Magic Quadrant for Unified Threat Management

Gartner RAS Core Research Note G00205369, John Pescatore, Bob Walder, 22 October 2010, R3494 01272011

Unified threat management devices provide all-in-one security in a single appliance. Is the one-stop-shop approach suitable for enterprise customers, or is UTM still aimed squarely at the small-and-midsize-business market?

WHAT YOU NEED TO KNOW

Different business and threat environments for small or midsize businesses (SMBs) result in significantly different network security requirements than those of large enterprises. Although branch offices of some larger enterprises have requirements that are similar to midsize businesses, this is not always the case. The unified threat management (UTM) market consists of a wide range of suppliers that meet the common core security requirements of smaller enterprises, but businesses need to make their decisions by mapping their threat and deployment patterns to the optimal offering.

MAGIC QUADRANT

Market Overview

UTM appliances are used by midsize businesses to meet required network security levels for Internet connectivity. For smaller businesses, those requirements are often driven by regulatory demands (such as the Payment Card Industry Data Security Standards), rather than any detailed security/risk analysis.

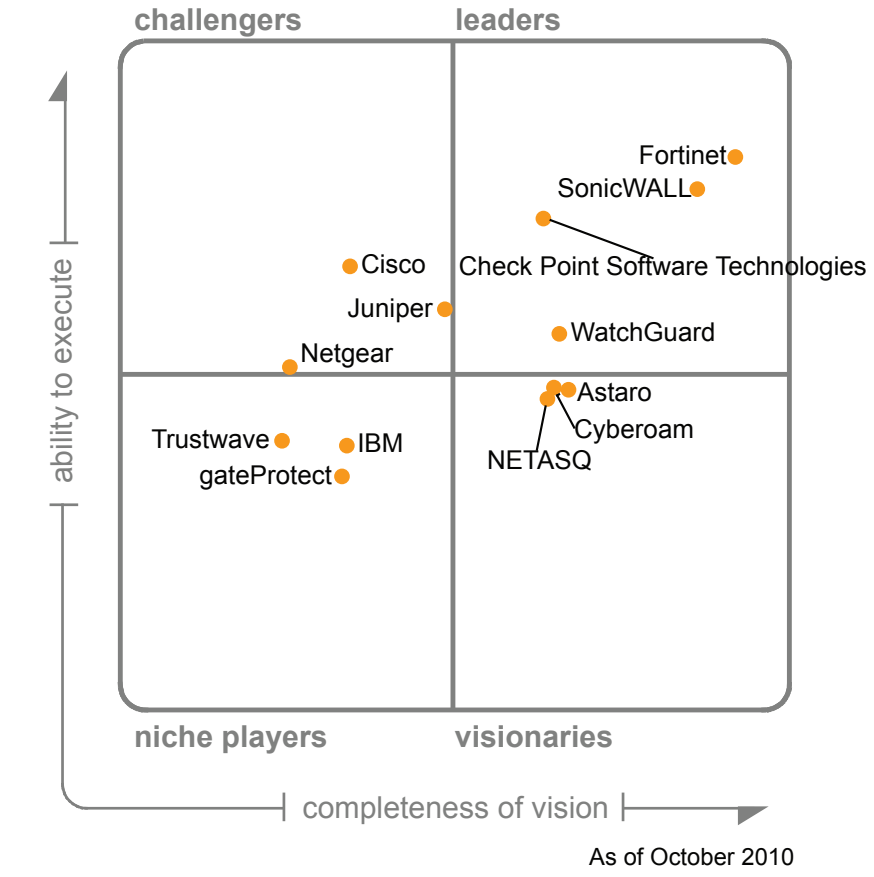
In the past, Gartner has called this market "SMB multifunction firewalls" and avoided using the term "unified threat management," because threats are never really "managed," and the protections within multifunction firewalls are rarely truly "unified." However, the term "UTM" now has broad recognition in the market, requiring a change of title (although not focus). This market is also distinguished from the enterprise and branch-office firewall markets, which generally require more-complex network security features and show very different selection criteria.

