G00226111

Magic Quadrant for Unified Threat Management

Published: 5 March 2012

Analyst(s): John Pescatore, Greg Young

Unified threat management devices provide small and midsize businesses with multiple network security functions in a single appliance. Future trends in mobility and delivering security as a service will slow growth in the UTM market.

Market Definition/Description

For 2011, Gartner estimates that worldwide revenue in the UTM market totaled approximately $1.28 billion, which represents 19.5% growth over our estimate for 2010 (see Note 1). Gartner believes the UTM market will continue to grow faster than many other security markets, but we 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 2017.

Gartner defines the UTM market as multifunction network security products used by small or midsize businesses (SMBs). Gartner defines midsize businesses as those with 100 to 1,000 employees, and with revenue ranging from $50 million to $1 billion. However, the majority of midsize businesses' annual revenue is in the range of $100 million to $500 million, with head count ranging from 200 to 1,000 employees. UTM products for this market need to provide the following functions as a minimum:

- Standard network stateful firewall functions
- Remote access and site-to-site virtual private network (VPN) support
- Web security gateway functionality (anti-malware, URL and content filtering)
- Network intrusion prevention focused on blocking attacks against unpatched Windows PCs and servers

All UTM products contain other security capabilities, such as email security, Web application firewalls or data loss prevention. However, SMBs rarely enable these functions. Features such as built-in secure wireless LAN support and browser-based management, which don't appeal to large enterprises, are highly valued by SMBs in this market. SMBs that are evaluating UTM solutions should do so based on which of the above controls they will actually use, the quality of vendor and channel (and managed services) support that is available, and whether the management interface matches the skill level of local administrators.

Especially under the current economic conditions, 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 and eliminating hidden fees while easing upgrades when economic conditions improve.
- Provide product management features that simplify deployment and operation.
- Invest in enabling value-added resellers (VARs) and local system integrators to add services onto product sales, since the channel is often the major influencer on the buyers of UTM products.
- Focus on the needs of midsize businesses for the right network security at the right price, rather than trying to upsell the customer to enterprise products and capabilities.
- Be early to add new security features that are showing up as separate point products.

We see the following positive trends driving growth in the UTM market:

- A growing number of small (fewer than 100 employees) businesses.
- 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 represents replacing an existing product with the incumbent's newer version, or the incumbent being dislodged by a competitor.
- Visibility of advanced targeted threats that have hit small businesses in North America, causing demand for increased firewall, intrusion prevention system (IPS) and Web security gateway features such as application control. This demand represents replacing an existing product (such as a simple firewalling router) with a UTM product, either with the incumbent's newer version or with the incumbent being dislodged by a competitor.
- SMBs in emerging countries buying their first UTM product 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-specific vendors.

There are also some downward trends:

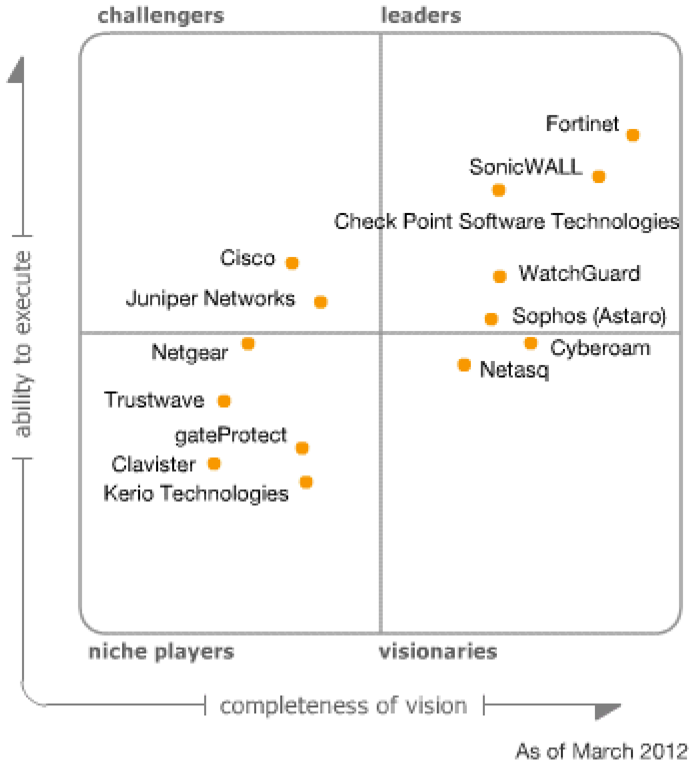
- The pricing and features of cloud-based secure Web gateway (SWG) services (see "Magic Quadrant for Secure Web Gateway") are very attractive to small businesses because they offer flexible pricing and meet the needs for securing mobile users. While most of those services only deal with Secure Sockets Layer (SSL) and HTTP traffic, they represent the majority of the needs of many small businesses, and can reduce their UTM needs to a simple firewall/router. Cloud-based SWG providers can also add support for other protocols, further diluting the demand for customer premises UTM solutions.
- The increased use of cloud-based email (such as Google Apps Premier Edition or Microsoft Office 365) reduces the demand for email security, since those services include integrated email antivirus.

