Magic Quadrant for Unified Threat Management (SMB Multifunction Firewalls)

Published: 20 June 2017 **ID:** G00316047

Analyst(s): Jeremy D'Hoinne, Rajpreet Kaur, Adam Hils

Summary

SMB multifunction firewalls, or UTM, provide SMBs and distributed enterprises with multiple security functions in a single appliance. Network security leaders should use this research to evaluate performance, security, ease of use, local support and technology's ability to handle new SMB practices.

Strategic Planning Assumptions

Through at least 2020, the firewall markets for SMBs and enterprises will remain distinct for deployment scope and depth of security.

By 2022, more than 50% of new SMB firewall deployment will tunnel web traffic to a cloud-based secure web gateway, up from less than 10% today.

By 2022, 25% of SMBs will use multifunction firewall as an on-premises monitoring and access broker to inventory and control SaaS usage, manage mobile devices, or assess endpoint security posture, up from less than 2% today.

By 2022, 10% of new distributed branch offices' firewall deployment will switch to firewall as a service, up from less than 1% today.

Market Definition/Description

Gartner defines the unified threat management (UTM) market as multifunction network security products used by small or midsize businesses (SMBs). Typically, midsize businesses have 100 to 1,000 employees (see Note 1). UTM vendors continually add new functions on the UTM platforms, and therefore they encompass the feature set of many other network security solutions, including, but not limited to:

- Enterprise firewall
- Intrusion prevention systems (IPSs)
- Remote access
- Routing and WAN connectivity
- Secure web gateway

Secure email gateway

While consolidation of security controls in a single "appliance" comes with compromises in performance, security efficacy and capability, these are compromises that many SMBs are willing to accept (see "What You Should Expect From Unified Threat Management Solutions"). Browser-based management, short learning curve for security policy configuration, embedded reporting, and localized software and documentation don't specifically appeal to large enterprises, but are highly valued by SMBs in this market.

Gartner sees very different demands from the large-enterprise and branch office firewall markets (see "Magic Quadrant for Enterprise Network Firewalls" and "Next-Generation Firewalls and Unified Threat Management Are Distinct Products and Markets"). These generally require more complex policy management workflow and network security features, and are optimized for very different selection criteria and price points.

The branch offices of larger companies often have different network security demands than midsize businesses, even though they may be of similar size. Large enterprises often use low-end enterprise products at their branch offices to ensure interoperability and to take advantage of economies of scale in getting larger discounts from their firewall vendors, and use the same management console for the headquarters and for the branches. For these reasons, Gartner allocates branch office firewall revenue to the enterprise firewall market, not the UTM market.

Small businesses with fewer than 100 employees have even more budgetary pressures and much lower risk awareness than larger organizations. Most security procurement decisions are driven by nontechnical factors, such as brand awareness, and rarely by competitive feature comparisons. Therefore, this Magic Quadrant focuses on the UTM products used by midsize businesses. Midsize organizations frequently manage the technology with in-house IT staff, or use a managed security service provider (MSSP) to handle the operational maintenance of the appliance, manage the configuration or handle the security monitoring.

Distributed organizations with highly autonomous offices, such as retail franchises, might total more than 1,000 employees, even if only a portion of these employees are connected to the IT infrastructure. Similar to SMB organizations, these organizations often have constrained budgets due to the large number of branches and often small IT security teams. Many UTM vendors have added features for this use case, with some vendors even focusing more on distributed organizations than on traditional SMBs.

SMBs and organizations with a large number of autonomous branches should be skeptical of the aspirational message from UTM vendors about the frequently exaggerated benefits of feature consolidation.

Magic Quadrant

Figure 1. Magic Quadrant for Unified Threat Management (SMB Multifunction Firewalls)

Source: Gartner (June 2017)

Vendor Strengths and Cautions

Barracuda Networks

Barracuda Networks is a Niche Player. It lacks visibility outside of the EMEA region and has relatively small market share. However, the vendor demonstrates continued growth and has made good strides in advanced threat detection and ease of deployment, and shows improvement in its product strategy.

Barracuda Networks, headquartered in Campbell, California, is a large vendor that delivers network security, backup and infrastructure solutions. Barracuda NextGen Firewall X-Series (NGX) comprises six models, including three desktop models. It embeds a web interface

designed for simpler use cases. Barracuda Cloud Control (BCC) is the cloud-based centralized management portal for the X-Series. Barracuda offers another line of firewall products, the NextGen Firewall (NGF) F-Series, targeting larger enterprises.

Recently, Barracuda announced the introduction of an F-Series firewall for Google Cloud, making it one of the only third-party firewalls to support Google Cloud. During the evaluation period for this Magic Quadrant, the vendor also released Zero Touch Deployment service for the F-Series to eliminate deployment complexity. No new X-Series models were recently introduced.

Barracuda Networks is a good candidate for SMBs looking for good total cost of ownership, or that require ease of deployment and high quality of support.

STRENGTHS

Marketing and sales execution: Barracuda has been effective in building sales channels that understand smaller midmarket customers, and continues to invest in its channels. Surveyed partners like the recent changes to the partner program. Barracuda has a growing visibility in SMB multifunction firewall client shortlists observed by Gartner, demonstrating particular strength in the education vertical. Barracuda is profitable, and its 2016 firewall revenue grew more than this market's average.

Capabilities: Surveyed clients mention advanced threat defense capabilities, ease of installation and management as product strengths.

Geographic strategy: Barracuda has a growing channel presence across North America, Europe and Asia/Pacific (APAC). Vendor support centers are available in several countries, and its support centers are conversant in numerous languages. In addition, the management console is available in 13 languages, and QuickStart guides are available in six.

Market understanding: With its simplified Cloud Control management console and its Zero-Touch CudaLaunch capabilities for simplified Client-2-Site VPN rollout, Barracuda X-Series appeals to smaller midsize businesses and MSSPs targeting SMBs that value simplicity in their firewall deployments.

Customer experience: Surveyed customers and resellers mention top-notch support as a primary reason to continue using Barracuda for SMB multifunction firewalls.

CAUTIONS

Capabilities: Despite its enterprise firewall (F-Series) having broad deployment in the public cloud (most notably in Microsoft Azure, and it became one of the first firewalls to offer a Google Cloud version), Barracuda X-Series still does not offer a virtual appliance, making it unusable for smaller midsize companies that wish to deploy resources to the public cloud.

Capabilities: Barracuda firewalls lack canned report for SaaS discovery and do not integrate with cloud access security brokers (CASBs). Barracuda does not offer endpoint solutions, and its firewalls cannot integrate with third-party endpoint protection solutions.

Market segmentation: The vendor does not offer a fully featured multifunction firewall appliance model under $500, as some of its competitors do.

Customer experience: Surveyed customers and Gartner clients note that the Barracuda firewalls have a slow web interface and lack management sophistication.

Product strategy: As they mature, midsize customers are unable to address more sophisticated use cases with X-Series; instead, they must graduate to F-Series, which has a different management console, and a different look and feel.

Sales strategy: Barracuda is not visible in Gartner clients' shortlists from South America, the Middle East and APAC. Barracuda does not have a mature channel structure or support centers in South America, making it difficult for prospects and customers in that region to receive effective service.

Check Point Software Technologies

Check Point Software Technologies is a Leader. The vendor continues to win SMB multifunction firewall selections based upon its enterprise-quality security features, ease of management and intuitive graphical user interface (GUI). Gartner believes Check Point has strengthened its vision via its product enhancements and innovations in ransomware protection.

Co-headquartered in Tel Aviv, Israel and San Carlos, California, Check Point is a large pure-play security vendor with more than 1,300 employees in R&D. Its product lines include SMB and enterprise firewalls (Security Gateway), endpoint protection against advanced threat (SandBlast Agent), mobile security (Sandblast Mobile) and virtual firewalls (vSEC for private and public cloud). Its SMB multifunction firewall line includes the 700, 1400, 3100, 3200, 5100, 5200, 5400 and 5600 lines of appliances, all introduced in 2016 or 2017.

Recent news includes the introduction of vSEC for the Google Cloud Platform and the availability of the R80 and R80.10 versions, with several improvements to the management console, better VPN performances and new endpoint protection against ransomware.

Check Point is a good shortlist candidate for midsize enterprises that require very good security with robust management interface.

STRENGTHS

Market understanding: Check Point continues to make investments to address SMB clients and MSSP requirements. Its recently announced Check Point Infinity relies on principles that appeal to smaller organizations with multifunction platforms, a block-first strategy and intuitive management for small teams.

