Magic Quadrant for Enterprise Network Firewalls

Published 4 October 2018 - ID G00337968 - 83 min read

By Analysts Adam Hils, Jeremy D'Hoinne, Rajpreet Kaur

In this mature market, vendors differentiate on feature strengths. Security and risk management leaders must consider the trade-offs between best-of-breed enterprise network firewall functions and risk tolerance.

Strategic Planning Assumptions

By 2022, 15% of enterprise firewall RFPs will include a requirement for the vendor to support and manage IaaS-native firewall policies.

In 2022, 10% new enterprise network firewall purchases will be purchased under an enterprise license agreement (ELA).

Virtualized versions of enterprise network firewalls will exceed 15% of market revenue by year-end 2023, up from less than 5% today.

Market Definition/Description

This document was revised on 13 November 2018. The document you are viewing is the corrected version. For more information, see the Corrections (https://www.gartner.com/en/about/policies/current-corrections) page on gartner.com.

The enterprise network firewall market represented by this Magic Quadrant is still composed primarily of purpose-built appliances for securing enterprise corporate networks, although virtual appliances across public and private cloud and heavily virtualized data centers are becoming more important. Products in this market must be able to support single-enterprise firewall deployments and large and/or complex deployments. These include traditional "big firewall" data center placements, branch offices, multitiered demilitarized zones (DMZs), and, increasingly, virtual versions for the data center and various cloud environments. Customers should have the option to deploy versions within Amazon Web Services (AWS), Microsoft Azure and Google Cloud public cloud environments. These products are accompanied by highly scalable (and granular) management and reporting consoles — on-premises or cloud-based — and there is a range of offerings to support the network edge, the data center, branch offices, and deployments within virtualized servers and the public cloud. All vendors in this market should support fine-grained application and user control. In effect, all vendors in the enterprise firewall market have what Gartner once called "next-generation firewalls (NGFWs)"; there is no longer a "next generation" in the firewall market.

The vendors that serve this market are identifiably focused on enterprises, as demonstrated by the proportion of their sales in the enterprise, and as delivered by their support, sales teams and channels. These vendors provide features dedicated to solving enterprise requirements and serving enterprise use cases.

What Has Changed?

All enterprise firewall vendors offer NGFW features to better enforce policy (application and user control) and detect new threats (intrusion prevention systems [IPSs], sandboxing and leveraging threat intelligence feeds). Enterprise firewall is now synonymous with NGFW (see "Next-Generation Firewall Hype Has Become an Obstacle for Enterprises"). Enterprise firewalls continue to replace stand-alone network IPS appliances at the enterprise edge. In some cases, the enterprise firewall intrusion detection and prevention system (IDPS) is good enough to deploy behind an enterprise firewall — replacing the previous stand-alone IDPS solution — if the IT security and risk leader is evaluating the enterprise firewall to replace the incumbent IDPS vendor. Although this is happening now, some enterprises will continue to choose to have best-of-breed IDPSs. Many enterprises are looking to firewall vendors to provide cloud-based malware detection instances to aid them in their advanced threat detection efforts, as a cost-effective alternative to stand-alone sandboxing appliances.

However, enterprise firewalls will not subsume all network security functions. More feature-inclusive all-in-one or unified threat management (UTM) approaches are suitable for small or midsize businesses (SMBs), but not for the remainder of the enterprise market.

The needs for enterprise branch office firewalls have become specialized, and they have diverged from UTM products. As part of increasing the effectiveness and efficiency of firewalls, branch office firewalls have integrated a more granular blocking capability than their UTM counterparts, going beyond port/protocol identification toward an integrated service view of network traffic. In short, they offer

the same levels of security efficacy as the primary gateway does. Having a subpar configuration and protection capability for branches is not acceptable today.

However, several enterprise branch office firewall and UTM vendors have introduced basic software-defined WAN (SD-WAN) capabilities, which could push their use cases further together in the future as enterprises seek this functionality.

Firewalls Do More Encryption Termination

Firewalls are becoming important vehicles for TLS termination. The primary use case is to inspect outbound traffic for threats, such as endpoints downloading malware and botnet command-and-control activity. TLS capabilities also allow them to act as lightweight data loss prevention (DLP) tools as they decrypt and inspect outbound traffic to determine if sensitive data is being sent out. The ability to decrypt encrypted traffic is becoming critical, as well over half of total traffic is encrypted today, and security tools are blind without visibility. However, customers that enable this capability are still frustrated by the substantial performance burden that in-firewall TLS decryption imposes. The looming move from TLS 1.2 to the TLS 1.3 standard will undoubtedly force changes in how enterprise firewall vendors process the traffic.

Policy Orchestration and Automation Become Critical

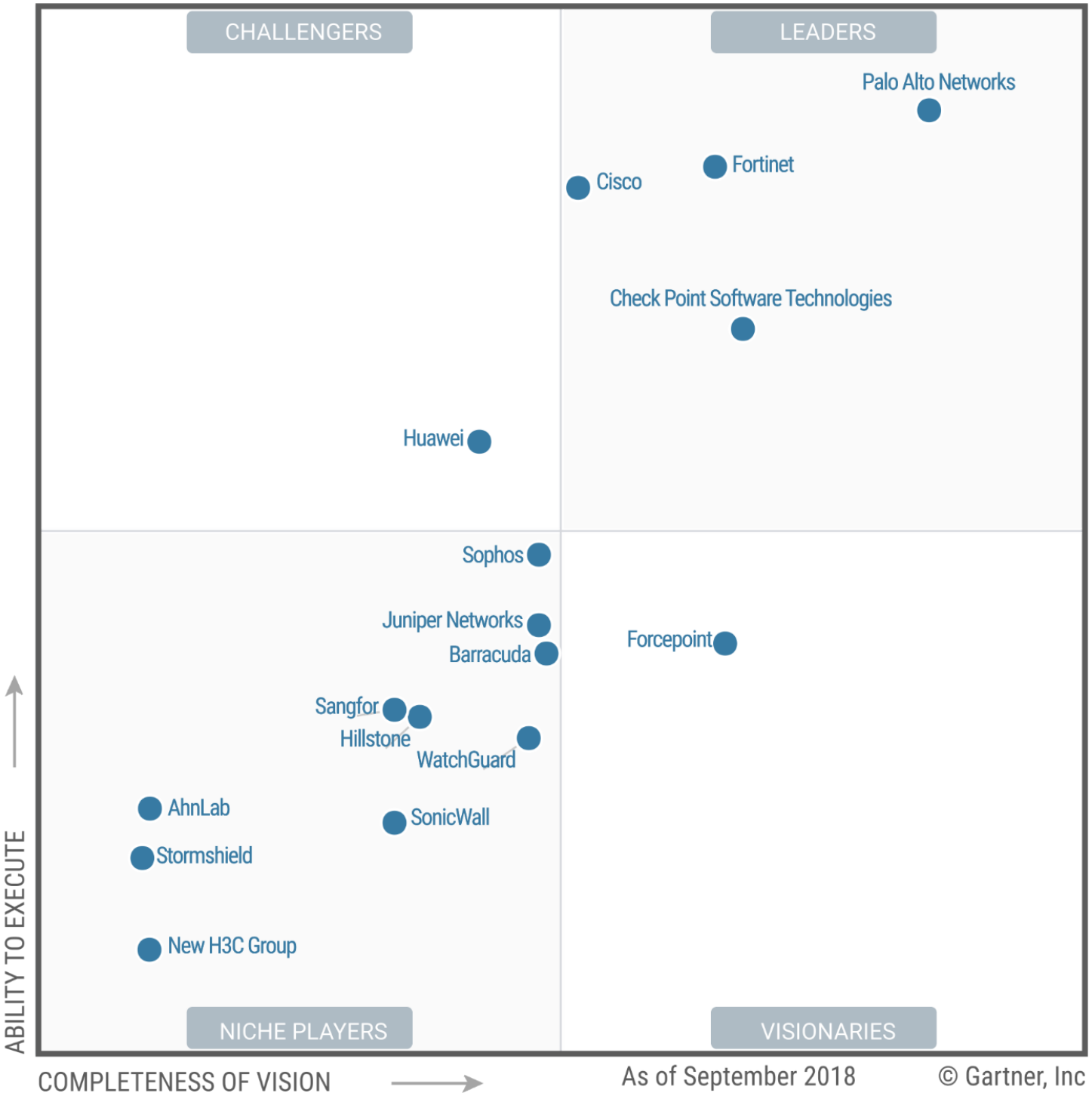
Leading-edge customers are planning, and sometimes implementing, principles of software-defined networking (SDN) and east-west microsegmentation. These customers seek vendors with some SDN support and forward-looking SDN roadmaps. More automated firewall policy orchestration will be key to these roadmaps. This orchestration will enable organizations — whose choice of VMware NSX, Cisco ACI or other SDN framework will drive firewall selection — to realize the agility and business benefits that SDN promises for each relevant SDN framework. Enterprise firewall vendors are not satisfying IT security and risk leaders in this area today.

Firewall Services Within IaaS Environments Become an Area of Differentiation

As more organizations are moving strategic workloads to the public cloud, an increasing number of them wish to protect those workloads with their incumbent enterprise firewall vendor. Today, these vendor offerings to AWS and Microsoft Azure are uneven. Some don't offer the same level of inspection that on-premises firewalls do, and they all lack sufficient policy automation. Enterprise firewall vendors must improve in these areas to remain relevant in the hybrid cloud era.

Magic Quadrant

Figure 1. Magic Quadrant for Enterprise Network Firewalls



Source: Gartner (October 2018)

Vendor Strengths and Cautions

AhnLab

Headquartered in South Korea, AhnLab is a regional security vendor offering network security, an endpoint security product and security consulting services primarily in South Korea. Its firewall product line is called AhnLab TrusGuard (TG). The TG firewall has 10 models with different model types: 31A to 400A model, which spans low and middle-end firewalls (up to 6 Gbps); 500A to 22000 model, which comprises high-end and data-center-ready firewalls (up to 100 Gbps). The firewall is Common Criteria-certified Evaluation Assurance Level 4 (EAL4) and TTA IPv6-verified, which is a South Korean certification, but does not have other third-party evaluations (such as ICSA Labs, NSS Labs or FIPS PUB 140-2).

Recent firewall product and feature enhancements include a virtual firewall for use in AWS environments, support for SaaS monitoring with DLP, IP blacklists, and AhnLab Threat Management System (TMS), integrated threat management for better threat detection and correlation.

The vendor is a good candidate for enterprises that are based in South Korea and looking for a local vendor with strong products and services. Also, existing AhnLab customers that are utilizing other AhnLab network and endpoint security products should consider AhnLab TG for better correlation utilizing AhnLab's centralized threat management solution.

