Magic Quadrant for Unified Threat Management

27 August 2015 | ID:G00269677

Analyst(s):

Jeremy D'Hoinne, Adam Hils, Greg Young, Rajpreet Kaur

Summary

Unified threat management devices provide small and midsize businesses with multiple network security functions in a single appliance. SMB buyers should carefully evaluate UTMs' performance when numerous security functions are enabled, and UTMs' ability to handle new SMB practices.

Strategic Planning Assumptions

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

By 2018, 30% of SMBs will use mobility management capabilities from their UTM platforms to enforce distinctive policies — up from 10% today.

Market Definition/Description

Gartner defines the unified threat management (UTM) market as multifunction network security products used by small or midsize businesses (SMBs). Typically, midsize businesses have 100 to 1,000 employees (see Note 1). UTM products must continually add new functions, and therefore encompass the feature set of many other network security solutions, including next-generation firewall, intrusion prevention systems (IPSs), secure Web gateway and secure email gateway. While consolidation comes with compromises in performance and capability, these are compromises that many SMBs are willing to accept (see "What You Should Expect From Unified Threat Management Solutions").

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

from the large enterprise and branch office firewall markets (see "Magic Quadrant for Enterprise Network Firewalls" and "Next-Generation Firewalls and Unified Threat Management Are Distinct Products and Markets"), which generally require more complex network security features, and are optimized for very different selection criteria. The branch offices of larger companies often have 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. For these reasons, Gartner allocates branch office firewall revenue to the enterprise firewall market, not the UTM market.

SMBs should be skeptical of the aspirational message from UTM vendors about the exaggerated benefits of feature consolidation. Security buyers should instead evaluate UTM devices based on the controls they will actually use, the performance they will get for those features, and the quality of vendor and channel (and managed services) support that is available.

Magic Quadrant

Figure 1. Magic Quadrant for Unified Threat Management

Source: Gartner (August 2015)

Vendor Strengths and Cautions

Aker Security Solutions

Based in Brazil, Aker Security Solutions is a network security vendor. Its portfolio has included UTM solutions (Aker Firewall UTM) since 1997, as well as secure Web gateway and secure email gateway. Aker Firewall UTM is composed of 14 models, with two models with wireless capabilities, all refreshed in 2013. Its single virtual appliance model can also run on VMware, Citrix XenServer and Microsoft Hyper-V.

In the past months, Aker has upgraded its IPS signature base, added Internet Message Access Protocol over SSL (IMAPS) support and a VPN client for iOS and Android through OpenVPN integration. It also now offers an option to support multiple users on a Windows Terminal server or Citrix workstation.

Aker is assessed as a Niche Player, because it operates mostly in Brazil and does not compete yet internationally. Aker Firewall UTM is a good shortlist candidate for small and midsize organizations in Brazil.

STRENGTHS

- Aker Firewall UTM provides a comprehensive set of UTM features, including application control, a variety of VPN options and link load balancing, wireless security, Secure Sockets Layer (SSL) VPN, and two choices each for an antivirus engine.
- Aker's clients and its channel partners cite ease of use, the vendor's local presence in Brazil, and the quality of its support as reason to select the vendor's UTM.
- Aker is one of the few vendors that provide graphical user interface (GUI), documentation and support in Portuguese, in addition to English.

CAUTIONS

- Aker does not appear in UTM evaluations outside of Brazil yet.
- Aker has a smaller development team for its UTM, and therefore is slower to release new features than many of its international competitors. Gartner believes that this is noticeable in upper-midmarket organization selections.
- Aker's UTM lacks network sandboxing and fine-grained role definition for centralized management, and does not provide a Web-based SSL VPN for remote users (using a Java applet is required). Some clients report that management console and reporting look dated.
- Aker does not provide an embedded Web interface that the smaller organizations appreciate. Instead, Aker's UTM always requires the installation of a management software component (Aker Control Center).

Barracuda Networks

Based in Campbell, California, Barracuda Networks is a large vendor providing network security, backup and infrastructure solutions, including Web and email security, Web application firewall, application delivery controllers and data backup. In February 2013, Barracuda released a new product line, the Barracuda Firewall (X

series), to complement Barracuda NG Firewall (F series), its incumbent range of firewalls, which are oriented toward larger enterprises' needs. Barracuda Firewall is composed of seven models, including two with wireless capabilities, but is still not available as a virtual appliance. It embeds a Web interface, designed for simpler use cases, and can be managed in the Barracuda Cloud Control portal.

In 2014, the vendor introduced Barracuda Security Suite, a single integrated server that offers full-featured versions of Barracuda Firewall, Barracuda Spam Firewall and Barracuda Web Filter. The vendor also recently released application-based link-load balancing and customized block pages for its Web proxy.

Barracuda is assessed as a Niche Player mainly because of the limited reach for its UTM product line outside of the EMEA region. The Barracuda Firewall series is a good shortlist candidate for North American and European SMBs that already use other Barracuda products, have stringent budget constraints or prize ease of deployment as a primary requirement.

