# Magic Quadrant for Unified Threat Management

**Published:** 30 August 2016 **ID:** G00291814
**Analyst(s):**

Jeremy D'Hoinne, Adam Hils, Rajpreet Kaur

## Summary

Unified threat management devices provide small or midsize businesses and heavily distributed enterprises with multiple network security functions in a single appliance. UTM buyers should evaluate performance, security, ease of use, local support and UTMs' ability to handle new SMB practices.

## Strategic Planning Assumptions

By 2020, 50% of SMBs will use mobility or wireless management capabilities from their UTM platforms to enforce distinctive policies, up from 10% today.

Through at least 2020, the firewall markets for SMB and enterprise firewalls will remain distinct.

## 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 vendors continually add new functions on the UTM platforms, and therefore, they encompass the feature set of many other network security solutions, including:

- Enterprise firewall
- Intrusion prevention systems (IPSs)
- Remote access
- Secure web gateway
- Secure email gateway

While consolidation comes with compromises in performance, security efficacy 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" ). These generally require more complex network security features and are optimized for very different selection criteria.

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

The branch offices of larger companies often have different network security demands than midsize businesses, even though they may be of similar size. Large enterprises often use low-end enterprise products at their branch offices to ensure interoperability and to take advantage of economies of scale 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.

Distributed organizations, with highly autonomous offices such as retail franchises, might total more than 1,000 employees, even if only a portion of these employees are connected to the IT infrastructure. Similar to SMB organizations, these organizations often have constrained budgets due to the large number of branches and often small IT security teams. Many UTM vendors have added features for this use case, with some vendors even focusing more on distributed organizations than on traditional SMBs.

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

# Magic Quadrant

**Figure 1.** Magic Quadrant for Unified Threat Management


*Source: Gartner (August 2016)*

## Vendor Strengths and Cautions

### Aker Security Solutions

Based in Brazil, Aker Security Solutions is a network security vendor founded in 1997. Its portfolio has included UTM solutions (Aker Firewall UTM), as well as secure web gateway and secure email gateway. Aker Firewall UTM is composed of 14 models: six Aker Firewall Minibox models — including two models with wireless capabilities — and eight Aker Firewall Enterprise Box models. Aker Control Center is the vendor's centralized management console software. Its single virtual appliance model can also run on VMware, Citrix XenServer and Microsoft Hyper-V.

In the past months, Aker has released three new appliances, improved its IPsec VPN and authentication modules, and released a new version of Aker Control Center.

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

### STRENGTHS

- Aker Firewall UTM provides a comprehensive set of UTM features, with flexible web-filtering options, including rule-matching criteria and per-user quota.
- Aker leverages multiple OEM partnerships to provide comprehensive and mature security signature datasets for its IPS and antivirus modules.
- Aker Control Center software can centrally manage UTMs and other solutions from the vendor.
- Aker has a faithful base of Brazilian clients and resellers that are willing to stick with Aker's UTMs for the future. Aker's clients and its channel partners cite ease of use and the vendor's strong local presence in Brazil as reasons to select its UTM.
- Aker is one of the few vendors that provides graphical user interface (GUI), documentation and support in Portuguese, in addition to English.

### CAUTIONS

- Aker's go-to market strategy is exclusively focused on Brazil, and the vendor does not appear in UTM evaluations outside of that country. The local economic situation has impacted Aker's recent growth dynamic.
- Aker is small UTM vendor with roughly 100 employees and fewer than 10,000 UTMs in production. Aker faces increasing competition from several global UTM companies targeting Latin America, which could threaten its long-term viability.
- Aker's UTM lacks network sandboxing and fine-grained role definition for centralized management. It does not include a dedicated feature for SaaS visibility, and does not provide a web-based Secure Sockets Layer (SSL) VPN for remote users (using a Java applet is required). The UTM is available in a variety of virtual-image formats, but integration on IaaS platforms is limited.
- Aker's clients would like to see improvement in the quality of the web application controls, web malware inspection, real-time dashboard and generated security reports.
- Aker does not provide an embedded web interface that smaller organizations can appreciate. Instead, Aker's UTM always requires the installation of a management software component (Aker Control Center).

## Barracuda Networks

Barracuda Networks, headquartered in Campbell, California, is a large vendor that provides network security, backup and infrastructure solutions. Barracuda NextGen Firewall X-Series (NGX) comprises nine 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. Barracuda Cloud Control is the cloud-based centralized management portal for the X-Series. Barracuda offers two more lines of firewall products: the NextGen Firewall (NGF) F-Series, targeting larger enterprises; and the S Series, made to facilitate VPN management for distributed small offices.

In recent months, Barracuda acquired a cloud access security broker (CASB) vendor, Sookasa, and got International Computer Security Association (ICSA) certification for

the F-Series (Network Firewalls/Enterprise certification) and X-Series (Network Firewalls/SMB certification). The vendor also released new appliances for the smaller organizations and VPN applications for IOS and Android (CudaLaunch). Recent features on the X-Series include antivirus for mail and FTP. Version 7.1 adds the availability of Barracuda network cloud-based sandboxing (Advanced Threat Detection).

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 focuses on the needs and budgets of midsize organization security, but its UTM is also implemented by larger companies. Surveyed partners and customers consistently cite the quality of vendor support as a clear differentiator from competitors.
- Barracuda NGX includes good quality of service (QoS) and web-filtering capabilities. It integrates with leading wireless vendors to gain increased visibility and control on Wi-Fi networks.
- Gartner clients report that they like Barracuda's simple licensing and the free access to the centralized management web portal, and unlike with many competitors, the price for software options is reasonable.
- Barracuda's recently released network sandboxing feature relies on a mature engine, already available on the F-Series. It can scan files for web, email (SMTP/SMTPS) and FTP.
- 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

- Barracuda is losing market share in Europe and faces increased competition from regional competitors.
- The Barracuda partners and customers cite the need for more advanced features on the X-Series, including higher-quality application and identity control. Barracuda Cloud Control lacks role-based administration. NGX lacks an SSL VPN web portal, and some of the smaller appliances don't support the feature.
- Barracuda X-Series and F-Series have different capabilities and roadmaps. The X-Series roadmap generally lags a few months behind the F-Series roadmap. The vendor also has two centralized management consoles: Cloud Control for the X-Series and NextGen Control Center, which is shared by the S-Series and F-Series.
- Gartner has observed that the multiple product lines still create confusion for channel and managed security service provider (MSSP) partners that offer the F-Series to their SMB clients, whereas Barracuda markets the X-Series only for SMB targets.

