Magic Quadrant for Unified Threat Management (SMB Multifunction Firewalls)

SMB multifunctional firewalls, or UTM, provide multiple security features in a single appliance to SMB and distributed enterprises. Security and risk management leaders should use this research to select the right vendor based on their requirements and geography.

Strategic Planning Assumptions

By 2023, 30% of small and midsize organizations selecting firewalls for new deployments will choose to select firewalls with mature endpoint correlation capabilities for better advanced threat prevention, up from less than 5% today.
By 2023, 50% of new firewall purchases in distributed enterprises will utilize SD-WAN features, up from less than 20% today.
By 2023, 10% of new distributed branch offices firewall deployment will switch to firewall as a service, up from less than 2% today.

Market Definition/Description

Gartner defines the unified threat management (UTM) market as multifunction firewalls used by small and midsize businesses (SMBs). Typically, midsize businesses have 100 to 1,000 employees.
UTM vendors continually add new functions on UTM platforms, and therefore, they encompass the feature set of many other network security solutions, including:

- Firewall
- Intrusion prevention systems (IPSs)
- VPN
- Secure web gateway (SWG)
- Centralized management console
- Advanced malware detection

Browser-based management, ease of configuration, embedded reporting, VPN, localized software, excellent partner support 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 network security features and are optimized for very different selection criteria. Small businesses with fewer than 100 employees have even more budgetary pressures and even fewer security pressures than larger organizations. Most security procurement

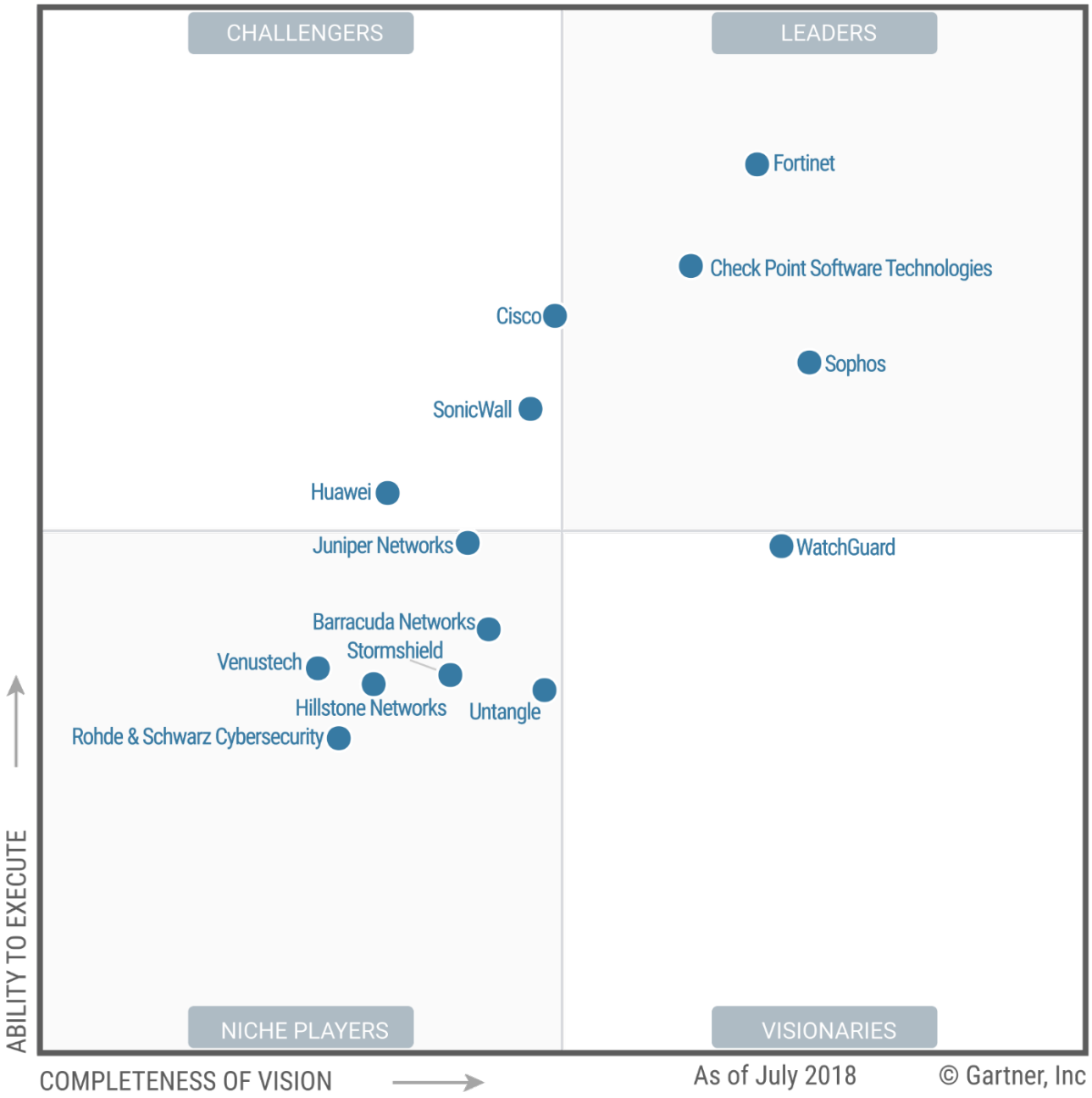
decisions are driven by nontechnical factors and rarely by competitive feature comparisons.

For these reasons, this Magic Quadrant focuses on the UTM products used by midsize businesses. 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 by getting larger discounts from their firewall vendors. For these reasons, Gartner allocates branch office firewall revenue to the enterprise firewall market, not the UTM market. 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 (September 2018)



Vendor Strengths and Cautions

Barracuda Networks

Barracuda Networks is evaluated as a Niche Player. Although the vendor has improved its visibility in other regions, it is still low, compared with its competitors in the UTM market in North America and the Asia/Pacific (APAC) region. Barracuda demonstrates consistent growth and has made progress in its advanced threat detection. The vendor continues to focus on public IaaS deployments and distributed enterprise use cases, where it has a majority of its client base.
Barracuda Networks, headquartered in Campbell, California, delivers network security, backup and infrastructure solutions. Barracuda continues to sell two separate product lines of firewalls, NextGen Firewall X-Series and CloudGen Firewall F-Series with differences in feature set, but is working toward consolidating both series, gradually stopping sales of the

X-Series and focusing on F-Series as its only firewall product line. The F-Series also comprises a virtual appliance with a full set of features, differentiated by only throughput capacity. CloudGen Firewall can be centrally managed via Barracuda Firewall Control Center, virtual and cloud-based (on Amazon Web Services [AWS], Microsoft Azure and Google Cloud).
Recent updates include a technology alliance to deliver security through the use of cloud-based solutions, such as a browser-based "unified workspace" with Awingu. Also, new appliance models were introduced in 2017, with an embedded DSL modem web interface.
Barracuda Networks is a good candidate for distributed SMBs looking for UTM, with strong VPN and better software-defined WAN (SD-WAN) capabilities. It is a favorable vendor for public IaaS deployments with support for multiple IaaS platforms and high quality of support.

Strengths

- **Sales Execution:** Barracuda F-Series UTM has a good presence on public IaaS platforms. It offers support for Microsoft Azure, AWS, VMware vCloud Air, Google Cloud Platform, and ProfitBricks, and plans to expand this to other public IaaS platforms.

- **Product Strategy:** Barracuda UTM has different levels of certifications: ICSA Labs (Advanced Threat Defense Certification Testing), FIPS 140-2 Level 1 (cryptography compliance for VPN) and AWS Competency. The AWS Competency Program is designed for partners that have demonstrated technical proficiency and proven customer success in specialized solutions, although its firewalls still lack Common Criteria certification.

- **Capabilities:** Barracuda VPN is rated high and considered the biggest strength of the product. Barracuda's Transport Independent Network Architecture (TINA) VPN client for Windows, macOS and Linux is included free with the base license. Barracuda also offers a strong sandboxing feature called Barracuda Advance Threat Protection in partnership with Lastline.

- **Customer Experience:** Surveyed customers and resellers continue to mention support as a strong reason to continue working with Barracuda. This includes, as a part of the basic firewall subscription, free direct basic support over the phone with a Barracuda technical assistance center (TAC).

- **Pricing Model:** Barracuda's pricing model is easy to consume, where most Barracuda firewall features like intrusion prevention system (IPS), link balancing, VPN, URL filtering and centralized management (Barracuda provides Barracuda Cloud Control [BCC] at no additional charge) are included. Components sold separately are Malware Protection, Advanced Threat Detection and Advanced Remote Access.

Cautions

- **Product Strategy:** Barracuda still maintains two separate firewall product lines — the X-Series and F-Series. There is difference in their functionalities. The cloud management portal supports only the X-Series and lacks support for the F-Series.

