Magic Quadrant for Unified Threat Management

19 July 2013 ID:G00245469
Analyst(s): Greg Young, Jeremy D'Hoinne

VIEW SUMMARY

Unified threat management devices provide small or midsize businesses with multiple network security functions in a single appliance. Buyers should focus on performance when every targeted feature is enabled, and on total cost of ownership instead of initial purchase price.

Market Definition/Description

Gartner defines the unified threat management (UTM) market as multifunction network security products used by small or midsize businesses (SMBs). Typically, midsize businesses have 100 to 1,000 employees, with revenue ranging from $50 million to $1 billion. UTM products for the SMB market must provide the following functions at a minimum:

- Standard network stateful firewall functions
- Remote access and site-to-site virtual private network (VPN) support
- Secure Web gateway (SWG) functionality (anti-malware, URL and application control)
- Network intrusion prevention focused on workstation protection

All UTM products contain various other security capabilities, such as email security, Web application firewalls (WAFs) and data loss prevention. However, the vast majority of SMBs only utilize the firewall, intrusion prevention and SWG functionalities. They also request a basic level of application control, mostly to restrict the use of Web applications and cloud services (such as social media, file sharing and so on). Features related to the management of mobile devices create a potentially attractive differentiator for this market (see "How Unified Threat Management Tackles the Consumerization of IT"). Browser-based management, basic embedded reporting, and localized software and documentation, which don't appeal to large enterprises, are highly valued by SMBs in this market. SMBs should evaluate UTM devices based on the controls they will actually use, the performance they will get for those features, and the quality of vendor and channel (and managed services) support that is available.

Given the continuing economic uncertainty, most SMBs have strong IT budgetary and staffing constraints. This causes them to highly value ease of deployment and use, strong local channel support, and flexible pricing. Leading UTM vendors will:

- Be aggressive and flexible in pricing, reducing upfront costs, eliminating hidden fees, and ensuring durable software and hardware support.
- Focus on midsize businesses' need for the right network security at the right price, rather than trying to upsell them to enterprise products and capabilities.
- Provide product management features that simplify deployment and ongoing operations.
- Make it easy for customers with evolving security needs to add licenses to existing platforms by unifying their support contract renewal dates.
- Offer efficient vendor technical support and easy-to-diagnose systems to value-added resellers (VARs), which often handle a large number of devices with understaffed technical teams.
- Be early to add new security features that are showing up as separate point products.

Many UTM vendors are heading toward the console and management being fully in the cloud. Gartner believes that, although it's convenient for the vendors to do so, a portion of the SMB market will not accept this exclusively cloud model for reasons of latency, trust, and being able to access the console when under attack. Reporting and log retention are well-suited to the cloud, but not exclusively.

For 2012, Gartner estimates that worldwide revenue in the UTM market totaled approximately $1.53 billion, which represents an 18.7% growth over our estimate for 2011 (see Note 1). Gartner believes

that the UTM market will continue to grow faster than many other security markets, but we also see a number of trends applying downward pressure on market growth. Regardless, we forecast continued growth in the UTM market of approximately 15% compound annual growth rate through 2018.

We see the following positive trends continuing to drive growth in the UTM market:

- A steady number of new, small (that is, fewer than 100 employees) organizations.
- SMBs in emerging countries buying their first UTM products to secure increasingly faster and more highly business-critical broadband Internet connections. This scenario represents "greenfield" growth for the market — often with a preference for country or region-specific vendors.
- A continued refresh of first-generation UTM products by SMBs — especially midsize businesses (100 to 999 employees), and especially in North America and Western Europe — due to product aging and the demand for higher-speed Internet connectivity. This demand drives the replacement of existing product with the incumbent's newer version, or replacement of the incumbent by a competitor.