- 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 a UTM appliance to the wired Internet service provider.
- 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 appliance and deploy enterprise network security platforms such as next-generation firewalls and SWGs.

Gartner believes the downward trends will outweigh the positive trends, thereby causing us to lower our long-term growth forecast for the UTM market from our previous outlook. These trends have also led to limited entries/exits of vendors into/from this market. In 2011, Sophos acquired Astaro and IBM exited the UTM market. There were no new startup vendors, but Clavister and Kerio Technologies satisfied Gartner's evaluation criteria and have been added in 2012. Barracuda Networks' current firewall product did not meet the UTM criteria, but its product road map indicates that it will be entering this area in the future (see Figure 1).

Magic Quadrant

Figure 1. Magic Quadrant for Unified Threat Management



Source: Gartner (March 2012)

Vendor Strengths and Cautions

Check Point Software Technologies

Check Point Software Technologies is a well-known pure-play security company that has been shipping UTM products since 2004. Headquartered in Israel with R&D in Israel and California, Check Point has a range of appliances and software "blades" that implement network security functions. Check Point's UTM offerings include the 2200, 4200 and 4800 appliances, which range from 2 Gbps to 6 Gbps of IPS throughput. The Check Point SG80 is aimed at branch offices and offers up to 750 Mbps of IPS throughput. The Check Point UTM-1 series ranges from 1 Gbps to 4 Gbps of IPS throughput. The Safe@Office appliances offer up to 1 Gbps of firewall throughput.

Strengths

- Trained personnel and external support are easy to find for Check Point products.
- Check Point offers a managed service starting at less than $20 per device per month, an aggressive price point compared with other managed service offerings.
- For the high end of the UTM market, Check Point management console is highly rated.

Cautions

- Check Point's product and service pricing often make its total capital expenses pricier than comparable offerings from competitors.
- Regional integrators and smaller VARs tend to recommend competing products for midsize businesses, often driven by Check Point licensing complexity and better SMB channel support from competitors.

Cisco

Cisco is the dominant network infrastructure vendor, and has a broad network security product portfolio. In the small and midsize space, Cisco has a number of product offerings. The Cisco RV Series of products provides VPN and firewall functions for the small office/home office (SOHO) environment. The SA500 Series Security Appliances provide UTM functionality that aligns with the needs of the midsize business market using IPS, email and Web security options, some of which include integrated wireless LAN (WLAN) access points. Low models of Cisco Integrated Services Routers (ISRs) and the Cisco Adaptive Security Appliances (ASA) are generally aimed more at branch offices than the UTM market. Several of these models have connectors to the Cisco ScanSafe Web security-as-a-service offering, which is attractive to small businesses.

Strengths

- Cisco's continued dominance in the network infrastructure market means its UTM products are often chosen without looking at competing offerings.

- Cisco has enhanced the support (which was already strong) it provides to its channel partners serving the midmarket.
- In the core firewall and IPS areas, Cisco's UTM capabilities are good enough at an attractive price.