- **Integration:** Barracuda UTM does not integrate with cloud access security brokers (CASBs). Barracuda does not offer endpoint solutions, and its firewalls do not offer a built-in integration with third-party endpoint protection solutions. Customers planning to integrate with third-party endpoint protection platform (EPP) solutions need to use REST APIs.

- **Capabilities:** Customers willing to simplify on appliance management and having a consistent set of features across all appliance should use F-Series. Some low-end X-Series appliances do not support dynamic routing protocols. Also, Barracuda utilizes different central management for F-Series (Barracuda Firewall Control Center) and X-Series (Barracuda Cloud Control). Two management interfaces create some confusion for customers looking to reduce the number of consoles to administer other Barracuda components (web application firewall [WAF], SWG and secure email gateway [SEG]) that use BCC.

- **Sales Strategy:** Although Barracuda has improved its visibility as the end-user installed base in some regions of North America and APAC, Gartner rarely sees Barracuda being shortlisted in these regions.

- **Customer Experience:** Surveyed customers have stated that on-appliance email filtering features and on-appliance reporting capabilities need to be upgraded and improved. The on-appliance email filtering also lacks end-user quarantine and support for POP3 emails.

Check Point Software Technologies

Check Point Software Technologies is evaluated as a Leader as it continues to have one of the largest UTM market shares. The vendor offers a complete set of features with a strong geographic strategy through distributed regional offices in different geographies and channels, along with support for multiple local regional applications and data loss prevention (DLP) data types.
Check Point is a pure-play global security vendor headquartered in Tel Aviv, Israel and San Carlos, California. Its product portfolio includes network security, endpoint protection, mobile threat defense and cloud security product lines. Its UTM and firewall product line is called Check Point Security Gateways.
Major news updates include launch of CloudGuard SaaS, which is its threat detection offering for SaaS. They also include the release of firmware R80.10 and the rebranding of its vSEC product offering as CloudGuard IaaS, extending support for AWS, Google Cloud Platform, Microsoft Azure, Microsoft Azure Stack, Oracle Cloud and Alibaba Cloud.
Check Point UTM solutions are a good candidate for SMBs who are looking for mature, on-premises, centralized management capabilities with strong UTM features and in-depth anti-ransomware and DLP capabilities.

Strengths

- **Product:** Check Point continues to focus on enhancing its threat prevention technologies such as anti-ransomware and CPU-level emulation capabilities. It does this by introducing early detonation technology, and a document and image extraction (CorelDRAW Image file) capability to improve prevention of zero-day exploits in web objects such as Adobe Flash objects.

- **Capabilities:** The URL filtering feature of Check Point allows “inform” and “ask” actions, in addition to basic “allow” and “deny” end-user actions. This enables users to explain the reason to access a particular website and also an enterprise to educate its users about the website.

- **Capabilities:** Check Point Security Gateways have granular, network-based DLP as a separate module with more than 700 premade data types for web traffic, FTP and email traffic. This feature can be utilized by SMBs that are looking for enhanced DLP capabilities with additional cost. With R80.10, Check Point also introduced a Content Awareness Software Blade that provides visibility and control over data transfers in the network traffic, using data types based on content, file type, and direction that doesn’t require a DLP license.

- **Vertical Strategy:** Check Point has a separate SMB-focused strategy with multiple UTM appliances. The models 700 and 1400 support internet, VDSL and 4G/LTE interfaces offering built-in routing capabilities to the enterprises. Check Point has strong partnerships with leading global and regional managed security service providers (MSSPs) that have good penetration in the SMB market. It also has partnerships with ISPs to offer security as a service to both of their customers.

- **Geographic Strategy:** The vendor has a strong geographic strategy with multiple regional offices and channel partners globally. It has regional TACs in Japan, China, India and Australia, as well as global TACs.

Cautions

- **Market Responsiveness:** Check Point has been quite slow in introducing new features that resonate with the SMB market for its UTM requirements, such as a dedicated SD-WAN feature and cloud management portal support for all the UTM models. It was late in introducing monitoring and threat detection capabilities for SaaS applications, but has now done so with its CloudGuard service.

- **Customer Feedback:** Surveyed clients and resellers have reported that technical support issues take higher resolution time when escalated past Level 1. As a result, advanced support issues take time to be identified and escalated.

- **Product:** In addition to its Security Management Portal (SMP), a centralized cloud management portal, Check Point has multiple different cloud portals such as license renewal portal and zero-touch deployment portal. This leads to multiple disjointed portals to perform different functions instead of the ease of managing from single portal.

- **Capability:** Check Point SMP is only available for 700 and 1400 series and lacks support for other models. SMP also lacks centralized support for other Check Point products such as endpoint protection and mobile threat prevention, and CloudGuard. Hence, it does not give a centralized cloud-based management capability to Check Point customers who have invested in multiple Check Point product lines.

- **Market Execution:** While the integration capability between the UTM and endpoint protection platforms is a desirable feature for small and midsize businesses, Gartner rarely sees clients buying Check Point endpoint protection with the Check Point UTM quotations.

Cisco

Cisco is evaluated as a Challenger and continues to deliver new capabilities through its Meraki MX product line designed for distributed sites, campuses and VPN concentrator. Other than Meraki MX, Cisco also sells Cisco Adaptive Security Appliance (ASA), Cisco ASA with FirePOWER services and Cisco Firepower with low-end appliances for midsize organization or branch office deployments for other SMB use cases.
Cisco is a global network infrastructure and security vendor, headquartered in San Jose, California. Its security portfolio includes firewalls (Firepower and Meraki MX), stand-alone IPS (Firepower), network traffic analysis (Stealthwatch), a secure internet gateway in the cloud (Umbrella) and CASB (Cloudlock). Cisco security solutions also include endpoint (Advanced Malware Protection [AMP] and AnyConnect) and cloud (Umbrella) solutions. Cisco addresses the UTM market through its multiple firewall product lines: MX, ASA, ASA with FirePOWER services and Firepower. Meraki MX products are managed through cloud-based management with SD-WAN capabilities for branch or distributed deployment. Cisco Firepower and ASA address the need for more in-depth security capabilities or the need to integrate with existing Firepower, TrustSec and AMP for endpoints.
Recent updates include Cisco introducing Meraki MX virtual firewall vMX100 for Azure and AWS. Cisco Meraki also released teleworker appliances that deliver 802.11ac Wave 2 wireless connectivity and appliances with 4 Gbps and 6 Gbps of firewall throughput. It also announced collaboration of Cisco Talos (Cisco's threat intelligence research team) with IBM's X-Force (IBM's security research team).
Cisco Meraki is a good shortlist candidate for all SMBs and distributed organizations, especially those looking for a mature, cloud-based management portal for managing and monitoring multiple UTM devices. Cisco ASA and Cisco Firepower are good choices for other small to midsize organization deployment use cases, such as perimeter and internal network segmentation.
Strengths

- **Marketing Execution:** Cisco Meraki MX has improved its visibility in vendor shortlists for distributed enterprises in the North American and European regions. Cisco ASA with FirePOWER services are a good candidate for SMBs looking for low-cost alternatives with mature security features.

- **Offering:** The new collaboration between Cisco Talos and IBM's X-Force will benefit features of the Meraki MX that leverage Talos threat intelligence (such as AMP, Threat Grid file analysis, and the Snort-based IPS).

- **Customer Experience:** Surveyed clients have stated that they like the product provisioning feature offered by Cisco Meraki MX and its simplicity. It allows deployment through branch offices without the need for technical staff at the branch, due to its ability to stage the configuration of the devices in the cloud dashboard before deploying.

- **Centralized Management:** Distributed organization clients appreciate the ability to use Meraki's unified management and monitoring solution for wireless, switches, firewall, site-to-site VPN and mobile device management. Multifirewall configuration is based on templates that can address infrastructure (wired, wireless, site-to-site VPN and firewall) configuration deployments. Cisco offers Cisco Defense Orchestrator, which is its cloud-based centralized management portal for Cisco ASA and Cisco ASA with FirePOWER services firewalls.

- **Capabilities:** Meraki MX implements SD-WAN features that can fail over or load balance the internet, MPLS, and 4G/LTE (by installing a USB modem). Failover and load balancing can be implemented based on performance or Classless Inter-Domain Routing (CIDR)/port numbers. As a result, SMBs looking for basic SD-WAN capabilities with UTM find Cisco Meraki MX a good candidate. It offers mature centralized VPN monitoring and management features, which are highly rated by clients.

Cautions

- **Sales Execution:** Cisco continues to sell multiple firewall product lines for SMBs, namely Cisco Meraki MX, Cisco ASA, Cisco ASA with FirePOWER services and Cisco Firepower. They have feature differences and different licensing models, which often create product and vendor management complexities within the SMBs.

