Magic Quadrant for Network Firewalls

Published 17 September 2019 - ID G00375686 - 86 min read

With firewall providers embedding multiple security features in firewalls and enabling integration and automation capabilities with other security products, firewalls are evolving into network security platforms.

Strategic Planning Assumptions

By 2024, 20% of new distributed branch office firewall deployments will switch to firewall as a service, up from less than 5% today.

By 2024, 25% of new firewall deployments will have users consider cloud-native firewall policy support of infrastructure as a service (IaaS) platforms as a mandatory selection criterion, from less than 5% today.

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

By 2024, 50% of new firewall purchases in distributed enterprises will utilize SD-WAN features with growing adoption of cloud-based services, up from less than 20% today.

Market Definition/Description

This year, Gartner has modified the definition of network firewalls. As we are observing more clients moving toward hybrid networks and seeking firewall capabilities in the cloud, cloud vendors are also offering native firewall capabilities to their clients. The traditional firewalls also offer support for these cloud platforms. Hence, starting this year, Gartner has started to also evaluate the native firewall capabilities of cloud providers, along with stand-alone firewall vendors. Also this year, the Magic Quadrants for Enterprise Firewalls and Unified Threat Management (UTM) have been consolidated into a single Magic Quadrant for Network Firewalls.

Gartner defines the network firewall market as follows: The network firewall market represented by this Magic Quadrant is composed primarily of firewalls offering bidirectional controls (both egress and ingress) for securing networks. These networks can be on-premises, hybrid (on-premises and cloud), public cloud or private cloud. Network firewalls can also offer additional capabilities such as application awareness and control, intrusion detection and prevention, advanced malware detection, logging, and reporting. The companies that serve this market have an identifiable focus on network-based firewall controls — as demonstrated by the proportion of their sales and delivered with their support, sales teams and channels.

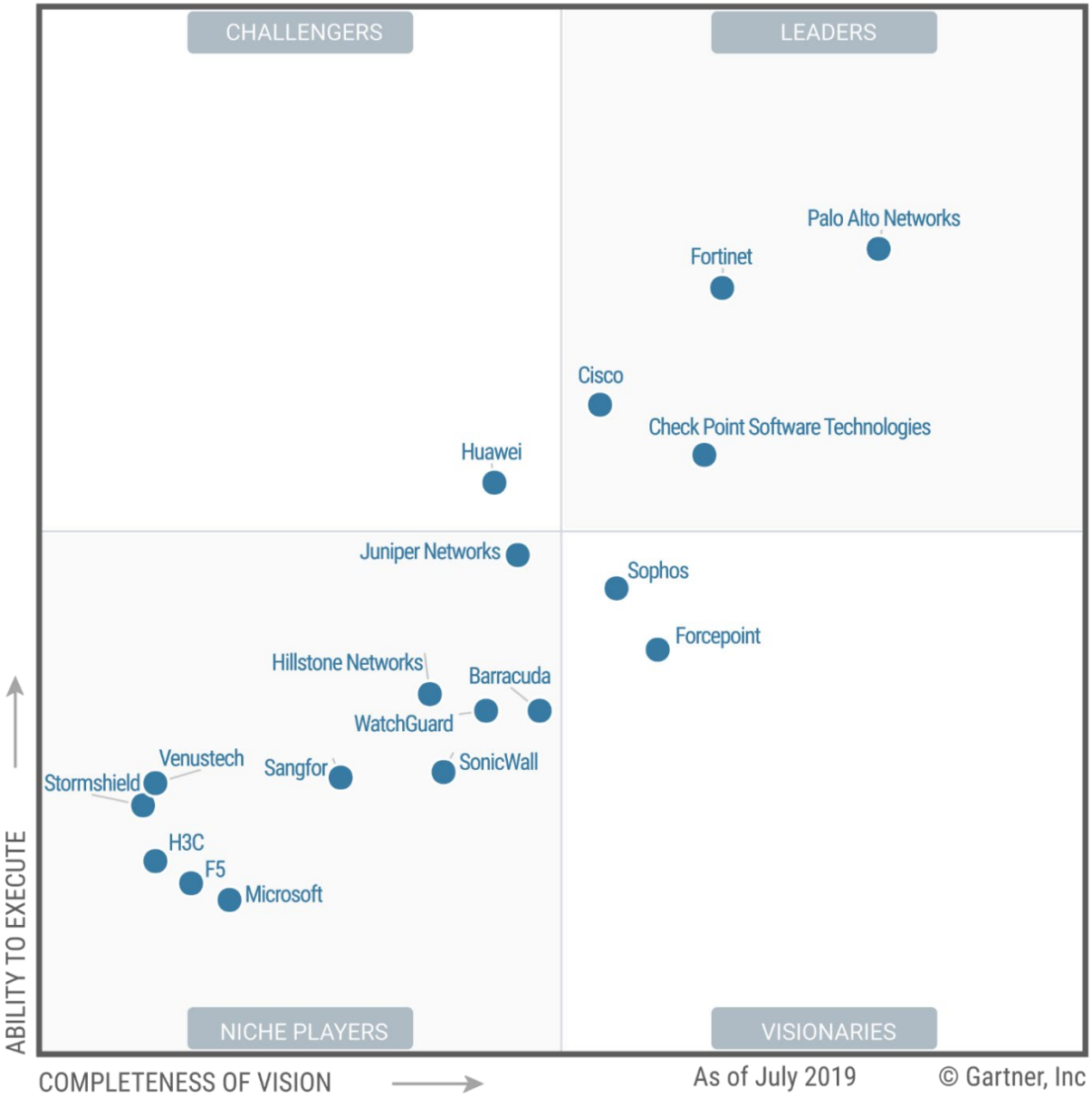
These vendors provide features dedicated to solve firewall requirements and serve firewall-related use cases.

This Magic Quadrant includes the following types of network firewalls:

- Purpose-built physical appliances
- Virtual appliances
- An embedded firewall module
- Firewall controls delivered from IaaS platform providers

Magic Quadrant

Figure 1. Magic Quadrant for Network Firewalls
Source: Gartner (September 2019)



Vendor Strengths and Cautions

Barracuda

Barracuda is based in Campbell, California. Its firewalls are visible on public IaaS platforms and in SD-WAN-related use cases on Gartner clients' shortlists. These days, with a growing number of firewall vendors offering support for public cloud, Barracuda is facing strong competition because of limited visibility in the on-premises firewall use case. The vendor continues to introduce enhancements related to support for public IaaS platforms and SD-WAN. It is primarily shortlisted by midsize enterprises.

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 the popular public IaaS platforms Amazon Web Services (AWS), Microsoft Azure and Google Cloud. Its firewall centralized management solution, Control Center, is only available as either a software appliance or a public cloud image. Its security portfolio extends beyond firewalls to web application firewalls, data protection and email security solutions.

Recent product updates include integration with macmon for network access control (NAC) and full integration, and support for Microsoft Azure Virtual WAN, as well as new firewall instances in Microsoft Azure, Google Cloud Platform and AWS. Barracuda also discontinued its hardware appliances for centralized management, focusing on virtual and IaaS deployments.

Strengths

- SD-WAN: Barracuda offers mature SD-WAN capabilities within its firewalls. It has extended this SD-WAN support, including VPN tunnels between Barracuda devices and support of the new Microsoft Azure Virtual WAN.
- Product: Barracuda continues to enhance support for public IaaS platforms. It offers easy-to-use templates for connecting on-premises environments to multiple public IaaS vendors, specifically AWS, Microsoft Azure and Google Cloud Platform for creating policies and rules. Cloud connections to all cloud providers are configured and monitored from the centralized management console.
- NAC: In addition to offering integration with macmon (an NAC vendor), the vendor offers a lightweight NAC solution called Barracuda Network Access Client combined with its SSL VPN solution for basic client health checks.
- Customer Feedback: Surveyed customers report higher-than-average overall satisfaction, with Barracuda highlighting ease of deployment, centralized management and service.
- Product Strategy: The retirement of the small and midsize business (SMB)-oriented X-Series and on-premises management appliance simplifies the overall product line and centralized management options.

Cautions

- Customer Experience: A lack of a complete set of APIs and missing integration with the Barracuda Content Shield endpoint security solution were cited as key concerns by customers surveyed. However, in the recent firmware release (8.0), the vendor has made enhancements by offering support for relatively more APIs.
- Sales Execution: While the vendor offers firewall appliances scaling from 1.2 Gbps to 46 Gbps (pure stateful inspection throughput), Gartner does not see them as a preferred shortlist for data center and enterprise perimeter use cases by Gartner clients.
- Marketing Execution: Resellers express concern that potential customers do not see the vendor as enterprise-grade or competing with larger competitors. Despite receiving high marks for ease of cloud connectivity with CloudGen Firewalls, the overall adoption rate of virtual firewall instances within IaaS as either pay-as-you-go or bring-your-own licenses remains low.
- Geographic Strategy: Barracuda remains primarily focused on North America and Europe, and is not often seen in South America, the Asia/Pacific region and the Middle East.
- Market Responsiveness: Barracuda lacks a FWaaS offering and any cloud access security broker (CASB) integration, which is a favorable requirement with the growing use of SaaS applications. The firewalls also lack support for SDN platforms.
- Sandboxing: The vendor lacks an on-premises network sandboxing product, but offers integration with Lastline.
- Product Certification: Barracuda firewalls lack certain certifications that are important to enterprises with heavy regulations such as Common Criteria EAL4.

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 firewalls are facing strong competition from leading firewall players in the market. Gartner is gradually noticing the vendor's decreasing visibility for different firewall use cases in client inquiries as compared to other Leaders. With Check Point now showing a focus on cloud and application security with acquisitions, if executed well, it can gain traction in these use cases.

Check Point's security portfolio, branded as the Check Point Infinity Architecture, includes enterprise firewall appliances (Security Gateway), virtual appliances available on the major cloud platforms (the CloudGuard brand, which includes CloudGuard IaaS, CloudGuard SaaS, CloudGuard Dome9 and CloudGuard Log.ic). 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's 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).

Checkpoint introduced four new Security Gateway appliances in the past year. In addition, it acquired Dome9 for cloud security posture management (CSPM) and ForceNock for web application and API

protection (WAAP) security. The vendor offers 23 Security Gateway models — from lower-end options to high-end appliances with 1.6 Tbps throughput.