Cautions

- While competitors made advances (such as adding application control features and more granular reporting), Cisco's network security product line stagnated in 2011.
- Cisco has laid out an aggressive road map for product improvements in 2012, but has had lots of organizational turmoil recently and many changes in strategy, resulting in missed deadlines.
- At the high end of the UTM market, Cisco's security management offerings are extremely weak, particularly in the amount of effort it takes to manage multiple appliances.

Clavister

With head offices in Sweden, Clavister sells UTM as part of the Security Gateway (SG) product line. Each SG model has a Pro option that has greater throughput and performance. The majority of Clavister's security business is in security gateways for carriers and service providers, and the company has significant business in the OEM of UTM technology elements. Clavister's primary focus is on the enterprise and telecommunications provider markets.

Strengths

- Clavister has a large number of devices under support, and the extent of the OEM business provides validation for the company's technology focus.
- Users rate management capabilities as strong when multiple UTM units are deployed.

Cautions

- It focuses on EMEA, with recent operations expanded to Asia/Pacific — and has a limited international presence compared with competitors.
- The company is spread across many horizontal industries and security lines of business, with few UTM models and a limited focus on SMB compared with competitors.
- Clavister does not have a Web application firewall, and security features such as application control will not be available in the UTM product until later in 2012.

Cyberoam

India-based Cyberoam has been shipping appliances since 2006. With a high level of channel loyalty and a strategy of adding in features not usually present in competing products, Cyberoam has expanded its sales and broadened its geographic coverage. Formerly focused solely on the midmarket, Cyberoam has expanded toward the consumer and SOHO placements.

Strengths

- Gartner sees Cyberoam often being selected where bandwidth is expensive or unreliable, for the multiple link management and 3G/WiMAX features.
- Users like logging, alerting and forensic capabilities via Cyberoam's iView, and the on-appliance Web Application Firewall.
- Cyberoam maintains a high level of loyalty from its channel partners.
- Industry-specific features such as outbound spam protection and SMS authentication sell well into hotel/hospitality/service providers.
- Cyberoam usually scores very well on price in the competitive UTM selections seen by Gartner.

Cautions

- Cyberoam is still not widely regarded as an option for global businesses due to limited support in North America and Western Europe.
- It is rarely seen on competitive shortlists, and rivals don't mention it as a "top competitor."

Fortinet

Fortinet, which is based in California, has been focused on UTM appliances since 2002. From the start, Fortinet has focused on using custom application-specific integrated circuits for network processing and content inspection to reach high performance levels. Fortinet offers nine FortiGate UTM appliances aimed at the midsize market, ranging from 20 Mbps to 1 Gbps of firewall throughput. Several versions offer integrated WLAN access points, while others include voice over IP gateway and IP PBX functionality.

Strengths

- Fortinet continues to have the highest visibility of UTM providers among Gartner clients, and is the company most frequently mentioned by competitors.
- The product line has aggressive price/performance points and an easy migration path as network speeds increase.
- The Fortinet UTM line has strong channel and managed security service provider (MSSP) support.
- FortiGuard Labs is a strong source of threat and vulnerability information.

Cautions

- While the management user interface has improved, it is still rated lower than competing offerings by Gartner clients.
- Users would like to see more flexible log filtering and viewing.

gateProtect

gateProtect, which is based in Germany, has been shipping UTM appliances since 2002. Its Series A appliances are the primary offerings aimed at midsize businesses. Overall, gateProtect's UTM models range from 1 Gbps to 18 Gbps of firewall throughput. All gateProtect appliances are also available as VMware images.

Strengths

- gateProtect's unique approach to graphical user interface simplifies administrative tasks and reduces configuration errors.
- It offers competitive pricing.

Cautions

- gateProtect has limited application awareness in firewall policies compared with competing offerings.
- It focuses on Germany and EMEA — and has a limited international presence compared with competitors.
- gateProtect has low visibility and rarely appears on Gartner client shortlists, nor is it referenced in inquiries.

Juniper Networks

Juniper is a large network infrastructure provider that has a wide range of firewall, IPS and remote access security solutions. Juniper's SRX Series Services Gateways include Juniper's UTM offering for midsize businesses as well as enterprise branch offices. This product line contains models that range from 650 Mbps to 7 Gbps of firewall throughput. In 2011, Juniper added the SRX110 (650 Mbps) and SRX210E (750 Mbps) models to the low end of the lineup. In late 2010, Juniper acquired Altor Networks, a vendor of software firewalls for virtualized environments, but Juniper does not have a virtual appliance offering for the midmarket.