- **Product:** Cisco continues to have different centralized on-premises management UIs for its different firewall products with Cisco Security Manager (CSM), Firepower Management Center (FMC), and a cloud-based management for Cisco Meraki MX. This creates serious management complexity issues for organizations using a mix of products.

- **Product Integration:** Cisco Meraki MX lacks integration with other security products from Cisco such as Cisco Cloudlock (CASB), Umbrella (legacy OpenDNS), and AMP for Endpoints (Cisco's endpoint protection platform).

- **Product Licensing:** Customers that want to combine MX-Series and Z-Series should be aware that the advanced security license (content filtering, web search filtering, Snort-based IPS and AMP) is available only to MX-series.

- **Capabilities:** All Meraki MX firewalls and the smaller Cisco Firepower appliance lack Transport Layer Security (TLS) decryption to inspect employee browsing over HTTPS. Meraki MX also lacks DLP capabilities, SSL VPN and email security, and does not inspect HTTP files for viruses on box, but sends file hashes to the AMP cloud infrastructure to determine if a file is malicious.

- **Customer Experience:** Surveyed clients have highlighted delays in technical support response time for Cisco Meraki MX. They have also stated Meraki's lack of

integration with other Cisco products as a weakness.

Fortinet

Fortinet continues to be a Leader, and leads in UTM market share with a huge margin over other UTM vendors in the market. It also leads in market and sales execution. Expansion of its product portfolio is helping with revenue growth and with winning big deals for midsize businesses that want to consolidate toward a single network security vendor. Fortinet is a network and security player, headquartered in Sunnyvale, California. It is regularly expanding its product portfolio, with recent additions FortiWeb (its web application firewall), FortiMail, FortiSandbox, FortiSIEM and FortiCASB. Its other products in the portfolio cover network security, endpoint security, wireless access points and switches. FortiGate firewalls are still its most popular and largest-selling product.
Recent updates include Fortinet expanding its support to multiple public IaaS platforms including Google, IBM and Oracle. It also introduced its E-Series firewall appliances. Major updates also include the release of FortiOS 5.6 in 2017 and FortiOS 6.0 in August 2018.
Fortinet continues to be visible on the UTM shortlists of SMB customers looking for strong security features with wireless security. It is also a good shortlist option for SMBs that are looking to consolidate toward a single vendor for other network security needs, such as web application firewalls, and security information and event management (SIEM). The vendor is also winning deals where SD-WAN adoption is the main use case.
Strengths

- **Sales Execution:** Fortinet is shortlisted frequently by SMBs, making it one of the top vendors with the largest market share in the UTM market. Fortinet is the most visible UTM vendor on the Gartner clients' shortlist.

- **Market Execution:** Fortinet displays strong market execution by focusing on partnership ties. It has strong partnership ties with multiple key MSSPs globally to support hybrid and traditional product deployment models. Its product strategy has a strong focus on MSSP-favorable features, such as centralized management offering multitenancy and administrative domains, XML/JSON APIs for back-end provisioning, and custom portals.

- **Product:** The integrated wireless controller feature in Fortinet's UTM solution is a strong and desirable feature for SMBs. Fortinet has integrated a full wireless controller into the firewall, thereby enabling management of the wireless network as part of the security solution. This is fully managed by FortiCloud and FortiManager.

- **Capability:** Fortinet offers unified control and management across its multiple product lines through Fortinet Security Fabric and continues to focus on enhancements across the Security Fabric features. This enables existing Fortinet customers using multiple Fortinet products to have central monitoring and control across different Fortinet devices in their networks or across multiple networks.

- **Product Strategy:** Fortinet has extended support for multiple cloud platforms — AWS, Azure, Google Cloud Platform, IBM Cloud, and Oracle Cloud Infrastructure (OCI; both VM and bare metal) — which shows its commitment to and focus on expanding in public IaaS platforms.

- **Offering:** Fortinet offers FortiGuard Industrial Security Service, which provides signature updates for common ICS/supervisory control and data acquisition (SCADA) protocols. This comes as a separate subscription, which can be utilized by SMBs operating these systems.

Cautions

- **Product Strategy:** Fortinet is focusing more on large enterprises and on larger deals involving multiple Fortinet products beyond just a firewall. This has impacted its presales support quality for SMBs. Some Gartner clients have reported poor presales support by Fortinet team, as compared with other leading competitors in the market.

- **Feature:** Fortinet UTM lacks built-in support for end-user email quarantine and email encryption. Clients have to use FortiMail, which is a separate product, to get these features.

- **Product:** FortiCloud, which is its centralized, cloud-based management portal, offers limited capabilities as compared to on-premises management capabilities and lacks granular functionalities.

- **Customer Experience:** Surveyed clients have indicated that major firmware upgrades come with major management UI changes that make firewall administration difficult, and involve a learning curve. They have also highlighted that firmware upgrades are buggy and need better testing before released.

- **Capabilities:** FortiClient for endpoint security offers only partial endpoint detection and response (EDR) feature. FortiCASB provides basic capabilities for SaaS monitoring and control, but lacks integration with FortiManager. Gartner has not seen the inclusion of FortiClient and FortiCASB with the firewall deals.

Hillstone Networks

Hillstone is evaluated as a Niche Player in this Magic Quadrant. This year, it has improved its market and sales execution by closing feature gaps via multiple technology partnerships. It is visible mostly in China with a strong focus on public IaaS platforms. It is showing some growth in Latin America and the Middle East.
Hillstone is a network security player headquartered in Beijing, China with its U.S. headquarters in Santa Clara, California. Its portfolio includes firewalls, network-based IPS (NIPS; S-Series), Server Breach Detection System (sBDS; I-Series) and cloud security solutions (CloudHive and CloudEdge). It also offers Hillstone Security Management (HSM) platform, Hillstone Security Audit (HSA) platform and Hillstone CloudView, a cloud-based security management platform for centralized management and auditing. Its firewall hardware appliances come as E-Series, T-Series and X-Series, has and as virtual firewalls via the CloudEdge product.
Recent updates include Hillstone's introduction of strong integration capabilities with multiple technology partners to close the feature gap in its firewall, such as sandbox integration with Lastline, CASB integration with Cloudscreen and endpoint integration with Jiangmin Technology. Hillstone has also introduced eight E-Series firewall models.

Hillstone is a good shortlist candidate for organizations in China and a few parts of Latin America where it has a skilled channel. Organizations that have hybrid networks and are looking for regional Chinese public IaaS platforms will find Hillstone a favorable option.

Strengths

- **Product Strategy:** Hillstone has a strong public IaaS cloud focus, particularly in China. Its Hillstone CloudEdge product line supports AWS, Azure, Alibaba Cloud globally and regionally. Hillstone CloudEdge supports all major local public clouds in China, such as Tencent Cloud, Jingdong Cloud, Huawei Cloud, Inspur Cloud and Sugon Cloud. As a result, it has a good presence in public IaaS platforms in China.

- **Market Responsiveness:** Hillstone has made major enhancements to fill the feature gaps in its firewalls with the introduction of anti-spam and DLP capabilities as features for SMB organizations. It has also released sandbox integration with Lastline, CASB integration with Cloudscreen and endpoint integration with Jiangmin, with which it also partners.

- **Product:** In addition to basic network security controls, such as antivirus and IPS, Hillstone offers advanced threat detection (ATD), abnormal behavior detection (ABD) and reputation detection features to detect advanced malwares in its firewalls. The abnormal behavior detection engine can perform network traffic analysis and identify abnormal behavior. ABD and ATD come as a combined subscription.

- **Capability:** Hillstone firewalls and intuitive reporting capabilities with interactive features are popular with end users. The cyber kill chain display map helps customers understand the malware activity and take action easily. Survey customers and resellers have cited kill chain display as a strong reporting feature.

- **Customer Feedback:** Hillstone firewalls offer good price-versus-performance value to customers and resellers, which has been highlighted as a strong product feature.

Cautions

- **Capability:** Hillstone lacks centralized management capabilities for its cloud management portal CloudView. CloudView features are more focused on offering centralized monitoring and alert functions. This limits its CloudView offering to only reporting and logging, with a lack of administration capabilities.

- **Product:** Hillstone sells different firewall model series, namely E-Series, X-Series, T-Series and the CloudEdge series for cloud platforms. These different series have multiple feature disparities creating buying confusion for the client base. For example, E-Series lacks anti-spam and support for StoneShield, which is Hillstone's advanced threat detection subscription. The T-Series lacks CASB integration.

- **Product:** Despite CASB integration with Cloudscreen, and endpoint integration with Jiangmin, Hillstone still lags in offering strong endpoint and CASB capabilities to the global SMB market, as these are local Chinese vendors with limited capabilities and are client-based. This feature will not be attractive for non-Chinese end users and resellers.

- **Sales Execution:** A majority of Hillstone firewall UTM sales is in China. While Hillstone is focusing on expanding to other regions, such as Europe and Latin America, Gartner does not see Hillstone being shortlisted by many clients outside China.

