

Cautions

- **Pricing strategy:** Although Check Point has succeeded in simplifying its pricing strategy, it lags behind its leading competitors in its ability to sell enterprise-level agreements to the largest customers.
- **Pricing execution:** In the past few years, Gartner analysts continued to receive a sizable amount of reports regarding dissatisfaction with pricing, which have slowly shifted from

a focus on total cost of ownership (TCO) to more on the high cost of renewing Check Point subscriptions.

- **Product strategy:** Check Point's strategy to integrate its security virtual machine (VM) with leading SD-WAN providers, rather than add native SD-WAN capabilities, creates a disadvantage against its leading competitors when competing for the branch perimeter appliance use case.
- **Support:** For providers with a long history and large market share, Gartner expects to receive more feedback on occasional support issues. While it improved last year, feedback on Check Point support, especially outside of North America, continues to be slightly worse than its competitors.

Cisco

Cisco is a Challenger in this Magic Quadrant. Cisco offers multiple firewall product lines, the primary ones being Cisco Firepower Threat Defense (FTD) Next-Generation Firewall (NGFW) Series and the Meraki MX series. Cisco also offers FWaaS as a part of its Umbrella secure internet gateway, and industrial firewalls (the ISA series).

Major updates include those around its Firepower Management Center user interface. It also introduced SecureX, an integrated management platform that enables visibility and control across network, endpoint, cloud and application security.

Cisco's firewall is a good fit for organizations that have experience with Cisco products and want to consolidate with the same vendor for their security and network products.

Strengths

- **Sales strategy:** Cisco has a broad product portfolio, and drives customers effectively toward enterprise ELAs, which often include firewall subscriptions and support. It is also an attractive proposition for clients that want to consolidate with a single vendor.
- **Capability:** Customers value the Talos threat research and advanced malware protection (AMP) features available on Firepower. Existing Sourcefire customers also like the IPS integration on Firepower. SecureX is the vendor's extended detection and response (XDR) platform that enables visibility and control across Cisco's network, endpoint, cloud and application security products.
- **Market execution:** Cisco Meraki MX provides a simplified security and networking experience to customers with distributed small offices that need easy-to-configure, deploy and manage networking and firewall solutions.
- **Feature:** Gartner clients remark on the high quality of Cisco's VPN, and report that the site-to-site VPN is stable and easy to configure. Many Gartner clients that replace their Cisco Adaptive Security Appliances (ASAs) with a firewall from a different vendor continue to use ASAs for VPN only.

Cautions

- **Product strategy:** Cisco offers multiple different security management portals, causing a lot of overlap and confusion within the end-user community. The vendor offers Cisco

Defense Orchestrator as a cloud-based centralized manager, Cisco Threat Response (CTR) cloud-based threat correlation, Security Analytics and Logging (SAL) cloud-based reporting portal, and the latest addition, the SecureX extended detection and response platform.

- **Product strategy:** Despite having multiple cloud security products, the vendor only offers support for AWS and Azure through Cisco NGFWv, and ASAv and ASA for Cisco Meraki vMX. These lack any integration with Cisco's Tetration, its cloud workload protection platform (CWPP) offering. As a result, Gartner seldom sees Cisco firewall deployments in public cloud IaaS scenarios.
- **Product strategy:** Cisco has different firewall product lines for different deployment use cases. The Meraki and FTD product lines are led by different product teams and have distinct capabilities and operating systems, leading to operational complexities despite consolidating toward a single vendor.
- **Sales execution:** Cisco continues to struggle to win firewall evaluations against competitors in pure firewall deals based on technical evaluation alone. "Cisco shops" are the predominant base of Cisco firewall customers.

Forcepoint

Forcepoint is a Visionary in this Magic Quadrant. During the evaluation period, it introduced several new firewall models. It also brought a new secure access service edge (SASE) offering to market. Other updates include enhancements to AWS and Azure integrations, and a browser-based interface for its Security Management Center (SMC) central management system, for easier administration.

Forcepoint firewalls are good shortlist candidates for distributed office use cases where clients are looking for mature SD-WAN, VPN and centralized management capabilities, and FWaaS. They have advanced clustering/high availability, and are also good candidates for midsize enterprises looking for mature advanced threat detection features.

Strengths

- **Product execution:** Forcepoint has strong SD-WAN and VPN capabilities. It plays to these strengths by releasing enhancements regularly. It maintains a single endpoint client approach for all its end-user connectivity, irrespective of the service. Forcepoint offers Wi-Fi on the smaller modules through additional modules.
- **Offering:** Forcepoint firewalls offer some unique capabilities such as built-in user and entity behavior analytics (UEBA) capability, and integration with AWS Sentinel and Azure Security Center as public IaaS support. There is seamless service-chaining between Forcepoint's firewalls and its web security and data loss prevention (DLP) products.
- **Product strategy:** This year, Forcepoint introduced its FWaaS. Other than that, it offers a compelling list of cloud security services: Forcepoint Web Security, Forcepoint CASB, Forcepoint Email Security, Forcepoint Dynamic User Protection and Forcepoint Dynamic Data Protection. This shows its strong product strategy toward offering a cloud security service model.

- **Centralized manager:** Forcepoint's centralized firewall manager, SMC, is a very intuitive and easy-to-use interface, and customer feedback is positive. Administrator roles can be defined, and mapped with select NGFWs, access control lists and domains. There is also an administrator privilege for approving pending changes with features such as drag-and-drop.