Management console: Check Point's reporting and management console and on-device GUIs are consistently rated very highly by midsize companies that need to handle complexity. R80 introduced integrated application control directly in the access policy. A SaaS discovery report is available.

Capabilities: Check Point's UTM solutions benefit from its enterprise-level security features, such as the Anti-Bot option, threat intelligence feeds and credible intrusion prevention system (IPS), backed up by a robust threat research team. Its solutions consistently get high scores in independent testing for threat detection rate. Check Point's sandboxing solution is now available for all of its firewall models.

Capabilities: Check Point provides a strong set of network options to protect against custom malware with its sandboxing subscription (SandBlast Emulation Service), a variety of threat intelligence feeds (ThreatCloud IntelliStore) and a feature that can automatically remove suspected harmful content from downloaded files (Threat Extraction).

Customer experience: Partners and customers note that creating and using objects easily is a particular strength. Some clients report that the compliance blade can facilitate audits of configuration in regulated environments. Client feedback on the new software versions in the R80.x family has been positive.

Marketing and sales execution: 2016 saw a clear uptick of SMBs opting for NGTP and NGTX feature bundles, allowing these organizations to utilize advanced security features without the complexity of having to buy and deploy eight to 10 software blades individually.

CAUTIONS

Sales strategy: Check Point is priced higher than its competitors. This is confirmed by Gartner clients who still cite price as the primary reason for not selecting Check Point solutions, and Gartner clients and surveyed customers and partners still note a relative lack of satisfaction with Check Point because of its high subscription renewal price.

Market responsiveness: Check Point can be slower than its competitors to release or improve features that appeal only to SMBs. The firewall still lacks a user quarantine for email. Unlike many of its competitors that support decryption for multiple protocols, Check Point can decrypt HTTPS only.

Capabilities: Some Gartner midsize clients report that, as they have conducted competitive evaluations, Check Point firewalls lack enough performance capacity to compete with lower-priced solutions. Gartner analysts noticed undersizing of the firewall appliance in many of these situations.

Capabilities: Check Point's web management interface is a trimmed-down version of the centralized management console. Check Point Security Gateways do not directly integrate with CASB vendors or leverage SaaS APIs for increased visibility or additional control options.

Marketing strategy: Gartner still sees Check Point mostly selling to its existing client base. However, the NGTX feature package has generated more interest among non-Check Point SMB customers.

Marketing execution: The abundance of branded names for features is confusing. Prospective midsize clients can't figure out the features behind the names, or are often unaware that Check Point has a line of multifunction firewalls with enterprise-quality features that could address their high security use cases.

Cisco

Cisco is a Challenger. Cisco demonstrates continued innovation for a segment of the market with its Meraki MX product line. Meraki MX and the traditional Firepower offering are developed in silos, without any integration, but are both needed to address some customer needs.

Cisco is a large network infrastructure and security vendor, headquartered in San Jose, California. It has a global presence and employs more than 73,000 employees. In recent years, the vendor has doubled down on cloud and security investments. Its security portfolio includes firewalls (Firepower and Meraki MX), IPS (Firepower), network traffic analysis (Stealthwatch) and CASB (Cloudlock). Cisco security solutions also include endpoint (AMP, AnyConnect) and Cloud (Cisco Umbrella) solutions.

Announcements relevant to SMB organizations include the release of the Firepower 2100 Series, a continuation of Cisco's effort to update its entire product line with preinstalled Firepower software. Cisco also made network sandboxing available on Meraki MX, and updated its cloud-based management console.

Cisco is a good shortlist contender for all SMBs and distributed organizations, when the relevant skills are available from the selected channel partner. Cisco Firepower is a good choice for midsize businesses, and Cisco Meraki is a good shortlist contender for distributed organizations, especially those with 10 to 100 offices.

STRENGTHS

Marketing execution: Cisco is a ubiquitous brand in network and security worlds. Cisco is one of the most visible vendor in UTM shortlists, and is now considered frequently even when not the incumbent solution. Meraki MX visibility, while still mostly limited to the U.S. and the U.K., has also improved, particularly in the retail industry.

Capabilities: Cisco's SMB clients like the ability to get enterprise-class security features with AMP, threat intelligence from the large Talos threat research team and IPS inherited from the Sourcefire acquisition (full IPS on Firepower; Sourcefire signatures on Meraki MX).

Centralized management: Distributed organization clients like the ability to use Meraki's unified management and monitoring solution for wireless, switches, firewall, site-to-site VPN and mobile device management.

Improvements: Cisco has released several features to offer integration between its security solutions, which appeals to SMB customers. It also continues to invest in improving its management with new versions of on-premises and cloud management console for Firepower.

Customer experience: Clients and prospects often describe Cisco as a trusted brand and trusted partner. Several U.S. clients gave Cisco good scores for client support. Meraki's users are strongly positive on ease of deployment and implementation.

CAUTIONS

Product strategy: The Meraki MX product line does not fully address all the use cases for SMB network security needs, and it continues to be developed as a separate effort from Cisco's corporate strategy. This dual-product-line offering available to SMB clients from Cisco often creates product management complexity and buying confusion. Cisco Cloud Defense Orchestrator and Meraki MX provide overlapping options for cloud-based centralized management.

Capabilities: All Meraki MX firewalls and the smaller Cisco Firepower appliance lack Transport Layer Security (TLS) decryption to inspect employee browsing over HTTPS. Meraki lacks email security and does not inspect http files for viruses, but sends file hashes to the Advanced Malware Protection (AMP) cloud infrastructure.

Market responsiveness: Gartner analysts see Meraki MX's recent release of Threat Grid sandboxing, months after most of its competitors, as an indication that Cisco's investment in Meraki is limited. For smaller organizations, Cisco still offers Cisco ASA appliances, which can be upgraded to use the Firepower firmware, but with noticeable performance impact, as no Firepower product is available yet for this segment.

Management console: Inferior management console quality, compared with leading solutions, has always been the most vocal complaint from Cisco ASA clients. In late 2016, Cisco released Firepower Device Management, an embedded web interface, but it is not yet full-featured, and lacks a zero-touch deployment option. In some industries (public sector, finance) and some European and Latin American countries, Meraki's cloud-based management console might not be a desirable option.

Customer experience: Clients mention that the quality of Firepower firmware updates could be better, as using the new features delivered on the latest version often creates support issues. Meraki MX clients with a large number of offices note that ease of use suffers with scale, and are frustrated with the limited access they have to diagnostic tools.

Sales execution: Several clients complain about increased costs and price list complexity. They also complain about accelerating product life cycles in recent years. Outside of North America, channel awareness and expertise on the Meraki MX solutions are scarce, creating situations where Firepower must replace Meraki for targeted use cases.

Fortinet

Fortinet is a Leader. It has strong presence in SMB shortlists and a strong feature/price/performance offering, which help make it a frequent choice for UTM. Fortinet is also the most frequently shortlisted vendor for SMB and distributed-office use cases. We believe its product vision quality has declined somewhat, relative to those of some competitors.

Headquartered in Sunnyvale, California, Fortinet has more than 4,600 employees globally, including more than 1,000 employees in R&D. Its portfolio of network and endpoint security solutions includes SMB and enterprise firewalls (Fortigate), endpoint protection platform

(FortiClient) and web application firewall (FortiWeb). Recent news includes the latest generation of hardware models (E Series) and tighter integration between the different products of its portfolio (Fortinet Security Fabric).

Fortinet is a good shortlist candidate for all SMBs, and for distributed offices with simple management needs or working with an MSSP.

STRENGTHS

Geographic strategy: Fortinet has the largest channel presence across all regions, and its customer base is vastly distributed. Vendor support centers are available in 10 countries. In 2016, the vendor announced the opening of a European data center, based in Germany, for its FortiCloud and FortiSandbox features.

Marketing and sales execution: Fortinet is the clear leader in this market. It is the most visible vendor in SMB multifunction firewall client shortlists observed by Gartner. Fortinet is profitable, and its 2016 revenue grew almost twice as fast than the market average. It is also the vendor most frequently cited as being the strongest competitor in this market by surveyed resellers.

Customer experience: Fortinet provides very good performance and pricing to its SMB customers. Results from survey and Gartner client inquiries are consistent in highlighting this.

Capabilities: Fortinet's security services are driven by a large threat research team. Dedicated application profiles for SaaS visibility and control are also available.