- **Offering:** Hillstone does not offer on-premises network sandboxing as a separate appliance. This is typically required by clients with sensitive data privacy needs in regions like Europe and the Middle East.

Huawei

Huawei moved to the Challengers quadrant this year, showing strong growth and expansion outside of China. Huawei continues to demonstrate a focus on the needs of SMBs. Its broader portfolio, with a focus on integration capabilities, also helps it to sell firewalls to its existing client base.
Huawei is a global information and communication vendor, headquartered in Shenzhen, China, 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 network division, which offers firewalls and application security products, along with distributed denial of service (DDoS) appliances. Its firewall product line is sold as Unified Security Gateway (USG) for enterprises and Eudemon for carriers. It also has centralized managers — namely Agile Controller, which is Huawei's platform to manage SDNs. Other centralized managers are eSight and SecoManager, while eLog is its centralized reporting platform. It offers Cybersecurity Intelligence System (CIS), which is its separate software-based advanced malware detection product utilizing technologies such as big data analytics and machine learning.
Major new updates include the USG6100 Series, support for Microsoft Azure, and hypervisor support for OpenStack, VMware, FusionSphere, Kernel-based Virtual Machine (KVM), Xen and Hyper-V. It released enhancements around cloud management features and advanced threat detection capabilities. It has also established a new cloud sandboxing service location: Europe.
Huawei's USG firewall is a good shortlist candidate for SMBs that are looking for good price versus performance with multiple features, especially in China, Latin America and Europe. Organizations that are already using Huawei product lines should consider USG for simplicity of single-vendor management and integration capabilities.
Strengths

- **Offering:** Huawei is an established infrastructure vendor with a broad product portfolio, including network, security and storage products. Organizations that want to consolidate toward a single vendor for ease of license management and integration find Huawei able to meet their requirements with multiple product lines.

- **Technical Architecture:** Huawei continues to focus on integration of its products with its centralized managers, Agile Controller and SecoManager. Surveyed clients have highlighted seamless integration of the Huawei firewall with network access control (NAC) controllers using Agile Controller as a strong feature.

- **Product:** Huawei continues to improve advanced malware detection capabilities through CIS, which is its big data analytics and machine learning platform. It integrates with SecoManager and provides centralized visibility of threats. It can be

purchased as a separate software-based product by security conscious enterprises that want on-premises advanced malware detection capabilities.

- **Capabilities:** Huawei USGs have an easy-to-manage appliance GUI. All the security controls can be applied from the firewall policies tab, including granular SSL decryption configuration and a license-managing capability. Its Cloud Access Security Awareness (CASA) feature offers monitoring and control of SaaS applications, proving more visibility and control over cloud-based SaaS applications.

- **Customer Feedback:** Surveyed clients have cited price versus performance as the main factor in selection of Huawei UTMs. They have highlighted that total cost of ownership (TCO) is less compared with other competitors in the market that offer similar feature set. Clients have also highlighted the seamless integration of UTM with Huawei NAC solution (Agile Controller) as a product strength for existing Huawei customers.

- **Sales Execution:** Besides China, Huawei firewalls are also visible on Gartner client shortlists in Latin America and the Middle East. To expand its presence in Europe, Huawei has introduced a European data center for cloud sandboxing services for its European clients.

Cautions

- **Capability:** Huawei's centralized cloud management portal still lags behind other leading firewall vendors. It lacks maturity and offers limited functionalities.

- **Market Responsiveness:** Huawei has been late in providing support for public cloud IaaS platforms. As a result, it has limited presence in the public cloud, with support for Huawei Enterprise Cloud, AWS Marketplace and Microsoft Azure Marketplace.

- **Offering:** Huawei USG firewalls do not support Alibaba Cloud, which leads in market share for public IaaS in China and is quite popular among end users in Asia. However, Huawei has its own IaaS platform, Huawei Cloud, which is one of the top IaaS providers in the region.

- **Customer Feedback:** Surveyed clients have reported that the on-appliance management GUI has not been updated recently and looks dated.

- **Product:** Huawei does not offer an endpoint protection platform for antivirus and advanced malware detection. It does offer support for Jiangmin and McAfee endpoints through its CIS product, which is a separate product. This does not make it a favorable shortlist candidate for organizations that prefer a single vendor of firewall and endpoint for ease of management and better correlation capabilities.

Juniper Networks

Juniper is evaluated as a Niche Player in this year's Magic Quadrant. This year it has introduced many missing features and has also shown small positive growth in UTM revenue after years of declining revenue. Juniper has shown improvement in sales and market execution.

Juniper Networks is a global network infrastructure vendor headquartered in Sunnyvale, California. Its broad product portfolio includes a range of network edge and management devices, routers, switches, SDN and enterprise firewalls (i.e., SRX Series firewalls).
The SRX product line has 15 distinct hardware platform models ranging from the 500 Mbps to the 2 Tbps.
Recent updates include multiple announcements and a commitment by Juniper to fill the missing product and feature gaps in its SRX product line. These updates include introduction of new midrange SRX models, Virtual SRX (vSRX) support for Google Cloud, launch of the on-premises Juniper ATP Appliance (the result of the Cyphort acquisition), and the launch of Juniper Sky Enterprise cloud management portal supporting EX switches and SRX firewalls. Juniper also announced partnerships with NetScope for CASB, Carbon Black for endpoint, Splunk for reporting, VMware for microsegmentation and ForeScout for NAC.
Juniper SRX is a good candidate for SMBs looking for multifunctional firewalls with strong on-box routing, switching and VPN capabilities, as well as existing Juniper networking customers looking for an integrated solution.

Strengths

- **Market Understanding:** Juniper has shown strong commitment to fill the missing product gaps and features in its SRX series. Its major product enhancements include a cloud management portal, integration with Carbon Black, specifically the Cb Response product, on-premises ATP, and improved security orchestration and reporting.

- **Marketing:** Gartner has observed improvement in Juniper's visibility, especially in social media and public forums. As per Gartner's analysis of 2017,Juniper was among the top five SMB firewall vendors discussed and promoted on public online platforms, with its Contrail Security offering being the most discussed topic.

- **Customer Feedback:** Juniper SRX offers strong switching and routing capabilities based on its EX Series and MX Series product lines. Granular quality of service (QoS) and SD-WAN capabilities using Contrail Security features have been rated high by the surveyed clients.

- **Offering:** Juniper SRX offers strong integration of Sky ATP and Juniper ATP Appliance with Carbon Black (specifically the Cb Response product) to offer better correlation capabilities for the detection of advanced malwares. Key features include autoblocking of IPs by SRX, based on the infected hosts list sent by Carbon Black and autoremediate action taken by Carbon Black based on feeds from Sky ATP. Gartner believes this integration to be a positive step by Juniper to address the missing endpoint correlation capability of Juniper SRX.

- **Technical Support:** Juniper's technical support is often rated higher by its clients and partners. They state that the technical support team offers quick resolution, which is one of the vendor's strengths.

Cautions

- **Pricing:** List pricing for Juniper SRX models is relatively higher than many other leading SMB multifunctional firewall vendors in the market. Surveyed resellers have indicated higher price to be a product limitation, which gives an advantage to

competitors in the space that are priced lower.

- **Customer feedback:** Surveyed customers and resellers have indicated that the web-filtering feature of Juniper needs an upgrade as the Forcepoint URL database offered by Juniper lacks ability for the administrator to reclassify URLs. This leads to a lack of customization of content-filtering policies.

- **Offering:** The Sky ATP offering, Juniper's cloud-based, advanced malware detection offering, is not available on SRX300 and SRX320 models, which is a disadvantage for smaller organizations that are using these models and want better advanced malware detection capabilities.

- **Customer Feedback:** Surveyed customers have indicated higher performance impact on the box when multiple security features are enabled, including IPS. The SRX datasheets lack joint throughput values with security features, which other leading vendors offer, and only provide individual throughput values of firewall, IPS, antivirus and VPN traffic.

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. It has 450 employees. Its portfolio includes a multifunction firewall product line, gateprotect UTM+, and a web application firewall (DenyAll Web Application Firewall, via the acquisition of DenyAll in 2017). The gateprotect firewalls are split into three main categories: Unified Line, Extended Line and Specialized Line. The Unified and Extend Lines are designed for SMB and small office/home office (SOHO) use cases. There are a total of 12 appliance models. Also, a wireless LAN (WLAN) module can be added as an optional component. In industrial, Rohde & Schwarz introduced the GP Tough, a hardened appliance.
Recent updates include Rohde & Schwarz Cybersecurity announcing a partnership with Radisys Corporation to deliver networking and security solution for European communications service providers (CSPs).
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

- **Sales Execution:** Rohde & Schwarz Cybersecurity keeps working to improve its coverage for new prospective clients. As a result, the vendor released the GP-U 50 appliance model to be offered as a managed firewall through MSSPs in healthcare. Also, the GP Tough appliance was designed to be used in industrial environments.