Cautions

- **Market execution:** Forcepoint focuses too heavily on the distributed office use case and support of the emerging SASE trend. While its firewalls have the potential to serve other use cases, the vendor's roadmap sacrifices data center features, potentially falling behind other vendors in the market.
- **Marketing:** Forcepoint does not have much market awareness, and is rarely mentioned as a shortlist candidate by Gartner clients. While it has some presence within the U.S. federal government sector, it lacks traction in other markets.
- **XDR:** The vendor lacks native endpoint detection and response (EDR) client integration capabilities. It also lacks firewall integration with third-party EDR clients.
- **Customer feedback:** Customers remark that Forcepoint's feature releases occur behind those of the leading vendors. This holds the vendor back from leading the market.

Fortinet

Fortinet is a Leader in this Magic Quadrant. The vendor offers multiple firewall virtual and hardware models to meet different firewall deployment use cases.

The major update this year has been the acquisition of OPAQ, a SASE cloud provider. New feature updates include multiple enhancements to the latest version of FortiOS, including integration support with Kubernetes through FortiOS 6.2 and release of the NP7 network processor.

Fortinet firewalls are leaders in integrated SD-WAN capabilities with advanced networking, making them top candidates for firewall-appliance-based distributed office use cases. They also lead in price versus performance, and are desirable candidates in price-conscious enterprises.

Strengths

- **Advanced networking:** Fortinet offers fully integrated SD-WAN capabilities in its firewalls. Fortinet Fabric Management Center (FMC) offers strong automation and orchestration capabilities for full mesh overlay links for secure connectivity capabilities between sites.
- **Product:** Fortinet's security fabric offers open API capabilities to integrate with third-party products in the client's ecosystem. It also offers GUI plug-ins to its API interface for several third-party products/partners such as AWS, Azure. VMware vCenter and others.
- **Product strategy:** FortiManager provides central management with additional Fortinet Fabric plug-ins, which offer management of FortiSwitch, FortiAP, FortiWifi, FortiWLM, FortiExtender and FortiAnalyzer.

- **Price execution:** One of the primary reasons Gartner has seen data center and large enterprises shortlisting Fortinet firewalls is their competitive price/performance ratio and bundled pricing models, which makes product licenses easy to consume and allows for a realistic estimation of TCO.

Cautions

- **Market execution:** Despite having a large product portfolio, Gartner does not see Fortinet clients tempted to consolidate toward its multiple product lines other than firewalls and web application firewalls (WAFs). Gartner finds a less aggressive vendor focus on developing and upgrading other security products to compete with the best of breed in the market, such as FortiNAC, FortiClient and FortiCASB. Also, the vendor lacks the automation capabilities of different security product lines with FortiGate firewalls.
- **Market responsiveness:** During the evaluation period of this research, Fortinet announced the acquisition of OPAQ, a SASE cloud provider, but still lacks an FWaaS offering. The vendor might start offering it as an independent solution immediately, considering the demand in the market. It is recommended that Gartner clients consider it as an independent offering, and evaluate the integration capabilities.
- **Market execution:** Despite Fortinet supporting multiple cloud platforms, Gartner generally does not see the vendor's firewalls shortlisted for the cloud deployment use case, as compared to other direct competitors. Gartner also finds that Fortinet lacks marketing and promotion related to the cloud deployment use case, making it seem like the vendor is more hardware-focused.
- **Customer feedback:** Fortinet continuously releases multiple different new feature enhancements for its firewall product, which often leads to new management changes in the UI. Clients have citied this as making firewall management more complex for day-to-day administration after the new update is applied.

H3C

H3C is a Niche Player in this Magic Quadrant. It is an infrastructure vendor. SecPath is its firewall product line. H3C also offers a dedicated industrial firewall product line, Industrial Control Security.

Major updates this year include multiple feature enhancements in advanced routing, firewalling capabilities and cloud support.

H3C is a good candidate for enterprises in China that want to consolidate toward a single vendor for their infrastructure requirements to reduce licensing complexities. It offers different firewall models to meet different firewall deployment use cases, with high-end data center models.

Strengths

- **Product portfolio:** Like many large Chinese security vendors, H3C also offers a broad range of network products in its portfolio that are ideal for network teams looking for vendor consolidation. Its firewalls offer built-in WAF and vulnerability scanning. H3C also offers a dedicated product line for industrial/OT security.

- **Scalability:** The vendor offers high-throughput firewalls for the data center use case. Its VSYS feature for firewall model M9000, can support more than 4,000 virtual firewall instances.
- **Market execution:** The H3C firewalls have a prominent presence in the telco vertical. The vendor offers strong support for OpenStack, especially for telcos that want to offer hosted security services to their clients. H3C SecCloud Operation Management Platform (OMP) is a centralized management platform for large-scale deployments and cloud deployments.
- **EDR:** H3C offers Terminal Safety Protection System (TSPS), an endpoint protection client. This client software provides EDR and antivirus functions. The TSPS management platform and firewall utilize Cybersecurity Situation Awareness Platform (CSAP) to analyze the information and trigger actions, notifying the TSPS platform to restrict the infected host's network access and infected file transmission, etc.