Strengths

- For multiple UTM appliance scenarios, Juniper's pricing was often cited as a reason for selection.

- For upper-end midsize businesses (500 to 999 employees), Juniper's NSM management console was highlighted for ease of deployment and management.

Cautions

- Compared with most competitors, Juniper's 2011 midmarket offerings did not advance in areas such as application control and spam filtering.
- Juniper has limited channel support for the midmarket UTM needs.
- Users cited Juniper's reporting as in need of improvement.

Kerio Technologies

Headquartered in California, Kerio first shipped a UTM (WinRoute) product in 2004. The Kerio Control Box appliance is offered in two models that range from 90 Mbps to 400 Mbps of IPS throughput. The Kerio Control software is also available to run on Windows servers or as a VMware Virtual Appliance.

Strengths

- It is easy to deploy and use, especially where other Kerio messaging and voice products are in use.
- It supports multiple antivirus signature feeds.

Cautions

- Kerio's visibility is very low, and its partner support is limited.
- Kerio's use of Sophos antivirus signatures is a disadvantage when competing with Astaro.

Netasq

Based in France, Netasq has been shipping UTM products since 1999. The Netasq U Series of appliances ranges from 200 Mbps to 1 Gbps of firewall throughput, with the U30 (200 Mbps) and U70 (600 Mbps) being the primary offerings aimed at SMBs. The U Series includes hardware VPN acceleration. Netasq also offers the V50, V100, V200 and V500 Virtual Appliances for SMBs, which run on VMware vSphere and Citrix XenServer. The V-series software is free for SMB use, but annual maintenance and update services require a fee.

Strengths

- Simplified licensing for procurement and support is cited as positive.
- Integration of the firewall and IPS engine increases throughput and eases deployment.
- Users continue to highly rate support from Netasq and channel partners.

Cautions

- Netasq has not increased visibility outside of Europe.
- Netasq's channel is not as extensive as many of its competitors, which puts it at a disadvantage when support in multiple regions is required.
- Users say the integration of UTM features beyond firewall and IPS needs improvement. Version 9 has addressed this issue.

Netgear

Based in California, Netgear is a large provider of networking and storage products that entered the UTM market in late 2009. The ProSecure UTM appliance line is the primary offering for midsize businesses, with six models ranging from 90 Mbps to 900 Mbps of firewall throughput. In 2011, Netgear introduced a 150-user version and a version with an integrated VDSL modem. Netgear also sells STM Series appliances, which provide Web and email security functions.

Strengths

- Netgear offers a low-cost solution with features tailored to the midmarket.
- It has a strong channel with good reach into midsize IT environments.
- The breadth of its midmarket product line covers security, backup and wireless/wired network infrastructure, providing easily integrated solutions for midsize businesses.

Cautions

- The Netgear brand has high visibility in consumer-oriented markets, but is not frequently mentioned by competitors or Gartner clients.
- It has limited application awareness in firewall policies. Netgear will address this in 2012.
- It has no multidevice centralized management. Support for multiunit management is on Netgear's road map.
- Netgear's product line has limited scalability.

SonicWALL

Headquartered in California, SonicWALL was acquired and taken private by private equity firm Thoma Bravo in 2010. SonicWALL has been shipping UTM products since 1998, and has two product lines aimed at the midmarket. The TZ Series ranges from 100 Mbps to 200 Mbps of firewall throughput, and includes an optional integrated WLAN access point. The NSA 200 Series supports firewall throughput of between 600 Mbps and 2.75 Gbps, and offers SSL inspection and application control.

Strengths

- SonicWALL has strong global partner and MSSP support.
- SonicWALL is well-known in the UTM space and appears frequently on Gartner client shortlists.
- The graphical elements of SonicWALL's management interface are consistently highly rated.
- SonicWALL's release of new features has kept up with midmarket needs, and has been matched by usability enhancements.