- **Capabilities:** Rohde & Schwarz Cybersecurity offers multiengine advanced malware detection capabilities with a built-in anti-malware signature-based engine, a cloud-based machine learning service and a third-party sandbox. It also partners with Webroot for endpoint protection.

- **Improvements:** The revamped gateprotect WebGUI offers easy-to-use capabilities, since most of Rohde & Schwarz Cybersecurity client base is small-to-lower-midsize organizations. The new WebGUI utilizes a visual topology of the network infrastructure, guiding the creation of policy rules and troubleshooting.

- **Capacities:** The Unified and Extended Lines offer a simplified user interface, with features preferred by small and midsize businesses, such as bandwidth control of VPN traffic and Wi-Fi access control, making the management of VPN traffic and Wi-Fi access easier.

- **Customer Experience:** Surveyed customers scored gateprotect very highly for the ease of use of the WebGUI management console and hardware quality.

Cautions

- **Market Segmentation:** Although the gateprotect product line includes models to serve larger organizations, the vendor is not visible on Gartner client shortlists for this segment. The small and lower-midsize organizations from Europe are where most of the vendor's customer base is deployed, and where its channel has experience.

- **Capabilities:** Rohde & Schwarz Cybersecurity lacks ready-to-use reports for SaaS discovery and does not integrate with CASBs. The UTM solutions also lack a centralized cloud-based management portal.

- **Capabilities:** Rohde & Schwarz Cybersecurity offers limited built-in density of Ethernet ports (switching) and lacks integrated management of wireless access points, extending visibility to the wireless networks. However, the higher-end models offer the support of extension modules with a higher number of Ethernet ports, which can be purchased separately.

- **Sales Execution:** Rohde & Schwarz Cybersecurity lacks support for public IaaS deployments, while a majority of its competitors support it.

- **Customer Experience:** Surveyed customers state that reporting on web usage and canned reports are basic and lag behind other competitors.

SonicWall

SonicWall is evaluated as a Challenger based on its market presence and strong SMB focus. This year, SonicWall demonstrated many improvements, enhancements and new partnership ties to catch up with the SMB market requirement, which it had been lacking. This move has made it a strong UTM vendor in the market. SonicWall has also shown strong UTM revenue growth as per Gartner's UTM market share research. SonicWall, headquartered in Milpitas, California, is an independent network security vendor. SonicWall employs more than 1,300 employees worldwide. Since the split from Dell, SonicWall has increased its partner channels through its sales training program on its SonicWall University platform. The SonicWall portfolio includes network security, access control, endpoint security, management, reporting and analytics, web application firewall, and email security product lines.

The latest updates include the announcement of an agreement between SonicWall and SentinelOne, whereby they will combine SentinelOne's endpoint protection with SonicWall's firewall solution. SonicWall also introduced a real-time memory inspection technique into its Capture ATP sandbox service. Multiple products such as Capture Security Center, SonicWave 802.11ac Wave2 access points and Network Security appliance (NSa) series firewall appliances have been released. It has also introduced its virtual appliance series Network Security virtual (NSv).
SonicWall is a good candidate for most SMB use cases, especially for organizations that want cost-effective integrated wireless access managed centrally from within the UTM product.

Strengths

- **Market Execution:** SonicWall has tried to close basic feature gaps in the first quarter of this year. Now it offers virtual appliances supporting public IaaS deployments and additional SSL and deep packet inspection (DPI)-based feature enhancements. It has enhanced its cloud-based management, reporting and analytics portal Capture Security Center (CSC), as well as Capture Client for the endpoints.

- **Product:** SonicWall offers a good set of appliances and access points with consolidated management. SMB clients value the consolidation of network and security capabilities.

- **Customer Experience:** Channel partners and surveyed customers demonstrate high satisfaction with hardware throughput, quality and ease of configuration.
Capabilities: SonicWall firewalls use a multiengine cloud-based sandbox that's based on four different technologies for malware detection. All four engines are delivered together as a unique product offering. This includes recently added Real-Time Deep Memory Inspection (RTDMI) into its Capture ATP sandbox service, to use memory analysis for threat detection.

- **Marketing Strategy:** As part of SonicWall's marketing strategy, it has been working to improve training to its channels across the globe. Its training initiative resulted in net-new partners with similar training as its internal sales team.

- **Capabilities:** SonicWall introduced an endpoint protection offering known as Capture Client as a result of a partnership with SentinelOne. This joint solution can be managed through Capture Security Center, which provides advanced malware prevention based on behavior-leveraging machine learning and malware remediation offering enhanced malware protection capabilities.

Cautions

- **Market Responsiveness:** SonicWall has been late in introducing common UTM features such as enhancements for ease of use, support for endpoint clients and virtual firewall models in the market as compared to other leading UTM vendors. The vendor has yet to prove its ability to lead with new features that resonate with the SMB market.

- **Capabilities:** The user interface has been enhanced with version 6.5. However, the UI still requires a bit more skill and time to configure advanced features that would

be applicable to midsize companies but not small businesses.

- **Capabilities:** At present, SonicWall provides basic SD-WAN capabilities, limited to 4G failover, multi-WAN failover, and fully qualified domain name (FQDN)/policy-based routing.

- **User Experience:** Surveyed customers that value command line interface (CLI) indicate that this capability needs improvement for troubleshooting purposes. Customers indicate it is difficult to find information through logging.

Sophos

Sophos remains a Leader this year because of its strong ongoing focus on enhancing advanced malware prevention capabilities through its firewalls and endpoint platform integration. It continues to be the market leader, offering mature and integrated management, monitoring and visibility capabilities of endpoints through a single console of its UTM offering, which provides ease of management and better prevention against advanced malware.
Sophos is a network and endpoint security vendor headquartered in Abingdon, U.K. Sophos' portfolio includes firewalls (XG Series, the older SG Series and CR series). Sophos has 19 XG models and three Remote Ethernet Devices (RED) models, which are plug-and-play devices for small offices. It still sells its old product lines, the SG and CR firewall Series. It also offers a number of other security solutions for endpoint security, wireless access point (Sophos AP Series), and unified endpoint management (Sophos Mobile). Sophos Firewall Manager (SFM) is the name of the centralized management software, and Sophos Central is the cloud-based centralized management portal for all Sophos security products.
Recent updates include a new version 17 for XG Firewall with enhanced application control leveraging endpoint integration, as well as an update to its Sandstorm cloud sandbox solution with integration from its next-generation endpoint product (Intercept X). Sophos is a good shortlist candidate for SMBs that are looking for multiple integrated features, such as email and web DLP, email encryption, and a web application firewall in their firewall. Sophos is also a good candidate for SMBs looking for strong and mature endpoint integration capabilities within their UTM solutions for ease of management and correlation of events.
Strengths

- **Sales Execution:** Sophos Cloud Firewall Manager is Sophos' cloud-based centralized management solution for partners to manage multiple firewalls across their customer deployments free of charge. The capabilities of Sophos Cloud Firewall Manager include a majority of the features available with the on-premises centralized management offering, which makes it easier for a partner to manage the firewalls.

- **Sales Strategy:** Sophos has a strong channel strategy, with a loyal channel base globally. It conducts regular partner-training and information-sharing programs worldwide. Gartner has seen that this channel has strong confidence in the Sophos team and its sales strategy, especially postacquisition of Cyberoam. Sophos' presales team receives positive reviews for working directly with the clients in regions like India and the Middle East, and is often scored high by customers.

- **Market Responsiveness:** Sophos continues to increase the visibility, detection and response capabilities of advanced threats to meet growing market requirement. It has also made enhancements to existing application control features in the firewalls for better visibility and control. Sophos also acquired Barricade for improving security analytics capabilities, and has integrated the deep learning capabilities of Invincea into its sandboxing product Sandstorm.

- **Product:** Sophos XG Firewalls offer multiple security features within their UTM solution that appeal to SMBs. This includes built-in web application firewalls, DLP-based encryption for emails and strong endpoint integration.

- **Customer Experience:** Surveyed Sophos customers have mentioned strong firewall and endpoint integration as the product's biggest strength, and also have indicated high satisfaction for the malware detection rate. This is because, in addition to traditionally managing the endpoint centrally from within the firewall UI, it has built strong advanced threat monitoring and response capabilities, using its Security Heartbeat feature, which is a part of its Synchronized Security system.

- **Capability:** Sophos has strong ransomware detection capabilities and constantly works toward improving it. Sophos shares threat and health-related intelligence between endpoints and firewalls using its Synchronized Security feature, to correlate and identify compromised systems. This enables the firewall to automatically isolate them to prevent the movement of ransomware. Recently, Sophos has announced Synchronized Application Control, another feature of Synchronized Security that utilizes the endpoint to provide added visibility into network application traffic.