STRENGTHS

- Barracuda has strong market share among SMBs, and customers benefit from good global sales and support presence. Barracuda has greatly increased partner training and certification for the Barracuda X Series in North America and Europe.
- Surveyed partners and customers consistently cite knowledgeable, responsive customer support as a clear differentiator from competitors.
- Gartner clients report that they like Barracuda's simple licensing, and that unlike many competitors, the price for software options is reasonable. Barracuda Cloud Control is included at no additional charge.
- Barracuda Networks offers a 30-day refund plan and a replacement program that includes a free new appliance every four years, keeping the average appliance life at below four years.

CAUTIONS

- The Barracuda X Series partners and customers cite the need for more advanced features, including higher quality application and identity control. Its cloud-based sandboxing feature is currently available for Web traffic only.
- The Barracuda X Series has not been scrutinized by any major third-party testing labs and has a limited number of certifications.
- Gartner believes that, while Barracuda has correctly assessed that SMB and enterprises have different needs, its two firewall lines still have more overlaps than differences, which complicates the work of its channel and can confuse SMB buyers.

Check Point Software Technologies

Check Point Software Technologies, headquartered in Tel Aviv, Israel, and with operations worldwide, is a large pure-play security company and, according to

Gartner, has the largest enterprise firewall market share. Its SMB product line is mostly across the 600, 1100, 2000 and 4000 lines of appliances. UTM can also be delivered via the cloud-based Capsule Cloud service, as a virtual appliance in the Check Point Security Gateway Virtual Edition, or on Amazon Web Services (AWS), Microsoft Azure and OpenStack. Fundamental to Check Point security gateway offerings is the set of software options referred to as Software Blades, which can be grouped together in bundles. SMBs often choose more blades than enterprises would.

Recent features includes mobile security features (Check Point Capsule), software-based performance improvement for traffic processing, improved coverage of industrial control system (ICS) protocols and a new threat mitigation software blade, Threat Extraction, which uses content reconstruction to remove suspected malicious content during transit.

Check Point is rated as a Leader because of its continued presence on SMB customer shortlists, its geographic coverage and its ability to beat competition based on its unique features. Check Point is a good choice for SMB organizations that do not consider low price as the most important criterion.

STRENGTHS

- Check Point's reporting and management console is consistently very highly rated by midsize companies that need to handle any complexity. The different support levels and options provide a good variety of options and prices.
- Check Point's UTM solutions benefit from its enterprise-level security features, such as ThreatCloud and Anti-Bot software options, in addition to the strong IPS module, which are all backed up by Check Point's large threat research team.
- Check Point provides a strong set of options to protect against custom malware with its sandboxing subscription (Threat Emulation Cloud Service), a variety of threat intelligence feeds (ThreatCloud IntelliStore) and a recently released feature that can automatically remove suspected harmful content from downloaded file (Threat Extraction).
- Check Point UTM integrates with the vendor's cloud-based security service for mobile and remote users, providing a unified security policy for mobile and corporate users.
- Check Point's strong investment and persistent strategy to address SMB clients translates into a good execution on its UTM roadmap.

CAUTIONS

- Gartner clients often cite price as the primary reason for not selecting Check Point solutions; however, this caution will not apply where best-of-breed features are sought foremost.
- Gartner sees Check Point mostly selling to its existing client base; however, Check Point has increased emphasis on its SMB value-added reseller (VAR)

support program since the last edition of this Magic Quadrant.

- Check Point offers many Software Blades and keeps adding new ones. It has made good progress in simplifying the sales offering with bundles, but resellers and clients report that they find it difficult to assess the overall performance impact of enabling more than a few options simultaneously.
- Check Point changes in legacy SMB branding strategy could cause some confusion in the market; however, this will diminish if the current strategy is maintained.

Cisco

Cisco, based in San Jose, California, has a complete access-layer product offering across wired and wireless, making it the largest network infrastructure provider. The vendor also owns a broad security portfolio, including secure email gateway, secure Web gateway, stand-alone IPS, enterprise firewall and UTM.

Since its acquisition of Sourcefire in 2013, Cisco is gradually integrating Sourcefire's IPS into its existing product lines. Cisco's strategy for SMBs mainly relies on its cloud-managed Meraki MX appliances, although they also offer the ASA 5500-X Series (five models) for small and midsize companies.

Recent product news includes further integration of Sourcefire IPS into the Cisco ASA product line. Cisco also offers Meraki UTM models with 802.11ac wireless capabilities, GeoIP blocking and policy-based routing.

Cisco is assessed as a Challenger because it has solid presence in midmarket organizations, but has yet to provide a harmonious vision for all the UTM use cases. Cisco is a good choice for its existing customers and a good shortlist contender for distributed organizations.

STRENGTHS

- Cisco's brand and market presence are strong assets when targeting SMB clients that want minimal complexity in their infrastructure and a simple procurement process.
- Cisco has recently introduced new ASA X Series models. The vendors' efforts to further integrate the management of Sourcefire IPS on the ASA platform enhance its ability to answer the stringent security needs of midmarket organizations looking for consolidated firewall and IPS modules.
- Cisco Meraki MX cloud-based centralized management offers a unified view of all Meraki UTM, wireless AP, switching and MDM products through the cloud.

CAUTIONS

- Cisco Meraki MX lacks email security, cloud-based sandboxing, SSL VPN for remote users and SSL decryption for HTTP. These functions are available in many competitive UTMs.