Cautions

- **Market execution:** H3C is more focused toward hardware and OpenStack product lines to support its native private cloud and telco-hosted platforms, only available on Alibaba Cloud. The vendor lacks direct security services offered to clients as SaaS. It also lacks a direct FWaaS offering.
- **Sales execution:** Despite a broad product line, the vendor lacks Enterprise Support Agreements (ESAs) to benefit H3C clients and reduce multiyear licensing complexities.
- **Geographic strategy:** The vendor has a presence primarily in China and lacks a presence in other parts of the Asia/Pacific region. Gartner does not see H3C being shortlisted by clients outside of China.

Hillstone Networks

Hillstone Networks is a Niche Player in this Magic Quadrant. It sells firewalls for different use cases under different product lines: E-Series NGFW, T-Series iNGFW, X-Series Data Center Firewall, CloudEdge (virtual NGFW), CloudHive (microsegmentation) and CloudPano (FWaaS in the China market only). Other than firewalls, Hillstone sells WAF, application delivery controller (ADC), network traffic analytics (NTA) and intrusion detection and prevention system (IDPS) products.

Product updates this year include IoT security (IP camera network protection) and enhancements related to policy optimization, reporting and SD-WAN.

Hillstone has a strong focus on supporting China's regional cloud. It offers firewall models for different firewall deployment use cases. It is a good shortlist candidate for enterprises looking for virtual firewalls for cloud in China.

Strengths

- **Product portfolio:** Hillstone offers a broad network security portfolio, ideal for enterprises seeking consolidation toward a single vendor. Besides firewalls, the vendor offers FWaaS in China via CloudPano, WAF, ADC, NTA and IPS products.

- **Microsegmentation:** Hillstone offers a dedicated firewall offering for the microsegmentation use case, called CloudHive. It continues to enhance CloudHive by adding advanced features. CloudHive offers policy assistant features and a policy duplication detection engine, which uses prelearning network traffic to help in policy optimization of east-west traffic. CloudHive also offers traffic visualization capabilities, automatic discovery of service chains and the ability to detect service down gradation.
- **Product strategy:** Hillstone was one of the first Chinese security vendors with a strong cloud security strategy. The vendor offers CloudPano in China. The Hillstone firewalls offer support for AWS, Azure, Alibaba Cloud, Tencent Cloud and Huawei Cloud as bring your own license (BYOL). They are also available as pay as you go (PAYG) on AWS and Alibaba Cloud.
- **Product portfolio:** The vendor offers Hillstone sBDS, its NDR platform, available globally, and a SIEM solution called iSource, currently sold only in China. This offers multiple product consolidation options for Hillstone firewall clients.

Cautions

- **Cloud portal:** Hillstone's CloudView, a cloud-based security management system, offers monitoring-only capabilities, confining the centralized product changes and upgrade management to an on-premises centralized manager only.
- **Feature:** Hillstone firewalls lack support for TLS 1.3, and do not support the selective SSL decryption feature based on selective categories.
- **Feature:** Hillstone firewalls offer basic firewall optimization features, limited only to duplicate objects and rule hits, whereas other vendors are enhancing this feature to offer more recommendations to administrators to fine-tune and optimize the configurations.
- **XDR:** Although Hillstone offers partnerships with global and regional EDR vendors, it offers basic integration. The vendor lacks a native EDR client and does not offer XDR capabilities.

Huawei

Huawei is a Challenger in this Magic Quadrant. It sells two separate firewall product lines: the USG and the Eudemon series.

Major features introduced this year are enhancements to threat detection, and SD-WAN and access management capabilities based on integrated risk assessment.

Huawei firewalls are a good shortlist candidate for clients looking for a complete firewall solution at competitive pricing primarily in Southeast Asia, Europe and Latin America. Also, Huawei firewalls are a good candidate as a part of large Huawei infrastructure deals, from a consolidation point of view.

Strengths

- **Product:** Huawei firewalls offer a CASB-like feature called cloud access security awareness, which enables administrators to manage access to cloud-based SaaS applications. This makes management of SaaS applications easier for administrators.

- **Price:** One of the primary selection criteria many Gartner clients cite for Huawei firewalls is its competitive price versus performance ratio. The vendor offers simple bundle-based subscriptions that are cost-effective and bring down the TCO as compared to many other competitors in the space.
- **Product strategy:** The vendor offers identity access management through a risk assessment model that uses its security orchestration, analytics and reporting (SOAR) and firewall. This involves third-party identity and access management (IAM) that can be integrated with the SOAR, enabling risk assessment for users. Access control is defined on the firewalls.
- **Market execution:** Huawei introduced its direct MSS services, especially targeted toward SMB clients, with managed detection and response (MDR) capabilities. This service is offered by the vendor using its native suite of security products and firewall. It will be useful for clients seeking managed firewall service directly from the vendor.

Cautions

- **Market responsiveness:** The vendor lacks an FWaaS offering. The cloud-based management offered for its firewalls provides basic administration features.
- **Market understanding:** The vendor lacks a strong product strategy around cloud security. It does not offer any cloud-based security services to clients. Huawei firewalls are also not available as PAYG on any public cloud platform. This makes the vendor a less desirable shortlist candidate for enterprises with hybrid environments.
- **Product strategy:** The vendor does not have a big partner ecosystem; as a result, the firewall does not offer integration with common security vendors, other than limited regional vendor partnerships such as with Jiangmin, Tencent and Bamboo.
- **Market execution:** The vendor does not offer a native EDR client; hence, it lacks XDR capabilities. Huawei firewalls do not offer direct integration with third-party EDR vendors, and the vendor has partnerships with only two regional EDR vendors, Jiangmin and Tencent, through its CIS platform.