Some trends will limit market growth:

- The increased use of smartphones, tablets and even 4G-equipped laptops moves more small business Internet traffic to direct connections to wireless data service providers, as opposed to through UTM appliances to wired Internet service providers (ISPs).
- The pricing and features of cloud-based SWG services (see "Magic Quadrant for Secure Web Gateways") are very attractive to small businesses because they offer flexible pricing and meet the needs for securing mobile users. While most of those services only deal with Secure Sockets Layer (SSL) and HTTP traffic, they represent most of the needs of many small businesses, and can reduce their UTM needs to a simple firewall/router. However, the SWG market is smaller than the UTM market and follows a slightly slower growth.
- The increased use of cloud-based email (such as Google Apps for Business or Microsoft Office 365) reduces the demand for email security, since those services include integrated email antivirus functionality.
- As lower-midsize companies grow to become upper-midsize and enterprise size, their security needs will get more complex, and they will outgrow their UTM appliances and deploy enterprise network security platforms, such as next-generation firewalls and SWGs.

Gartner believes that the downward trends now balance the positive trends and might put increased pressure on the market in the future, thereby causing us to maintain our UTM market growth forecast from our previous outlook. These trends have also led to limited entries/exits of vendors into/from this market. In 2012, Cassidian CyberSecurity, a subsidiary of the EADS Group, acquired Netasq. Arkoon Network Security, Barracuda Networks, Endian and eSoft did not meet the inclusion criteria.

Magic Quadrant

Figure 1. Magic Quadrant for Unified Threat Management

Source: Gartner (July 2013)

Vendor Strengths and Cautions

Check Point Software Technologies

Check Point Software Technologies is one of the largest pure-play security companies, and has been expanding from the enterprise security market to the UTM market since 2004. Check Point has been very active in the UTM segment. In the past 18 months, it has targeted SMBs with new appliances (primarily the 600 and 1100 series), with part of a global product line update (referred to as the "2012

appliances") and with the release of a common operating system (OS) for every security gateway (GAiA). Its SMB portfolio now includes 11 appliances and a cloud-based security service. Fundamental to Check Point firewall offerings is the set of software options referred to as Software Blades.

Strengths

- Check Point's reporting and management console is highly rated by midsize companies. Known primarily as an enterprise security provider, Check Point has expanded into the SMB space for midsize companies that are seeking premium firewall products.
- Check Point's UTM solutions benefit from its enterprise-level security features, such as ThreatCloud and Anti-Bot. The Software Blades approach allows for customization of features.
- Selective direct user involvement with its UserCheck technology improves security awareness and reduces the risk of policy infringement.
- The consolidation of the appliance portfolio and the unification of the different Software Blades under the GAiA OS will ease maintenance and reduce the learning curve for SMB resellers and end users.
- Check Point has very strong capabilities for virtualized versions and securing virtualization.

Cautions

- Price is often cited as the primary reason for not selecting Check Point solutions.
- Check Point has approximately 30 different Software Blades. Having so many options creates an overly complex pricing scheme for many SMBs and small resellers, compared with the competition. Blade packages, however, are available for the purpose of simplification.

Cisco

Cisco uses its network infrastructure placements as an entree to bundle in adjunct security solutions for SMBs. Cisco now addresses SMBs with the ISA500 Series for small businesses (four models), the ASA 5500-X Series for midsize companies (two models) and the cloud-managed MX series (six appliances) based on the Meraki solutions (acquired in 2012). In addition to the dedicated security solutions, Cisco has a large portfolio of network solutions that can provide security features, such as the Integrated Services Router (ISR).

Strengths

- Cisco support is rated well by Gartner customers; its entrenchment in the network infrastructure makes it easy to find well-trained staff to support Cisco security implementations.
- The ISA500 Series and ASA 5500-X Series show feature improvements compared with the previous generations of products; the removal of the requirement for hardware add-in modules for intrusion prevention or content inspection allows the new ASA product line to compete with other midsize UTM devices.
- The cloud-based MX series provides an easy way to centrally manage distributed organizations looking for PCI compliance.
- The integration of Cisco AnyConnect with the ISA500 Series and the ASA 5500-X Series, in addition to the existing Cisco client for mobile devices, makes Cisco a good choice for SMBs with many mobile users.

Cautions

- Cisco's UTM devices have low visibility among Gartner SMB clients and do not generate many inquiries, because clients view Cisco primarily as an enterprise security player. The vendors we surveyed continue to identify Cisco as one of the most replaced brands.
- Cisco's 2012 UTM refresh showed that it could catch up with basic SMB needs, but it still has to demonstrate its ability to drive the market.

