G00263955

Magic Quadrant for Enterprise Network Firewalls

Published: 22 April 2015

Analyst(s): Adam Hils, Greg Young, Jeremy D'Hoinne

"Next-generation" capability has been achieved by the leading products in the network firewall market, and competitors are working to keep the gap from widening. Buyers must consider their operational realities, the burden of switching, and the trade-offs between "best-of-breed" function and costs.

Strategic Planning Assumptions

Virtualized versions of enterprise network safeguards will not exceed 10% of market revenues by year-end 2018, up from less than 5% today.

Less than 40% of enterprise Internet connections today are secured using next-generation firewalls (NGFWs). By year-end 2018, this will rise to at least 85% of the installed base, with 90% of new enterprise-edge purchases being NGFWs as more enterprises realize the benefits of application and user control.

By 2018, 85% of new deals for network sandboxing functionality will be packaged with network firewall and content security platforms.

Fewer than 2% of deployed enterprise firewalls will have Web antivirus actively enabled on them through 2016, although more than 10% of enterprises will have paid for it.

Market Definition/Description

The enterprise network firewall market represented by this Magic Quadrant is composed primarily of purpose-built appliances for securing enterprise corporate networks. Products must be able to support single-enterprise firewall deployments and large and/or complex deployments, including branch offices, multitiered demilitarized zones (DMZs) and, increasingly, the option to include virtual versions, often within the data center. These products are accompanied by highly scalable (and granular) management and reporting consoles, and there is a range of offerings to support the network edge, the data center, branch offices and deployments within virtualized servers.

The companies that serve this market are identifiably focused on enterprises — as demonstrated by the proportion of their sales in the enterprise; as delivered with their support, sales teams and

channels; but also as demonstrated by the features dedicated to solve enterprise requirements and serve enterprise use cases.

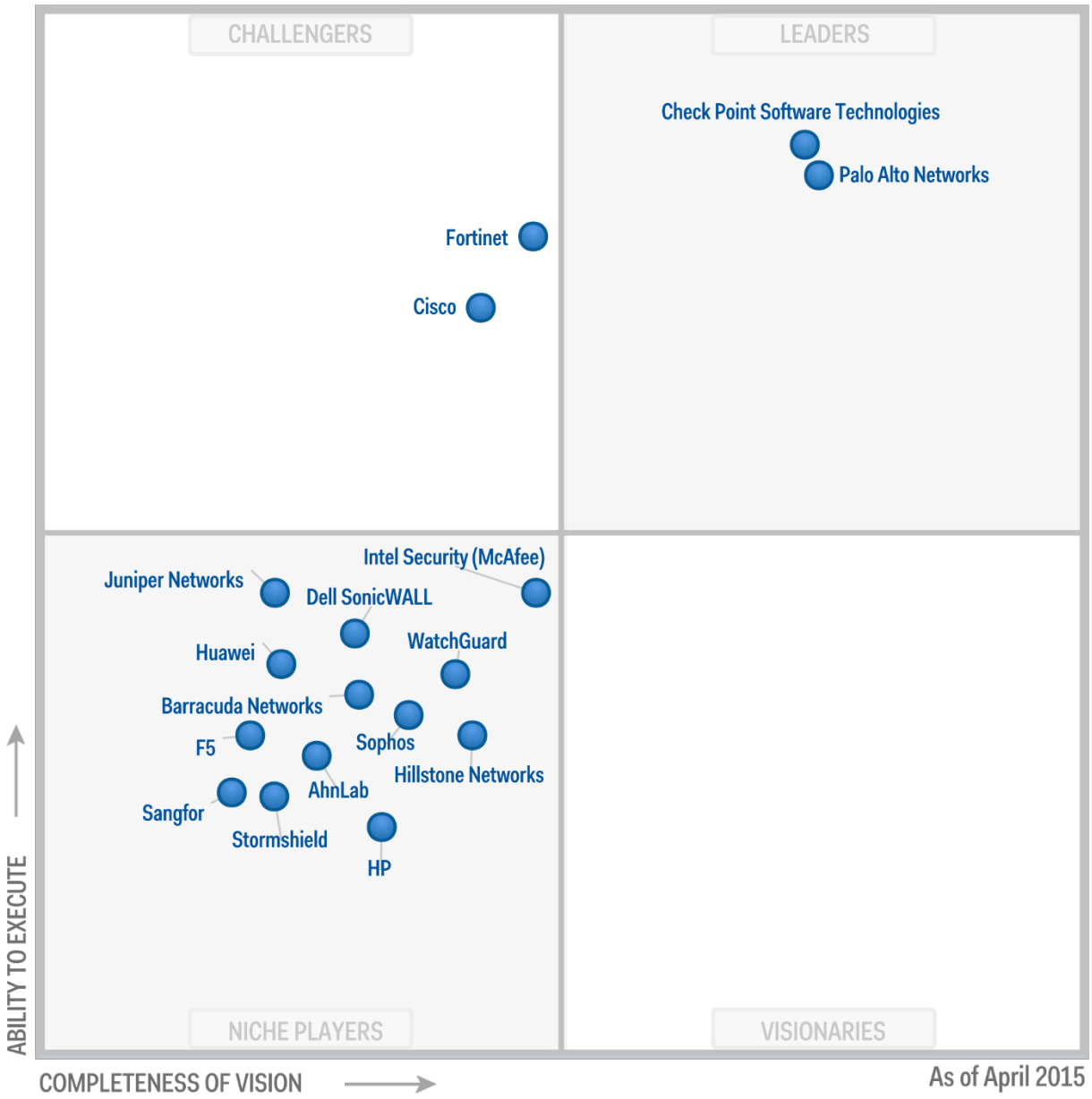
As the firewall market continues to evolve, NGFWs add new features to better enforce policy (application and user control) or detect new threats (intrusion prevention systems [IPSs], sandboxing and threat intelligence feeds). The stand-alone Secure Sockets Layer (SSL) VPN market has largely been absorbed by the firewall market. Eventually, the NGFW will continue to subsume more of the stand-alone network IPS appliance market at the enterprise edge. This is happening now; however, some enterprises will continue to choose to have best-of-breed IPSs embodied in next-generation IPSs (NGIPSs). More recently, enterprises have begun looking to firewall vendors to provide cloud-based malware-detection instances to aid them in their advanced threat efforts, as a cost-effective alternative to stand-alone sandboxing solutions (see "Market Guide for Network Sandboxing").

However, next-generation firewalls will not subsume all network security functions. All-in-one or unified threat management (UTM) approaches are suitable for small or midsize businesses (SMBs), but not for the enterprise (see "Next-Generation Firewalls and Unified Threat Management Are Distinct Products and Markets").

The needs for branch-office firewalls are becoming specialized, and they are diverging from, rather than converging with, UTM products. As part of increasing the effectiveness and efficiency of firewalls, they will need to truly integrate more-granular blocking capability as part of the base product, go beyond port/protocol identification and move toward an integrated service view of traffic, rather than merely performing "sheet metal integration" of point products.

Magic Quadrant

Figure 1. Magic Quadrant for Enterprise Network Firewalls



Source: Gartner (April 2015)

Vendor Strengths and Cautions

AhnLab

South Korea-based AhnLab is a long-established security vendor. Known mostly for antivirus software, AhnLab's network security offerings include firewalls, IPSs and advanced threat solutions. AhnLab began offering a firewall product under the TrusGuard brand in 2007, and now there are 10 models. The firewall is Common-Criteria-certified EAL4, but does not have other third-party evaluations (such as ICSA Labs, NSS Labs or FIPS PUB 140-2).

AhnLab is assessed as a Niche Player for enterprises, because most of its wins are within a specific geography — South Korea — and/or are associated with an expansion of the endpoint security business, not because the vendor competes on best-of-breed enterprise firewall features.

Strengths

- South Korea clients should consider AhnLab for their firewall shortlists, given its significant local market share and support presence.
- The model range is very broad; the engine was designed to minimize distributed denial of service, including features optimized for handling smaller packet sizes.
- AhnLab's endpoint product customers can have the same vendor provide them with their network firewall solution, reducing vendor management challenges.