Juniper Networks

Juniper Networks is a Challenger in this Magic Quadrant. Its firewall product line is SRX. It also offers Contrail Security Orchestration (CSO) as a service, which is sold as part of the vendor's FWaaS offering.

Major features introduced recently are SecIntel, Juniper's distributed threat intelligence (TI) shared between SRX firewalls, switches, routers and access points (APs) enhancements around IoT security; enhanced support for public cloud; support for 5G; and network security enhancements.

Juniper firewalls meet all the firewall deployment use cases, including containers. Juniper firewalls are a good shortlist candidate for network teams looking to consolidate network and firewall components with a single vendor.

Strengths

- **Product strategy:** Juniper Connected Security is the vendor's product strategy that focuses on integration of its network product lines with its firewalls. In addition to centralized management and reporting, Juniper introduced a shared TI offering called SecIntel, which is integrated with Juniper's SRX, MX, EX/QFX and Mist AP product lines.
- **Market execution:** Juniper firewalls are available as PAYG on multiple public IaaS platforms such as AWS, Microsoft Azure, IBM Cloud and Google Cloud Platform, making it one of the few firewall vendors supporting maximum public IaaS platforms as PAYG. Its container-based firewall, cSRX, is available on the AWS container marketplace.
- **Offering:** Juniper's Junos Space Security Director offers mature firewall policy orchestration and reporting capabilities. It has multiple different policy filters to provide search based on different objects, including metadata/security tags. It also offers an intuitive reporting dashboard where the highest-consuming applications can be directly blocked through the monitoring dashboard display.
- **Scalability:** While Juniper offers high-throughput firewalls, its Junos Space Security Director centralized manager can scale to manage a large number of different Juniper devices, including switches and routers.

Cautions

- **Market execution:** While other network security vendors in the market are expanding their security product portfolios through acquisitions, Juniper is not. It primarily works through vendor partnerships for offerings like network access control (NAC), EDR, NTA, etc., instead of expanding outside SRX firewalls.
- **Product strategy:** Juniper continues to promote itself as a network-centric vendor. It has a continuous product strategy that works toward integration of SRX firewalls with its other Juniper network products. This makes it a desirable candidate for network teams as opposed to security teams.
- **Feature:** The vendor's application control feature is still not rated high compared to its competitors. It lacks granularity and offers limited subcontrols for many applications. It is recommended that clients evaluate the level of controls to make sure it meets their requirements.
- **Offering:** Juniper continues to offer multiple different centralized managers with distinct features, including Junos Space Security Director, Juniper Sky Enterprise and Juniper Contrail Service Orchestration. This requires clients to use multiple management tools based on their use cases.

Microsoft

Microsoft is a Niche Player in this Magic Quadrant. It offers a firewall as part of its Azure networking services. Azure Firewall can be managed and monitored by the vendor's built-in tools or by third-party network security policy management solutions.

In the last year, Microsoft released Azure Firewall Manager, its centralized firewall policy management solution. Microsoft Azure Firewalls have attained the ICSA Labs Corporate Firewall Certification. The vendor also added support for multiple public IPs and availability zones, including the "four nines" SLA. The firewall also supports more NAT configurations, and Azure IP groups can be included in the firewall rules and multiple other network related features.

Azure Firewall remains a good shortlist candidate for enterprises automating their Azure infrastructure.

Strengths

- **PaaS:** Azure Firewall is fully integrated with the Azure platform, starting with the on-demand pricing. The product includes built-in high availability, auto-scaling and availability zone support. Azure Firewall leverages Microsoft Threat Intelligence Cloud.
- **Roadmap execution:** The vendor has shown that it delivers new features as planned, but takes the time for a long beta before making a feature generally available.
- **Centralized management:** Azure Firewall Manager, the centralized policy portal, allows rules to be deployed across multiple Azure Firewall instances, with support for global and local policies. The firewall can forward the web traffic to third-party secure web gateway (SWG) products. Migration of such rules is facilitated by importing policies from individual Azure Firewall configurations.
- **Geographic presence:** Microsoft Azure is a global IaaS infrastructure with strong resiliency and stringent SLAs, making it easier for distributed organizations to deploy firewalls close to all their local points of presence.

Cautions

- **Product strategy:** Azure Firewall is a recent purpose-built product intended to meet Azure's IaaS client needs. It lacks many features that stand-alone firewall providers have included for years, such as URL filtering or IDPS. The vendor does not rush to achieve a comprehensive feature set, but releases improvements regularly.
- **Ease of use:** Security teams lacking Azure operation skills report that configuring the firewall using the standard UI looks more difficult than with the vendor's appliance-based competitors. They specifically mention that the firewall policy lags behind the competition.
- **Feature:** Azure Firewall does not decrypt TLS traffic and lacks cloud-delivered sandboxing for file inspection. It only supports IPv4.
- **Customer feedback:** Clients adopting multicloud find that adopting a third-party firewall vendor common across public cloud vendors is operationally easier than developing expertise in native public cloud firewall skills.

Palo Alto Networks

Palo Alto Networks is a Leader in this Magic Quadrant. Along with selling firewalls as hardware and virtual appliances, the vendor also offers FWaaS, via Prisma Access.