Strengths

- **Customer Experience:** Gartner receives positive feedback about AhnLab technical support and its professional services team. The surveyed AhnLab TG firewall customers have given high scores to the vendor's technical support and professional services, citing quick responses and smooth product deployment experiences.
- **Sales Execution:** AhnLab is a strong security vendor in South Korea offering endpoint security, network security products and computer emergency response team (CERT) services in the region. It has a good presence in government and services verticals, with a big telco network as its existing client base.
- **Capability:** AhnLab has recently introduced better visibility and monitoring of SaaS applications with data loss prevention for these applications. This feature can help enterprises control and monitor the flow of data between users and these applications.
- **Capability:** The AhnLab TG firewall supports SSL VPN and IPsec. It offers browser-based endpoint security for SSL VPN users called AhnLab Online Security (AOS). AOS performs end-user machine checks through SSL VPN client such as AV and key logger checks before allowing access.
- **Product:** AhnLab has developed TMS, its big data centralized integrated threat management platform. This platform collects and correlates the threat intelligence from all other AhnLab products, including the TG firewall, TG IPX (IPS) and Sandbox TG DPX (anti-distributed denial of service [DDoS]). This will offer existing AhnLab customers that are utilizing multiple AhnLab products to get more visibility into their networks.

Cautions

- **Sales Execution:** AhnLab primarily sells in South Korea and is rarely shortlisted by clients outside that region. Its major presence is within distributed offices and SMB organizations. It has less presence with large enterprise-grade customers.
- **Product:** It does not offer any firewall hardware box with support for multiple virtual instances within. This type of deployment is requested by enterprise-level customers that want to run segmented separate networks primarily for compliance and security reasons.
- **Capability**: AhnLab offers advanced threat protection (ATP) network sandboxing as a separate appliance, not as a cloud-based service. So customers requiring an ATP network sandboxing feature will have to spend more, and will have to manage yet another appliance.
- **Product Strategy:** AhnLab still lacks enterprise-grade feature such as support for SDN and public IaaS platforms like Azure and Google Cloud, which are being offered by majority of enterprise firewall vendors to support the hybrid network requirements of their clients. Its AWS firewall was just released in 2Q18.
- **Market Execution:** AhnLab firewalls lack any third-party independent testing lab reports, such as such as ICSA Labs, NSS Labs or FIPS PUB 140-2, which many competitors have, and this makes it difficult for it to sell outside South Korea.

Barracuda

Based in Campbell, California, Barracuda targets organizations looking for cost-effective security solutions. Its firewall product line (CloudGen Firewall F-Series) includes physical and virtual appliances. It is available on IaaS platforms AWS, Microsoft Azure and Google Cloud. Its firewall centralized management solution (Firewall Control Center) is available as a hardware or software appliance. Its security portfolio also includes a web application firewall, data protection and email security solutions.

In January 2018, Barracuda acquired PhishLine, an email security awareness/computer-based training company. In March 2018, private equity investment firm Thomas Bravo completed the acquisition of Barracuda.

Recent product news shows a focus on industrial use cases, with the release of rugged appliances and support for specialized protocols. Barracuda has also made its centralized management available on the Google Cloud Platform, and further improved its integration with AWS and Microsoft Azure, along with its SD-WAN feature.

Barracuda is a good shortlist candidate for distributed enterprises. Large enterprises looking for cost-effective edge firewalls should include Barracuda in their shortlists but should request peer references and validate channel partner experience if they have high

throughput requirements for Layer 7 firewall features.

Strengths

- **Technical Support:** Surveyed customers, Gartner clients and feedback from Peer Insights all cite Barracuda technical support as being strong and responsive. Channel partners also like the quality of vendor support.
- **Sales Execution:** Barracuda is visible in distributed organizations' shortlists. A majority of its enterprise customers have more than 10 branches. Barracuda F-Series UTM products have a good presence on public IaaS platforms. Barracuda offers support for Microsoft Azure, AWS, VMware vCloud Air, Google Cloud Platform and ProfitBricks, and plans to expand this to other public IaaS platforms as well.
- **Sales Strategy:** Barracuda's total cost of ownership (TCO) is frequently better than its direct competitors when customers purchase multiple firewall devices.
- **Features:** Barracuda includes flexible options for URL filtering, including warning and override pages and user quotas. It also integrates with Zscaler to offload the inspection of the web traffic.
- **Features:** Barracuda customers cite the strong VPN features, including the proprietary VPN protocol (Transport Independent Network Architecture [TINA]), as a reason to select the vendor's firewall.

Cautions

- **Product Strategy:** The ongoing merger of the F-Series and the SMB-oriented X-Series continues to create additional complexity, such as duplicate choice for the management console of the F-Series. X-Series was scheduled to move to end-of-sale status in September 2018.
- **Technical Architecture:** Barracuda's centralized management console is available on Windows-only software, lacking a more flexible web-managed appliance. Gartner has had limited client feedback on how Barracuda's F-Series firewall alerts might influence security operations center (SOC) requirements.
- **Geographic Strategy:** Barracuda is not visible on enterprise firewall shortlists from large global enterprises, and in the Asia/Pacific and Middle East regions.
- **Product Execution:** The CloudGen Firewall lacks Common Criteria evaluation, limiting its appeal to some potential customers. Customers and surveyed resellers mentioned more hardware incidents recently, and attribute those to the newness of the product line.
- **Features:** The CloudGen Firewall lacks the ability to run multiple instances of its software on a single hardware appliance. It does not support active-active high-availability clustering. While the vendor is making progress in the right direction, surveyed customers would like to see better APIs to fully automate centralized management.

Check Point Software Technologies

Check Point Software Technologies is a global pure-play security vendor, with headquarters in Tel Aviv, Israel, and San Carlos, California. Its security portfolio, branded as the Check Point Infinity Architecture, includes enterprise firewall appliances (Security Gateway), virtual appliances available on the major cloud platforms (vSEC Security Gateway, recently rebranded CloudGuard IaaS). The SandBlast brand encompasses threat prevention technologies, including network sandboxing appliances, an endpoint security solution (Sandblast Agent) and a mobile security solution (SandBlast Mobile). Check Point centralized management suites (Security Management, SmartEvent and Compliance) are available as a physical appliance (Smart-1 security management appliance) or as software, with a Windows-based management console (SmartConsole).

Customers can purchase two bundles, including the firewall appliance, and a year's worth of security subscription: Next Generation Threat Prevention (NGTP), including core security and threat inspection features, and Next Generation Threat Extraction (NGTX), which adds network sandboxing (threat emulation), and content disarm and reconstruction (threat extraction).

In addition to the regular hardware refresh for its firewall and the launch of smaller management appliances, Check Point has launched its Infinity security architecture and a new SaaS security product (CloudGuard SaaS), and added support for Google Cloud and Alibaba Cloud for CloudGuard IaaS. More recently, Check Point introduced Check Point Next Generation Threat Prevention with improved machine learning capabilities. The vendor has also made significant changes in its pricing strategy, with the introduction of an all-inclusive global enterprise-level agreement, priced per protected user.

Enterprises looking for a firewall providing high-security threat inspection features, and ready to invest to get a high-quality management solution that supports the more complex policy management workflow, such as in the hybrid data center use case, should consider Check Point in their shortlists.

Strengths

- **Pricing Strategy:** After initial success in simplifying its firewall pricing bundles, Check Point is focused on simplifying large-enterprise pricing, with an all-inclusive, global enterprise-level subscription (Check Point Infinity Total Protection). This is priced per protected user and includes all software, security subscriptions, service and support, in addition to a predefined budget for hardware purchase and renew.
- **Product Execution:** Check Point has one of the largest threat research teams of vendors evaluated in this research. It also offers a third-party threat intelligence feed as an additional option for its customers, further increasing the scope of its threat intelligence offering. The vendor's cloud-based sandboxing subscription has now reached a substantial customer base and contributes to improving the vendor's threat intelligence dataset.
- **Partners:** Check Point has a strong ecosystem of technology partners, making it easier for large organizations to integrate Check Point in a broader ecosystem. Check Point also has a well-established channel, including partners experienced in larger, more complex deployments, in many countries.
- **Vertical strategy:** For many years, Check Point has invested heavily on building specialized offerings to respond to vertical-specific challenges in various industries, including telecommunications, industrial systems/critical infrastructure, healthcare, financial institutions and local governments.
- **Capabilities:** Customers give good scores to Check Point's continued ability to provide high security and good management, even for complex and highly exposed environments. Its management suite includes several features such as Multi-Domain Security Management and SmartProvisioning to specifically serve managed security service providers (MSSPs).
- **Geographic Strategy:** Check Point has invested significantly in its global support operations, especially in its local support centers in the Asia/Pacific region.

Cautions

- **Marketing Execution:** Check Point manages to maintain a perception of providing high-security solutions among its customer and prospects, but fails to revitalize its brand as an innovator. It loses market share to Fortinet and Palo Alto Networks, and is less frequently visible in firewall shortlists than in the past.
- **Market Responsiveness:** R80.10 was released more than a year ago, after an almost two-year release cycle for the R80.0 version. Its TLS acceleration cards, announced in 2016, are not yet available.
- **Performance:** Customers and surveyed resellers perceive performance issues, giving lower scores for overall performance compared to other rated aspects of Check Point's firewall. Sustaining performance under high load and getting the right product sizing are the most frequently mentioned issues.
- **Features:** Check Point cannot apply quality of service when using multiple WAN links. It can decrypt only HTTPS, missing the decryption support for FTPS and SSH that some organizations require.
- **Technical Support:** Surveyed customers mention that to get good support from the vendor, you need to pay for the higher support plans. They also mention insufficient documentation in the form of "how to" recipes. The vendor is trying to remedy this with its CheckMates community portal, launched in 2017.

Cisco

Cisco, headquartered in San Jose, California, is a large infrastructure vendor. Its product portfolio includes multiple infrastructure products and services. Firewalls are part of its security product line. In addition to firewalls, Cisco has a broad portfolio of additional security products and capabilities. These include advanced endpoint security, network traffic analysis (Stealthwatch), secure web gateway (SWG), DNS security (Umbrella), email security, network access control, and a cloud access security broker (CASB) — with Talos threat intelligence included with all Cisco security products at no cost.

Cisco continues to sell multiple firewall product lines: Cisco Adaptive Security Appliance (ASA), Cisco ASA with FirePOWER Services and Cisco Firepower. It also sells the Cisco Meraki MX UTM product line with separate cloud-based management targeting branch office use cases. Cisco ASA and Cisco Firepower have separate on-premises centralized managers: Cisco Security Manager (CSM) and Firepower Management Center (FMC). While Cisco ASA with FirePOWER Services requires both of the aforementioned managers to administer the ASA and ASA with FirePOWER services separately, Cisco Meraki MX can be centrally managed using only a cloud-based management portal. Cisco has also introduced Cisco Defense Orchestrator (CDO), its cloud-based centralized manager to manage Cisco ASA, Cisco ASA with FirePOWER Services and Cisco Firepower Threat Defense (FTD).

During the evaluation period, Cisco introduced the new Firepower 2100 Series models. It also released Snort v3.0 and enhancements around integration of Cisco security product lines.

Cisco firewalls are a good shortlist item for enterprises that are already a Cisco house or that prefer to consolidate their security architecture with single vendor. The vendor is a good candidate for enterprises looking for single-vendor security integration for better visibility.