Market understanding: Fortinet offers integration between many products in its portfolio, including firewalls, endpoint, wireless access point and switches. The concept, named Fortinet Security Fabric, gives customers willing to invest in multiple Fortinet solutions a unified view of their infrastructure and the ability to manage AP and switches directly from the Fortigate console. It also allows integration with Fortinet's endpoint solution (FortiClient) to perform a health check before authorizing a connection to the network.

CAUTIONS

Capabilities: Fortinet lags behind its direct competitors in cloud-based management that appeals to distributed offices in cloud enthusiast industries, such as retail and education. FortiCloud is Fortinet's first step in providing centralized management from a cloud portal. It integrates FortiView, but lacks fully featured centralized management of the configuration.

Malware prevention: Fortinet has a small base of customers using its cloud-based network sandboxing feature. Surveyed resellers report the lowest deployment rate of network sandboxing for vendors evaluated in this research. It also gets a low satisfaction score for the quality of its HTTPS decryption feature.

Customer experience: Surveyed clients and resellers expressed concerns about the lack of intuitiveness of the management console. Gartner also observed similar issues with clients managing distributed offices with a small in-house team.

Customer experience: Fortinet customers have reported difficulty in obtaining easy, responsive support from the Fortinet ecosystem.

Sales strategy: Gartner has observed that list prices in proposals outside of North America can be significantly higher than in the U.S. While a small uplift is expected, Fortinet clients outside of North America should verify competitive pricing propositions and not rely only on Fortinet's reputation for good pricing.

Hillstone Networks

Hillstone is a Niche Player in the UTM Magic Quadrant. It is visible mostly in China and South East Asia, but is slowly growing in Latin America. Its product strategy is more focused toward carrier and enterprise use cases, and lacks focus toward all SMB use cases, as its UTM is missing features such as email security and endpoint security.

Hillstone Networks is headquartered in Beijing, China, with regional headquarters in Sunnyvale, California. Hillstone is an established network security player in South East Asia and trying to expand in other regions. Other than UTMs, Hillstone also offers enterprise firewalls (T-Series and X-Series). Its portfolio also includes Network Intrusion Prevention System (NIPS; S-series), Server Breach Detection System (sBDS; I-Series) and cloud security solutions (CloudHive and CloudEdge). It also offers Hillstone Security Management Platform (HSM) and Hillstone Security Audit Platform (HSA) for centralized management and audit. In 2016, Hillstone introduced a few major features, such as Cloud Sandbox and HTTPS decryption.

Hillstone is a good shortlist candidate for organizations in China, or where skilled channel partners are available, especially where there is a need for a unified console for managing hybrid networks with a mix of cloud and on-premises firewall appliances.

STRENGTHS

Capabilities: Clients report that the real-time monitoring dashboard provides useful features to easily investigate incidents, even for nonsecurity experts.

Capabilities: The advanced monitoring feature of VPN tunnels in Hillstone UTMs makes it a good candidate for distributed branch offices connected through site-to-site VPN tunnels. The centralized management and monitoring offers features such as VPN topology monitoring, multiple device status and traffic monitoring, which helps the administrator understand the branch device status and VPN connection to headquarters.

Technical architecture: The cloud-based management portal CloudView provides support for multiple Hillstone product lines, including UTM and enterprise firewall (Hillstone E-series next-generation firewall [NGFW] and T-series intelligent NGFW [iNGFW]). At present, CloudView offers basic capabilities with strong monitoring and reporting features. This feature provides centralized monitoring capabilities to clients using multiple Hillstone product lines.

Infrastructure as a Service (IaaS): Hillstone's virtual CloudEdge firewalls support all the major regional local cloud platforms in China, including carrier cloud (China Unicom, China Telecom, China Mobile), Jindong Cloud, Huawei Cloud, AliCloud and other global public

clouds, such as Amazon Web Services (AWS) and Microsoft Azure. This makes Hillstone a good shortlist candidate for organizations that want to secure their cloud network with the same on-premises UTM vendor.

Technical support: Surveyed clients and resellers give high scores to technical support, citing quick resolution and turnaround time.

CAUTIONS

Product strategy: Hillstone's strategy is focused on enterprise and carrier use cases, giving higher priority to features relevant to this market, such as virtualization and support for software-defined networks (SDNs). This diverts some of its R&D investment from SMBs, which typically look for multiple easy-to-use security features in their UTM.

Geographic strategy: Since Hillstone is targeting markets outside China, but still has most of its firewall sales in China, prospective clients should be cautious of the experience of Hillstone's partners, because the firewall may be a new solution for them.

Capabilities: Hillstone firewalls lack SaaS monitoring and control functionality. They do not offer any specific reports for SaaS applications. CloudView is only offered in China, lacks any centralized configuration and deployment capabilities, and only offers monitoring and reporting capabilities.

Capabilities: Hillstone UTMs lack email security features, which remain an important feature for SMBs and a shortlisting criteria. It also lacks integration with Office 365 to provide additional visibility and control for the service.

Capabilities: Hillstone UTMs do not offer any inbuilt endpoint protection platform (EPP), and also lack support for any third-party EPP.

Huawei

Huawei is a Niche Player. It has limited presence outside of China. The vendor is making progress in other regions, such as Latin America and Middle East. Gartner believes the vendor shows greater vision thanks to its increased focus on SMB needs. However, features like a cloud-based management portal and advanced malware prevention need more granularity to compete with Leaders in the market.

Headquartered in Shenzhen, China, Huawei is a global information and communication vendor, offering security and data communication solutions for enterprise and carrier networks. Huawei has a large portfolio of infrastructure and telecom products operating under multiple divisions. Huawei Security is part of its networking and security division, which offers firewalls and application security products along with distributed denial of service (DDoS) appliances, but has its own security sales team and dedicated channel partners to sell them.

In 2016, Huawei introduced four new appliances and two virtual appliances for AWS and Xen. It released features including network sandboxing, cloud-based management portal of UTMs and enhancements to its centralized management tool, eSight, all of which fill in feature gaps.

Huawei's Unified Security Gateway (USG) UTM is a good shortlist candidate for SMBs that are already using other Huawei product lines, and those that are looking for basic UTM features at a good price, especially in China and Latin America, where the vendor has a good UTM presence.

STRENGTHS

Platform: Huawei has a broad network, security and data communications product portfolio, which makes it a good contender for organizations that look to maintain single vendor relationship. In China, it strongly competes with leading vendors.

Capabilities: Huawei USG's quota-based user traffic management feature has been mentioned as one of the strongest features of the product, both by surveyed clients and resellers.

Centralized management: Huawei has developed a centralized software-based management platform, eSight, which is capable of managing its security and data communications product lines. Huawei's customers that are using its various security and data communication product lines can thus easily manage the different products. The recent enhancements to eSight include a drag-and-drop feature, policy provisioning and synchronization, and backup and rollback.

Capabilities: The vendor has developed Cloud Access Security Awareness (CASA) for monitoring and controlling SaaS applications over the cloud. This includes such features as SaaS application and behavior recognition; SaaS behavior control, such as file blocking; and login blocking, which provides organizations with more visibility and control over their cloud-based SaaS applications.

Sales execution: Surveyed resellers and clients report that Huawei's USG UTM offers good value for the price, as compared to other international vendors available in the region.

CAUTIONS

Capabilities: Although Huawei provides a cloud-based management portal for its Agile Controller UTMs, it still lags behind in terms of control and management features that can be centrally applied on the UTM devices.

IaaS: Huawei USG UTM is not yet available on Azure, leading organizations using Azure to look to different vendors.

Marketing execution: Huawei lacks strong marketing messaging around security, as well as a dedicated regional channel market and sales strategy for its security solutions in regions outside China, such as Europe and South East Asia. Regional value-added resellers (VARs) struggle to promote Huawei against other international vendors with very strong regional teams and regional market strategies, such as multiple distributors, local sales engineers, and better channel training and support to compete in those regions.

Technical architecture: Huawei USG UTMs do not provide an EPP feature for antivirus and anti-malware on the endpoints. It offers third-party endpoint integration only with McAfee solutions.

Customer experience: Customers report that Huawei's documentation and brochures in regional languages other than Chinese are not updated regularly and can be outdated.

Juniper Networks

Juniper Networks moved from the Challenger to the Niche Players quadrant. The vendor has struggled with its sales execution, which resulted in a drop in their UTM market share, slipping customer satisfaction and lack of SMB-focused product strategy.