- Barracuda S-Series relies on Barracuda proprietary VPN (Transport Independent Network Architecture, or TINA), which forces the use of Barracuda on both ends of a VPN tunnel, preventing customers from using VPN-native IPsec gateways embedded in Microsoft Azure and Amazon Web Services (AWS) on the cloud side.

## Check Point Software Technologies

Check Point Software Technologies, headquartered in Tel Aviv, Israel, and with operations worldwide, is one of the largest pure-play security companies and, according to Gartner, has the largest enterprise firewall market share. Check Point has emerged in the UTM market primarily due to the increase in threats driving SMBs to look for a "premium" SMB offering. Its UTM product line includes the 600, 700, 1100, 1400, 2200, 3200, 4000 and 5000 lines of appliances. UTM can also be delivered via the cloud-based Capsule Cloud service, as a virtual appliance (Check Point vSEC Gateway) as part of VMware NSX or Cisco Application Centric Infrastructure (ACI) SDN deployments, or on 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 acquired together in bundles. Recent bundle packages have allowed Check Point SMB customers to purchase the NGTP (Next Generation Threat Prevention) and NGTX (Next Generation Threat Extraction) versions of Check Point UTMs. NGTP groups eight UTM blades in a discounted bundle; NGTX includes all the NGTP features, then adds the Threat Emulation and Threat Extraction blades. SMBs often choose more blades than large enterprises would.

Recent features include Anti-Bot and SSL inspection extended down to the smaller product lines; "zero-touch" deployment that improves ease of installation for SMBs; an updated version of SMP (Security Management Portal), a web-based tool that allows SMBs to more easily administer their UTM deployments; and R80, a complete rewrite of Check Point's central management.

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 the strength of its channel and its unique features. Check Point is a good choice for SMB organizations that do not consider low price as the most important criterion and that are looking for a premium or high-security UTM.

### STRENGTHS

- Check Point's reporting and management console is consistently rated very highly by midsize companies that need to handle any complexity. The different support levels and options provide a good variety of options and prices. The addition of SMP offers SMBs a simplified approach to accomplishing basic administration.
- Check Point's UTM solutions benefit from its enterprise-level security features, such as SSL decryption and Anti-Bot option, in addition to its strong IPS module, which customers and partners have noted as a particular area of strength.
- 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 feature that can

automatically remove suspected harmful content from downloaded file (Threat Extraction).

- Check Point UTM has invested in accelerating SSL/Transport Layer Security (TLS) decryption in its UTMs, providing midsize customers a more realistic possibility of increasing visibility with less performance degradation.
- Check Point's strong investment and persistent strategy to address SMB clients translates into a good execution on its UTM roadmap.

**CAUTIONS**

- Gartner clients still cite price as the primary reason for not selecting Check Point solutions, and surveyed Check Point stakeholders note a relative lack of satisfaction with Check Point because of high subscription renewal price. However, this caution will not apply where best-of-breed security features are sought.
- Gartner sees Check Point mostly selling to its existing client base. However, Gartner has recently seen the NGTX feature package stir some interest among non-Check Point SMB customers.
- Communication with channel partners and end-user customers could be improved. Gartner SMB clients who are Check Point customers are sometimes unaware of released Check Point features and models that could address their needs.
- Although Check Point offers many software blades and keeps adding new ones, and despite the good progress in simplifying the sales offerings with bundles, resellers and clients report licensing complexity remains an issue.

## 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.

Cisco's official UTM offering is the cloud-managed Meraki MX Series of products. Cisco's portfolio also includes the ASA 5500-X series with FirePOWER Services (five models) that can serve small or midsize companies. Gartner observes that SMBs are purchasing these ASA appliances and the new FirePOWER models, and as a result, we include both product lines here.

Since its acquisition of Sourcefire in 2013, Cisco has integrated Sourcefire's IPS and Advanced Malware Protection (AMP) into its existing product lines. In August 2015, Cisco acquired OpenDNS for DNS security. Recent product news includes three new Meraki UTM appliances and unified central management for ASA with FirePOWER Services. Cisco also now offers an SD-WAN feature and active/active load-balanced VPN. Recently introduced features include 802.1X wired port authentication for small branch models.

Cisco is assessed as a Challenger because it has solid presence in midmarket organizations, but has yet to provide a converged vision for all the UTM use cases.

The Cisco ASA 5500-X product line is a good choice for its existing customers, and Cisco Meraki is 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. Its recent acquisitions and feature development in the security space show commitment to further enhance its existing solutions.
- Cisco has recently introduced new Firepower models. The vendor's efforts to further integrate the management of Sourcefire IPS on the Firepower 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, MDM products and, recently, IP phones through the cloud. The vendor has also recently added SD-WAN capabilities. The recent launch of Sourcefire AMP complements the Sourcefire IPS to provide enterprise-grade security to Cisco's SMB clients.
- Cisco Meraki customers note cloud management and ease of use as strengths in the Cisco Meraki UTM offerings.

### 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. Surveyed customers mention lack of SSL decryption as a particular shortcoming, and note a lack of granularity in policy management and role-based control.
- Cisco ASA customers report some throughput degradation after upgrading to the version with FirePOWER Services. Gartner SMB clients and resellers serving SMBs frequently complain about Cisco's ASA management console. Gartner has yet to receive feedback that the latest release improved the situation.
- 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 often creates product management complexity for some clients using Cisco ASA on the core network, but considering Meraki MX for distributed offices — or for clients looking for a more seamless upgrade path as the organization grows.
- Despite recent improvements in North America, Cisco does not generate many inquiries from SMB clients for its Meraki MX offering.