- The Meraki MX product line does not fully address all the use cases for SMB network security needs, and the management consoles for Cisco ASA X and Cisco Meraki are totally separate. This dual product-line offering available to SMB clients from Cisco might create complexity for some clients using Cisco ASA on the core network, but considering Meraki MX for distributed offices.
- Cisco does not generate many inquiries from SMB clients for its Meraki MX offering.

Dell

Dell, with headquarters in Round Rock, Texas, is a leading computer manufacturer that has diversified its activity in infrastructure and security. Its UTM portfolio is branded Dell SonicWALL and includes 12 models. Dell SonicWALL is composed of two product lines that are sold to the SMB market: the SonicWALL TZ Series for the smallest businesses, refreshed in 2015; and the SonicWALL Network Security Appliance (NSA) Series for small and midsize companies, with models released in 2013 and 2015. The Dell product portfolio includes firewall appliances targeting large enterprises (SuperMassive), and wireless access points (Dell SonicPoint) that can be managed from the Dell SonicWALL UTM console. Dell also provides other network security solutions, such as SSL VPN and email security gateway.

Dell recently refreshed its Dell SonicWALL line for small organizations with eleven new TZ products, notably adding 802.11ac wireless and SSL decryption. It has also added support for its most recent wireless access point (Dell SonicPoint).

Dell is a Challenger in this Magic Quadrant mainly because of its comprehensive portfolio and the ability for customers of Dell's other product lines to leverage existing partnerships with the vendor. Dell is a good shortlist candidate for SMBs, especially for current Dell customers.

STRENGTHS

- Dell's global presence and brand facilitates cross-selling of security solutions, especially for SMB organizations that prefer to minimize their number of software and hardware providers.
- Clients like the product robustness and the comprehensive set of features. The application visibility module contains a large database and can provide good visibility over the usage of SaaS applications.
- Dell SonicWALL has a larger R&D team dedicated to UTM than many of the UTM vendors cited in this report, including a large in-house security lab that creates all its IPS signatures.

CAUTIONS

- Dell SonicWALL lacks sandboxing and embedded custom reporting. Aggregated multifirewall reporting is available using SonicWALL Analyzer reporting, as a paid option per firewall.
- Gartner has observed that the competition continues to aggressively chase

Dell SonicWALL's channel partners. Competition between channel partners and Dell's direct sales approach is frequently cited as the reason why Dell's partners have moved to another vendor.

- While Dell's visibility in UTM shortlist remains high, Gartner has observed an increased number of UTM selections where Dell SonicWALL was the incumbent solution, but not the preferred vendor for the product upgrade.
- Gartner clients cite issues with the management console and report that the antivirus catch rate can vary.

Fortinet

Fortinet is a large security vendor with headquarters in Sunnyvale, California. It offers almost 40 different UTM appliance models (FortiGate) aimed at the small and midsize market, including wireless, DSL and Power over Ethernet (PoE) versions. FortiGate is also available as a virtual appliance, with five models that are priced based on CPU core count. On-premises centralized management (FortiManager) and reporting (FortiAnalyzer) solutions complement the UTM offering. The comprehensive security product portfolio, composed of tokens and host agents (FortiClient), is designed to appeal to VARs and managed security service providers (MSSPs) as the route to sales.

Fortinet's roadmap continues to be driven by regular hardware and software updates, with 11 new FortiGate appliances in 2014 and six models so far in 2015. Fortinet also simplified FortiGate deployment with new configuration wizards, enhanced FortiGate's integration with the cloud sandbox, and introduced new FortiView dashboards in order to improve event monitoring.

Fortinet is assessed as a Leader because it set the bar for the UTM market in terms of performance and price, and often is the first vendor to add new modules to further expand UTM feature set. Fortinet is a good candidate for all UTM use cases.

STRENGTHS

- Fortinet continues to be the most highly visible UTM provider among Gartner clients. It also owns the largest market share, growing faster than the market average, and has the largest base of certified channel partners for UTM technology.
- Fortinet has a very large R&D team and support centers across all regions. Gartner continues to view Fortinet as setting the cadence in the UTM market, driving its competitors to react.
- Fortinet was one of the first vendors to integrate file sandboxing capabilities, and it is backed up by the large FortiGuard Labs threat research team. The vendor has announced more than 3,000 customers using file sandboxing, while most of its competitors remain silent about customer adoption.
- Fortinet provides an aggressive price/performance proposition, which is often a decisive factor for budget-constrained SMBs. Its UTM bundle in a single SKU

is a predictable, easy way for SMB security buyers to get multiple safeguards.

- The combination of wireless access point management, Wi-Fi analytics, high port density and Power over Ethernet (PoE), along with the availability of price-competitive UTM appliances (and a variety of other security products), appeals to small businesses looking for more than a security gateway and to distributed retail organizations.

CAUTIONS

- The frequent hardware and software updates make it more difficult to maintain a consistent level of expertise across Fortinet's widely distributed channel, which sometimes causes discrepancies in presales and support quality.
- Gartner clients report issues related to Fortinet UTM regarding the usability of the FortiManager centralized management, and to lower-than-expected performance when enabling security features.
- Fortinet customers have reported difficulty in obtaining easy, responsive support from the Fortinet ecosystem.