Clavister

Clavister, which is headquartered in Sweden, targets primarily ISPs with its cloud services. It addresses SMBs through its branded security appliances, the Eagle Series and Wolf Series. Also, Clavister's technology is provided as an OEM solution.

Strengths

- The security quality of Clavister's products is often mentioned by its customers. Also, its ISO 9001:2008 certification and two-year standard return-and-repair warranty appeal to SMBs that weight reliability highly.
- The Clavister X8 series of rugged appliances is a good fit for specific midsize vertical industries.

Cautions

- The focus on core firewall needs, rather than completeness of features, translates into a competitive gap for specific use cases.
- Gartner has not observed notable client interest outside of Europe, and Clavister has generated a very low level of inquiry from Gartner clients over the past 12 months.
- Clavister was never cited as a competitive threat by surveyed vendors.

Cyberoam

Based in India, Cyberoam is a pure-play vendor for the UTM market, focusing solely on SMBs. Over the past nine months, it released its NG Series with 12 new appliances and five virtual appliances. Cyberoam consistently communicates about the integration of user identity in every component of the UTM configuration, and about the availability of Web Application Firewall on the UTM.

Strengths

- Cyberoam's product development approach of providing competitive pricing, coupled with the regular addition of new features, has proved to be a successful choice for the SMB market.
- Its well-organized management interface minimizes the burden implied by the presence of numerous features.
- Cloud-based centralized management, which is free for certified partners, can be a valuable asset for managed security service providers (MSSPs).
- Users report that they like the built-in reporting capabilities.

Cautions

- Cyberoam's visibility remains low with Gartner clients, and it is not yet cited as a threat by surveyed vendors and resellers.
- Cyberoam does not yet have a significant sales presence in North America.
- Gartner believes that Cyberoam's channel marketing is overly focused on perceived competitor shortcomings, rather than on promoting its own brand and benefits to customers.

Dell

Dell acquired SonicWALL in 2012 and kept SonicWALL as the name of its firewall product line. Dell sells two product lines to the SMB market: the SonicWALL TZ Series for the smallest businesses and the SonicWALL NSA Series for small and midsize companies. It also targets the enterprise market with its SonicWALL SuperMassive Series, competing with established enterprise players on the price/performance ratio. Dell also provides SSL VPN and email security gateway.

Strengths

- Gartner often sees Dell shortlisted based on the SonicWALL brand being well-established in the SMB market.
- Many customers report to Gartner that the TZ Series product line is a cost-effective solution with very good overall performance. Low total cost of ownership (TCO) is often cited as a reason for choosing Dell SonicWALL products.
- The TZ Series' clean wireless features are available for smaller locations, and Gartner has observed that retailers are interested in these noteworthy features.
- Dell's overall focus on midsize organizations aligns well with a UTM offering, and Dell's broad logistical capabilities assist with deployments involving multiple geographies.

Cautions

- Surveyed vendors claimed that Dell SonicWALL is a brand they often replace. Gartner has observed that SonicWALL's acquisition by Dell has caused disruption for prospects that don't have an existing Dell relationship because of changes in the channel.

- Gartner views Dell's efforts to move toward the enterprise markets as alienating the SMBs. The latest SonicOS releases — which have an increased number of features targeting the higher-end of midsize markets and enterprises, as well as a marketing focus on the SuperMassive Series — increase this perception.

Fortinet

Fortinet is a security vendor based in California. It offers 10 FortiGate UTM appliance models aimed at the small and midsize market. The security product portfolio, including tokens and host agents (FortiClient), is designed to appeal to VARs as the route to SMB sales. With two new models in 2012 (FortiGate-60D and FortiGate-100D), Fortinet continues to rely on its custom application-specific integrated circuit (ASIC) architecture to provide a high price/performance ratio. The fifth major version of Fortinet's OS brought a new set of features aimed at managing phones and tablets, trying to further expand the scope of UTM and to pressure competitors with advanced features.

Strengths

- Fortinet continues to have the highest visibility of UTM providers among Gartner clients, and it is the company most frequently mentioned by the vendors we surveyed as a significant SMB competitive threat.
- Because Fortinet designs and builds its own ASIC (FortiASIC), and uses little OEM software (compared with most UTM vendors), it provides a very aggressive price/performance proposition, which is important to SMBs that typically have limited security budgets.
- Fortinet has a very large R&D team. Gartner views Fortinet as setting the cadence in the UTM market, driving its competitors to react.
- Fortinet has a strong channel presence and provides local support in numerous countries.