## Dell SonicWALL

Dell, headquartered in Round Rock, Texas, is a long-established global computer manufacturer with expanded business in infrastructure, security and services. It acquired SonicWALL in 2012 and started selling UTM under the Dell SonicWALL brand. In June 2016, Dell announced the spinoff of Dell Software Group to Francisco

Partners and Elliott Management, which includes the Dell SonicWALL division as well. The transaction is not completed yet.

The Dell SonicWALL UTM portfolio comprises two product lines: the SonicWALL TZ Series for the small networks, refreshed in 2015, and the SonicWALL Network Security Appliance (NSA) Series for midsize networks. The vendor also offers the SuperMassive series for enterprise networks. Dell SonicWALL product portfolio also includes wireless access points (SonicPoint), WAN Acceleration Appliance (WXA) series, mobile access, email security and encryption solutions. SonicWALL Global Management System (GMS) is the centralized management solution for their multiple product lines. It is offered as an appliance, a virtual appliance or software.

With recent software releases, the vendor added multiengine support for its cloud-based sandboxing subscription (Capture ATP Service). The recent releases also included SSL/TLS decryption enhancements and improvements to web-filtering capabilities (Content Filtering Service 4.0).

Dell SonicWALL is a Challenger in this Magic Quadrant mainly because of its global presence and brand visibility in UTM shortlists. Dell SonicWALL is a good shortlist candidate for SMBs.

## STRENGTHS

- Dell SonicWALL's comprehensive security offering is popular with SMBs that have a long-established relationship with the vendor. The vendor offers cost and functionality appropriate for SMBs.
- The vendor's latest release of multiengine support from VMRay, Lastline and SonicWALL for cloud-based network sandboxing is a unique approach for midsize organizations looking for advanced malware detection.
- Their Application Intelligence and Control module provides visibility to identify applications, including SaaS applications. Through this feature, an administrator can monitor all applications (including SaaS) in real time with network bandwidth information. This makes monitoring and control of applications easier to manage, especially for SMBs.
- Clients like the product's robustness and its comprehensive set of features. The application visibility module contains a large database and can provide good visibility over the usage applications, including SaaS.
- 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

- The recent announcement of SonicWALL spinning off from Dell is the second big organizational change in less than four years. While the new entity has a stable and experienced management team, the motivation and level of financial support from its new investor is unclear.
- Gartner has observed that SonicWALL's competitors manage to cast doubts in prospective clients' minds, resulting in some clients discarding SonicWALL from shortlists because of uncertainty.

- Prospective and existing SonicWALL customers, especially those who acquired SonicWALL's UTM through Dell's channel, should gauge the level of recent change in this organization. They should ensure that they will continue to receive the same level of technical and support resources that they were receiving as a part of Dell.
- Dell SonicWALL lags behind its direct competitors in endpoint integration and has not yet released a multitenant cloud-based management portal that MSSPs and distributed organizations like. The vendor lacks UTM delivered as a virtual appliance.
- Gartner clients cite issues with the first level of technical support.

## Fortinet

Fortinet, headquartered in Sunnyvale, California, has a broad portfolio of security solutions and owns the largest market share of the UTM market. With the first UTM appliance shipped in 2002, it now has a comprehensive range of UTM appliances under the Fortigate product line. Fortinet also offers high-end firewalls for enterprise networks. To complement its UTM offering, Fortinet offers centralized management and reporting solutions (FortiManager and FortiAnalyzer). It also offers a broad product portfolio (Fortinet Security Fabric) that includes switches, WAN appliances, wireless LAN, advanced threat detection, ADCs, secure email gateway, web application firewall and a few more network security products.

Fortinet had its major OS release in December 2015, and the roadmap for 2016 includes a complete refresh of its UTM line and enhancements to the cloud sandbox, as well as other feature additions. It offers its management console in multiple regional languages.

Fortinet is assessed as a Leader because it continues to have a strong global presence with one of the best UTM offerings in terms of price and performance. It is often among the first UTM vendors to innovate and introduce new features. It is the most frequently shortlisted candidate for all the SMB use cases.

### STRENGTHS

- Gartner continues to see Fortinet in most SMB client shortlists across the globe. It is one of the few vendors with a global presence, through a large channel presence, and is seen competing with local vendors in every region. It owns the largest market share, growing faster than the market average. Fortinet also has a very large R&D team and support centers across all regions.
- Fortinet has extended the capabilities of its Cloud Access Security Inspection (CASI) module to provide monitoring and control of SaaS activities, such as credentials used, files downloaded, files uploaded, videos viewed and so on. The CASI module also supports cloud applications, such as YouTube, Dropbox and Baidu.
- Fortinet is often the first UTM vendor to use its large in-house R&D team to innovate and add a new feature in response to the requirements of SMB networks.

- Fortinet not only wins SMB clients based on features, but it also continues to offer a strong price/performance proposition. Offering its UTM bundle as a single SKU provides an easier pricing option for SMB security buyers.
- 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 both small businesses looking for more than a security gateway and to distributed retail organizations.

**CAUTIONS**

- The large range of appliances, and 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.
- Fortinet provides basic cloud-based management, which includes logging, as compared to other competitors in the market, which provide more advanced cloud-based management and control.
- Gartner has observed that list prices in proposals outside of North America can be significantly higher than in the U.S. While a small uplift is expected, Fortinet clients outside of North America should verify competitive pricing propositions and not rely only on Fortinet's reputation for good pricing.
- The FortiGuard FortiSandbox Cloud service lacks detailed logging and is basic when compared with some of its competitors.
- Fortinet customers have reported difficulty in obtaining easy, responsive support from the Fortinet ecosystem.

## Hillstone Networks

Hillstone Networks is based in Beijing, China, with regional headquarters in Sunnyvale, California. Hillstone is a network security vendor with three lines of firewalls. The E-Series includes 13 hardware models to serve SMBs. The T-Series targets larger organizations, and the X-Series is for the data center. Two virtual appliances (CloudEdge and CloudHive) are available. The vendor portfolio also includes network IPS.

During the past 12 months, Hillstone has improved its support for Internet Protocol version 6 (IPv6) and introduced its first version of botnet mitigation and SSL decryption.