Cautions

- The TrusGuard firewall is not often seen in enterprise selections in the Gartner client base. AhnLab was not listed by any vendor we surveyed as a significant enterprise competitive threat.
- AhnLab does not offer virtual firewall models, and has not yet integrated its Malware Defense System (MDS) malware detection appliance with its firewall.
- AhnLab does not allow multiple administrators to make rule changes simultaneously, placing it at a disadvantage in large enterprises.

Barracuda Networks

Campbell, California-based Barracuda Networks has been focused primarily on selling a wide range of security storage, and infrastructure appliances and cloud services to midsize businesses and small-enterprise markets at low prices. The Barracuda enterprise firewall offering is the NG Firewall, whereas the Barracuda Firewall series targets SMBs. The NG Firewall has application control and reputation services, while the Barracuda NG Firewall Vx is a virtual version, and there is a Microsoft Azure instance. An advanced threat option has been added with the Barracuda advanced threat detection (ATD) option, repackaged from ATD vendor Lastline, providing a competitive choice versus competing firewalls.

Barracuda is assessed as a Niche Player for enterprises because Barracuda does not effectively sell its enterprise-capable product to enterprises other than in Western and Central Europe and in certain public cloud deployments.

Strengths

- The Barracuda NG Firewall is a good option for customers that already have other Barracuda products or are located in Western or Central Europe.
- The Barracuda management console scores well in selections for simple deployments. The NG Firewall tied for the highest score in a survey to references for IPS function.
- The Barracuda NG Firewall is a strong competitor in situations where price is highly weighted in the selection. The NG Firewall showed a strong correlation for selections in a survey for high availability and clustering.
- Gartner has observed a considerable increase in NG Firewall sales since the previous edition of the Magic Quadrant.

Cautions

- Barracuda customers are primarily SMBs, and the vendor does not yet have well-established enterprise network security channels or support outside of Western and Central Europe.
- Although having differentiated products for enterprises and SMBs is good and reflects their different needs, Barracuda's product naming is confusing for enterprise clients. The Barracuda Firewall series targets SMBs, while the Barracuda NG Firewall series targets enterprises.
- No vendor we surveyed listed Barracuda as a significant enterprise competitive threat. Although we see Barracuda Firewall in SMB deals, Barracuda is not visible on the firewall shortlists of Gartner enterprise customers, except in some regions, notably Germany and Austria. Most interest has come from incumbent customers that have other Barracuda products.

Check Point Software Technologies

Check Point Software Technologies is co-headquartered in Tel Aviv, Israel, and San Carlos, California. Its portfolio includes next-generation firewalls, threat prevention, Web security, endpoint, mobile security, cloud security and distributed denial of service (DDoS) solutions. Check Point's enterprise firewall product line includes 17 appliances and two chassis for hardware blades, scaling up to 400 Gbps. It can also be delivered as a virtual appliance, deployed on VMware, Amazon Web Services (AWS), OpenStack and Microsoft Azure, or delivered as software. Check Point firewall capabilities can be expanded by predefined packages of additional software blades. Customers can supplement Check Point's firewall with an advanced threat offering (Check Point Threat Cloud), and can add additional threat intelligence feeds from third parties (Check Point Intellistore) and integrate Check Point's firewall with its Mobile Security suite to enforce security policy for mobile users (using Check Point Capsule).

Gartner assesses Check Point Software as a Leader for enterprise firewalls because a good score during technical evaluation continually drives new client wins and contributes to retaining a large portion of its existing customer base. Check Point also shows strong execution on its enterprise-focused roadmap to deliver features targeting the various firewall placement use cases for enterprises.

Strengths

- Check Point has one of the largest existing enterprise client bases and continues to appear frequently on final shortlists for enterprise firewall selection. It is able to support these clients globally with a strong channel presence and a significant internal team devoted to firewall feature development.
- Its comprehensive product portfolio allows Check Point to be deployed in a variety of enterprise use cases. The new chassis solutions further expand Check Point's ability to scale to the largest data centers and to adapt to their future growth requirements.
- Check Point firewalls consistently get high scores from clients on security and ease of management in complex environments. It continues to invest in its management suite, with several features in the R80 version intended to improve the auditability and manageability of the security policy, and it has finally merged the network and application components in a unified policy.
- Gartner believes that Check Point's strategy to support VMware NSX, OpenStack and Cisco Application Centric Infrastructure (ACI) is a good signal for clients considering Check Point security solutions when they evaluate software-defined network (SDN) projects.

Cautions

- Price is the most common factor invoked by Gartner clients to introduce competition for Check Point solutions at renewal time or as a reason to favor competition during shortlists. Gartner analysts noticed that hardware platforms submitted in reseller proposals tend to be more tightly sized, and see it as a tactic to control total costs. In a few reported client situations, undersizing was a clear reason for performance issues, and caused unnecessary back-and-forth discussion to get the adequate model.
- In 2014, Gartner observed a higher than usual number of clients reporting stability issues with Check Point solutions, and unexpected long resolution time. This peaked in 2Q14, then plateaued at a lower lever during the second half of the year. Gartner analysts observed that many of these incidents involved clusters of new hardware platforms running the first versions of the unified GAiA OS, with the situation improving as Check Point simplified the number of supported legacy versions.
- Check Point customers are often slow to adopt new software options like its threat emulation software blade. Gartner believes that reasons include insufficient results of marketing operations to support the launch of these options, as well as the fact that Check Point clients are not willing to subscribe to additional software options after the initial sizing, in fear of

performance issues. This increases the time for these new options to become mature, as they benefit from a lower amount of client feedback.

Cisco

San Jose, California-based Cisco has a broad network security product portfolio across firewall/IPS, Web security and email security tiers. The firewall offering is primarily via the Adaptive Security Appliance (ASA) brand that includes an IPS released in 2014. ASA with FirePOWER services is the ASA with the Sourcefire IPS Advanced Malware Protection (AMP) and application visibility and control added in. Cisco's virtual firewalling lines, the ASAv and the VSG, require the presence of the Nexus 1000v virtual switch.

For a while, Cisco will have two primary console offerings. First, the Adaptive Security Device Manager (ASDM) can function as an on-the-device single-instance manager. In addition, the combination of FireSIGHT — which manages the IPS function for ASA with FirePOWER services — and Cisco Security Manager — which manages the ASA firewall — is the alternative for ASA with FirePOWER services. Gartner expects that Cisco will unite the Cisco management console in the short term.

Before the introduction of ASA with FirePOWER services, Gartner saw Cisco winning firewall procurements mostly through sales/channel execution or aggressive discounting for large Cisco networks customers. With the introduction of ASA with FirePOWER services in September 2014, Cisco became more able to compete in the NGFW field

Cisco is assessed as a Challenger for enterprises. Gartner did not see it displacing Leaders based on vision or features, and we rarely saw Cisco release firewall innovations that caused Leaders to react.

Strengths

- The Enterprise License Agreement (ELA) for security software and hardware adds value for Cisco security customers that are undertaking multiyear deployments and wish to maintain a timetable and product flexibility.
- Gartner clients consistently rate the Cisco support network as excellent, and it is the most-often-cited reason for loyalty to Cisco security products. The vendor has strong channels, broad geographic support and wide availability of other security products. Surveyed Cisco firewall clients consistently ranked the availability and presence of other products from Cisco within their networks as the most important factor in their selection of the vendor.
- Cisco offers a wide choice in firewall platforms. The primary offering is the stand-alone firewall ASA, but firewalls are also available via the Firewall Services Module blade for 6500 and 7600 series switches, on Cisco's ASA for virtual data center and cloud environments, and on Cisco's Internetwork Operating System (IOS)-based Integrated Services Router. Gartner views the Platform Exchange Grid (pxGrid) initiative to allow third-party components onto the ASA as the most promising development in the Cisco firewall roadmap.

- The integration of reputation features across Cisco security products is a strength. The rich context provided by the FirePOWER services integration adds to this advantage.
- The inclusion of Sourcefire IPS within ASA has improved the quality of the ASA IPS and application control.