Strengths

- Pricing Strategy: Check Point offers a simple pricing model where appliances come with a choice of three bundles of subscriptions: Next Generation Firewall (firewall, intrusion detection and prevention system [IDPS], application control and URL filtering), Next Generation Threat Prevention (Next Generation Firewall features plus antivirus, anti-spam and anti-bot), and Next Generation Threat Prevention & SandBlast NGTX (NGTP plus sandboxing and content disarm and reconstruction). Check Point also offers the Infinity Total Protection ELA, as well as a-la-carte pricing.
- Product Execution: Check Point has one of the largest threat research teams among the vendors evaluated in this research. It also offers a third-party threat intelligence feed as an additional option for customers, further increasing the scope of its threat intelligence offering. The vendor's attach rates for its add-on products are higher than many competitors, which improves its threat intelligence capabilities.
- Partners: Check Point has a historically strong partner ecosystem, with VMware, Silver Peak, Microsoft and Radware being the recent additions. The vendor has also launched a new partner program called Check Point Engage that rewards providers that strengthen relationships with Check Point customers focused on cloud and mobile over hardware purchases.
- Scalability: Check Point has invested heavily in building specialized offerings to respond to vertical-specific challenges, including ruggedized appliances for critical infrastructure, telecom-specific hyperscale, and protocols such as GTPv1, GTPv2, Diameter, SCTP and SS7. The Maestro Hyperscale Orchestrator appeals to certain verticals like telecommunications and carrier-grade networks that value extremely high throughput capacities.
- Feature: Check Point continues to lead in centralized management offerings, even for very large, complex and highly exposed environments. Its management suite includes several features such as multidomain security management and smart provisioning to specifically serve managed security service providers (MSSPs).
- Product Support: Check Point supports a large number of private, hybrid and public IaaS environments with its CloudGuard IaaS product line, including VMware NSX, Cisco ACI, AWS, Microsoft Azure and Azure Stack, Google Cloud Platform, Oracle Cloud, OpenStack, and Alibaba Cloud. With Dome9, Check Point is showing a growing focus on public IaaS.

Cautions

- Marketing Execution: Gartner estimates that, in 2018, Check Point lost market share to its rivals and increasingly is less visible in Gartner client inquiries. Client surveys indicate that the vendor is often left off of shortlists when clients are considering replacement of incumbent firewall vendors.

- Market Responsiveness: Check Point is lagging its competition in introducing a full FWaaS offering. The vendor continues to lack the SD-WAN focus found with other firewall vendors.
- Product: Check Point Security Management Portal (SMP; cloud-based management console) is only available for limited firewall models and lacks support for the entire firewall series. Check Point firewalls also lack support for TLS 1.3; the product currently downgrades TLS 1.3 connections to TLS 1.2 when decrypting traffic.
- Customer Feedback: Customers and surveyed resellers perceive performance issues requiring purchase of larger appliances than anticipated, giving lower scores for overall performance, especially when enabling multiple features such as DLP. While Check Point is one of the most shortlisted firewalls for public IaaS platforms, clients cite that the installation and deployment process is not a smooth experience and often requires professional services or help from the support team.
- Marketing Strategy: Check Point continues to market Infinity as both an architecture and an ELA around the concept of generational threat protection (currently Gen V). Gartner clients express confusion around this messaging and which solutions the vendor can provide to help protect their environment. Check Point lacks strong positioning and product messaging.
- Technical Support: Gartner clients continue to cite that Level 3 escalations take longer than Level 1 and Level 2 escalations, and that the vendor lacks in timely updated communication while the team is working on it.

Cisco

Cisco is a large network, infrastructure and security vendor, based in San Jose, California. It continues to offer multiple firewall models for different use cases, although many models under the different firewall product lines overlap with each other. Cisco firewalls continue to be part of large Cisco infrastructure deals. Gartner does observe the vendor being shortlisted by existing Cisco clients as one of the firewall vendors. Its vision of cloud and automation, if executed well, can help the vendor gain traction in related use cases.

Cisco's security product portfolio includes many solutions, including firewalls, and it has grown continually over the past few years, mainly through acquisitions. It offers endpoint security client Cisco AMP, Cisco AnyConnect (VPN client), Stealthwatch and Stealthwatch Cloud (network traffic analysis [NTA]), secure web gateway (SWG), email security, network access control and a CASB — with Talos threat intelligence included with Cisco security products.

Cisco continues to sell multiple firewall product lines: Cisco Adaptive Security Appliance (ASA) 5500-X Series and Adaptive Security Virtual Appliance (ASAv), its virtual firewall appliances; Cisco Firepower NGFW Series, which also exists in the form of virtual appliances (NGFWv); the Meraki MX series; and Cisco IOS Firewall. The vendor also offers two industrial firewalls (the ISA series)

Cisco Umbrella is the vendor's cloud DNS security and secure web gateway. Cisco Tetration started as cloud visibility software, and recently evolved into an agent-based firewall for application and microsegmentation.

Cisco Threat Response (CTR) is the Cisco web portal for threat investigation, adding context and an indicator of compromises to events sent from registered Cisco security products.

The vendor continues its effort to build a unified centralized management console with Cisco Defense Orchestrator (CDO), which aims at managing all of its firewall product lines. The Cisco Meraki MX series also offers cloud-based management targeting distributed organization use cases. Firepower Management Center (FMC) is Cisco's on-premises centralized management offering, available for Cisco ASA 5500-X and Firepower devices only.

Strengths

- Sales Execution: Cisco's global footprint is a big asset when trying to convince large organizations to purchase its firewalls and adjacent security products. Gartner analysts see a large number of organizations signing ELAs with Cisco, including for a large number of Cisco Firepower firewalls. Many clients describe themselves as "Cisco shops."
- Marketing Execution: Cisco owns a broad portfolio of network and security solutions. Gartner sees the vendor enthusiastically promoting the integration and automation roadmap within its products as a strong marketing and sales strategy, which is also resonating with end users. It is also an attractive proposition for clients that want to consolidate toward a single vendor. During inquiries, Gartner clients mention the Cisco integration story among the different Cisco products as a primary reason for the purchase.
- Capability: Customers and resellers continue to give high scores to Talos threat research and to advanced malware protection (AMP) features available on Firepower. Existing Sourcefire customers also like the IDPS integration on Firepower.
- Capability: Cisco Meraki MX appeals to distributed organizations looking for ease of deployment and maintenance. Cisco Meraki MX's proprietary auto-VPN and SD-WAN simplify site-to-site VPN deployments when using only Meraki devices.
- Feature: The Cisco AnyConnect VPN client offers support for most mobile devices and their OSs. Gartner constantly receives inquiries in which clients rate the VPN offered by the vendor as higher compared to other vendors. They state that the VPN tunnels are stable and users do not experience disconnected sessions. Many Gartner clients that replace their Cisco ASAs with a firewall from a different vendor continue to use ASAs for VPN only.

Cautions

- Project Execution: While Cisco has made progress on its competitive positioning, it struggles to win firewall evaluation against other competitors in pure firewall deals based on technical evaluation alone. This puts Cisco in a difficult spot when the three vendors offer similar prices, which is more frequent than in the past due to recent pricing strategy changes from Cisco and its competitors.

- Product Execution: Cisco clients that have purchased multiple Cisco security products with Cisco Firepower firewall to utilize integration and automation capabilities, as highlighted by the vendor at the time of sales, are often disappointed when they don't work in their environment. Gartner clients often cite the lack of automation between Cisco ISE (NAC solution) and Cisco Firepower as quite frustrating. Gartner highly recommends that clients evaluate the integration capabilities between different Cisco products before purchase.
- Product Execution: Cisco Meraki MX, Firepower and, increasingly, Viptela can be relevant in overlapping use cases for distributed organizations with SD-WAN requirements. As the three solutions do not have full feature parity, prospective clients and Cisco resellers struggle to build an architecture when it needs to combine multiple solutions. CDO is still a work in progress and lacks fully featured unified management, which could help with the issue.
- Capabilities: Cisco Firepower lacks SD-WAN features and zero-touch deployment. Gartner observes that Cisco clients are less likely to use application control, TLS decryption and URL filtering features. Surveyed customers also express frustration with the lack of comprehensive real-time logging and reporting solutions.
- Geographic Strategy: Gartner is noticing declining visibility of Cisco firewalls in pure firewall deals outside North America in client inquiries. The vendor is more visible in other regions as part of large Cisco infrastructure deals. Gartner has also observed more focus by the vendor on expanding the Cisco Meraki MX product line in the U.S. and U.K.
- Capabilities: Cisco clients continue to complain about their inability to effectively deploy Firepower virtual machines on IaaS platforms. They mention stability issues and feature inconsistencies. Gartner also does not see Cisco being deployed on public cloud, compared to competitors.
- Customer Experience: Cisco scored lower than average on surveyed customers' satisfaction with quality of support. This aligns with what Gartner analysts observe during client inquiries, where the ability to get timely answers has been reported as degrading over time, especially when facing issues with centralized management features.
- Capability: Cisco Firepower's management API lags in maturity behind its direct competitors. This has noticeable consequences, such as delays in support from network security policy management tools (NSPM), and the absence of integration, notably with any third-party endpoint detection and response (EDR) tools.

F5

F5, based in Seattle, Washington, is a leading data center application delivery controller vendor. It continues to focus on data center and CSP use cases for its firewall module deployment. Clients using F5 or procuring application delivery products for the vendor should consider using the firewall module offered by the vendor. The primary use case for using the vendor's firewall is vendor consolidation, higher throughput requirements and advanced routing capabilities.

F5's Advanced Firewall Manager (AFM) module, as a part of its BIG-IP appliances, is sometimes visible in the vendor's quotations with other products offered. Gartner comes across existing F5 clients that want to evaluate the firewall capabilities offered by the vendor with other firewall vendors in the market. F5 firewalls have limited visibility in data centers and large enterprise deployment.

F5's security portfolio includes a WAF solution, access policy manager (APM), web fraud protection (WebSafe), and a DDoS mitigation solution, DDoS Hybrid Defender (DHD). Under the Silverline brand, F5 delivers a cloud WAF and DDoS protection. Its firewall product relies on the BIG-IP appliances (21 models, from 5 Gbps up to 320 Gbps) and VIPRION chassis (six models, up to 1.2TB throughput) hardware platforms, running the F5 Traffic Management Operating System (TMOS). F5 also offers 11 virtual appliances (F5 Virtual Editions [VE]) and centralized management (BIG-IQ) for its BIG-IP solutions.

Recent product news includes multiple enhancements related to routing, traffic inspection and DDoS mitigation.

Strengths

- Product Strategy: F5's software is optimized for data center and ISP infrastructure protection use cases with its highly scalable architecture, native load balancing support and focus on carrier-grade issues such as carrier-grade network address translation (CGNAT) and DDoS capabilities.
- Feature: The vendor offers strong load balancing and DDoS mitigation capabilities. This offers clients the ability to consolidate firewall functionality with mature application delivery and security capabilities. However, all the features come as separate products with dedicated subscriptions.
- Customer Experience: F5's customers report better-than-average satisfaction with the vendor's technical support. Customers also report above-average performance of the F5 firewall, and cite performance and throughput as key deciding factors when selecting F5 for their firewall.
- Product Strategy (IaaS): F5 partners with multiple public IaaS cloud service providers including Alibaba, AWS, Azure, Google Cloud Platform, IBM and Oracle, making it a desirable shortlist candidate for mutlicloud deployments.
- Product: F5 offers strong TLS decryption in its BIG-IP appliance, as well as a dedicated TLS decryption appliance (SSL Orchestrator). F5 fully supports RFC 8446 TLS 1.3 decryption in TMOS 14.1.0.1 and higher, well ahead of many other firewall vendors, making SSL decryption capabilities stronger than the competitors.
- Geographic Presence: F5 is a long-established application delivery vendor with a large, loyal global channel. The vendor also has a direct presence through regional offices worldwide. This makes it a strong global vendor.