This year, Palo Alto Networks announced the acquisition of CloudGenix, a cloud-based SD-WAN vendor. The vendor also introduced SD-WAN, support for TLS 1.3, and other feature- and product-related updates.

Palo Alto Networks' firewall is a good shortlist candidate for clients looking for a firewall with premium subscriptions at a premium price. With a broad product portfolio, the vendor also can be a good candidate for clients looking to consolidate with a single vendor for their various security requirements.

Strengths

- **Market execution:** Palo Alto Networks was an early hardware firewall vendor introducing FWaaS in the market. Recently, it introduced DLP to Prisma Access. The vendor's hybrid network firewall clients use Prisma Access for their remote users and branch office setups.
- **Sales strategy:** Palo Alto Networks offers flexible ELA and ESA deals. These are becoming popular with clients interested in procuring different product lines with multiyear deals, leading to easy-to-consume licensing models for clients making large deals with the vendor.
- **Product:** Palo Alto Networks firewalls offer strong granular application controls for social media applications and an application-usage-based policy optimization feature. Gartner clients often highlight granular application control as one of the primary reasons for shortlisting the firewall. The firewall offers TLS usage monitoring for traffic across different versions of TLS.
- **Market responsiveness:** The vendor shows a strong focus on cloud security — the Prisma product line is focused on it. The offering includes different security products, including microsegmentation, FWaaS and CWPP.

Cautions

- **Pricing:** Palo Alto Networks continues to be one of the most expensive vendors in the firewall market. Gartner clients are often dissatisfied with the renewal cost, which does not come with similar discounts received on support and services when buying the firewall for the first time. This makes the TCO higher and, in a few cases, clients are switching to a less expensive vendor.
- **Offering:** The vendor lacks a direct cloud-based centralized manager offering for its firewall appliances. It offers an on-premises centralized manager, Panorama, which can also be deployed in the cloud by the client.
- **Offering:** Despite the vendor offering multiple security product lines, most of them have a dedicated management interface for administration, thus they work as stand-alone products. Gartner clients using multiple Palo Alto Networks' product lines beyond firewalls often highlight the lack of a centralized management interface as a drawback.
- **Customer feedback:** Clients have reported scalability issues with large Prisma Access deployments beyond 60,000 users. Also, clients report connectivity issues with Prisma Access in a few places, such as the Asia/Pacific region and Latin America.

Sangfor

Sangfor is a Niche Player in this Magic Quadrant. Its firewall product line is called Sangfor Next Generation Application Firewall (NGAF), available in the form of physical and virtual appliances.

Major features rolled out this year include the introduction of XDR, NTA and UEBA in Cyber Command with endpoint automation; Platform-X, a cloud-based centralized manager; and a network policy configuration optimization feature.

Sangfor shows a strong cloud security vision and product strategy with multiple SaaS-based security services. It is an ideal shortlist candidate for enterprises that want to consolidate with a single vendor for multiple security needs.

Strengths

- **Product portfolio:** Sangfor offers a large security product portfolio. FWaaS is offered via Sangfor Cloud Shield. Other than firewalls, the vendor offers an SSL VPN appliance, IAM, endpoint security, mobile device management, advanced treat detection and a security management solution. Consulting and MDR services are also offered. All this makes it a good shortlist candidate for enterprises looking to consolidate with a single vendor.
- **Market responsiveness:** Sangfor is one of the few Chinese firewall vendors showing a strong cloud security vision. Sangfor firewalls support AWS Global, AWS in China, Azure, Alibaba Cloud, Tencent Cloud, Huawei Cloud and Sangfor HCI/XY clouds. The vendor offers different SaaS-based security services, cloud-based vulnerability assessment (cloud VA), cloud-based WAF (cloud WAF), cloud-based anti-DDoS (in cooperation with Tencent) and a cloud-based SWG (ISSP), which are more globally adopted as opposed to hardware appliances.
- **XDR:** Sangfor introduced XDR capabilities this year. Sangfor XDR (Cyber Command) integrated NTA and UEBA capabilities with Sangfor NGAF. The vendor offers a centralized log and event management center for firewalls, endpoints and SWGs. The XDR also provides an endpoint host block and quarantine through firewall. Sangfor also offers Platform-X, its cloud-based threat correlation platform.
- **Market execution:** The vendor offers MDR directly to end users as a part of its MSS offering. It also offers the Cloud Eye service, which can actively and continuously detect assets of users and provide continuous risk assessment, real-time monitoring, tampering disposal and emergency confrontation services for internet service.

Cautions

- **Offering:** The vendor does not have a PAYG firewall offering on Alibaba Cloud, which is one of the largest public IaaS providers in the region. In fact, Sangfor firewalls are only available as PAYG on the Sangfor HCI cloud.
- **Geographic presence:** The vendor continues to have a major presence in China, and a very limited presence in other parts of Southeast Asia.
- **Sales execution:** Despite having higher-end firewall models, Gartner finds Sangfor to be more prominent in the midsize use case as opposed to other firewall use cases.

- **Sales execution:** Despite a broad product portfolio, Gartner does not find vendor sales teams promoting ELA deals to customers that encourage end users to consolidate for multiple security products with Sangfor. Gartner has found more a la carte contracts and quotations from the vendor, and Sangfor offering bundled pricing models.

SonicWall

SonicWall is a Niche Player in this Magic Quadrant. The vendor offers multiple firewall product lines, branded as TZ Series, NSA Series, SuperMassive Series, NSsp Series and NSv Series.