Based in Sunnyvale, California, Juniper Networks is a global network infrastructure vendor. Its broad product portfolio includes a range of network edge and management devices, routers, switches, SDN and enterprise firewalls (SRX series firewalls).

Over the past year, Juniper has made enhancements to its advanced cloud-based malware prevention service, Sky ATP, as well as enhancements to its centralized firewall management, Security Director. It has also introduced four new SRX UTM models.

Juniper is a good shortlist contender for upper-midsize organizations already using other Juniper products.

STRENGTHS

Technical support: Juniper's technical support is always rated highly by both VARs and end users. They often cite the technical support team as being friendly and offering quick response. Other than offering support in English, Juniper also offers support in multiple regional languages, including Arabic, French, German, Russian, Spanish, Ukrainian, Serbian-Croatian, Polish, Tagalog, Japanese, Korean and Mandarin.

Geographic strategy: Juniper Networks has a strong worldwide presence, with a network of channel partners and technology integration partners in various regions.

Capabilities: Customers and VARs have reported the web-filtering capabilities of Juniper SRX through Websense as one of best product features. Juniper offers three different web-filtering licenses: the Local Web Filtering option, which is offered free of charge; Enhanced Web Filtering, which uses cloud-based Websense Master Database URL; and Websense Redirect, which redirects the web traffic to an on-premises Websense appliance.

Capabilities: Juniper Networks is known for providing good-quality hardware appliances. Its SRX series has strong integrated routing and switching capabilities from the MX-Series routers and EX-Series switches.

Sales strategy: Juniper Networks offers a free Sky ATP subscription on SRX platforms, including SRX340, 345, 550M and other enterprise firewall models. This basic subscription only scans .exe files for web traffic over HTTP and HTTPS.

Improvements: Juniper has enhanced the firewall management interface and the logging and reporting capabilities in Junos Space Security Director by making it more interactive. Junos Space Security Director also supports automated actions from event view, including single-click blocking options for users, applications, geographies or threat events.

Technical architecture: Juniper has designed Juniper's Software-Defined Secure Networks (SDSN) Platform to equip its customers with centralized policy, detection and enforcement across various Juniper platforms, such as routers, switches and firewalls. In 2016, it extended the SDSN Policy Enforcer feature with automated enforcement on EX/QFX switches, and plans to extend this support further to third-party switches, private clouds and public cloud (AWS).

CAUTIONS

Product strategy: Juniper's product strategy lacks focus for SMB security use cases. Its product strategy and roadmap are more focused toward enterprises and carrier-class requirements.

Capabilities: Juniper SRX still lacks features desired by SMBs, such as strong, mobile VPN clients, end-user quarantine for spam, and endpoint security management. It has just released SSL encapsulation of IPsec traffic for remote hosts as a work-around for its lack of native SSL VPN capabilities. The vendor does not offer cloud-based management of Juniper SRX, which can be an important feature for cloud enthusiast industries, such as retail and education.

Sales execution: Juniper is hardly visible in SMB multifunction firewall client shortlists observed by Gartner. The vendor is quickly losing market share.

Advanced malware prevention: Juniper's advanced malware prevention subscription known as Sky ATP is not available on smaller UTM models SRX 110 and SRX 220d 200. Sky ATP can inspect HTTP and HTTPS, but does not support IMAP. The vendor has only released support for SMTP in March 2017.

Technical architecture: Juniper lacks an EPP offering. Juniper security information and event management (SIEM) supports many third-party endpoint solutions, but there is not yet any integration between SRX firewalls and third-party endpoint protection platform vendors. The vendor has recently announced an API and partnerships to integrate with third-party endpoint vendors in the future.

Customer experience: Juniper receives below-average scores for ease of initial deployment, stability of its firmware updates and the quality of its app control feature.

Rohde & Schwarz Cybersecurity

Rohde & Schwarz Cybersecurity is a Niche Player. It primarily serves German customers and has limited reach in the upper-midsize market segment. It lags behind other vendors in terms of execution, especially around market responsiveness, and expressed customer satisfaction has slightly declined over the evaluation period.

Rohde & Schwarz is a Germany-based electronics group that has acquired several vendors to build its cybersecurity division, and has 450 employees. Its portfolio includes a multifunction firewall product line, gateprotect (named after a company acquired in 2014), and a web application firewall, DenyAll, acquired in 2017. It also offers several encryption management products.

Recent news includes a refresh of the gateprotect appliances and a rebranding of the firewall and UTM portfolios. Its firewall product line now comprises the Unified, the Extended and the Specialized Lines.

Rohde & Schwarz Cybersecurity is a good shortlist candidate for German SMBs and for small organizations in other EMEA countries where certified gateprotect channel partners are available.

STRENGTHS

Organization: Rohde & Schwarz continues to invest in cybersecurity. It is already one of the larger European vendors for network security.

Capabilities: eGUI, the management console for gateprotect firewalls, includes the ability to build and visualize a network topology map of the filtering policy.

Sales execution: Several clients cite that they selected Rohde & Schwarz because it is a German vendor. The vendor successfully markets its German R&D and "no backdoor" policy as competitive advantages against its U.S.-based competitors. This appeals to local resellers and to a portion of the European market, especially small government agencies.

Customer experience: Customers score gateprotect very highly for the ease of use of the eGUI management console, especially when defining a security policy.

Geographic strategy: The management interface and documentation are available in German for all the firewall product lines. The gateprotect management console is also available in Italian, Spanish, French and Turkish. Support is available in German, French and English.

CAUTIONS

Marketing strategy: Rohde & Schwarz Cybersecurity is hampered with the required investments to merge its firewall product lines and to migrate to the web version of its management console. Its strategic vision is slowly moving away from SMBs to target larger organizations, promoting enterprise features higher in the roadmap priority.

Market segmentation: Rohde & Schwarz Cybersecurity solutions will not be appropriate for upper-midmarket organizations that have enterprise-class requirements. It also has a relatively small sales and presales team to address this market. The gateprotect product line includes models to serve larger organizations, but the vendor is not visible in Gartner client shortlists for this segment. The small and lower-midsize organizations from Europe are where most of the vendor customer base is deployed, and where its channel has experience.

Capabilities: Gateprotect lacks network sandboxing and threat intelligence feeds. Its centralized management (Command Center) is in beta only, and there are no centralized monitoring and reporting solutions yet. Legacy centralized management and monitoring solutions are still available for the unified line only. Several differences in capabilities exist between the Unified and Extended Lines.

Customer experience: Gateprotect gets low scores for its high rate of false positives, its centralized management and the poor number of available security reports. Organizations with multiple offices might have to juggle between the two flavors of eGUI management console that exist: the Windows software for smaller appliances, and the more recent web version for midsize products.

Organization: Some gateprotect resellers cite negative consequences of the Gateprotect acquisition and product line refresh, including new rules, price list changes and lack of flexibility, and too-fast end-of-life of legacy products.

SonicWall

SonicWall is a Challenger. It benefits from its remaining market presence, and its legacy of being a strong SMB and network security brand, with a global presence through a long-established channel. The vendor is less visible with Gartner clients in recent UTM deals, reflecting its poor market execution. Its product strategy has also impacted its vision. SonicWall has been late in introducing new features such as advanced malware protection, and still lacks a cloud management portal and a virtual appliance offering, both of which have been offered for some time by other UTM vendors in the market.

SonicWall, headquartered in Santa Clara, California, is a long-established network security vendor. It employs more than 1,200 employees. Until last year, SonicWall was under Dell as Dell SonicWALL, and after the split, it is an independent vendor company. The SonicWall portfolio includes network security, access control and email security product lines. It did not release any new UTM models in 2016, nor during the first half of 2017. In May 2017, SonicWall has launched its cloud management portal (Cloud GMS).

SonicWall remains a good candidate for most SMB use cases, especially organizations that want to offer cost-effective integrated wireless access managed centrally from within the UTM.

STRENGTHS

Market segmentation: SonicWall UTMs have a good presence among more than 50 distributed-office use cases, with site-to-site IPsec VPN connectivity. SonicWall offers solid IPsec site-to-site VPN tunnels that can be scaled very easily to multiple sites.

Capabilities: Surveyed SonicWall customers and channel partners have given high ratings to the TLS inspection engine (Deep Packet Inspection of Secure Sockets Layer; DPI-SSL) for its ability to limit throughput degradation. SonicWall firewalls use a multiengine cloud-based sandbox. This approach makes it a good shortlist candidate for SMBs looking for a strong advanced malware protection cloud service.