Cautions

- Sales Execution: F5 rarely appears on Gartner client competitive shortlists for enterprise firewall selection, and often complements other firewalls rather than replacing them. In addition, there has been significant turnover in its sales leadership, impacting reseller relationships over the past year.
- Customer Experience: F5's customers generally report satisfaction with its product, but are reluctant to provide unqualified recommendations of it due to a lack of common firewall features, which prevents it from being used in certain use cases such as end-user perimeter firewalls. Surveyed clients have reported more reliance on the vendor's professional services because of a lack of sufficient product documentation and steep learning curve as product limitations.
- Product: The F5 firewall lacks advanced threat detection features such as anti-malware and sandboxing, native or third-party endpoint security integration, and support for SD-WAN, which are commonly provided by vendors competing in the enterprise firewall market.
- Product Strategy: F5 does not offer a set of low-end appliances, a multitenant FWaaS option, NAC integration or cloud-based management consoles, and tends to focus its products on carrier-grade networks and large enterprise internal data center use cases. Unlike other vendors in the market, the network team is most likely to manage F5 due to its integration with the application delivery controller and, therefore, may not be managed or considered by security teams for firewall use cases.
- Market Responsiveness: F5 includes an IDPS feature based on a limited number of SNORT signatures. Gartner advises that customers looking for high-security, network-based intrusion prevention solutions augment the F5 IDPS because it is not as robust or mature as other offerings seen in the network firewall market today.

Forcepoint

Forcepoint is a security vendor headquartered in Austin, Texas. Its firewalls continue to be visible primarily in distributed office use cases where clients are looking for mature SD-WAN, VPN and centralized management capabilities. Gartner sees good potential in the firewall to meet other use cases, but sees a delay in market responsiveness and a lack of focus to expand the customer base beyond distributed office use cases by Forcepoint.

The vendor offers a firewall (Forcepoint NGFW), web and email security gateways (Forcepoint Web Security and Forcepoint Email Security), data loss prevention (Forcepoint DLP), an insider threat solution (Forcepoint Insider Threat), a cloud access security broker (Forcepoint CASB), and user and entity behavior analytics (Forcepoint UEBA). It also offers government-specific security solutions.

Virtual Forcepoint firewalls offer support for Azure and AWS, where they are available, as pay as you go as well.

Forcepoint's recent news includes the introduction of five new compact desktop models. Other updates include support for new, compact desktop models (33x and 5x series), and feature enhancements for SD-WAN and networking. Support for auto-scaling and management for its visual firewalls with virtualized environments (AWS, Azure, VMware, etc.) is available.

Strengths

- Market Execution: The majority of the installed base for Forcepoint firewalls with mature VPN and SD-WAN capabilities is in distributed office use cases. Even the vendor is keen to focus on this use case by continually introducing more enhancements for VPN and SD-WAN.
- Product: Security Management Center (SMC), which is the vendor's centralized management offering, is very intuitive and easy to use. SMC is available as a management appliance, management appliance ISO image and software. It offers features such as drag and drop, which is very smooth. SMC provides granular administrator access control. Administrator roles can be defined, and mapped with select NGFWs, access control lists and Domains. There is also an administrator privilege for approving pending changes with features such as drag and drop. Surveyed clients have also highly rated SMC and scored it higher in ease of management.
- Feature (IDPS): The vendor has a legacy reputation of mature IDPS offers. Forcepoint utilizes threat intelligence from McAfee GTI and the Lastline reputation service, in addition to Forcepoint TI. Forcepoint firewalls offers best-of-breed firewall clustering capabilities, with a mature load balancing capability between different appliance models and running different firmware. Surveyed clients have also highly rated the firewall clustering capabilities, which are easy to manage and failover is transparent to the network.
- Automation: Forcepoint offers cloud provisioning tools and automated scripts for DevOps use cases. The vendor offers public GitHub project SMC Python and SMC integration for Ansible.
- Feature (VPN): Forcepoint firewalls offer easy-to-configure VPN templates. The vendor has a large installed base of multiple branch office VPN use cases. The UI offers easy-to-monitor-and-manage multiple VPN tunnels.
- Capability: The vendor offers built-in UEBA capabilities, bringing advanced threat detection capabilities beyond network sandboxing without the need for an additional subscription. The Forcepoint firewall platform collects data from network engines (physical/software/virtual/cloud variants), endpoint intelligence agents and via Syslog feeds from other third-party solutions deployed within an organization.

Cautions

- Market Execution: Forcepoint sells multiple product lines, out of which Web Security, its SWG product, seems to be the primary product where most R&D work is focused. Gartner finds that the vendor focuses less on its firewall product line as a result, keeping it confined to distributed office use cases. While Gartner thinks that Forcepoint has good experience and a good R&D team, the firewall has the potential to be one of the industry leaders if the vendor focused more toward this product line.
- Marketing: Forcepoint lacks strong marketing of its firewall products; as a result, it does not have much visibility on client shortlists. Despite the firewall offering mature threat detection capabilities, the marketing team markets its SD-WAN and VPN capabilities most of the time, resulting in a lack of awareness within the end-user base.

- Offering: The vendor lacks EDR client integration capabilities. It also lacks firewall integration with third-party EDR clients.
- Product Strategy: Despite having a strong client base and a focus on distributed office use cases, the vendor does not offer a cloud-based management portal, as offered by most competitors. The vendor also lacks FWaaS, despite offering multiple other cloud-based product lines.
- Customer Feedback: Surveyed clients have reported that the vendor's Level 1 support is not competent enough to deal with common support issues and escalates them further, creating longer escalation cycles.

Fortinet

Fortinet is a network and security player, headquartered in Sunnyvale, California. This year, Fortinet firewalls continue to be visible in distributed office deals where integrated SD-WAN is the primary selection criterion. They are also seen as replacing dedicated routers and act as an edge appliance with firewalls. Fortinet is also a favorable firewall shortlist for customers that cite pricing as an important selection criterion. The vendor offers a range of firewall models to meet multiple firewall deployment use cases. It also offers support for bare metal and virtual firewalls for Alibaba Cloud, AWS, Azure, Google Cloud Platform, IBM Cloud and Oracle OCI IaaS platforms.

The other products in Fortinet's portfolio cover network security, endpoint security, security information and event management (SIEM), NAC, wireless access points and switches. FortiGate firewalls are still the vendor's most popular and best-selling product.

In 2018 and 2019, Fortinet introduced new FortiGate models 6000F, 3600E, 3400E, 600E and 400E Series. It also had two major firmware releases with enhancements for the FortiGate firewall, new SD-WAN ASIC, virtual security processors, and centralized management and reporting software. It continues to work toward integration through APIs and security fabric.

Strengths

- SD-WAN: Fortinet offers integrated SD-WAN capabilities within its E-Series firewalls, which makes it a favorable shortlist candidate for distributed enterprise use cases. It comes with capabilities like application-based routing, especially for SaaS applications like Office 365 that are easy to configure. The vendor also offers features such as multipath automated failover for specific applications based on health performance, latency, jitter and packet loss, which enhance the performance of the applications.
- SSL Decryption: This year, Fortinet introduced support for TLS 1.3 in the FortiOS 6.2 release. This feature enhances existing deeper inspection capabilities for the Web Filter profile with flow-based inspection mode enabled and for the SSL/SSH Inspection profile.
- Integration: Fortinet continues to extend integration capabilities using security fabric and APIs with AWS, Azure, Google Cloud Platform and Alibaba, and develops tools to offer automation. Some of the capabilities include security fabric integration using AWS Lambda, and automatically updating dynamic addresses for

AWS using Fabric Connectors. The vendor also offers playbooks for integration of Ansible and Terraform modules.

- Geographic Presence: FortiGate firewalls continue to be visible on Gartner client firewall shortlists in different regions, competing with regional players. Regional players have also citied Fortinet as one of the top three competitors for them locally.
- Sales Execution: Fortinet works closely with many MSSPs globally that are offering Fortinet firewalls as hosted services to their clients. The vendor has specific licensing models for its VM-Series appliances specific to MSSPs. FortiManager and FortiAnalyzer also offer multiple multitenancy features that can be extended using APIs.
- Licensing: While the majority of Gartner clients generally complain about complex licensing by most enterprise-grade firewall vendors, Fortinet has maintained its simpler licensing by offering bundle-based licensing, which is easier to understand and renew for end users.

Cautions

- Visibility: Despite support for multiple cloud IaaS platforms, FortiGate is not visible on Gartner client shortlists as a preferred firewall on IaaS platforms, compared to prominent competitors that have more visibility in this use case.
- Product: Although Fortinet offers security fabric and API integration capabilities for integration of its products, it lacks mature direct integration capabilities of its firewalls with other security products in the portfolio for threat correlation. The vendor offers basic visibility into infected hosts and their vulnerabilities through FortiClient as a dashboard widget, but lacks mature direct threat correlation capabilities with FortiGate. FortiManager and FortiManager Cloud lack the management controls of FortiWeb, FortiSIEM and FortiCASB.
- Offering: The vendor has more focus on hardware-based offerings than cloud service offerings. Fortinet lacks cloud-based outbound filtering services such as FWaaS directly to its clients, especially for distributed office and roaming user use cases that prefer cloud-based services rather than hardware appliances.
- Customer Feedback: Fortinet clients often cite that the logs offered are not easy to drill through to find an incident and are more complicated compared to other firewall market leaders.
- Customer Experience: Surveyed clients have reported on the management complexities of the firewall as more and new features are added. This also leads to frequent UI changes, which makes administration complex. Clients have cited that application control is not tightly integrated with the firewall, and creates administration complexity while creating firewall rules.

H3C

H3C is headquartered in Beijing and Hangzhou, China. Until 2016, it operated as a subsidiary of Hewlett Packard Enterprise (HPE) and now is a part of Tsinghua Unigroup. It is an infrastructure vendor with a large

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

H3C continues to introduce different security offerings in its products. The SecPath firewall offers support for UniCloud public IaaS platforms as bring your own license (BYOL) only. The firewalls are primarily shortlisted by clients in China, where the vendor has its largest installed base.

The vendor's SecPath firewall family comprises 14 physical appliances and virtual firewall models.

Recent product news includes the introduction of a new SMB series and performance enhancements.

Strengths

- Product Offering: H3C's firewall offers a separate industrial firewall product line called Industrial Control Security, which includes an industrial control firewall, project monitoring and host security software.
- Offering (NTA): The vendor offers an NTA platform branded as a security situation awareness system that collects network traffic flow data and other data across the entire network. The product also combines machine learning to offer correlated data and display based on heat maps and other graphic forms. The product can be integrated with the firewall to take policy-based actions.
- Offering (NAC): The vendor offers a native NAC solution with integration capabilities with its firewall. The NAC solution is called the H3C intelligent Management Center (iMC), and it delivers centralized management capabilities across cloud and data centers, end-user management, campus network, and wireless management.
- Product: The centralized Security Service Manager (SSM) extends product management to other H3C products, such as its WAF and load balancer, in addition to firewalls, thus offering centralized management capabilities to H3C customers that have the above-mentioned products from the vendor. SSM also offers management and visibility capabilities into the native controls offered by UniCloud, a Chinese public IaaS vendor.
- Customer Feedback: Surveyed clients have reported ease of management and operation as the vendor's strengths.