Cautions

- Gartner clients select Cisco firewall products more often when security offerings are added to a Cisco infrastructure, rather than when there is a shortlist with competing firewall appliances. In the survey sent to vendors, Cisco's product was the second most frequently listed as the one vendors claimed to replace the most; however, it was also listed this year as No. 2 in the vendor list of perceived competitive threats.
- Cisco's security console offerings consistently score low versus competitors in assessments conducted by Gartner clients. However, Gartner believes that moving completely to the Sourcefire FireSIGHT will bring improvements.
- Cisco scored lower than most competitors in a Gartner survey of users for overall client satisfaction.
- Cisco ASA has a firewall console integration of a local sandbox-based advanced targeted attack (ATA) cloud instance or appliance through Advanced Malware Protection (AMP); however, Gartner clients choose AMP not for its undifferentiated sandboxing capability, but for other ATA detection strengths. Cisco can improve its ATA-associated sandboxing if it integrates its 2014 acquisition of ThreatGRID.

Dell SonicWALL

Dell, which is headquartered in Round Rock, Texas, sells enterprise network firewalls under the Dell SonicWALL name. The majority of Dell SonicWALL's business had been selling UTM to midsize enterprises, with the SuperMassive line aimed at enterprises, and at competitive price/performance points. Other Dell SonicWALL security products include SSL VPNs, email security gateways, clean wireless offerings, data encryption offerings, identity management offerings, managed security service provider (MSSP) offerings under the SecureWorks brand, and backup/recovery offerings. The company's firewall offerings are in four branded lines: SuperMassive, E-Class Network Security Appliance (NSA), NSA and TZ. Gartner observes a strong correlation between SonicWALL purchases and incumbent Dell customers.

Dell SonicWALL is assessed as a Niche Player for enterprises, in part because it hasn't brought innovative security features to market in a timely manner, and its sales channels and marketing programs haven't effectively reached enterprise buyers.

Strengths

- Dell SonicWALL's broad model range is a good option for distributed enterprises with many remote-office deployments requiring many smaller devices, such as in retail or franchise outlets, or with Type C enterprises (see Note 1). Gartner has observed that the Dell SonicWALL channel

has migrated the core firewall business into more midsize organizations or into organizations that already had a strong Dell SonicWALL relationship.

- For current Dell customers that want to have fewer security vendors, Dell SonicWALL is a good choice because of its wide range of products and available SMB-oriented feature set.
- The SuperMassive line has achieved market traction in high-throughput firewall deployments, such as carriers and service providers, in which firewall throughput, low latency and price per protected megabits-per-second are foremost; in a survey to users, customers ranked throughput and speed as the foremost selection criterion supporting this assessment.

Cautions

- As reported by Gartner clients, Dell SonicWALL is not yet widely viewed as an enterprise strategic security player; rather, it is perceived as a midsize brand associated with the greater Dell brand. Gartner rarely sees Dell SonicWALL in most Type A and Type B enterprise firewall selections; however, this is not a "Caution" for other organizations.
- Dell SecureWorks presents a potential channel conflict for sales to other MSSPs, which can view Dell SonicWALL as part of a competitor. Gartner analysts have observed competitors using this argument to gather channel partners from Dell SonicWALL.
- Dell SonicWALL scored low as a significant enterprise competitive threat by the vendors we surveyed, and scored poorly in a survey to users in regard to false positives for IPS in the firewall.
- The product lines TZ and NSA are aging. Dell SonicWALL prospects should ask to see roadmaps for evidence of future innovation plans.

F5

F5, based in Seattle, is a leading data center application delivery vendor. In addition to the traffic management modules (GTM and LTM) that are the core of F5's Application Delivery Controller (ADC) offering, security modules include Application Security Manager (ASM), its Web application firewall, and the Advanced Firewall Manager (AFM), a network firewall. Its firewall product offering relies on the Big-IP appliances (14 models, from 5 Gbps up to 80 Gbps) and Viprion chassis (four models, up to 640 Gbps) hardware platforms, running the F5 Traffic Management Operating System (TMOS). F5 also offers virtual appliances (F5 VE) and centralized management (Big-IQ) for its Big-IP solutions. Gartner views F5 as successfully using security as a competitive feature in the ADC market rather than being a pure play in the firewall market.

F5 is assessed as a Niche Player for the enterprise firewall market, because its firewall offering is visible only in a limited number of use cases, mostly sold as an add-on of other features to existing F5 customers.

Strengths

- F5's software is optimized for data center and ISP infrastructure protection use cases. It includes IPv6 compatibility, robust routing optimization and SDN features. Gartner also expects F5 to add integration with its firewall and its Silverline DDoS protection offering.
- F5's customer give good scores to its hardware platform for its ability to scale. This includes hardware acceleration and 40 Gbps network interfaces, but also strong SSL optimization capabilities, which are often a weak spot of other firewall platforms.
- F5 dedicates significant efforts to security features and shows its customers a commitment to consider security as a central topic of its roadmap. This is a positive sign for these clients that can add a firewall component to their existing data center deployment at a fraction of the cost required by the acquisition of a dedicated appliance. Gartner expects F5 to compete in data-center-only deals when architecture complexity is low; Gartner has already seen F5 compete well in firewall placements for hosting providers.

Cautions

- F5 does not appear on Gartner client competitive shortlists for enterprise firewall selection, except when customers already own F5 ADC and evaluate F5's upgrade options. F5 is not seen yet as a competitive threat by other firewall vendors evaluated in this market.
- F5 is missing the critical competitive component of a stand-alone Internet-facing firewall to protect users and servers where an ADC is not required, and lacks entry-level appliances required for branches and small headquarters.
- F5 lacks an IPS module and only recently introduced secure Web gateway (SWG) services. The application control feature is limited to what users get from SWG and Web application firewall (WAF) modules, but has yet to be covered by a unified software component. Gartner believes that F5's efforts to cover a broad feature set could hurt its ability to provide sufficient depth for the core features used in enterprise firewall use cases.
- As F5's firewall modules are likely to be used as a data center supplement to a perimeter firewall, F5's integration with only one firewall policy management software (FireMon) limits security buyer options.

Fortinet

Sunnyvale, California-based Fortinet has long focused on using purpose-built hardware to produce enterprise firewall and UTM appliances with a wide range of features at strong price/performance points. It offers a broad security portfolio and has some presence in network infrastructure. The firewall features in Fortinet's enterprise firewall products can now meet most of the needs of firewall-focused large-enterprise buyers.

Fortinet continues to make progress within the Gartner customer base, especially in branch office or retail deployments, but increasingly in more widespread enterprise use cases. In addition, it is very competitive in data center evaluations in which high-performance, low-latency stateful firewalls are

the primary need. Fortinet is a significant threat to competitors in this market because of its hardware expertise, competitive pricing and accelerating revenue growth. It is a viable shortlist contender for most enterprise firewall use cases.

Fortinet is assessed as a Challenger, mostly because we see it displacing competitors on value and performance, but struggling against Leaders in mainstream enterprise selections based on features and vision. Fortinet does not often release features that cause Leaders to react.

Strengths

- Fortinet has a large hardware R&D team and uses it to go to market quickly with higher-performance chipsets. Fortinet continually delivers new functions in the application-specific integrated circuit and operating system, providing extensive pressure on competitors and pleasing the channel.
- Fortinet offers a good price/performance ratio and a wide model range, including bladed appliances for large enterprises and carriers, as well as SMB and branch office solutions.
- In addition to enterprise NGFW deployments, Fortinet is well-suited to deployments in carriers, data centers, service providers and distributed enterprises (for example, retail and franchises).
- Fortinet has a well-articulated strategy regarding virtualization, public cloud and SDN, and has a promising partnership with VMware NSX.