Hillstone is a Niche Player because, despite its investment in North America, it primarily sells its UTM solution to Chinese SMB organizations. Hillstone is a good shortlist candidate for SMB organizations in the Asia/Pacific (APAC) region. Outside of this region, SMB organizations should verify the experience of the channel because Hillstone's UTM may be a new solution for these partners.

**STRENGTHS**

- Hillstone Networks offers all-inclusive, one-year licensing, making it simple for the enterprise to purchase its UTM. Clients give very good marks to Hillstone's price/performance positioning compared with its competition.

- Hillstone's portfolio for virtualized environments offers a combination of CloudEdge (virtual appliance) and CloudHive (microsegmentation), which is attractive to heavily virtualized SMB organizations.
- Hillstone Networks' security features appeal to security-conscious midsize organizations. Its reporting dashboard enables good drill-down in security incidents and gets positive scores from its clients and surveyed resellers.
- The vendor can detect a large number of Chinese and international SaaS applications.

**CAUTIONS**

- Hillstone primarily targets the large enterprise market. It serves SMB organizations, but its roadmap is biased toward larger organizations' needs.
- Hillstone does not offer network sandboxing and lacks anti-spam for email security. It offers malware detection only on the T-Series. Clients report that antivirus and URL filtering could be improved.
- The vendor has just introduced an SSL decryption feature, and there is little production experience with it.
- Gartner estimates that more than 95% of Hillstone UTM sales are in China. The vendor's international development efforts to date are focused on larger enterprises first.

## Huawei

Huawei is a global information and communication technology provider based in Shenzhen, China. Huawei is widely known for its networking products. The vendor's portfolio includes network infrastructure solutions. Since 2009, Huawei has provided firewalls to SMBs and enterprises through its Unified Security Gateway (USG) product line. Centralized management software is also available. USG can be delivered as a virtual appliance and is available through the AWS marketplace.

In recent months, the vendor invested in expanding its international channel for UTM, with a focus on the Middle East and Latin America.

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

**STRENGTHS**

- Clients give high ratings to Huawei for its good prices and hardware quality.
- Huawei's application control supports a large number of applications, including SaaS, and is integrated with its IPS engine to improve efficacy.
- Huawei has a good set of global and local certifications, including Common Criteria EAL4+ and ICSA for its SMB firewall appliances.
- Huawei has a large number of clients using IPv6. All firewall networking functions and UTM features are fully functional in IPv6.

**CAUTIONS**

- Huawei sells a majority of its UTM solution as an add-on to its existing network clients, mostly in China, despite good growth in Latin America. Gartner estimates that more than 80% of Huawei's UTM sales are in Asia/Pacific. SMB customers in other regions should first assess the level of commitment of Huawei's local channel partners to the SMB market.
- Huawei's primary focus is on enterprise firewall and branch security use cases. This focus might divert development priorities away from SMB needs for all-in-one security platforms. The vendor lacks a cloud-based sandboxing option and does not offer UTM integration with endpoint software.
- Huawei rarely appears in Gartner SMB client shortlists outside of China.
- Huawei partners outside of China mention that the management console could be more intuitive, and that the reporting function, while comprehensive, looks a bit dated.

## Juniper Networks

Headquartered in Sunnyvale, California, Juniper Networks is a global network infrastructure vendor. It has a broad portfolio that covers network and security solutions. Its UTM offering (SRX Series) includes 19 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 (Secure Services Gateway [SSG] Series and Integrated Services Gateway [ISG] Series), and one virtual appliance is available.

Over the past year, Juniper released new SRX models and added SSL/TLS traffic inspection support and a first version of a cloud-based sandboxing subscription (Sky ATP). The vendor has also tuned its centralized management software (Security Director), along with the on-box UI, to simplify UTM deployment and daily operations.

Juniper is evaluated as a Challenger because it has good presence on SMB shortlists when the primary needs are stateful firewall, VPN and IPS, and also because of its recent improvements in roadmap execution for the SRX Series. Juniper UTM is a good choice for conservative SMB organizations looking for a reliable integrated routing and security platform at midrange price when compared against competitive UTM offerings.

### STRENGTHS

- Juniper has global presence, with robust channel and integration technology partner networks. It offers regional support centers in North America, Europe, APAC and Australia. Its UTM products have a comprehensive set of certifications.
- Juniper has a broad range of hardware appliances to support a wide variety of scalability and performance requirements. The vendor also gets good marks from users on the robustness and durability of its hardware appliances.
- Juniper's understanding of diverse customer environments makes it a good choice for complex network infrastructures or when support is a critical component of the purchase decision. The vendor offers scripting and automation tools to reduce management burden.

- The majority of Juniper customers and partners commended Juniper's ability to integrate security, VPN and network features. The networking expertise of the vendor's support is frequently mentioned as a differentiator.

**CAUTIONS**

- Juniper rarely appears on Gartner SMB customer shortlists for UTM when required features include more than firewall, VPN and IPS. In 2015, the vendor slowed this trend, but it continues to lose market share against its competitors.
- Juniper had focused its security product development efforts on high-end enterprise data centers and carriers. Gartner has observed that several of Juniper's resellers also have other UTM vendors in their portfolios for simple SMB use cases. The vendor refreshed the low end of its SRX portfolio in the second half of 2015.
- Customers stated that the usability and web UI need improvement, leading them to favor the use of the command line interface (CLI). They frequently mention the security policy as being too complex to manage when combining network and application-based security features. Gartner has yet to receive client feedback about the improvements brought by the latest version of the Security Director management console.
- The vendor does not draw a distinction between enterprise branch and SMB needs, which leads to a more conservative roadmap than the leading UTM vendors. Cloud-based sandboxing's adoption is still ramping up. There is limited integration between SRX and endpoint software for threat correlation of the unified dashboard.

## Rohde & Schwarz Cybersecurity

Based in Germany, Rohde & Schwarz Cybersecurity is the security business unit of electronics group Rohde & Schwarz (R&S). Rohde & Schwarz Cybersecurity's portfolio includes a network security portfolio, gateprotect, named after a company acquired in 2014.