Gartner

Gartner defines midsize businesses as those with 100 to 1,000 employees, and revenue ranging from $50 million to $1 billion. However, the majority of midsize business annual revenue is in the range of $100 million to $500 million, with head count ranging from 200 to 1,000. Multifunction network security appliances, commonly called UTM appliances, are frequently used across midsize businesses due to their particular security requirements. Midsize businesses look at security differently and show different buying behaviors compared with larger enterprises. The primary areas of difference are (in order of importance):

- Limited or nonexistent skilled security staff drives the need for ease of installation, configuration and use or, alternatively, outsourced solutions.
- Lower visibility to threats drives less corporate attention to security.
- 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 IT staff and IT security budgets require lower price points for acquisition and ownership.

Figure 1. Magic Quadrant for Unified Threat Management



Source: Gartner (October 2010)

This Magic Quadrant focuses on midsize businesses, as described above. At the very low end of the market, small businesses with 50 to 200 employees have much more budgetary pressure and even less security pressure. Although many vendors also have products focused at the very low end, most procurement decisions are driven by nontechnical factors and rarely feature competitive comparisons.

Market Definition/Description

In 2009, the worldwide UTM market was worth approximately $1.5 billion, representing 25% growth over Gartner's 2007 estimate, with a forecast of 20% to 25% compound annual growth rate through 2012. This market is largely driven by turnkey appliance solutions, although there are pure software UTM solutions available.

Although the enterprise firewall market is highly penetrated, midsize businesses are often buying their first UTM product, or upgrading from a very simple firewall product, representing much higher unit growth than in the enterprise market. However, price pressure in this market is much more intense, resulting in significantly lower price points, which decrease the average overall revenue growth.

The UTM market continues to be highly competitive, with a mix of large and small vendors. Although many of the products in the market look like "Swiss army knives" with just about every possible network security function thrown into the mix, in talking with

Gartner clients and vendor customer references using the products, we find the most important security controls to be (in priority order):

- 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

Other features, such as e-mail security, Web application firewalls or data loss prevention, are rarely enabled. Features such as built-in secure wireless LAN support that don't appeal to large enterprises are highly valued in this market. Midsize businesses that are evaluating UTM solutions should evaluate products based on which of the above controls they will actually use, the quality of vendor and channel (and managed services) support available, and whether the management interface matches the skill level of local administrators.

The financial and staffing constraints on midsize businesses put a high premium on ease of use, vendor/channel support and price/performance. Leading vendors will:

- Focus on the simplicity of deployment and operation.
- Provide proactive attention to channel partners, because value-added resellers or local system integrators will often be the greatest influencers of this market, especially at the low end of the midsize range.
- Use aggressive pricing that reduces upfront costs and enables easy upgrading as business conditions improve.
- Simplify the pricing model, avoiding multiple subscription costs and hidden fees that kick in after the first year.
- Focus on midsize enterprise needs, rather than attempting to force downsized enterprise products and strategies into this market.

Similar products are often used at branch offices of larger enterprises. However, we consider branch-office firewalls to be part of the enterprise firewall network market, because they're often selected and deployed as extensions of the central firewalls, are tied in with WAN optimization strategies, and require a minimal set of network security features (mainly intrusion prevention and URL filtering) beyond simple firewall and site-to-site VPN support. For this reason, large enterprise firewall vendors have a slow success rate in the midsize market, because the core needs (for example, ease of use and "check the box" security) are radically different from those required by large enterprises. Firewall vendors that successfully sell to both markets tend to have two lines of products with clear differentiation (not just different SKUs) between the product lines. Similarly, vendors that succeed in the midsize market often fail as they try to move upstream, because simply having a faster UTM product does not meet large enterprise needs. Indeed, the plethora of features and capabilities included in typical UTM products will often count against vendors when selling into the enterprise, which requires higher performance and fewer security "bells and whistles."