Cautions

- The frequent hardware and software updates make it harder to maintain a consistent level of expertise across Fortinet's widely distributed channel, which sometimes causes support issues.
- Users often report a noticeably greater-than-documented impact on performance when using Web antivirus and URL filtering. Customers should take this into account and assess actual performance when doing competitive evaluations and product sizing.

gateprotect

Gateprotect is a German company, headquartered in Hamburg. It focuses on the SMB and MSSP markets, with nine models targeting companies composed of 10 to 10,000 users. Gateprotect emphasizes its management interface, and uses its proprietary solution (eGUI) to configure the UTM. It develops the core of its software (v.9), but relies on OEM partners that are specialized in their field for some security inspections. In 2012, gateprotect secured a new round of investment that was intended to accelerate its international expansion. It provides virtual images of its appliances and a centralized management tool for MSSPs.

Strengths

- Gateprotect visual configuration emphasizes the ease of creation of security policies, focusing on saving time for end-user and technical support services.
- Gateprotect maintains what Gartner views as a very competitive software release cycle to answer the needs of SMBs.

Cautions

- Gateprotect has low visibility and rarely appears on Gartner client shortlists (although there is a slight increase in Latin America).
- Increased efforts to expand beyond EMEA are still developing within the markets Gartner observes.

Huawei

Huawei is a China-based company with a primary focus on network infrastructure solutions. Its Unified Security Gateway (USG) product line includes seven models targeting SMBs. Huawei operates in 40 countries, and its revenue comes mainly from China, Africa and the Middle East. The company recently invested significantly in developing its channel to better address SMBs.

Strengths

- Existing customers of Huawei's network solutions will get a good price for value and a shorter learning curve with its UTM devices.
- The USG product line includes a comprehensive set of network options (such as 3G, xDSL and Wi-Fi).
- Huawei is leveraging its hardware and software to deliver a very attractive price/performance proposition. Because the vendor has a very large security portfolio, other offerings (such as its secure wireless and tablet containers) can provide end-to-end security options for SMBs.

Cautions

- Like most infrastructure vendors, Huawei's main focus remains network and larger enterprises or carriers. To address the SMB market, it has yet to shift its road map priorities toward core SMB market needs.
- Huawei has low visibility outside the Asia/Pacific region for its security products.
- Its investment in the UTM market is still recent, resulting in software that is lagging behind other solutions. However, Gartner views the Huawei UTM road map as very positive.

Juniper Networks

Juniper Networks is a network infrastructure vendor based in California. It has a broad portfolio that covers network and security solutions. Its UTM offering (SRX Series) includes seven models and relies on the Junos OS, which is the common platform for network and security appliances of Juniper's portfolio. The vendor has enhanced its Web filtering with reputation-based scoring, and made application control and visibility (AppSecure) available to the SRX Series.

Strengths

- The use of a common OS for security and network components reduces training costs and complexity for UTM buyers that have other Juniper products in place.
- Users often cite good performance as the top reason to select Juniper.

Cautions

- As an enterprise vendor, Juniper's road map and product strategy are not focused on the SMB market.
- Compared with its enterprise/carrier channel, Juniper has a limited dedicated channel focused on the UTM market.

Kerio

Kerio is a U.S. company based in California. It has been selling UTM devices since 2004. The Kerio Control Box appliance is offered in two models: as a software appliance (ISO file) or as a virtual appliance. Kerio has added URL filtering, IPv6 and IPsec VPN support.

Strengths

- Users report to Gartner ease of use and product quality as the main reasons for choosing Kerio.
- Vendor support is also highly rated.

Cautions

- Kerio generates a very low level of inquiry from Gartner clients, and it does not have an extensive specialized channel to address the UTM market.
- Kerio's default license is limited to five users. The competition frequently offers unlimited users out of the box.
- Kerio provides a limited set of features and appliance choices, compared with its competitors.