The gateprotect portfolio includes two UTM product lines, gateprotect UTM and gateprotect UTM+, and an enterprise firewall product line, gateprotect NP+. Gateprotect UTM is the new name of the legacy gateprotect appliances targeted to SMBs. It is managed by eGUI, its software-based policy management software, leveraging a graphical (icon-based) visualization of the security policy. Gateprotect UTM+ integrates R&S Cybersecurity deep packet inspection engine (ipoque) and relies on a web version of the eGUI management (WebGUI). Rohde & Schwarz Cybersecurity also provides VPN appliances (TrustedVPN) and a mobile traffic analytics platform (R&S Net Reporter).

In 2016, Rohde & Schwarz Cybersecurity released its UTM+ appliance product line and its firmware version, including the WebGUI management console and single-pass traffic inspection engine, as part of the UTM+ product line.

Rohde & Schwarz Cybersecurity is assessed as a Niche Player because most of its UTM sales are in Germany, and its effort to expand its UTM reach to upper midsize organizations is still nascent. It is a good shortlist candidate for German organizations

and for existing midmarket clients in other countries where certified gateprotect channel partners are available.

### STRENGTHS

- Clients highly rate Rohde & Schwarz Cybersecurity's vendor support and the ease of use of the eGUI console. They also cite a low number of false alerts as a reason for light operational workload.
- Rohde & Schwarz Cybersecurity's consequent investment in security shows a strategic commitment to further enhance the network security product lines.
- The vendor 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 and other non-U.S. aligned geographies, especially small government agencies.
- The management interface and documentation are available in German for all the firewall product lines. The gateprotect UTM management console is also available in Italian, Spanish, French and Turkish.

### CAUTIONS

- The gateprotect UTM and firewall product lines are emerging from a recent complete overhaul. The management console, features and roadmaps can be different among the product lines.
- Gartner expects channel partners targeting upper-midmarket organizations and their clients to be confused by the overlapping choices. Upper-midmarket clients interested in the gateprotect UTM+ solution should first verify the vendor's local presence and the channel's experience with the solution.
- Many Rohde & Schwarz Cybersecurity resellers are only skilled on eGUI software, available only on the gateprotect UTM product line, which is dedicated to smaller organizations and simpler use cases. Despite a long beta, gateprotect WebGUI, the web management interface for UTM+, is still unproven. A centralized management console is not yet available for gateprotect UTM+.
- Approximately 70% of Rohde & Schwarz Cybersecurity customers are in Germany, and the company has only a limited number of large-scale implementations. The gateprotect line continues to grow very slowly and therefore loses market share to the broad range of competitors in the UTM market.
- Network sandboxing is not available with gateprotect, and the product has limited IPv6 support. Its real-time monitoring and reporting console lags behind its competitors.

## Sophos

Sophos is based in Boston, Massachusetts, and Oxford, U.K. It initially started as an endpoint security vendor and is now a large security vendor with a broader product portfolio, including network and mobile security solutions. Its UTM product line consists of three different product lines: Sophos XG series, which includes 19 models, all of which were introduced in 2015, and the Sophos SG Series and

Cyberoam CR Series, which together include 29 models. Sophos UTMs are also available as virtual appliances with integration on AWS IaaS platform.

Sophos offers smaller models for small branches, branded as Sophos RED (Remote Ethernet Device) appliances. Additionally, it has a strong endpoint portfolio of products that compete well in the SMB market. The Sophos Synchronized security feature shows telemetry for the firewall and the endpoint on a single dashboard. Sophos provides management consoles in multiple regional languages. It also provides documentation in some regional languages.

This year, Sophos has made UI enhancements in its Sophos Firewall operating system (SFOS) for Sophos XG UTMs and extended its support to Microsoft Azure Cloud and Azure Stack. It has also introduced new email security features and an IPsec module with support for dynamic tunnels.

Sophos is assessed as a Leader because it continues to grow its market share based on features, support services and customer trust in its UTM roadmap. Sophos is a good UTM shortlist contender for SMBs, especially in Europe and APAC regions.

## STRENGTHS

- Sophos UTMs continue to be rated higher at ease of management. And with the single-pane view for its SFOS, Sophos has enhanced its ease of management capabilities further.
- Sophos grows faster than market average, taking market share from competitors in many different regions.
- Sophos' cloud-based management (Sophos Cloud Firewall Manager) provides complete centralized management. Able to manage up to 1,000 devices, it is more scalable than the Sophos on-site central management.
- Sophos Synchronized Security feature is tightly integrated in the management interface and also provides a unified dashboard. It is still not fully mature, but shows promise in enhancing the security posture of midmarket organizations willing to make the effort to integrate UTM and an endpoint.
- Sophos' extensive regional presence in Europe has led to good local presales and support presence. Cyberoam channel presales provide easy availability and quick resolution, and also receive positive feedback.

## CAUTIONS

- Although Sophos says that it will support the three UTM product lines for an undisclosed period, prospective customers should confirm the roadmap and support services long-term availability for the CR and SG Series.
- Gartner observes that Sophos' channel is only slowly adopting the new XG series and often elect to offer the CR and SG appliances that its technical team are more familiar with. Prospective customers should verify that the current capabilities and enhancement plans for the product they are offered meet their deployment and operations requirements.
- Sophos' new XG UTM solutions lack network sandboxing, which is an important requirement for upper-midsize organizations and MSSP partners and is provided by many of Sophos' direct competitors.

- Gartner receives mixed feedback from SMB customers about postsales technical support timeliness and overall quality in North America.

## Stormshield

Stormshield, headquartered in France, is a fully owned subsidiary of Airbus Defence and Space. Its UTM product line (Stormshield Network Security) includes nine models for SMBs. It also has three firewall models for enterprise networks and seven virtual UTM models. Stormshield UTM is available on AWS and Microsoft Azure platforms. Its product portfolio also comprises network, data and endpoint security solutions. Stormshield offers subscription-based cloud reporting based on its Network Event Analyzer solution. Reports are sent to customers by email.