For these reasons, Gartner believes that the UTM market remains squarely focused on midsize enterprises. Growth in this market will be driven by three scenarios:

1. Midsize businesses in North America and Western Europe are refreshing their first-generation multifunction firewalls with higher capacity and better Web security gateway features to deal with increased botnet and other targeted Web threats. This market represents replacing an existing product either with the incumbent's newer version or with the incumbent being dislodged by a competitor.
2. Midsize businesses in other geographies are moving to broadband Internet connectivity and are buying their first business-class UTM product. This scenario represents greenfield growth for the market, often with preference for country-specific vendors.
3. Midsize and large enterprises that, either due to economic downturns or due to changes in IT and security governance from centralized to distributed, are looking to take advantage of low price points and "check the box" capabilities. Barring another downturn, Gartner does not see this scenario as a major contributor to market revenue.

Threats continue to evolve over time, and audit and regulatory demands will drive midsize businesses to demand more-advanced features, but we do not believe there will be major changes in these scenarios before 2012. A larger driver will be the selection of preferred UTM products by managed security service providers (MSSPs) that target the midsize market. Gartner believes that those MSSPs will affect midsize business UTM selection, but we do not believe that UTM vendors that offer managed services based on their own products will have any advantage in the UTM market.

Inclusion and Exclusion Criteria

Inclusion Criteria

UTM companies that met the market definition/description were considered for 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
  - E-mail security
  - They regularly appeared on Gartner midsize client shortlists for final selection.
  - They achieved UTM product sales (not including maintenance and so forth) 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.
- Products aren't usually deployed as the primary, Internet-facing firewall (for example, proxy servers and network intrusion prevention system [IPS] solutions).
- Products are built around personal firewalls, host-based firewalls, host-based IPSs and Web application firewalls – all of which are distinct markets.
- Solutions are typically delivered as MSS, to the extent that product sales didn't reach the $5 million threshold.

O2Security and eSoft were evaluated, but didn't meet the inclusion requirements for this Magic Quadrant. Gartner will continue to monitor their progress.

As pure managed service vendors, Untangle and Network Box USA were assessed, but not included in this Magic Quadrant.

Added

- gateProtect
- Trustwave
- Netgear

Dropped

- Clavister failed to respond to survey requests and does not appear in Gartner shortlists or client inquiries.
- McAfee retired the SnapGear product line and does not currently have a product to address this market.

Evaluation Criteria

Ability to Execute

Product/Service: This also includes customer satisfaction in deployments, and considers factors related to getting products sold, installed, supported and in users' hands. Strong execution means that a company has demonstrated to Gartner that its products are successfully and continuously deployed in midsize businesses, and win a large percentage in competition with other vendors. Companies that execute strongly generate pervasive awareness and loyalty among Gartner clients, and generate a steady stream of inquiries to Gartner. Execution isn't primarily about company size or market share, although those factors can affect a company's ability to execute. Sales are a factor; however, winning in competitive environments through innovation, quality of product and ease of use is foremost over revenue. Key features, such as ease of deployment, console quality, price/performance, range of models, secondary product capabilities (such as logging, event management and compliance), 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. Pre- and post-sales 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 total cost of ownership (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 this category 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.

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 (October 2010)	

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 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 pre- and post-product 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 into 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 leading competitors on features are foremost.

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	Sandard
Vertical/Industry Strategy	No Rating
Innovation	Standard
Geographic Strategy	Low
Source: Gartner October 2010)	

Leaders

The Leaders quadrant contains vendors at the forefront of making and selling multifunction firewall 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. Challenger 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 they 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, then Niche Players can be shortlisted.

Vendor Strengths and Cautions

Astaro

Astaro's Security Gateway product line consists of a range of hardware, software and virtual appliances designed for midsize businesses. The latest version provided improvements in management, administration and reporting, while still maintaining ease of use.

Access to the basic firewall/VPN package is free (for limited use for up to 50 addresses), with a separate network security subscription offering load balancing, site-to-site VPN, and Secure Sockets Layer (SSL) VPN capabilities. Customers can also purchase the Web security subscription (antivirus, anti-spam and anti-malware) or e-mail subscription (such as SMTP/POP). Virtual appliances are available for VMware and Citrix environments.

Strengths

- Support for Cisco's IPsec clients simplifies the migration path from Cisco PIX firewalls.
- Ease of entry and a free-of-charge offering enable firewall administrators to "try before they buy."
- Customers like the ease of use.