Capabilities: SonicWall offers multiple wireless AP management and control features within its firewall portfolio. The majority of its customers utilize this feature. It is a favorable vendor for SMBs that offer wireless access in their organizations.

Centralized management: SonicWall Global Management System (GMS) offers a centralized management solution for SonicWall firewalls, SonicPoints (access points), Dell Networking X-series switches and WAN Acceleration Appliance (WXA) series devices. This

offering is useful for SonicWall customers that are using multiple product lines.

Technical architecture: SonicWall offers integration with Kaspersky and McAfee for enforcement of their endpoints through SonicWALL UTMs. This helps the clients to centrally enforce the endpoint platforms. It also offers integration capabilities with SonicWall Mobile Connect, which offers a SSL VPN mobile app for various mobile clients, including iOS 7.0+, Android 4.1+, macOS 10.9+, Windows 10 and Windows 10 Mobile devices, and Chrome OS 45+.

Marketing strategy: SonicWall has a strong network of loyal channels across the globe that are pleased about SonicWall becoming an independent vendor again. SonicWall communicates its product strategy and roadmap to them on a regular basis, and also offers good sales and technical support.

CAUTIONS

Market segmentation: SonicWall lacks a virtual appliance offering for its firewalls and UTMs; therefore it has no presence over the public clouds. This forces organizations with hybrid networks to consider another vendor for their cloud networks.

Marketing execution: Gartner less frequently sees SonicWall being shortlisted by clients. The vendor has recently experienced a decline in revenue. Gartner attributes many of these issues to the succession of ownership changes and subsequent disruption to the company.

Market responsiveness: SonicWall has been slow in providing new features and enhancing its existing capabilities. Surveyed clients have also reported that the wireless AP management feature has not been enhanced to offer more unique capabilities.

Customer satisfaction: Gartner continues to receive mixed feedback on SonicWall customer support, especially from upper-midsize organizations.

Capabilities: SonicWall has just released the first version of its cloud-based management portal, and still lacks zero-touch deployment.

Capabilities: Despite having a separate product line for email security and encryption, SonicWall has not integrated all those features in the inbuilt email security UTM feature.

Sophos

Sophos is a Leader in the UTM Magic Quadrant. It continues to gain market share due to ease of use, security feature richness and successful integration with its endpoint product. It demonstrates strength in its product vision and roadmap execution, relative to those of some competitors. Sophos is a frequently shortlisted vendor for lower-midsize business and distributed-office use cases.

Headquartered in Abingdon, U.K., and in Burlington, Massachusetts, Sophos has more than 3,000 employees globally. Its portfolio includes a mix of network and endpoint security solutions. Its firewall product line consists of Sophos XG Series, which includes 19 models, all of which were introduced in 2015 and refreshed in 4Q16; and the legacy Sophos SG Series. Sophos UTMs are available as virtual appliances with integration on the AWS and Azure IaaS

platforms. Endpoint security products include Sophos Endpoint and Intercept X. Sophos has Synchronized Security, an integration between its UTM and Sophos Endpoint product. Sophos offers a number of other security solutions, including mobile security and encryption.

Recent news includes the introduction of a new set of XG firewalls that support Sophos Sandstorm and Synchronized Security, and the acquisition of Invincea, an advanced-threat-focused endpoint vendor.

Sophos is also a good shortlist contender for SMBs, especially those that value ease of use, security features and firewall/endpoint integration.

STRENGTHS

Capabilities: A majority of surveyed customers and partners mention security feature richness and breadth as a reason for the selection of Sophos. Continued execution on an aggressive roadmap has strengthened prospective buyers' view of Sophos UTM as a security leader.

Sales execution: Sophos has a significant IaaS presence relative to most UTM competitors. The SG line has an integrated Web Application Firewall feature, which is useful in making Sophos UTM increasingly relevant to public cloud deployments.

Capabilities: Sophos customers and partners cite on-box UI quality and the ease with which they can interact with it as strong positives.

Technical architecture: With Security Heartbeat, the recently added capability to isolate endpoints missing a heartbeat, Sophos Synchronized Security is maturing and has become a recognized differentiator. The feature is tightly integrated in the management interface and provides a unified dashboard. It is still evolving, but shows increasing promise in enhancing the security posture of midmarket organizations willing to make the effort to integrate firewall and an endpoint.

Customer experience: Sophos is the only UTM vendor to offer three months of free support, along with a one-year warranty for customers that want to try Sophos UTM before committing to paying for a support contract.

CAUTIONS

Product strategy: Although Sophos says that it will support the two UTM product lines for an undisclosed period, the vendor focuses its roadmap on the XG Series. Prospective customers should confirm the roadmap and support services' long-term availability for the SG Series.

Product strategy: Although the XG platform has recently added support for network sandboxing and Synchronized Security, it is still not at feature parity with SG. Gartner has observed that adoption for the new platform is slow.

Customer experience: XG Series is a completely new solution when compared to the Cyberoam CR Series. Former Cyberoam channel partners might still have limited experience with Sophos products. Existing Cyberoam customers should carefully evaluate the cost of

migrating from the CR Series to the XG platform, the tools provided by the vendor and the channel experience with the XG software.

Capabilities: Sophos lacks SaaS discovery reports, and does not offer on-device CASB features or integration with CASB vendors for improved visibility and better control of SaaS activity.

Customer experience: Gartner clients and surveyed Sophos stakeholders mention occasional issues with customer support in terms of response time and ability to access expert resources to solve complex issues.

Stormshield

Stormshield is in the Niche Players quadrant. It has demonstrated recent product improvements. Stormshield is a subsidiary of Airbus Defence and Space, based in France, with a strong regional focus. It employs more than 200 employees. Stormshield portfolio includes firewalls (Stormshield Network Security), EPP (Stormshield Endpoint Security) and data encryption (Stormshield Data Security).

Recent news includes several product improvements: a refresh of the low-end appliances and new models with integrated Wi-Fi, the release of a new centralized management solution, the addition of an automated risk score for hosts, and real-time monitoring features embedded on the web management function.

Stormshield is a good shortlist contender for EMEA organizations with a few locations when local skilled channel support is available.

STRENGTHS

Geographic strategy: Stormshield's dense channel coverage in Europe makes it a frequent contender on SMB shortlists, and it has a large installed base of European SMBs. The vendor also regularly updates its European certifications and ensures that it offers dedicated features for regional regulations and compliance requirements.

Customer experience: Several customers and resellers gave excellent scores and described the security policy as combining intuitive controls for most use cases and more advanced capabilities when needed. Hardware quality also received a good average score.

Improvements: Stormshield has released entry-level appliances with integrated wireless. Customers cite good integration of the IP reputation feature in the security policy, and improved user access management and integration with the user directory in the latest version of Stormshield Visibility Center, its centralized reporting solution.

Operations: Stormshield continues to invest in developing its sales workforce in countries where the vendor previously had minimal involvement; it is also beginning to target new regions, including North America. To support this expansion, similar investments are being made in support and R&D.

Capabilities: Stormshield integrates a vulnerability detection engine and offers the ability to adapt the security policy for vulnerable hosts directly from the monitoring console. The performance degradation when enabling IPS is one of the lowest for vendors evaluated in

this research.

CAUTIONS

Customer experience: The recent feedback on Stormshield support has declined, compared with previous years. Surveyed customers point out that it is difficult to find relevant step-by-step technical documentation.

False positives: The Stormshield IPS engine is in prevention mode by default. This is good for security, but the large amount of false alerts when deploying the firewall has been a consistent subject of feedback over the recent years from end users and resellers.

Marketing strategy: Stormshield invests significantly less of its revenue in marketing compared to the Leaders evaluated in this research. Channel partners report that they don't find what they need from the available tools.

Product strategy: Innovations often lack sufficient polish and continued investment after first release to clearly impact user experience.

Capabilities: Surveyed customers give poor scores to the email security features (anti-spam quality and lack of user quarantine), as well as to the basic URL filtering and antivirus modules (Stormshield is also offering a premium subscription for antivirus and URL filtering). Customers would like further improvement in the real-time monitoring after the release of the version 3.

Centralized management: Stormshield's centralized reporting and management receive lower scores than similar offerings from its direct competitors. Its latest attempt to solve this issue, Stormshield Management Center, is still unproven and far from feature parity with the solutions from its competitors. The vendor does not offer a cloud-based centralized management console, nor the zero-touch deployment features that distributed organizations prefer.