Stormshield owns a mix of global and regional certifications, with EAL4+ certification, EU Restricted and NATO Restricted. It also has French government certification for its security products. Stormshield has its management console and documentation in a few regional European languages, including German, French and Polish.

In 2016, Stormshield released a cloud-based network sandboxing feature (Stormshield Breach Fighter), leveraging its endpoint security behavioral engine. It has added a new appliance model for industrial environments called SNi40.

Stormshield is evaluated as a Niche Player in the UTM market because its presence is limited to a few European countries only. It is a good UTM contender for SMBs in Europe, especially France, Germany, and Belgium, the Netherlands and Luxembourg (Benelux), where it has strong local presence.

### STRENGTHS

- Airbus is a strong brand, and it has European and French government certifications. Stormshield's dense channel coverage in Europe makes it a frequent contender on SMB shortlists, with a large installed base of European SMBs.
- Customers and partners cite high performance with IPS enabled, Extended URL filtering quality and vendor support as differentiators. They like the recently launched reporting solution delivered as a virtual appliance.
- Stormshield integrates a vulnerability detection engine and offers the ability to adapt the security policy for vulnerable hosts directly from the monitoring console.
- Stormshield has a good appliance upgrade program, which reduces the product refresh cost for existing clients, and also provides competitive pricing to replace a competitor's UTM.

### CAUTIONS

- Stormshield's roadmap execution lags behind most of the vendors evaluated in this research. Features are released 18 to 24 months after competitors' releases. The vendor lags UTM models with integrated Wi-Fi, lacks user and device risk scoring integration in the security policy, and has just released sandboxing. The vendor does not provide integration with any endpoints — its own or a third party's — except for VPN connectivity and to allow Stormshield's endpoint to use the user directory hosted on a UTM appliance.

- Network sandboxing is unproven, requires the premium-priced Kaspersky Anti-Virus option, and is not available on the smaller UTM appliances. Surveyed customers noted that Stormshield's ability to support mobile devices, and to integrate them in the security policy, needs improvement compared with leading vendors of UTM products.
- Channel partners mention that the vendor lags behind Leaders in its marketing execution, and needs improvement to compete in the global market. They also report that the price list has recently become more complex and can negatively impact competitive positioning for distributed organizations.

## Untangle

Untangle is an IT security vendor, founded in 2003, with headquarters in San Jose, California. Untangle primarily serves small offices/home offices (SOHOs) and midsize organizations. Untangle NG Firewall is available in eight physical appliance models, including two models with integrated Wi-Fi. NG Firewall is predominantly sold as a software appliance installed by its SMB clients. The vendor also offers an endpoint antivirus, acquired in 2014 and primarily targeting consumers, under the Total Defense brand.

The Untangle NG Firewall management console relies on application racks, where selected applications for a chosen policy show up as clickable icons that open the configuration of the software module. The management interface is available in English, Chinese, Spanish, Portuguese, German and Italian.

With its 12.1 release, Untangle has updated its management interface, adding dashboard widgets and rethinking its embedded reporting. The version also improves performance and lets users authenticate through their Google or Facebook accounts. The vendor has also recently released a threat intelligence feed (ScoutIQ).

Untangle is a good shortlist contender for small and lower-midsize organizations, especially in North America. Upper-midsize organizations should evaluate their functionality and scaling needs against Untangle's capabilities.

### STRENGTHS

- Untangle offers a free version of its UTM, delivered as a software appliance, and discounted packages for government and nonprofits. Every application, including security features, is available for a 14-day trial.
- Untangle has a faithful client base in North America that gives very good marks to the intuitive interface and how it simplifies UTM deployment and operations.
- Untangle offers cost and functionality appropriate for SMBs. Its customer references indicate that total cost of ownership (TCO) is often lower than corresponding products from most competitors in the UTM market space.

### CAUTIONS

- Untangle claims more than 40,000 UTM installations and is profitable, but is one of the smallest vendors evaluated in this research, with fewer than 100 employees.

- Untangle makes most of its UTM sales in North America. Outside of this region, the vendor does not appear on Gartner client shortlists. Gartner estimates that more than 90% of Untangle's UTM customers have fewer than 500 employees.
- Untangle provides functionality relevant to companies that have a few locations and simple architecture, but it does not offer an appropriate solution for companies that are more heavily distributed, such as centrally managed retail or local government organizations.
- Untangle NG Firewall lacks a centralized management console and a cloud-based sandboxing option.

## Venustech

Venustech, headquartered in Beijing, China, is a large security vendor that was founded in 1996. Venusense UTM includes 38 models, with different models for the Chinese and international markets. Venusense UTM is also available as a virtual appliance. Management interface is available in Chinese, English and Japanese. Along with firewalls, Venustech's broad product portfolio comprises IPS, web application firewall, security information and event management (SIEM) and endpoint security.

In recent months, Venustech has introduced cloud-based sandboxing and launched virtual UTM appliances.

Venustech is evaluated as a Niche Player for the UTM market because it is a regional Chinese player, with the majority of its sales coming from banking and government clients in China. It's a good UTM contender for SMBs in China looking for local channel support and services. Prospective customers in other countries should first verify the availability of local technical skills for presales and postsales support.

### STRENGTHS

- Venustech has a strong local presence in China and a robust partner network, providing reliable local support and security operations center (SOC) services.
- The integration capabilities of Venusense UTM with Venusense endpoint management software, and the ability to share threat analysis results with the Venusense Advanced Persistent Threat (APT) solution, make it a good shortlist candidate for existing Venustech customers looking to improve their protection against malware.
- Its email security features include encryption for outbound emails and end-user quarantine, a feature which is highly valued by SMBs in that part of the region.
- Clients give high ratings to the UTM solution's antivirus catch rate, competitive price for upper midmarket use cases and ease of use.

### CAUTIONS

- Venustech is visible in Chinese government and banking shortlists, but faces strong competition from many local Chinese UTM players, as well as a few global vendors that have invested in the region and are more frequently seen in Gartner client's shortlists.