Cautions

- Astaro has limited visibility among Gartner clients outside of EMEA.
- Users have reported that the IPS can be difficult to tune accurately to eliminate false positives.

Check Point Software Technologies

Check Point Software Technologies is one of the largest vendors in the enterprise security market. It offers five product lines for the midsize business: Series 80, UTM-1, software versions for installation on general-purpose servers using the SecurePlatform (SPLAT) environment, Safe@Office/SofaWare Technologies, and appliances from OEMs.

Series 80 and UTM-1 appliances are packaged with security solutions focused on midsize business needs, and can include one or more security modules – termed "software blades" – including firewall, intrusion prevention, antivirus, anti-spyware, DLP, URL filtering, Web security, and anti-spam software blades. Additional blades can be added as needed, and virtual appliances are available. Check Point VSX-1 virtual appliances include Firewall, SmartDefense (IPS), Antivirus and URL Filtering. Check Point VE virtual appliances include the full UTM feature set – Firewall, IPS, Antivirus, Anti-Malware and URL Filtering.

Strengths

- Check Point has strong centralized management capabilities.
- Its software blade architecture allows customers to change the appliance configuration easily.
- It's easy to find security personnel and support contractors with Check Point experience.
- Customers report that support is strong.

Cautions

- Some users have reported that the pricing structure of the software blades can make entry-level configurations for smaller businesses more expensive than with previous licensing arrangements.
- Much of the Check Point channel is not targeted at the midsize business.
- No user/group awareness in firewall policies exists in the current version.
- Gartner clients and independent tests report that Check Point's IPS signature quality is low.

Cisco

Cisco UTM products for the small (one to 250 users) business are in four product lines: the Cisco RV Series Small Business Routers (formerly Linksys), the Cisco SA Series Small Business Security Appliances, the Cisco Integrated Services Routers (ISR), and the Cisco Adaptive Security Appliances (ASA). UTM products for the midsize (250 to 1,000 users) business are in two product lines: the Cisco Integrated Services Routers (ISR) and the Cisco Adaptive Security Appliances (ASA).

A wide range of products provides a migration path from entry-level to higher-capability devices, and familiarity with the Cisco infrastructure products within an enterprise often makes this range a first choice for branch-office deployments.

Strengths

- Cisco's widely recognized brand worldwide makes it an almost automatic choice for most shortlists.
- Users like the security of a global support and sales operation.
- Cisco provides a smooth transition from entry-level to higher-capability devices for small businesses as they grow.

Cautions

- No user/group awareness in firewall policies exists in Cisco's current version.
- There's limited application awareness in firewall policies.
- Pricing is not always competitive.
- Cisco lacks an understanding of the midsize business market due to an ingrained enterprise mind-set. Customers report that Cisco salespeople often use a midsize business opportunity to upsell other higher-value Cisco products/services.

Cyberoam

Based in India, which is also home to the majority of its installed base, Cyberoam has several integrated UTM appliances in its CRi range aimed at the midsize business market. These products provide a complete set of features, including firewall, VPN (SSL VPN and IPsec), gateway antivirus and anti-spyware, gateway anti-spam, IPS, content and application filtering, and bandwidth management and multiple-link management on a single platform.

The company attempts to differentiate on identity-based network access, which provides access control that links IP addresses with directory identity (such as Active Directory), application control and bandwidth management.

Strengths

- Cyberoam has continued to expand its distribution network outside its native India, particularly in EMEA.
- It has excellent logging, alerting and forensic capabilities via Cyberoam iView.
- Cyberoam has a forward-thinking partner/training program.
- It is focused on the midsize space.
- It offers competitive pricing.

Cautions

- Cyberoam is still not widely regarded as a “global player” due to limited penetration in the U.S., despite its presence in more than 75 countries.
- It is rarely seen on competitive shortlists, and rivals don’t mention it as a “top competitor.”