Cautions

- **Product Strategy:** Despite selling three firewall product lines, XG, SG and CR, Sophos continues to focus on enhancing the features of the XG Series. SG and CR Series are still supported by the vendor, and Sophos recently refreshed its SG and XG firewall series. Gartner recommends that clients carefully evaluate the roadmap and firmware updates in case they still want to make new purchases of CR Series and SG Series, because of product familiarity.

- **Customer Feedback:** Gartner has noted declining customer satisfaction, particularly about ease of deployment and management of the XG Series.

- **Capabilities:** Sophos does not offer a dedicated SD-WAN feature and lacks dynamic, application-centric path selection. However, it does offer limited SD-WAN-related features such as QoS, link balancing (based on volume [weight]), sessions, protocol and a source/destination IP/port.

- **Capabilities:** Sophos currently lacks a centralized cloud management portal for end users. It offers Sophos Cloud Firewall Manager, which provides centralized cloud-based management only to its partners.

- **Customer Experience:** Surveyed customers rated Sophos' UTM solution limited in on-box reporting capabilities. Based on customer feedback, the built-in interface of the appliance is very limited. To get better reporting out of all the Sophos platform,

customers need to use iView.

Stormshield

Stormshield is evaluated as a Niche Player. Although the vendor offers a good feature set for SMBs, its visibility continues to be limited to European countries where regional certifications and client references are rated higher. Stormshield is focusing on expanding into other European countries and the Middle East via channel partnerships and by offering support in local languages.
Stormshield, a European infrastructure security vendor, is headquartered in Issy-les-Moulineaux, France. It is a subsidiary of Airbus CyberSecurity. Stormshield's portfolio includes firewalls (Stormshield Network Security), EPP (Stormshield Endpoint Security) and data encryption (Stormshield Data Security). It also sells two separate centralized management products, Stormshield Management Center (SMC) for end users and Stormshield Network Centralized Manager (SNCM) for telcos and large enterprises.
In 2017, Stormshield announced several partnerships to improve General Data Protection Regulation (GDPR) compliance through the use of cloud data sharing (via Oodrive, OneDrive and Dropbox). Also, the alliance with Panda Security is complementary to the Stormshield endpoint security product.
Stormshield is a good shortlist contender for EMEA organizations with a few locations and when local skilled channel support is available. It is a good candidate for defense and government organizations in France that seek local product certification and client references.
Strengths

- **Market Execution:** Stormshield firewalls have multiple regional product certifications (such as EU Restricted, NATO Restricted and ANSSI Qualification), which makes it a favorable shortlist candidate for government organizations, particularly in France. Its recent regulations, such as GDPR, make the vendor a good contender for SMB use cases in the region.

- **Geographic Strategy:** The vendor demonstrates a strong European strategy. It offers documentation and technical support in English, French, Spanish, Italian, Arabic and German. Even the product UI is available in French, English, German, Polish and Magyar. It shows a consistently strong commitment to the European region, with regional product certifications and GDPR compliance.

- **Customer Experience:** Customers have described Stormshield's management interface as easy to use and very intuitive. Also, the interface offers an ability to anonymize user data through the analysis of logs.

- **Capabilities:** Stormshield offers dynamic filtering of internal hosts based on their reputation (Dynamic Host Reputation). The firewall also integrates a vulnerability detection engine and offers the ability to adapt the security policy for vulnerable hosts directly from the monitoring console. Its IPS includes signatures and protocol parsing for operational technology (OT) networks, which provide better detection and prevention against OT-based vulnerabilities.

- **Product:** Stormshield offers its own EPP (Stormshield Endpoint Security) and data encryption (Stormshield Data Security). Stormshield also has a partnership with Panda Security to offer its endpoint solution, Panda Adaptive Defense, as a third-

party endpoint protection partner. There is some level of collaboration between the firewall and these two products — for example, generation of an alert on the firewall and sharing the same user database.

Cautions

- **Sales Execution:** Stormshield has most of its deployments as on-premises, based on European certifications. While the message that it is a European company might be a positive in Europe, other regions do not consider it a deciding factor.

- **Product Strategy:** Despite having its own endpoint and data protection product lines, Stormshield lacks mature integration of these products with its firewalls. Although there's growing demand from SMBs for integration of endpoint agents and firewalls for better management and detection capabilities, the vendor offers only basic alert features between the firewall and endpoint agent.

- **Market Responsiveness:** Stormshield lacks a cloud-based management interface. This feature is already available from many other UTM vendors in the market and is quite popular with SMB clients and MSSPs.

- **Capability:** Stormshield lacks an active-active high-availability feature in its firewalls. The surveyed vendor resellers have highlighted this as a product weakness, especially to participate in public tenders.

- **Customer Feedback:** Surveyed customers have highlighted poor technical support through Stormshield partners outside of France as a product weakness.

Untangle

Untangle is evaluated as a Niche Player. Despite having an SMB-only focus, it still lacks SMB features such as DLP, SSL VPN and endpoint integration. A majority of its sales are in the U.S.
Headquartered in San Jose, California, Untangle is a UTM vendor targeting small and lower-midsize organizations. Its UTM appliances come as the xSeries, uSeries and mSeries, with a total of 11 models. In January 2018, it introduced four new models. Its UTM solutions can be deployed as software-based NG Firewalls, which can be deployed on third-party appliances, hardware, virtual appliances and public IaaS platforms; with a majority of mentioned deployments as software-based firewalls.
In 2017, Untangle released its cloud-based management solution, which is offered as SaaS through Untangle cloud. The vendor has released a threat intelligence service (ScoutIQ). It has also introduced a new admin UI and updates to the VPN offering.
Untangle is a good shortlist candidate for small and lower-midsize organizations in North America that are looking for software-based firewalls with simple, easy-to-manage interfaces.
Strengths

- **Product Strategy:** Untangle offers flexible deployment models for its NG Firewalls, which gives end users multiple deployment choices. It is offered as a software or as an appliance. Software can also be deployed on third-party appliances, as well as third-party routers.

- **Innovation:** Untangle NG Firewall comes with an innovative application-widget-based UI and is designed for easy management. Administrators find managing application widgets extremely useful. The day-to-day administration is also made simple without needing to sift through multiple screens. Surveyed customers and value-added resellers (VARs) have cited ease of management as its strongest feature.

- **Sales Strategy:** Untangle offers a flexible licensing model for its NG Firewall. Licensing comes in monthly, annual, and three- or five-year software licenses. Untangle's software-based NG Firewalls are less expensive than other hardware-based firewalls in the market. It offers all-inclusive technical support within the subscription bundles.

- **Market Execution:** Untangle offers its software-based firewall free of change. It can be downloaded from the website and used with free applications, which are offered with it. For premium applications, the vendor offers a 14-day trail, marketed as freemium, which is attractive to SMBs. Untangle also offers its centralized management portal, Command Center, to manage as many as five gateways for free.

- **Capability:** Untangle offers multiple ways of decrypting SSL traffic. It offers SNI-based, certificate-based and selective-traffic-based SSL decryption. This gives enterprises the option to offer different levels of decryption capabilities for different types of traffic, especially to meet different regulations.

- **Product:** Untangle has developed ScoutIQ, which is its cloud-based threat intelligence platform. It is offered to existing customers at no extra cost. This improves the malware detection capabilities, which are offered as a part of the Virus Blocker feature.

Cautions

- **Sales Execution**: Untangle UTM solutions have most of their deployments in small organizations as software. Its product strategy is also more focused on smaller SMBs for less than 500 employees.

- **Capability:** Untangle does not offer premium, advanced threat detection as a separate subscription, and its network sandboxing offering is bundled with its Virus Blocker subscription. It does not have specialized offerings for ransomware detection, which is a desirable feature among SMBs. It also lacks a SaaS monitoring and control feature, which is gradually becoming an important shortlisting criteria by SMBs with increasing use of SaaS applications.

- **Offering:** Untangle UTM does not offer SSL VPN and DLP capabilities, which are provided by many competitors. Many SMBs find basic DLP capabilities useful, especially for compliance reasons. Untangle also lacks integration with third-party endpoint protection platforms and does not offer its own endpoint agents. This makes it an unfavorable candidate for SMBs that want ease of administration and better correlation capabilities with their UTM solutions.

- **Marketing:** Untangle UTM lacks third-party independent lab certifications, such as Common Criteria and Federal Information Processing Standards (FIPS), which are highly regarded by government and regulated organizations, especially in the U.S. where they sell the most.

- **Product:** Untangle does not offer on-premises centralized management. It offers a cloud management portal based on a SaaS model, which provides basic management capabilities but lacks zero-touch deployment and provision features.