Hillstone Networks

Hillstone Networks is a pure network security player, with headquarters in Beijing and operations in Sunnyvale, California. Its UTM portfolio includes 15 hardware models released in 2009 and the most recent models introduced in 2014 (E series). Two virtual appliances are also available.

Hillstone has recently improved its Internet Protocol version 6 (IPv6) compatibility and its application control module. It also supports SSL traffic decryption and has released a VPN client for iOS and Android. Also, the company is currently offering an upgrade path for its older firewalls to its Hillstone Unified Intelligent Firewall, which delivers anomaly detection and reputation scoring for hosts and networks. The vendor continues to develop its channel in Asia/Pacific (APAC) and Latin America.

Hillstone is a Niche Player because it primarily sells its UTM to Chinese SMB organizations. Hillstone is a good shortlist candidate for SMB organizations in the APAC region.

STRENGTHS

- Hillstone's UTM includes host reputation and network monitoring features that can help detect infected hosts.
- Clients give good scores to the vendor's UTM performance, the flexibility of its quality of service (QoS) engine and the quality of support provided in China.
- Hillstone Networks' security features appeal to security-conscious midsize organizations.

CAUTIONS

- Hillstone primarily targets the large enterprise market. It serves SMB organizations, but its roadmap is biased toward larger organization needs.
- Hillstone does not offer network sandboxing. It also lacks anti-spam and other email security features that some organizations still require.
- Hillstone clients report that they would like to see better activity reporting and improved Web filtering.
- Hillstone is not visible in UTM competitive shortlists outside of China. Its international channel is a developing effort, and prospective clients should verify the local availability of technically savvy partners.

Huawei

Huawei is a large network infrastructure supplier headquartered in Shenzhen, China. In 2009, Huawei launched its Unified Security Gateway (USG) product line to address the Enterprise and the SMB markets. The line now includes more than 25 models, including a large number of appliances with wireless capabilities. Centralized management software is available. Large UTM appliances can run several UTM software instances, but the vendor does not provide virtual UTM appliances to run on the top of leading hypervisors.

Recent updates include four new hardware models (for sale in China only), as well as improved application control and performance.

Huawei is rated as a Niche Player because it predominantly sells its UTM to its existing clients. Huawei's UTM is a good contender for SMBs in China and for its current large-enterprise customers in other countries.

STRENGTHS

- Clients often cite good prices, especially for support service, as a decisive factor in selecting Huawei's solutions.
- Huawei customers like the ease of installation, facilitated by a helpful installation wizard.
- Huawei has a large number of clients using IPv6. All firewall networking functions and UTM features are fully functional in IPv6.

CAUTIONS

- Though its 2014 percentage of sales outside of APAC grew slightly in 2014, Huawei sells a majority of its UTM in this region and struggles to grow market share outside of it. SMB customers in other regions should first assess the level of commitment of Huawei's local channel partners to the SMB market.
- Like most infrastructure vendors, Huawei's leverage is in its existing customer base of large enterprises and carriers. This focus on larger markets might divert development priorities away from SMB needs.
- Huawei partners mention that the Huawei central management GUI is too technical and difficult to use. Huawei also lags behind most of its competitors

when it comes to email security.

Juniper Networks

Juniper Networks is a network infrastructure vendor based in Sunnyvale, California. It has a broad portfolio that covers network and security solutions. Its UTM offering (SRX Series) includes 13 models and relies on the Junos OS, which is the common platform for network and security appliances in Juniper's portfolio. Other product lines can support UTM capabilities (SSG Series and ISG Series), and two virtual appliances are available.

In 2014, Juniper introduced the Spotlight Secure threat intelligence platform, SSL Forward Proxy for AppSecure, central management support for SRX UTM, and integrated reporting and logging in Security Director. Juniper integrated UTM in its vSRX, allowing customers to use its virtual firewall appliances as virtual UTMs with a utility pricing model. During the same period, Juniper sold off its NAC and mobility solutions. Juniper has lost considerable market share against rivals during 2014, with its market share decreasing by 35%.

Juniper is evaluated as Challenger because it has good presence on SMB shortlists when stateful firewall, VPN and IPS are the primary needs, but does not displace leaders on UTM deals based on its features or vision for the SMB market. Juniper UTM is a good choice for existing Juniper customers. Other SMB customers should first verify the experience of their local channel with Juniper security solutions for an SMB use case.

STRENGTHS

- UTM buyers that already use Juniper technology can leverage their existing relationship with the vendor to get a lower price and quickly learn how to manage its UTM.
- Juniper has a broad range of hardware appliances to support a wide variety of scalability and performance requirements.
- Juniper's understanding of diverse customer environments makes it a good choice for complex network infrastructure or when support is a critical component of the purchase decision.
- Juniper customers and partners express satisfaction with the quality and timeliness of Juniper's support.

CAUTIONS

- Juniper rarely appears on Gartner SMB customer shortlists for UTM when more than firewall, VPN and IPS is required.
- Juniper appears to be focusing its security product development efforts on high-end enterprise data centers and carriers, not on the SMB audience. Juniper did not release a new model of its UTM hardware appliance in 2014.
- Juniper does not have a dedicated cloud-based malware detection sandbox,

causing SMB customers to either go without one or to deploy alternative sandbox solutions from other vendors, thereby increasing costs and adding another management console.