Netasq

Netasq, founded in 1998, is a French UTM vendor that was acquired by Cassidian CyberSecurity, a subsidiary of the EADS Group. The U Series, its product offering for SMBs, includes six appliances along with virtual appliances. Netasq developed its own intrusion prevention system (IPS) and application detection engine. In 2012, Netasq completely renewed the UTM product lines (the S models) with increased performance and IPsec hardware acceleration. It also changed its service offer — extending it for up to five years.

Strengths

- Netasq has a simple service offering with a low-cost bundle that's often cited as good for TCO.
- Integration of application versioning and vulnerability detection are often cited as criteria for choosing Netasq.
- Users consistently say that support from Netasq and channel partners is very good.

Cautions

- The majority of Netasq's customers are in EMEA, and the company has low visibility among Gartner customers.
- Gartner believes that the acquisition by Cassidian will lead to a shift in Netasq's focus from SMBs to larger enterprises and governments, potentially taking the development and capability focus away from SMB customers.

Sophos

Sophos is headquartered in Boston and in Oxford, U.K. It was initially providing endpoint security solutions, and in 2011, it integrated a UTM offer with the acquisition of the German-based company Astaro. The acquisition went smoothly and did not slow the pace of new releases. Sophos now offers eight UTM appliances to protect companies with 10 to 5,000 users. Version 9.1, the latest release of its OS, adds management features for Sophos endpoints. The vendor continues to offer free UTM software (software appliance or virtual appliance) for home usage, and it benefits from an active community that provides quick feedback on emerging needs.

Strengths

- Sophos' ease of use consistently rates high among customers that Gartner has interviewed. Monitoring and configuration are well-integrated.
- The interface contains general guidance on what each feature does. This recognizes the SMB reality that not all operators are firewall experts.
- Sophos Remote Ethernet Device (Red) appliances are a competitive advantage when it comes to secure small branch offices.
- New Wi-Fi features added in Version 9 make it easy to manage temporary guests with vouchers and time or quota limits.

Cautions

- Customers report to Gartner that quality of service, VPN features and visibility into user activity need improvement.
- Sophos' UTM device is present less often on Gartner clients' shortlists than other Leaders' UTM devices.
- Sophos' application control features need to be expanded beyond the Web and better integrated with users in the firewall policy.

WatchGuard

WatchGuard, a U.S. company with headquarters based in Seattle, was one of the first to ship UTM platforms to the market. Its portfolio for SMBs is composed of 11 models (XTM 2, 3, 5 and 8 Series). WatchGuard's comprehensive offer also includes Web- and email-dedicated gateways. WatchGuard is a well-established UTM vendor with a strong focus on the SMB market. It has launched virtual appliances, and has extended its offer to MSSPs with a new program and a specific cloud-based solution for initial deployment (RapidDeploy).

Strengths

- Customers often cite the low initial price as a reason to select WatchGuard.
- WatchGuard has a strong and loyal channel presence in many countries.
- Recent hardware and software upgrades have brought significant performance improvements.
- An increased focus on MSSP needs reflects positively on the overall user experience.

Cautions

- WatchGuard offers a large number of products and services that are often very similar. Channel partners and buyers tell Gartner this is confusing.
- WatchGuard scored low as a significant UTM competitive threat by the vendors we surveyed.

Vendors Added or Dropped

We review and adjust our inclusion criteria for Magic Quadrants and MarketScopes as markets change. As a result of these adjustments, the mix of vendors in any Magic Quadrant or MarketScope may change over time. A vendor appearing in a Magic Quadrant or MarketScope one year and not the next does not necessarily indicate that we have changed our opinion of that vendor. This may be a reflection of a change in the market and, therefore, changed evaluation criteria, or a change of focus by a vendor.

Added

- Huawei was added.
- Dell acquired SonicWALL, which was in the previous Magic Quadrant, and the brand name has changed to Dell.

Dropped

- Trustwave was not included because it sells UTM primarily as an element of a bundled managed service offering rather than as appliances.
- Netgear was dropped because it focuses on a subset of the SMB market.