Cautions

- Despite some improvements in 2014, management capability compared with the competition remains the reason most often listed by Gartner clients as the reason why Fortinet was shortlisted but not selected by enterprises. However, where multiple firewalls share the same policy, the Fortinet console is more competitive.
- Although it's reduced the number of appliances in its overall Fortigate product line, Fortinet still supports more versions and models (with often overlapping specifications) than many of its competitors. Gartner believes that the number of appliances and software versions impacts customer support.
- Gartner believes that Fortinet's Feature Select, which provides preset initial configuration options or bundles of features, doesn't effectively communicate the support of the varying use cases of many enterprises or can convey to customers that the NGFW is just a subset of the full UTM suite rather than a "made-for-enterprise" solution.
- While Fortinet's marketing mix became much more enterprise-focused in 2014, previous UTM-oriented marketing has created a lingering brand disadvantage with some enterprise security buyers.

Hillstone Networks

Based in Beijing and Sunnyvale, California, Hillstone Networks is a pure-play firewall vendor. Its firewall portfolio is composed of three product lines, the T-Series (3 models), the E-Series (13 models) and the X-Series (two chassis), with firewall throughput ranging from 1 Gbps to 360 Gbps. Hillstone has added network behavior anomaly detection into its firewall, and offers virtual versions in its virtual Elastic Firewall Architecture (vEFA).

Although it is aggressively moving to increase sales in more regions by expanding its worldwide partner ecosystem, Hillstone is assessed as a Niche Player because it is visible to Gartner only in one region, with a majority of its sales in China.

Strengths

- Hillstone has a strong presence in China, and offers dedicated firewall models for this market. Surveyed customers in China give good scores to direct vendor support.
- Hillstone's recent release of a firewall with behavior-based policy (named Intelligent Next-Generation Firewall) indicates a motivation to bring further innovation to the enterprise firewall market.
- Hillstone integrates with FireMon and AlgoSec policy management software, which can facilitate purchase decision for international companies willing to use a local vendor in the Asia/Pacific region.

Cautions

- Hillstone Networks' firewalls are not yet seen in enterprise selections among the Gartner client base outside of Asia/Pacific. Gartner also observes increasing competition for Hillstone in China from local and regional vendors.
- Surveyed customers indicate that performance degradation when enabling intrusion prevention is higher than the leading vendors evaluated in this market.
- Surveyed customers frequently cite management interface as an area that requires improvement.

HP

Palo Alto, California-headquartered HP has two lines of firewalls. The first is the new TippingPoint Next-Generation Firewall (NGFW) line; the second line is composed of F5000 and F1000, formerly of H3C Technologies in China. These two lines are on distinct code bases, are under different consoles and are supported by different groups within HP. The new TippingPoint NGFW (x86-compatible) is the redesign of the older TippingPoint IPS, which is based on custom application-specific integrated circuits (ASICs). As such, there is no direct hardware upgrade path from the IPS to the NGFW. However, both continue to be sold. There are six models of NGFW, all bearing the "S" prefix. HP is adding an advanced threat sandbox solution via a local appliance based on Trend Micro's Deep Discovery Inspector, which will work with HP's NGFW and IPS via the integration with the HP TippingPoint Security Management System console.

HP is assessed as a Niche Player, mostly because Gartner has not yet seen the new firewall product on shortlists (see "Vendor Rating: HP" for more information) or as fully featured as most Challengers and Leaders. HP has the potential to be a disruptive influence and a market challenger through continued product advancement and utilization of the HP channel.

Strengths

- The proven TippingPoint IPS engine brings a very good quality of IPS to the new NGFW line, which is of interest to incumbent TippingPoint IPS deployments that are looking to replace a firewall, or to those deployments in which IPS needs are more highly ranked than other firewall features. In a Gartner survey, the most mentioned reason for buying the HP firewall was already having other HP security products.
- In a survey of firewall users, HP NGFW scored highest for user satisfaction regarding quality of IPS relating to false negatives and positives.
- There is a good range of models in the new firewall line, meaning new adopters are less likely to have to wait for new models to consider deployments.
- The TippingPoint NGFW and IPS are managed under the HP TippingPoint SMS console, which will already be familiar to HP IPS customers.

Cautions

- Enterprise firewall buyers are often hesitant to invest in something that doesn't have a proven track record in this market. HP has been slow to execute on a roadmap and add new features to its firewall to allow it to compete for general enterprise business by being "RFP ready." However, incumbent HP customers may still find this to be a shortlist option. Gartner clients rarely included HP firewalls in the shortlists we observed.
- As is often the case with new products, the surveyed HP users most often cited that the SMS console needs improvement in managing the new firewalling capabilities, and support was not rated highly.
- Based on conversations with Gartner clients who are also HP Tipping Point's prospects and customers, Gartner views HP as trending toward re-emphasizing stand-alone IPSs over firewalls, as they are challenged in gaining share in the firewall market. HP NGFW prospects and customers should evaluate HP's NGFW release cadence and feature quality, as well as the timely delivery of roadmap capabilities to determine continued investment and priority.

Huawei

Shenzhen, China-based Huawei has been shipping firewall products for more than a decade (for more information, see "Vendor Rating: Huawei"), and off a variety of other network security appliances, including anti-DDoS and IPSs. The range of firewall appliances and models is extensive, especially for higher-throughput options, and for customers that already have Huawei products and wish to expand that business to firewalls. Unified Security Gateway (USG) is the primary enterprise

line, and Eudemon is the line for carriers and service providers. More Huawei firewall revenue is derived from carriers, ISPs and cloud and service providers than from enterprises and SMBs.

Huawei is assessed as a Niche Player for enterprises over the evaluation period, mostly because we see it mostly in a narrow geographic segment, and because we did not see it frequently displacing Leaders or Challengers based on vision or feature.

Strengths

- Gartner assesses Huawei as having a very good overall network security strategy and a large security research team.
- Customers whose networks are based primarily on Huawei infrastructure products can include Huawei firewalls. Users report to Gartner that Huawei appliances perform as expected under load.
- The top end of the Huawei firewall line has a very high throughput and is a good shortlist candidate for carriers. Most deployments Gartner observes are higher-throughput deployments.
- Huawei delivered and improved some application control and other NGFW features in 2014, largely targeted to enterprise customers. Its upcoming roadmap addresses enterprise-oriented features.

Cautions

- Huawei has limited competitive visibility outside the Asia/Pacific region; however, there is some increasing competitive presence and growth in EMEA.
- Interviewed users reported that they would like to see better features in the Web graphical user interface (GUI) console, and consistently asked for better reporting.
- Huawei lags the competition in partnering with firewall policy management vendors, preventing it from fully fulfilling some enterprise compliance and security needs.
- Huawei has taken considerable steps to address concerns about relying on technology developed in China; however, this concern continues to be a security sales challenge in some markets, especially North America.

Intel Security (McAfee)

Intel firewalls are sold under the McAfee brand. McAfee, which is now part of Intel Security (based in Santa Clara, California), sells security controls at the endpoint, server and network layers. Intel (McAfee) network security is best-known for Network Security Platform (NSP), its network IPS product line. Intel Security obtained its network firewall in 2013 from Finland-based Stonesoft, whose product is now called the McAfee Next Generation Firewall (NGFW). The McAfee NGFW has a good range of models (scaling up to 120 Gbps), including a virtualized version, and has performed well in third-party testing. (Intel Security has an advanced threat offering [ATD] that becomes more effective the more Intel McAfee safeguards are in place.)

Gartner believes that, in the near future, Intel Security will have a single hardware platform supporting the McAfee NGFW and NSP, which is the IPS product.

Intel Security is assessed as a Niche Player for enterprises because it primarily sells alongside other Intel and McAfee security products rather than beating Leaders in shortlists.

Strengths

- The breadth of the Intel Security threat intelligence and reputation feeds is a positive quality element and leverages the Intel Security footprint on endpoints, secure Web gateways, email security gateways and IPSs.
- The McAfee NGFW firewall line has long been a leader in high-availability technology, and it has very reliable clustering and active/active configuration. It focused early on anti-evasion technology, and protected customers well as attacks evolved to include firewall and deep inspection evasiveness.
- The visibility of ePolicy Orchestrator (ePO) host information within the firewall reporting and console tools is of interest to current Intel Security ePO customers.
- In a Gartner survey of clients, the McAfee NGFW scored very high in overall client satisfaction.