Untangle

Untangle is in the Niche Players quadrant. The vendor is committed to serve lower-midsize businesses first, and has limited market reach outside of the U.S. The vendor continues to receive marks of high customer satisfaction. Despite expected short-term interferences, Gartner notes a renewed ambition following its recent acquisition.

Untangle is a U.S. vendor, based in San Jose, California. Its product portfolio includes software and appliance versions of its firewall solutions.

In September 2016, Untangle was acquired by an equity firm, but the endpoint solution (Total Defense) acquired in 2014 by Untangle was not part of this acquisition. A new CEO has been named. A first version of a cloud-based centralized management solution was launched in February 2017. The vendor has also released a threat intelligence service (ScoutIQ).

Untangle is a good candidate for small and lower-midsize organizations, especially in North America. Upper-midsize organizations should evaluate their functionality and scaling needs against Untangle's capabilities.

STRENGTHS

Sales execution: Untangle offers a free version of its UTM, delivered as a software appliance, which is popular among the smaller offices and for remote workers. Every application, including security features, is available for a 14-day trial.

Capabilities: Several clients and resellers cite ease of implementation, interface flexibility and the quality of the numerous embedded reports as the key reasons to work with Untangle.

Customer experience: As in previous evaluations, vendor support gets great scores and some of the most positive comments from customers and resellers surveyed for this research. Its dynamic community also provides useful resources for newcomers.

Improvements: Untangle has improved its user interface with its latest version. Its value proposition for central management is progressing, with the recent addition of a first version of its cloud-based global control, which started with centralized device monitoring. The availability of a threat intelligence service is a good addition for Untangle's target customers that are concerned about malware campaigns.

Marketing execution: Untangle can be offered as software, to be installed on standard hardware. It serves its channel of smaller resellers and is useful for organizations willing to evaluate the product.

CAUTIONS

Market segmentation: Gartner estimates that more than 90% of Untangle's UTM customers have fewer than 500 employees. A large majority of its clients are U.S.-based. Its approach of cloud-centralized management is promising, but it is not yet feature-complete, which prevents Untangle from addressing distributed organizations and large MSSPs.

Marketing execution: Untangle does not offer 24/7 support, nor other enterprise-class support options that upper-midsize organizations and large resellers want. Its products have not received any certifications. Untangle has less experience with hardware appliance sales than its direct competitors.

Organization: Untangle remains one of the smallest vendors evaluated in this research, with fewer than 100 employees. This can impact the vendor's ability to devote resources to grow and innovate with market needs.

Capabilities: Untangle's largest physical appliances offer a throughput of 2 Gbps only. It has limited policy verification features and lacks role-based management. It also lags behind its competitors for advanced networking features.

Capabilities: Untangle lacks cloud-based sandboxing. It does not offer any dedicated monitoring for SaaS inventory and monitoring.

Venustech

Venustech is a Niche Player. Its visibility in SMB shortlists is limited to China and Japan. Venustech is a long-established security player in China and offers the foundational UTM features in its UTM series, but has some gaps to fill compared with its competitors.

Headquartered in Beijing, China, Venustech has a large product portfolio, which includes web application firewall, SIEM, endpoint security, vulnerability scanner and IDS, along with firewalls for SMBs and enterprises (Venusense UTM).

Venusense UTM is a good candidate for existing Venustech customers in China, and for SMBs that are looking for a good local vendor with strong regional support in China as well as a cost-effective UTM offering.

STRENGTHS

Capabilities: Venustech is one of the few UTM vendors offering granular DLP for both email and web traffic. It also offers outbound email encryption, which is not offered by many UTM vendors in the market and strengthens its email filtering feature.

Capabilities: Surveyed VARs and clients highly rate the IPS feature of Venusense UTM, and mention it as one of the top features.

Capabilities: The application control feature has a large database of applications, including Chinese applications such as Youku, TongHuaShun and LeTV, which makes it a desirable vendor as compared to other international vendors that lack local applications in their databases.

Technical support: Vendor technical support has received positive reviews and is cited as responsive. The majority of customers opt for direct vendor support and are very satisfied with it.

Sales strategy: Venustech licensing is pretty straightforward and follows a bundled pricing model for both support and maintenance. It offers its software subscription free of charge for the first year. It has dedicated firewall models for China and other models for the international market.

CAUTIONS

Geographic strategy: Venustech does not have any presence outside China, except for a limited presence in Japan.

Sales strategy: The international version of its low-end Venusense UTM is priced significantly higher than the competition.

Capabilities: Venusense UTMs cannot decrypt HTTPS or other TLS-encrypted traffic. The cloud-based sandboxing is unproven and has not yet been part of any independent test.

Technical architecture: The vendor lacks a cloud-based management portal for managing multiple UTMs, especially for a distributed-office use case. Venustech addresses this use case by hosting virtual appliances of its centralized management software.

IaaS: Venusense UTM is not available as an instance on any public clouds, which compels organizations to go with a different UTM vendor for their cloud environments.

Capabilities: Venusense UTMs lack support for monitoring and managing SaaS applications, which is provided by some of Venustech's competitors and is a desirable feature for SMBs that are adopting more SaaS applications.

WatchGuard

WatchGuard is in the Visionaries quadrant. It continues to drive an ambitious roadmap while growing its customer base at pace with the overall market. WatchGuard's product vision and roadmap execution have slightly improved relative to those of some competitors.

Based in Seattle, Washington, WatchGuard is a privately held network security vendor that is over 20 years old, has more than 500 employees and is well-established in the multifunction firewall market. It provides SMB and enterprise firewalls, secure email gateways, endpoint security, and wireless APs. The Firebox UTM product line includes 15 physical appliances, some of which with embedded wireless capabilities. WatchGuard offers virtual appliances, including XTMv, FireboxV and Firebox Cloud, for public cloud deployment.

Recent WatchGuard news includes the introduction of the Threat Detection and Response (TDR) capability, which uses a cloud-based threat scoring engine to correlate events seen in the network or on the endpoint. The endpoint presence is enabled by the WatchGuard Host Sensor, technology which came from the acquisition of Hexis HawkEye.

WatchGuard is a good shortlist candidate for SMB organizations and distributed enterprises in need of a broad set of security and infrastructure features, or a cloud-based visibility and management console.

STRENGTHS

Product strategy: Midmarket customers like the free endpoint threat detection software packaged with the Firebox UTM. While the offer is still new, it will potentially benefit limited-budget midsize customers looking to detect and stop active threats in the network.

Capabilities: WatchGuard customers and partners value highly the simplicity and depth of the reporting and analysis capabilities of WatchGuard Dimension. For example, the WatchGuard Dimension reporting tool includes an interactive heat map view (FireWatch) that is useful for quickly identifying network issues created by a specific user or application.

Customer experience: Overall ease of use is an oft-cited positive attribute noted by WatchGuard stakeholders. They cite ease of implementation, ease of policy setup and a low rate of false positives as examples.

Geographic strategy: WatchGuard has a global presence across regions and continues to grow its already-large channel presence.

Capabilities: WatchGuard's customers and resellers report that WatchGuard UTM performs well under load with all features enabled.

CAUTIONS

Product strategy: WatchGuard has lagged behind competitors in public cloud firewall development and deployments. The vendor released Firebox Cloud for AWS in the first quarter of 2017, but has yet to release a version for Microsoft Azure.

Sales strategy: The WatchGuard channel comprises a lot of smaller resellers. Prospective clients should ensure that the appropriate technical expertise for WatchGuard is available.

Sales execution: Gartner midsize clients do not mention WatchGuard in their shortlists as frequently as they mention Leaders.

Customer experience: Some surveyed WatchGuard stakeholders mention longer-than-average time lags between the time an issue is reported and the time they receive a response.

Product execution: WatchGuard customers report that Threat Detection and Response is not fully integrated with WatchGuard Dimension.

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

No vendor was added. Dell SonicWall is now SonicWall, after the split from Dell.

Dropped

Aker Security Solutions did not meet the revenue criteria. The vendor does most of its business in Brazil, and the local currency negatively impacted the vendor's ability to meet the criteria.

Inclusion and Exclusion Criteria

Inclusion Criteria

UTM companies that meet the market definition and description were considered for this report under the following conditions:

They shipped UTM software and/or hardware products — targeted to midsize businesses — that included capabilities in the following feature areas at a minimum:

Network security (stateful firewall and intrusion prevention)

Web security gateway

Remote access for mobile employees (VPNs)

Email security

They achieved UTM product sales (not including maintenance or other service fees) of more than $9 million in 2016, and within a customer segment that's visible to Gartner. They also achieved this revenue on the basis of product sales, exclusive of managed security service (MSS) revenue.