Strengths

- **Product Execution:** Cisco Talos, which is the vendor's centralized threat intelligence team, offers strong threat research powering multiple Cisco network security platforms. Surveyed Cisco firewall customers and partners have rated Talos as a strong product differentiator. In addition to its own feeds into Talos, Cisco has a strong partnership alliance of multiple public and private security feeds, including open-source communities, and key partnership contributions include the Cyber Threat Alliance, NATO, CenturyLink, KISA, NICT, and IBM.
- **Capability:** Cisco Firepower 4100 Series and 9300 appliances have Radware DDoS mitigation with Virtual DefensePro (vDP), which can be enabled as an add-on module, making it the only firewall providing enterprise-grade DDoS mitigation capabilities without purchasing an additional DDoS mitigation product.
- **Sales Strategy:** Cisco has shown the ability to execute on selling many of its security software and support offerings under broad-ranging security ELAs. These packages provide significant savings for enterprise security and risk leaders who want to consolidate the number of security vendors they manage.
- **Market Responsiveness:** Cisco offers machine learning capabilities with SPERO, a machine learning engine used by Cisco Advanced Malware Protection (AMP) and Firepower utilizing active heuristics. This addresses the end-user market looking for better advanced threat detection capabilities as an important firewall shortlisting criterion.
- **Market Execution:** Cisco Firepower Next-Generation IPS (NGIPS) — with AMP — is rated higher and competes strongly in the market where IPS capability is a strong selection use case. Surveyed Cisco partners have also highlighted Cisco Firepower NGIPS as a strong feature. The vendor has also received third-party independent lab ratings for security effectiveness in breach detection systems (BDSs).

Cautions

- **Product Execution:** Cisco continues to sell different firewall product lines, namely Cisco ASA, Cisco ASA with FirePOWER Services and Cisco Firepower. This generates lot of confusion with the end-user market, which is not sure which firewall type will be the right fit. Cisco also sells the Cisco Meraki MX firewall product line with separate cloud-based management, targeting branch office use case. There is a lack of clarity regarding the differences in security services and hardware capabilities of these products.
- **Product Strategy:** Cisco offers different on-box UIs and on-premises centralized management for its various firewall product lines, as mentioned above. Cisco ASA and Cisco ASA with FirePOWER Services utilize Adaptive Security Device Manager (ASDM), while Cisco Firepower firewalls utilize Firepower Device Manager (FDM) for on-box administration. Also, while Cisco ASAs require CSM and Cisco Firepower requires FMC for on-premises centralized management, Cisco ASA with FirePOWER Services requires both CSM and FMC to manage the respective interfaces of the same firewall device, which creates operational overhead.
- **Go-to-Market Execution:** The learning curve for existing Cisco customers moving away from Cisco ASA toward Cisco Firepower is almost equivalent to moving to a non-Cisco firewall. The management interface and the administrative experience is altogether different. As a result, Gartner has observed Cisco's existing clients shortlisting other firewall vendors in addition to Cisco Firepower for evaluation of capabilities.
- **Customer Experience:** The surveyed Cisco Firepower customers and partners have reported initial implementation issues with the FTD code, specifically highlighting frequent restart of Snort processes, which led to multiple operational issues. They also reported that this

took the Cisco Technical Assistance Center (TAC) more than the usual time for resolution. Snort restart issues were largely addressed in FTD version 6.2.3, released in April 2018.

- **Capability:** Cisco firewalls do not integrate with any third-party endpoint detection and response (EDR) tools and only offer integration capabilities with its own Cisco AMP endpoints for detection of malware. Cisco Firepower appliances also lack SSL VPN functionality.

Forcepoint

Based in Austin, Texas, Forcepoint is a pure-play security vendor. It offers a firewall (Forcepoint NGFW), web and email security gateways (Forcepoint Web Security and Forcepoint Email Security), a data loss prevention offering (Forcepoint DLP), an insider threat solution (Forcepoint Insider Threat), a cloud access security broker offering (Forcepoint CASB), and a user and entity behavior analytics offering (Forcepoint UEBA), in addition to government-specific security solutions. The vendor has more than 2,500 employees. The Forcepoint NGFW product line was acquired from Intel Security in 2016, along with McAfee Firewall Enterprise (Sidewinder was part of the Secure Computing acquisition by McAfee in 2008).

Forcepoint's recent news includes the availability of eight new hardware appliances (NGFW 330, 331, 335, 1101, 1105, 2101, 2105, 6205), and the NGFW virtual offerings on Azure and Hyper-V. The vendor also introduced Advanced Malware Detection (AMD), which is cloud- and on-premises-based sandboxing.

Forcepoint has demonstrated consistently good feature quality and has been executing on its roadmap. The vendor is a valid shortlist candidate on enterprise firewall shortlists for distributed organizations.

Strengths

- **Product Execution:** Forcepoint has successfully productized good SD-WAN capabilities into firewalls for branch offices of distributed enterprises. The vendor has also taken advantage of its cloud security portfolio by doing service chaining with its fully featured secure web gateway.
- **Customer Experience:** Customers give excellent scores to the centralized management console, Forcepoint NGFW Security Management Center (SMC), and high availability. In fact, the ability to do robust clustering is a differentiator, and a high percentage of Forcepoint customers deploy two or more units in active-active mode.
- **Capabilities:** Independent tests continue to grant Forcepoint NGFW better results for attack detection than some of the Leaders evaluated in this research. The vendor has a historical focus on building detection engines resistant to evasion techniques, and this focus is reflected in recent group test results.
- **Ease of Use:** A zero-touch deployment is available for Forcepoint NGFW. The filtering policy commit process integrates an optional approval workflow. SMC includes easy-to-use filters and visualizations to ease the analysis of incidents.
- **Geographic Strategy:** In addition to being highly visible on EMEA shortlists, Forcepoint has increased its percentage of revenue derived from the North American region to nearly half of its firewall sales.

Cautions

- **Geographic Strategy:** Forcepoint NGFW continues to have much lower visibility among enterprise firewall buyers in North America and the Asia/Pacific region than in Europe. In 2017, Forcepoint recruited more channel partners in North America.
- **User Experience:** North American customers note that the user community is small and there are not enough qualified third-party vendors to support it. It can be difficult for customers to hire expert engineers to work with Forcepoint NGFW.
- **Market Responsiveness:** Forcepoint has no integration with market-leading security information and event management (SIEM) Splunk except for the basic ability to forward syslogs to it. Forcepoint can also forward syslogs to other SIEM applications. The vendor has no EDR or endpoint protection platform (EPP) tool, and has few integrations with third-party tools except for McAfee endpoint protection software. Some enterprises value firewall/endpoint integration for a fuller picture of security.
- **Capabilities:** Forcepoint's firewall offering does not yet fully integrate with the recently acquired Forcepoint CASB, relying instead on service chaining the CASB solution to the firewall without enabling full orchestration from the firewall console.
- **Product Strategy:** Forcepoint has been late in its approach to securing cloud environments. Its NGFW has very little public and private cloud presence. Forcepoint NGFW's high availability is less appealing for SDN and IaaS use cases, where part of the resiliency

requirements are handled by the infrastructure. Forcepoint NGFW added support for Microsoft Azure in October 2017, lagging many competitors.

Fortinet

Fortinet is a network and security player, headquartered in Sunnyvale, California. It is regularly expanding its product portfolio with FortiSIEM and FortiCASB being recent additions. The vendor's other products in the portfolio cover network security, endpoint security, SIEM, wireless access points and switches. FortiGate firewalls are still the vendor's most popular and largest selling products.

In 2017, Fortinet introduced its E-Series firewall appliances, namely FortiGate 100E, 200E, 300E, 500E, 3900 and 7000 Series; in 2018, Fortinet has released its 6000 Series. It also expanded its support to multiple public IaaS platforms, including Google, IBM and Oracle.

Fortinet recently announced the acquisition of Bradford Networks, a network access control (NAC) solution provider. Fortinet also announced a closer collaborative partnership with IBM X-Force Threat Management services.

Feature news includes the release of FortiOS 5.6 in 2017 and FortiOS 6.0 in early 2018, with a primary focus on enhancements such as improved automation across the Fortinet Security Fabric and fabric support for various products within and outside the Fortinet portfolio, using Fabric Connectors. The Fortinet Security Fabric aims to provide visibility and protection across the entire network in an automated, integrated fabric of security controls. The vendor also added the WAN Path Controller to its combined enterprise firewall with SD-WAN offering.

Fortinet continues to be visible by Gartner on the firewall shortlists of enterprise-grade customers for whom pricing is the primary selection criterion. The vendor is continuously adding new products to its portfolio to compete in large network security deals with its firewall, web application firewall (WAF), SIEM and FortiSandbox.

Strengths

- **Sales Execution:** Fortinet continues to be one of the most visible vendors in Gartner client shortlists for firewall by enterprise customers looking for a perimeter security use case.
- **Customer Experience:** Surveyed customers have highlighted competitive price for performance as one of the strongest reasons to shortlist the vendor, along with support for multiple features that other leading firewall vendors offer at higher cost.
- **Product:** Fortinet is the only firewall vendor that offers support for IBM and Oracle public IaaS cloud platforms in addition to AWS, Azure and Google Cloud. This makes it a favorable shortlist candidate for enterprises using these IaaS cloud platforms.
- **Capabilities:** Fortinet offers unified control and management across its multiple product lines through Security Fabric, and continues to focus on enhancements across the Security Fabric features. The Security Fabric supported components are FortiGate firewalls, SIEM access points, endpoint security, secure email and web application firewall. This enables existing Fortinet customers who are using multiple Fortinet products to have unified monitoring and control across different Fortinet devices in their network or across multiple networks.
- **Geographic Strategy:** Fortinet firewalls are visible across geographies and compete strongly with regional firewall vendors. The vendor has both channel and direct presence across the globe, including a large focus on developing markets.

Cautions

- **Marketing:** Fortinet still lacks recognition as a strong enterprise-grade firewall with premium features and is primarily shortlisted because of better pricing with bundled features. The vendor lacks premium subscription and support services desired by enterprise-grade customers.
- **Product Strategy:** Fortinet's product strategy is more focused on expanding its portfolio with products like FortiWeb, FortiSIEM and FortiClient, and enhancing Security Fabric features. It lacks enhancements to its firewall product. Gartner has observed the vendor's sales and marketing teams strongly promoting and focusing on sales of larger deals involving multiple Fortinet products. Gartner clients have reported poor presales support for smaller deals that only involve a pair of firewalls.
- **Customer Experience:** Gartner receives mixed feedback on Fortinet technical support. Gartner clients and surveyed clients have reported poor technical support on new product models and new features. They have also reported that the technical support team took longer than usual for the resolution of product- and feature-related issues.

- **Innovation:** Fortinet lacks in innovation in firewall features and capabilities. Although it is quick to develop features and introduce them in the firewall, it fails to innovate and be the first vendor to introduce enterprise-grade firewall features in its products.

Hillstone

Hillstone is headquartered in Beijing, China, with regional headquarters in Santa Clara, California. The vendor is an established network security player offering perimeter, cloud and server security solutions.

Physical appliances include E-Series NGFW, T-Series iNGFW and X-Series Data Center Firewall. Virtual platforms are CloudEdge (virtual firewall) and CloudHive (for microsegmentation), Hillstone Security Management (HSM) platform, Hillstone Security Audit (HSA) platform, and Hillstone CloudView, for cloud-based security management, comprising the central management portfolio.