Rohde & Schwarz (gateprotect)

Germany-based Rohde & Schwarz (gateprotect) is a pure-play security vendor. Gateprotect was founded in 2002 and acquired by the large German electronics group, Rohde & Schwarz, in 2014. Rohde & Schwarz also acquired a small enterprise firewall company called Adyton Systems, now part of the gateprotect portfolio. Gateprotect's UTM portfolio includes nine appliances. Virtual appliances and centralized management are also available. Gateprotect's management interface (eGUI) implements a graphical (icon-based) visualization of the network topology as a way to simplify the configuration of the security policy.

Gateprotect recently added a reverse proxy and minor improvements to its eGUI software.

Gateprotect is assessed as a Niche Player because most of its UTM wins are in Europe, and its UTM appeals mainly to lower-midsize businesses. Gateprotect is a good shortlist candidate for SMBs in Germany and small organizations in EMEA countries when certified gateprotect channel partners are available.

STRENGTHS

- Clients and channel partners give positive ratings to vendor support and ease of use, especially for lower-midsize organizations. Clients also provide positive comments on production performance that matches what is advertised on the datasheets.
- Gateprotect markets its German R&D and "no backdoor" policy as competitive advantages against its U.S.-based competitors. This appeals to a portion of the EMEA market, especially in small government agencies.
- Gateprotect operates as an independent entity, but now benefits from Rohde & Schwarz's sales and support channel, which should increase gateprotect's ability to reach and support UTM clients outside of Europe.

CAUTIONS

- Gateprotect is growing at a slower pace than the market. The vendor roadmap execution has been impacted negatively by the acquisition and the merger of Adyton and gateprotect technologies, with only a few new features released in the last 24 months.
- Gateprotect does not offer network sandboxing and lacks IPv6 support. It also lags behind its competition in the number of activity reports it can offer.
- Most of gateprotect's UTM sales come from the small and lower-midsize organizations in Europe, with its largest installed base in Germany. Its brand awareness and channels in other countries are still more limited. Clients interested in gateprotect UTM should first verify the vendor's local presence

and the channel's experience with the solution.

Sophos

Based in Boston, Massachusetts, and Oxford, U.K., Sophos is a large security vendor that initially provided endpoint security before adding network and mobile security solutions to its portfolio. After its acquisition of Cyberoam Technologies, the Sophos UTM portfolio includes 29 models from its Sophos (SG Series) and Cyberoam (CR Series) brands. Sophos UTM is also available as a virtual appliance. It also offers its three models of remote Ethernet device (RED) appliances for small branches that are centrally managed using a Sophos UTM.

Sophos recently announced a large UTM product line refresh with 14 new SG models and six new CR models. New features include email encryption, user quotas for Web browsing and a unified reporting solution (Sophos iView). In July 2015, the vendor went public on London Stock Exchange.

Sophos is assessed as a Leader because, despite the efforts created by the integration of Cyberoam, it continues to grow its market share based on features and customer trust in its UTM roadmap. Sophos is a good UTM shortlist contender for SMBs, especially in Europe and APAC regions.

STRENGTHS

- Sophos' SG UTM series' ease of use consistently rates high. The interface contains general guidance on what each feature does, which is useful for SMB operators, who are not all security experts.
- Sophos channel support is rated high. Support for Cyberoam products is easily available through chat, email and phone, and is active in providing presales support for quick resolution.
- Sophos has good endpoint integration, allowing the firewall to push wireless and VPN policies for mobile devices, and can also restrict access to wireless networks for noncompliant mobile devices.
- Sophos SG UTM series support is available in a variety of European languages, and its local presales and support presence receives positive scores from Gartner customers.

CAUTIONS

- Gartner believes that Sophos' dual-line UTM products and expected rationalization may be confusing to existing customers looking for a product upgrade in the next 12 months.
- Except for the reporting solutions, there has not been any significant integration between the two product lines since the acquisition of Cyberoam. Gartner believes that managing two UTM product lines is a significant burden for the vendor and channel sales, presales and support teams.
- Since the acquisition of Cyberoam, Sophos has expanded outside of Germany and the U.K. with increased visibility in Southeast Asia and the Middle East,

but the vendor continues to be more concentrated regionally and still has lower visibility in North American shortlists than its direct competitors.

Stormshield

France-based Stormshield is a subsidiary of Airbus Defence and Space, and is the result of an operational merger between two French firewall vendors in 2013 (Arkoon and Netasq). In addition to firewalls and UTM, the vendor provides endpoint and data security solutions. Its UTM product line (Stormshield Network Security) comprises 10 appliances and seven virtual appliances. It is also available on AWS and recently released a Microsoft Azure version. Stormshield developed its own IPS, which is enabled in the default UTM configuration.

Recent changes include a new appliance targeting upper-midsize organizations (SN910) and its Stormshield Network Security 2.0 rollout, with improved policy-based routing, performance optimization, and OpenStack/KVM/HyperV support.