Recent company news includes the introduction of new models in the TZ Series and a new operating system featuring multi-instance multitenancy and on-premises ATP appliances. In addition, SonicWall launched NSv for KVM, expanded PAYG models, and introduced low-cost virtual firewall models for public cloud. Other updates include product- and feature-related enhancements.

SonicWall is a suitable shortlist candidate for midsize enterprises that seek an easy-to-install firewall with a wide range of security features at a good value. Customers with public cloud use cases should evaluate whether support for Azure and AWS only is enough.

Strengths

- **Offering:** Capture Security Center (CSC), the vendor's cloud-based manager, offers a complete set of centralized management for all its products, and offers features such as a bulk firmware upgrade and a pushing of rules. Customers often mention ease of deployment and configuration using the zero-touch deployment feature integrated within CSC.
- **Product:** SonicWall's on-premises centralized manager, Global Management System (GMS) and cloud-native Network Security Manager (NSM), offers mature management and multitenancy features desired by MSSPs. Like CSC, in addition to managing firewalls, GMS can also manage and report on SonicWall's Secure Mobile Access and email security, integrated SonicWall wireless access points, switches, and WAN acceleration solutions, offering centralized management capabilities for multiple product lines.
- **Feature:** Customers value the wireless features embedded in the firewall and available separately, They comment on the value of all products — specifically wireless — being managed in one console.
- **CASB:** SonicWall offers CASB capabilities in SonicWall Cloud App Security (CAS). It offers security for SaaS applications such as Office 365 and G Suite by offering cloud-based email scanning and access controls, and preventing the upload of sensitive or confidential files and data.

Cautions

- **Sales execution:** While SonicWall's product portfolio has added much more offering breadth and feature depth, its firewalls are not particularly visible on Gartner client shortlists.

- **Market execution:** The vendor lacks an FWaaS offering, making it a less-desirable shortlist candidate for the distributed enterprise use case, and those that want to move away from appliance-based firewalls and remote working use cases seeking FWaaS capabilities.
- **Cloud security:** Despite introducing multiple virtual appliances, the vendor's firewalls still lack support for Cisco ACI, something that is offered by most of its competitors in the market. SonicWall also offers limited support for public IaaS platforms, with support only for AWS as PAYG.
- **Customer feedback:** During the evaluation period, customers mention some difficulty and delay in getting Level 1 support calls answered, although they are more satisfied with the quality of premier support.

Sophos

Sophos is a Visionary in this Magic Quadrant. Its firewall product line is XG.

During this evaluation period, Sophos introduced the Xstream architecture (Xstream SSL Inspection, Xstream DPI Engine and Xstream Network Flow FastPath). Other new features include enhancements to improve SD-WAN capabilities, advanced threat detection and central management.

Sophos continues to lead the market with its XDR capabilities between firewall and endpoint security products. It is prominent in midsize use cases. The vendor wins deals primarily because of its XDR capabilities, cost savings and ease-of-use capabilities.

Strengths

- **Offering:** Sophos continues to enhance its TLS 1.3 decryption performance and threat detection lead among its midsize-enterprise-competitive cohorts. It supports software-based TLS decryption with end-to-end TLS 1.3 decryption, without downgrade, and includes a comprehensive exception list in its default configuration.
- **Market execution:** Sophos offers cloud-native policy control with Cloud Optix through a separate offering. It also offers the Managed Threat Response service directly to end users.
- **Sales execution:** Sophos highly promotes its mature XDR capabilities and wins deals by offering easy pricing models and huge cost savings on the TCO of both firewalls and endpoint security, and a bundled deal. These days, it is also packaging its MDR services, making Sophos an ideal security vendor for midsize organizations.
- **Product:** Sophos continues to lead in the XDR use case as compared to other firewall vendors with similar offerings, but lacks advanced integration and automation. It shares threat- and health-related intelligence between endpoints and firewalls using the Synchronized Security feature to correlate and identify compromised systems, enabling firewalls to automatically isolate the infected endpoints.

Cautions

- **Market responsiveness:** The vendor lacks an FWaaS offering, making it a less favorable shortlist candidate for remote working and for enterprises that want to switch to FWaaS for their branch offices.
- **Visibility:** Sophos firewalls are not frequently seen on Gartner SMB clients' shortlists and have reduced visibility as compared to other direct competitors in the market.
- **Product strategy:** The vendor continues to focus on midsize enterprise use cases and has no visibility in enterprise edge use cases, despite offering high-throughput models. Sophos also offers limited firewall support for public IaaS and does not seem to have a strong product strategy around it.
- **Sales execution:** Sophos firewalls are more often being shortlisted when bundled with the vendor's endpoint security, rather than for firewall-only deals. With other vendors also offering endpoint security products, gradually Sophos will have to be more innovative and explore other firewall use cases beyond XDR.

Stormshield

Stormshield is a Niche Player in this Magic Quadrant. Other than firewalls, the vendor offers Stormshield Endpoint Security and Stormshield Data Security products. It also offers dedicated industrial firewalls, SNi40 and SNi20.

Major updates to Stormshield's firewalls are firmware performance improvements and other enhancements related to firewall security features.

Stormshield firewalls are good shortlist candidates for SMBs, especially government clients in Europe due to their European certifications and OT security use case. Being local to the European region, the vendor offers strong regional support.