Cautions

- Execution: H3C firewalls only offer support for UniCloud as BYOL. They are available as pay as you go only as VPN and NAT gateways. Clients that want to avail themselves of a complete feature set of H3C firewalls on public cloud must use a BYOL model only.
- Market Responsiveness: The vendor lacks integrated SD-WAN capabilities in its firewalls, which is a desirable feature for distributed enterprise connectivity.
- Technical Feature: H3C firewalls do not support TLS 1.3-based decryption.

- Geographic Strategy: The vendor has a presence primarily in China and lacks a presence in other parts of the Asia/Pacific region. Gartner does not see H3C being shortlisted by clients outside China.

Hillstone Networks

Hillstone Networks is headquartered in Suzhou, China, with regional headquarters in Santa Clara, California. The vendor is an established network security player offering perimeter, cloud and server security solutions. Hillstone firewalls are well suited for shortlists in enterprises with hybrid networks, such as on-premises, cloud and virtualized environments, mainly in China, Southeast Asia and Latin America.

Hillstone firewalls have dedicated firewall product lines for microsegmentation and public IaaS platforms. Hence, they are favorable candidates for hybrid networks. Primarily shortlisted by clients in China, the vendor has shown a growing installed base in Europe, the Middle East and Africa, and Latin America.

The vendor offers multiple firewall product lines, namely the E-Series NGFW, T-Series iNGFW and X-Series Data Center Firewall. It also offers CloudEdge (virtual NGFW), CloudHive (microsegmentation) and CloudPano (hosted FWaaS through telcos, in the China market only). CloudEdge offers support for AWS, Azure, Alibaba Cloud, Tencent Cloud and Huawei Cloud. Other security products include IDPS, WAF, application delivery controller, ABG, DLP and DAP (with a few products only available in the Chinese market).

In 2018, the vendor introduced two new models: X10800 and CloudEdge VM04. Other product updates include threat detection enhancement and firmware releases.

Hillstone is one of the few Chinese network security vendors that is gradually expanding into other regions outside China such as Latin America, Southeast Asia, the Middle East and Europe.

Strengths

- Microsegmentation: Hillstone CloudHive is a dedicated product line that offers mature microsegmentation capabilities with VMware NSX. CloudHive offers features such as live visual mapping, autodiscovery of new virtual networks and threat detection across virtual machines (VMs) centrally.
- Platform: The vendor offers Hillstone sBDS, its NTA platform, available globally. This platform uses different detection technologies including NTA to perform advanced threat detection and analytics for Hillstone clients. The vendor also offers a SIEM solution called iSource, currently sold only in China.
- Offering: The vendor offers behavioral analysis as an additional subscription on its T-Series firewalls. This makes it a favorable shortlist candidate for enterprises looking for additional threat detection capabilities within their firewalls beyond network sandboxing.
- Customer Feedback: Surveyed clients have highly rated the VPN feature of the firewalls, stating they are easy to configure and manage between multiple sites.

Cautions

- SD-WAN: Hillstone firewalls lack SD-WAN capabilities, which are being offered by many competitors today. This makes them less desirable candidates for distributed office connectivity use cases.
- Product Execution: The vendor offers different product lines of firewall appliances, namely the T-Series, E-Series and X-Series, creating confusion within the end-user base when comparing feature distinctions among them.
- Offering: The vendor does not offer on-premises network sandboxing. This is a requirement for regulated clients that cannot send data off-premises.
- Feature: Although Hillstone offers partnerships with global and regional EDR vendors, it does not offer a common threat correlation portal to benefit firewall users that are looking for better threat detection capabilities.
- Visibility: Despite the vendor claiming expansion outside of China, Hillstone firewalls are rarely seen on client shortlists outside China and Latin America.
- Marketing: The vendor lacks strong marketing of its firewalls in the end-user market as it is targeting international markets and competing with global players that have better marketing campaigns. This results in a lack of recognition in the end-user market outside of Asia.
- Product: The vendor offers a basic cloud-based firewall manager that is limited to monitoring only and lacks additional centralized management controls, such as change management and zero-touch provisioning of firewalls.

Huawei

Huawei is a large infrastructure vendor based in Shenzhen, China. Its firewalls continue to expand their customer base in Southeast Asia, the Middle East and Latin America. They have a strong presence in telcos and are also visible in the infrastructure bundled deals of Huawei.

Huawei firewalls include the Unified Security Gateway (USG), Eudemon and virtual series. USG is the primary enterprise line, and Eudemon is the model line for carriers and service providers. Agile Controller, eSight and SecoManager are the central management platforms that support the USG line. Other than firewalls, the vendor also sells IDPS, anti- DDoS, SIEM and web application firewall product lines under its security portfolio.

Huawei firewalls are good candidates for customers already using Huawei products or looking toward consolidation of network and security products from the same vendor, because of integration and ease of centralized management. Huawei offers multiple product models for different firewall deployment use cases. It also offers mature SD-WAN capabilities for distributed office use cases.

Product news for this year includes enhancements related to SD-WAN, IDPS and web UI.

Strengths

- Ease of Management: Huawei firewalls have an easy-to-create firewall rule UI. It offers a single UI instance to create firewall policy and apply security policies that is easy to administer. Surveyed clients have also reported it as one of the strengths of the product.
- Offering: Agile Controller is the vendor's NAC solution. It is also offered in a cloud version. It has two versions: one is for data center networks, called AC DCN. The other is called AC Campus, for campus or enterprise use. Both versions can be closely integrated with the firewall by a callback feature and offer automation capabilities to segment the network.
- Product: The vendor offers an on-premises centralized manager called SecoManager, which has dedicated policy orchestration features such as policy tuning and a policy simulator. It also offers a visualization feature for new policies to show their impact on traffic.
- Feature: Huawei firewalls offer support for TLS 1.3, enabling deeper SSL decryption and traffic inspection capabilities for encrypted traffic.
- Offering: The vendor offers deception capabilities in its firewall appliances. These are offered in a separate product image that can be mounted on the firewall appliances and managed from within the firewall UI as a separate feature. Although the deception platform offered today is basic, it offers additional threat detection capabilities in the firewalls. It is recommended that clients evaluate the performance impact of running this image on the firewall appliance before enabling it.
- Integration: Huawei offers direct integration capabilities with its big data analytics SIEM solution, Cybersecurity Intelligence System (CIS). The integration is offered as a built-in option within the firewall UI that can be simply turned on, making it easy to integrate and use in conjunction with Huawei firewalls.

Cautions

- Execution: Huawei firewalls lack integration capabilities with third-party security vendors, especially SIEM providers. Surveyed vendors have highlighted this as a drawback of the USG firewalls. Clients face issues in sending the firewall logs to third-party SIEM vendors. The vendor also lacks direct integration and correlation capabilities between its firewalls and third-party EDR solutions, and requires a CIS platform for correlation. Hence, it is strongly recommended that clients evaluate the integration capabilities between Huawei firewalls and third-party solutions in their ecosystem as an important shortlisting criterion.
- Public Cloud: Despite offering appliance support for multiple public IaaS providers in a BYOL model, the vendor's offering is not available on any IaaS platforms as pay as you go, while most firewall vendors support pay-as-you-go licensing models for more than one IaaS platform.
- Feature: The vendor offers basic centralized cloud management capabilities through its cloud portal. It can only be used to manage limited features on the firewalls, and lacks centralized firmware upgrades and zero-touch provisioning capabilities on a group of firewalls.

- Sales Execution: Huawei firewalls lack a uniform presence within different firewall use cases such as SMBs, perimeters and distributed offices. Gartner still sees most firewall procurement as being part of larger Huawei infrastructure deals most of the time, rather than firewall-only deals.
- SDN: Huawei firewalls offer support only for the Huawei CloudFabric platform and lack support for other common SDN platforms as offered by major firewall players. This increases the dependency of clients on Huawei's SDN infrastructure.
- Product Strategy: The vendor lacks a focus on cloud-based services related to firewalls and their users. Most of the features offered by the vendor are appliance-based. Huawei lacks outbound filtering cloud services for roaming users and distributed offices as a SaaS offering.

Juniper Networks

Juniper Networks is a network infrastructure vendor headquartered in Sunnyvale, California. It aligns its products with a security focus under the Juniper Connected Security banner, which provides automated and centralized security policy definitions through the Juniper Policy Enforcer engine. This utilizes Juniper switches, routers and firewalls for security profiling and threat detection and enforcement, while integrating directly into the Juniper Sky Enterprise cloud platform. While the SRX firewalls offer a complete set of security features, they are still not very visible on client shortlists.

Juniper's broad product portfolio includes a range of network edge and management devices, routers, switches, SDNs and enterprise firewalls (i.e., the SRX Series firewalls). The Virtual SRX firewalls offer support for AWS, Microsoft Cloud and IBM SoftLayer public IaaS platforms, both as BYOL and pay-as-you-go licensing models. The SRX hardware appliance product line has 15 distinct hardware platform models, ranging from 500 Mbps to 2 Tbps.

Recent updates include the introduction of cSRX firewall for container workloads. The vendor also introduced different feature enhancements, including routing and VPN features, Policy Enforcer integration with AWS and Azure, and Nutanix integration with vSRX. The SRX firewall also got FIPS certification.

Strengths

- Product: Juniper's centralized on-premises manager product, called Junos Space Security Director, offers mature orchestration capabilities as the vendor continues to enhance the product constantly. The product offers mature multitenancy features favorable for MSSPs, such as support for up to 100 simultaneous admin logins, where all of them can simultaneously perform tasks. The product offers a policy administration feature straight out of the dashboard. The vendor also offers a firewall rule creation wizard with policy analysis for autoplacement of the new rule, which avoids shadowing. The feature also alerts in cases of duplicate rules.
- Feature: Juniper extends support for Policy Enforcer, firewall policy builder and its firewall rule creation wizard to AWS and Azure, simplifying the creation of centralized firewall policies for cloud workloads that can otherwise be challenging.

- Scalability: Juniper SRX firewalls come in multiple models to meet all firewall use cases. The vendor offers one of the highest-performing firewall models — the SRX5000 series — offering throughput of up to 2 Tbps and utilized by telcos primarily.
- Integration: Juniper has a large partner ecosystem to which it has extended API integration. It offers integration capabilities between SRX and NAC vendors like Forescout Technologies, HPE (Aruba), Pulse Secure, and CASBs Netskope and CipherCloud. The NAC integration extends to Juniper switches, enabling the use of Policy Enforcer to quarantine the infected endpoint.
- Product Strategy: Integration with Carbon Black (CB) Response (EDR) is provided, which leverages Juniper Sky ATP TAXII server to retrieve STIX packages of malware discovered by Juniper Sky ATP. CB Response will extract the IOCs it supports and compare them to all the endpoints it manages. It provides the ability to identify whether someone else has been infected on the network. CB Response also leverages the Juniper Sky ATP Infected Host API to update the list of infected hosts when it identifies a host as compromised based on different threat feeds.