Cautions

- SonicWALL's push into the high end with SuperMassive may divert resources and focus from the UTM market.
- SonicWALL does not offer a virtual appliance for the UTM space.

Sophos (Astaro)

Based in Massachusetts, with R&D in Germany, Astaro has been shipping UTM products since 2001. Astaro was acquired by endpoint security vendor Sophos in May 2011, but the Astaro branding will be maintained until the next major release in April 2012. Its UTM product line is branded as the Astaro Security Gateway. Hardware appliances are available that range from 45 Mbps to 575 Mbps of overall UTM throughput. The Astaro Security Gateway is available in hardware and software versions that support firewall, IPS, VPN and other functions. The product is also available as a virtual appliance that runs on VMware, Citrix, KVM and Hyper-V, along with an Amazon Machine Image (AMI) for Amazon's EC2. Astaro offers a series of Gateway "Extension" products, such as Wi-Fi access points and remote management appliances that integrate with the Astaro Command Center management console.

Strengths

- Astaro's Red appliance and secure access point products enable it to offer very attractive bundles to vertical industries such as retail, healthcare and education.
- Ease of deployment, use and expansion are consistently cited as decision factors favoring Astaro.
- The acquisition of Astaro by Sophos should increase financial resources and channel strength, and improve visibility.

Cautions

- Astaro has not shown up on many Gartner client shortlists, and is not cited by competitors in our surveys as a major factor.
- Users are looking for improvements in the granularity of Astaro's reporting, which Sophos plans to address in a 2012 release.

- Sophos must avoid the temptation to drive toward UTM solutions that depend on Sophos on the endpoint.

Trustwave

Based in Illinois, Trustwave is a large and rapidly growing service provider that focuses on the worldwide PCI compliance requirements. Trustwave has acquired a number of security products over the years, such as SecurePipe's managed services business and Linux-based firewall/VPN technology in 2006. SecurePipe had deployed firewall/VPN technology as early as 1996. The Trustwave Unified Threat Management appliance is available in three models: The XS-10 has a combined firewall and VPN throughput of 150 Mbps, while the TS-100 and TS-200 ranges are rated 130 Mbps to 300 Mbps. Trustwave offers a UTM managed service based on these devices.

Strengths

- Trustwave offers managed UTM services that provide a low-cost means of meeting PCI and other network security requirements.
- Trustwave's pricing is aggressive and attractive for many smaller businesses.
- Trustwave's management platform is simple and easy to use for environments that do not require frequent policy changes.

Cautions

- The Trustwave UTM offerings did not advance in 2011 compared with competitors.
- Trustwave's visibility in the UTM market, outside of PCI-centric environments, is very low.
- Trustwave's UTM offerings have a very low level of channel support outside of Trustwave's own services.

WatchGuard

Privately held WatchGuard is headquartered in Washington and has been shipping UTM appliances since 2000. WatchGuard's primary UTM offering for midsize businesses is the XTM 5 Series, which is composed of models ranging from 850 Mbps to 2.3 Gbps. WatchGuard also offers XTM 2 Series and XTM 3 Series UTM appliances for small businesses, and the Extensible Content Security (XCS) line of email/Web security appliances for midsize businesses that already have separate firewall solutions. WatchGuard XTMv is a virtual appliance that runs on VMware.

Strengths

- A balance between ease of use and strong security is consistently cited as a reason why clients choose WatchGuard.

- WatchGuard had the highest use rate of multiple features (beyond firewall, IPS and URL blocking) of all vendors.
- Users and channel partners report high reliability on the appliances and strong support from WatchGuard.

Cautions

- WatchGuard has decreased in visibility to Gartner clients, and was less frequently mentioned by competitors compared with other vendors.
- Users cite shortcomings in reporting performance and functionality.
- MSSP support for WatchGuard appliances is limited compared with the major competitors.

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

- Clavister
- Kerio Technologies

Dropped

- IBM announced its end of support for the Proventia Network Multi-Function Security product line in November 2011.