Cautions

- Gartner believes that having the McAfee network security unit within a primarily host-based security company — which is itself within a large endpoint-focused chip manufacturer — remains a significant challenge. Intel Security was not listed by any vendor we surveyed as a significant enterprise competitive threat, and Intel is not established as being a strong brand in network security.
- Intel Security currently has two different network IPS engines across the McAfee NGFW and NSP (IPS) products. Rationalizing and centrally administering these from one management console will present challenges.
- Intel Security is rarely seen on Gartner client network firewall shortlists, and Gartner estimates that the market share is small at less than 5%.

Juniper Networks

The firewall offerings of Sunnyvale, California-based Juniper Networks are in multiple model lines: SRX SSG, NS, ISG and the virtualized version of SRX (vSRX). The Juniper SRX Security Service Gateway offers routing as a basic firewall element, and runs the same Junos operating system as other Juniper infrastructure components. Gartner considers routing in the firewall as being of interest to a limited segment of customers. Juniper has AppSecure for application control and visibility integrated IPS and threat intelligence feeds. Juniper's Junos Space Security Design is the current security management platform.

Juniper is assessed as a Niche Player for enterprises, mostly because we see it selected in concert with other Juniper offerings, rather than displacing competitors based on its vision or features, and we see it being replaced in enterprise environments more often than we see it selected. Juniper is, however, shortlisted and/or selected in mobile service provider deployments and large-enterprise data center deployments, primarily because of price and high throughput on its largest appliances.

Strengths

- Customers whose networks are already standardized on Juniper's Junos-based infrastructure products can benefit from the Space Security Design console because it is part of the Junos Space network management platform. Interviewed users often selected the firewalls, with throughput weighted highly in their selection.
- Good options exist for high-throughput, purpose-built appliances, especially in the higher-end SRX models, because Gartner sees Juniper mostly deployed in large data centers.
- Juniper has a strong range of branch-office firewalls complementing the enterprise products. These branch-office firewalls include WAN and cellular backup technologies.
- Juniper SRX is a good shortlist candidate in deployments for service providers or hosters where stateful firewall throughput is valued foremost and price is weighted highly.
- Juniper offers a threat intelligence platform supporting third-party feeds and enabling deployment to enforcement points. This capability will appeal to enterprises that use multiple third-party threat intelligence feeds.

Cautions

- Gartner does not assess Juniper as currently having a compelling or differentiated security vision, or one that is well-known to non-Juniper customers. In 2014, Juniper released its first NGFW feature set, well behind most of the firewall vendors evaluated in this research.
- Some Gartner clients have cited a need for support and platform stability improvements. Users that Gartner surveyed report hardware failures over the past 12 months.
- Gartner believes that most enterprises want an operating system in their security products that differs from the one in infrastructure components.
- Juniper has continued losing security market share in the past year, and has experienced declining year-over-year revenue in a growing market. The company must address fundamental sales and marketing challenges and demonstrate that it can win back customers and market share with its newer capabilities.

Palo Alto Networks

Palo Alto Networks is a California-based pure-play network security company that has been shipping enterprise firewalls since 2007. Palo Alto Networks is known mostly for its innovations in application control and for improving integrated IPS in firewalls. The firewall product line includes 18 models, with a maximum throughput of 120 Gbps for the PA-7050, released in 2014. With the

acquisition of Cyvera (rebranded as Traps), Palo Alto Networks now offers a second endpoint product, in addition to the existing GlobalProtect. Palo Alto's cloud-based network sandbox service, WildFire, saw high attach rates for new and existing customers in 2014. Palo Alto's work with VMware NSX has provided customers another option for placing Palo Alto products in virtualized data centers.

Palo Alto Networks is assessed as a Leader, mostly because of its NGFW focus, and because of its consistent visibility in Gartner shortlists for advanced firewalls use cases, frequently beating competition on feature quality.

Strengths

- Gartner clients consistently rate the Palo Alto Networks App-ID and IPS higher than competitors' offerings for ease of use and quality.
- The firewall and IPS are closely integrated, with App-ID implemented within the firewall and throughout the inspection stream. This "single pass" is assessed as a design advantage by Gartner clients, as opposed to the unnecessary inspection that can occur in competing products that process traffic in serial order.
- Palo Alto Networks was consistently on most NGFW competitive shortlists seen by Gartner, and in the survey to vendors, it was most mentioned as the strongest competitor with which these vendors compete.
- The roadmap focus on VMware NSX displays strong leadership toward solving clients' future problems. Palo Alto shifted focus correctly to east-west segmentation rather than whole data center firewall virtualization.
- The WildFire advanced threat appliance and cloud service are popular add-ons with new and incumbent Palo Alto Networks firewall customers, giving them an option versus third-party advanced threat appliance solutions.

Cautions

- Gartner clients report Palo Alto Networks' direct sales and resellers being overly optimistic about the performance impact of turning on antivirus (that is, Web anti-malware), and conflating antivirus with IPS and/or other features, or claiming a 0% performance impact when enabling the antivirus (AV) function, which is not credible with customers. Gartner believes that this approach has eroded customer trust in the Palo Alto Networks brand.
- Gartner does not see Palo Alto reproducing its firewall success in its attempt to enter the endpoint market. Gartner considers Palo Alto's entry into the endpoint market as a high risk move that could dilute company attention into a nonadjacent market and could alienate the network security buying center. The endpoint should be addressed through a third-party ecosystem or pushed stronger as an independent effort.
- The company must develop a better third-party product support ecosystem.

- Like other vendors with leading products, Palo Alto Networks is challenged to win selections in which price is weighted more than security features, as in Type C enterprises (see Note 1). It also does not offer the smaller appliances that competitors position in distributed enterprise deals.
- The clients we interviewed would like to see better log handling at scale. Also, the client complaints we receive regarding Palo Alto Networks usually relate to management console issues at scale, or anecdotes of channel partner shortcomings.

Sangfor

Headquartered in Shenzhen, China, and founded in 2000, Sangfor provides WAN optimization, access management and network security solutions, including firewall, SSL VPN and Internet access management. Sangfor started shipping its enterprise firewall product line (Next-Generation Application Firewall) in 2011. It now features 16 models, for a firewall throughput of up to 80 Gbps. Sangfor does not offer a virtual appliance.

Sangfor is evaluated as a Niche Player for enterprise firewall because it serves a narrowed segment of the market and operates mostly in China.

Strengths

- Sangfor clients like the ease of installation, reporting on security and high performance. They also cite competitive price as a reason for selecting the solution.
- Cloud-based sandboxing and active vulnerability scanning are available on Sangfor's firewall at no additional charge.

Cautions

- Gartner does not see Sangfor firewalls being shortlisted outside of China. Internationalization of the Sangfor firewall product line is still an ongoing process. Potential customers outside of China should first verify the availability of vendor support and product documentation for their use case, and request references for organizations in the same region.
- Surveyed customers showed a majority of upper-midsize/small-enterprise use cases, with a limited number of firewalls for a single customer.
- Sangfor's enterprise firewall is new compared with most of its competitors, and several features are still unproven, with a quickly growing number of deployments but a limited existence.

Sophos

Sophos is a security company headquartered in Oxford, U.K., that is primarily known for its endpoint security solution. Its enterprise firewall portfolio mainly consists of two product lines, the SG series (14 models, from 1.5 Gbps to 60 Gbps) and the NG product line, resulting from the acquisition of India-based Cyberoam (19 models, from 400 Mbps to 160 Gbps). The two remote Ethernet device (RED) models allow remote VPN connections for small branches. Sophos firewalls

are also available in virtual appliance format and can run on AWS. Sophos also sells secure Web gateways and secure email gateways in addition to its endpoint security and mobile security solutions.

Sophos' Niche Player position in this Magic Quadrant reflects its focus on upper-midmarket and smaller-enterprise needs, which is shown, too, in the limited visibility for Sophos firewalls on data center and larger enterprises' shortlists.