Cautions

- Feature: The application control feature of Juniper is still not rated high compared to its competitors. It lacks granularity and offers limited subcontrols for many applications.
- Product Strategy: The vendor has a primary focus on introducing features on hardware appliances and lacks mature cloud-based service offerings for roaming users and distributed use cases such as a direct FWaaS offering.
- Offering: Juniper offers multiple different centralized managers with distinct features, including Junos Space Security Director (centralized security manager), Juniper Sky Enterprise and Contrail Service Orchestrator. This requires clients to use multiple manager tools based on their use case. Surveyed clients have also reported multiple nonintegrated managers as a product weakness.
- Support: Surveyed clients have reported that they often come across firmware-related bugs that are unknown to the vendor, thus creating longer support escalations. Juniper does not offer bug bounty programs.
- Customer Feedback: Juniper SRX clients have reported that the process of upgrading firmware on the firewalls is not smooth. They have mentioned that the upgrade process forces the reboot of primary and secondary firewalls, and does not failover during upgrade.
- Visibility: Juniper SRX firewalls are still not very visible on the firewall shortlists of Gartner clients as compared to competitors. They have also been mentioned as one of the most replaced firewalls by the participating vendors in this Magic Quadrant.

Microsoft

Microsoft, based in Redmond, Washington, offers Azure, a large IaaS platform. Azure supports third- party partners that provide security controls for their customers; since September 2018, Azure has had its own set of firewall services, Azure Firewall. Currently, Azure Firewall is managed by the Azure portal or command line interface, and central management is available through third parties such as Tufin, AlgoSec and Barracuda. Reporting is offered through Azure Monitor. Also included among Microsoft Azure security offerings are Azure DDoS and Azure WAF (global and regional). The vendor also offers separate connectivity offerings such as Azure ExpressRoute and VPN.

Company news includes the launch of Azure Firewall and the continued refinement of Azure security services. During the evaluation period, Microsoft has continued its bold initiative with partners to help secure its cloud while launching various native security services. The vendor continues building out a strong threat intelligence capability that informs all its security offerings.

Azure Firewall is a good candidate for protection in regional Azure clouds for application teams that value agility, automation and autoscaling, with solid native firewalling controls.

Strengths

- Product Execution: Early customers note that Microsoft has taken their input into account, and has implemented feature requests from early trials or has included suggested features in its product roadmap.
- Pricing: Azure Firewall has a simple pricing model that is easy to consume and utilize. The vendor offers hourly deployment charges and per-GB data processing charges, making the pricing structure simple.
- Product Strategy: Azure's cloud-native firewall helps to simplify the Azure environment, making policy changes, debugging and autoscaling easier than they are with third-party tools. This helps DevOps-oriented customers with ever-changing workloads maintain security with minimal operational friction.
- Marketing Strategy: Microsoft does not overpromise on its firewall capabilities. Gartner clients report that the vendor suggests using a strong partner ecosystem to add security in high-security use cases. This helps Azure customers trust that Microsoft will deliver the security it promises from its native firewall offering.
- Capabilities: Microsoft has a robust threat intelligence team that informs its firewall product. Customers like the approach to filtering outbound internet traffic with fully qualified domain name (FQDN) intelligence. Azure firewalls also offer support for service tags and FQDN tags for better rule creation.
- Geographic Presence: Microsoft Azure has a good geographic presence globally. As a result, it has better visibility than many other vendors that are available in limited regions.

Cautions

- Product: Azure firewall only meets network firewall deployment use case of Microsoft Azure customers.
- Offering: Microsoft's firewall offering lacks IDPS and advanced threat detection capabilities, which are often requirements for security teams choosing firewall platforms. As a result, Azure clients have to use third-party threat detection and IDPS tools.

- Pricing: Microsoft requires a different firewall in each region. Azure customers note that this can lead to much higher costs, and can cause more operational expense with added administration and management complexity, especially considering the lack of a central management console.
- Capabilities: Surveyed customers note the need for more predefined Layer 7 protocols and improved logging to ease the auditing process.

Palo Alto Networks

Santa Clara-based Palo Alto Networks is a large security vendor with more than 5,800 global employees, shipping firewalls since 2007. In addition to enterprise firewall physical and virtual appliances, the vendor's products include EDR software, threat intelligence, SaaS security, cloud compliance and policy management tools, and security orchestration, automation, and response (SOAR). The vendor has delivered integrations between its offerings as a security operating platform, managing it from its Panorama management console. Palo Alto Networks has made use of its Cortex offering to build out its third-party ecosystem, enabling partners to build applications that interact with the Palo Alto Networks platform.

Palo Alto Networks firewalls continue to lead the firewall market share, showing strong revenue growth. Its firewalls have the most visibility on firewall shortlists in Gartner client inquiries. Introduction of Prisma Access and the Prisma cloud offering show the vendor's growing focus on cloud services.

Company news includes the acquisition of Twistlock, a container security technology, and PureSec, a serverless security solution. In addition, the vendor has recently repackaged its cloud security solutions under the name Prisma and its offering of solutions for security operations under the name Cortex.

During 1H19, Palo Alto Networks released its 9.0 version, introducing DNS Security Service. As part of this release, it also introduced a series of line cards for its PA-7000 line of appliances, in hopes of increasing throughputs with security protections enabled.

Strengths

- Sales Strategy: Gartner has noted an increasing number of Palo Alto Networks firewalls being bought under the vendor's ELA contract as part of a larger security platform play. Some Gartner clients express interest in using the Panorama management platform as the orchestration point for the vendor's integrated solutions. Surveyed customers and resellers value the platform approach.
- Offering: Palo Alto Networks is the first hardware-based firewall vendor offering direct FWaaS as a SaaS model. Its Prisma Access FWaaS offers outbound filtering capabilities. Gartner has seen some positive adoption of the product for branch offices and roaming user use cases.
- Sales Strategy: Customers report that more of their Palo Alto Networks spend is on subscriptions rather than hardware, making security budgeting more predictable. Surveyed customers rated Palo Alto Networks' firewall as one of the most likely firewalls they were considering renewing without conducting a competitive evaluation.

- Product Execution: In 1H19, Gartner clients reported improved SSL decryption performance. If this improvement continues, the enhanced capability, plus the line cards introduced for the PA-7000 Series to improve performance, will make Palo Alto Networks more suitable for large-scale data center deployments.
- Product Strategy: The Twistlock and PureSec acquisitions demonstrate a vision of anticipating customers' mid- to long-term needs as they construct new workloads using microservices and serverless environments. Palo Alto Networks is building a very broad cloud ecosystem, announcing new public cloud support for Alibaba Cloud and Oracle Cloud, and for private cloud/SDN and hybrid use cases, with support for Cisco Enterprise Network Compute System (ENCS), VMware Cloud for AWS and NSX, and Nutanix.
- Client Feedback: Surveyed firewall respondents list Palo Alto Networks as the vendor they most often evaluate. This tracks with Gartner client inquiries, as Palo Alto Networks is the vendor most visible on client shortlists.
- Customer Experience: Gartner clients have highly rated the vendor's presales team making the evaluation period smoother. They cite its presales services as being highly professional in terms of offering quality of support during the evaluation period irrespective of the size of the deal — something they indicate other competitors lack.

Cautions

- Pricing: Even with improved price/performance ratios at the branch office, price is frequently cited by Gartner clients as a reason not to select Palo Alto Networks. The chassis-based data center firewalls (PA-7050 and PA-7080) are called out as being very expensive compared to other solutions.
- Product Strategy: As the vendor continues to expand its product portfolio by acquiring early-stage security technologies. Gartner observes that these are sometimes released to customers before reaching maturity, leading to early customer dissatisfaction. Before purchasing these new products, Gartner recommends that clients carefully evaluate the capabilities of new product acquisitions to ensure that they can fulfill their requirements.
- Execution: Palo Alto Networks came to market with a tightly engineered firewall, which was also evident in early product acquisitions such as Cyvera (endpoint traps) and Morta Security (integrated into WildFire). However, the increasing pace of acquisitions over the past few years has resulted in loosely federated components without the same level of integration seen previously. This is evident in recent acquisitions such as Evident.io, RedLock, CirroSecure (now Prisma SaaS), Demisto, Secdo and LightCyber which were branded as stand-alone product lines and recently repackaged under the Prisma and Cortex offerings .
- Product Strategy: Gartner clients and surveyed customers and partners continue to 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: Gartner clients note performance issues within public cloud environments. Some cite the necessity of deploying high-availability (HA) pairs of virtual firewalls in IaaS cloud, thus increasing costs and

the solution's operational footprint, and adding to a less-than-smooth deployment experience on the public cloud.

- Feature: Palo Alto Networks firewalls lack an integrated SD-WAN feature and offer it through partnerships with third-party vendors. The vendor also lacks a cloud-based management portal offered as a SaaS model.
- Customer Feedback: Surveyed clients have indicated a decline in the quality of technical support, with the growing number of customers in the vendor's installed base.

Sangfor

Based in Shenzhen, China, Sangfor is an IT infrastructure and security vendor. It is a regional Chinese vendor with a growing focus on cloud service offerings, including a FWaaS offering, that Chinese competitors lack. It is primarily focused on midsize enterprises and has a major presence in Southeast Asia, with some client base in Europe and the Middle East. Its technical support is highly rated by surveyed clients.

Its firewall product line is called Sangfor Next Generation Application Firewall (NGAF), available in the form of physical and virtual appliances. The virtual models are available as BYOL on AWS and Alibaba Cloud. Its centralized management, Sangfor Branch Business Center (BBC), is offered as a separate appliance. In addition, Sangfor offers Security Butler, a cloud-based portal offering firewall log monitoring, security analysis and basic incident response Other security solutions include network and application vulnerability management SaaS, SSL VPN, WAN optimization (WANO), software-defined infrastructure, and SWG solutions.

Recent product news includes enhancements in threat detection capabilities by integrating the vendor's sandboxing and threat intelligence services.

Strengths

- Product Strategy: Sangfor offers multiple cloud-based services for clients, including FWaaS (Cloud Eye, a cloud-based network vulnerability scanning tool, and Cloud Shield, a WAF that is only available to the Chinese market); Neural-x, a threat intelligence service; and Security Butler, a threat analysis portal. This makes Sangfor a favorable candidate for distributed office use cases.
- Product: The vendor offers a native EDR client. It offers threat intelligence correlation of firewall and EDR on its threat analysis cloud platform, Sangfor Butler, offering firewall users additional threat detection capabilities.
- Feature: Sangfor NGAF offers a configuration wizard for security policy deployment and modification, which has been highly rated by surveyed clients. The wizard offers virtual network mapping during a new change request.
- Client Feedback: Sangfor BBC, its on-premises centralized manager, has been highly rated by clients as an easy-to-use product, making management of multiple firewalls simpler. BBC can also be used to manage

many other Sangfor products such as SWG, WANO, SD-WAN and SSL VPN .The vendor also offers a cloud-based manager, X-Central, with the same capabilities as BBC.