- More than 95% of Venustech's UTM clients are based in China. Its international development is nascent, starting with Japan. Prospective customers from other countries should verify the experience of its partners because the UTM may be a new solution for these partners.
- Venustech's UTM solution lacks an SSL decryption feature and provides limited visibility with its embedded reports. Clients would like to see a lower-priced, entry-level UTM for smaller offices.

## WatchGuard

Seattle-based WatchGuard is a privately held network security vendor. Established more than 20 years ago, WatchGuard is a well-established player in the UTM market. It provides UTM, secure email gateways and remote manageable wireless APs. The Firebox UTM product line includes 14 physical appliances, including appliances with embedded wireless capabilities, and XTMv, a virtual UTM solution.

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 four new Firebox appliances targeted at branch offices and SMB customers. New features include a wireless deployment map, rogue access detection, botnet mitigation and mobile security.

WatchGuard recently acquired the technology assets of Hexis Cyber Solutions' HawkEye G, a threat detection and response technology. Once integrated, the technology will provide the opportunity for WatchGuard to improve its advanced threat capabilities, adding endpoint presence.

WatchGuard is evaluated as a Visionary because of its ability to quickly respond with new software options to emerging needs from midmarket organizations. WatchGuard is a good shortlist candidate for SMB organizations and distributed enterprises, in any location, in need of a broad set of features or a cloud-based visibility and management console.

### 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 UTM performs well under load with all features enabled.
- WatchGuard customers tout the vendor support organization's ability to respond quickly and effectively to critical reported issues.
- 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.

### CAUTIONS

- Gartner SMB clients do not mention WatchGuard in their shortlists as frequently as they mention Leaders.

- WatchGuard customers report scalability issues with Dimension when hundreds of firewalls are under management.
- Gartner data indicates that WatchGuard grew slightly below UTM market average.
- The vendor's product strategy is significantly influenced by the use case of distributed organizations. It is too early to determine if recent acquisition of Hexis HawkEye will provide positive additions for SMB 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

- Untangle and Venustech were added in 2016.

#### Dropped

- No vendor was dropped, but gateprotect was renamed Rohde & Schwartz Cybersecurity.

## 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 $8 million in 2015, 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 with 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 $8 million threshold.

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

## Evaluation Criteria

### Ability to Execute

- **Product or Service:** Key features are weighted heavily, including:
    - Ease of deployment and operation
    - Console quality
    - Price and performance
    - Range of models
    - Secondary product capabilities (including logging, mobile device management, integrated Wi-Fi support and remote access)
    - The ability to support multifunction deployments
- **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. Presale and postsale 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.

**Table 1.** Ability to Execute Evaluation Cri

| **Evaluation Criteria** |
| --- |
| Product or Service |
| Overall Viability |
| Sales Execution/Pricing |
| Market Responsiveness/Record |
| Marketing Execution |
| Customer Experience |
| Operations |

*Source: Gartner (August 2016)*

## 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; it also includes 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 most important.

**Table 2.** Completeness of Vision Evaluation C

| **Evaluation Criteria** |
| --- |
| Market Understanding |

**Table 2.** Completeness of Vision Evaluation C

| Evaluation Criteria |
| --- |
| Marketing Strategy |
| Sales Strategy |
| Offering (Product) Strategy |
| Business Model |
| Vertical/Industry Strategy |
| Innovation |
| Geographic Strategy |

*Source: Gartner (August 2016)*

## 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 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 sees heavy competition regardless of region. The market growth is leveling out and becoming closer to the other network security markets.

For 2015, Gartner estimates that the UTM market grew at 18.0% to reach a total of approximately $2 billion.

Fortinet continues to own the largest market share in the UTM market (see Note 2) — with more than twice the revenue of its closest competitor, Dell SonicWALL — and grows faster than the market average. Vendors who had recent mergers now have various growth trajectory. Sophos (who acquired Cyberoam in 2014) continues to outgrow the market. French Stormshield (Merger between Arkoon and Netasq in 2013) grows slightly higher than market average, whereas its German competitor, Rohde & Schwarz (acquired gateprotect and Adyton in 2014), had almost flat revenue in 2015 (see "Market Share Analysis: Unified Threat Management (SMB Multifunction Firewalls), Worldwide, 2016 Update" ).

### The Best Use Case for UTM Is All-in-One SMB Security

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 very 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 focusing more on distributed organizations made of autonomous offices such as franchises. This drives vendors to spend more on a centralized management console, aimed at serving MSSPs and channel partners looking to automate repetitive provisioning and deployment tasks.

Most clients and resellers continue to understand UTM as multifunction SMB firewalls, but vendors shift naming strategy based on their best-fit use case. Many vendors include "enterprise firewall" in their product line name, even the vendors who primarily serve SMBs and drive their product roadmap more on increasing the number of available features than improving the depth and quality of each module. This context could create confusion in enterprise and SMB buyers' minds, but Gartner analysts did not observe this during client inquiry. In a survey of security and IT leaders about firewalls (see Note 3), there was a clear difference on how buyers perceive UTM and next-generation firewalls (NGFWs). When asking the question "Which of the following statements do you believe to be true with these products (next-generation firewall and UTM)?" answers show:

- A difference of 24 percentage points in favor of UTM (43% vs. 19%) for being a good fit for small organizations, and a difference of 17 points in favor of UTM for being a good fit for midsize businesses.
- Conversely, the difference is 32 points in favor of NGFWs for being a good fit for larger enterprises.

Clients also expect higher performance from NGFWs (plus 45 percentage points compared with UTM), but accept the compromise associated with UTM. The higher expectation for NGFWs on application visibility (plus 37 percentage points in favor of NGFWs) could be a surprise because most UTM platforms now claim to have application visibility and control features. However, Gartner observes vast discrepancies between UTM vendors in the number of applications handled, the ease of integration of applications in the security policy, and the quality of the reports and real-time dashboards.