Fortinet

Fortinet is well-established as a UTM provider with a wide model range. All Fortinet security technologies are developed in-house – it doesn’t resell products from others – and Fortinet has its own antivirus, URL and IPS signature research teams. Fortinet offers 20 multifunction firewall models, many of which are suitable for midsize business deployments. The FortiOS 4.0 release includes WAN optimization, application control, data leakage prevention and SSL inspection.

Fortinet’s midsize offering is based on a single appliance, including firewall, IPS, VPN, traffic shaping, antivirus, anti-spyware, anti-spam, Web content filtering and application control (for example, instant messaging and peer to peer).

Fortinet has opted to use custom ASICs for network and content processing to provide high levels of performance at low prices. Models are available with built-in wireless access points, and PC Card slots extend the security capabilities to wireless broadband deployments for mobile retail and small office/home office applications.

The Web-based management interface is consistent across all Fortinet appliances, although it is not always the most intuitive to use. The separate FortiManager appliance is used for centralized management.

Strengths

- Fortinet shows up on most shortlists and continues to innovate. In the midsize market, it is considered a “safe choice,” owing to its strong presence in this market.
- Fortinet’s use of custom hardware, combined with aggressive pricing, continues to provide high levels of price/performance.
- It has flexible application- and user-aware firewall policy capabilities, tied closely to IPS policies.
- It has a good migration path in terms of device capacities and capabilities from entry level to small enterprise.

Cautions

- Fortinet’s IPS is difficult to tune accurately.
- The user interface (UI) is not the most intuitive, especially for nonexperts.
- A lack of independent performance testing hampers the ability for more-advanced purchasers to verify Fortinet’s performance claims.
- On-device logging and reporting are very basic. Users complain that there is too little memory on the devices to perform analysis – a separate FortiAnalyzer product is required.

gateProtect

gateProtect is a German company that focuses on producing multifunction security appliances. A number of UTM appliances are available: The O-series is for companies with 10 to 15 users, the A-series is for 20 to 100 users, and the X- and Z-series are for companies with up to 10,000 users.

The main reason customers choose gateProtect over its competitors is because of its unique graphical user interface (eGUI). The configuration desktop is process-oriented, rather than being presented as a list of firewall rules, as with most of the competition. The administrator places icons, representing the relevant network components, on the screen, and defines the data flows and permitted services between those icons in a graphical drag-and-drop manner. When the configuration is complete, the data is sent to the gateProtect configuration engine, which analyzes the configuration and converts the graphical representation into a set of network rules.

A virtual appliance offering is available for VMware environments.

Strengths

- gateProtect’s unique approach to GUI simplifies administrative tasks.
- It offers competitive pricing.

Cautions

- gateProtect has limited application awareness in firewall policies.
- 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 or is referenced in inquiries (mainly German clients).

IBM

Long a leading purveyor of enterprise IPS, IBM offers its all-in-one firewall, the Proventia Network Multi-Function Security (MFS) product, which is available in seven models. During the past year, IBM has refined its go-to-market strategy with MFS to align it more with midsize market needs. IBM has lowered prices on some models to bring them more in line with competing products. Its latest release includes a Web application firewall.

Strengths

- The ISS brands retain value to security decisions makers, mainly because of the continued visibility of X-Force.
- IBM offers one of the most accurate IPSs on the market.
- Its central administration and reporting are strong.

Cautions

- No user/group awareness in firewall policies exists in IBM's current version.
- The Proventia brand has been hurt due to lack of attention since the ISS acquisition. IBM's reorganization putting the ISS business unit into the Tivoli software business unit makes long-term focus on the UTM market questionable.
- Gartner does not often see UTM shortlists containing IBM, and instances of customers replacing IBM UTM devices have increased in the past 12 months.
- Customers continue to complain that the device response is sluggish during management operations.

Juniper

Juniper first introduced UTM capabilities for NetScreen security appliances in 2001. In 2009, it introduced the SRX Series Services Gateways for the branch, which reflect the movement across the security product line to the Junos operating system in affordable form factors. Direct management access is provided to all Junos devices via the J-Web Web-based interface, while the Juniper Network and Security Manager (NSM) provides a single centralized management interface across all the products.