Strengths

- A growing number of Sophos endpoint customers shortlist Sophos as a potential firewall, citing ease of use, potential product synergies and simplified procurement as the main reasons for selecting the vendor.
- The Sophos Cloud management offering combines mobile, endpoint and network management, and appeals to vastly distributed enterprises and organizations with a large mobile workforce.
- The Sophos roadmap shows a good understanding of the needs of midsize and smaller enterprises clients, their target market, and how they plan to address overlaps between their two firewall product lines, increase cross-synergies across their solutions, and fill the remaining gaps in their security portfolio.
- Sophos leads the market in AWS features and market penetration, and is a good choice for AWS-only placements.

Cautions

- Sophos' visibility on Gartner enterprise client shortlists remains low, and is almost exclusively from existing Sophos customers.
- Sophos still maintains two firewall product lines, and will be delivering its unified next-generation product in mid-2015. Customers must ensure their Sophos appliances can receive the firmware upgrade in order to take advantage of the new platform.
- Gartner believes that midmarket and large enterprise have different needs and expectations for centralized management and reporting solutions. Sophos' current management and reporting offerings are oriented toward UTM use and distributed organizations, and get lower scores in competitive evaluations where complex policy and stringent workflow requirements are highly weighted; however, Sophos is a good choice for upper-midmarket customers, smaller enterprises and Type C enterprises.

Stormshield

Stormshield (formerly Arkoon+Netasq), headquartered in France, has been a pure-play network security vendor for more than 15 years, selling UTM systems and enterprise firewalls with integrated IPSs and vulnerability management. In 2012, Airbus Defence and Space — CyberSecurity (formerly Cassidian CyberSecurity, a subsidiary of EADS Group) acquired Netasq. In April 2013, it acquired

Arkoon, another French security company with firewalls and endpoint protection platforms. The two groups have united under the Stormshield brand, and have introduced the Stormshield Network Security line. These products are composed of nine appliances, ranging from 400 Mbps to 80 Gbps.

Virtual versions are also available with the V series, and at the AWS Marketplace.

Stormshield is assessed as a Niche Player for enterprises, mostly because it best serves midsize businesses and government agencies in Western and Central Europe.

Strengths

- Stormshield is a European vendor and benefits from local certifications, such as the "EU Restricted" or specific assessment from the French government, which is of interest to EU governments and agencies looking for simpler procurement or a local provider. Its ownership (Airbus) adds credibility to French government and defense customers.
- Stormshield has quickly executed on a plan to produce a new product line, giving a clear choice to prospects and existing clients from the former companies when considering a firewall refresh.
- Stormshield has a wide range of virtual appliances and AWS-based instances, making it a good candidate to protect hybrid networks.
- Customers cite IPS quality as a main reason they select Stormshield as their network firewall.

Cautions

- The majority of Stormshield's penetration, visibility and channel is focused on EMEA, especially France. The vendor has not been part of NGFW selections that Gartner has seen.
- The burden of maintaining software support for 36 models may stress Stormshield's R&D resources and its ability to execute on its technology roadmaps.
- Stormshield lacks the ability to apply quality of service (QoS) rules based on application detection.

WatchGuard

WatchGuard is a Seattle-based network security company that has primarily seen success in selling UTM products to midsize enterprises. Its XTM series of products spans performance and feature ranges demanded by large enterprises; however, WatchGuard's branding, channel support and management capabilities tend to be more oriented toward SMBs. WatchGuard also has products that include SSL VPN, email and Web security product lines.

The XTM-branded firewall models fall into two categories: The XTM 2 Series and XTM 5 Series are UTM, while the XTM 8 Series and the XTM 1520 and above are targeted at the enterprise. Since WatchGuard's introduction of the "NGFW Bundle" option for appliances in 2011 and the 2014 release of APT Blocker, WatchGuard's cloud-based malware detection offering based on Lastline

technology, the company has solutions that better suit prospective enterprise buyers than the UTM-only approach, though we have not seen much enterprise traction yet.

WatchGuard is assessed as a Niche Player for enterprises, mostly because it serves SMBs and distributed enterprises. However, we do not often see it displacing Leaders for the edge firewall use case based on features. Moreover, it is not present on data center shortlists.

Strengths

- WatchGuard's strong price/performance points have enabled it to win price-sensitive competitions across retail, branch office, remote office and Type C distributed enterprise deployments.
- WatchGuard continues to invest in enterprise use cases, with enhanced IPv6 and better traffic management released in 2014, along with APT Blocker.
- Users report high satisfaction with the WatchGuard management console. Enterprise models are correctly targeted at NGFWs rather than UTM functionality.
- The cloud-based reporting solution WatchGuard Dimension, with its executive dashboard and traffic heat maps, has proven to be a good addition to the set of features that is targeting areas where many firewalls will be deployed, such as in franchises or retail stores, or via an MSSP. The interactive heat map view (FireWatch) is useful to quickly identify network issues created by a specific user or application.

Cautions

- Gartner rarely sees WatchGuard in most Type A and Type B enterprise firewall selections. Enterprise-class channels and support will need to be expanded if WatchGuard wishes to compete in a broader segment of enterprises. For example, WatchGuard does not have the option for large enterprises to deploy a WatchGuard resident engineer, a requirement for some enterprise deployments.
- WatchGuard scored low as a significant enterprise competitive threat by the vendors we surveyed, and it has low visibility in Gartner's customer base.
- WatchGuard lags behind the Leaders in articulating a comprehensive data center strategy, and in including SDN in its roadmap.

Vendors Added and Dropped

We review and adjust our inclusion criteria for Magic Quadrants and MarketScopes as markets change. As a result of these adjustments, the mix of vendors in any Magic Quadrant or MarketScope may change over time. A vendor's appearance in a Magic Quadrant or MarketScope 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

Sangfor was added to the Magic Quadrant. Arkoon+Netasq was renamed Stormshield, which now appears in the Magic Quadrant.

Dropped

No vendors were dropped.

Inclusion and Exclusion Criteria

Inclusion Criteria

Network firewall companies that meet the market definition and description were considered for this research under the following conditions:

- Gartner analysts have assessed that the company has the ability to effectively compete in the enterprise firewall market.
- The company regularly appears on shortlists for selection and purchases.
- The company demonstrates a competitive presence in enterprises and sales.
- Gartner analysts consider that aspects of the company's product execution and vision merit inclusion.
- The vendor has achieved enterprise firewall product sales (not including maintenance) in the past calendar year of more than $10 million, and within a customer segment that is visible to Gartner.

Exclusion Criteria

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

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

- The company primarily has a network IPS with a non-enterprise-class firewall.

The company has personal firewalls, host-based firewalls, host-based IPSs and WAFs (see Note 2) — all of which are distinctly separate markets.

Evaluation Criteria

Ability to Execute

- **Product or service:** This includes service and customer satisfaction in enterprise firewall deployments. Execution considers factors related to getting products sold, installed, supported and in users' hands. Strong execution means that a company has demonstrated to Gartner analysts that products are successfully and continually deployed in enterprises, and that the company wins a large percentage in competition with other vendors. Companies that execute strongly generate pervasive awareness and loyalty among Gartner clients, and also generate a steady stream of inquiries to Gartner analysts. Execution is not primarily about company size or market share, although those factors can affect a company's Ability to Execute. Sales are a factor; however, winning in competitive environments through innovation and quality of product and service is more important than revenue. Key features are weighted heavily, such as foundation firewall functions, console quality, low latency, range of models, secondary product capabilities (logging, event management, compliance, rule optimization and workflow), and the ability to support complex deployments and modern DMZs. Having a low rate of vulnerabilities in the firewall is important. The logistical capabilities for managing appliance delivery, product service and port density matter. Support is rated on the quality, breadth and value of offerings through the specific lens of enterprise needs.
- **Overall viability:** This includes overall financial health, prospects for continuing operations, company history, and demonstrated commitment in the firewall and security markets. Growth of the customer base and revenue derived from sales are also considered. All vendors were required to disclose comparable market data, such as firewall revenue, competitive wins versus key competitors (which are compared with Gartner data on such competitions held by our clients) and devices in deployment. The number of firewalls shipped or the market share is not the key measure of execution. Rather, we consider the use of these firewalls to protect the key business systems of enterprise clients, and those being considered on competitive shortlists.
- **Sales execution/pricing:** We evaluate the company's pricing, deal size, installed base, and use by enterprises, carriers and MSSPs. This includes the strength of the vendor's sales and distribution operations. Presales and postsales support is evaluated. Pricing is compared in terms of a typical enterprise-class deployment, and includes the cost of all hardware, support, maintenance and installation. Low pricing will not guarantee high execution or client interest. Buyers want good results more than they want bargains, and think in terms of value over sheer low cost. Cost of ownership over a typical firewall life cycle (three to five years) is assessed, as is the pricing model for conducting a refresh while staying with the same product and replacing a competing product without intolerable costs or interruptions. The robustness of the enterprise channel and third-party ecosystem is important.