The vendor can provide at least three reference customers willing to talk to Gartner, or Gartner has had sufficient input from Gartner clients on the product.

Exclusion Criteria

There was insufficient information for assessment, and the company didn't otherwise meet the inclusion criteria or isn't actively shipping products yet.

Products aren't usually deployed as the primary, internet-facing firewall (for example, proxy servers and IPS solutions).

Products are built around personal firewalls, host-based firewalls, host-based IPSs and web application firewalls — all of which are distinct markets.

Solutions are typically delivered as a managed security service (MSS), to the extent that product sales did not reach the $9 million threshold.

In addition to the vendors included in this report, Gartner tracks other vendors that did not meet our inclusion criteria because of a specific vertical market focus, UTM revenue and/or competitive visibility levels. These vendors include Aker Security Solutions, Cato Networks, Endian, GajShield, ilem Group, My Digital Shield, Netgear, North Coast Security Group, Quick Heal, Sangfor Technologies, SecPoint, Secucloud, Secui, Smoothwall and ZyXEL.

Evaluation Criteria

Ability to Execute

Product or Service: Core goods and services that compete in and/or serve the defined market. This includes current product and service capabilities, quality, feature sets, and skills. Key features that are weighted heavily include:

Ease of deployment and operation

Console quality

Price/performance

Range of models

The ability to support multifunction and distributed organization deployments

Secondary product capabilities (such as logging, SaaS and mobile device management, integration with endpoint, integrated Wi-Fi support, and remote access)

Overall Viability: This includes a vendor's overall financial health, prospects for continuing operations, company history, and demonstrated commitment to the multifunction firewall and network security market. Growth of the customer base and revenue derived from sales are also considered. All vendors are required to disclose comparable market data, such as multifunction firewall revenue, competitive wins versus key competitors (which is compared with Gartner data on such competitions held by our clients) and devices in deployment. The

number of multifunction firewalls shipped isn't a key measure of execution. Instead, we consider the use of these firewalls and the features deployed to protect the key business systems of Gartner midsize business clients.

Sales Execution/Pricing: This includes, the number of deals, visibility in shortlists, the installed base, and the strength of sales and distribution operations in the vendors. Presale and postsale support are evaluated. Pricing is compared in terms of a typical midsize business deployment, including the cost of all hardware, support, maintenance and installation. Low pricing won't guarantee high execution or client interest. Buyers want value more than they want bargains, although low price is often a factor in building shortlists. The total cost of ownership during a typical multifunction firewall life cycle (which is three to five years) is assessed, as is the pricing model and bundling approach for adding security safeguards. In addition, the cost of refreshing the products is evaluated, as is the cost of replacing a competing product without intolerable costs or interruptions.

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 to changing market demands.

Marketing Execution: The clarity, quality, creativity and efficacy of programs designed to deliver the organization's message in order to influence the market, promote the brand, increase awareness of products and establish a positive identification in the minds of customers. This "mind share" can be driven by a combination of publicity, promotional, thought leadership, social media, referrals and sales activities.

- We also recognize companies that are consistently identified by our clients and often appear on their preliminary shortlists.

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

- 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. These also include management experience and track record, and the depth of staff experience — specifically in the security marketplace. Gartner analysts also monitor repeated release delays, frequent changes in strategic directions and how recent organizational changes might influence the effectiveness of the organization.

Table 1. Ability to Execute Evaluation Criteria

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

Source: Gartner (June 2017)

Completeness of Vision

Market Understanding: Ability to understand customer needs and translate them into products and services. We consider how vendors show a clear vision of their market — listen, understand customer demands, and can shape or enhance market changes with their added vision. These include providing a track record of delivering on innovation that precedes customer demand, rather than an "us, too" roadmap and an overall understanding and commitment to the security market (specifically the SMB network security market).

- 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. Vendors can't merely state an aggressive future goal. They must enact a plan, show that they're following it and modify the plan as they forecast how market directions will change.

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

  Sales Strategy: A sound strategy for selling that uses the appropriate networks, including indirect sales and channel management, marketing, service, and communication. We look at partners that extend the scope and depth of market reach, expertise, technologies, services and their customer base. This also includes preproduct and postproduct support, value for

pricing, and clear explanations and recommendations for detection events and deployment efficacy. Building loyalty through credibility with a full-time midsize business security and research staff demonstrates the ability to assess the next generation of requirements.

Offering (Product) Strategy: The emphasis is on the vendor's product roadmap, current features, leading-edge capabilities, virtualization and performance. The quality of the security research labs behind the security features is considered. Credible, independent third-party certifications, such as Common Criteria, are included. Integration with other security components is also weighted, as well as product integration with other IT systems. As threats change and become more targeted and complex, we weight vendors highly if they have roadmaps to move beyond purely signature-based, deep-packet inspection techniques. In addition, we weight vendors that add mobile device management to their offerings and are looking to support SMB organizations that use cloud-based services.

Business Model: The design, logic and execution of the organization's business proposition to achieve continued success. This includes the process and success rate of developing new features and innovation, and R&D spending.

Innovation: This includes product innovation, such as R&D; quality differentiators, such as performance, virtualization, and integration with other security products; a management interface and clarity of reporting.

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. These include the ability and commitment to service geographies, such as distributed multinational organizations deployments and MSSPs.

The more a product mirrors the workflow of the midsize-business operations scenario, the better the vision. Products that aren't 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 category. Reducing the rule base, offering interproduct support and beating competitors to market with new features are most important.

Table 2. Completeness of Vision Evaluation Criteria

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

Vertical/Industry Strategy	Not Rated
Innovation	High
Geographic Strategy	Low

Source: Gartner (June 2017)

Quadrant Descriptions

Leaders

The Leaders quadrant contains vendors at the forefront of making and selling UTM products that are built for midsize-business requirements. The requirements necessary for leadership include a wide range of models to cover midsize-business use cases, support for multiple features, and a management and reporting capability that's designed for ease of use. Vendors in this quadrant lead the market in offering new safeguarding features and in enabling customers to deploy them inexpensively without significantly affecting the end-user experience or increasing staffing burdens. These vendors also have a good track record of avoiding vulnerabilities in their security products. Common characteristics include reliability, consistent throughput, and products that are intuitive to manage and administer.

Challengers

The Challengers quadrant contains vendors that have achieved a sound customer base, but they aren't leading with features. Many Challengers have other successful security products in the midsize world and are counting on the client relationship or channel strength, 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 product bundles that others can't. Many Challengers hold themselves back from becoming Leaders because they're obligated to set security or firewall products as a lower priority in their overall product sets.

Visionaries

Visionaries have the right designs and features for the midsize business, but lack the sales base, strategy or financial means to compete globally with Leaders and Challengers. Most Visionaries' products have good security capabilities, but lack the 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. Where security technology is a competitive element for an enterprise, Visionaries are shortlist candidates.

Niche Players

Most vendors in the Niche Players quadrant are enterprise-centric or small-office-centric in their approach to UTM devices for SMBs. Some Niche Players focus on specific vertical industries or geographies. If SMBs are already clients of these vendors for other products, then Niche Players can be shortlisted.

Context

SMBs have significantly different network security requirements from those of large enterprises, due to different threat environments, different business pressures and different levels of staffing. Although the branch offices of some larger enterprises have requirements that are similar to midsize businesses, this is not always the case. The UTM market consists of a wide range of suppliers that meet the common core security requirements of SMBs, but businesses need to make their decisions by mapping their threat and deployment patterns to optimal offerings.

Market Overview

The market for multifunction SMB firewalls (still also known as UTM) is mature and sees heavy competition regardless of region. The market growth is leveling out and becoming closer to the other network security markets.

> For 2016, Gartner estimates that the UTM market grew at 12.7% to reach a total of approximately $2.3 billion.

Fortinet continues to own the largest market share in the UTM market (see Note 2) — with more than twice the revenue of its closest competitors, SonicWall, Check Point Software Technologies and Sophos— and grows much faster than the market average (see "Market Share Analysis: Unified Threat Management (SMB Multifunction Firewalls), Worldwide, 2016").

The last Magic Quadrant for UTM was published in August 2016. This evaluation period for this research was a bit shorter, to align publication date with the enterprise network firewall Magic Quadrant.