Stormshield is evaluated as a Niche Player for the UTM market because most of its sales come from a limited number of European countries. Stormshield is a good UTM contender for SMBs in Europe, and has some presence in the Middle East and Asia. Regions outside of Europe should first monitor the availability and experience of the local channel.

STRENGTHS

- Stormshield has a simple service offering with two main bundles: a low-cost bundle and a premium bundle that includes Kaspersky Anti-Virus and vulnerability detection modules.
- Customers and partners cite ease of deployment, IPS design and throughput, and support quality as differentiators.
- Customers and partners based in Europe often report that they select Stormshield because it is a European vendor. The vendor has recently added German-language support on its management console.

CAUTIONS

- Despite longtime efforts, Stormshield does not have significant market share outside of France. Europe is a much more fragmented market than North America or other regions with large countries, and as such, it requires strong investment for each new targeted country outside of the vendor's home market.
- Stormshield partners surveyed by Gartner mention overall brand presence and marketing execution as an area for potential improvement. They note that Stormshield could do a more consistent job of describing its product line and its performance and security advantages.
- Stormshield does not offer cloud-based sandboxing or appliances with integrated wireless. Its Web management console integrates limited real-time event monitoring.

WatchGuard

Seattle-based WatchGuard is a privately held network security vendor. Established almost 20 years ago, WatchGuard has been a well-established player in the UTM market. It provides UTM, secure email gateways and remote manageable wireless APs. The UTM product lines (XTM and Firebox) include 23 physical appliances, including appliances with embedded wireless capabilities, and two virtual offerings: one for virtual UTM (XTMv), and another combining secure Web gateway, email security and data loss prevention (XCSv).

WatchGuard has a cloud-based reporting and monitoring solution (WatchGuard Dimension). WatchGuard APT Blocker is a full-featured, cloud-based network sandbox available as a subscription for all appliances. Recent changes include the release of Dimension 2.0 and five new Firebox appliances, targeting small and lower-midsize organizations.

WatchGuard is evaluated as a Visionary because of its ability to quickly respond to emerging needs from midmarket organizations with new software options. WatchGuard is a good shortlist candidate for SMB organizations in any geographic location in need of a broad set of features or currently relying on an MSSP for managing and monitoring their UTM.

STRENGTHS

- WatchGuard provides cloud-based sandboxing (APT Blocker), and reports are directly integrated in its centralized dashboard cloud service (WatchGuard Dimension).
- WatchGuard's customers and resellers report that WatchGuard has a full portfolio of UTM and related features, combined with a reasonable price and a pricelist without complexity, and includes clear trade-up options.
- WatchGuard has demonstrated a strong Ability to Execute on its roadmap, leveraging its platform modularity to quickly add new modules.
- The WatchGuard Dimension reporting tool includes an interactive heat map view (FireWatch) that is useful for quickly identifying network issues created by a specific user or application. Since the last edition of this Magic Quadrant, this has been the most-mentioned feature by Gartner clients considering WatchGuard.

CAUTIONS

- Gartner SMB clients do not often mention WatchGuard as already considered for their UTM selections.
- Gartner believes that WatchGuard's shifts in campaign and strategy have made it difficult for buyers to identify consistent differentiators in the WatchGuard offerings. However, Watchguard's recent refocus on both the UTM market and delivery of Dimension has allowed for recognition to increase.

- Gartner data indicates the WatchGuard UTM market share stagnated 2014.
- The vendor's product strategy is significantly influenced by the use case of distributed organizations.

Vendors Added and 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's appearance 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. It may be a reflection of a change in the market and, therefore, changed evaluation criteria, or of a change of focus by that vendor.

Added

- No new vendors were added for 2015.

Dropped

- Clavister was dropped because it did not meet Gartner's inclusion criteria for this Magic Quadrant.
- Cyberoam was dropped because it was acquired by Sophos.

Inclusion and Exclusion Criteria

Inclusion Criteria

UTM companies that meet the market definition and description were considered for this report under the following conditions:

- They shipped UTM software and/or hardware products — targeted to SMBs — that included capabilities in the following feature areas at a minimum:
    - Network security (stateful firewall and intrusion prevention)
    - Web security gateway
    - Remote access for mobile employees (VPNs)
    - Email security
- They regularly appeared on Gartner midsize-client shortlists for final selection.
- They achieved UTM product sales (not including maintenance or other service fees) of more than $7 million in 2014, and within a customer segment that's visible to Gartner. They also achieved this revenue on the basis of product sales, exclusive of managed security service (MSS) revenue.
- The vendor can provide at least three reference customers willing to talk to Gartner, or Gartner has had sufficient input from Gartner clients on the product.

Exclusion Criteria

- There was insufficient information for assessment, and the company didn't otherwise meet the inclusion criteria or isn't actively shipping products yet.
- Products aren't usually deployed as the primary, Internet-facing firewall (for example, proxy servers and 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 a managed security service (MSS), to the extent that product sales did not reach the $7 million threshold.

In addition to the vendors included in this report, Gartner tracks other vendors that did not meet our inclusion criteria because of a specific vertical market focus and/or UTM revenue and/or competitive visibility levels, including Endian, GajShield, ilem Group, My Digital Shield, Netgear, North Coast Security Group, Quick Heal, Sangfor, SecPoint, Secui, Smoothwall, Trustwave, Untangle and ZyXEL.