- **Market responsiveness/record:** This evaluates the vendor's ability to respond to changes in the threat environment, and to present solutions that meet customer protection needs rather than packaging up fear, uncertainty and doubt. This criterion also considers the provider's history of responsiveness to changes in demand for new features and form factors in the firewall market, and how enterprises deploy network security.
- **Marketing execution:** Competitive visibility is a key factor; it includes which vendors are most commonly considered to have top competitive solutions during the RFP and selection process, and which are considered top threats by the others. In addition to buyer and analyst feedback, this ranking looks at which vendors consider the others to be direct competitive threats, such as by driving the market on innovative features co-packaged within the firewall, or by offering innovative pricing or support offerings. An NGFW capability is heavily weighted, as are enterprise-class capabilities, such as multidevice management, virtualization, adaptability of configuration and support for enterprise environments. Unacceptable device failure rates, vulnerabilities, poor performance, and a product's inability to survive to the end of a typical firewall life span are assessed accordingly. Significant weighting is given to delivering new platforms for scalable performance in order to maintain investment, and to the range of models to support various deployment architectures.
- **Customer experience and operations:** These include management experience and track record, as well as the depth of staff experience — specifically in the security marketplace. The greatest factor in these categories is customer satisfaction throughout the sales and product life cycles. Low latency, throughput of the IPS capability and how the firewall fared under attack conditions are also important. Succeeding in complex networks with little intervention (for example, one-off patches) is highly considered.

Table 1. Ability to Execute Evaluation Criteria

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

Source: Gartner (April 2015)

Completeness of Vision

- **Market understanding and marketing strategy:** This includes providing a track record of delivering on innovation that precedes customer demand, rather than an "us, too" roadmap. We also evaluate the vendor's overall understanding of and commitment to the security and network security markets. Gartner makes this assessment subjectively by several means, including interaction with vendors in briefings and feedback from Gartner customers on information they receive concerning roadmaps. Incumbent vendor market performance is reviewed year by year against specific recommendations that have been made to each vendor, and against future trends identified in Gartner research. Vendors cannot merely state aggressive future goals; they must put plans in place, show that they are following their plans, and modify those plans as they forecast how market directions will change. Understanding and delivering on enterprise firewall realities and needs are important, and having a viable and progressive roadmap and continuing delivery of NGFW features is weighted very highly. The NGFW capabilities are expected to be integrated to achieve correlation improvement and functional improvement.
- **Sales strategy:** This includes preproduct and postproduct support, value for pricing, and providing clear explanations and recommendations for detecting events, including zero-day events. Building loyalty through credibility with a full-time enterprise firewall staff demonstrates the ability to assess the next generation of requirements. Vendors need to address the network security buying center correctly, and they must do so in a technically direct manner, rather than selling just fear or next-generation hype. Channel and third-party security product ecosystem strategies matter insofar as they are focused on enterprises.
- **Offering (product) strategy:** This criterion focuses on a vendor's product roadmap, current features, NGFW integration and enhancement, virtualization and performance. Credible, independent third-party certifications include the Common Criteria for Information Technology Security Evaluation. Integration with other security components is also weighted, as well as product integration with other IT systems. We also evaluate how the vendor understands and serves the enterprise branch office and data center. Innovation, such as introducing practical new forms of intelligence to which the firewall can apply policy, is highly rated. An articulated, viable strategy for addressing the challenges in SDN deployments is important.
- **Business model:** This includes the process and success rate for developing new features and innovation; it also includes R&D spending.
- **Vertical/industry strategy and geographic strategy:** These include the ability and commitment to service geographies and vertical markets, such as complex enterprise multinational deployments, MSSPs, carriers or governments.
- **Innovation:** This includes R&D and quality differentiators, such as:
  - Performance, which includes low latency, new firewall mechanisms, and achieving high IPS throughput and low appliance latency.
  - Firewall virtualization and securing virtualized environments.

- Integration with other security products.
- Management interface and clarity of reporting — that is, the more a product mirrors the workflow of the enterprise operation scenario, the better the vision.
- "Giving back time" to firewall administrators by innovating to make complex tasks easier, rather than adding more alerts and complexity.

Products that are not intuitive in deployment, or operations that are difficult to configure or have limited reporting, are scored accordingly. Solving customer problems is a key element of this criterion. Reducing the rule base, offering interproduct support and leading competitors on features are foremost.

Table 2. Completeness of Vision Evaluation Criteria

Evaluation Criteria	Weighting
Market Understanding	High
Marketing Strategy	Medium
Sales Strategy	Medium
Offering (Product) Strategy	High
Business Model	Medium
Vertical/Industry Strategy	Medium
Innovation	High
Geographic Strategy	Low

Source: Gartner (April 2015)

Quadrant Descriptions

Leaders

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

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 are slow to work toward a strong NGFW capability — or they have other security products that are successful in the enterprise and are counting on the relationship, rather than the product, to win deals. Challengers' products are often well-priced, and, because of their strength in execution, these vendors can offer economical security product bundles that others cannot. Many Challengers hold themselves back from becoming Leaders because they are obligated to place security or firewall products at a lower priority in their overall product sets. Firewall market Challengers will often have significant market share, but trail smaller market share Leaders in the release of features.

Visionaries

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

Niche Players

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

Context

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

Market Overview

As the first line of defense between external threats and enterprise networks, firewalls need to continually evolve to maintain effectiveness, responding to changes in threats as well as changes in enterprise network speed and complexity. The firewall market is highly penetrated in the larger markets (North America, Western Europe and mature Asia/Pacific), which means that, to protect their installed base, incumbents must add improved capabilities and increase performance, or face either replacement by innovative market entrants or commoditization by low-cost providers. Firewall policy management (FPM) products are increasingly being used to manage complexity (see Note 3).

Next-Generation Firewalls

One key area of firewall evolution that has been supported is what Gartner (in 2009) called "NGFW features" — namely, integrated deep packet inspection intrusion detection, application identification and granular control. The key differentiators in these areas are IPS effectiveness, as demonstrated through third-party testing under realistic threat and network load conditions, and fine-grained policy enforcement in approximately the top 40 business applications. Identity-based policy enforcement, or the ability to enforce policy on thousands of applications, has been highly touted but used infrequently.

Because it is highly penetrated, the firewall market is driven by refresh cycles. We have seen some common patterns in the firewall market as enterprises with three- to five-year-old firewalls and IPSs evaluate replacement:

- Enterprises not currently using any IPSs migrate to NGFWs with minimal use of advanced features.
- Enterprises with firewalls and stand-alone IPSs that are employed primarily in detection mode (that is, using minimal signature sets) migrate to NGFWs using the built-in IPS capabilities.
- Enterprises with firewalls and stand-alone IPSs that are used for active prevention, with large signature sets and some custom signatures, migrate to NGFWs for the firewall with application control and user context, but continue using stand-alone IPSs.
- High-security environments upgrade to NGFWs for the firewall, and upgrade IPSs to NGIPSs (see "Defining Next-Generation Network Intrusion Prevention").
- Organizations are looking to extend their on-premises firewall vendor into infrastructure as a service (IaaS) cloud providers.