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 as a minimum:
  - Network security (stateful firewall and intrusion prevention)
  - Web security gateway

  - 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 $5 million during the past year, 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 company didn't otherwise meet the inclusion criteria, or isn'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 Web application firewalls — 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 $5 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 (such as 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 multifunction firewall revenue, competitive wins versus key competitors (which is compared with Gartner data on such competitions held by our clients), and devices in deployment. The number of multifunction firewalls shipped isn't a key measure of execution. Instead, we consider the use of these firewalls and the features deployed to protect the key business systems of Gartner midsize business clients.

Sales Execution/Pricing: This includes pricing, the number of deals, the installed base, and the strength of sales and distribution operations in the vendors. 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 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 cycle. Also important is ease of use, overall throughput across different deployment scenarios, and how the firewall fares under attack conditions (see Table 1).

Table 1. Ability to Execute Evaluation Criteria

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

Source: Gartner (March 2012)

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 interaction with vendors in briefings and 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, and 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 aren't intuitive in deployment, or operations that are difficult to configure or have limited reporting, are scored accordingly. Solving customer problems is a key element of this category. Reducing the rule base, offering interproduct support and beating competitors to market with new features are foremost (see Table 2).

Table 2. Completeness of Vision Evaluation Criteria

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

Source: Gartner (March 2012)

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 a product that's 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 in their approach to UTM devices for midsize businesses. Some Niche Players focus on specific vertical industries or geographies. If midsize companies are already clients of these vendors for other products, or fit into those geographies or vertical industries, then Niche Players can be shortlisted.

Context

Different business and threat environments for SMBs result in significantly different network security requirements from those of large enterprises. 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 Standards), 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 second attribute most often used 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 Gartner analysts speak with have between 100 and 999 employees, and have 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):

- 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 their 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. 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 do sell successfully to both 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 pressure and even less security pressure. 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.

Recommended Reading

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

"Magic Quadrants and MarketScopes: How Gartner Evaluates Vendors Within a Market"

"Magic Quadrant for Enterprise Network Firewalls"

"Magic Quadrant for Unified Threat Management"

"Astaro Acquisition Will Extend Sophos' Midmarket Security Offerings"

Evidence

- Webmonkey survey of references provided by vendors
- Continuing stream of client inquiries on UTM area
- Vendor briefings from vendors
- Open-source research of vendor websites and user comment sites
- Proprietary source search by Gartner Secondary Research Services

Note 1 UTM Revenue Differentiation

As discussed in the Market Overview section, 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 and skills, 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 pre-sales activities and the structure that supports them. This includes deal management, pricing and negotiation, pre-sales 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 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.

Regional Headquarters

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

Japan Headquarters
Gartner Japan Ltd.
Aobadai Hills, 6F
7-7, Aobadai, 4-chome
Meguro-ku, Tokyo 153-0042
JAPAN
+81 3 3481 3670

European Headquarters
Tamesis
The Glanty
Egham
Surrey, TW20 9AW
UNITED KINGDOM
+44 1784 431611

Latin America Headquarters
Gartner do Brazil
Av. das Nações Unidas, 12551
9° andar—World Trade Center
04578-903—São Paulo SP
BRAZIL
+55 11 3443 1509

Asia/Pacific Headquarters
Gartner Australasia Pty. Ltd.
Level 9, 141 Walker Street
North Sydney
New South Wales 2060
AUSTRALIA
+61 2 9459 4600

The information contained in this publication has been obtained from sources believed to be reliable. Gartner disclaims all warranties as to the accuracy, completeness or adequacy of such information and shall have no liability for errors, omissions or inadequacies in such information. This publication consists of the opinions of Gartner's research organization and should not be construed as statements of fact. The opinions expressed herein are subject to change without notice. Although Gartner research may include a discussion of related legal issues, Gartner does not provide legal advice or services and its research should not be construed or used as such. Gartner is a public company, and its shareholders may include firms and funds that have financial interests in entities covered in Gartner research. Gartner's Board of Directors may include senior managers of these firms or funds. Gartner research is produced independently by its research organization without input or influence from these firms, funds or their managers. For further information on the independence and integrity of Gartner research, see "Guiding Principles on Independence and Objectivity" on its website, http://www.gartner.com/technology/about/ombudsman/omb_guide2.jsp.