Evaluation Criteria

Ability to Execute

- **Product or Service:** Key features — such as ease of deployment and operation, console quality, price/performance, range of models, secondary product capabilities (including logging, mobile device management, 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 of 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/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.

Evaluation Criteria	Weighting
Product or Service	High
Overall Viability	Medium
Sales Execution/Pricing	High
Market Responsiveness/Record	Medium
Marketing Execution	Low
Customer Experience	Medium
Operations	Medium

Table 1. Ability to Execute Evaluation Criteria

Source: Gartner (August 2015)

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" roadmap and an overall understanding and commitment to the security market (specifically, the SMB network security market). Gartner makes this assessment subjectively by several means, including interaction with vendors in briefings and feedback from Gartner clients on information they receive concerning roadmaps. Incumbent vendor market performance is reviewed yearly against specific recommendations that have been made to each vendor, and against future trends identified in Gartner research. 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 roadmap, 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. Integration with other security components is also weighted, as well as product integration with other IT systems. As threats change and become more targeted and complex, we weight vendors highly if they have roadmaps to move beyond purely signature-based, deep-packet inspection techniques. In addition, we weight vendors that add mobile device management to their offerings and are looking to support SMB organizations that use cloud-based services.

Business Model: 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.

Evaluation Criteria	Weighting
Market Understanding	High
Marketing Strategy	High
Sales Strategy	Medium
Offering (Product) Strategy	Medium
Business Model	Medium
Vertical/Industry Strategy	Not Rated
Innovation	High
Geographic Strategy	Low

Table 2. Completeness of Vision Evaluation Criteria

Source: Gartner (August 2015)

Quadrant Descriptions

Leaders

The Leaders quadrant contains vendors at the forefront of making and selling UTM products that are built for midsize-business requirements. The requirements necessary for leadership include a wide range of models to cover midsize-business use cases, support for multiple features, and a management and reporting capability that's designed for ease of use. Vendors in this quadrant lead the market in offering new safeguarding features, and in enabling customers to deploy them inexpensively without significantly affecting the end-user experience or increasing staffing burdens. These vendors also have a good track record of avoiding vulnerabilities in their security products. Common characteristics include reliability, consistent throughput, and products that are intuitive to manage and administer.

Challengers

The Challengers quadrant contains vendors that have achieved a sound customer base, but they aren't leading with features. Many Challengers have other successful security products in the midsize world and are counting on the client relationship or channel strength, rather than the product, to win deals. Challengers' products are often well-priced, and because of their strength in execution, these vendors can offer economic security product bundles that others can't. Many Challengers hold themselves back from becoming Leaders because they're obligated to set security or firewall products as a lower priority in their overall product sets.

Visionaries

Visionaries have the right designs and features for the midsize business, but lack the sales base, strategy or financial means to compete globally with Leaders and Challengers. Most Visionaries' products have good security capabilities, but lack the performance capability and support network. Savings and high-touch support can be achieved for organizations that are willing to update products more frequently and switch vendors, if required. Where security technology is a competitive element for an enterprise, Visionaries are good shortlist candidates.

Niche Players

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

Context

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

Market Overview

The UTM market is mature, and many SMB organizations are now renewing their UTM technology for the third of fourth time, rather than acquiring it for the first time. The market growth is slowing and becoming closer to the other network security markets. In 2014, Sophos acquired Cyberoam, continuing the recent trend of consolidation in the UTM market. Rohde & Schwarz acquired German vendors gateprotect and Adyton, which now both operate under the gateprotect brand.

For 2014, Gartner estimates that the UTM market grew at 11.0% to reach a total of approximately $1.64 billion (see "Market Share Analysis: Unified Threat Management (SMB Multifunction Firewalls), Worldwide, 2015 Update" and Note 2).

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

These differences between SMB and large-enterprise expectations are one of the major reasons why many of firewall vendors that sell successfully to the enterprise and SMB markets tend to have separate software or even product lines for each market. SMB and enterprise buying centers also have different expectations for their perimeter gateway, even if, with a few exceptions, UTM products and larger enterprise firewalls might compete for the same budget, as explained in " Next-Generation Firewalls and Unified Threat Management Are Distinct Products and Markets." After a long period of UTM vendors chasing larger enterprises, Gartner has observed an inflection in this strategy, with vendors acknowledging the need to focus more on network security needs that are relevant for an SMB organization.

In 2014, SSL decryption and network sandboxing were the most visible new features, even if the addition of sandboxing is more difficult for the smaller vendors, with limited OEM offering. Network sandboxing is mostly sold as a premium option, which could limit its adoption in the SMB market (see "Market Guide for Network Sandboxing"). Gartner believes that vendors are still learning how to position sandboxing and other recent security detection methods (threat intelligence feeds,

command and control detection) when compared to incumbent antivirus and IPS options. As the technology and marketing message matures, new pricing and bundling strategy could further expand the adoption of these features.

SMB organizations also start to see a need for SSL decryption, principally to enforce Web filtering policy and prevent malware infection. This creates additional performance issues and product sizing difficulties for the UTM channel, sometimes leading to customer dissatisfaction when forced to stop decrypting SSL traffic because of unacceptable user experience.