During the evaluation period, Hillstone delivered nine new hardware models, including a high-end data center model that the vendor claims can reach 1 terabit per second in performance.

Product news includes integration with network cloud sandbox vendor Lastline and CASB vendor cloudscreen, as well as achievement of a VMware-ready certification for the CloudHive microsegmentation solution. The vendor improved TLS/SSL decryption capabilities and performance for its virtual firewalls.

Hillstone is one of the few Chinese network security vendors that is gradually expanding into other regions outside China, such as Southeast Asia, Europe, the Middle East and Africa, and Latin America. It has expanded its channels in different regions.

Hillstone firewalls are well-suited for shortlists in enterprises with hybrid networks, such as on-premises, cloud and virtualized environments in the previously mentioned regions.

Strengths

- **Product Strategy:** CloudHive and CloudEdge (with support for multivendor public clouds) aid hybrid enterprises in their quest to move to a single vendor, helping to reduce the management complexity many hybrid network customers experience. Hillstone's recent VMware NSX certification helps complete this story.
- **Features:** Customers and partners like Hillstone's strong networking features such as granular quality of service (QoS) and advanced high availability and clustering. Users have rated Hillstone's abnormal behavior detection network traffic analysis feature as one of the product's strengths. They also appreciate the Insight screen with the kill chain map, as it shows the exact status of every attack.
- **Public Clouds:** Hillstone's virtual CloudEdge firewalls support all the major regional local cloud platforms in China, including carrier cloud (China Unicom, China Telecom and China Mobile), Jindong Cloud, Huawei Cloud, AliCloud and other global public clouds like AWS and Azure. Hillstone also provides CloudEdge for network function virtualization (NFV) to support customer NFV efforts.
- **Segmentation:** Hillstone CloudHive offers a microsegmentation solution for virtual VMware networks along with CloudEdge virtual firewalls for networks in the cloud. This offering makes Hillstone a strong vendor for cloud security use cases.

Cautions

- **Marketing Execution:** Surveyed partners have indicated that Hillstone still lacks brand recognition outside China. Now that Hillstone has built out its partner list in several non-China regions, Gartner believes the vendor needs to focus more on strong marketing in those regions, where there are multiple strong firewall vendors with strong marketing.
- **Customer experience:** Hillstone customers note that documentation for new features could be clearer, and the user interface and reporting need improvement.
- **Product Strategy:** Dividing the firewall product line into E-Series (NGFW) and T-Series (intelligent NGFW [iNGFW]) is confusing to prospects deciding which to evaluate.
- **Product Execution:** Hillstone only offers cloud-based network sandboxing and does not offer it as a separate appliance on its price list. Gartner has observed that many enterprises with large data centers that want to build a private cloud for scanning their traffic against advanced malware seek an on-premises network sandboxing appliance, as opposed to a cloud service. This will lead such enterprises to select a different vendor, as Hillstone does not offer this.

Huawei

Shenzhen, China-based Huawei has been shipping firewall products for more than a decade, and offers a variety of other network security appliances, including anti-DDoS and IPS. Huawei ships a wide range of firewalls for customers that already have Huawei products and wish to expand their business to firewalls. Unified Security Gateway (USG) is the primary enterprise line, and Eudemon is the model line for carriers and service providers. eSight, Agile Controller and SecoManager are the central management platforms that support the USG line. Huawei USG firewalls have been certified by ICSA, at the EAL4+ under Common Criteria. Related security services can be used via the USG6000V virtual gateway to implement virtual multitenant separation.

Huawei released a new USG6100 line during the evaluation period for this Magic Quadrant. Recent features include enhanced clustering support and enhanced cloud security features. Huawei now has a virtual firewall that supports Azure. The vendor also opened a new cloud sandboxing location in Europe.

Huawei has executed a fast ramp-up in market presence, particularly in EMEA; however, we still do not see it frequently displacing Leaders based on vision or features.

Huawei is a relevant shortlist candidate for value-conscious enterprises located in the Asia/Pacific region or EMEA, especially enterprises with high-performance needs.

Strengths

- **Marketing and Sales Execution:** Huawei's firewall sales greatly outgrew the overall enterprise firewall market during the evaluation period, demonstrating new perceived value.
- **Geographic Strategy:** Huawei has developed a strong channel in EMEA, and is focusing a significant part of its growth plans on the Middle East and Latin America, which are its two fastest-growing regions.
- **Product Execution:** Huawei is executing on its roadmap, particularly around public cloud use cases. Surveyed Huawei stakeholders cite application control as a particularly strong feature.
- **Portfolio Strategy:** Customers with networks based primarily on Huawei infrastructure products include Huawei firewalls on their shortlists. Huawei customers still like that the firewalls are well-integrated with their infrastructure components.
- **Product Strategy:** Surveyed customers and partners like that Huawei provides good throughput for a low price. Throughput/performance was a consistently listed reason for consideration.

Cautions

- **Product Strategy:** Huawei does not release new capabilities as fast as its leading competitors. The vendor spends considerable focus on building features for service providers. Gartner enterprise clients that want first-to-market security capabilities do not often consider Huawei USG as a shortlist candidate.
- **Product Execution:** Huawei users continue to comment that they would like enhanced reporting and a better GUI, and that configuration through the GUI could be made easier.
- **Marketing Execution:** Huawei continues to have limited competitive visibility outside the Asia/Pacific region and EMEA, although Latin American awareness is growing. The vendor consistently takes meaningful steps to address concerns about relying on technology developed in China; however, this concern continues to be a security sales challenge in some markets, especially North America.
- **Customer Experience:** Some customers outside of the Asia/Pacific region note perceived lack of local support as a negative, especially when they need help resolving issues with the technology.

Juniper Networks

Juniper Networks, headquartered in Sunnyvale, California, is a networking infrastructure vendor with a long track record of providing network security capabilities. Its physical enterprise firewall line, the SRX Series, comprises 12 models. Juniper has two virtual firewalls — vSRX and cSRX. The cSRX is a firewall that can protect containerized environments. Its Security Director is the central management platform. The vendor offers AppSecure for application control and visibility, integrated IPS, integrated threat intelligence feeds, and a new cloud-based anti-malware service (Sky Advanced Threat Protection [ATP]). In addition, Juniper has Software-Defined Secure Network (SDSN), which aims to integrate security into all elements of the network infrastructure, whether it is Juniper's or another vendor's, in order to minimize the impact of any compromised device.

Juniper's recent enterprise firewall news includes SDSN Policy Enforcer support for third-party switches with ForeScout, private cloud with Contrail and VMware for NSX, and public cloud (for AWS). Juniper also recently introduced the SRX4600, an extension of its midrange enterprise firewall line. The vendor was certified as IPv6-ready. Finally, in vSRX news, Juniper provided versions for Azure and Hyper-V, as well as multicore version with eight cores and 16 cores.

Juniper is a good shortlist candidate for enterprises that desire high throughput and good security at a low price, and the ability for the firewall to support advanced routing scenarios. It is also suitable for enterprises buying security and networking in the same buying center.

Strengths

- **Product Execution:** Surveyed customers and partners often note satisfaction with the SRX's ease of configuration, rich interface and ease of performing deep analysis of real-time events, often citing these as primary reasons for selection and continued usage. Juniper has a strong range of branch office firewalls complementing its enterprise products.
- **Product Strategy:** Juniper has a strong SDN security story around vSRX, cSRX and the Juniper Contrail SDN framework, supporting it with its developing SDSN schema. The extension of SDSN to enforce policy on third-party switches shows meaningful commitment to push SDSN outside of Juniper infrastructure boundaries. The vendor is the first vendor in the enterprise firewall space to offer a container-focused firewall.
- **Product Performance:** Good options exist for high-throughput, purpose-built appliances, especially in the higher-end SRX models, because Gartner sees Juniper often deployed in large data centers. The vSRX offering is highly rated for performance relative to other virtual firewalls, and is cited for strong clustering and advanced routing capabilities. The clustering has improved during this evaluation period, as Juniper introduced 8- and 16-core versions.
- **Marketing Execution:** During the evaluation period for this Magic Quadrant, Gartner began to see some nonincumbent Juniper shops asking about Juniper firewalls that they had moved away from in years past. Juniper's marketing about Sky ATP and SDSN, and news of the Cyphort acquisition, seem to have sparked a bit of interest among Gartner clients. Continued emphasis on these items will encourage more existing customers to stick with Juniper and, if this marketing execution is consistent and sustained, could inspire more potential prospects to evaluate the SRX line.

Cautions

- **Innovation:** Gartner clients and surveyed customers and partners continue to perceive that Juniper lags behind its major competitors in releasing new security features. Surveyed customers did not mention innovation or roadmap as a reason for selecting Juniper firewalls, despite the vendor's early lead in areas such as containerized security.
- **Product Execution:** Juniper has a legacy of being late to market with some features compared to some competitors in areas such as application control, public cloud support and advanced malware detection. As a result, Gartner clients often express a lack of confidence in Juniper's security strategy. These gaps have been remedied over the past two years, but Juniper must continue to execute and deliver a steady stream of competitive security features to rebuild confidence in its channel and customer base.
- **Product Strategy:** Gartner believes that most enterprises want an operating system in their security products that differs from the one in network infrastructure components.
- **Marketing Execution:** Surveyed partners all pointed to marketing support as the chief weakness in Juniper's overall security approach. Gartner agrees. SDSN messaging is overly complicated and Juniper should aggressively develop and promote its new unified cybersecurity platform messaging. The real-world value of Juniper security tools is not clearly articulated so that prospects and customers will feel compelled to consider Juniper as a strong candidate for their use cases.
- **Sales Execution:** Juniper has continued to lose security market share in the past year, and has experienced declining year-over-year revenue in a growing market; however, it posted double-digit year-over-year revenue growth for the past three quarters. The vendor must more effectively address fundamental sales challenges, and demonstrate that it can win back customers and market share with its newer capabilities.

New H3C Group

New H3C Group was established in November 2003 and is headquartered in Hangzhou, China. Until 2016, it operated as a subsidiary of Hewlett Packard Enterprise (HPE) and now is a part of Tsinghua Unigroup. It is a strong infrastructure vendor in China with a large

portfolio, including security products that also cover firewalls, cloud computing products, switches, routers, wireless LAN (WLAN) products and management products.

Its SecPath firewall family comprises 14 physical appliances, which scale up to 320 Gbps, and five virtual models.

During the evaluation period, the vendor released a SecBlade module for high-end firewalls, along with a line of SMB-focused firewalls. New H3C also worked on enhancing advanced threat detection efficacy.

While the vendor is focusing more on introducing new product offerings for different growing markets, it still lacks the market understanding and strong product strategy for meeting all enterprise firewall use cases. It lacks multiple built-in security features, such as network sandboxing, SD-WAN capabilities and SaaS application monitoring, which the majority of competitors in the region offer.

The vendor's firewalls should be considered by clients based in China that are already using its products and are looking for a high-performance, strong firewall with basic security features.