Based on the customer research survey for this Magic Quadrant (which aligns with Gartner inquiry except for firewall features, see Note 3), the most common features deployed on a UTM are:

- Firewall (90% — however, based on inquiry, we observe a number close to 100%)
- URL filtering (77%)
- IPS (70%)
- Web antivirus (51%)
- IPsec (63%) and SSL (46%) VPN
- Application control (46%)
- User control (41%)
- Anti-spam (41%)
- Quality of service (41%)

Will UTM Become a Meta-Security Platform?

Leading vendors create new marketing messages after they attempt to convert a point product into a meta-security platform, positioned at the edge of the corporate network, but tightly integrated with other security solutions and cloud services. First integrations are with endpoint solutions, often limited to the solution from the firewall vendors, with the promise of a unified monitoring dashboard and flexible security policy based on endpoint posture assessment. Some vendors offer integrated management of wireless access points, extending visibility to the wireless networks. More vendors have added a SaaS discovery report, allowing SMB to inventory unmanaged SaaS. The next step is tighter integration between the firewall and the SaaS offerings frequently seen in SMBs, such as Office 365 or file-sharing services, to improve monitoring and control options. Direct integration with a CASB could be another option. The CASB market is quickly growing, and the panel of features that CASB vendors offer larger enterprises is more comprehensive than what UTM vendors can easily provide (see "Market Guide for Cloud Access Security Brokers").

Midsize organizations have smaller teams, and therefore face lower organizational friction than larger enterprises. They use channel partners more frequently for implementing security solutions. This combination of criteria makes it easier to envision the integration of multiple security solutions. Prospective customers of the integrated approach should conduct a separate evaluation of each considered technology, and only then evaluate the benefits of the integrated approach. These more complex evaluation procedures are often out of reach for budget- and resource-constrained SMBs. Midsize organizations will often trust their channel partner. However, channel partners have already built a portfolio of security solutions from different vendors. This could create issues; for example, a firewall vendor may start to promote integration with its own endpoint, whereas the channel partner also sells third-party solutions. Midsize organizations should assess the level of expertise of their channel partners on all the considered solutions, but also try to identify the resellers' biases.

Ease of Use and Price Continue to Drive SMB Purchases

In previous years, the term "unified threat management" was used by vendors and channel partner to convey the notion of good price for value. Most clients and resellers continue to understand UTM as SMB multifunction firewalls, but a majority of vendors have stopped using the UTM name to highlight their platform concept instead. However, SMBs and enterprises continue to have different expectations for their perimeter gateway. SMBs remain focused on total cost of ownership, ease of use and the ability to run multiple security features on a single platform. These differences are one of the major reasons why many of firewall vendors that sell successfully to the enterprise and SMB markets develop specific features for each market. With a few exceptions, multifunction SMB products and larger enterprise firewalls might compete for the same budget, as explained in "Next-Generation Firewalls and Unified Threat Management Are Distinct Products and Markets."

Many vendors evaluated in this research continue to focus more on distributed organizations made of autonomous offices, such as franchises. They invest more in cloud-based centralized management consoles, aimed at serving MSSPs and channel partners looking to automate

repetitive provisioning and deployment tasks. Some vendors already offer zero-touch deployment, relying on firewall appliances in default factory settings' ability to touch base with cloud management to get its prepared configuration.

Ransomware and Encrypted Traffic Are Top Challenges for SMBs

SMB organizations face a growing need for SSL decryption, principally to enforce web-filtering policies and to prevent malware infection. In "Predicts 2017: Network and Gateway Security," Gartner anticipates that through 2019, more than 80% of enterprises' web traffic will be encrypted. Consequently, a growing number of malware attacks, including ransomware, will move to use HTTPS to covert initial infection and command and control communications.

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

Decrypting SSL/TLS on a UTM creates organizational issues, such as ensuring an employee's right to privacy, and technical challenges, such as performance issues and product sizing difficulties for the firewall channel. End-user experience is likely to be affected, too. Some application traffic cannot be decrypted, and firewall vendors do a poor job at providing an up-to-date list of exceptions, leading to blocked traffic. In our client reference survey for this Magic Quadrant (see Note 3), despite the self-evaluation bias that generally results in inflated numbers, and the fact that references provided by vendors tend to use more features than the market average, only 32% of the respondents answered that they were decrypting HTTPS traffic.

The fear of ransomware infection drives the adoption of cloud-based sandboxing subscriptions. The promise of automated quarantine of infected hosts triggers additional interest from SMBs to integrate the endpoint with the network firewall.

The End of the Thick "All-in-One" Physical Appliance Era Is Slowly Approaching

More UTM providers now target distributed organizations that have needs similar to those of midsize organizations. This includes MSSPs for SMBs and distributed enterprises such as retailers, healthcare organizations and small government agencies. Despite centralized purchase and maintenance centers, each office is similar to an autonomous organization.

Placing the management and monitoring consoles fully in the cloud is generally a first step. MSSPs like the turnkey solution, but end-user organizations should evaluate whether hosting their firewall configuration, including the filtering policy, in the cloud is acceptable. Reporting and log retention are well-suited to the cloud, but not exclusively. More frequent user interface updates are also a real advantage to the cloud. From an economic perspective, utilizing a cloud management solution should at least minimize management costs. In Gartner client surveys (see Note 3 consideration about self-evaluation bias), when asked about future scenarios for their UTM purchase:

- 29% are likely (15%) or very likely (14%) to consider a cloud-based management console

15% are likely (11%) or very likely (4%) to consider a cloud-based secure web gateway

14% are likely (8%) or very likely (6%) to consider moving all the security features to a firewall as a service (FWaaS) solution

Due to the increasing share of encrypted traffic, Gartner analysts hear more frequently from distributed organizations, but also from upper-midsize organizations, that they consider shifting and lifting web security features from the edge firewall to a cloud-based secure web gateway to reduce their dependency on the appliance. As more vendors will offer direct integration with their own cloud-based secure web gateway, or one from a third-party vendor, this will become a valid option for most organizations, even if the privacy and residency challenges could slow down adoption in some regions.

WAN edge infrastructure is also changing rapidly, with the growth of SD-WAN and virtualized customer premises equipment (vCPE) platforms in branches (see "Market Guide for WAN Edge Infrastructure"). These thinner on-premises approaches could increasingly compete with UTM vendors' offerings, and both markets could ultimately merge, with security workloads transferred to a cloud infrastructure.

Gartner first added firewall as a service to the "Hype Cycle for Infrastructure Protection, 2016." (https://www.gartner.com/document/3367417) Gartner defines FWaaS as follows:

> Firewall as a service (FWaaS) is a firewall delivered as a cloud-based service or hybrid solution (that is, cloud plus on-premises appliances). The promise of FWaaS is to provide simpler and more flexible architecture by leveraging centralized policy management, multiple enterprise firewall features and traffic tunneling to partially or fully move security inspections to a cloud infrastructure.

The promise, especially for distributed organizations and MSSPs, is to better manage complexity and reduce dependency on thick on-premises hardware such as UTM.

> It took eight years for cloud-based secure web gateways to represent 27% of the total market. Based on today's level of interest, the transition to the cloud could take more time for UTM.

Gartner believes that, although it's convenient for the vendors to do so, a portion of the SMB market will not accept this exclusively cloud model due to latency and the need to access the console when under attack. In some regions and industry verticals, limited trust in a foreign supplier and other privacy concerns would be additional reasons to avoid the cloud model.

Note 1
Small or Midsize Business Market Definition

Gartner generally defines SMBs by the number of employees and/or annual revenue they have. The primary attribute used most often is the number of employees. Small businesses usually have fewer than 100 employees, while midsize businesses are usually defined as companies with between 100 and 1,000 employees. The secondary attribute used most often is annual revenue. Small businesses are usually defined as those with less than $50 million in annual revenue, while midsize businesses are defined as those with less than $1 billion in annual revenue. Typically, 80% of the companies that Gartner analysts speak with have between 100 and 999 employees, and revenue of $100 million to $500 million (see "Gartner's Small and Midsize Business Market Definition, 2013 Update").

Note 2
UTM Revenue Differentiation

Gartner does not include branch office firewall revenue as UTM revenue. The market size and growth are estimated compared with numbers from the previous UTM Magic Quadrant.

Note 3
Customer and Reseller Survey

In addition to hundreds of end-user inquiries about firewall that Gartner analysts conduct every year, Gartner surveys its clients, but also end-user references and reseller references submitted by vendors.

Self-evaluation surveys tend to give inflated numbers compared to reality, and numbers should not be taken literally. When results are included in this research, it is because they accurately reflect how the different answers rank, and the general trends.

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.