- Technical Support: The vendor's technical support is rated high by surveyed customers.

Cautions

- Sales Execution: Sangfor firewalls are primarily deployed by midsize enterprises and the vendor also focuses its product development around SMB use cases. Sangfor is not very visible within enterprise and data centers in Gartner client inquiries.
- Customer Feedback: Surveyed clients have reported the built-in logging and reporting in the Sangfor firewall lacks granularity and the logs are complex to search through, requiring them to purchase a dedicated reporting tool for advanced reporting capabilities. The on-premises dedicated reporting and logging appliance is only available in Chinese.
- Presence: Sangfor is a regional vendor with most of its clients based in China. Although it is working toward expanding in other regions of Asia, Europe and the Middle East, Gartner primarily sees it being shortlisted by clients in Southeast Asia.
- Customer Feedback: Surveyed clients have reported that the midsize models of Sangfor firewalls not offering default 10 Gigabit interfaces is a weakness for enterprise customers looking for faster performance.
- Product: The vendor only offers support for its native SDN platform, Sangfor HCI. It also offers pay-as-you-go licensing models only for its native Sangfor HCI public IaaS platform and Alibaba Cloud. It is not available as pay as you go on AWS, where it is available as BYOL only.

SonicWall

SonicWall is based in Milpitas, California, and is a network security player. Today, the vendor offers multiple firewall product lines, branded as TZ Series, NSa Series, SuperMassive Series, NSsp Series and NSv Series. The NSv series supports VMware ESXi, Microsoft Hyper-V, and both BYOL and pay-as-you-go support for Microsoft Azure and AWS.

SonicWall firewalls have their primary client base in midsize enterprises. Although the vendor has high-performing data center appliances, Gartner does not see them in this use case. The vendor has been introducing multiple product-related enhancements for the past three years, to offer a complete set of features. Overall, the visibility of the vendor on firewall shortlists is decreasing.

In addition to firewalls, SonicWall also sells wireless, remote access email security, cloud application security and endpoint security products.

Recent company news includes the introduction of multiple new models in the NSa, NSsp and TZ Series.

Other recent updates include the introduction of a secure SD-WAN feature, adding zero-touch deployment through cloud management, Cloud App Security, Capture Security Center (CSC) for centralized management of all products, and Analyzer 2.0, which is SonicWall's flow analytics solution.

Strengths

- Offering: CSC, the vendor's cloud-based manager, offers a complete set of centralized management for all its products and offers features such as a bulk firmware upgrade and a pushing of rules. This year, SonicWall has also introduced a zero-touch deployment feature integrated within CSC. This service is available in one freemium offering, Management Lite, and three paid subscription packages — Management, Management and Reporting, and Analytics.
- Product: SonicWall's on-premises centralized manager, Global Management System (GMS), offers mature management and multitenancy features desired by MSSPs. Like CSC, in addition to managing firewalls, GMS can also manage and report on SonicWall's Secure Mobile Access and Email Security, integrated SonicWall wireless access points, and WAN acceleration solutions, offering centralized management capabilities for multiple product lines.
- CASB: SonicWall offers CASB capabilities in the SonicWall Cloud App Security offering. It offers security for SaaS applications such as Office 365 and Google Suite by offering cloud-based email scanning and access controls, and preventing the upload of sensitive or confidential files and data. It also offers role-based policy tools, data classification and loss prevention. This product is integrated with the cloud manager CSC, offering centralized management and visibility and control of SaaS application usage.
- Technical Support: Surveyed clients and resellers have consistently cited direct support for the vendor as high quality and very responsive. Clients have especially reported that support drastically improved after SonicWall spun off Dell.

Cautions

- Sales: Gartner is seeing declining SonicWall firewall revenue. It was the only UTM vendor with a revenue decline (-3.9%) in 2018. Gartner also doesn't see it as a favorable shortlist candidate based on client inquiries.
- Market Responsiveness: The vendor lacks strong market responsiveness as per the demands of clients. It was late in introducing virtual appliances, and in support for public cloud and SD-WAN. Gartner finds that SonicWall has been closing gaps, rather than introducing innovative features. Despite introducing multiple virtual appliances, its firewalls still lack support for SDN platforms, something being offered by the majority of its competitors in the market.
- Product: The vendor lacks an on-premises sandboxing appliance, a desirable feature for highly regulated enterprises that do not want their data to leave the premises, particularly in emerging regions such as the Middle East, Asia and Latin America.

- Customer Feedback: Surveyed clients have reported a lack of mature logging as one of the product weaknesses in GMS. They have specifically mentioned the logging details around firewall-rule-administration-related changes, which are not detailed enough. Clients have also highlighted the lack of SAML support for multifactor authentication (MFA) as a product weakness.
- Product Strategy: The vendor lacks integration capabilities with third-party NAC platforms. This makes SonicWall a less desirable shortlist candidate for enterprises seeking correlation and integration capabilities between their NAC products to disconnect infected hosts.

Sophos

Sophos is a network and endpoint security vendor headquartered in Abingdon, U.K. It took over the second-largest UTM vendor market share position in 2018. Sophos continues with its strong firewall and endpoint security integration product strategy. It is visible in SMB use cases, but lacks visibility in enterprise and data center use cases.

The vendor's portfolio includes firewalls (the XG Series and SG 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 APX) and multicloud protection (Sophos Cloud Optix),. 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 hardware models and three Remote Ethernet Device (RED) models, which are plug-and-play remote tunneling devices for SD-WAN use cases in remote offices. Sophos also offers support for AWS and Azure, both as pay as you go and BYOL, through its virtual firewalls. It still sells and actively develops both the XG and SG product lines. The range of XG models starts with the XG 86 (3 Gbps throughput) up to the XG 750 (100 Gbps throughput).

This year, Sophos completed a hardware refresh of existing models. The key new features introduced include enhancements to its Synchronized Security system, air gap support, Chrome authentication and a central cloud management portal for XG firewalls and other Sophos products.

Strengths

- Innovation: Sophos is one of the few firewall vendors catering to midsize enterprises that can decrypt TLS 1.3 natively instead of forcing a downgrade to TLS 1.2. Sophos acquired Avid Secure in 2019 to provide a new multicloud visibility capability called Sophos Cloud Optix, which helps customers manage cloud security posture management in AWS, Microsoft Azure and Google Cloud. In addition, it added cloud-based management capabilities for its XG firewall line.
- Market Responsiveness: Sophos continues to increase visibility, detection and response capabilities of advanced threats to meet the growing market requirement. It also added a CASB-lite function to its firewalls primarily focused on visibility of SaaS usage use cases.

- Sales Strategy: Sophos has a strong channel strategy with many partners located around the globe and, over the past year, has grown an already sizable and loyal channel base substantially. It conducts regular partner training and information-sharing programs worldwide. 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.
- Product: 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: Customers surveyed cite strong presales support and ease of implementation as key differentiators in choosing Sophos for network firewalling. An intuitive management interface and tight integration with Sophos products are also cited frequently as key strengths of the product.

Cautions

- Product Strategy: Sophos' product strategy is more focused on midsize enterprises and currently fails to meet some enterprise deployment use cases, including providing high-throughput appliances. Sophos continues to pursue a strategy of integration with its own products in lieu of third-party support for items such as CASB and endpoint protection platforms. In addition, there is no third-party NAC integration with the firewall to support more advanced enterprise response capabilities when an NAC solution detects a compromised endpoint.
- Market Segmentation: Sophos maintains most of its presence in small to midsize enterprises, which are heavily centralized to one site or a few locations. Resellers report a lack of brand awareness around Sophos, and Gartner rarely sees Sophos show up on client shortlists, especially in larger enterprises.
- Customer Experience: Gartner clients frequently cite the firewall and endpoint (Intercept X) integration capability as a primary reason to shortlist Sophos firewalls as opposed to any other firewall feature the vendor offers. Gartner clients purchasing Sophos firewalls beyond the mentioned primary use case must evaluate other features and third-party endpoint protection platform (EPP) integration capabilities offered by the product before shortlisting the vendor. Gartner clients have reported issues with virtual IaaS versions of Sophos, especially in HA scenarios, and have highlighted that the basic support subscription is not sufficient to help with public IaaS deployment issues, requiring them to upgrade to premium support to get desirable support.
- Product: Sophos firewalls lack certifications that are important to enterprises with heavy regulations such as Common Criteria EAL4. 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, enterprise customers utilizing other commercial EDR vendors will not be able to utilize and share endpoint-related threat intelligence with their firewalls.

- Offering: Sophos still lags behind its competitors in cloud-based security offerings such as FWaaS, DL, and integration with third-party CASBs to support more advanced CASB use cases.

Stormshield

Stormshield is a credible shortlist contender for European organizations, especially local government agencies or enterprises working with local government agencies and looking for a vendor that works to continuously lower total cost of ownership (TCO) of hardware through software updates. Stormshield largely serves customers in a few countries in Western Europe; however, it recently closed its U.K. office in anticipation of Brexit.

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 in popular private and public cloud platforms, including VMware, AWS and Microsoft Azure. Centralized management (Stormshield Management Center [SMC]) and reporting (Stormshield Visibility Center [SVC]) are available as software appliances.

Stormshield offers its SNS firewall appliances ranging from the SN160 model (1GB of throughput) through the SN6100 (140GB of throughput). Stormshield provides industrial protocol protection on all firewalls and also offers a ruggedized version for field use, the SNi40.

Stormshield released a free public version of its Breach Fighter sandbox in 2019 and new virtualized appliances called Elastic Virtual Appliances, including a pay-as-you-go program for MSSPs and cloud providers.

Strengths

- Customer Experience: Customers surveyed cite ease of implementation, configuration and upgradability as key strengths of the product. Stormshield is cited as having a strong TCO compared to other firewall vendors because of its easy licensing and upgrade sales strategy.
- Product: Advanced threat detection, IDPS and other features of the product focus on the protection of industrial IoT (IIoT) across all product lines, which is unique in this market. With the addition of the public Breach Fighter sandbox, clients can test the efficacy of the sandbox to detect malicious files unique to their environment before attaching the sandbox to their firewall. In addition, it has JavaScript Content Disarm and Reconstruction features as part of its offering when filtering web content.
- Sales Execution: Stormshield is growing its firewall revenue at an above-average rate compared to other small vendors in this Magic Quadrant. It continues to expand into other verticals outside its primary focus.

- Vertical Strategy: Stormshield focuses sales and support in certain verticals, such as manufacturing, energy, government, defense, critical communication and transportation. This gives Stormshield a strong understanding and support of industries and country-specific issues across Europe.
- Operations: Stormshield maintains its investment in nationwide and regional certifications to better serve European local government agencies and enterprises that work with them. Clients with a heavy presence in France, Germany and other European countries that may need a firewall with embedded SD-WAN support should consider Stormshield on their shortlists for evaluation.