Strengths

- **Portfolio:** New H3C has a large portfolio of products and offerings. It offers a range of solutions for data centers, cloud infrastructure and big data. Product offerings include servers, storage products, security products, networking and software. This gives an advantage to end users that want to maintain a single vendor relationship for their broad range of infrastructure products.
- **Security Architecture:** The vendor offers H3C SecCenter Management Center for centrally managing the security devices on a network. It includes the function modules IPS Manager, UTM Manager, Firewall Manager and intelligent Traffic Analysis System (iTAS). This gives an advantage to existing customers, providing centralized management of a variety of devices.
- **Offering:** New H3C Group also offers H3C SecBlade FW modules, which can be used on H3C switches (S5800, S7500E, S9500E or S12500) and routers (SR6600 and SR8800). These SecBlade FW modules help customers extend network security capabilities within their existing H3C switches and routers.
- **Customer Experience:** Virtualization is a strong capability in the New H3C Group firewall, enabled by the Intelligent Flow Forwarding (IFF) and Security ONE Platform (SOP) features of the SecPath M9000 Multi Service Security Gateway Series. The IFF feature is designed to implement distributed traffic flow and the SOP feature offers a virtual firewall function using container-based virtualization technology.
- **Capabilities:** Since New H3C Group is a large infrastructure vendor, it has invested a large amount to develop a high-end testing center and lab with enhanced testing capabilities. This shows commitment from the vendor to deliver reliable products and services to the market.

Cautions

- **Product Strategy:** New H3C Group's firewall offerings and feature enhancements are still more focused on carrier and large data center use cases that operate in highly virtualized environments. This has led to a lack of focus on meeting all enterprise firewall use cases, especially perimeter security for enterprises.
- **Features:** The vendor's firewalls lack an advanced malware network sandboxing feature, which is offered by a most firewall vendors, including those in China. This leaves customers needing to select a separate vendor for advanced malware capabilities, as opposed to having those capabilities as an add-on feature of their existing firewalls. New H3C does not offer any CASB integration and lacks SaaS monitoring and management features, which increasingly are sought by enterprises with growing adoption of SaaS applications.
- **Marketing Execution:** The vendor's firewalls lack recognition and brand value among enterprises in its local market. During this evaluation period, regional vendors did not list it as a leading competitor, whereas two other Chinese vendors were mentioned.
- **Geographic Strategy:** Unlike some in-country competitors, New H3C Group is unknown outside of China.

Palo Alto Networks

Based in Santa Clara, California, Palo Alto Networks is a large security vendor with more than 5,100 employees. It has been shipping enterprise firewalls since 2007, and its 2017 revenue exceeded $1.75 billion. In addition to enterprise firewall physical and virtual appliances, Palo Alto Networks' products include endpoint software (Traps and GlobalProtect), threat Intelligence (AutoFocus), and SaaS

security (Aperture). The vendor has built integrations between its offerings as a security operating platform, and has recently introduced its Application Framework program, wherein third parties can build applications that will integrate with Palo Alto Networks platform.

Company news includes the acquisition of Secdo, an EDR vendor that has capabilities that Palo Alto Networks will integrate into Traps. Additionally, Evident.io, an API-based security and compliance cloud company, was acquired and is now part of Palo Alto's cloud security offering.

Palo Alto Networks has recently released a firewall-as-a-service offering, GlobalProtect Cloud Service, to secure remote offices and mobile users. It has also introduced Magnifier, the first application built on the vendor's Application Framework; it provides behavioral analytics with technology from the LightCyber acquisition. Palo Alto Networks also released its cloud-based Logging Service. Additionally, with added hardware acceleration and software modifications in its PAN-OS 8.1 release, the vendor has enhanced its TLS decryption capabilities.

The company released a new ruggedized hardware model (PA-220R), two new intermediate appliances (both in the PA-800 Series), refreshed its PA-3000 Series, available since 2011, with the PA-3220, PA-3250 and PA-3260 models, and added PA-5280 to the PA-5200 Series introduced in 2017.

Palo Alto Networks enjoys continued success in competitive enterprise firewall selections, and has high customer satisfaction for its application visibility capabilities.

It is a solid contender for all enterprises, especially when evaluations give more weight to feature and management quality than to price.

Strengths

- **Product Strategy:** The vendor's refresh of its product line across 2017 and early 2018 brought more competitive price/performance ratios to the market. GlobalProtect Cloud Service, Palo Alto Networks' recently-introduced firewall-as-a-service offering, has gained notable early traction.
- **Marketing Execution:** Palo Alto Networks remains the pure-play security vendor with the highest visibility on enterprise firewall shortlists, across all industries. Customers like its story, and surveyed customers point to innovation and Palo Alto Networks' roadmap as primary factors in its selection.
- **Sales Execution:** Palo Alto Networks maintains a very high growth rate. The vendor enjoys high attach rates for Threat Prevention (IPS and antivirus), URL filtering, and WildFire (cloud sandboxing). During the evaluation period, Gartner observed Palo Alto Networks' Enterprise License Agreement — encompassing its product portfolio — being used more frequently.
- **Capabilities:** The Application Command Center (ACC) includes visibility of sanctioned and unsanctioned SaaS applications. Combined with its automated event aggregation, and filtering and drill-down options, it is easy to understand application flows and related risks.
- **Customer Experience:** Palo Alto Networks continues to score highly for overall customer satisfaction, and vendor support is noted as a strength.
- **Improvements:** The vendor's ability to support a higher number of decrypted concurrent TLS connections, previously enhanced by hardware improvements, has been further realized with software modifications. Gartner clients report that on-box decryption performance is more competitive.

Cautions

- **Pricing:** Even with improved price/performance ratios in recently released products, price is frequently cited by Gartner clients as a reason not to select Palo Alto Networks. The vendor has a smaller market share than its direct competitors in some of the European countries and Asia. Organizations from these regions should evaluate local resellers more stringently and request local references, especially in regions where the vendor does not provide direct vendor support.
- **Product Strategy:** Gartner clients and surveyed customers note that early versions after a major software release have bugs and are not production-ready. Very large releases require more time to stabilize.
- **Product Execution:** The number of virtual instances supported on a single appliance is lower than the number supported by major competitors. The vendor's customers would prefer to have better clustering capabilities in the physical firewalls.
- **Customer Experience:** Despite recent scalability enhancements, the vendor's centralized management solution, Panorama, manages fewer firewalls than most competitors' central managers do. Some clients still cite that Panorama can become slow when managing a

large number of appliances.

Sangfor

Based in Shenzhen, China, Sangfor is a large IT infrastructure and security vendor. The vendor employs more than 3,500 staff, and is implemented internationally through multiple regional headquarters, including in the Asia/Pacific region (Singapore, Malaysia, Hong Kong, Indonesia, etc.), the U.S. (Fremont, California), and the Middle East region (Dubai, UAE), as well as Europe (Italy). Sangfor brands its firewall product line (Next Generation Application Firewall [NGAF]) as a combination of network and web application firewall, available in the form of physical and virtual appliances. Centralized management (Sangfor Branch Business Center [BBC]) and centralized reporting (Situation Awareness System) appliances are available. In addition, Sangfor offers other security solutions, including network and application vulnerability management SaaS, SSL VPN, network optimization (WAN Optimization [WANO]), software-defined infrastructure and SWG solutions.

Recently, Sangfor announced the availability of firewall-as-a-service and new threat intelligence options. Recent firewall updates include UI simplification, policy templates and geo-IP improvements.

Sangfor serves a narrow segment of the market, with its presence mostly limited to a few countries in the Asia/Pacific region, and primarily serving upper-midsize organizations. The vendor is a good shortlist contender for customers that expect good analytics and understanding of their security posture. Prospects outside of China should first verify the local presence of the vendor, and the ability to get the required technical support, especially organizations with international deployments.

Strengths

- **Organization:** Sangfor is a large company, with sizable R&D focused on enterprise firewall and its threat research team.
- **Technical Architecture:** Customers like that it is easy to integrate the firewall with the vendor's cloud-based web proxy.
- **Feature:** Sangfor provides strong security analytics dashboards, displaying the main attack phases and leveraging a multiple-analytics-engine approach to offer vulnerability, user and even some level of business context. Customers praise Sangfor's ability to quickly grasp the whole situation and security posture of their environments.
- **Product Execution:** Customers give a good score to the hardware and software update quality. They also cite the clear reports and visualization as very helpful when deploying the solution.
- **Support:** Surveyedcustomers and resellers give a good score to Sangfor's support, especially for the vendor's ability to answer in a timely and detailed manner.

Cautions

- **Geographic Strategy:** Sangfor's firewalls are visible to Gartner only in the Asia/Pacific region. Sangfor technical support is mostly centralized from the Malaysian call center, with two other call centers in mainland China. The vendor provides support in English, but not in other European or South American languages.
- **Market Segmentation**: Sangfor sells primarily to midsize enterprises and is more rarely seen in very large organizations.
- **Product Execution:** Sangfor firewalls have not participated in any recent independent testing proving the efficacy of the IPS engine and resistance to evasion attempts. Sangfor does not offer firewall models with integrated Wi-Fi, unlike many of its midmarket competitors. It also lacks inexpensive appliances for the smaller branches.
- **Features:** Surveyed customers would like to see a more responsive UI. The cloud sandboxing emulation is limited to Windows operating systems. The vendor's firewall appliances lag dedicated hardware acceleration for SSL decryption.
- **Technical Architecture:** Sangfor NGAF lacks integration with IaaS platforms. It is not yet available on the AWS Marketplace, Microsoft Azure or the English language version of the Alibaba Cloud Marketplace. Because of partial IPv6 support, Sangfor firewalls might not integrate well in dual-stack environments.

SonicWall

Now based in Santa Clara, California, SonicWall was spun out of Dell in 4Q16 and is now a private stand-alone company owned by Francisco Partners. SonicWall's enterprise firewall portfolio comprises a total of nine virtual appliances ranging from one to 16 cores in its

Network Security virtual (NSv) series. There are five physical appliances across the TZ Series — aimed at small branches or distributed enterprise businesses; eight models of its Network Security appliance (NSa) series for midsize enterprises; and the Network Security services platform (NSsp) series for large enterprises, data center deployments and service providers.

SonicWall has two central management system options — the legacy Global Management System (GMS) and the recently released Capture Security Center. SonicWall's Capture Security Center allows customers to control and manage, configure, and perform analytics on network traffic with its TZ and NSa product lines. In addition to its GMS console, which targets large-enterprise environments, SonicWall also offers Analyzer for additional reporting and traffic analysis for large enterprises.

Recent company news includes the release of Capture Client endpoint software. Capture Client leverages SentinelOne technology in tandem with SSL Certificate management and malware "roll-back" capabilities. Capture Cloud Platform combines Capture Threat Network intelligence with its Capture Security Center. The launch of the SonicWall NSsp chassis-based product line targets service providers, large data centers and higher education institutions.

SonicWall is still not visible on a large number of enterprise shortlists, and it does not yet address some enterprise data center use cases. The vendor is a good shortlist candidate for value-conscious enterprises that desire good throughput and security effectiveness at a reasonable price and a solid firewall appliance that is easy to manage.