In 2009, Juniper grew its position in the midsize market with products and partnerships tailored to this segment, and added routes to market via an extensive OEM relationship with Dell. Through a partnership with Altor Networks, Juniper provides virtual instances of firewall and IPS.

Strengths

- Customers consistently cite low cost and ease of installation, including VPN configuration, as their reasons for selecting Juniper.
- Juniper's management features are a differentiator in scenarios in which there are multiple devices, or in larger midsize deployments.

Cautions

- Juniper has historically been focused on the carrier and enterprise market, and has only recently started to target the midsize market via its OEM arrangement with Dell and via managed service options.
- Juniper has no application awareness in the current range, although the AppSecure technology will eventually migrate down from the SRX platform.
- It has no Active Directory integration for administrative access.
- Migration from the ScreenOS operating system toward Junos on all its firewall platforms has occupied Juniper's full attention, seeming to leave little time for innovation aimed at the midsize market.

Netgear

Well-known in the SMB world mainly for its low-cost wired and wireless network products, Netgear has entered the security market with its ProSecure brand, which entails the UTM Series and the STM Series (Web and e-mail threat) appliances.

Three models in the UTM Series cover from five to 100 user offices, all based on the same stable in-house-developed code base.

Netgear is the only UTM provider that can provide a solution across three primary midsize infrastructure challenges: security (ProSecure), data backup/protection (ReadyNAS) and network infrastructure (Netgear switching and wireless LANs). Each will talk to the other, allowing ProSecure logs to be written securely to ReadyNAS, for example. This breadth of solution offering and ability to pull together solution sets is more important to the SMB market than the enterprise customer, who is far more likely to seek out best-of-breed point solutions. Significant corporate infrastructure appears to have been put in place during the past 12 months to enable the company to move effectively from a predominantly consumer focus into the midsize market.

Strengths

- Netgear offers a low-cost solution.

- It has a strong channel and is familiar with midsize IT environments.
- The breadth of its solution covers security, backup and infrastructure – it's a one-stop shop for smaller businesses.

Cautions

- The Netgear brand is seen as consumer-oriented.
- It has limited application awareness in firewall policies.
- It has no multidevice centralized management.
- Netgear's product line has limited scalability.
- Netgear has yet to prove itself in the business security arena.

NETASQ

Founded in 1998, NETASQ is a French company focused on the UTM space. It designs and markets hardware UTM appliances based on a derivative of FreeBSD, which combines a network and application firewall with embedded antivirus, anti-spam, VPN, IPS and content-filtering functionality.

NETASQ has an innovative pricing model, with the basic device requiring no maintenance fee, and including Clam AntiVirus for anti-malware scanning and NETASQ's own Web filtering. Pro-level capabilities are provided for a single annual maintenance fee, which upgrades the software to Kaspersky for anti-malware, and Optinet for Web filtering.

Although based on BSD, NETASQ has replaced the stack and performs a lot of work at the driver level, thus reducing the amount of context switching required to maintain high levels of performance. The IPS engine is based mainly on protocol anomaly detection (80%, the remaining 20% being signature-based) to keep performance high and configuration to a minimum.

Virtual appliances are available, supporting both VMware and Citrix environments. There is no initial cost for the virtual appliance, only an annual maintenance charge for the update services.

Strengths

- NETASQ has good price/performance and one annual maintenance fee for pro-level services.
- Protocol anomaly weighted detection for the IPS simplifies deployment and configuration (IPS is enabled by default) and maintains high levels of performance, which is important for less-technical midsize business environments.
- Users report that support is very good, both from channel partners and from NETASQ directly.

Cautions

- NETASQ is very focused on its home market (France), with limited global presence outside EMEA.
- Some customers report difficult installations.

SonicWALL

SonicWALL, a longtime firewall vendor, offers three classes of products for UTM customers: TZ for smaller customers; Network Security Appliance (NSA) for lower-end midsize businesses (100 to 499 employees); and NSA E-Class for upper-end midsize (500 to 1,000 employees) and small enterprises. In addition to its own URL-filtering service, SonicWALL provides support for Websense URL filtering, but, otherwise, uses in-house technology for its multifunction firewall. SonicWALL's latest version has HTTPS inspection and application control.