Inclusion and Exclusion Criteria

Inclusion Criteria

The following minimum requirements were used to determine which UTM companies met the criteria to be included in this Magic Quadrant under the following conditions:

- They shipped UTM software and/or hardware products — targeted to midsize businesses — that included capabilities in the following feature areas at a minimum:
  - Network security (stateful firewall and intrusion prevention)
  - Web security gateway
  - Remote access for mobile employees (VPNs)
  - Email security
- They 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 $7 million in 2012, 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.

Exclusion Criteria

- There was insufficient information for assessment, and the companies didn't otherwise meet the inclusion criteria, or aren't yet actively shipping products for revenue.
- Products aren't usually deployed as the primary Internet-facing firewall (for example, proxy servers and network IPS solutions).
- Products are built around personal firewalls, host-based firewalls, host-based IPSs and WAFs — all of which are distinct from this market.

- Solutions are delivered primarily as an integral part of MSSs, to the extent that product sales didn't reach the $7 million threshold.

Evaluation Criteria

Ability to Execute

Product/Service: Key features — such as ease of deployment and operation, console quality, price/performance, range of models, secondary product capabilities (for example, logging, integrated Wi-Fi support and remote access), and the ability to support multifunction deployments — are weighted heavily.

Overall Viability: This includes a vendor's overall financial health, prospects for continuing operations, company history, and demonstrated commitment to the multifunction firewall and network security market. Growth of the customer base and revenue derived from sales are also considered. All vendors are required to disclose comparable market data, such as UTM revenue, competitive wins versus key competitors (which is compared with Gartner data on such competitions held by our clients), and devices in deployment. The number of UTM devices shipped isn't a key measure of execution. Instead, we consider the use of these solutions and the features deployed to protect the key business systems of Gartner midsize business clients.

Sales Execution/Pricing: This includes pricing, the number of deals, the installed base, and the strength of sales and distribution operations in the vendors. Presales and postsales support is 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 TCO during a typical multifunction firewall life cycle (which is three to five years) is assessed, as is the pricing model 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 includes 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 provider's history of responsiveness.

Marketing Execution: This addresses awareness of the product in the market. We recognize companies that are consistently identified by our clients and often appear on their preliminary shortlists.

Customer Experience and **Operations:** These include management experience and track record, and the depth of staff experience — specifically in the security marketplace. The greatest factor in these categories is customer satisfaction throughout the sales and product life cycles. Also important are ease of use, overall throughput across different deployment scenarios, and how the firewall fares under attack conditions (see Table 1).

Evaluation Criteria	Weighting
Product/Service	High
Overall Viability (Business Unit, Financial, Strategy, Organization)	Standard
Sales Execution/Pricing	High
Market Responsiveness and Track Record	Standard
Marketing Execution	Low
Customer Experience	Standard
Operations	Standard

Table 1. Ability to Execute Evaluation Criteria
Source: Gartner (July 2013)

Completeness of Vision

Market Understanding and **Marketing Strategy:** These include providing a track record of delivering on innovation that precedes customer demand, rather than an "us, too" road map 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 via interactions with vendors in briefings and via feedback from Gartner clients on information they receive concerning road maps. Incumbent vendor market performance is reviewed yearly against specific recommendations that have been made to each vendor, and against future trends identified in Gartner research. Vendors can't merely state an aggressive future goal. They must enact a plan, show that they're following it and modify the plan as they forecast how market directions will change.
Sales Strategy: This includes preproduct and postproduct support, value for pricing, and clear explanations and recommendations for detection events and deployment efficacy. Building loyalty through credibility with a full-time midsize business security and research staff demonstrates the ability to assess the next generation of requirements.
Offering (Product) Strategy: The emphasis is on the vendor's product road map, current features, leading-edge capabilities, virtualization and performance. The quality of the security research labs behind the security features is considered. Credible, independent third-party certifications, such as Common Criteria, are included. Integrating 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 road maps to move beyond purely signature-based, deep packet inspection techniques. In addition, we weight vendors that are looking to add cloud-based services to their offerings.
Business Model: This includes the process and success rate of developing new features and innovation, along with R&D spending.
Innovation: This includes product innovation (such as R&D) and quality differentiators (such as performance, virtualization, integration with other security products, a management interface and clarity of reporting).
Geographic Strategy: This includes the ability and commitment to service geographies.
The more a product mirrors the workflow of the midsize business operations scenario, the better the vision. Products that are counterintuitive in deployment, or operations that are difficult to configure or have limited reporting, are scored accordingly. Solving customer problems is a key element of this category. Reducing the rule base, offering interproduct support and beating competitors to market with new features are very important components of a good vision (see Table 2).