## Growing Encrypted Traffic Makes SMBs Even More Blind to What Happens on Their Network

Of surveyed organizations with fewer than 1,000 employees, 83% have an in-house IT security team of five or fewer full-time employee (FTE), and 43% have two or fewer (see Note 3). With thin security staff, SMBs expect streamlined technology to minimize the time they spend managing the UTM or they delegate management to a service provider. When surveying UTM reseller and end-user references sent by vendors (see Note 4), they give the lowest score for the reporting feature and frequently express dissatisfaction with the quality and relevance of generated reports. Satisfaction on application visibility is also below the average score given to feature quality. With misfit monitoring capabilities, SMB security administrators turn away from using the UTM, and 10% of these midsize businesses even confess that they do

not monitor alerts at all. Another example of this weak point is that only a few UTM vendors offer a SaaS discovery report.

SMB organizations also face a growing need for SSL decryption, principally to enforce web-filtering policy and to prevent malware infection. A recent Cisco report shows that HTTPS ranged from 36.74% to 40.2% of the web traffic during the first four months of 2016. Secure web gateway vendor Blue Coat estimates that HTTPS represents 35% of the traffic, and grows 20% every year. Gartner clients have measured up to 80% of encrypted traffic. Blue Coat and Cisco also observe that malware slowly transitions from HTTP to HTTPS. [1]

Gartner estimates than less than 10% of SMB organizations decrypt HTTPS on their UTM. This means that 90% of the SMB organizations relying on UTM for web security are blind to the more advanced threats that use HTTPS for transport.

Decrypting SSL/TLS on a UTM 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.

## Adoption of New Features by SMB Organizations Takes Time

Vendors are still learning how to position network sandboxing and other recent security detection methods (threat intelligence feeds and command and control detection) when compared with incumbent antivirus and IPS options.

In a survey of security and IT leaders about firewalls (see Note 3):

- Only 23% of SMB organizations (n = 31) were already using network sandboxing, compared with 38% (n = 34) for enterprises with more than 10,000 employees.
- When asked about the top three security features needed for next product selection, 14% of organizations (n = 65) cited malware sandboxing.

Vendor references surveyed for this Magic Quadrant tend to be the more advanced users. Still:

- Only 10% of the end-user references report that they use cloud-based sandboxing.
- 27% of the UTM resellers answer that they typically deploy it (see Note 4).

Gartner estimates that SMB organizations would benefit from advanced malware protection, but the lack of cost-effective bundles that integrate AV and sandboxing often inflates the UTM budget beyond what SMB security buyers are ready to pay. SMB organizations should verify first their ability to manage the alerts and favor short-term subscriptions until cost-effective bundles become available.

A few vendors have now released integration between UTM and endpoint solutions for improved visibility and potentially faster incident remediation, but market adoption hasn't been noticeable yet.

Only 11% of respondents put integration with endpoint as one of the top three security features for their next UTM selection.

SMBs would face less severe organizational issues because they are more likely to have a single buying center for endpoint and network security solutions, but the vendors still struggle to demonstrate that the value is higher than the constraints. SMB organizations should always assess the quality of each solution compared with the competition, and then evaluate that there are real benefits of integrating both solutions from the same vendor.

## Is Cloud a Threat or an Opportunity for UTM?

More UTM 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.

Placing the management and monitoring consoles fully in the cloud is generally a first step. MSSPs like the turnkey solution, but end-user organizations should evaluate if hosting their firewall configuration, including the filtering policy, in the cloud is acceptable. Reporting and log retention are well-suited to the cloud, but not exclusively. More frequent user interface updates are also a real advantage. From an economic perspective, utilizing a cloud management solution should at least minimize the management costs. 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.

In the "Hype Cycle for Infrastructure Protection, 2016," Gartner has added a new technology called "firewall as a service," which Gartner defines as follows:

> Firewall as a service (FWaaS) is a firewall delivered as a cloud-based service or hybrid solution (that is, cloud plus on-premises appliances). The promise of FWaaS is to provide simpler and more flexible architecture by leveraging centralized policy management, multiple enterprise firewall features and traffic tunneling to partially or fully move security inspections to a cloud infrastructure.

The promise, especially for distributed organization and MSSPs, is to better manage complexity and reduce dependency on thick on-premises hardware such as UTM.

> It took eight years for cloud-based secure web gateway to represent 27% of the total market. Based on today's level of interest, the transition to the cloud could take more time for UTM.

As a nascent technology approach, the FWaaS still has limited visibility in SMB organizations:

- Only 13% of surveyed UTM client references will consider an FWaaS approach for their next UTM product refresh.
- Only 3% said that they are "very likely" to do so (see Note 4).

Gartner analysts hear slightly more frequently from distributed organizations that they consider shifting and lifting web security features from the UTM to a cloud-based

secure web gateway to reduce their dependency on the UTM and keep the same hardware for a longer time. Replacement of UTM by alternate solution is not a short-term alternative, and transition will take time.

## Evidence

[1] "Cisco 2016 Midyear Cybersecurity Report" (see page 2, and figure 24 on page 35); Blue Coat: "Encrypted Traffic Management"

## Note 1
## Small or Midsize Business Market Definition

Gartner generally defines SMBs by the number of employees and/or annual revenue they have. The primary attribute 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 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.

## Note 3
## Gartner Firewall and UTM Survey

In October 2015, Gartner surveyed 155 IT and business leaders with an IT component to their role on firewalls: 37% of respondents were from North America, 11% Latin America, 41% EMEA and 10% APAC region.

Respondents were required to have a knowledge base for firewall products and involvement in purchasing firewall products.

The survey was developed collaboratively by a team of Gartner analysts covering Technology and Service Providers, TSP Data Center and Security Research and was reviewed, tested and administered by Gartner's Research Data and Analytics team.

The results of this study are representative of the respondent base and not necessarily the market as a whole.

For the question on security team size, the number of respondent group is too small to be representative for the whole market (n = 40), but it gives a good indication of what Gartner observes when asking the same question during client inquiries.

# Note 4
# Gartner UTM Magic Quadrant Surveys

In the context of this Magic Quadrant research, Gartner asked every vendor to submit end-user and reseller references. Gartner then sent an online survey to these references and aggregated the answers. The 2016 surveys happened between February and April 2016, and included 102 end-user references and 74 reseller references.

Vendor reference samples tend to be biased toward the more complex end-user organizations and the larger or faithful resellers. This influences the results toward higher results when asking about feature adoption.

# 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.