Alternatively, a few providers now target distributed organizations that have needs close to those of midsize organizations. This includes MSSPs for SMBs and distributed enterprises such as retailers, healthcare organizations and small governmental agencies. Despite centralized purchase and maintenance centers, each office is similar to an autonomous organization.

Vendors focusing on the distributed organization use case are now heading toward placing the management and monitoring consoles fully in the cloud. Gartner believes that, although it's convenient for the vendors to do so, a portion of the SMB market will not accept this exclusively cloud model for reasons of latency, and need to access the console when under attack. In some regions and industry verticals, limited trust in a foreign supplier and other privacy concerns would be additional reasons to avoid the cloud model. Reporting and log retention are well-suited to the cloud, but not exclusively.

UTM vendors increasingly are fighting over initial purchase prices, and all vendors manage to win deals on the strength of this sole advantage, based on the targeted vertical and geographic area. In the longer term, the security market for SMB might be influenced by the increased adoption of mobile technology, cloud services and — for upper-midsize businesses — virtualized demilitarized zone (DMZ) and data center. While there is no visible actor that could disrupt the UTM market yet, alternate approaches, such as endpoint and mobile device management or secure Web gateway hosted in the cloud, could become more serious contenders.

Note 1

Small and Midsize Market Definition

Gartner generally defines SMBs by the number of employees and/or annual revenue they have. The primary attribute that is used most often is the number of employees. Small businesses usually have fewer than 100 employees, while midsize businesses are usually defined as companies with fewer than 1,000 employees. The secondary attribute that is used most often is annual revenue. Small businesses are usually defined as those with less than $50 million in annual

revenue, while midsize businesses are defined as those with less than $1 billion in annual revenue. Typically, 80% of the companies that Gartner analysts speak with have between 100 and 999 employees, and revenue of $100 million to $500 million (see "Gartner's Small and Midsize Business Market Definition, 2013 Update").

Note 2

UTM Revenue Differentiation

Gartner does not include branch office firewall revenue as UTM revenue. The market size and growth are estimated compared with numbers from the previous UTM Magic Quadrant.

Evaluation Criteria Definitions

Ability to Execute

Product/Service: Core goods and services offered by the vendor for the defined market. This includes current product/service capabilities, quality, feature sets, skills and so on, whether offered natively or through OEM agreements/partnerships as defined in the market definition and detailed in the subcriteria.

Overall Viability: Viability includes an assessment of the overall organization's financial health, the financial and practical success of the business unit, and the likelihood that the individual business unit will continue investing in the product, will continue offering the product and will advance the state of the art within the organization's portfolio of products.

Sales Execution/Pricing: The vendor's capabilities in all presales activities and the structure that supports them. This includes deal management, pricing and negotiation, presales support, and the overall effectiveness of the sales channel.

Market Responsiveness/Record: Ability to respond, change direction, be flexible and achieve competitive success as opportunities develop, competitors act, customer needs evolve and market dynamics change. This criterion also considers the vendor's history of responsiveness.

Marketing Execution: The clarity, quality, creativity and efficacy of programs designed to deliver the organization's message to influence the market, promote the brand and business, increase awareness of the products, and establish a positive identification with the product/brand and organization in the minds of buyers. This "mind share" can be driven by a combination of publicity, promotional initiatives, thought leadership, word of mouth and sales activities.

Customer Experience: Relationships, products and services/programs that enable

clients to be successful with the products evaluated. Specifically, this includes the ways customers receive technical support or account support. This can also include ancillary tools, customer support programs (and the quality thereof), availability of user groups, service-level agreements and so on.

Operations: The ability of the organization to meet its goals and commitments. Factors include the quality of the organizational structure, including skills, experiences, programs, systems and other vehicles that enable the organization to operate effectively and efficiently on an ongoing basis.

Completeness of Vision

Market Understanding: Ability of the vendor to understand buyers' wants and needs and to translate those into products and services. Vendors that show the highest degree of vision listen to and understand buyers' wants and needs, and can shape or enhance those with their added vision.

Marketing Strategy: A clear, differentiated set of messages consistently communicated throughout the organization and externalized through the website, advertising, customer programs and positioning statements.

Sales Strategy: The strategy for selling products that uses the appropriate network of direct and indirect sales, marketing, service, and communication affiliates that extend the scope and depth of market reach, skills, expertise, technologies, services and the customer base.

Offering (Product) Strategy: The vendor's approach to product development and delivery that emphasizes differentiation, functionality, methodology and feature sets as they map to current and future requirements.

Business Model: The soundness and logic of the vendor's underlying business proposition.

Vertical/Industry Strategy: The vendor's strategy to direct resources, skills and offerings to meet the specific needs of individual market segments, including vertical markets.

Innovation: Direct, related, complementary and synergistic layouts of resources, expertise or capital for investment, consolidation, defensive or pre-emptive purposes.

Geographic Strategy: The vendor's strategy to direct resources, skills and offerings to meet the specific needs of geographies outside the "home" or native geography, either directly or through partners, channels and subsidiaries as appropriate for that geography and market.