Strengths

- **User Experience:** SonicWall receives high scores for ease of management. Users report that it is easy to set up and use and is a good choice for less complicated networks.
- **Product Performance:** SonicWall customers and partners note that the vendor does a very good job of handling SSL/TLS decryption on-box without massive performance degradation, and the vendor has improved its capabilities during the evaluation period. Overall product performance remains a strength for SonicWall.
- **Product Strategy:** The cloud-based Capture Advanced Threat Protection service takes a multiengine approach to advanced threat detection, where its most differentiating feature is its ability to utilize real-time deep memory inspection that it claims detects threats other sandboxes do not. This approach continues to get good feedback from customers, and it has received relatively quick uptake from net new customers, some of which cite Capture ATP as a motivator to purchase.
- **Sales Execution:** Cost management is an often-stated reason for SonicWall product selection. Gartner clients cite that SonicWall products remain on the low end of the cost range. With the improvements the vendor has made in simplifying the management and analytics experience, management labor costs are reduced.
- **Marketing Strategy:** SonicWall has made a sustained effort to rebuild its channels with aggressive outreach and an innovative partner training program. Its continued investment in channel and marketing programs may raise visibility among Gartner clients.

Cautions

- **Product Strategy:** SonicWall's long lag time in introducing a virtual firewall has made it increasingly less relevant to modern data center use cases as enterprises adopt public cloud IaaS and conduct private cloud projects. As SonicWall releases relevant platform-specific virtual firewalls, prospects should test them thoroughly for integration with the specific cloud platform.
- **Product Execution:** SonicWall Capture ATP lacks the ability to inspect JavaScript to provide visibility on SaaS usage.
- **Customer Experience:** While support overall seems improved, customers note some support responsiveness and quality issues on earlier software releases that are still technically under support.
- **Marketing Execution:** Gartner sees SonicWall being shortlisted by enterprise clients less frequently. Gartner attributes some of this to the succession of ownership changes and subsequent disruptions to the company.

Sophos

Sophos is a network and endpoint security vendor headquartered in Abingdon, U.K. The vendor's portfolio includes firewalls (XG Series, SG Series and CR series), endpoint security (Sophos Endpoint Protection and Intercept X), mobile security, secure email gateway, email phishing training, secure web gateway, server security, encryption, wireless access point (Sophos AP), and unified endpoint management (Sophos Mobile). Sophos Firewall Manager is the name of the centralized management software, and Sophos Central is the cloud-based centralized management portal for all Sophos security products.

Sophos has 19 XG models and three Remote Ethernet Devices (RED) models, which are plug-and-play devices for small offices. It still sells and actively develops its other product lines, the SG and CR firewall series.

During the evaluation period for this Magic Quadrant, Sophos refreshed its large and midsize SG and XG firewall models. It has been focusing on improving visibility, protection and response on networks by enhancing the Synchronized Security offering for better correlation of firewall and endpoint Sophos products.

Sophos is a good shortlist candidate for midsize enterprises looking for multiple integrated features such as email and web DLP, email encryption, and a web application firewall in their firewalls. It should be also considered by enterprises looking for strong integration of Sophos firewall and Sophos endpoint capabilities for prevention of ransomware attacks.

Strengths

- **Sales Strategy:** Sophos has a strong channel strategy, with a loyal channel base globally. It conducts regular partner training and information sharing programs worldwide. Gartner has seen channels with strong confidence in the Sophos team and its sales strategy, especially postacquisition of Cyberoam. Sophos' presales team receives positive reviews for directly working with clients in regions like India and the Gulf Cooperation Council (GCC), and is often scored highly by customers.
- **Capability:** Sophos has strong ransomware detection capabilities and constantly works toward improving them. 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 them to prevent the movement of ransomware. Also, technologies like exploit-based detection and CryptoGuard to detect ransomware attacks in real time on Sophos' endpoint Intercept X product have made ransomware detection stronger.
- **Customer Experience:** The surveyed Sophos customers mentioned strong firewall and endpoint integration as the product's biggest strength, and also haveshown high satisfaction with the malware detection rate. The reason for this is that, in addition to traditionally managing the endpoint centrally from within the firewall UI, Sophos has built strong advanced threat monitoring and response capabilities using Security Heartbeat as a part of Synchronized Security.
- **Market Responsiveness:** Sophos continues to increase visibility, detection and response capabilities of advanced threats to meet the growing market requirement. It also acquired Barricade for improving security analytics capabilities, and integrated the deep learning capabilities of Invincea, which it acquired, into its sandboxing product, Sandstorm.
- **Product:** Sophos is one of the few firewall vendors that runs a bug bounty program, through bug bounty program vendor Bugcrowd, which is its responsible disclosure program. This program rewards the qualifying bugs based on severity, as assessed by Sophos' security team.

Cautions

- **Product Strategy:** Sophos' product strategy is more focused on midsize enterprises and hence fails to meet some enterprise deployment use cases. Features such as a built-in web application firewall, DLP and email encryption are more desirable to the midsegment that the vendor is focused on.
- **Market Segmentation:** Sophos maintains a majority of its presence in midsize enterprises. It fails to be visible to Gartner in other enterprise deployment use cases such as security of SDN, perimeter security of large enterprises and security of hybrid environment.
- **Customer Experience:** The surveyed Sophos customers have citied that initial deployment of the XG Series can be challenging because of a lack of good product documentation. They have added that product installation documentation lacks in-depth network and interconnectivity details, which leads to deployment challenges. The general feedback of Sophos surveyed clients indicates that the vendor's product documentation needs improvement. In May 2018, Sophos relaunched its XG self-help section to bolster documentation quality and quantity.
- **Product:** Sophos firewalls are not currently Common Criteria EAL4-certified, which is an important shortlisting criterion for enterprises that run under a regulated environment. Sophos firewalls also lack integration with third-party EDR tools, and offer integration only with Sophos' endpoint product, Intercept X. Features like Synchronized Security only work with Sophos' endpoint product. As a result, the enterprise customers utilizing other commercially available EDR vendors will not be able to utilize and share endpoint-related threat intel with their firewall.
- **Capabilities:** Sophos firewalls lack additional SaaS control features and offer basic SaaS discovery and visibility through their application control feature. They also lack integration with any third-party CASB vendor. Sophos does not offer firewall hardware with

multiple firewall instances for enterprises that wish to run multiple virtual instances inside the same firewall box for regulation or segmentation reasons.

Stormshield

Stormshield operates as an independent subsidy of Airbus Cybersecurity, based in Paris. Its product portfolio combines firewall (Stormshield Network Security [SNS]) and endpoint solutions (Stormshield Endpoint Security [SES] and Stormshield Data Security [SDS]). SNS firewalls are available as physical and virtual appliances, and on AWS and Microsoft Azure marketplaces. Centralized management (Stormshield Management Center [SMC]) and reporting (Stormshield Visibility Center [SVC]) are available as software appliances.

Stormshield has recently upgraded its midsize enterprise appliances, and announced technical integrations with antivirus vendor Panda Software. Stormshield has also added industrial protocol support for the oil and gas verticals and other industrial verticals. Stormshield SNS now includes log masquerading as a feature enabled by default on the firewall management interface as a tool for EU General Data Protection Regulation (GDPR) compliance.

Stormshield largely serves customers in a few countries in Western Europe. The vendor is a credible shortlist contender for European organizations, especially local government agencies or enterprises working with local government agencies, looking for a vendor ready to modify its roadmap to better serve their future needs.

Strengths

- **Capabilities:** Customers looking for strong threat inspection capabilities on an edge firewall give good scores to the protocol decoding engine and passive vulnerability scanner, which allow them to easily combine protection and detection techniques.
- **Performance:** Surveyed customers and resellers mention the ability to reach performance advertised on the data sheet, and the overall performance under load as reason to stick with the solution.
- **Vertical Strategy:** Stormshield has released a firewall model to be deployed in manufacturing plants, and to secure programmable logic controllers (PLCs), by adding support for the more common protocols present in these environments to its protocol analysis engine.
- **Compliance:** Stormshield maintains its investment in nationwide and regional certifications to better serve European local government agencies and enterprises that work with them. The GDPR has a strong influence on Stormshield's recent roadmap, leading to ad hoc features released to help with the privacy requirements.

Cautions

- **Market Responsiveness:** Stormshield's feature gap with leading vendors in this research is widening, due to a lower pace of new feature delivery and rare improvements beyond initial implementations.
- **Sales Execution:** Stormshield has one of the smallest enterprise firewall revenues of the vendors evaluated in this research, constraining its ability to feed new R&D efforts. The vendor also struggles with matching competitors' attach rates for software subscriptions, such as cloud sandboxing.
- **Capabilities:** Stormshield's firewalls have one of the most granular management roles, but offer very limited support for concurrent use of the management and centralized consoles. Initial product deployment still requires local-touch intervention through a USB stick. The vendor's firewall appliances lag behind dedicated hardware acceleration for SSL decryption.
- **Capabilities:** The vendor does not support active-active high availability. It lacks features for easier integration in SDN architectures. The cloud sandboxing emulation is limited to a few Windows operating systems.
- **Geographic:** Stormshield has no direct vendor presence in the Americas. The vendor has limited visibility outside of Western Europe and Poland, and is not visible on shortlists for clients from North America, China, India or Japan. The management interface lacks support for languages frequently available from competitors, such as Spanish, simplified and traditional Chinese, and Japanese.

WatchGuard

WatchGuard is a network security vendor with headquarter in Seattle, Washington. Its firewall product line (Firebox) includes physical and virtual appliances. Firewall models are also available on AWS and Microsoft Azure. Its centralized management suite includes two components. Dimension is primarily focused on monitoring and reporting, with some centralized policy features. It is available as a virtual appliance or as a cloud service. WatchGuard System Manager (WSM) is centralized management software for Firebox appliances and is

available on Windows server. WatchGuard's portfolio also includes wireless access points with integrated security features, and multifactor authentication (MFA).

Early in the evaluation period, WatchGuard released its endpoint detection and response solution (Threat Detection and Response), composed of host sensors (available on Windows and Linux) and managed by Firebox appliances. The service relies on cloud analytics gathering feedback from the sensors to provide malware detection and remediation. The vendor also refreshed its firewall appliance product line, and improved VPN and routing modules.

Major news includes the acquisition of Percipient Networks and subsequent launch of DNSWatch, a DNS layer filtering and phishing education service, as well as the acquisition of Datablink and subsequent launch of AuthPoint, a cloud-based MFA service.

WatchGuard should be included on the shortlists of distributed enterprises, and of organizations looking for a vendor capable of offering malware detection with integrated endpoint and firewall products.

Strengths

- **Geographic Strategy:** WatchGuard has a global presence and a strong ecosystem of faithful channel partners, making it easy for distributed enterprises to find local relevant skills when deploying an edge firewall. It recently increased its efforts to improve its reach in the Asia/Pacific region.
- **Sales Strategy:** WatchGuard has one of the simplest pricing structures available to enterprise clients, with two subscription bundles (basic and total security), accompanied with a support-only option for the edge firewall and VPN-only use case. Included in every package is 24/7 channel-based support. A predefined number of host sensors are included with the total security bundle.
- **Capabilities:** WatchGuard's centralizedmonitoring portal, Dimension, continues to get good scores from its customers. Its cloud centralized management provides a zero-touch deployment option (RapidDeploy), making it easier to provision and implement branch firewalls. First feedback on the new threat detection capabilities is promising.
- **Capabilities:** The VPN application for mobile includes health check features.