Evaluation Criteria	Weighting
Market Understanding	High
Marketing Strategy	High
Sales Strategy	Standard
Offering (Product) Strategy	Standard
Business Model	Standard
Vertical/Industry Strategy	No Rating
Innovation	High
Geographic Strategy	Low

Table 2. Completeness of Vision Evaluation Criteria
Source: Gartner (July 2013)

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 economic security 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 good shortlist candidates.

Niche Players

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

Context

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

Market Overview

UTM appliances are used by midsize businesses to meet the requirements for secure Internet connectivity. For many small businesses, those requirements are often driven by regulatory demands (such as the PCI Data Security Standard), driving low to medium levels of security. Gartner sees very different demands from the enterprise and branch office firewall markets (see "Magic Quadrant for Enterprise Network Firewalls"), which generally require more-complex network security features, and show very different selection criteria.

Gartner generally defines SMBs by the number of employees and/or annual revenue they have. The primary attribute that is used most often is the number of employees. Small businesses usually have

fewer than 100 employees, while midsize businesses are usually defined as companies with fewer than 1,000 employees. The secondary attribute that is used most often is annual revenue. Small businesses are usually defined as those with less than $50 million in annual revenue, while midsize businesses are defined as those with less than $1 billion in annual revenue. Typically, 80% of the companies that Gartner analysts speak with have between 100 and 999 employees, and revenue between $100 million and $500 million.

The primary characteristic of midsize companies is that they are organizations with resource-constrained IT departments. They have a relative constraint in capital expenditures, operational budgets, number of IT staffers and depth of IT skills when compared with large enterprises. In keeping with this, UTM appliances are frequently used across midsize businesses as a low-cost way of meeting their network security requirements. Midsize businesses look at security differently, and show different buying behaviors compared with larger enterprises. The primary areas of difference are the following (in order of importance):

- A limited or nonexistent skilled security staff drives the need for ease of installation, configuration and use of channel-managed solutions.
- Less complex use of the Internet results in lower demand for high-end security features, such as application-level security and custom intrusion prevention filters.
- Limited security budgets drive acquisition costs to represent more than 60% of the overall decision weighting.
- Small businesses often perceive that they are not visible to attackers and, therefore, don't require as much security. However, financially motivated attackers have targeted small businesses, and the publicity over successful attacks has changed these businesses' perception.

The branch offices of larger companies have very different network security demands from midsize businesses, even though they may be of similar size. Gartner views branch offices' firewalls as extensions of the central firewall strategy (see "Bring Branch Office Network Security Up to the Enterprise Standard"). This drives large enterprises to often use low-end enterprise products at their branch offices to ensure interoperability, and to take advantage of economies of scale in getting larger discounts from their firewall vendors. This is not true in all cases, but in general, it is one of the major reasons why firewall vendors that sell successfully to the enterprise and SMB markets tend to have separate product lines for each market. For these reasons, Gartner allocates branch office firewall revenue to the enterprise firewall market, not the UTM market.

Small businesses with fewer than 100 employees have even more budgetary pressures and even fewer security pressures. Most security procurement decisions are driven by nontechnical factors and rarely feature competitive comparisons. For these reasons, this Magic Quadrant focuses on the UTM products used by midsize businesses, as defined above.

STRATEGIC PLANNING ASSUMPTIONS

Replacement of UTM by cloud options will remain at less than 5% through 2016; however, by then, most UTM devices will leverage cloud-assisted security and management features.

By 2016, 15% of SMBs will use mobile device management capabilities from their UTM platforms to handle mobility — up from less than 1% today.

NOTE 1
UTM REVENUE DIFFERENTIATION

Gartner does not include branch office firewall revenue as UTM revenue.

EVALUATION CRITERIA DEFINITIONS

Ability to Execute

Product/Service: Core goods and services offered by the vendor that compete in/serve 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 (Business Unit, Financial, Strategy, Organization): 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 and Track 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 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.