Cautions

- Market Responsiveness: Stormshield continues to lag in cloud features such as a lack of an FWaaS offering or a cloud-based firewall management console. Despite offering a cloud-based sandbox, it has very low attach rates from customers. The recently introduced Elastic Virtual Appliance (EVA) virtual firewall product line lacks autoscaling in IaaS environments.
- Sales Execution: Despite growth in revenue and a desired focus to expand to EMEA and the Asia/Pacific region, Stormshield remains one of the smallest firewall vendors by revenue in this research. It has a minimal to no presence in the Americas, the Middle East, Africa and the Asia/Pacific region.
- Product: While Stormshield completely relies on its in-house IDPS threat intelligence team for signature development, the size of the team is relatively smaller than most other competitors. At present, the vendor also lacks support for TLS 1.3. The management console interface appears less sophisticated than other consoles on the market.
- Geographic Strategy: Stormshield continues to focus its resources in Europe with limited sales channels and support for the rest of the world. Gartner recommends that clients carefully evaluate Stormshield’s ability to support an organization outside of its primary service areas, as technical support and languages supported within the management console are limited.
- Customer Experience: Customers surveyed report a higher-than-average hardware failure rate compared to other vendors in the market and a significant number of issues that impact availability. In addition, customers cite challenges with depth and availability of technical documentation, which lead to reliance on vendor training and support.

Venustech

Venustech is headquartered in Beijing, China. Venusense is a good firewall candidate for Venustech customers in China that are looking for a good local vendor with strong regional support in China and Japan, as well as a cost-effective firewall offering. The vendor is also a favorable shortlist candidate in China, where clients prefer security products from the same vendor because of its large product portfolio.

Venustech sells multiple firewall product lines, namely Venusense Unified Threat Management, Venusense Firewall (FW) and Venusense Next-Generation Firewall (NGFW). It also sells a dedicated industrial firewall product line, Venusense Industrial Firewall (IFW). Other than firewalls, the vendor sells WAF, IDPS,

vulnerability scanner, VPN, USM (SIEM), APT, ADM (anti-DDos) and physical security products. It also sells FlowEye, its firewall policy management and NTA solution.

This year, the vendor introduced cloud protection based on the VenusEye Threat Intelligence Center and a high-level firewall model with 720GB throughput.

Strengths

- Centralized Firewall Policy Management: Venustech FlowEye is the vendor's firewall policy management and NTA solution. The product can perform centralized firewall policy management beyond Venustech firewalls, extending support to all leading global and regional firewall players such as Fortinet, Check Point Software Technologies, Palo Alto Networks, Juniper Networks, Cisco and H3C. Some of the other key features offered by this product are configuration comparison, firewall migration and virtual network mapping. This helps large Venustech firewall users and MSSPs to fine-tune their policies along with centrally managing other firewall brands.
- Offering (NTA): Venusense FlowEye collects raw traffic and flow records (for example, NetFlow, Sflow and IPFIX) to analyze network traffic. It performs abnormal behavior detection through a variety of abnormal traffic, including Trojan channel detection, ARP spoofing detection, network scanning behavior detection, worm detection and DDoS attack detection. It comes as a separate appliance.
- Product: Venustech has a dedicated industrial firewall product line with different models. Venusense IFW supports the in-depth filtering based on Modbus/TCP, Modbus/RTU, nIEC104, OPC and Ethernet/IP. Beyond basic firewall features, the IFW also offers support for industrial IPS, industrial VPN, and flow self-learning for supervisory control and data acquisition system (SCADA), distributed control system (DCS), programmable control system (PCS), and programmable logic controller (PLC) protocols and applications.
- Product Strategy: The vendor has a threat intelligence (TI) correlation platform that is a separate product, called VenusEye Threat Intelligence platform. This platform correlates TI from different resources and products of VenusEye, and offers centralized correlation and threat scoring based on the built-in templates. This product has a direct integration with the Venustech firewall from within the administration UI, which makes it easy to use for firewall users that require additional threat intelligence.
- Customer Feedback: Surveyed vendors have rated ease of use and management of Venustech firewalls as high.

Cautions

- Public Cloud: Venustech firewalls lack support for pay-as-you-go licensing for public IaaS platforms, while the majority of firewall vendors offer it. The vendor currently only supports BYOL for Alibaba Cloud and Tencent Cloud.
- Offering: The vendor only offers an on-premises sandboxing appliance and lacks cloud-based sandboxing services, which most competitors offer as an add-on subscription.

- Offering: Venustech lacks integration capabilities with EDR vendors and does not offer its own EDR client. Some clients prefer additional threat intelligence and correlation capabilities between their firewall and endpoint for advanced threat detection capabilities.
- Customer Feedback: Surveyed clients have reported the built-in firewall reporting feature as basic and requiring additional products such as an SIEM or a TI center subscription for better detailed reporting.
- Geographic Presence: Venustech primarily sells its products in China and is not seen as a preferred shortlist candidate outside of that country; however, the vendor is trying to expand in Southeast Asia.

WatchGuard

WatchGuard is a network security vendor with headquarters in Seattle, Washington. Its firewalls have a large SMB client base. The vendor focuses on simplified firewall administration and management. It offers mature malware detection features, compared to other SMB-focused vendors.

WatchGuard's firewall product line (Firebox) includes physical and virtual appliances. Firewall models are also available on AWS and Microsoft Azure. Its management suite includes three components: the recently released WatchGuard Cloud, WatchGuard Dimension and WatchGuard System Manager (WSM). WatchGuard Dimension and WatchGuard Cloud are primarily focused on monitoring and reporting. WatchGuard Dimension is available as a virtual instance on-premises or deployed into an IaaS instance, whereas WatchGuard Cloud is delivered as a service. WSM is centralized management software for Firebox appliances and is available only installed on a Windows server. WatchGuard's portfolio also includes wireless access points with integrated security features such as DNS protection and MFA.

WatchGuard offers a range of appliances, from a low-end Firebox T15 model (400 Mbps maximum throughput) up to the Firebox M5600 model (60 Gbps maximum throughput).

In 2019, in addition to WatchGuard Cloud, WatchGuard launched a zero-touch SD-WAN offering and DNSWatch, a recursive DNS service aimed at adding additional web protection to its product lines. The vendor launched IntelligentAV, which adds Cylance as AI-based antivirus protection to supplement the existing Bitdefender antivirus engine. The vendor also released the 12.4 version of its Fireware firmware, adding native TLS 1.3 decryption support.

Strengths

- Customer Experience: WatchGuard enjoys higher-than-average scores from Gartner clients surveyed for this research, with high marks for ease of deployment, service and support, as well as for quality of product features.
- Product: WatchGuard is one of the few vendors catering to the midsize enterprise that can decrypt TLS 1.3 natively, offering deeper traffic inspection of encrypted traffic.
- Offering: The addition of DNSWatch allows companies to add recursive DNS-level protection from a single vendor without having to deploy additional hardware or services. The vendor offers dual scan from Cylance

as part of its Intelligent AV subscription and Threat Detection and Response (TDR), its threat correlation platform. It offers an approach to endpoint security that supports multiple third-party endpoint antivirus vendors, allowing for correlation and response with their firewalls from the cloud.

- Product Strategy: WatchGuard continues to be focused on SMBs and provides features specific to the midsize market. New feature additions like SD-WAN and enhancements in VPN are an example of the same.
- Customer Feedback: WatchGuard customers have reported relatively lower performance impacts when enabling multiple features as a strength. As a result, the vendor has high attach rates for many of its additional firewall offerings, including cloud sandboxing, IDPS, URL filtering and threat intelligence.

Cautions

- Marketing Execution: WatchGuard is not frequently cited on customer shortlists for evaluation compared to its competitors and has become much less visible in Gartner client inquiries. WatchGuard is not visible on Asia/Pacific region's clients' firewall shortlists.
- Market Segmentation: WatchGuard has a full line of appliances supporting very small to medium-high throughput needs, as well as support for virtual and IaaS environments. The vendor has a major presence in SMBs, and lacks a presence in enterprise and data center firewall and public IaaS deployment use cases.
- Product: At present, the cloud-based manager offered by WatchGuard primarily offers reporting and visibility features. It also has another management interface, the WatchGuard Dimension offering, with similar limited functionality. WSM, which is available on-premises only, offers mature management capabilities. Customers surveyed for this research expressed concerns about having multiple management consoles.
- Product: WatchGuard provides some lightweight DLP capabilities, but does not support ICAP for integration with enterprise DLP solutions. The product also lacks support for some key features desired by enterprise-grade customers, such as an open API, integration with NAC and SDN support.
- Feature: The WatchGuard firewall IDPS offering uses a single OEM partner for a signature set with no in-house team focused on writing signatures. In addition, it has no ability to add or customize signatures, does not include the ability to fail open, and lacks behavior analysis.
- Offering: WatchGuard does not have a FWaaS offering for extending branch and mobile worker protections, and only offers a partnership with a single CASB vendor instead of owning or integrating with additional third-party CASB vendors.

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

- F5: F5 was part of the Magic Quadrant for Enterprise Firewalls, but was dropped in 2016 because of the vendor's lack of focus in enhancing security features in its product. This year, Gartner has once again included the vendor because of our modified definition of network firewalls and the visibility of AFM (the firewall module) in F5 deals.
- Microsoft: With the increasing adoption of public clouds, public IaaS vendors are introducing native firewall capabilities in their offerings. With Microsoft Azure being one of the most visible IaaS providers in client inquiries this year, Gartner has evaluated the vendor.
- Venustech: The Chinese security player has been added to this research. While Venustech was already part of the Magic Quadrant for UTM, it also meets the inclusion criteria for this year's enterprise firewall Magic Quadrant.

Dropped

Because of the change in inclusion criteria, the following vendor has been dropped as it no longer meets it:

- 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.

Inclusion and Exclusion Criteria

The inclusion criteria represent the specific attributes that Gartner analysts believe are necessary for inclusion in this research. Vendors that provide network firewall functions that meet the market definition and description were considered for this research under the following conditions:

- Gartner analysts have assessed that the company can effectively compete in the network firewall market.
- Gartner has determined that the vendor is a significant player in the market, due to market presence, competitive visibility or technology innovation.
- The company demonstrates a competitive presence in enterprises and sales for enterprise and/or cloud networks.

- The vendor meets the firewall revenue criteria of $30 million in 2018. In the case of IaaS vendors, at least 50% of the installed base should be using the native firewall controls they offer.
- The vendor must demonstrate minimum signs of global presence:
  - Gartner received strong evidence that more than 10% of its customer base is outside its home region.
  - The vendor can provide at least three references outside its home region.
- The provider offers 24/7 direct support, including phone support (in some cases, this is an add-on, rather than being included in the base service).
- Vendors appearing in Gartner client inquiries, their competitive visibility, their client references and their local brand visibility are considered to determine inclusion.