Cautions

- **Market Segmentation:** WatchGuard has a full line of virtual and cloud-based products to support virtual, IaaS and hybrid environments, but does not focus on large enterprise/data center deployments, and therefore lacks visibility in this market.
- **Product Execution** While WatchGuard conducts extensive public beta testing prior to any major firmware release, surveyed customers mention that the quality of the new features could be improved with a longer beta version. They also would like to see WSM take the same direction as Dimension, with more flexible, pervasive deployment options.
- **Features:** WatchGuard lacks the ability to run multiple instances of the firewall software on a physical appliance. It lacks support for the ICAP protocol, a mechanism frequently used by the upper-midsize customers for redirecting traffic to a sandboxing or DLP solution.
- **Market Responsiveness:** While WatchGuard approaches cloud-based application security with a combination of strong MFA and the company's Access Portal feature, it does not provide a full CASB or integrate with leading CASB vendors, a drawback for enterprise firewall prospects with CASB requirements.

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 the Magic Quadrant.

Dropped

No vendors were dropped from the Magic Quadrant.

Inclusion and Exclusion Criteria

Inclusion Criteria

Network firewall vendors 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 enterprise firewall market.
- The company regularly appears on shortlists for selection and purchase.
- The company demonstrates a competitive presence in enterprises and sales.
- Gartner analysts consider that aspects of the company's product execution and vision merit inclusion.

Exclusion Criteria

Network firewall vendors may have been excluded from this research for one or more of the following reasons:

- The vendor has minimal or negligible apparent market share among Gartner clients, or it is not actively shipping products.
- The vendor is not the original manufacturer of the firewall product. This includes hardware OEMs, resellers that repackage products that would qualify from their original manufacturers, as well as carriers and ISPs that provide managed services. We assess the breadth of OEM partners as part of the evaluation of the firewall, and we do not rate platform providers separately.
- The vendor's products sell as network firewalls, but do not have the capabilities, scalability and ability to directly compete with the larger firewall product/function view. Products that are suited for SMBs (such as UTM firewalls, or those for small office/home office placements) are not targeted at the market this Magic Quadrant covers (enterprises) and are excluded.
- The vendor primarily has a network IPS with a non-enterprise-class firewall.
- The vendor has personal firewalls, host-based firewalls, host-based IPSs and WAFs (see Note 1) — all of which are distinctly separate markets.

Evaluation Criteria

Ability to Execute

Product or Service: This includes service and customer satisfaction in enterprise firewall deployments. Execution considers factors related to getting products sold, installed, supported and in users' hands. Strong execution means that a company has demonstrated to Gartner analysts that products are successfully and continually deployed in enterprises, and that the company wins a large percentage in competition with other vendors. Companies 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. Sales are a factor; however, winning in competitive environments through innovation and quality of product and service is more important than revenue. Key features are weighted heavily, such as foundation firewall functions, console quality, low latency, range of models, secondary product capabilities (logging, event management, compliance, rule optimization and workflow), and the ability to support complex deployments and modern DMZs. Having a low rate of vulnerabilities in the firewall is important. The logistical capabilities for managing appliance delivery, product service and port density matter. Support is rated on the quality, breadth and value of offerings through the specific lens of enterprise 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 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 company's pricing, deal size, installed base, and use by enterprises, carriers and MSSPs. This includes the strength of the vendor's sales and distribution operations. 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. Cost of ownership over a typical firewall life cycle (three to five years) is assessed, as is the pricing model for

conducting a refresh while staying with the same product and replacing a competing product without intolerable costs or interruptions. The robustness of the enterprise channel and third-party ecosystem is important.

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.

Marketing Execution: Competitive visibility is a key factor; it includes which vendors are most commonly considered to have top competitive solutions during the RFP and selection process, and which are considered top threats by the others. In addition to buyer and analyst feedback, this ranking 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. An NGFW capability is heavily weighted, as are enterprise-class capabilities, such as multidevice management, virtualization, adaptability of configuration and support for enterprise environments. Unacceptable device failure rates, vulnerabilities, poor performance and 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 and Operations: These include management experience and track record, as well as the depth of staff experience — specifically in the security marketplace. The greatest factor in these categories is customer satisfaction throughout the sales and product life cycles. Low latency, throughput of the IPS capability and how the firewall fared under attack conditions are also important. Succeeding in complex networks with little intervention (for example, one-off patches) is highly considered.

Table 1: Ability to Execute Evaluation Criteria

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

Source: Gartner (October 2018)

Completeness of Vision

Market Understanding and Marketing Strategy: This includes providing a track record of delivering on innovation that precedes customer demand, rather than an "us, too" roadmap. We also evaluate the vendor's overall understanding of and commitment to the security and network security markets. Gartner makes this assessment subjectively by several means, including interaction with vendors in briefings and feedback from Gartner customers on information they receive concerning roadmaps. Incumbent vendor market performance is reviewed year by year against specific recommendations that have been made to each vendor, and against future trends identified in Gartner research. Vendors cannot merely state aggressive future goals; they must put plans in place, show that they are following their plans and modify those plans as they forecast how market directions will change. Understanding and delivering on enterprise firewall realities and needs are important, and having a viable and progressive roadmap and continuing delivery of NGFW features are weighted very heavily. The NGFW capabilities are expected to be integrated to achieve correlation improvement and functional improvement.

Sales Strategy: This includes preproduct and postproduct support, value for pricing, and clear explanations and recommendations for detecting events, including zero-day events. Building loyalty through credibility with a full-time enterprise firewall staff demonstrates the ability to assess the next generation of requirements. Vendors need to address the network security buying center correctly, and they

must do so in a technically direct manner, rather than selling just fear or next-generation hype. Channel and third-party security product ecosystem strategies matter insofar as they are focused on enterprises.

Offering (Product) Strategy: This criterion focuses on a vendor's product roadmap, current features, NGFW integration and enhancement, virtualization and performance. Credible, independent third-party certifications include the Common Criteria for Information Technology Security Evaluation. Integration with other security components is also evaluated, as well as product integration with other IT systems. We also evaluate how the vendor understands and serves the enterprise branch office and data center. Innovation, such as introducing practical new forms of intelligence to which the firewall can apply policy, is highly rated. An articulated, viable strategy for addressing the challenges in SDN deployments is important, as is evidence of execution within cloud and virtualized environments.

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

Geographic Strategy: These include the ability and commitment to service geographies and vertical markets, such as complex, enterprise multinational deployments, MSSPs, carriers or governments.

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

- Performance, which includes low latency, new firewall mechanisms, and achieving high IPS throughput and low appliance latency.
- Firewall virtualization and securing virtualized environments.
- Integration with other security products.
- Management interface and clarity of reporting — that is, the more a product mirrors the workflow of the enterprise operation scenario, the better the vision.
- "Giving back time" to firewall administrators by innovating to make complex tasks easier, rather than adding more alerts and complexity.
- Products that are not intuitive in deployment, or operations that are difficult to configure or have limited reporting, are scored accordingly. Solving customer problems is a key element of this criterion. Reducing the rule base, offering interproduct support and leading competitors on features are foremost.

Table 2: Completeness of Vision Evaluation Criteria

Evaluation Criteria ↓	Weighting ↓
Market Understanding	High
Marketing Strategy	Medium
Sales Strategy	Medium
Offering (Product) Strategy	High
Business Model	Medium
Vertical/Industry Strategy	Not Rated
Innovation	High
Geographic Strategy	Medium

Source: Gartner (October 2018)

Quadrant Descriptions

Leaders

The Leaders quadrant contains vendors that build products that fulfill enterprise requirements. These requirements include a wide range of models, support for virtualization and virtual LANs, and a management and reporting capability that is designed for complex and high-volume environments, such as multitier administration and rule/policy minimization. A solid NGFW capability is an important element, as enterprises continue to move away from having dedicated IPS appliances at their perimeter and remote locations. Vendors in this quadrant lead the market in offering new features that protect customers from emerging threats, provide expert capability rather than treat the firewall as a commodity and have a good track record of avoiding vulnerabilities in their security products. Common characteristics include handling the highest throughput with minimal performance loss, offering options for hardware acceleration and offering form factors that protect enterprises as they move to new infrastructure form factors.

Challengers

The Challengers quadrant contains vendors that have achieved a sound customer base, but they are not consistently leading with differentiated next-generation capabilities. Many Challengers have not fully matured their NGFW capability — or they have other security products that are successful in the enterprise and are counting on the relationship, rather than the product, to win deals. Challengers' products are often well-priced, and, because of their strength in execution, these vendors can offer economical security product bundles that others cannot. Many Challengers hold themselves back from becoming Leaders because they choose to place security or firewall products at a lower priority in their overall product sets. Firewall market Challengers will often have significant market share, but trail smaller market share leaders in the release of features.

Visionaries

Visionaries have the right designs and features for the enterprise, but they lack the sales base, strategy or financial means to compete consistently with Leaders and Challengers. Most Visionaries' products have good NGFW capabilities, but lack in performance capabilities and support networks. Savings and high-touch support can be achieved for organizations that are willing to update products more frequently and to switch vendors if required. If firewalling is a competitive element for an enterprise, then Visionaries are good shortlist candidates. Vendors that do not have strong NGFW capabilities are supplementing them in a defensive move, while vendors that have strong NGFW offerings are focused on manageability and usability. Gartner expects the next wave of innovation in this market to focus on better, more automated east-west microsegmentation in public cloud and SDN environments.

Niche Players

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

Context

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

Market Overview

As the first line of defense between external threats and enterprise networks, firewalls need to continually evolve to maintain effectiveness, responding to the continuing evolution in threats as well as to changes in enterprise network speed and complexity. Firewalls have high adoption and penetration rates in all markets. This means that, to protect their installed base, incumbents must add improved capabilities and increase performance, or face either replacement by innovative market entrants or commoditization by low-cost providers. Network security policy management (NSPM) products are increasingly used to manage complexity, especially in multivendor situations (see Note 2).

The Death of the Firewall Has Been Greatly Exaggerated

As the network boundary morphs, some predict the demise of the enterprise firewall. The argument is that all infrastructure and applications will move to various clouds, rendering traditional firewalls obsolete. However, experience shows that such massive transitions are extremely slow; as firewall management platforms become primary orchestration points for multiple cloud-delivered services, they will remain critical pieces in an enterprise's security puzzle. Certainly, over time, infrastructure changes will begin slowing

firewall growth, but not for several years. In fact, Gartner's latest end-user spending forecast shows growth through the forecast period ending in 2022.

During the evaluation period, end-user spending for the firewall market grew more than 13% to $11.32 billion. For 2018, Gartner estimates that the firewall market will grow approximately 9%. We also forecast that this market will grow from $11.32 billion in 2018 to almost $14.5 billion in 2022, reflecting declining growth rates toward the end of the forecast period. Gartner believes that the firewall market is "at capacity": Firewall refreshes remain constant at a five-year average, so even if great new products emerge, incumbent firewalls are rarely refreshed before they reach maturity. This refresh dynamic results in the market being linear, rather than having "macrorefresh" cycles or "bumps" of refreshes, as in other markets.