Strengths

- **Product offering:** Stormshield offers vulnerability assessment as a firewall feature. It provides a view of assets in the networks, operating systems and applications run with its version, and provides a warning when a known vulnerability affects the installed OS/application version.
- **Product strategy:** The vendor offers a strong product strategy toward OT security. While Stormshield offers dedicated industrial firewalls in SNi40 and SNi20 (introduced in 2020), its IPS firewall feature covers a wide range of SCADA/ICS/IoT infrastructure protocols, such as BACnet/IP, CIP, Ethernet/IP and IEC 60870-5-104.
- **Product:** Stormshield offers an easy-to-use network firewall with a complete offering at competitive pricing. It offers multiple integrated features in its firewalls, making it a suitable shortlist candidate for SMBs. The vendor offers built-in DLP features for web and email files, with end-to-end encryption. Broad coverage of OT protocols and an integrated vulnerability management feature make this offer unique compared to many other direct competitors in the market.

- **Feature:** Stormshield firewalls utilize external reputable third-party indicators of compromise for their cloud-based sandboxing service as a third-party source, instead of relying solely on their native TI.

Cautions

- **Market responsiveness:** The vendor lacks an FWaaS offering for remote users and distributed offices that want to use cloud-based services instead of firewall appliances.
- **Product strategy:** Stormshield firewalls lack a strong focus on cloud security. They are not available as PAYG on any public cloud platforms. The vendor also lacks a cloud-based management portal for its firewalls.
- **Offering:** The centralized firewall manager lacks multitenancy features desirable for MSSs. Features such as policy optimization are not offered. Stormshield firewalls do not support TLS 1.3 decryption.
- **Market execution:** Despite being an Airbus subsidiary, Stormshield is relatively slower in introducing new product updates and enhancements as compared to other competitors, as more international firewall vendors are competing with regional players. The vendor has a European presence that is more concentrated toward certain regions with limited use cases.

Venustech

Venustech is a Niche Player in this Magic Quadrant. It sells multiple firewall product lines, including Venusense Unified Threat Management, Venusense WAF and Venusense NGFW. It also sells a dedicated industrial firewall product line, Venusense IFW.

This year, Venustech introduced SD-WAN capabilities, an NGFW based on ARM and VCloud SaaS. It also developed enhancements to its industrial security offering.

Venustech is a good shortlist candidate for enterprises in China that want to consolidate with a single vendor for their different security products. It offers high-throughput firewalls at competitive pricing ideal for enterprise edge and data center use cases.

Strengths

- **Feature:** Venustech offers granular DLP feature support for endpoints, web and email traffic; it comes as a separate subscription. Detection methods include keywords, regular expressions, file attributes, file fingerprints, classification fingerprints and mail recipients.
- **Market execution:** Venustech continues to focus on industrial security use case. The vendor offers a dedicated IFW product line with different models. IFW offers support for in-depth filtering based on Modbus/TCP, Modbus/RTU, nIEC104, OPC and Ethernet/IP, and provides enhanced feature support beyond basic firewall features.
- **Centralized firewall policy management:** Venustech's Venusense FlowEye is the vendor's firewall policy management and NTA solution. The product can perform centralized firewall policy management beyond Venustech firewalls, extending support to

all leading global and regional firewall players such as Fortinet, Check Point Software Technologies, Palo Alto Networks, Juniper Networks, Cisco and H3C.

- **Product strategy:** The vendor has a TI correlation platform that is a separate product, called VenusEye Threat Intelligence Center. This platform correlates TI from different VenusEye resources and products, and offers centralized correlation and threat scoring based on built-in templates. This product has a direct integration with the Venustech firewall from within the administration UI, which makes it easy to use for firewall users that require additional TI.

Cautions

- **Public cloud:** Venustech firewalls lack support for public IaaS platforms, while most firewall vendors offer it. The vendor also does not offer a direct FWaaS offering.
- **Offering:** The vendor only offers an on-premises sandboxing appliance and lacks cloud-based sandboxing services, which most competitors offer as an add-on subscription.
- **TLS decryption:** Venustech firewalls do not offer TLS traffic decryption. It claims to use TI and certificate-based inspection.
- **Geographic presence:** Venustech primarily sells its products in China and has a limited presence in Japan; however, the vendor is trying to expand in Southeast Asia.

WatchGuard

WatchGuard is a Niche Player in this Magic Quadrant. Its portfolio of security products and services includes the following firewalls: Firebox; Firebox T35-R, the industrial firewall model; FireboxV and Firebox Cloud. Additional offerings include multifactor authentication, endpoint and wireless product lines.

Major updates include the addition of Access Portal (reverse proxy), Firebox system management from WatchGuard Cloud, support for TLS 1.3 inspection and DNSWatchGO.

WatchGuard is a good shortlist candidate for SMBs looking for a complete firewall solution that is easy to use and has simplified pricing.

Strengths

- **Market execution:** As WatchGuard recently completed the acquisition of Panda Security (and its server and endpoint security), this broadens its portfolio toward mature endpoint security, as opposed to the basic endpoint security client it currently has. Clients must check the integration timelines of this newly acquired vendor with WatchGuard firewalls and Panda's security. As of now, Panda products are being sold as stand-alone offerings by WatchGuard.
- **Offering:** The vendor offers the Threat Detection and Response cloud-based threat correlation portal. This portal offers combined TI-based analytics through WatchGuard's current endpoint agent, host sensor and firewall, combining network and endpoint-based events. This feature also offers automation through which infected hosts isolate themselves from the network.