The vendor must provide evidence to support meeting the above inclusion requirements.

Vendors to Watch

Amazon Web Services: AWS is headquartered in Seattle, The native firewall controls in AWS are offered as Security Groups and Network Access Control Lists (ACLs). Its other security offerings include AWS Web Application Firewall, AWS Shield, AWS Firewall Manager, Amazon GuardDuty, Amazon Inspector and Amazon Macie.

VMware: VMware's service-defined firewall is tuned for east-west and internal traffic flows. This distributed software architecture includes a stateful Layer 7 firewall that runs in the hypervisor. It provides visibility and control (including access control policies based on Layer 4 through Layer 7 attributes, AppID and user ID) for virtualized, bare metal, container and public cloud workloads with a single object-based policy framework and manager.

Evaluation Criteria

Ability to Execute

Product or Service: This includes service and customer satisfaction in network firewall deployments. Execution considers factors related to getting products sold, installed, supported and in users' hands. Strong execution means that a company has demonstrated to Gartner analysts that its products are successfully and continually deployed in enterprises and/or cloud environments, 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 and secondary product capabilities (logging, event management, compliance, rule optimization and workflow).

Having a low rate of vulnerabilities in the firewall is important. The logistical capabilities for managing appliance delivery or enabling firewall functions for additional workloads in cloud environments, product service and port density matter. Support is rated on the quality, breadth and value of offerings through the specific lens of enterprise/cloud needs.

Overall Viability: This includes overall financial health, prospects for continuing operations, company history, and demonstrated commitment in the firewall and security markets. Growth of the customer base and revenue derived from sales are also considered. All vendors are required to disclose comparable market data, such as firewall revenue, competitive wins versus key competitors (which are compared with Gartner data on such competition held by our clients), and devices or instances in deployment. The number of firewalls shipped or the market share is not the key measure of execution. Rather, we consider the use of these firewalls to protect the key business systems of enterprise clients and those being considered on competitive shortlists.

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

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

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.

Unacceptable device or software failure rates, vulnerabilities, poor performance, and a product's inability to survive to the end of a typical firewall life span are assessed accordingly. Significant weighting is given to delivering new platforms for scalable performance in order to maintain investment, and to the range of models to support various deployment architectures.

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

availability of user groups, service-level agreements, etc. The greatest factor in these categories is customer satisfaction throughout the sales and product life cycle. Also important is ease of use, overall throughput across different deployment scenarios and how the firewall fares under attack conditions.

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

Table 1: Ability to Execute Evaluation Criteria

Enlarge Table

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 (September 2019)

Completeness of Vision

Market Understanding: This is the ability to understand customer needs and translate them into products and services. Vendors must show a clear vision of their market — listen, understand customer demands, and can shape or enhance market changes with their added vision. 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 network firewall realities and needs is important, and having a viable and progressive roadmap and continuing delivery of innovative new features are weighted very highly. The new capabilities are expected to be integrated to achieve correlation improvement and functional improvement. Gartner makes this assessment subjectively by several means, including interaction with vendors in briefings and feedback from Gartner clients on information they receive concerning roadmaps. Incumbent vendor market performance is reviewed yearly against specific recommendations that have been made to each vendor, and against future trends identified in Gartner research.

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

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

Offering (Product) Strategy: This criterion focuses on a vendor's product roadmap, current features, network firewall feature integration and enhancement, virtualization and performance. Integration with other security components is also weighted, as well as product integration with other IT systems. 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.

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

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

- Performance, which includes low latency, new firewall mechanisms and achieving high throughput and low appliance latency.

- Firewall virtualization and securing virtualized environments. This includes public and private cloud environments.
- Integration with other security products.
- Management interface and clarity of reporting — that is, the more a product mirrors the workflow of the enterprise/cloud 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.

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

Table 2: Completeness of Vision Evaluation Criteria

Enlarge Table

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

Evaluation Criteria	Weighting
Geographic Strategy	Medium

Source: Gartner (September 2019)

Quadrant Descriptions

Leaders

The Leaders quadrant contains vendors that build products that fulfill enterprise requirements around firewalls. 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. These vendors have led the market with innovation. They are quicker to respond to the end-user market. They meet all the firewall deployment use cases. They have a large market share. Vendors in this quadrant lead the market in offering new features that protect customers from emerging threats, meet the requirement of evolving hybrid networks including public and private cloud, 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, support for private and public cloud platforms, 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 firewall 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 lead in innovation, but are limited to one or two firewall deployment use case. They have the right designs and features, but they lack the sales base, strategy or financial means to compete consistently with Leaders and Challengers. Sometimes it is a conscious decision of the vendor to only focus on limited firewall use cases rather than all of them. Most Visionaries' products have good NGFW capabilities, but lack in performance capabilities and support networks. The vendors in this quadrant show strong vision and

market leading innovation in use cases such as automated east-west micro segmentation in public cloud and SDN environments, and innovative threat detection automation capabilities.

Niche Players

Most vendors in the Niche Players quadrant have their prime installation base or are prominent in a particular use case, such as data centers or telcos, distributed enterprises, SMBs, and public IaaS. Some of these vendors that offer a firewall as a module with their other services/components consciously focus on a particular use case. Vendors in this quadrant lack in execution because of a limited client base and do not show innovation. Some of these vendors are confined to particular regions and are not present in other regions.

Context

Starting this year, Gartner has consolidated the Magic Quadrants for UTM and Enterprise Firewalls into a single Magic Quadrant for Network Firewalls, because of the same vendors offering firewalls both for SMBs and enterprises in both the Magic Quadrants. Gartner also observed that the vendors claiming to be focused on enterprise only use cases also kept adding multiple functions to their firewalls. Both the SMB and enterprise requirements continue to overlap, with similar requirements of activating multiple features, better performance, better advanced threat detection techniques and to some extent, consolidation toward a single vendor for other security needs.

Market Overview

In 2018, worldwide market firewall revenue rose by 15.9% in 2018 (compared to 17.5% in 2017 and 15.2% in 2016). While the firewall vendors continue to offer multiple features within their firewalls, the overall subscription cost is now higher. While firewall vendors are offering built-in features within their firewall products, they are also offering services and products that work in conjunction with firewalls, such as CASB and EDR, which are gradually gaining in popularity. Within this, the SMB multifunctional firewalls market grew 10.1% in 2018, with SD-WAN adoption being a strong driver. Gartner also observed interest among clients in various cloud-based outbound filtering services offered by firewall vendors for distributed office and roaming employee use cases.

This year, Gartner firewall inquiries displayed a growing focus on:

- Support for public IaaS platforms and related features
- Cloud service offerings
- SD-WAN
- Advanced threat detection features

Hence, besides the other features mentioned in the evaluation criteria for this Magic Quadrant, Gartner has highly rated the vendors in these additional features and services, considering the keen interest shown by Gartner clients.

This year, we have not seen any new major features introduced by the majority of firewall vendors. Most vendors have introduced feature enhancements for:

- Threat detection
- Centralized management and orchestration
- Support for better TLS version
- SD-WAN
- Performance

With growing adoption of hybrid multicloud environments, more enterprises will rely on their traditional firewall players for network security controls as an additional layer of protection beyond native cloud controls.

The major highlights of the results received from the surveyed firewall reference customers this year are:

- IDPS, application control and URL filtering continue to remain the top three security features being used, in addition to pure firewall functionality. This year, we have also seen VPNs as one of the top security features being used by customers, beyond the top three mentioned.
- As per the survey, this year Gartner also saw the growth in adoption of CASB and EDR offered by firewall vendors. We are also observing small growth in firewall deals with additional products such as CASB and EDR licenses included.
- Eighty-nine percent of surveyed clients agreed that, if given the option, they would prefer the consolidation of advanced features like NTA, EDR, network sandboxing, UEBA and deception features on their firewalls, as opposed to using them as separate, stand-alone platforms. As per the inquiries received by Gartner firewall analysts, we are observing that clients are keen to shortlist the vendors based on the different technologies they offer to deal with advanced threats, beyond IDPS, anti-malware and sandboxing. Gartner has also observed vendors like Palo Alto Networks and Cisco promoting their EDR clients for better correlation of threats between firewalls and endpoints. While we see some adoption on the part of these clients in the midsize segment, enterprise-grade customers still prefer to use stand-alone EDR vendors. Among surveyed clients, 64% citied that they are using a stand-alone EDR product. Firewall vendors are offering ELA deals to clients to sell multiple products and service deals.
- Fifty percent of surveyed clients highlighted that they are using public IaaS today. While 22% of them stated they are using native firewall controls offered by IaaS providers, 19% stated that they use their existing on-premises firewall to protect the cloud, and the remaining 9% highlighted that they use a third-party vendor for the same. Gartner analysts are receiving a growing number of firewall selection inquiries for which the

level of support for IaaS platforms offered by the firewall vendor is an important selection criterion, even if the client is not using public cloud today.

- There has been growth in the firewall usage use case on the public cloud. Despite the majority of firewall vendors offering BYOL and pay-as-you-go models for Tier 1 IaaS providers, they currently lack centralized management capabilities to manage the firewall rules and native IaaS controls. As a result, clients should consider dedicated tools as NSPM, such as Tufin, AlgoSec, FireMon and Skybox Security, to manage their hybrid network security controls.

  Although some firewall vendors do have a dedicated offering for public clouds, they are not yet integrated with a firewall centralized manager. Some sample offerings in this space are:

- Check Point Software Technologies CloudGuard Dome9
- Cisco Stealthwatch Cloud and Cisco Tetration
- Fortinet Security Fabric
- Juniper Networks Junos Space Security Director
- Palo Alto Networks Prisma Cloud

  Gartner clients have reported issues with the deployment of firewalls on the public cloud not being smooth, but are being helped by the technical support team of the vendor. Broadly speaking, most firewall vendors have been slow in offering mature controls and support for public IaaS providers to meet end-user demands:

- Among the total surveyed clients, 23% stated that they use API integration capabilities offered by their firewall vendor with other security products in their network. While Gartner recommends that clients integrate the security solutions for better automation and correlation capabilities, API integration has not been easy for most enterprises. As a result, it is more confined to large enterprises and data center deployments.

  The FWaaS market is still not gaining much traction because of meeting only the branch office egress traffic use case. It is not capable of meeting the following use cases:

- Internal segmentation
- Throughput requirements for larger sites
- Performance issues where internet bandwidth is an issue

  Gartner has seen some traction with the GlobalProtect FWaaS offered by Palo Alto Networks among the vendor's existing client base for the branch office egress traffic use case. A few other independent FWaaS vendors in this space are:

- Cato Networks
- Digital Shield
- OPAQ
- Versa
- Zscaler

The ongoing and escalating geopolitical trade conflicts in the global market are likely to impact the supply chain needed to build and deliver hardware including security appliances such as network firewalls. This will expose many Chinese vendors to this risk. It is highly recommended that clients pay close attention to these global developments and their impact on the supply chain disruptions before finalizing shortlisting them outside China.

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.

By Rajpreet Kaur, Adam Hils, Jeremy D'Hoinne, John Watts