Enterprise Firewalls Are Next-Generation Firewalls

One key area of firewall evolution that has been widely supported is what Gartner (in 2009) called "NGFW features" — namely, integrated deep packet inspection intrusion prevention, application identification and granular user control. The key differentiators in these areas are IPS effectiveness, as demonstrated through third-party testing under realistic threat and network load conditions, and fine-grained, user-based policy enforcement in the top business and social media applications. Identity-based policy enforcement, or the ability to enforce policy on thousands of applications, remains a defining feature.

All enterprise firewall vendors today offer NGFWs. For new firewalls, there is no distinction between an enterprise firewall and an NGFW.

Because it is saturated, the firewall market is driven by refresh cycles of four to five years. Gartner estimates that the transition to NGFW from traditional firewalls will complete within the next two years. We have seen some common patterns in the firewall market as enterprises with three- to five-year-old firewalls and IPSs evaluate replacement:

- Enterprises with traditional firewalls seek to have application and user visibility in the firewall, and to require enforcement options in their next refresh.
- Enterprises not currently using any IPSs migrate to NGFWs with minimal use of advanced features.
- Enterprises with firewalls and stand-alone IPSs that are employed primarily in detection mode (that is, using minimal signature sets) migrate to NGFWs using the built-in IPS capabilities.
- Enterprises with firewalls and stand-alone IPSs that are used for active prevention, with large signature sets and some custom signatures, migrate to NGFWs for the firewall with application control and user context, but continue using stand-alone IPSs.
- High-security environments upgrade to NGFWs for the firewall, and upgrade IPSs to NGIPSs.
- Organizations look to extend their on-premises firewall vendor into IaaS cloud providers.
- Enterprises seek NGFW functionality as they transition from physical data center to virtualized environments and SDN.

UTM and Enterprise Firewalls — Branches of the Family Tree

Historically, UTM vendors have and continue to target SMB clients. However, in the past few years, the large UTM vendors have tried to expand beyond their traditional use case by stretching into the large enterprise market. They now try to sell high-throughput UTM to enterprise clients that score price competitiveness higher than security. Gartner sees some limited success for Type C enterprises (see Note 3), but it is mostly restricted to two use cases: distributed Type C enterprises (mostly in the retail industry), and firewall-only for network segmentation at low cost. However, the UTM approach fails to convince Type A and Type B enterprises that require mature application and user control capabilities and granular policy management for complex networks.

UTM vendors also face difficulties in building a strong sales and support channel for enterprises (similarly, enterprise firewall vendors underestimate the work of building an SMB channel). Most enterprise buyers are also wary of shortlisting a UTM vendor because of its primary focus on SMBs and limited brand awareness.

Some Enterprises Are Stepping Up to the Platform

Gartner sees more enterprise clients buying into firewall vendor "platform" value propositions, wherein they buy, often under an ELA contracting vehicle, all or most of a vendor's security portfolio, including such items as endpoint security, SWG, advanced threat detection and CASB services. These ELAs usually include software and support at a heavily discounted rate compared to list price across the same line items. Leading enterprise firewall vendors have these offerings or are planning to have them.

Security and risk leaders who decide to consolidate the enterprise's security vendors using a platform approach must decide whether the cost and product integrations that platforms potentially provide are worth the risk of having non-best-of-breed tools at certain layers. In addition, they should ensure that teams that manage different parts of the security stack, such as system administrators managing endpoint security, are aligned with training on deploying new tools.

Tales From Decrypt

Enterprises face a critical need for TLS decryption, principally to enforce web-filtering policy and to prevent malware infections. In "Predicts 2017: Network and Gateway Security," Gartner anticipates that, through 2019, more than 80% of enterprise web traffic will be encrypted. Consequently, a growing number of malware attacks, including ransomware, will move to use HTTPS to subvert initial infection and command-and-control communications.

By 2020, more than 60% of organizations will fail to decrypt HTTPS efficiently, missing most targeted web malware.

Decrypting SSL/TLS on a firewall creates organizational issues, such as ensuring employees' right to privacy, and technical challenges, such as performance issues and product sizing difficulties for the firewall channel. End-user experience is likely to be affected too. Some application traffic cannot be decrypted, and firewall vendors do a poor job at providing an up-to-date list of exceptions, leading to traffic being blocked. In the client reference survey — despite the self-evaluation bias that generally results in inflated numbers, and the fact that references provided by vendors tend to use more features than the market average — only 29% of the respondents answered that they were decrypting HTTPS traffic. Interestingly, that matches the 29% noted in last year's Magic Quadrant.

Virtualized Firewalls: Hype Accelerates and Demand Follows

As data center virtualization has continued, SDN projects become more numerous, and as IaaS deployments become more common, demand for virtualized environment support has grown. Performance and the ability to manage firewall policy through a single integrated management console for stand-alone appliances or virtual appliances are key differentiators. Gartner has not seen the firewall features of virtualization platforms (such as those offered with VMware or AWS) as a major competitor to mainstream firewall vendors because the need for separation of duties drives clients to doubt the infrastructure's ability to protect itself. Gartner covers virtual/cloud firewall vendors such as GuardiCore, Illumio and vArmour, but they have nascent but growing adoption. VMware's NSX work with several leading firewall vendors has created buzz for virtualizing and securing data centers, networks and east-west segmentation, and some lean-forward customers have adopted these. Adoption is growing quickly, and the numbers are getting larger. Performance remains a barrier to wider deployment: Almost all network firewalls today are delivered on purpose-built appliances because of the poorer performance of running firewalls on general-purpose servers. Almost all operating systems within firewall appliances are uniquely hardened, subject to stringent third-party security evaluations. Security-minded enterprises are also rightly skeptical of running firewalls within a hypervisor that is between the threat and the firewall.

Another big issue in deploying virtual firewalls in SDN or IaaS projects is the inability of enterprise virtual firewalls to automatically spin up appropriate policy as servers are spun up. Agility is one of the key business benefits of SDN and IaaS, and the need for human interaction with firewall policy detracts from the business benefits these agile architectures bring with them. The enterprise firewall vendor community is making strides here, but policy automation and orchestration have a long way to go.

Gartner Magic Quadrant vendor survey data continues to show that virtual firewall revenue accounts for far less than 5% of enterprise firewall market revenue, and just over 5% of total units shipped. Client market inquiries show an increased interest in virtual firewalls, and vendors are scrambling to meet that demand by attempting to increase virtual firewall performance and by automating firewall policy orchestration in dynamic environments.

Firewall as a Service, at Your Service

Firewall as a service (FWaaS) is a multifunction firewall delivered as a cloud-based service or hybrid solution (that is, cloud plus on-premises appliances; see "Emerging Technology Analysis: Firewall as a Service"). FWaaS is primarily delivered as a multitenancy infrastructure that is shared among multiple enterprises. The promise of FWaaS is to provide simpler and more flexible architecture by leveraging centralized policy management, multiple enterprise firewall features and traffic tunneling to partially or fully move security inspections to a cloud infrastructure. FWaaS today aims to provide network security services to small offices and mobile users.

This space is growing quickly from very small numbers. The small branch office use case is tied to the rise of SD-WAN. With more distributed internet breakouts, more distributed security services are needed. At this point, several enterprise firewall vendors and startups offer FWaaS, and some Gartner clients are evaluating FWaaS as an alternative to sprawling physical appliances across a large number of branch offices.

Evidence

This Magic Quadrant research was conducted in accordance with Gartner's well-defined methodology. The analysis in this research was based primarily on interviews and interactions during hundreds of enterprise firewall inquiries with Gartner clients since the previous iteration of this Magic Quadrant. It was also based on recent Gartner Peer Insights surveys, relevant vendor news and evidence gathered from relevant vendor financial statements. We also considered surveys completed by vendors, vendor briefings conducted at the request of vendors throughout the year, interviews with references provided by vendors and supporting Gartner quantitative research on market share.

Guidelines for responding to the full survey were provided at the time of issue. Responses were, nevertheless, of variable quality. Responses that were lower quality (for example, respondents ignored the question, used poor grammar, were unable to explain key concepts, were unable to provide high-quality explanations of use cases, or were unable to go beyond technical capabilities and demonstrate an understanding of the business environment), or that did not meet the guidelines, generally tended to score lower. Vendors that declined to provide a survey response were assessed by Gartner as to what their likely reply would have been (usually, this was in relation to specific revenue breakdowns). Some vendors declined to answer certain questions due to market restrictions, and, therefore, did not fare as well under some of the scoring criteria.

We asked for a specific number of references from each vendor (n = 95), and each reference customer was supplied with a structured survey. References were scored on the basis of their quality and what they told us. For each vendor, we took into account the comments from that vendor's references, as well as what other vendors' customers said about that particular vendor. Vendors could be notably affected by the inability to have a sufficient number of reference customers providing input.

Note 1
Buyer Confusion Concerning WAFs

The advent of application control in firewalls has led to some natural confusion regarding the NGFW and WAF markets in the minds of buyers. Today, these markets remain very distinct. The critical difference is one of direction: Application control in NGFWs is concerned primarily with applications that are external to the enterprise (for example, P2P and Facebook), whereas WAFs are concerned with protecting custom web applications on servers that are internal to the enterprise. Although a few firewalls offer optional WAF modules, these are rarely enabled. Instead, we see WAFs deployed as a stand-alone product (such as from Imperva), an off-premises service (such as from Akamai) or within an ADC (such as from F5).

Note 2
Network Security Policy Management Tools

Third-party network security policy management (NSPM) tool vendors (such as AlgoSec, FireMon and Tufin) continue to exploit the absence of firewall consoles to optimize, visualize and reduce firewall rules and policies. Although the NSPM market is still somewhat small, it's growing fast, and the customers requiring help with complexity are the very largest. Additionally, very large enterprises may have firewall products from different vendors — sometimes by accident via acquisition rather than through choice, because a single-vendor solution is usually the best choice. In other cases, an enterprise may be in the midst of a multistage rollout of a new platform. Enterprises that deploy some of their infrastructure to the public cloud may choose to use native cloud firewalls there, in addition to maintaining the incumbent firewalls in the physical infrastructure. All NSPM vendors support multiple firewall products (including, in some cases, cloud-resident firewalls), whereas no firewall vendor will effectively manage a competing product. In addition, NSPM vendors are expanding into managing other network security devices, such as IPSs.

Note 3
Types A, B and C Enterprises

Enterprises vary in their aggression and risk-taking characteristics. Type A enterprises seek the newest security technologies and concepts, tolerate procurement failure, and are willing to invest for innovation that might deliver lead time against their competition; this is the "lean forward" or aggressive security posture. For Type A enterprises, technology is crucial to business success.

Type B enterprises are "middle of the road." They are neither the first nor the last to bring in a new technology or concept. For Type B enterprises, technology is important to the business.

Type C enterprises are risk-averse to procurement, perhaps investment-challenged and willing to cede innovation to others. They wait, let others work out the nuances and then leverage the lessons learned; this is the “lean back” security posture that is more accustomed to monitoring rather than blocking. For Type C enterprises, technology is not critical to the business and is clearly a supporting function.

Evaluation Criteria Definitions

Ability to Execute

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

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

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

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

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

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

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

Completeness of Vision

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

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

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

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

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

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

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

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