Venustech

Venustech is evaluated as a Niche Player because its visibility is limited to China and Japan. Venustech primarily offers a UTM product for mostly small to lower-midsize companies. It lags behind other vendors in terms of execution on an offering that accommodates SMB and distributed use cases.
Headquartered in Beijing, China, Venustech has a large product portfolio, which includes a web application firewall, an application delivery controller (ADC), an IPS, a unified security management platform (SIEM) and a penetration testing service, along with firewalls for SMBs and enterprises (Venusense UTM).
Recent updates include Venustech launching its Chengdu security operations center (SOC) and CloudTrust security cloud platform as part of its strategy of expansion in the Chinese security market.
Venusense UTM is a good candidate for Venustech customers in China, and SMBs that are looking for a good local vendor with strong regional support in China and Japan, as well as a cost-effective UTM offering.
Strengths

- **Technical Architecture:** Venusense UTM offers integration with the Venusense Unified Security Management (USM) platform. USM is Venustech's big data security management platform. The UTM product can collect data and react based on analysis results.

- **Product:** The vendor offers integration of its UTM with Venusense endpoint management software. The UTM product offers support for internal network endpoint access control with DLP capabilities, offering basic NAC features from within the UTM.

- **Capabilities:** Venustech UTM continues to offer a granular DLP feature for HTTP, FTP, POP3, IMAP and STMP that is not being offered by many UTM vendors in the market.

- **Capabilities:** Venusense UTM offers application control features with support for regional Chinese and Japanese applications, such as Youku, Tonghuashun and LeEco, which makes it a desirable regional vendor for SMBs seeking regional application control.

- **Customer Feedback:** The vendor continues to receive positive reviews by surveyed clients about its strong technical support. Surveyed clients also have highlighted ease of management as product strength.

Cautions

- **Geographic Strategy:** Venustech does not have any presence outside China, except for a limited presence in Japan. Customers outside of these two regions should verify the level of support, including languages available beyond Japanese, Chinese and English.

- **Capabilities:** The product lacks an SD-WAN feature. It also doesn't offer active-active and active-passive link-balancing features.

- **Capabilities:** Venusense offers a cloud management portal VCloud for centralized management of its UTM product, and lacks an on-premises management platform. The capabilities of VCloud are confined to only basic management and reporting capabilities. The portal lacks a centralized rule change feature for a group of UTM solutions.

- **Product Strategy:** The vendor does not provide support for any public IaaS platforms, despite a strong adoption of public IaaS platforms in China.

- **Product:** Venusense lacks an SSL decryption feature. It also does not provide a CASB feature for monitoring and managing SaaS applications.

WatchGuard

WatchGuard is in the Visionaries quadrant, as it continues to focus on the security requirements of the SMB market. It consistently introduces enhancements to improve advanced threat prevention capabilities and correlation capabilities between its endpoints and UTM. Its roadmap also displays a strong focus on improving the detection and response capabilities of an end-user network.
WatchGuard is headquartered in Seattle, Washington. Its product portfolio includes UTM offerings, multifactor authentication (MFA) endpoint security and wireless APs. Its UTM product line is called Firebox. WatchGuard Dimension is its centralized management product. WatchGuard also offers virtual appliances, including XTMv, FireboxV, and Firebox Cloud for public cloud deployment. Its endpoint product is called WatchGuard Host Sensor. Recent WatchGuard news includes the introduction of six new T Series (tabletop) UTM models and four new, high-performance, M Series (rack mount) UTM models. Major news includes the acquisition of Percipient Networks and the launch of DNSWatch, and also the acquisition of Datablink and subsequent launch of AuthPoint, a cloud-based MFA service. The vendor also introduced enhancements to its VPN offering.
WatchGuard is a good shortlist candidate for SMBs and distributed enterprises in need of a comprehensive feature set, with easy bundled licensing.
Strengths

- **Product Strategy:** WatchGuard has a strong SMB strategy focus, which is reflected in its product, sales strategy and roadmap items. It offers multiple features that are desirable for SMBs. It has simple bundled licensing and a strong channel-only strategy that also includes small partners that sell only to small and lower-midsize organizations.

- **Product:** WatchGuard offers WatchGuard Host Sensor, as a part of its Total Security Suite license. It is continuously working toward building better correlation capabilities between Host Sensor and its UTM product to help organizations detect and respond to advanced threats. This offering is attractive for SMB buyers with

smaller security teams that are looking for consolidation toward a single vendor.

- **Customer Experience:** Surveyed customers have ranked WatchGuard's new Threat Detection and Response (TDR) product as one of the greatest strengths of the Total Security Suite licensing bundle. Surveyed partners have highly rated the WatchGuard RapidDeploy feature, which is a remote deployment and provisioning feature.

- **Market Responsiveness:** WatchGuard introduced ThreatSync, its new cloud-based correlation and threat-scoring engine, which uses event data collected from WatchGuard Firebox, endpoints and cloud intelligence feeds. This aligns with the growing market demand for better correlation between network and endpoint devices, which provides better detection and remediation capabilities for advanced malware.

- **Capabilities:** WatchGuard UTM offers strong web protection features, in partnership with Forcepoint for URL filtering. It offers customizable block pages and options for password bypass for end users. It has introduced a new DNSWatch feature, which provides phishing education via a block page that includes video education.

Cautions

- **Market Responsiveness:** The Dimension portal, which is WatchGuard's centralized cloud-based management portal for both partners and end users, offers very limited configuration-change-related capabilities. It lacks mature change management capabilities, such as the ability to change firewall rules and apply firmware updates on a group of UTM solutions centrally. WatchGuard also offers a separate cloud portal for TDR and DNSWatch.

- **Customer Feedback:** Surveyed customers have reported WatchGuard lacks strong integration between its separate management systems, especially the Dimension, TDR and wireless product lines.

- **Marketing:** WatchGuard lacks strong end-user-focused marketing and promotion compared to its direct UTM competitors in the market. This is especially related to a lack of awareness for new features and product enhancements within the end-user SMB client base.

- **Capability:** WatchGuard's UTM lacks CASB functionality and offers basic SaaS reporting and control, using the application control feature as a part of its basic subscription. It also lacks granular SaaS management and control features, only provided by a CASB.

Vendors Added and Dropped

We review and adjust our inclusion criteria for Magic Quadrants as markets change. As a result of these adjustments, the mix of vendors in any Magic Quadrant may change over time. A vendor's appearance in a Magic Quadrant one year and not the next does not necessarily indicate that we have changed our opinion of that vendor. It may be a

reflection of a change in the market and, therefore, changed evaluation criteria, or of a change of focus by that vendor.

Added

No vendors were added.

Dropped

No vendors were dropped.

Inclusion and Exclusion Criteria

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

To qualify for inclusion, vendors with UTM products that meet the market definition and description were considered for this research 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)
  - Advanced malware detection
  - Centralized management console
- They regularly appeared on Gartner midsize client shortlists for final selection.
- They achieved UTM product sales (not including maintenance or other service fees) of more than $9 million in 2017, 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.

Vendors to Watch

Gartner is observing a growing adoption of Palo Alto Networks firewalls by midsize businesses. The vendor is releasing different models favorable for this vertical. This vendor is being shortlisted by security-conscious midsize businesses that are looking for mature application control and advanced malware prevention capabilities.

Evaluation Criteria

Ability to Execute

Product/Service: Core goods and services that compete in and/or serve the defined market. This includes current product and service capabilities, quality, feature sets, skills, etc. This can be offered natively or through OEM agreements/partnerships as defined in the market definition and detailed in the subcriteria. Key features that are weighted heavily include:

- Ease of deployment and operation
- A cloud-based management portal
- Console quality
- Price/performance
- Range of models
- Secondary product capabilities (such as logging, visibility for SaaS applications, SD-WAN capabilities, mobile device management, integrated Wi-Fi support and remote access)
- The ability to support multifunction and distributed organization deployments

Overall Viability (Business Unit, Financial, Strategy, Organization): Viability includes an assessment of the organization's overall financial health, as well as the financial and practical success of the business unit. It views the likelihood of the organization to continue to offer and invest in the product, as well as the product position in the current portfolio. 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 existing Gartner data), 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 criterion refers to the organization'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. It also includes the number of deals, visibility in shortlists, the installed base, and the vendor's strength of sales and distribution operations. Presales and postsales 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 and Track Record: This criterion describes the 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: This criterion refers tothe 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, promotions, thought leadership, 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 are rated. Specifically, this includes quality supplier/buyer interactions, technical support or account support. This may also include ancillary tools, customer support programs, availability of user groups, service-level agreements, etc.
The quality and responsiveness of the escalation process, transparency, and stability of firmware are evaluated. 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 is key to the operations criterion. 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

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 (September 2018)
Completeness of Vision

Market Understanding: This criterion refers to the ability to understand customer needs and translate them into products and services. It includes vendors that show a clear vision of their market — listen, understand customer demands, and can shape or enhance market changes with their added vision.
This criterion includes 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 especially around the security needs of the SMB market

segment. UTM vendors will not be evaluated merely based on an aggressive future goal, but rather on how they enact a plan, follow it and also modify the plan with the changing market direction.