UTM Can't Compete With NGFWs in Enterprises

Historically, UTM vendors targeted SMB clients. However, in the past few years, the large UTM vendors have tried to expand beyond their traditional use case. They now try to sell UTM to enterprise clients that score price competitiveness higher than security. Gartner sees some limited success for Type C enterprises, but it is restricted to two use cases: distributed Type C enterprises (mostly in the retail industry), and stateful firewall for network segmentation at low cost. However, the UTM approach fails to convince Type A and Type B enterprises that require NGFW capabilities

and do not consolidate Web antivirus on the Internet-facing firewall (see "Next-Generation Firewalls and Unified Threat Management Are Distinct Products and Markets").

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

Virtualized Firewalls: Hype Outruns Demand

As data center virtualization has continued, demand for virtual appliance support has grown. Performance and the ability to manage firewall policy through a single integrated management console for stand-alone appliances or virtual appliances are key differentiators. Gartner has not seen the firewall features of virtualization platforms (such as those offered with VMware) as a major competitor to mainstream firewall vendors because the need for separation of duties drives clients to doubt the infrastructure's ability to protect itself. Gartner covers virtual-only firewall vendors such as vArmour and Illumio, but has not seen significant adoption. Early VMware work with Palo Alto Networks, and now Check Point and Fortinet, has created some buzz for virtualizing data centers and networks and east-west segmentation, but few customers have adopted these, though adoption is growing quickly. As other virtualization platforms such as Xen and Hyper-V gain traction, managing heterogeneous virtualized firewalls from existing physical firewall vendors, virtualization platform vendors and virtual-only firewalls will present a challenge. Performance remains a barrier to wider deployment: Almost all network firewalls today are delivered on purpose-built appliances because of the poorer performance of running firewalls on general-purpose servers. Almost all operating systems within firewall appliances are uniquely hardened, subject to stringent third-party security evaluations. Security-minded enterprises are also rightly skeptical of running firewalls within a hypervisor that is between the threat and the firewall.

Gartner market data indicates that, in 2014, the number of virtual versions of firewalls sold remained flat at less than 2%. Among the 95 reference customers surveyed for this Magic Quadrant, 0% listed "virtual version available" as a top three reason they selected their current vendor, whereas 53% selected "throughput/speed" as a top three reason, and approximately 30% of respondents selected "price" (34%), "management console/reporting" (32%), "IPS" (32%), "application control" (29%), and "high availability/clustering" (27%).

No dynamic shift toward virtual appliances will occur until a fundamental change to the current network security virtualization market is made and demand drives vendor innovation.

The Firewall Market Slows Down on Acquisitions, but Remains Dynamic

Acquisitions in the firewall space slowed down in 2014 from 2013's breakneck pace, but growth remained robust.

During the evaluation period, the firewall market grew 9.5% to $9.5 billion. For 2015, Gartner estimates the firewall market will grow approximately 10% to reach $10.5 billion in 2015. We also forecast that this market will reach a compound annual growth rate of 10% through 2017, and will

be elevated by the addition of firewall add-ons such as IPSs and advanced threat defenses. Gartner believes that the firewall market is "at capacity": Although the growth rate is just around 10%, this is the largest security product market (fast approaching $10 billion), and incremental market growth is significant. Firewall refreshes remain constant at a five-year average, so even if great new products emerge, incumbent firewalls are rarely refreshed before they reach maturity. This refresh dynamic results in the market being linear, rather than having macrorefresh cycles or "bumps" of refreshes, as in other markets.

Have Some Advanced Threat Detection With That Firewall

Advanced threat detection using a network sandbox, pioneered by FireEye, has become a rapidly growing market. As advanced threat defense/detection further penetrates the mainstream market, firewall vendors have introduced solutions over the past three years. These firewall-attached sandboxes are delivered mostly as cloud-based sandboxes priced as subscription-based services. Most of the firewall vendors evaluated here either deliver a network sandbox today, or have it on their short-term roadmaps. Some of these are built by the firewall vendors, others are delivered through third-party partnerships.

Thus far, we've seen firewall-connected sandboxes appeal mostly to budget-constrained Type B enterprises that would rather maintain single-console control over their firewall than deploy a separate platform. As the desire to defend against the advanced threat more fully permeates the mainstream market, we expect that customers will increasingly turn to their firewall vendors for their network sandboxing needs (see "Market Guide for Network Sandboxing").

Confusing Use of "Application" and "Firewall" in Three Distinct Products

Overlapping terminology and unclear marketing can lead to confusion among the three distinct issues of application control, WAFs and firewalls on application delivery controllers (ADCs). The firewall application control approaches used by most NGFW vendors (such as Check Point, Dell SonicWALL, Fortinet and Palo Alto Networks) are mostly about controlling access to external applications, such as Facebook and peer-to-peer (P2P) file sharing.

WAFs are different: They are placed primarily in front of Web servers in the data centers. Pure-play WAF companies (such as Imperva) or data center infrastructure vendors that provide WAF technology within their ADCs are concerned with protecting custom internal Web applications.

While some ADC vendors (such as F5) are now offering network firewalling within their ADCs as well, Gartner does not see NGFW and WAF technologies converging because they are for different tasks at different placements. Most traffic to enterprise Web servers remains encrypted until it reaches the ADC, meaning the owners of firewalls and IPSs face the difficult decision of whether to engage SSL inspection, which involves a termination and re-encryption of these sessions (see "Security Leaders Must Address Threats From Rising SSL Traffic" and "Web Application Firewalls Are Worth the Investment for Enterprises").

As Gartner advises clients, most enterprises have a single brand of network firewall for all placements, including Internet-facing, virtualized, data center and branch (see "One Brand of Firewall Is a Best Practice for Most Enterprises"). These data center firewalls will be challenged to

gain any noteworthy share until they can provide competitive firewalling for all enterprise placements. They can, however, serve a specialized niche of placements, such as in cases where the data center is a separate business with its own firewall operations staff.

Acronym Key and Glossary Terms

ADC	application delivery controller
AFM	Advanced Firewall Manager
ASA	Adaptive Security Appliance
ATA	advanced targeted attack
ATD	advanced threat detection
AWS	Amazon Web Services
DDoS	distributed denial of service
DMZ	demilitarized zone
FIPS	U.S. Federal Information Processing Standards
FPM	firewall policy management
GUI	graphical user interface
IP	Internet Protocol
IPS	intrusion prevention system
IPv6	Internet Protocol version 6
MSSP	managed security service provider
NGFW	next-generation firewall
NGIPS	next-generation IPS
P2P	peer-to-peer
SMB	small or midsize business
SSL	Secure Sockets Layer
UTM	unified threat management
VE	Virtual Edition
VPN	virtual private network
WAF	Web application firewall

Gartner Recommended Reading

Some documents may not be available as part of your current Gartner subscription.

"How Markets and Vendors Are Evaluated in Gartner Magic Quadrants"

"Magic Quadrant for Intrusion Prevention Systems"

"Magic Quadrant for Unified Threat Management"

Evidence

This Magic Quadrant was conducted in accordance with Gartner's well-defined methodology. The analysis in this research was based primarily on interviews and interactions during firewall inquiries with Gartner clients since the 2014 "Magic Quadrant for Enterprise Network Firewalls." We also considered surveys completed by vendors, vendor briefings conducted at the request of vendors throughout the year, interviews with references provided by vendors, and supporting Gartner quantitative research on market share.

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

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

Note 1 Type A, B and C Enterprises

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

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

Type C enterprises are risk-averse to procurement, perhaps investment-challenged and willing to cede innovation to others. They wait, let others work out the nuances and then leverage the lessons learned; this is the "lean back" security posture that is more accustomed to monitoring rather than blocking. For Type C enterprises, technology is critical to the business and is clearly a supporting function.

Note 2 Buyers' Confusion Concerning WAFs

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

Note 3 FPM Tools

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

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.

GARTNER HEADQUARTERS

Corporate Headquarters
56 Top Gallant Road
Stamford, CT 06902-7700
USA
+1 203 964 0096

Regional Headquarters
AUSTRALIA
BRAZIL
JAPAN
UNITED KINGDOM

For a complete list of worldwide locations,
visit http://www.gartner.com/technology/about.jsp