The SonicWALL TZ family of firewall appliances is a compact form-factor device aimed at the midsize market. It features a Web-based interface with integrated gateway antivirus, anti-spyware and intrusion prevention. Both wired and wireless appliances are available to meet varied configuration requirements.

The NSA and E-Class product lines are available for midsize businesses and small enterprises. Role-based, hierarchical, centralized management capabilities are provided via its Global Management System (GMS).

Strengths

- SonicWALL appears frequently on customer shortlists. It is perceived as a "safe choice," owing to its strong presence in this market.
- It was one of the first to ship application and user-ID-aware firewall capabilities, which are accessible via an easy-to-use management interface.
- Its GMS product for centralized, hierarchical, role-based management is strong.
- The recent merger with Thoma Bravo will provide a stable financial base to move the company forward.
- SonicWALL understands and supports the midsize business channel.
- It keeps the development of security modules in-house, reducing reliance on third parties for continued support and development.

Cautions

- There is a danger that the company will lose its focus on the midsize market as it attempts to push into the enterprise space.

- SonicWALL does not use recognized third-party software for key functions (such as malware scanning). Some users see this as an issue.

- The company still retains the image of a low-end, commoditized platform provider, and not enough is done to highlight the investment in hardware development. A lack of independent testing hampers the ability of more-advanced purchasers to verify performance.

Trustwave

Trustwave is a large provider of Payment Card Industry compliance management services to small, midsize and enterprise customers worldwide. Trustwave has acquired a number of security products that it offers both as stand-alone products and as part of MSSs.

Trustwave now offers a Managed Unified Threat Management service. This provides firewall, gateway antivirus, VPN, IPS, remote access control and Web content filtering capabilities consolidated in a single piece of customer premises equipment (CPE) administered and managed by Trustwave. Currently, only low-throughput CPE devices are provided, aimed squarely at small businesses and the low end of the midsize market.

The service is designed to meet compliance requirements for PCI DSS, Sarbanes-Oxley controls, Graham-Leach-Bliley, and other regulations.

Strengths

- No in-house expertise is required for configuration, updating or monitoring.

- Trustwave fulfills compliance requirements (such as SOX controls and PCI DSS encryption).

- It provides 24/7 notification and response.

- It offers cost and space savings over component-specific appliance purchases.

Cautions

- Low-performance devices may not be suitable for some midsize businesses.

- No independent testing has been done on the CPE or the service.

- The major focus of Trustwave is on PCI compliance services, which may drive product updates.

WatchGuard

U.S.-based WatchGuard's e-Series line of all-in-one firewalls for the midsize business is split into three sublines containing 13 models: Edge, Core and Peak serve small, low-end midsize, and upper-end midsize businesses, respectively.

The XTM family of network security appliances offers an additional 16 models covering businesses of all sizes, from 50 users up to 10,000. The suite of management tools includes a centralized console, a command line interface and a Web UI with privilege-based roles.

Fireware XTM is the underlying OS of the XTM series, and includes HTTPS inspection and application blocking. WatchGuard was also early to market with reputation-based protection for SMBs, following its acquisition of BorderWare last year. Security modules can be bundled or licensed separately for flexibility. The acquisition of BorderWare provided a new range of content security appliances, as well as strong reputation services. Now that the acquisition is complete, there are signs that WatchGuard is reasserting itself in this market.

Strengths

- WatchGuard is known for its ease of use, with strong management and real-time monitoring tools.

- Its 3G Extend accessory line enables customers to provide primary or backup Internet access over 3G cellular networks, secured by a firewall.

- WatchGuard demonstrates flexibility in licensing and deploying security modules.

- Customers report high reliability.

- It has a strong EMEA channel for a U.S. company.

Cautions

- WatchGuard has been less likely to be first to market with features demanded by Gartner clients, although this situation appears to be improving.

- It conducts little or no real independent testing (outside of magazine reviews) for a company pushing into the small enterprise market.

- It has a confusing and cluttered product line.

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.

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.