Marketing Strategy: This criterion refers to a clear, differentiated messaging consistently communicated to partners and end users. Gartner makes this assessment based on the product positioning and a clear market understanding, especially after or before a major change (for example, feature enhancements, partnerships, introducing a product line, etc.). This will include feedback by Gartner clients on the vendor's marketing strategy.

Sales Strategy: A sound strategy for selling that uses the appropriate networks including direct and indirect sales, marketing, service, and communication is evaluated. Partners that extend the scope and depth of market reach, expertise, technologies, services and their customer base are taken into consideration.
This criterion includes preproduct and postproduct support, value for pricing, licensing models, and clear explanations and recommendations for detection events and deployment efficacy (for example, direct sales and direct technical support for SMBs). Building loyalty through credibility with a full-time midsize business security and research staff demonstrates the vendor's ability to assess the next generation of requirements.

Offering (Product) Strategy: This criterion describes an approach to product development and delivery that emphasizes market differentiation, functionality, methodology, and features as they map to current and future requirements.
The emphasis is on the vendor's product roadmap, current features, leading-edge capabilities, virtualization and performance. UTM vendors will be evaluated based on the product capabilities and features favorable for SMBs, such as mature centralized management interface, VPN features, and endpoint integration, which are beyond basic enterprise firewall features. 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 are evaluated. This includes the process and success rate for developing new features and innovation. It also includes R&D spending.

Vertical/Industry Strategy: The strategy to direct resources (sales, product, development), skills, and products to meet the specific needs of individual market segments, including verticals is evaluated for this criterion.
UTM vendors will be evaluated against their strategy specific to SMBs. Examples include direct SMB sales strategy, direct SMB technical support and an SMB-focused roadmap. Vendor presence in different SMB use cases and for SMB customers will also be evaluated. This criterion will also evaluate a vendor's strategy related to MSSPs, in terms to specific feature enhancements and alliance partnerships with them.
Innovation: This criterion includes product innovation, such as R&D, and quality differentiators relevant to SMBs and distributed organizations, but also relevant to the channel supporting them, including MSSPs. This includes features such as performance, ease of use (deployment, operational maintenance and supervision), improved

management, visibility and control of SaaS applications, integration with other security products, and clarity of reporting. The ability to provide good security against threats targeting SMBs organizations (typically malware activity), and good visibility of user activity are also considered.

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 is evaluated.

UTM vendors will be assessed based on their specific strategy related to different geographic factors such as geographic presence directly and through partners, regional TACs, and regional application control.

Table 2: Completeness of Vision Evaluation Criteria

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 (September 2018)

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 are becoming more security conscious because of the increase in number of SMB-focused attacks. According to the 2017 Ponemon Institute report, "SMBs are having slightly more data breaches involving personal information and the size of data breaches is larger."[1] As a result, UTM vendors are working toward offering in-depth features with better performance to meet the growing security demands from SMBs. The typical challenges of a majority of SMBs remain the same:

- Limited IT budgets, although Gartner has observed this situation is gradually improving after recent high-profile attacks.
- Smaller IT teams, which means many SMBs are considering using an MSSP to manage UTM solutions.
- No specialized dedicated network security staff.
- Regulation and compliance requirements.

Market Overview

The UTM market grew 11.8%, from $1.95 billion in 2016 to $2.18 billion in 2017. There are several providers participating in this market, though the top five account for 68% of the market share. The fastest-growing regions were Greater China, the Middle East and North

Africa, and North America (see “Market Share: Unified Threat Management [SMB Multifunction Firewalls], Worldwide, 2017”).
Fortinet continues to own the largest market share in the UTM market — with more than twice the revenue of its closest competitors Check Point Software Technologies and Sophos — and to grow much faster than the market average.
The UTM market continues to grow and evolve. This year, UTM vendors focused on enhancements across ransomware detection, SaaS monitoring and control, endpoint client integration, SD-WAN capabilities, and cloud-based management. Also, with the increase in SSL traffic, end users are looking for decryption capabilities on their perimeter devices, which require better-performing UTM boxes.

Evolving End-User Requirements With Evolving Threat Landscape and Networks

With the evolving network and threat landscape, small and midsize organizations are facing the following security challenges:

- Increase in the number of ransomware attacks
- Low visibility and control of Internet of Things (IoT) devices in the network
- Ever-growing use of personal devices to access the wireless network
- Roaming employees
- Increasing SSL traffic
- Smaller security teams with no SOC, which make detection and response of advanced threats a challenging task
- Increase in adoption of SaaS applications

As a result of above mentioned security challenges, the UTM market continues to evolve and the UTM vendors are working toward building and enhancing the following functionalities:

- **Performance:** Performance has always been a pain point for UTM users, especially when they are considering enabling multiple features on their UTM products. With the increase in SSL traffic and targeted attacks over SSL, SMBs are looking for multiple SSL decryption techniques that they can apply on their traffic with minimal impact on the performance of the UTM offering. In 2017 and 2018, Gartner has observed a majority of UTM vendors introducing multiple models with better performance capabilities.
- **Cloud-Based Management Portal:** Ease of management continues to be the demand of small and midsize organizations for 2018. As a result, a mature cloud-based management portal to manage and monitor multiple UTM solutions is being introduced and enhanced by many UTM vendors.
- **SD-WAN:** Gartner is observing an increase in the requirement of secure connectivity of branch offices; as a result, clients are considering software-defined WAN as a possible option. Also, as per Gartner’s SD-WAN Strategic Planning

Assumption: “By 2020, more than 50% of WAN edge infrastructure refresh initiatives will be based on SD-WAN versus traditional routers, up from less than 5% today.”

- **Anti-Ransomware:** Although part of advanced malware, ransomware has hit SMBs with a relative increase in the number of attacks. As a result, SMBs are looking for advanced ransomware detection and recovery features on their UTM solution. UTM vendors are working toward offering advanced anti-ransomware features with endpoint correlation capabilities for better detection.

- **Consolidated Endpoint Detection and Response Capabilities:** SMBs and enterprises are keen on consolidating multiple features toward a single security vendor for better detection and correlation of advanced threats. As a result, in 2018 UTM vendors have focused on improving the capabilities of their existing endpoint agents and partner with third-party EPPs in case they do not have their own endpoint agents.

- **SaaS Monitoring and Control:** As per the end-user survey conducted by Gartner for this Magic Quadrant of the reference clients, “52% of surveyed end users indicated that they are using Office 365.” Gartner has also observed an increase in use of SaaS applications by SMBs. As a result, they are looking for better SaaS monitoring and control features in their UTM or integration with third-party CASBs.

As a result of the end-user survey conducted by Gartner of the reference clients for this Magic Quadrant, we found the following:

- **The main reason for an end-user organization to shortlist a particular UTM vendor was product features.** Although SMBs are looking for better product features when shortlisting UTM vendors, per Gartner client inquiries pricing is still the main shortlisting criteria for SMBs to select a UTM.

- **Eighty-three percent of organizations have on-premises UTM deployment, as opposed to only 10% with hybrid deployments and 6% with cloud deployments.** While there is a slight movement to the cloud, the majority of SMB UTM deployments are still on-premises.

- **The top three key factors to final selection of a UTM vendor were product functionality and performance, overall cost, and product roadmap and future vision.** This going in conjunction with what Gartner observes in inquiries. The primary shortlisting criterion is still pricing,followed by performance, which is rated high when shortlisting a UTM vendor.

- **A majority of surveyed customers have also highlighted that they have direct vendor support as opposed to through a reseller.** Gartner observes that SMBs are highly reliant on partners for support and implementation services, as they are easy to reach and offer support in local languages.

As per the end-user survey conducted by Gartner for this Magic Quadrant, the most common features deployed on a UTM offering in addition to the firewall are:

- Intrusion prevention: 89%
- URL filtering: 89%
- IPsec VPN: 79%
- Application control: 78%
- SSL VPN: 67%
- Web antivirus: 63%
- Centralized management console: 61%
- Identity control: 44%

Impact of the Firewall-as-a-Service Market

Firewall as a service (FWaaS) is a multifunction security gateway delivered as a cloud-based service or hybrid solution (that is, cloud plus on-premises appliances), which is fully managed through a cloud-based portal. Gartner can see awareness of this market within the distributed office enterprise space. FWaaS is appealing to organizations looking to move away from maintaining multiple physical firewall appliances at different sites and from renewing licenses frequently, and toward an operating expenditure (opex) model, which is easier to manage and less time-consuming as the primary use case. Sample vendors in this space include Cato Networks, Palo Alto Networks (GlobalProtect), Omninet, OPAQ, Secucloud and Zscaler.

Evidence

[1] "2017 State of Cybersecurity in Small & Medium-Sized Businesses (SMB)," Ponemon Institute.

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.