- **Customer feedback:** Clients often cite pricing with simplified bundled licensing and ease of use as the primary reasons to shortlist the vendor's firewalls. Firebox is bundled with one of two security service packages: Total Security Suite or Basic Security Suite.
- **Offering:** The vendor offers DNSWatchGO as a stand-alone cloud-based service. The addition of DNSWatchGO allows companies to add recursive DNS-level protection from a single vendor without having to deploy additional hardware or services.

Cautions

- **Offering:** The vendor lacks an FWaaS offering. This makes it a less desirable shortlist candidate for enterprises looking to move toward FWaaS for remote work and branch office use cases, as opposed to an appliance-based approach.
- **Product:** The vendor lacks a mature cloud-based management portal. The current offering is WatchGuard Cloud, which is primarily focused on monitoring and reporting.
- **Market execution:** While the direct competitors of WatchGuard have been moving beyond firewalling capabilities to lead in overlapping use cases like public IaaS and mature distributed offices, WatchGuard has been primarily focusing on providing firewalls for SMB use cases only. However, the recent Panda Security acquisition can help WatchGuard expand beyond firewall use cases and offer overlapping capabilities based on an integration product strategy and timelines.
- **Sales execution:** Despite being a global vendor, WatchGuard firewalls are not frequently seen shortlisted by Gartner clients as compared to direct competitors. It has more end-user visibility in the North American region, and is rarely seen in Asia/Pacific region firewall deals for SMBs.

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

No vendors were added to this Magic Quadrant.

Dropped

No vendors were dropped from this Magic Quadrant.

Inclusion and Exclusion Criteria

The inclusion criteria represent the specific attributes that analysts believe are necessary for inclusion in this research.

Vendors that provide network firewall functions that meet the market definition and description were considered for this research under the following conditions:

- Gartner analysts have assessed that the vendor can effectively compete in the network firewall market.
- Gartner has determined that the vendor is a significant player in the market, due to market presence, competitive visibility and/or technology innovation.
- The vendor demonstrates a competitive presence in enterprises and sales for enterprise and/or cloud networks.
- The vendor must meet the firewall revenue criteria of $30 million in 2019, as applicable to vendors selling firewall hardware appliances/virtual firewalls/FWaaS. In the case of IaaS vendors, at least 50% of the installed base should be using the native firewall controls offered by them.
- The vendor must demonstrate minimum signs of a global presence, including:
    - Gartner received strong evidence that more than 10% of its customer base is outside its home region.
    - It offers 24/7 direct support, including phone support (in some cases, this is an add-on, rather than being included in the base service).
    - The vendor appearing in Gartner client inquiries, its competitive visibility, its client references and its local brand visibility are considered to determine inclusion.

Vendors must provide evidence to support meeting the above inclusion requirements.

Evaluation Criteria

Ability to Execute

Product or Service: This includes service and customer satisfaction in network firewall deployments. Execution considers factors related to getting products sold, installed, supported and in users' hands. Strong execution means that a vendor has demonstrated to Gartner analysts that its products are successfully and continually deployed in enterprises and/or cloud environments, and that the vendor wins a large percentage in competition with other vendors.

Vendors that execute strongly generate pervasive awareness and loyalty among Gartner clients, and also 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. While sales are a factor, winning in competitive environments through innovation and quality of product and service are more important than revenue. Key features are weighted heavily, such as foundation firewall functions, console quality, low latency and secondary product capabilities (logging, event management, compliance, rule optimization and workflow). Having a low rate of vulnerabilities in the firewall is important. The logistical capabilities for managing appliance delivery or enabling firewall functions for additional workloads in cloud environments, product service and port density matter. Support is rated on the quality, breadth and value of offerings through the specific lens of enterprise/cloud needs.

Overall Viability: This includes overall financial health, prospects for continuing operations, company history, and demonstrated commitment in 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, competitive wins versus key competitors (which are compared with Gartner data on such competitions held by our clients), and devices or instances in deployment. The number of firewalls shipped or the market share is not the key measure of execution. Rather, we consider the use of these firewalls to protect the key business systems of enterprise clients and those being considered on competitive shortlists.

Sales Execution/Pricing: We evaluate the vendor's pricing, deal size, installed base and, in the case of cloud vendors, the number of customers using native firewall controls. This includes the strength of the vendor's sales and distribution operations. Presales and postsales support is evaluated. Pricing is compared in terms of a typical enterprise-class deployment, and includes the cost of all hardware, support, maintenance and installation. Low pricing will not guarantee high execution or client interest. Buyers want good results more than they want bargains, and think in terms of value over sheer low cost.

Market Responsiveness/Record: This evaluates the vendor's ability to respond to changes in the threat environment, and to present solutions that meet customer protection needs rather than packaging up fear, uncertainty and doubt. This criterion also considers the provider's history of responsiveness to changes in demand for new features and form factors in the firewall market, and how enterprises deploy network security. The criterion will also cover the capability of the vendor in securing hybrid networks and/or cloud networks because of rapid adoption of these networks.

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. In addition to buyer and analyst feedback, this criterion looks at which vendors consider the others to be direct competitive threats, such as by driving the market on innovative features co-packaged within the firewall, or by 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 accordingly. Significant weighting is given to delivering new platforms for scalable performance in order to maintain investment, and to the range of models to support various deployment architectures.

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

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