Magic Quadrant for Unified Threat Management (SMB Multifunction Firewalls)

Published 20 September 2018 - ID G00336625 - 69 min read

By Analysts Rajpreet Kaur, Claudio Neiva

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

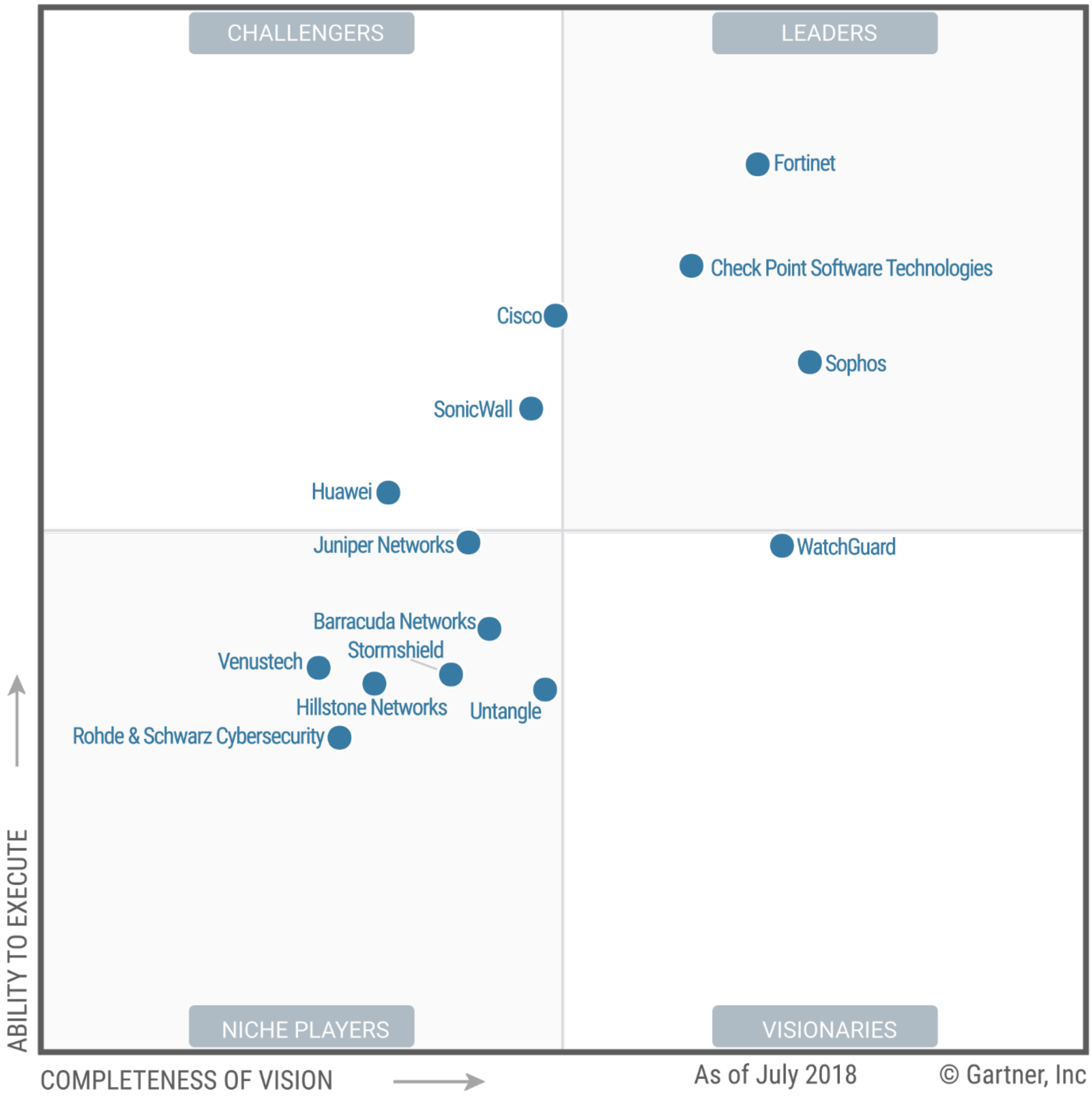
Browser-based management, ease of configuration, embedded reporting, VPN, localized software, excellent partner support and documentation don't specifically appeal to large enterprises, but are highly valued by SMBs in this market. Gartner sees very different demands from the large-enterprise and branch 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 MSSPfavorable 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.